Completeness Theorems for All Finite Stateless 2-Party Primitives

Daniel Kraschewski

Institute of Cryptography and Security, Department of Informatics,
Karlsruhe Institute of Technology, Germany

kraschew@ira.uka.de

Abstract

Since Kilian showed in 1988 that oblivious transfer (OT) is complete in the sense that every secure multi-party computation can be realized from this primitive, cryptographers are working on reductions of OT to various other primitives. A long-standing open question in this context is the classification of finite stateless 2-party primitives (so-called "cryptogates"), i.e. trusted black boxes that can be jointly queried by two parties, have finite input and output alphabets, and do not change behavior depending on time or input history. Over the decades, completeness criteria have been found for deterministic cryptogates (i.e. primitives without internal randomness), noisy channels, and symmetric (i.e., both parties receive the same output) or asymmetric (i.e., only one party receives any output at all) randomized cryptogates. However, the known criteria for randomized primitives other than noisy channels only hold in presence of passive adversaries (i.e., even corrupted parties still follow the protocol).

We complete this line of research by providing simple but comprehensive combinatorial completeness criteria for *all* finite stateless 2-party primitives. I.e., for the first time there are completeness criteria for randomized primitives that are neither symmetric nor asymmetric (but give different outputs to the querying parties), and we overcome the limitation that previous results for randomized primitives with input from *both* parties only regarded passive adversaries. A fundamental tool of our approach is a powerful lemma from real algebraic geometry, which allows us to base a cryptographic security proof on a rather "game-theoretic" approach.

As a corollary of our work, every non-complete example of a finite stateless 2-party primitive is essentially symmetric. This relationship between non-completeness and symmetric output behavior was previously only known for *deterministic* cryptogates.

Keywords: oblivious transfer, complete primitives, information-theoretic security, universal composability, secure function evaluation.

Contents

1 Introduction

Oblivious transfer was introduced in [Rab81] as a trusted erasure channel. Later, in [Cré88] it was proven to be equivalent to $\binom{2}{1}$-OT, its currently most used variant, which allows a designated receiver Bob to learn only one of two bits sent by a designated sender Alice. Since the OT primitive turned out to be complete in the sense that it allows for arbitrary secure multi-party computation [Kil88, GL91, CGT95, IPS08], for numerous primitives it has been investigated whether OT can be reduced to them. In our work we exhaustively treat this question for a class of primitives that we call "finite randomized 2-party functions". Each such primitive is characterized by some finite alphabets $\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}$, a probability distribution $\mathcal{R}$ with finite support R and a mapping $f : \Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}} \times R \to \Omega_{\mathrm{A}} \times \Omega_{\mathrm{B}}$. Upon input $x \in \Upsilon_{\mathrm{A}}$ from Alice and $y \in \Upsilon_{\mathrm{B}}$ from Bob, the primitive internally samples a random $r \leftarrow \mathcal{R}$, computes $(a, b) = f(x, y, r)$ and outputs a to Alice and b to Bob. Equally, one can characterize any finite randomized 2-party function by its input and output alphabets $\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}$ and a family $\{\phi_{x,y}\}_{x\in\Upsilon_{\mathrm{A}}, y\in\Upsilon_{\mathrm{B}}}$ of probability mass functions over $\Omega_{\mathrm{A}} \times \Omega_{\mathrm{B}}$, such that on input $x \in \Upsilon_{\mathrm{A}}$ from Alice and $y \in \Upsilon_{\mathrm{B}}$ from Bob the primitive with probability $\phi_{x,y}(a, b)$ outputs a to Alice and b to Bob. Regarding our work, the latter notation turns out much more convenient and therefore will be used throughout the body of this paper.

Our work generalizes the results of [KMQ11], where the completeness question was solved for the special case of *deterministic* 2-party functions, i.e. $f(x, y, r)$ is independent of the randomness r, or alternatively $\{\phi_{x,y}\}_{x\in\Upsilon_{\mathrm{A}}, y\in\Upsilon_{\mathrm{B}}} \subseteq \{0, 1\}^{\Omega_{\mathrm{A}}\times\Omega_{\mathrm{B}}}$. Although some general ideas from the deterministic case do carry over straightforwardly, crucial techniques do not—cf. [KMQ10, Section 5]. In addition to an appropriate representation of randomized functions, we need to develop an entire tool set of technical lemmata, some of which may be of independent interest.

1.1 Related work

General related work. In the literature one finds OT protocols for bounded-classical-storage [CCM98] and bounded-quantum-storage models [DFR$^+$07] as well as noisy classical [CK88, DKS99, DFMS04, CMW05, Wul09, IKO$^+$11] and quantum channels [Yao95, May95, May96], the latter taking commitments for granted. An entire line of research deals with implementing OT from tamper-proof hardware assumptions [BOGKW88, GKR08, CGS08, Kol10, GIMS10, GIS$^+$10, DKMQ11, CKS$^+$11]. There are reductions of $\binom{2}{1}$-OT to weaker OT versions that leak additional information [CK90, DKS99, Wul07] and to Rabin-OT [Cré88]. OT-combiners implement OT from granted sets of OTs with faulty members [MPW07, HIKN08]. For reversing the direction of $\binom{2}{1}$-OT a protocol is known with optimal number of OT queries [WW06]. Relative to computational assumptions, all-or-nothing laws have been shown [BMM99, HNRR06, MPR10], i.e. all considered non-trivial primitives are complete.

Precursory results to our work. The line of research we deal with in this paper was initiated by [Kil91], where completeness criteria for deterministic symmetric 2-party functions (i.e., both parties receive the same output, computed deterministically from their inputs) without any additional computational assumptions were provided. This line of research was continued by [Kil00], providing completeness criteria for deterministic asymmetric 2-party functions (i.e., only one party receives any meaningful output, computed deterministically from both parties' inputs). Randomized symmetric and asymmetric 2-party functions (i.e., a single output symbol, computed from both parties inputs and some secret randomness, is handed over either to both parties or only to one party) were also treated in [Kil00], but only with respect to passive adversaries (i.e., even corrupted parties still follow the protocol). Rather recently, the completeness criteria of [Kil91, Kil00] for deterministic 2-party functions were unified and generalized by [KMQ11], now covering *all* deterministic 2-party functions, what for the first time in the literature also included 2-party functions that give different outputs to Alice and Bob. Meanwhile, [CMW05] also provided exhaustive completeness criteria with respect to active adversaries (i.e., corrupted parties may arbitrarily deviate from the protocol) for a special class of randomized asymmetric 2-party functions, namely noisy channels. We now complete this line of research. Our main theorem unifies and generalizes all known completeness criteria for symmetric, asymmetric, deterministic and randomized 2-party functions.

Independently of our work, a unified and generalized formulation of the completeness criteria from [Kil91, Kil00, CMW05, KMQ11] was found by [MPR12]. Their result is equivalent to our criteria, but they only give a proof with respect to passive adversaries. Proving their conjecture for active adversaries was left as an open problem.

1.2 Our contribution

Results. We give a complete characterization of *all* finite randomized 2-party functions that allow for information-theoretically secure implementation of OT. For the reduction we provide a protocol scheme, which is universally composable—cf. [Can01]. Our characterization is based on surprisingly simple combinatorial criteria and our results are tight: Necessity of our criteria still holds, even if only correctness and privacy of the implemented OT are required. As a remarkable corollary of our work all non-complete finite 2-party functions turn out essentially symmetric.

Our work exceeds known completeness criteria in two ways. Firstly, we overcome the limitation that previous results for randomized primitives with input from *both* parties only regarded passive adversaries. Secondly, our results also cover randomized primitives that are neither symmetric nor asymmetric (but give different meaningful outputs to Alice and Bob).

Techniques. Our starting point is a very generic protocol scheme, such that all perfectly undetectable attack strategies do comply with certain polynomial equations and hence form an algebraic variety. One major part of our work consists in finding protocol parameters, such that this algebraic variety collapses to trivial attack strategies that do not affect security at all. Using powerful tools from real algebraic geometry (namely the Łojasiewicz Inequality) and probability theory (namely the Hoeffding Inequality), we can then link real protocol runs to idealized attack strategies and thereby prove cryptographic security of our construction. This approach for protocol design and proving security might be of further interest, independently of our concrete classification results.

1.3 Organization of this paper

The basic structure of this paper follows [KMQ11], though nearly all technical details in our case are way more complex. We briefly present our results in Section 2, where we first refer to the used notion of security (Section 2.1), then introduce the basic concepts needed for formulation of our results (Section 2.2), state our classification results (Section 2.3), and finally give a short overview about how our approach matches former completeness criteria in the literature (Section 2.4). In Section 3 we give an exposition of how one can prove our results. All formal proofs of our main technical contribution are located in Section 4; to make it self-contained, all needed definitions, notations and lemmata from the rest of the paper are also restated there.

2 Presentation of our results

Before we get started, we introduce two handy notations, which will make things much easier in the upcoming sections.

Functionality: $\mathcal{F}_{\mathrm{SFE}}^{(F)}$

Let F be characterized by a family of probability mass functions $\{\phi_{x,y}\}_{x\in\Upsilon_{\mathrm{A}},y\in\Upsilon_{\mathrm{B}}} \subseteq \mathrm{pmf}(\Omega_{\mathrm{A}}\times\Omega_{\mathrm{B}})$, where $\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}$ are Alice's input and output alphabet and $\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}$ are Bob's input and output alphabet.

- Upon receiving input (x,i) from Alice, verify that $(x,i) \in \Upsilon_{\mathrm{A}}\times\mathbb{N}$ and that there is no recorded tuple $(\tilde{x}, i, \texttt{Alice})$; else ignore that input. Next, record $(x, i, \texttt{Alice})$ and send $(\texttt{processing}, \texttt{Alice}, i)$ to the adversary.
- Upon receiving input (y,i) from Bob, verify that $(y,i) \in \Upsilon_{\mathrm{B}}\times\mathbb{N}$ and that there is no recorded tuple $(\tilde{y}, i, \texttt{Bob})$; else ignore that input. Next, record $(y, i, \texttt{Bob})$ and send $(\texttt{processing}, \texttt{Bob}, i)$ to the adversary.
- As soon as there are recorded tuples $(x, i, \texttt{Alice})$ and $(y, i, \texttt{Bob})$ for the same index i, generate randomly $(a,b) \in \Omega_{\mathrm{A}}\times\Omega_{\mathrm{B}}$ according to the distribution specified by $\phi_{x,y}$, and store (a, b, i).
- Upon receiving a message $(\texttt{Delivery}, \texttt{Alice}, i)$ from the adversary, verify that there is a stored tuple (a, b, i); else ignore that message. Next, output (a, i) to Alice and henceforth ignore all messages $(\texttt{Delivery}, \texttt{Alice}, i)$ with the same index i.
- Upon receiving a message $(\texttt{Delivery}, \texttt{Bob}, i)$ from the adversary, verify that there is a stored tuple (a, b, i); else ignore that message. Next, output (b, i) to Bob and henceforth ignore all messages $(\texttt{Delivery}, \texttt{Bob}, i)$ with the same index i.

When a party is corrupted, the adversary is granted unrestricted access to the channel between $\mathcal{F}_{\mathrm{SFE}}^{(F)}$ and the corrupted party, including the ability of deleting and/or forging arbitrary messages; i.e., the adversary can arbitrarily send and receive messages on behalf of the corrupted party.

Figure 1: The ideal functionality for secure evaluation of a 2-party function F. Adapted and simplified version of the Secure Function Evaluation functionality in [Can01]. Note that via the parameter i only the same multi-session ability is achieved as in [Can01] by multiple session IDs.

Finite sums of function values: Given any set T with finite subset $S \subseteq T$ and some mapping $g : T \to \mathbb{R}$, let $g(S) := \sum_{\omega\in S} g(\omega)$. For functions with more arguments we use the canonical extension of this notation, e.g. $h(a, B, C, d) := \sum_{\beta\in B,\gamma\in C} h(a, \beta, \gamma, d)$.

Spaces of probability mass functions: Given some finite alphabet Ω, we denote the set of all probability mass functions over Ω by $\mathrm{pmf}(\Omega)$, i.e. $\mathrm{pmf}(\Omega) = \big\{\rho : \Omega \to \mathbb{R}_{\geq 0} \;\big|\; \rho(\Omega) = 1\big\}$.

We also use the following standard notions.

Negligibility: A function $\mu : \mathbb{N} \to \mathbb{R}_{\geq 0}$ is negligible (in the parameter k), if $\lim_{k\to\infty} \mu(k)\cdot f(k) = 0$ for every polynomial $f \in \mathbb{R}[X]$.

Indistinguishability: Two random variables X, Y are (statistically) indistinguishable, if their statistical distance $\frac{1}{2}\sum_{\alpha}\big|\mathbf{P}[X = \alpha] - \mathbf{P}[Y = \alpha]\big|$ is negligible in some security parameter.

2.1 Notion of security

Our main contribution is the construction and security proof of a generic reduction protocol that implements OT from any appropriate 2-party function. For the definition what "security" means, we lean on one of the strongest commonly used notions of security: the Universal Composability (UC) framework of [Can01]. However, our results also hold with respect to all weaker security notions that still require secure function evaluation to be private (i.e., no party can learn anything that cannot be learned from its function input and function output) and correct (i.e., if all parties follow the protocol, the desired function value is evaluated correctly).

In the UC framework, security is defined by comparison of an *ideal model* and a *real model*. The protocol of interest is running in the latter, where an adversary $\mathcal{A}$ coordinates the behavior of all corrupted parties. In the ideal model, which is secure by definition, an ideal functionality $\mathcal{F}$ implements the desired protocol task and a simulator $\mathcal{S}$ tries to mimic the actions of $\mathcal{A}$. An environment $\mathcal{Z}$ is plugged either to the ideal or the real model and has to guess, which model it is actually plugged to. When $\mathcal{Z}$ cannot distinguish between ideal and real model, the protocol is considered *UC-secure*. More formally, UC-security requires that for every adversary $\mathcal{A}$ there exists a simulator S, such that for all environments $\mathcal{Z}$ the view of $\mathcal{Z}$ in the real model (with adversary $\mathcal{A}$) is indistinguishable from the view of $\mathcal{Z}$ in the ideal model (with simulator $\mathcal{S}$). Since all our results are of information-theoretic nature, the adversarial entities $\mathcal{A}, \mathcal{S}$ and the environment $\mathcal{Z}$ are computationally unbounded (but nonetheless the running time of a simulator $\mathcal{S}$ will always be polynomial in the running time of the according adversary $\mathcal{A}$, as it is usually desired).

If the views of $\mathcal{Z}$ in the ideal model and the real model are distributed identically, we speak of *perfect* security; if there is some negligible statistical distance between these views, we have only *statistical* security. As already mentioned, one also differentiates between *passive* adversaries (i.e., corrupted parties still follow the protocol) and *active* adversaries (i.e., corrupted parties may deviate from the protocol arbitrarily). For further details we refer to [Can01].

Since our protocol scheme implements $\binom{2}{1}$-OT from some given 2-party function, we also need a so-called *hybrid functionality* in the real model that provides access to the latter. See Figure 1 for a formal definition of the hybrid functionality used. As $\binom{2}{1}$-OT itself is just a special 2-party function that on input $(b_0, b_1) \in \{0,1\}^2$ from Alice and $c \in \{0,1\}$ from Bob with probability 1 outputs b_c to Bob and a special "nothing" symbol $\perp$ to Alice, we can omit an explicit definition of the ideal OT functionality and instead use an accordingly instantiated version of the functionality from Figure 1.

2.2 Basic concepts

Finite randomized 2-party functions. A finite randomized 2-party function can be characterized by its input and output alphabets and output distributions (cf. Figure 1). By $\mathfrak{F}_{\mathsf{fin}}$ we denote the set of all tuples $(\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi)$, where $\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}$ are non-empty finite alphabets and $\phi := \{\phi_{x,y}\}_{x \in \Upsilon_{\mathrm{A}}, y \in \Upsilon_{\mathrm{B}}}$ is a family of probability mass functions over $\Omega_{\mathrm{A}} \times \Omega_{\mathrm{B}}$, i.e. $\phi \subseteq \mathrm{pmf}(\Omega_{\mathrm{A}} \times \Omega_{\mathrm{B}})$. The intuition behind this is that the considered 2-party function on input $x \in \Upsilon_{\mathrm{A}}$ from Alice and $y \in \Upsilon_{\mathrm{B}}$ from Bob outputs a to Alice and b to Bob with probability $\phi_{x,y}(a,b)$.

For convenience we will not always differentiate pedantically between the mathematical object $F \in \mathfrak{F}_{\mathsf{fin}}$ and the corresponding primitive $\mathcal{F}_{\mathrm{SFE}}^{(F)}$, but from the context should always be clear what is meant.

Canonical and condensed canonical representations. Our notion of $\mathfrak{F}_{\mathsf{fin}}$ turns out a bit too detailed, since Alice and Bob can always locally relabel their input-output tuples without any side effects. For our purposes there is no need to distinguish between some $F \in \mathfrak{F}_{\mathsf{fin}}$ and any relabeled version of F. Therefore, we introduce the concept of *canonical representations*. Given any $F \in \mathfrak{F}_{\mathsf{fin}}$, we cannot just write down a function table for F, since each input tuple only specifies an output distribution rather than a concrete output tuple. However, for each individual input tuple we can represent the respective joint output distribution by a probability matrix with rows labeled by Alice's output symbols and columns labeled by Bob's output symbols. Then, we can arrange these "inner" probability matrices in an "outer" block matrix with rows labeled by Alice's input symbols and columns labeled by Bob's input symbols (see first two tables in Figure 2 for an example).

Moreover, we also want to abstract from the fact that, e.g., Bob could always concatenate the result of a local coin toss to his output, thus formally doubling the size of his output alphabet just by

$$\begin{array}{cc|cc|cc|cc|}
 & & \mathbf{0} & & \mathbf{1} & & \mathbf{2} & \\
 & & \mathit{0} & \mathit{1} & \mathit{0} & \mathit{1} & \mathit{0} & \mathit{1} \\ \hline
\mathbf{0} & \mathit{0} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{2} \\
 & \mathit{1} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{2} \\ \hline
\mathbf{1} & \mathit{0} & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{3} & 0 & 0 \\
 & \mathit{1} & \frac{1}{4} & \frac{1}{4} & \frac{1}{3} & \frac{1}{3} & 0 & 1 \\ \hline
\end{array}
\qquad
\begin{array}{|cc|cc|c|} \hline
\frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \\
\frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \\ \hline
\frac{1}{4} & \frac{1}{4} & & \frac{1}{3} & \\
\frac{1}{4} & \frac{1}{4} & \frac{1}{3} & \frac{1}{3} & 1 \\ \hline
\end{array}
\qquad
\begin{array}{|c|cc|c|} \hline
1 & \frac{1}{2} & \frac{1}{2} & 1 \\ \hline
\frac{1}{2} & & \frac{1}{3} & \\
\frac{1}{2} & \frac{1}{3} & \frac{1}{3} & 1 \\ \hline
\end{array}$$

Figure 2: Different representations of a 2-party function that on input $x \in \{0,1\}$ from Alice and $y \in \{0,1,2\}$ from Bob outputs some uniformly random $a, b \in \{0,1\}$, subject to the condition that $a + b \geq x \cdot y$ and $b \geq y - 1$. To the left, inputs (bold) and outputs (italic) are displayed grayed out. The matrix in the middle is a *canonical representation* of the same 2-party function with zero probabilities omitted for better readability; the right matrix is a *condensed canonical representation.*

an easily reversible local computation. Such local coin tosses appear in a canonical representation as pairwise linearly dependent columns within the same block column, or pairwise linearly dependent rows within the same block row respectively. However, we can easily get rid of them just by adding up the respective linearly dependent rows or columns. If all local coin tosses are removed from a canonical representation this way, we call it *condensed* (cf. last table in Figure 2).

Isomorphism. Note that the condensed canonical representation of a finite 2-party function is unique up to permutations of rows within single block rows, permutations of columns within single block columns, and permutation of rows and/or columns of the outer block matrix. Now, if two given 2-party functions $F, F' \in \mathfrak{F}_{\mathsf{fin}}$ have the same (set of) condensed canonical representations, we call them *isomorphic.* Obviously, isomorphism is an equivalence relation on $\mathfrak{F}_{\mathsf{fin}}$ and any two isomorphic 2-party functions $F, F' \in \mathfrak{F}_{\mathsf{fin}}$ can be straightforwardly implemented from each other with perfect security.

Redundancy and equivalence. Our notion of isomorphism will turn out very handy for formulation of our classification results with respect to passive adversaries, but for active adversaries we need one additional concept. In particular, there may exist input symbols that a corrupted party never needs to use, since one can always learn strictly more by inputting something else. Given any $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$, we call an input symbol $y' \in \Upsilon_{\mathrm{B}}$ *redundant*, if a corrupted Bob instead of sending y' to F can always replace this input by an appropriately distributed random choice from $\Upsilon_{\mathrm{B}} \setminus \{y'\}$ and still perfectly simulate honest behavior. This is possible, if Alice's output distribution is not changed at all and Bob can reconstruct an appropriately distributed output $b' \in \Omega_{\mathrm{B}}$ from his actual input-output tuple (y, b). Formally, $y' \in \Upsilon_{\mathrm{B}}$ is *redundant*, if there exist an "input replacement strategy" $\iota \in \mathrm{pmf}(\Upsilon_{\mathrm{B}})$ and an "output reconstruction strategy" $\{\lambda_{y,b}\}_{y \in \Upsilon_{\mathrm{B}}, b \in \Omega_{\mathrm{B}}} \subseteq \mathrm{pmf}(\Omega_{\mathrm{B}})$, such that $\iota(y') = 0$ and for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $b' \in \Omega_{\mathrm{B}}$ it holds:

$$\phi_{x,y'}(a, b') = \sum\nolimits_{y \in \Upsilon_{\mathrm{B}},\, b \in \Omega_{\mathrm{B}}} \iota(y) \cdot \phi_{x,y}(a, b) \cdot \lambda_{y,b}(b')$$

For input symbols $x \in \Upsilon_{\mathrm{A}}$, redundancy is defined analogously. If neither Υ_{A} nor Υ_{B} contains any redundant input symbols, we say that F is *redundancy-free.*

W.l.o.g., malicious parties never use redundant input symbols, since they can gather exactly the same or even strictly more information by the respective input replacement and output reconstruction strategies. Also, there is no need to constrain what honest parties may learn. Therefore, regarding active adversaries we can consider any 2-party functions *equivalent* when they only differ in some redundant input symbols. Formally, any 2-party functions $F, F' \in \mathfrak{F}_{\mathsf{fin}}$ are *equivalent*, if they can be made isomorphic by successive removal of redundant input symbols. Note that a step-by-step removal of one symbol at a time is crucial here: There may exist two input symbols that are both redundant, but after removing one of them, the other one is not redundant any more—e.g., $\Upsilon_{\mathrm{B}} = \{y, y'\}$ with $\phi_{x,y}(a,b) = \phi_{x,y'}(a,b)$ for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $b \in \Omega_{\mathrm{B}}$.

It will turn out that the *redundancy-free version* of any given $F \in \mathfrak{F}_{\mathsf{fin}}$ is unique up to isomorphism and thus equivalence of 2-party functions in the sense above is indeed an equivalence relation on $\mathfrak{F}_{\mathsf{fin}}$. However, due to lack of some required technical tools at this point, we postpone the proof to Section 4.3 (see Corollary 19).

2.3 Completeness criteria for *all* finite randomized 2-party functions

With the concepts from Section 2.2 we can now formulate our classification results. We just state the mere assertions here; for an outline of the proof we refer to Section 3.

Definition (OT-cores)**.** Given $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$, an *OT-core* of F is a non-diagonal full-rank 2×2-submatrix of the canonical representation; i.e., for the corresponding input-output tuples $(x,a), (x',a') \in \Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}$ and $(y,b), (y',b') \in \Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}}$ we have the following inequation with at most one zero factor:

$$\phi_{x,y}(a,b) \cdot \phi_{x',y'}(a',b') \neq \phi_{x',y}(a',b) \cdot \phi_{x,y'}(a,b')$$

In this situation, we also call $\big\{(x,a),(x',a')\big\} \times \big\{(y,b),(y',b')\big\}$ an *OT-core* of F.

Theorem (Classification Theorem)**.** *For every $F \in \mathfrak{F}_{\mathsf{fin}}$ it holds:*

1. *OT can be implemented from $\mathcal{F}_{\mathrm{SFE}}^{(F)}$ statistically secure against* passive *adversaries, iff F has an OT-core.*
2. *OT can be implemented from $\mathcal{F}_{\mathrm{SFE}}^{(F)}$ statistically secure against* active *adversaries, iff the redundancy-free version of F has an OT-core.*

Definition (Symmetric 2-party functions)**.** A 2-party function $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ is *symmetric*, if $\phi_{x,y}(a,b) = 0$ for all $x \in \Upsilon_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$, $a \in \Omega_{\mathrm{A}}$, $b \in \Omega_{\mathrm{B}}$ with $a \neq b$.

Lemma (Symmetrization Lemma)**.** *Every 2-party function $F \in \mathfrak{F}_{\mathsf{fin}}$ that has no OT-core (and thus by our Classification Theorem is not complete) is isomorphic to a symmetric 2-party function.*

2.4 Comparison with criteria from the literature

The latest known completeness criteria[1] for finite 2-party functions can be subsumed by the following four theorems.

[KMQ11, Theorem 1]: A deterministic 2-party function $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ allows for implementation of OT statistically secure against *passive* adversaries, iff for the mappings $f_{\mathrm{A}} : \Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}} \to \Omega_{\mathrm{A}}$ defined by $f_{\mathrm{A}}(x,y) = a :\Leftrightarrow \phi_{x,y}(a, \Omega_{\mathrm{B}}) = 1$ and $f_{\mathrm{B}} : \Upsilon_{\mathrm{A}} \times \Upsilon_{\mathrm{B}} \to \Omega_{\mathrm{B}}$ defined by $f_{\mathrm{B}}(x,y) = b :\Leftrightarrow \phi_{x,y}(\Omega_{\mathrm{A}}, b) = 1$ there exist $x, x' \in \Upsilon_{\mathrm{A}}$ and $y, y' \in \Upsilon_{\mathrm{B}}$, such that $f_{\mathrm{A}}(x,y) = f_{\mathrm{A}}(x,y')$, $f_{\mathrm{B}}(x,y) = f_{\mathrm{B}}(x',y)$, and $\big(f_{\mathrm{A}}(x',y), f_{\mathrm{B}}(x,y')\big) \neq \big(f_{\mathrm{A}}(x',y'), f_{\mathrm{B}}(x',y')\big)$.
A deterministic 2-party function $F \in \mathfrak{F}_{\mathsf{fin}}$ allows for implementation of OT statistically secure against *active* adversaries, iff its redundancy-free version allows for implementation of OT statistically secure against passive adversaries by the criterion above.

[1] Meanwhile, a unification and generalization of these criteria has been found by an independent work [MPR12]. Their criteria are equivalent to ours, but they give only a proof with respect to passive adversaries.

[CMW05, Main result]: A noisy channel allows for implementation of OT statistically secure against *active* adversaries, iff its redundancy-free version is no parallel composition of noiseless and/or capacity-zero channels.

[Kil00, Theorem 1.3]: An asymmetric $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \{\bot\}, \Omega, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ allows for implementation of OT statistically secure against *passive* adversaries, iff there exist $x, x' \in \Upsilon_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$ and $z, z' \in \Omega$, such that $\phi_{x,y}(\bot, z) > \phi_{x',y}(\bot, z) > 0$ or it holds that $\phi_{x,y}(\bot, z) > 0$, $\phi_{x',y}(\bot, z) > 0$, $\phi_{x,y'}(\bot, z') > 0$ and $\phi_{x',y'}(\bot, z') = 0$.

[Kil00, Theorem 1.2]: A symmetric $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega, \Omega, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ allows for implementation of OT statistically secure against *passive* adversaries, iff there exist $x, x' \in \Upsilon_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$, $z \in \Omega$, such that $\phi_{x,y}(z, z) > 0$, $\phi_{x,y'}(z, z) > 0$ and $\phi_{x,y}(z, z) \cdot \phi_{x',y'}(z, z) \neq \phi_{x,y'}(z, z) \cdot \phi_{'x,y}(z, z)$.

It is straightforward to verify that all these completeness criteria are direct corollaries of our Classification Theorem. However, the literature cited above differs substantially in the used protocol constructions and also the proof techniques. Our approach is most comparable with that of [KMQ11], who also provided a Symmetrization Lemma for deterministic 2-party functions. We generalize their notions of "redundancy" (q.v. Section 2.2), "OT-cores" (q.v. Section 2.3) and "cheating situations" (q.v. Section 3.1.2), and we also adopt their basic protocol scheme for generation of correlated data (q.v. Section 3.1.1). However, due to increased complexity the similarities are limited to a fairly abstract level. Core proof techniques of [KMQ11] are strictly bound to the deterministic case—cf. [KMQ10, Section 5]—and therefore new solutions (including a powerful lemma from real algebraic geometry, q.v. Section 4.6) are needed for randomized primitives.

3 How to prove the Classification Theorem

Necessity of our criteria. By our Symmetrization Lemma and [Kil00, Theorem 1.2] it directly follows that OT-cores are necessary for completeness with respect to passive adversaries. Moreover, the proof in [Kil00, Section 4.1] for necessity of OT-cores holds in the same way with respect to active adversaries. So, at this point we only need to give a proof for the Symmetrization Lemma.

Proof-sketch. Let some arbitrary $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ be given that has no OT-core. We have to show that F is symmetric up to isomorphism. Our first observation is that we can replace Bob's output symbols by normalized versions of the respective column vectors in the condensed canonical representation of F, i.e. upon Bob's input y we replace his function output b by the following $\mathbb{R}^{\Upsilon_\mathrm{A} \times \Omega_\mathrm{A}}$-vector:

$$\frac{1}{\phi_{\Upsilon_\mathrm{A},y}(\Omega_\mathrm{A}, b)} \cdot \big(\phi_{x,y}(a, b)\big)_{x \in \Upsilon_\mathrm{A}, a \in \Omega_\mathrm{A}}$$

Since by construction there are never any two linearly dependent columns within the same block column of a condensed canonical representation, this replacement of output symbols is an isomorphism of 2-party functions. Analogously, we can replace Alice's output symbols; let $\hat{\Omega}_\mathrm{A} \subseteq \mathbb{R}^{\Upsilon_\mathrm{B} \times \Omega_\mathrm{B}}$ and $\hat{\Omega}_\mathrm{B} \subseteq \mathbb{R}^{\Upsilon_\mathrm{A} \times \Omega_\mathrm{A}}$ denote the new output alphabets.

Now we exploit that F has no OT-core. Given any $\hat{a} \in \hat{\Omega}_\mathrm{A}$ and $\hat{b}, \hat{b}' \in \hat{\Omega}_\mathrm{B}$ with $\phi_{\Upsilon_\mathrm{A},\Upsilon_\mathrm{B}}(\hat{a}, \hat{b}) > 0$ and $\phi_{\Upsilon_\mathrm{A},\Upsilon_\mathrm{B}}(\hat{a}, \hat{b}') > 0$, it must hold that $\hat{b} = \hat{b}'$, as otherwise the two-column matrix $(\hat{b}, \hat{b}')$ would contain a non-diagonal full-rank 2×2-matrix and thereby we had an OT-core. Analogously, for all $\hat{a}, \hat{a}' \in \hat{\Omega}_\mathrm{A}$ and $\hat{b} \in \hat{\Omega}_\mathrm{B}$ with $\phi_{\Upsilon_\mathrm{A},\Upsilon_\mathrm{B}}(\hat{a}, \hat{b}) > 0$ and $\phi_{\Upsilon_\mathrm{A},\Upsilon_\mathrm{B}}(\hat{a}', \hat{b}) > 0$ it must hold that $\hat{a} = \hat{a}'$. Thus, Alice and Bob have always full information about each other's output and the function can as well announce the complete output tuple $(\hat{a}, \hat{b})$ to both of them in the first place. □

Sufficiency in the passive case. Given some $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, \phi) \in \mathfrak{F}_\mathsf{fin}$ that has an OT-core, and given that there is only a passive adversary, we can easily implement a non-trivial noisy channel (shown to be complete in [CMW05, Wul09, IKO$^+$11]) by the following protocol:

0. Alice's channel input alphabet S is the set of all her possible input-output tuples for F, i.e., $S = \big\{(x,a) \in \Upsilon_\mathrm{A} \times \Omega_\mathrm{A} \;\big|\; \phi_{x,\Upsilon_\mathrm{B}}(a, \Omega_\mathrm{B}) > 0\big\}$. Let k denote the security parameter.
1. Alice and Bob query F for k times with uniformly random input, thus generating input-output tuples $(x_1, a_1), \ldots, (x_k, a_k) \in \Upsilon_\mathrm{A} \times \Omega_\mathrm{A}$ and $(y_1, b_1), \ldots, (y_k, b_k) \in \Upsilon_\mathrm{B} \times \Omega_\mathrm{B}$ respectively.
2. Alice announces some $i \in \{1, \ldots, k\}$, chosen such that (x_i, a_i) is her intended channel input.
3. Bob's noisy channel output is (y_i, b_i).

Since F has an OT-core and even corrupted parties still follow the protocol, the implemented channel is not completely decomposable into noiseless channels and/or channels with zero capacity. This is straightforward to verify and suffices to implement OT by the abovementioned literature.

Sufficiency in the active case. As we are already done with necessity of our criteria in the active and passive case and also sufficiency in the passive case, so to speak "75%" of our Classification Theorem are proven. However, the vastly major part still lies ahead of us. For proving sufficiency in the active case, i.e. proving that in presence of an active adversary OT can still be reduced to any redundancy-free 2-party function that has some OT-core, we need an entire new tool set of technical lemmata and several sophisticated results from the literature. The high level idea of the reduction approach is as follows. First, Alice and Bob generate some amount of correlated data by repeatedly querying the given 2-party function with random input. Within a subsequent test step each party has to partially unveil its data, so that significant cheating can be detected. Then, in a similar approach as in the passive case, the remaining data is used for implementation of non-trivial noisy channels: Alice just announces her channel inputs one-time-pad encrypted with her part of the correlated data, and Bob, since his view gives him only partial information about the used one-time pads, can only recover noisy versions of Alice's channel inputs. However, things will turn out a bit more complicated than in the passive case, since corrupted parties can try to gather some additional information by occasionally deviating from the protocol.

The first part (secure generation of correlated data, q.v. Section 3.1) is much more challenging than the second part (building OT from correlated data, q.v. Section 3.2). The former needs numerous novel techniques (see Section 4 for the formal proofs), whereas the latter mainly consists in rather straightforward adaptions of nowadays folklore techniques from the literature.

3.1 Secure generation of correlated data

In this section we explain how one can securely generate non-trivially correlated data from any redundancy-free 2-party function that has some OT-core. The main idea, borrowed from [KMQ11], is to use inputs belonging to a specific OT-core with relatively high probability and all other inputs only with relatively low probability—the latter will just serve for test purposes. In the first instance, we refer to [KMQ11, Section 3.1] for a discussion why an all-over uniform input distribution is not suitable and why still all input symbols have to be used with some significant probability. Since deterministic 2-party functions are only a special case of randomized 2-party functions, their arguments especially hold for our situation. However, note that our example in Figure 3.a also illustrates the problem with all-over uniform input distributions. In this example, a corrupted Bob can substitute a query on the first input symbol and a query on the second input symbol by two queries on the third input symbol. So, instead of uniformly choosing from his complete input alphabet, he can always input the last input symbol and thereby always get full information about Alice's input-output tuple. Furthermore, note that our example in Figure 3.b also illustrates

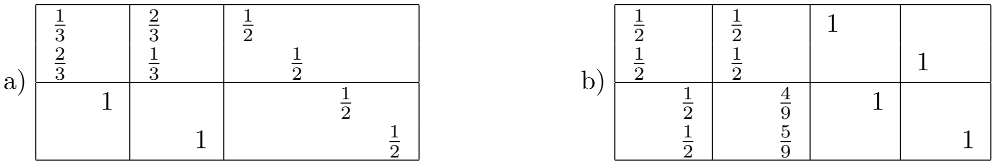
a)
$\frac{1}{3}$ $\frac{2}{3}$
$\frac{2}{3}$ $\frac{1}{3}$
$\frac{1}{2}$ $\frac{1}{2}$
1 1 $\frac{1}{2}$ $\frac{1}{2}$
b)
$\frac{1}{2}$ $\frac{1}{2}$
$\frac{1}{2}$ $\frac{1}{2}$
1 1
$\frac{1}{2}$ $\frac{1}{2}$
$\frac{4}{9}$ $\frac{5}{9}$
1 1

Figure 3: a) Example for illustration that not every OT-core is useful for us: The first two block columns contain an OT-core, but can be subsumed by the last block column.
b) Example for illustration that redundancy here is more complex than in the deterministic case: The first block column is redundant (it can be subsumed by the last two), but the second is not.

that in general one cannot completely neglect all input symbols that do not belong to the chosen OT-core. In this example, if Alice only uses one of her input symbols all the time, this means that effectively we can remove one of the block rows and all of a sudden the redundancy-free version of the remaining part even has no OT-core any more.

3.1.1 The protocol for generating correlated data

Basic scheme. Basically, our protocol for generation of correlated data follows the very generic construction of [KMQ11]. It roughly proceeds as follows (for a formal description see Section 4.5).

1. **Invocation of F:** Alice and Bob query the underlying 2-party function F with random input for k times (k being the security parameter) and record their respective input-output tuples. A protocol parameter assigns what concrete input distributions are to be used.
2. **Check A:** Alice challenges Bob on some polynomial subset of the recorded data, where he has to reveal his input-output tuples. Alice aborts the protocol, if the joint distribution of her own input-output tuples and Bob's claimed input-output tuples appears faulty. The test set is then removed from the recorded data.
3. **Check B:** This step equals the previous one with the roles of Alice and Bob interchanged.
4. **Output:** Both parties announce where they have used input symbols that were only for test purposes. All corresponding elements are removed from the recorded data. When too much of the recorded data has been deleted, the protocol is aborted; else each party outputs its remaining string of recorded input-output tuples.

The crucial difference to the protocol scheme of [KMQ11] is in the check steps Check A and Check B. In the scheme of [KMQ11], Alice checked in Check A that each of Bob's claimed input-output tuples (y', b') was consistent with her own respective input-output tuple (x, a) in the sense that $\phi_{x,y'}(a, b') \neq 0$, and that each of Bob's claimed input symbols occurred with the right frequency independently of her own input. This does not suffice in the randomized setting any more, as one can also see from the example in Figure 3.b. In this example, the redundant first block column and the non-redundant second block column differ only very slightly in their output distributions. Thus, if Alice only checked that Bob's claimed input-output tuples do not directly contradict her own input-output tuples, then Bob could substitute his second input symbol in this example right the same way he can already substitute the first input symbol. For this reason, in the check steps Check A and Check B of our protocol scheme described above each party must examine the *joint distribution* of its own input-output tuples and the other party's claimed input-output tuples.

Parameter choice. We have the following wish list to our protocol scheme:

- The challenge sets in the protocol steps Check A and Check B must be sufficiently large, so that any significant deviation from the prescribed input distributions can be detected.

- We want that even a malicious choice of the challenge sets does not substantially influence the joint distribution of the recorded input-output tuples.
- All input symbols must be used with sufficiently high probability, so that the problem illustrated in Figure 3.b does not emerge.
- In the last protocol step, where all data is deleted that does not belong to the chosen OT-core inputs, no corrupted party should be able to modify the recorded data's joint distribution more than by a vanishingly small amount.

Obviously, the first two objectives conflict with each other, and so do the last two. However, what might first sound like a paradox, can be achieved by a polynomially vanishing lower bound for the input probabilities and also a polynomially vanishing relative size of the challenge sets. More concretely, for every input symbol that is only for test purposes we choose an input probability of magnitude $O(k^{-\alpha})$ with constant $\alpha > 0$, and the challenge sets have size $O(k^{\frac{1}{2}+\beta})$ with constant $\beta < \frac{1}{2}$ (cf. Section 4.5)—for technical reasons we even choose $\beta < \frac{1}{6}$. Thus, there exists some constant $\varepsilon > 0$, such that $k - k^{1-\varepsilon}$ recorded input-output tuples from the first protocol step remain untouched throughout the rest of the protocol and are finally part of the output.

3.1.2 Idealized attack strategies

In the step Check A of the protocol scheme introduced in Section 3.1.1, instantiated with any $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$, a corrupted Bob can of course try to pretend to have used another input distribution than he actually did. Analogously, a corrupted Alice can try to cheat in Check B, but for symmetry reasons it will suffice to consider the case of a corrupted Bob. We start our security considerations by introducing a very idealized notion of attack strategies. This notion comprises only perfectly undetectable attacks, but it will turn out later that *every* possible attack strategy is close to such a perfect strategy.

Cheating strategies. A *cheating strategy* of Bob is a triple (ι, λ, ω), consisting of

- an "actual input distribution" $\iota \in \mathrm{pmf}(\Upsilon_\mathrm{B})$,
- a "lying strategy" $\lambda := (\lambda_{y,b})_{y \in \Upsilon_\mathrm{B}, b \in \Omega_\mathrm{B}} \subseteq \mathrm{pmf}(\Upsilon_\mathrm{B} \times \Omega_\mathrm{B})$ in the sense that in the protocol step Check A an input-output tuple (y, b) is claimed as (y', b') with probability $\lambda_{y,b}(y', b')$,
- and a "claimed input distribution" $\omega \in \mathrm{pmf}(\Upsilon_\mathrm{B})$,

such that for all $x \in \Upsilon_\mathrm{A}$, $a \in \Omega_\mathrm{A}$, $y' \in \Upsilon_\mathrm{B}$, $b' \in \Omega_\mathrm{B}$ and with $\upsilon \in \mathrm{pmf}(\Upsilon_\mathrm{A})$ denoting Alice's input distribution it holds:

$$\underbrace{\upsilon(x) \cdot \omega(y') \cdot \phi_{x,y'}(a, b')}_{\text{expected joint probability of } (x,a) \text{ and } (y',b')} \quad = \quad \underbrace{\sum\nolimits_{y \in \Upsilon_\mathrm{B},\, b \in \Omega_\mathrm{B}} \upsilon(x) \cdot \iota(y) \cdot \phi_{x,y}(a, b) \cdot \lambda_{y,b}(y', b')}_{\text{claimed joint probability of } (x,a) \text{ and } (y',b')}$$

Note that we can cancel $\upsilon(x)$ on both sides, since Alice uses her complete input alphabet and thus $\upsilon(x) > 0$ for all $x \in \Upsilon_\mathrm{A}$. I.e., Bob's cheating strategies are actually independent of Alice's input distribution; they either work for all of them or for none. Further note that ω is no arbitrarily selectable parameter but already completely fixed by ι and λ. In particular, for all $x \in \Upsilon_\mathrm{A}$, $y' \in \Upsilon_\mathrm{B}$ it holds:

$$\omega(y') \;=\; \omega(y') \cdot \phi_{x,y'}(\Omega_\mathrm{A}, \Omega_\mathrm{B}) \;=\; \sum\nolimits_{y \in \Upsilon_\mathrm{B},\, b \in \Omega_\mathrm{B}} \iota(y) \cdot \phi_{x,y}(\Omega_\mathrm{A}, b) \cdot \lambda_{y,b}(y', \Omega_\mathrm{B})$$

Last but not least, an easily verifiable but very important feature of cheating strategies lies in their relation to redundancy: An input symbol $y' \in \Upsilon_\mathrm{B}$ is redundant, iff there exists a cheating strategy (ι, λ, ω), such that $\iota(y') = 0$ and $\omega(y') = 1$. This directly follows from our definitions.

Cheating situations. Our notion of cheating strategies turns out a bit cumbersome for the following reason. Obviously, a corrupted Bob can follow a mixed strategy, e.g. by following half the time some cheating strategy (ι, λ, ω) and half the time some other cheating strategy $(\iota', \lambda', \omega')$. For the resulting cheating strategy $(\bar{\iota}, \bar{\lambda}, \bar{\omega})$ it is intuitively clear that $\bar{\iota} = \frac{1}{2} \cdot \iota + \frac{1}{2} \cdot \iota'$ and $\bar{\omega} = \frac{1}{2} \cdot \omega + \frac{1}{2} \cdot \omega'$. On first glance one might also expect that $\bar{\lambda} = \frac{1}{2} \cdot \lambda + \frac{1}{2} \cdot \lambda'$, but this will not be true in general! E.g., if $\iota(y) = 0 < \iota'(y)$ for some $y \in \Upsilon_\mathrm{B}$, then we have that $\bar{\lambda}_{y,b} = \lambda'_{y,b}$ for all $b \in \Omega_\mathrm{B}$. To circumvent this inconvenience, we introduce the equivalent but more practical notion of *cheating situations*. Given Bob's cheating strategy (ι, λ, ω) and Alice's input distribution $\upsilon \in \mathrm{pmf}(\Upsilon_\mathrm{A})$, we define the corresponding cheating situation $\eta \in \mathrm{pmf}\big((\Upsilon_\mathrm{A} \times \Omega_\mathrm{A}) \times (\Upsilon_\mathrm{B} \times \Omega_\mathrm{B})^2\big)$ as follows:

$$\eta\big((x,a),(y,b),(y',b')\big) := \upsilon(x) \cdot \iota(y) \cdot \phi_{x,y}(a,b) \cdot \lambda_{y,b}(y',b')$$

The intuition behind this is that instead of focusing on the cheating party's plan, we just count how often which kind of situation occurs during the protocol step Check A. More precisely, the value $\eta\big((x,a),(y,b),(y',b')\big)$ is the relative frequency of the event that Alice's input-output tuple is (x,a), Bob's actual input-output tuple is (y,b), and Bob's claimed input-output tuple is (y',b'). Consequently, we can write:

$$\begin{aligned} \eta|_\mathrm{A}(x) &:= \eta\big((x,\Omega_\mathrm{A}),(\Upsilon_\mathrm{B},\Omega_\mathrm{B}),(\Upsilon_\mathrm{B},\Omega_\mathrm{B})\big) = \upsilon(x) \\ \eta|_\mathrm{B}^{\mathsf{true}}(y) &:= \eta\big((\Upsilon_\mathrm{A},\Omega_\mathrm{A}),(y,\Omega_\mathrm{B}),(\Upsilon_\mathrm{B},\Omega_\mathrm{B})\big) = \iota(y) \\ \eta|_\mathrm{B}^{\mathsf{fake}}(y') &:= \eta\big((\Upsilon_\mathrm{A},\Omega_\mathrm{A}),(\Upsilon_\mathrm{B},\Omega_\mathrm{B}),(y',\Omega_\mathrm{B})\big) = \omega(y') \end{aligned}$$

Our definition directly implies that every cheating situation η fulfills the following four conditions.

1. For all $x \in \Upsilon_\mathrm{A}$ it holds that $\eta|_\mathrm{A}(x) > 0$.
2. For all $x \in \Upsilon_\mathrm{A}$, $a \in \Omega_\mathrm{A}$, $y \in \Upsilon_\mathrm{B}$, $b \in \Omega_\mathrm{B}$ it holds:
$$\eta\big((x,a),(y,b),(\Upsilon_\mathrm{B},\Omega_\mathrm{B})\big) = \eta|_\mathrm{A}(x) \cdot \eta|_\mathrm{B}^{\mathsf{true}}(y) \cdot \phi_{x,y}(a,b)$$
3. For all $x \in \Upsilon_\mathrm{A}$, $a \in \Omega_\mathrm{A}$, $y' \in \Upsilon_\mathrm{B}$, $b' \in \Omega_\mathrm{B}$ it holds:
$$\eta\big((x,a),(\Upsilon_\mathrm{B},\Omega_\mathrm{B}),(y',b')\big) = \eta|_\mathrm{A}(x) \cdot \eta|_\mathrm{B}^{\mathsf{fake}}(y') \cdot \phi_{x,y'}(a,b')$$
4. For all $x \in \Upsilon_\mathrm{A}$, $a \in \Omega_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$, $b, b' \in \Omega_\mathrm{B}$ with $\eta\big((\Upsilon_\mathrm{A},\Omega_\mathrm{A}),(y,b),(\Upsilon_\mathrm{B},\Omega_\mathrm{B})\big) > 0$ it holds:
$$\eta\big((x,a),(y,b),(y',b')\big) = \eta\big((\Upsilon_\mathrm{A},\Omega_\mathrm{A}),(y,b),(y',b')\big) \cdot \frac{\eta\big((x,a),(y,b),(\Upsilon_\mathrm{B},\Omega_\mathrm{B})\big)}{\eta\big((\Upsilon_\mathrm{A},\Omega_\mathrm{A}),(y,b),(\Upsilon_\mathrm{B},\Omega_\mathrm{B})\big)}$$

Note that these conditions basically are a polynomial equation system, of which we will take great advantage later. Let $\mathfrak{N}_\mathrm{B}^{(F)}$ denote the set of all $\eta \in \mathrm{pmf}\big((\Upsilon_\mathrm{A}\times\Omega_\mathrm{A})\times(\Upsilon_\mathrm{B}\times\Omega_\mathrm{B})^2\big)$ that fulfill them. We show now that actually $\mathfrak{N}_\mathrm{B}^{(F)}$ is just the set of all cheating situations. Given any $\eta \in \mathfrak{N}_\mathrm{B}^{(F)}$, we find some $\iota, \omega \in \mathrm{pmf}(\Upsilon_\mathrm{B})$ and $\lambda := (\lambda_{y,b})_{y\in\Upsilon_\mathrm{B}, b\in\Omega_\mathrm{B}} \subseteq \mathrm{pmf}(\Upsilon_\mathrm{B}\times\Omega_\mathrm{B})$, such that for all $y, y' \in \Upsilon_\mathrm{B}$, $b, b' \in \Omega_\mathrm{B}$ we have:

$$\begin{aligned} \iota(y) &= \eta|_\mathrm{B}^{\mathsf{true}}(y) \\ \omega(y') &= \eta|_\mathrm{B}^{\mathsf{fake}}(y') \\ \lambda_{y,b}(y',b') &= \frac{\eta\big((\Upsilon_\mathrm{A},\Omega_\mathrm{A}),(y,b),(y',b')\big)}{\eta\big((\Upsilon_\mathrm{A},\Omega_\mathrm{A}),(y,b),(\Upsilon_\mathrm{B},\Omega_\mathrm{B})\big)} \quad \text{if } \eta\big((\Upsilon_\mathrm{A},\Omega_\mathrm{A}),(y,b),(\Upsilon_\mathrm{B},\Omega_\mathrm{B})\big) > 0 \end{aligned}$$

Since η meets the four conditions above, we have that (ι, λ, ω) is a cheating strategy:

$$\begin{aligned} &\textstyle\sum_{y\in\Upsilon_\mathrm{B},\, b\in\Omega_\mathrm{B}} \iota(y) \cdot \phi_{x,y}(a,b) \cdot \lambda_{y,b}(y',b') \;=\; \sum_{y\in\Upsilon_\mathrm{B},\, b\in\Omega_\mathrm{B}} \dfrac{\eta\big((x,a),(y,b),(\Upsilon_\mathrm{B},\Omega_\mathrm{B})\big) \cdot \lambda_{y,b}(y',b')}{\eta|_\mathrm{A}(x)} \\ &= \tfrac{1}{\eta|_\mathrm{A}(x)} \cdot \textstyle\sum_{y\in\Upsilon_\mathrm{B},\, b\in\Omega_\mathrm{B}} \eta\big((x,a),(y,b),(y',b')\big) \;=\; \omega(y') \cdot \phi_{x,y'}(a,b') \end{aligned}$$

Likewise, η is a corresponding cheating situation:

$$\eta|_{\mathrm{A}}(x)\cdot\iota(y)\cdot\phi_{x,y}(a,b)\cdot\lambda_{y,b}(y',b')=\eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big)\cdot\lambda_{y,b}(y',b')=\eta\big((x,a),(y,b),(y',b')\big)$$

Advantages of our notion of cheating situations. In contrast to the more intuitive notion of cheating strategies, our definition of cheating situations enjoys some very handy structure: When we fix Alice's input distribution, the remaining set of cheating situations is a bounded convex polytope in the affine space $\mathbb{R}^{(\Upsilon_{\mathrm{A}}\times\Omega_{\mathrm{A}})\times(\Upsilon_{\mathrm{B}}\times\Omega_{\mathrm{B}})^2}$, spanned by finitely many vertices (cf. Lemma 10). Furthermore, cheating situations inherit two important features from cheating strategies. Firstly, cheating situations can be considered independent of (honest) Alice's input distribution, since they can be rescaled canonically to any input distribution that assigns non-zero probability to every $x\in\Upsilon_{\mathrm{A}}$ (q.v. Lemma 8). Secondly, an input symbol $y'\in\Upsilon_{\mathrm{B}}$ is redundant, iff there exists a cheating situation $\eta\in\mathfrak{N}_{\mathrm{B}}^{(F)}$, such that $\eta|_{\mathrm{B}}^{\mathsf{true}}(y')=0$ and $\eta|_{\mathrm{B}}^{\mathsf{fake}}(y')=1$. For redundancy of y' it even suffices that $\eta|_{\mathrm{B}}^{\mathsf{true}}(y')<\eta|_{\mathrm{B}}^{\mathsf{fake}}(y')$ and $\eta|_{\mathrm{B}}^{\mathsf{true}}(y)\geq\eta|_{\mathrm{B}}^{\mathsf{fake}}(y)$ for all $y\in\Upsilon_{\mathrm{B}}\backslash\{y'\}$. This results from some useful decomposability features of the algebraic structure $\mathfrak{N}_{\mathrm{B}}^{(F)}$, but for now we skip all the technical details and instead just refer to Section 4.3.

Last but not least, cheating situations are also unaffected by another disadvantage of cheating strategies that misleads intuition: If $\lambda_{y,b}(y',b')>0$, this does not necessarily mean that Bob ever really replaces an input-output tuple (y,b) by (y',b'); as well, it might be the case that $\iota(y)=0$ (i.e., Bob did not use the input symbol y at all). In contrast, if $\eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y',b')\big)>0$, then Bob has in fact replaced the corresponding portion of actual input-output tuples (y,b) by claimed input-output tuples (y',b').

3.1.3 Robust OT-cores

We aim at an instantiation of the protocol scheme described in Section 3.1.1, such that the inputs belonging to some chosen OT-core of the underlying 2-party function F are used with relatively high probability and all other inputs have relatively low probability. However, if $\tilde{y},\tilde{y}'$ are Bob's OT-core inputs and there exists a cheating situation $\eta\in\mathfrak{N}_{\mathrm{B}}^{(F)}$, such that $\eta|_{\mathrm{B}}^{\mathsf{true}}(\{\tilde{y},\tilde{y}'\})=0$ and $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\{\tilde{y},\tilde{y}'\})=1$, then we have no security guarantee (cf. Figure 3.a). We need at least that $\eta|_{\mathrm{B}}^{\mathsf{true}}(\{\tilde{y},\tilde{y}'\})=1$ for all $\eta\in\mathfrak{N}_{\mathrm{B}}^{(F)}$ with $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\{\tilde{y},\tilde{y}'\})=1$; otherwise a corrupted Bob can always substitute a substantial fraction of his OT-core queries by other inputs. Surprisingly, this is not only a necessary precondition for security, but it will even turn out sufficient. The key idea is to choose protocol parameters, such that the prescribed probability of non-OT-core inputs is high enough for cheating detection, but still so small that only cheating strategies (ι,λ,ω) with $\omega(y)=0$ for all non-OT-core inputs y may work. This might first sound like a paradox, but can be achieved by polynomially vanishing probabilities for the non-OT-core inputs (cf. Section 3.1.1).

However, first and foremost we need to show that there always exists an OT-core fulfilling the abovementioned criterion, if only the redundancy-free version of the considered 2-party function has any OT-core at all (see Figure 3.a for a negative example). Moreover, we also need analogous security against a possibly cheating Alice, and we must rule out that every OT-core found secure against a cheating Bob is insecure against a cheating Alice and vice versa. We achieve this all at once by the next lemma (cf. Lemma 25).

Lemma. *Let some $F:=(\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},\Omega_{\mathrm{A}},\Omega_{\mathrm{B}},\phi)\in\mathfrak{F}_{\mathsf{fin}}$ be given that is redundancy-free and has an OT-core. Then there also exists an OT-core within the same rows of the canonical representation of F, such that for Bob's corresponding input symbols $\bar{y},\bar{y}'$ and every cheating situation $\eta\in\mathfrak{N}_{\mathrm{B}}^{(F)}$ with $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\{\bar{y},\bar{y}'\})=1$ we have that $\eta|_{\mathrm{B}}^{\mathsf{true}}(\{\bar{y},\bar{y}'\})=1$.*

By this lemma, given any OT-core, we find an OT-core within the same rows of the canonical representation, such that this new OT-core is secure against a potentially cheating Bob. Analogously, starting from the OT-core secure against Bob, we find an OT-core within the same columns of the canonical representation, such that this new OT-core is secure against a potentially cheating Alice. Since in the second step Bob's involved input symbols stay the same, the finally found OT-core is also still secure against a cheating Bob.

Now, we give a proof-sketch for this lemma, which is a core element of our line of argument. Note that, although our notion of cheating situations can be seen as a generalization of the corresponding concept in [KMQ11], this proof is independent—cf. [KMQ10, Section 5].

Proof-sketch. Let $(\tilde{x},\tilde{a}),(\tilde{x}',\tilde{a}') \in \Upsilon_{\mathrm{A}}\times\Omega_{\mathrm{A}}$ and $(\tilde{y},\tilde{b}),(\tilde{y}',\tilde{b}') \in \Upsilon_{\mathrm{B}}\times\Omega_{\mathrm{B}}$ denote Alice's and Bob's input-output tuples belonging to the initially given OT-core. W.l.o.g., $\phi_{\tilde{x},\tilde{y}}(\tilde{a},\tilde{b}) > 0$ and $\phi_{\tilde{x}',\tilde{y}}(\tilde{a}',\tilde{b}) > 0$.

If $\tilde{y} = \tilde{y}'$, i.e. the initially given OT-core lies within a single block column of the canonical representation, then existence of a cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ with $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\{\bar{y},\bar{y}'\}) = 1 > \eta|_{\mathrm{B}}^{\mathsf{true}}(\{\bar{y},\bar{y}'\})$ would imply that the input symbol simultaneously denoted by $\tilde{y}$ and $\tilde{y}'$ is redundant (cf. Corollary 18). So, in this case things are easy. Else, i.e. if $\tilde{y} \neq \tilde{y}'$, we need a more abstract view of cheating situations to keep arguments traceable. Let $\mathfrak{X}_{\mathrm{B}}^{(F)}$ denote the set of all mappings $\xi : \Upsilon_{\mathrm{B}} \to \mathbb{R}$ for that there exist some $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ and $\gamma \in \mathbb{R}_{>0}$, such that $\gamma \cdot \xi(y) = \eta|_{\mathrm{B}}^{\mathsf{fake}}(y) - \eta|_{\mathrm{B}}^{\mathsf{true}}(y)$ for all $y \in \Upsilon_{\mathrm{B}}$. The intuition behind this is merely that $\xi(y) > 0$ if Bob claims to have input y more often than he actually did, and $\xi(y) < 0$ if Bob claims to have input y less often than he actually did. We will make use of the following properties of this notation:

- The set $\mathfrak{X}_{\mathrm{B}}^{(F)}$ is closed under positive linear combination, i.e. $\gamma \cdot \xi + \gamma' \cdot \xi' \in \mathfrak{X}_{\mathrm{B}}^{(F)}$ for all $\gamma,\gamma' \in \mathbb{R}_{>0}$ and $\xi,\xi' \in \mathfrak{X}_{\mathrm{B}}^{(F)}$. This straightforwardly follows from the fact that Alice's input distribution $\eta|_{\mathrm{A}}$ of every cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ can be canonically rescaled, and the fact that the set of all cheating situations with the same input distribution of Alice is convex.
- If for some $y' \in \Upsilon_{\mathrm{B}}$ there exists a $\xi \in \mathfrak{X}_{\mathrm{B}}^{(F)}$ with $\xi(y') > 0$ and $\xi(y) \leq 0$ for all $y \in \Upsilon_{\mathrm{B}}\setminus\{y'\}$, then y' is redundant. This is just a reformulation of the redundancy criterion that there exists an $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ with $\eta|_{\mathrm{B}}^{\mathsf{true}}(y') < \eta|_{\mathrm{B}}^{\mathsf{fake}}(y')$ and $\eta|_{\mathrm{B}}^{\mathsf{true}}(y) \geq \eta|_{\mathrm{B}}^{\mathsf{fake}}(y)$ for all $y \in \Upsilon_{\mathrm{B}}\setminus\{y'\}$.

Further, for any $Y \subseteq \Upsilon_{\mathrm{B}}$ let $\Psi_F(Y)$ denote the set of all input symbols y that a corrupted Bob can use although the protocol prescribes to use only input symbols from Y, i.e.:

$$\Psi_F(Y) \;=\; \left\{ y \in \Upsilon_{\mathrm{B}} \;\middle|\; \text{there exists an } \eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}\text{, such that } \eta|_{\mathrm{B}}^{\mathsf{true}}(y) > 0 \text{ and } \eta|_{\mathrm{B}}^{\mathsf{fake}}(Y) = 1 \right\}$$

Note that by the convex combinability of cheating situations we always find some $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, such that $\eta|_{\mathrm{B}}^{\mathsf{fake}}(Y) = 1$ and $\eta|_{\mathrm{B}}^{\mathsf{true}}(y) > 0$ for *all* $y \in \Psi_F(Y)$. Thus, we also always have some $\xi \in \mathfrak{X}_{\mathrm{B}}^{(F)}$, such that $\xi(y) = 0$ for all $y \notin \Psi_F(Y)$ and $\xi(y) < 0$ for all $y \in \Psi_F(Y)\setminus Y$. Further note that always $\Psi_F(Y) \subseteq \Psi_F(Y')$ for all $Y \subseteq Y'$, that $\Psi_F(\Psi_F(Y')) = \Psi_F(Y')$, and that hence $\Psi_F(Y) \subseteq \Psi_F(Y')$ for all $Y \subseteq \Psi_F(Y')$ (cf. Lemma 23).

Now we can start with our argumentation. First of all, we divide $\Psi_F(\tilde{y},\tilde{y}')$ into the following three subsets (cf. Figure 4):

- Let $\tilde{Y}'$ denote the set of all $y' \in \Psi_F(\tilde{y},\tilde{y}')$, such that for some $b' \in \Omega_{\mathrm{B}}$ the $\{(\tilde{x},\tilde{a}),(\tilde{x}',\tilde{a}')\}\times\{(\tilde{y},\tilde{b}),(y',b')\}$-submatrix of the canonical representation of F is an OT-core; i.e., since by assumption $\phi_{\tilde{x},\tilde{y}}(\tilde{a},\tilde{b}) > 0$ and $\phi_{\tilde{x}',\tilde{y}}(\tilde{a}',\tilde{b}) > 0$, we just need:

$$\phi_{\tilde{x},\tilde{y}}(\tilde{a},\tilde{b}) \cdot \phi_{\tilde{x}',y'}(\tilde{a}',b') \neq \phi_{\tilde{x}',\tilde{y}}(\tilde{a}',\tilde{b}) \cdot \phi_{\tilde{x},y'}(\tilde{a},b')$$

	$\tilde{y}$		$\tilde{y}'$	$\tilde{Y}$							$\tilde{Y}'$							$\tilde{Y}_0$			
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
$\cdots$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{2}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{1}{12}$	$\frac{1}{8}$	$\frac{1}{6}$	$\frac{1}{8}$	$\frac{5}{9}$	1	$\frac{1}{4}$	0	0	0	0	0	$\cdots$
$\cdots$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{1}{12}$	$\frac{1}{8}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{4}{9}$	0	0	$\frac{1}{3}$	$\frac{1}{4}$	0	0	0	$\cdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Figure 4: Illustration of the construction of the input sets $\tilde{Y}, \tilde{Y}', \tilde{Y}_0$. Input symbols from $\tilde{Y}$ have an OT-core together with $\tilde{y}'$, but not with $\tilde{y}$; inputs from $\tilde{Y}'$ have an OT-core together with $\tilde{y}$; inputs from $\tilde{Y}_0$ cannot be completed by $\tilde{y}$ or $\tilde{y}'$ to have an OT-core. Note that always $\tilde{y} \in \tilde{Y}$ and $\tilde{y}' \in \tilde{Y}'$, which is not displayed in order to keep the graphic simple.

- Let $\tilde{Y}$ denote the set of all $y \in \Psi_F(\tilde{y}, \tilde{y}')\backslash\tilde{Y}'$, such that for some $b \in \Omega_\mathrm{B}$ the $\{(\tilde{x}, \tilde{a}), (\tilde{x}', \tilde{a}')\} \times \{(y, b), (\tilde{y}', \tilde{b}')\}$-submatrix of the canonical representation of F is an OT-core; i.e., $\phi_{\tilde{x},y}(\tilde{a}, b) > 0$ and $\phi_{\tilde{x}',y}(\tilde{a}', b) > 0$ and for all $\hat{b} \in \Omega_\mathrm{B}$ we have:
$$\phi_{\tilde{x},\tilde{y}}(\tilde{a}, \tilde{b}) \cdot \phi_{\tilde{x}',y}(\tilde{a}', \hat{b}) = \phi_{\tilde{x},y}(\tilde{a}, \hat{b}) \cdot \phi_{\tilde{x}',\tilde{y}}(\tilde{a}', \tilde{b})$$
- Let $\tilde{Y}_0$ denote the set of all $y_0 \in \Psi_F(\tilde{y}, \tilde{y}')$, such that for all $b_0 \in \Omega_\mathrm{B}$ neither the $\{(\tilde{x}, \tilde{a}), (\tilde{x}', \tilde{a}')\} \times \{(\tilde{y}, \tilde{b}), (y_0, b_0)\}$-submatrix nor the $\{(\tilde{x}, \tilde{a}), (\tilde{x}', \tilde{a}')\} \times \{(y_0, b_0), (\tilde{y}', \tilde{b}')\}$-submatrix of the canonical representation of F is an OT-core; i.e., $\phi_{\tilde{x},y_0}(\tilde{a}, \Omega_\mathrm{B}) = \phi_{\tilde{x}',y_0}(\tilde{a}', \Omega_\mathrm{B}) = 0$.

Our proof is by contradiction and hence w.l.o.g. we assume that $\Psi_F(y, \tilde{y}') = \Psi_F(\tilde{y}, \tilde{y}')$ for all $y \in \tilde{Y}$ and $\Psi_F(\tilde{y}, y') = \Psi_F(\tilde{y}, \tilde{y}')$ for all $y' \in \tilde{Y}'$—keep in mind that $\Psi_F(Z) \subseteq \Psi_F(\tilde{y}, \tilde{y}')$ for all $Z \subseteq \Psi_F(\tilde{y}, \tilde{y}')$ as mentioned above. Now we pick some arbitrary $y' \in \Psi_F(\tilde{y}, \tilde{y}')$; w.l.o.g. $y' \in \tilde{Y}'$. By assumption we find some $\xi', \xi'' \in \mathfrak{X}_\mathrm{B}^{(F)}$, such that for all $y \in \Upsilon_\mathrm{B}$ it holds:

$$\begin{aligned} &\xi'(y) > 0 \text{ if } y \in \{\tilde{y}, y'\} && \xi''(y) > 0 \text{ if } y \in \{\tilde{y}, \tilde{y}'\} \\ &\xi'(y) = 0 \text{ if } y \notin \Psi_F(\tilde{y}, \tilde{y}') && \xi''(y) = 0 \text{ if } y \notin \Psi_F(\tilde{y}, \tilde{y}') \\ &\xi'(y) < 0 \text{ if } y \in \Psi_F(\tilde{y}, \tilde{y}')\backslash\{\tilde{y}, y'\} && \xi''(y) < 0 \text{ if } y \in \Psi_F(\tilde{y}, \tilde{y}')\backslash\{\tilde{y}, \tilde{y}'\} \end{aligned}$$

Let $\xi := \xi'(y') \cdot \xi'' - \xi''(y') \cdot \xi'$, whereby for all $y \in \Upsilon_\mathrm{B}$ we get:

$$\begin{aligned} &\xi(y) > 0 \text{ if } y = \tilde{y} \\ &\xi(y) = 0 \text{ if } y \notin \Psi_F(\tilde{y}, \tilde{y}') \text{ or } y = y' \\ &\xi(y) < 0 \text{ if } y \in \Psi_F(\tilde{y}, \tilde{y}')\backslash\{\tilde{y}, \tilde{y},' y'\} \end{aligned}$$

Moreover, it must hold that $\xi(\tilde{y}') > 0$, since otherwise $\xi(y) \leq 0$ for all $y \in \Upsilon_\mathrm{B}\backslash\{\tilde{y}\}$ and hence $\tilde{y}$ would be redundant. Iteration of this construction yields some $\hat{\xi} \in \mathfrak{X}_\mathrm{B}^{(F)}$, such that for all $y \in \Upsilon_\mathrm{B}$ we have:

$$\begin{aligned} &\hat{\xi}(y) > 0 \text{ if } y \in \{\tilde{y}, \tilde{y}'\} \\ &\hat{\xi}(y) = 0 \text{ if } y \notin \{\tilde{y}, \tilde{y}'\} \cup \tilde{Y}_0 \\ &\hat{\xi}(y) < 0 \text{ if } y \in \tilde{Y}_0 \end{aligned}$$

Switching back to cheating situations or cheating strategies respectively, this means that Bob can use his input symbols $\tilde{y}, \tilde{y}'$ less frequently than prescribed and substitute them by input symbols from $\tilde{Y}_0$. However, this cannot be (the following arguments can probably be followed best through a concrete example, e.g. Figure 4): Since $\phi_{\tilde{x},Y_0}(\tilde{a}, \Omega_\mathrm{B}) = 0$ and $\phi_{\tilde{x}',Y_0}(\tilde{a}', \Omega_\mathrm{B}) = 0$, but $\phi_{\tilde{x},\tilde{y}}(\tilde{a}, \tilde{b}) > 0$ and $\phi_{\tilde{x}',\tilde{y}}(\tilde{a}', \tilde{b}) > 0$ and also $\phi_{\tilde{x},\tilde{y}'}(\tilde{a}, \tilde{b}') + \phi_{\tilde{x}',\tilde{y}'}(\tilde{a}', \tilde{b}') > 0$, this substantially decreases Alice's overall frequency of input-output tuples $(\tilde{x}, \tilde{a})$ and $(\tilde{x}', \tilde{a}')$ and thus cannot be an undetectable cheating strategy. □

3.1.4 Robust OT-cores in real protocol runs

In this section we consider real protocol runs of the protocol scheme introduced in Section 3.1.1, instantiated with some arbitrary $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$. Unfortunately, there is no guarantee that a corrupted Bob always follows *exactly* a cheating strategy in the idealized sense of Section 3.1.2. For instance, he can as well try to exploit that Alice has to tolerate some statistical noise in the protocol step Check A. However, we show now that indeed our notion of cheating situations is a very suitable approximation of what may happen during a real protocol run. To make formulas more readable, we use the following self-suggesting notation.

Notation (Almost equality). For any $a, b, c \in \mathbb{R}$, by "$a = b \pm c$" we denote that $|a - b| \leq c$.

Linking real protocol runs to idealized attack strategies. Our starting point for linking real protocol runs to idealized attack strategies is the Hoeffding Inequality. We need it in the following form, which directly follows by [Hoe63, Theorem 1].

Lemma (Hoeffding Inequality). *Let any $n \in \mathbb{N}$, $c \in \mathbb{R}_{>0}$ and a binomially distributed random variable X with expected value $\mathbf{E}(X)$ be given. Further let $\mathbf{P}[0 \leq X \leq n] = 1$. Then it holds:*

$$\mathbf{P}\big[|X - \mathbf{E}(X)| \geq c\big] \;\leq\; 2 \cdot \exp\left(\tfrac{-2c^2}{n}\right)$$

By [Hoe63, Section 6], this lemma also holds true if X is distributed hypergeometrically.

Following [KMQ10, Lemma 15], we instantiate the Hoeffding Inequality with $n := k$ and $c := k^{\Delta}$, where k denotes our security parameter and $\Delta > \frac{1}{2}$ is constant. Thereby we get that the probability $\mathbf{P}\big[|X - \mathbf{E}(X)| \geq k^{\Delta}\big]$ is upper bounded by $2 \cdot \exp\big(-2k^{2\Delta-1}\big)$. I.e., it vanishes exponentially in k and hence is negligible, or in other words, $X = \mathbf{E}(X) \pm k^{\Delta}$ with overwhelming probability.

The most apparent application of the Hoeffding Inequality is Alice's choice of the challenge set in the protocol step Check A. This random choice is a hypergeometric sampling process and by the hypergeometric version of the Hoeffding Inequality it follows that the joint distribution of Alice's and Bob's input-output tuples in the challenge set is a good approximation of their overall joint distribution of input-output tuples. Moreover, for any $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$, $b \in \Omega_{\mathrm{B}}$ and with $\upsilon \in \mathrm{pmf}(\Upsilon_{\mathrm{A}})$ denoting Alice's input distribution it holds: Whenever in the first protocol step Bob inputs y, then with probability $\upsilon(x) \cdot \phi_{x,y}(a, b)$ this counts to the number of events where Alice's input-output tuple is (x, a) and Bob's input-output tuple is (y, b). Therefore, Bob's input strategy can be seen as a binomial sampling process, and thus the binomial version of the Hoeffding Inequality applies. Analogously, the hypergeometric version of the Hoeffding Inequality applies to Bob's lying strategy in the step Check A. Skipping some further details, in the end this yields: If for each $(x, a, y, b, y', b') \in \Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}} \times \Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}} \times \Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}}$ we count the relative frequency of the event that Alice's input-output tuple is (x, a), Bob's actual input-output tuple is (y, b) and Bob's claimed input-output tuple is (y', b'), then with overwhelming probability the resulting $\mathbb{R}^{(\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2}$-vector ν fulfills the defining conditions of cheating strategies as introduced in Section 3.1.2, up to some error of magnitude $k^{-\varepsilon}$ with constant $\varepsilon > 0$ (cf. Lemma 34). In particular, with $\upsilon \in \mathrm{pmf}(\Upsilon_{\mathrm{A}})$ denoting Alice's prescribed input distribution, we have:

1. For all $x \in \Upsilon_{\mathrm{A}}$ it holds that $\nu|_{\mathrm{A}}(x) := \nu\big((x, \Omega_{\mathrm{A}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) = \upsilon(x) \pm k^{-\varepsilon}$.
2. For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$, $b \in \Omega_{\mathrm{B}}$ it holds:
$$\nu\big((x, a), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) = \nu|_{\mathrm{A}}(x) \cdot \nu\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, \Omega_{\mathrm{B}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) \cdot \phi_{x,y}(a, b) \pm k^{-\varepsilon}$$
3. For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y' \in \Upsilon_{\mathrm{B}}$, $b' \in \Omega_{\mathrm{B}}$ it holds:
$$\nu\big((x, a), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (y', b')\big) = \nu|_{\mathrm{A}}(x) \cdot \nu\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (y', \Omega_{\mathrm{B}})\big) \cdot \phi_{x,y'}(a, b') \pm k^{-\varepsilon}$$

4. For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$, $b, b' \in \Omega_{\mathrm{B}}$ with $\nu\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) > 0$ it holds:
$$\nu\big((x,a),(y,b),(y',b')\big) = \nu\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y,b), (y',b')\big) \cdot \frac{\nu\big((x,a),(y,b),(\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)}{\nu\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y,b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)} \pm k^{-\varepsilon}$$

The last three items[2] above can be seen as a polynomial equation system over $\mathbb{R}^{(\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2}$, such that the defining multivariate polynomials solely depend on F, the cheating situations from Section 3.1.2 are always in the zero locus of these polynomials, and all these polynomials evaluate on ν to something bounded by $k^{-\varepsilon}$. Now, we are going to exploit the latter and derive an estimation for the distance of our $\mathbb{R}^{(\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2}$-vector ν from $\mathfrak{N}_{\mathrm{B}}^{(F)}$. This is where real algebraic geometry comes into play.

Lemma (Łojasiewicz Inequality [Łoj59, Theorem 17])**.** *Let some $n \in \mathbb{N}$, an open set $U \subseteq \mathbb{R}^n$, a compact set $K \subset U$, and a real analytic function $h : U \to \mathbb{R}$ with non-empty zero locus Z be given. Then, there exist some constants $c, d \in \mathbb{R}_{>0}$, such that for all $\nu \in K$ it holds:*
$$\inf_{\eta \in Z} \|\nu - \eta\| \;\leq\; c \cdot \big|h(\nu)\big|^d$$

Unfortunatley, the Łojasiewicz Inequality is not directly applicable in our case. The primary reason is that each cheating strategy $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ does not only have to fulfill the abovementioned polynomial equations (which translates to $\eta \in Z$ in terms of the Łojasiewicz Inequality), but it must also hold that $\eta \in \operatorname{pmf}\big((\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2\big)$. Therefore, we need the following adaption of the Łojasiewicz Inequality (q.v. Lemma 35).

Lemma. *Let $n \in \mathbb{N}$ and some polynomial $f \in \mathbb{R}[X_1, \dots, X_n]$ be given, such that the variety $V := \big\{\nu \in \mathbb{R}^n \;\big|\; f(\nu) = 0\big\}$ is not empty. Furthermore, let a bounded convex polytope $P \subset \mathbb{R}^n$ be given, such that $V \cap P \neq \emptyset$. Then for every norm there exist some constants $c, d \in \mathbb{R}_{>0}$, such that for all $\nu \in P$ it holds:*
$$\min_{\eta \in V \cap P} \|\nu - \eta\| \;\leq\; c \cdot \big|f(\nu)\big|^d$$

We instantiate this lemma with $P := \operatorname{pmf}\big((\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2\big)$ and $f := \sum_{p \in S} p^2$, where the set S just contains the polynomials from our polynomial equation system above. Thereby, we can show that with overwhelming probability either the considered protocol run is aborted or the vector ν described above is $\big(c \cdot |S| \cdot k^{-2\varepsilon d}\big)$-close to a cheating strategy $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$. We skip all further technical details here (q.v. Section 4.6), but a final caveat seems in place: In general, the last lemma above is not true without the condition that P is a polytope, even if P is still assumed to be convex and compact! Also note that our whole line of argument would be vastly more complicated with cheating strategies instead of cheating situations, what again proves usefulness of the latter concept.

Exploiting decomposability of cheating situations. So far, we have reached two essential insights. On the one hand, by Section 3.1.3 we can find OT-cores, such that for Bob's corresponding input symbols $\bar{y}, \bar{y}'$ and every cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ with $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\{\bar{y}, \bar{y}'\}) = 1$ we have that $\eta|_{\mathrm{B}}^{\mathsf{true}}(\{\bar{y}, \bar{y}'\}) = 1$ (cf. left diagram in Figure 5). On the other hand, by the considerations above we know that a real protocol run with overwhelming probability is either aborted or there exists a cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, such that $\eta|_{\mathrm{B}}^{\mathsf{true}}$ is $k^{-\varepsilon}$-close to Bob's actual input distribution and $\eta|_{\mathrm{B}}^{\mathsf{fake}}$ is $k^{-\varepsilon}$-close to Bob's claimed input distribution. Since otherwise Alice aborts the protocol, the latter also implies that $\eta|_{\mathrm{B}}^{\mathsf{fake}}$ is $k^{-\varepsilon}$-close to Bob's prescribed input distribution.

[2] We shall just ignore the first item in this more intuitive overview. It will be formally needed to estimate $\min_{x \in \Upsilon_{\mathrm{A}}} \nu|_{\mathrm{A}}(x)$, but it plays a somewhat special role, since Alice's input distribution υ depends on the security parameter k (cf. Section 3.1.1). All other equations are independent of k, except for the respective error terms $k^{-\varepsilon}$.

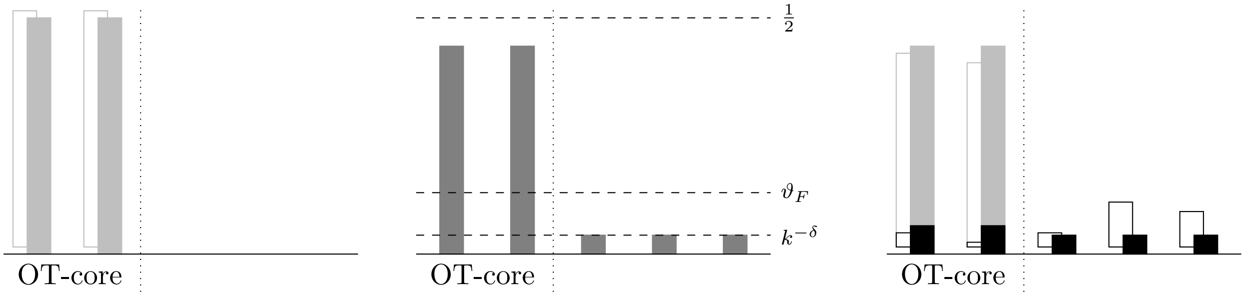

Figure 5: What we know (left), what we have (middle), and what we can conclude (right). Filled bars stand for claimed input probabilities, non-filled bars stand for actual input probabilities.
Left diagram: When Bob claims to have used only inputs that belong to the chosen OT-core, we know that he actually has done so.
Middle diagram: In real protocol runs we must tolerate that Bob sometimes claims to have used inputs not belonging to the chosen OT-core.
Right diagram: Decomposition of the claimed input distribution from the middle diagram into a large part, where the guarantee from the left diagram applies, and a polynomially vanishing rest.

Now we want to tie these two things together, but we have the following problem. As discussed right at the start of Section 3.1, the support of Bob's prescribed input distribution must be his complete input alphabet Υ_{B}. Hence, we must also tolerate in the protocol step Check A that Bob sometimes claims to have used an input symbol that does not belong to the chosen OT-core. Thereby, we only get that $\eta|_{\mathrm{B}}^{\mathsf{fake}}(y') \leq k^{-\delta}$ for all $y' \in \Upsilon_{\mathrm{B}} \setminus \{\bar{y}, \bar{y}'\}$ with constant $\delta > 0$, rather than $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\Upsilon_{\mathrm{B}} \setminus \{\bar{y}, \bar{y}'\}) = 0$ (cf. middle diagram in Figure 5).

We solve this problem by exploiting the fact that, up to rescaling of Alice's input distribution $\eta|_{\mathrm{A}}$, the set $\mathfrak{N}_{\mathrm{B}}^{(F)}$ is the convex hull of a finite spanning set $\{\dot{\eta}_1, \ldots, \dot{\eta}_n\} \subseteq \mathfrak{N}_{\mathrm{B}}^{(F)}$. Since $k^{-\delta}$ becomes arbitrarily small for increasing security parameter k, but there exists some constant $\vartheta_F > 0$ with $\dot{\eta}_i|_{\mathrm{B}}^{\mathsf{fake}}(y') \notin (0, \vartheta_F)$ for all $y' \in \Upsilon_{\mathrm{B}}, i \in \{1, \ldots, n\}$, we can conclude that our initially given cheating situation η consists only in small part of cheating situations $\dot{\eta}_i$ with $\dot{\eta}_i|_{\mathrm{B}}^{\mathsf{fake}}(\Upsilon_{\mathrm{B}} \setminus \{\bar{y}, \bar{y}'\}) > 0$ (cf. right diagram in Figure 5). Thus, we only introduce an additional error of magnitude $O(k^{-\delta})$, if we approximate a cheating Bob's behavior by a cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ with $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\{\bar{y}, \bar{y}'\}) = 1$. So, after all we can utilize that our chosen OT-core does not allow for non-trivial cheating situations, and we can conclude that Bob has to play honestly up to some polynomially vanishing fraction of his inputs.

Secure generation of correlated data. Putting things together, we have shown that in the protocol scheme introduced in Section 3.1.1, if instantiated appropriately, even corrupted parties cannot deviate too much from the prescribed input distributions without being caught cheating. Furthermore, the final protocol output consists for the most part of such "almost honestly" generated data (cf. the final discussion of Section 3.1.1), even if a corrupted party chooses a challenge set maliciously in one of the check steps, and/or lies in the final output step about which inputs did not belong to the chosen OT-core. Altogether, our protocol produces some "slightly manipulable correlated data" (SMCD). We want to grasp this by defining an according functionality, which is implemented by our protocol in the UC sense, but first we need to introduce some suitable notation.

Notation. Given a finite string s over some alphabet Ω, let $|s|$ denote the length of s. By $|s|_\alpha$ with $\alpha \in \Omega$ we denote the number of appearances of α in s. By $s[i]$ with $i \in \{1, \ldots, |s|\}$ we denote the i-th element of s. For some given strings s_{A} and s_{B} of the same length, we define the *compound string* $s_{\mathrm{A}} \times s_{\mathrm{B}}$, whose i-th element is just the tuple $\big(s_{\mathrm{A}}[i], s_{\mathrm{B}}[i]\big)$.

Functionality $\mathcal{F}_{\text{SMCD}}^{(G,\varepsilon)}$

Parametrized by a constant $\varepsilon > 0$ and $G := (\Lambda_{\text{A}}, \Lambda_{\text{B}}, \psi)$, where Λ_{A} and Λ_{B} are finite alphabets and $\psi \in \text{pmf}(\Lambda_{\text{A}} \times \Lambda_{\text{B}})$, such that $\psi(\alpha, \Lambda_{\text{B}}) > 0$ for all $\alpha \in \Lambda_{\text{A}}$ and $\psi(\Lambda_{\text{A}}, \beta) > 0$ for all $\beta \in \Lambda_{\text{B}}$. Let k denote the security parameter and let $\Delta := 1 - \varepsilon$.

- Wait for the adversary to send a compound string $t_{\text{A}} \times t_{\text{B}}$, such that $k - k^{1-\varepsilon} \leq |t_{\text{A}} \times t_{\text{B}}| \leq k$ and for all $\alpha \in \Lambda_{\text{A}}$, $\beta \in \Lambda_{\text{B}}$ it holds:
$$|t_{\text{A}} \times t_{\text{B}}|_{(\alpha,\beta)} \;=\; k \cdot \psi(\alpha, \beta) \pm k^{\Delta}$$
  Further, if Alice is uncorrupted, it must hold that $t_{\text{A}} \in \Lambda_{\text{A}}^*$ (but not necessarily $t_{\text{B}} \in \Lambda_{\text{B}}^*$). Analogously, if Bob is uncorrupted, it must hold that $t_{\text{B}} \in \Lambda_{\text{B}}^*$ (but not necessarily $t_{\text{A}} \in \Lambda_{\text{A}}^*$).

  If such a compound string $t_{\text{A}} \times t_{\text{B}}$ is sent for the first time, resample each $t_{\text{A}}[i]$ and/or $t_{\text{B}}[i]$ as follows:
  - If no party is corrupted, resample the complete tuple $\big(t_{\text{A}}[i], t_{\text{B}}[i]\big)$ according to ψ.
  - If only Alice is corrupted and $t_{\text{A}}[i] \in \Lambda_{\text{A}}$, then resample $t_{\text{B}}[i]$, s.t. $\mathbf{P}\big[t_{\text{B}}[i] = \beta\big] = \frac{\psi(t_{\text{A}}[i],\beta)}{\psi(t_{\text{A}}[i],\Lambda_{\text{B}})}$.
  - If only Bob is corrupted and $t_{\text{B}}[i] \in \Lambda_{\text{B}}$, then resample $t_{\text{A}}[i]$, s.t. $\mathbf{P}\big[t_{\text{A}}[i] = \alpha\big] = \frac{\psi(\alpha,t_{\text{B}}[i])}{\psi(\Lambda_{\text{A}},t_{\text{B}}[i])}$.
  - If both parties are corrupted or $\big(t_{\text{A}}[i], t_{\text{B}}[i]\big) \notin \Lambda_{\text{A}} \times \Lambda_{\text{B}}$, then neither resample $t_{\text{A}}[i]$ nor $t_{\text{B}}[i]$.

  Next, record the resulting compound string $t_{\text{A}} \times t_{\text{B}}$. Henceforth, ignore any further $t_{\text{A}} \times t_{\text{B}}$-messages from the adversary.
- Upon receiving a message $(\texttt{Delivery}, \texttt{Alice})$ from the adversary, verify that there is a stored compound string $t_{\text{A}} \times t_{\text{B}}$; else ignore that message. Next, output t_{A} to Alice and henceforth ignore all messages $(\texttt{Delivery}, \texttt{Alice})$.
- Upon receiving a message $(\texttt{Delivery}, \texttt{Bob})$ from the adversary, verify that there is a stored compound string $t_{\text{A}} \times t_{\text{B}}$; else ignore that message. Next, output t_{B} to Bob and henceforth ignore all messages $(\texttt{Delivery}, \texttt{Bob})$.
- Upon receiving any message from Alice or Bob, just forward it to the adversary, inclusive the original sender ID.

Figure 6: Ideal functionality for correlated data generation by our protocol scheme based on finite randomized 2-party functions. Corrupted parties have full control over the order of their output string, since order is nowhere checked in our protocol scheme. The resampling just ensures that corrupted parties have no information about honest parties' outputs, other than what they learn by their own output. The condition that $\psi(\alpha, \Lambda_{\text{B}}) > 0$ and $\psi(\Lambda_{\text{A}}, \beta) > 0$ for all $\alpha \in \Lambda_{\text{A}}$, $\beta \in \Lambda_{\text{B}}$ is needed to avoid division by zero during the resampling process. The constant Δ is motivated by the Hoeffding Inequality (q.v. Section 3.1.4); w.l.o.g. we always have that $\varepsilon < \frac{1}{2}$ and thus $\Delta > \frac{1}{2}$.

Now, let us consider the protocol scheme from Section 3.1.1, instantiated as follows.

- The underlying 2-party function $F := (\Upsilon_{\text{A}}, \Upsilon_{\text{B}}, \Omega_{\text{A}}, \Omega_{\text{B}}, \phi) \in \mathfrak{F}_{\text{fin}}$ is redundancy-free.
- The canonical representation of F has an OT-core that is robust in the sense of Section 3.1.3.
- Alice and Bob each have to use their respective OT-core inputs $\bar{x}, \bar{x}'$ and $\bar{y}, \bar{y}'$ with equal probability, and all other input symbols with some polynomially vanishing probability.
- There exists some constant $\varepsilon > 0$, such that $k - k^{1-\varepsilon}$ elements of the final output strings are generated honestly, even if one party is corrupted (cf. the final discussion in Section 3.1.1).

Given such a setting, our protocol implements the functionality $\mathcal{F}_{\text{SMCD}}^{(G,\varepsilon)}$ defined in Figure 6, where $G = (\Lambda_{\text{A}}, \Lambda_{\text{B}}, \psi)$, instantiated as follows (cf. Section 4.8):

$$\Lambda_{\text{A}} = \{\bar{x}, \bar{x}'\} \times \Omega_{\text{A}} \qquad\qquad \Lambda_{\text{B}} = \{\bar{y}, \bar{y}'\} \times \Omega_{\text{B}} \qquad\qquad \psi\big((x,a),(y,b)\big) = \frac{\phi_{x,y}(a,b)}{\big|\{\bar{x}, \bar{x}'\} \times \{\bar{y}, \bar{y}'\}\big|}$$

$$\text{a)}\ \begin{array}{|cccc|}\hline \frac{1}{6} & \frac{1}{3} & \frac{1}{2} & \\ \hline \frac{1}{6} & \frac{1}{3} & & \frac{1}{2} \\ \hline \end{array} \qquad \text{b)}\ \begin{array}{|cccc|}\hline \frac{1}{12} & \frac{1}{6} & \frac{1}{4} & \\ \frac{1}{12} & \frac{1}{6} & & \frac{1}{4} \\ \hline \end{array} \qquad \text{c)}\ \begin{array}{|ccc|}\hline \frac{1}{4} & \frac{1}{4} & \\ \frac{1}{4} & & \frac{1}{4} \\ \hline \end{array}$$

Figure 7: Canonical representation of a 2-party function (a), the resulting correlated data distribution (b), and condensed version of the latter (c).

3.2 Reduction of OT to correlated data

In Section 3.1 we have seen how to securely generate non-trivially correlated data from any redundancy-free 2-party function that has some OT-core. Now we have to implement OT from such data, i.e. we have to construct an OT protocol based on the functionality $\mathcal{F}_{\mathrm{SMCD}}^{(G,\varepsilon)}$ in Figure 6. This protocol construction is only a minor contribution, since in large part the used techniques are just adopted from the standard literature (cf. Section 1.1) and in particular from [CMW05].

Note that in a straightforward manner we can identify $G := (\Lambda_\mathrm{A}, \Lambda_\mathrm{B}, \psi)$ with a special 2-party function $F := (\{\epsilon\}, \{\epsilon\}, \Lambda_\mathrm{A}, \Lambda_\mathrm{B}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ with $\phi_{\epsilon,\epsilon} = \psi$, although the functionality $\mathcal{F}_{\mathrm{SMCD}}^{(G,\varepsilon)}$ works completely different from $\mathcal{F}_{\mathrm{SFE}}^{(F)}$. However, our notions of canonical representations, condensed canonical representations, isomorphism (q.v. Section 2.2) and OT-cores (q.v. Section 2.3) directly carry over (cf. also Figure 7). Our notion of redundancy does not apply, since there are no meaningful inputs anymore. In the upcoming subsections we always consider the functionality $\mathcal{F}_{\mathrm{SMCD}}^{(G,\varepsilon)}$, where $G = (\Lambda_\mathrm{A}, \Lambda_\mathrm{B}, \psi)$ and G has some OT-core. W.l.o.g., G is always given in condensed form, meaning that the rows of its canonical representation are pairwise linearly independent and so are the columns.

3.2.1 Refining the correlated data

Removal of unnecessary output symbols. The joint distribution ψ can still be fairly complex, but by the following protocol we can iteratively remove specific symbols from Λ_A and also analogously from Λ_B, until $|\Lambda_\mathrm{A}| = |\Lambda_\mathrm{B}| = 2$ and thus w.l.o.g. $\Lambda_\mathrm{A} = \Lambda_\mathrm{B} = \{0, 1\}$. Let $\hat{\alpha}$ denote the symbol to be removed from Λ_A. W.l.o.g., G is given in condensed form, i.e. there is no other row in the canonical representation that linearly depends on the $\hat{\alpha}$-row. For our upcoming protocol we will also need that the $\hat{\alpha}$-row in the canonical representation of G is no convex combination of any other rows. And since we do not want to destroy the last OT-core of G by removal of $\hat{\alpha}$, there must exist some OT-core outside of the $\hat{\alpha}$-row. However, as one verifies straightforwardly, $\hat{\alpha}$ can always be chosen this way, if only $|\Lambda_\mathrm{A}| > 2$ (remember that we assumed G to be given in condensed form) and G has an OT-core at all. The protocol for removing $\hat{\alpha}$ now just proceeds as follows.

1. Alice announces the index set $I := \big\{ i \in \mathbb{N} \;\big|\; t_\mathrm{A}[i] = \hat{\alpha} \big\}$.
2. Bob verifies that $\big| t_\mathrm{B}[I] \big|_\beta = k \cdot \psi(\hat{\alpha}, \beta) \pm k^\Delta$ for all $\beta \in \Lambda_\mathrm{B}$, where $t_\mathrm{B}[I]$ denotes the substring of t_B indexed by I; otherwise he aborts the protocol. If there exists any $\beta \in \Lambda_\mathrm{B}$, such that $\psi\big(\Lambda_\mathrm{A} \backslash \{\hat{\alpha}\}, \beta\big) = 0$ and $\big| t_\mathrm{B}[I] \big|_\beta < \big| t_\mathrm{B} \big|_\beta$, he also aborts the protocol.
3. Alice and Bob remove the elements indexed by I from t_A and t_B respectively.

Note that Alice cannot lie substantially often, if only the $\hat{\alpha}$-row in the canonical representation is no convex combination of other rows. Thus, we can implement this way $\mathcal{F}_{\mathrm{SMCD}}^{G',\varepsilon'}$ from $\mathcal{F}_{\mathrm{SMCD}}^{G,\varepsilon}$, where $0 < \varepsilon' < \varepsilon$ and G' is obtained from G just by removing $\hat{\alpha}$ from Λ_A and some rescaling of ψ. In particular, we have that $G' = (\Lambda'_\mathrm{A}, \Lambda_\mathrm{B}, \psi')$, where $\Lambda'_\mathrm{A} = \Lambda_\mathrm{A} \backslash \{\hat{\alpha}\}$ and $\psi'(\alpha, \beta) = \frac{\psi(\alpha,\beta)}{1-\psi(\hat{\alpha},\Lambda_\mathrm{B})}$ for all $\alpha \in \Lambda'_\mathrm{A}, \beta \in \Lambda_\mathrm{B}$. Note that this also linearly scales down the security parameter by the factor $1 - \psi(\hat{\alpha}, \Lambda_\mathrm{B})$. Moreover, after removing the $\hat{\alpha}$-row from the canonical representation of G, several columns may become pairwise linearly dependent, what results in a considerably smaller condensed canonical representation of G'. However, as long as the canonical representation of G without the $\hat{\alpha}$-row still contains an OT-core, G' will also have one—full-rank submatrices cannot be completely destroyed by just adding up pairwise linearly dependent columns. So, by iterated removal of single input symbols, we end up with a condensed canonical representation that just *is* an OT-core. Finally, if $\psi(\alpha, \Lambda_{\mathrm{B}}) > \psi(\alpha', \Lambda_{\mathrm{B}})$ for some $\alpha, \alpha' \in \Lambda_{\mathrm{A}}$, we let Alice analogously remove some α-elements from t_{A}, so that afterwards $\psi(\alpha, \Lambda_{\mathrm{B}}) = \psi(\alpha', \Lambda_{\mathrm{B}})$ for all $\alpha, \alpha' \in \Lambda_{\mathrm{A}}$.

This removal of unnecessary output symbols and balancing of Alice's output distribution is UC-secure; the simulator construction and security proof can be sketched as follows. Talking in terms of the UC framework, we are in the $\mathcal{F}_{\mathrm{SMCD}}^{(G,\varepsilon)}$-hybrid model and want to implement the ideal functionality $\mathcal{F}_{\mathrm{SMCD}}^{G',\varepsilon'}$. If no party is corrupted, the simulator basically needs to send a compound string of correct length to the ideal functionality $\mathcal{F}_{\mathrm{SMCD}}^{G',\varepsilon'}$, and he can produce such a string simply by simulating a complete protocol run with honest parties. If Alice is corrupted, basically all she can do is trying to choose the index set I maliciously. Note that $|t_{\mathrm{A}}|_{\Lambda_{\mathrm{A}}} \geq k - |\Lambda_{\mathrm{A}} \times \Lambda_{\mathrm{B}}| \cdot k^{\Delta}$ by the construction of $\mathcal{F}_{\mathrm{SMCD}}^{(G,\varepsilon)}$, i.e. $t_{\mathrm{A}}[i] \notin \Lambda_{\mathrm{A}}$ for at most $|\Lambda_{\mathrm{A}} \times \Lambda_{\mathrm{B}}| \cdot k^{\Delta}$ indices i. Further, by the Hoeffding Inequality we have for every $\beta \in \Lambda_{\mathrm{B}}$ that with overwhelming probability $\left|t_{\mathrm{A}} \times t_{\mathrm{B}}[I]\right|_{\Lambda_{\mathrm{A}} \times \{\beta\}} = \sum_{\alpha \in \Lambda_{\mathrm{A}}} \left|t_{\mathrm{A}}[I]\right|_{\alpha} \cdot \frac{\psi(\alpha,\beta)}{\psi(\alpha,\Lambda_{\mathrm{B}})} \pm k^{\Delta}$, and hence $\left|t_{\mathrm{B}}[I]\right|_{\beta} = \sum_{\alpha \in \Lambda_{\mathrm{A}}} \left|t_{\mathrm{A}}[I]\right|_{\alpha} \cdot \frac{\psi(\alpha,\beta)}{\psi(\alpha,\Lambda_{\mathrm{B}})} \pm \big(1 + |\Lambda_{\mathrm{A}} \times \Lambda_{\mathrm{B}}|\big) k^{\Delta}$. Since otherwise Bob aborts the protocol, this implies that $\sum_{\alpha \in \Lambda_{\mathrm{A}}} \left|t_{\mathrm{A}}[I]\right|_{\alpha} \cdot \frac{\psi(\alpha,\beta)}{\psi(\alpha,\Lambda_{\mathrm{B}})} = k \cdot \psi(\hat{\alpha}, \beta) \pm \big(2 + |\Lambda_{\mathrm{A}} \times \Lambda_{\mathrm{B}}|\big) k^{\Delta}$, or in other words:

$$\sum_{\alpha \in \Lambda_{\mathrm{A}}} \frac{|t_{\mathrm{A}}[I]|_{\alpha}}{k \cdot \psi(\alpha,\Lambda_{\mathrm{B}})} \cdot \psi(\alpha, \beta) \ = \ \psi(\hat{\alpha}, \beta) \pm \big(2 + |\Lambda_{\mathrm{A}} \times \Lambda_{\mathrm{B}}|\big) k^{-\varepsilon}$$

Since by assumption the $\hat{\alpha}$-row in the canonical representation of G is bounded away from the convex hull of all other rows, this eventually yields that Alice must choose the index set I correctly up to some $O(k^{1-\varepsilon})$-error. This is simulatable, since the ideal functionality $\mathcal{F}_{\mathrm{SMCD}}^{G',\varepsilon'}$ even tolerates $k^{1-\varepsilon'}$-errors, and we have chosen $\varepsilon' < \varepsilon$. Finally, a corrupted Bob can just maliciously abort the protocol, which can be simulated trivially.

Balancing of Bob's output distribution. By the method above we have implemented $\mathcal{F}_{\mathrm{SMCD}}^{(G,\varepsilon)}$ with $G = (\Lambda_{\mathrm{A}}, \Lambda_{\mathrm{B}}, \psi)$, such that w.l.o.g. $\Lambda_{\mathrm{A}} = \Lambda_{\mathrm{B}} = \{0,1\}$ and $\psi(0, \Lambda_{\mathrm{B}}) = \psi(1, \Lambda_{\mathrm{B}})$. Moreover, w.l.o.g. we have that $\psi(0,0) \cdot \psi(1,1) > \psi(1,0) \cdot \psi(0,1)$; otherwise we just have to interchange the meaning of "0" and "1" on either Alice's or Bob's side. We now further refine the correlated data, such that afterwards the joint distribution is completely balanced in 0 and 1. Therefor, we need to extend Bob's alphabet Λ_{B} by a special erasure symbol "$\perp$". In particular, we implement something similar to $\mathcal{F}_{\mathrm{SMCD}}^{(G',\varepsilon')}$ with $G' = (\{0,1\}, \{0,1,\perp\}, \psi')$, such that $\psi'(0,\perp) = \psi'(1,\perp) > 0$ and $\psi'(0,0) = \psi'(1,1) > \psi'(1,0) = \psi'(0,1)$. However, in doing so we will halve the security parameter.

1. Alice deletes $\big||t_{\mathrm{A}}|_0 - |t_{\mathrm{B}}|_1\big|$ elements from t_{A}, such that afterwards $|t_{\mathrm{A}}|_0 = |t_{\mathrm{B}}|_1$. She announces the corresponding indices to Bob, who deletes the according elements from t_{B}, too. If afterwards $|t_{\mathrm{B}}|$ is not an even number or Alice announced more than k^{Δ} indices, Bob aborts.
2. Alice randomly permutes t_{A} subject to the condition that afterwards $t_{\mathrm{A}}[i] \neq t_{\mathrm{A}}[i+1]$ for all odd indices i. She announces the permutation to Bob, who permutes t_{B} the same way.
3. Alice and Bob locally generate new strings $t'_{\mathrm{A}} \in \{0,1\}^*$ and $t'_{\mathrm{B}} \in \{0,1,\perp\}^*$ of half length as follows:

$$\begin{aligned}
t'_{\mathrm{A}}[i] &:= 0 \quad \text{if } \big(t_{\mathrm{A}}[2i-1], t_{\mathrm{A}}[2i]\big) = (0,1) & \qquad t'_{\mathrm{B}}[i] &:= 0 \quad \text{if } \big(t_{\mathrm{B}}[2i-1], t_{\mathrm{B}}[2i]\big) = (0,1)\\
t'_{\mathrm{A}}[i] &:= 1 \quad \text{if } \big(t_{\mathrm{A}}[2i-1], t_{\mathrm{A}}[2i]\big) = (1,0) & \qquad t'_{\mathrm{B}}[i] &:= 1 \quad \text{if } \big(t_{\mathrm{B}}[2i-1], t_{\mathrm{B}}[2i]\big) = (1,0)\\
& & t'_{\mathrm{B}}[i] &:= \perp \quad \text{if } t_{\mathrm{B}}[2i-1] = t_{\mathrm{B}}[2i]
\end{aligned}$$

4. Bob aborts the protocol, if it holds:
$$|t'_{\mathrm{B}}|_{\perp} \;>\; \frac{k}{2}\cdot\frac{\psi(0,0)\cdot\psi(1,0)+\psi(0,1)\cdot\psi(1,1)}{\psi(0,\Lambda_{\mathrm{B}})\cdot\psi(1,\Lambda_{\mathrm{B}})}+k^{\Delta}$$
5. Alice outputs t'_{A} and Bob outputs t'_{B}.

This way we get:

$$\begin{aligned}
\psi'(0,0) &= \frac{\psi(0,0)\cdot\psi(1,1)}{2\cdot\psi(0,\Lambda_{\mathrm{B}})\cdot\psi(1,\Lambda_{\mathrm{B}})} & \qquad \psi'(0,\perp) &= \frac{\psi(0,0)\cdot\psi(1,0)+\psi(0,1)\cdot\psi(1,1)}{2\cdot\psi(0,\Lambda_{\mathrm{B}})\cdot\psi(1,\Lambda_{\mathrm{B}})}\\
\psi'(0,1) &= \frac{\psi(0,1)\cdot\psi(1,0)}{2\cdot\psi(0,\Lambda_{\mathrm{B}})\cdot\psi(1,\Lambda_{\mathrm{B}})} & \qquad \psi'(1,\perp) &= \frac{\psi(1,0)\cdot\psi(0,0)+\psi(1,1)\cdot\psi(0,1)}{2\cdot\psi(0,\Lambda_{\mathrm{B}})\cdot\psi(1,\Lambda_{\mathrm{B}})}\\
\psi'(1,0) &= \frac{\psi(1,0)\cdot\psi(0,1)}{2\cdot\psi(0,\Lambda_{\mathrm{B}})\cdot\psi(1,\Lambda_{\mathrm{B}})} & &\\
\psi'(1,1) &= \frac{\psi(1,1)\cdot\psi(0,0)}{2\cdot\psi(0,\Lambda_{\mathrm{B}})\cdot\psi(1,\Lambda_{\mathrm{B}})} & &
\end{aligned}$$

Note that Bob just cannot cheat at all, but he must prevent Alice from maliciously choosing a permutation that yields $t_{\mathrm{A}}[i]=t_{\mathrm{A}}[i+1]$ for substantially many odd indices i in the first step. This is what the fourth protocol step is needed for. According to the Hoeffding Inequality, $|t'_{\mathrm{B}}|_{\perp}$ is raised asymptotically by $\Omega(\bar{n}-k^{\Delta})$, where $\bar{n}$ denotes the number of odd indices i with $t_{\mathrm{A}}[i]=t_{\mathrm{A}}[i+1]$ after the permutation. Thus, a corrupted Alice is caught cheating with overwhelming probability, if $\bar{n}\notin O(k^{\Delta})$. Moreover, a corrupted Bob has no control over the order of the final output strings any more, due to Alice's random permutation in the first protocol step. Putting things together, there exist some constants $\varepsilon',\varepsilon'',\tilde{\varepsilon},\tilde{\nu}\in(0,1)$, particularly $\tilde{\nu}=\psi'(\{0,1\},\perp)$ and $\tilde{\varepsilon}=\frac{\psi'(0,1)+\psi'(1,0)}{1-\tilde{\nu}}$, such that we have now the following situation with κ denoting the new security parameter.

- Alice's output is a uniformly random string $t'_{\mathrm{A}}\in\{0,1\}^{\kappa}$.
- Bob's output $t'_{\mathrm{B}}\in\{0,1,\perp\}^{\kappa}$ is randomly generated according to the following probabilities:
$$\begin{aligned}
\mathbf{P}\big[t'_{\mathrm{B}}[i]=t'_{\mathrm{A}}[i]\big] &= (1-\tilde{\nu})\cdot(1-\tilde{\varepsilon})\\
\mathbf{P}\big[t'_{\mathrm{B}}[i]=\neg t'_{\mathrm{A}}[i]\big] &= (1-\tilde{\nu})\cdot\tilde{\varepsilon}\\
\mathbf{P}\big[t'_{\mathrm{B}}[i]=\perp\big] &= \tilde{\nu}
\end{aligned}$$
- If Alice is corrupted, she may choose her output $t'_{\mathrm{A}}\in\{0,1\}^{\kappa}$ arbitrarily and afterwards learn some additional information about up to $\kappa^{1-\varepsilon'}$ arbitrarily chosen elements of t'_{B}.
- For up to $\kappa^{1-\varepsilon''}$ random indices $i\in\{1,\ldots,\kappa\}$, a corrupted Bob my learn some additional information about $t'_{\mathrm{A}}[i]$.

Note that $\tilde{\varepsilon}<\frac{1}{2}$, since $\psi'(0,0)=\psi'(1,1)>\psi'(1,0)=\psi'(0,1)$ by construction. The implemented functionality is different from $\mathcal{F}_{\mathrm{SMCD}}^{(G',\varepsilon')}$, insofar as a corrupted Bob has no longer control over his output order or for which indices i he gets additional information about $t'_{\mathrm{A}}[i]$, but a corrupted Alice can now arbitrarily choose her output string t'_{A} provided that $|t'_{\mathrm{A}}|_{\{0,1\}}\geq\kappa-\kappa^{1-\varepsilon'}$. Nonetheless, we still have a UC-secure implementation of this modified version of $\mathcal{F}_{\mathrm{SMCD}}^{(G',\varepsilon')}$. The respective simulator construction and security proof are pretty similar to those for our protocol above for removal of unnecessary output symbols.

3.2.2 Building OT from the refined correlated data

Let $\varepsilon', \varepsilon'', \tilde{\varepsilon}, \tilde{\nu}, \kappa, t'_{\mathrm{A}}, t'_{\mathrm{B}}$ as above. If Alice is honest, we can easily implement from this a non-trivial binary symmetric erasure channel (BSEC) that allows Alice to send κ bits and then shuts down: To send the i-th bit, say $m[i]$, Alice just has to announce $\tilde{m}[i] := m[i] \oplus t'_{\mathrm{A}}[i]$ to Bob. Bob then can recover a noisy version $m'[i]$ of $m[i]$ by computing $m'(i) = \tilde{m}[i] \oplus t'_{\mathrm{B}}[i]$ with the convention that $0 \oplus \bot = 1 \oplus \bot = \bot$. Obviously, the implemented BSEC has the following properties:

- If Bob is honest, the erasure probability is $\tilde{\nu}$.
- If Bob is corrupted, the erasure probability is still lower bounded by $\tilde{\nu} - \kappa^{-\varepsilon''}$.
- If Bob is honest, the error probability is $(1 - \tilde{\nu}) \cdot \tilde{\varepsilon}$.
- If Bob is corrupted, the error probability is still lower bounded by $(1 - \tilde{\nu}) \cdot \tilde{\varepsilon} - \kappa^{-\varepsilon''}$.

I.e., the differences between the channel characteristics for an uncorrupted and a corrupted Bob are polynomially vanishing in the security parameter. Especially, the channel parameters for a corrupted Bob do converge to the corresponding parameters of the honest case. This is good enough, so that our BSEC can be transformed into OT statistically secure against a corrupted receiver party Bob just by applying one of the protocols from the literature [CMW05, Wul09, IKO$^+$11]. Note that although only [IKO$^+$11] is explicitly stated in the UC framework, the security proofs of the other approaches can also be turned into UC proofs rather simply.

However, we still have to take care of a corrupted Alice, who can additionally learn $t'_{\mathrm{B}}[i]$ for up to $\kappa^{1-\varepsilon'}$ arbitrarily chosen indices i. We deal with this as follows. Instead of implementing a single BSEC that can be used κ times, we implement $\ell := \lfloor \kappa^{1-\varepsilon'} + 1 \rfloor$ BSECs that each can be used $\lambda := \lfloor \kappa / \ell \rfloor$ times. We just use the first λ elements of t'_{A} and t'_{B} for the first BSEC, the next λ elements of t'_{A} and t'_{B} for the second BSEC, and so on. Analogously to above, this gives us ℓ OTs with polynomially downscaled security parameter λ, each of which is statistically UC-secure against a corrupted receiver Bob. But now, since a corrupted Alice can cheat at most $\kappa^{1-\varepsilon'}$ times, at last one of these OTs is also statistically UC-secure against Alice. Finally, we can use a simple standard combiner to achieve a fully (i.e. against both parties) UC-secure OT instance:

0. Let (b_0, b_1) denote Alice's respective sender input and let c denote Bob's choice bit.
1. Alice chooses two ℓ-bit strings $\hat{b}_0, \hat{b}_1 \in \{0,1\}^\ell$ uniformly at random, subject to the condition that $\bigoplus_{i=1}^{\ell} \hat{b}_0[i] = b_0$ and $\hat{b}_0[i] \oplus \hat{b}_1[i] = b_0 \oplus b_1$ for all $i \in \{1, \ldots, \ell\}$.
   Bob chooses $\hat{c} \in \{0,1\}^\ell$ uniformly at random, subject to the condition that $\bigoplus_{i=1}^{\ell} \hat{c}[i] = c$.
2. For each $i \in \{1, \ldots, \ell\}$, Alice and Bob run OT with sender input $\big(\hat{b}_0[i], \hat{b}_1[i]\big)$ from Alice and choice bit $\hat{c}[i]$ from Bob, such that all ℓ OT instances are secure against Bob and at least one instance is secure against Alice.
3. Bob computes and outputs $b_c = \bigoplus_{i=1}^{\ell} \hat{b}_{\hat{c}[i]}[i]$.

It is not hard to verify that this protocol is correct, hides c from Alice, and Bob may learn at most one of the bit values b_0, b_1. Even if Alice maliciously chooses $(\hat{b}_0, \hat{b}_1)$ such that $\hat{b}_0[i] \oplus \hat{b}_1[i]$ is not the same for all $i \in \{1, \ldots, \ell\}$, this means no security violation: It only randomizes Bob's final output, which she could as well achieve by choosing her protocol input (b_0, b_1) just uniformly at random in the first place.

This whole construction can easily be proven UC-secure, since by UC-security of the ℓ OT subprotocols in step 2 of our combiner even for corrupted parties the corresponding inputs $\big(\hat{b}_0[i], \hat{b}_1[i]\big)$ and $\hat{c}[i]$ are always well-defined. We only have to take into account that a corrupted Alice may additionally learn up to $\ell - 1$ bits of $\hat{c}$. However, this is just pure randomness, uncorrelated with everything else. The general idea of how the simulation in the ideal model works can be described as follows.

- If Alice is corrupted, the simulator lets her run the protocol with a simulated instance of Bob, whose choice bit c is just uniform randomness. After step 2 the simulator can easily extract $b_c = \bigoplus_{i=1}^{\ell} \hat{b}_{\hat{c}[i]}[i]$, compute $b_{\neg c} = b_c \oplus \hat{b}_o[j] \oplus \hat{b}_1[j]$ with j corresponding to an OT instance that were secure against Alice, and finally send (b_0, b_1) to the ideal functionality.
- If Bob is corrupted, the simulator lets him run the protocol with a simulated instance of Alice, whose sender input (b_0, b_1) is just uniform randomness. At the beginning of the final iteration of step 2 the simulator can easily extract $c = \bigoplus_{i=1}^{\ell} \hat{c}[i]$, send c to the ideal functionality, and thus learn b_c. Then, if $b_c \neq \bigoplus_{i=1}^{\ell} \hat{b}_{\hat{c}[i]}[i]$, he just has to flip the bit values of $\hat{b}_0[\ell]$ and $\hat{b}_1[\ell]$ in the simulated Alice's memory before he resumes simulating the rest of step 2. This is perfectly indistinguishable from a real protocol run, unless a corrupted Bob can gather some information about $\hat{b}_0[i] \oplus \hat{b}_1[i]$ for any $i \in \{1, \ldots, \ell\}$. However, the latter is ruled out by security against Bob of the underlying ℓ OT instances.

Once again, we omit the fully detailed UC proof, since it does not contain any additional technical insights. This concludes our more informal exposition of how one can prove the Classification Theorem from Section 2.3.

4 Formal part

In this section, we formally prove that secure generation of correlated data (in the sense of Figure 6) can be implemented from any redundancy-free 2-party function $F \in \mathfrak{F}_{\mathsf{fin}}$ that has some OT-core. This is our main technical contribution, since OT can be reduced to such correlated data by rather standard techniques (q.v. Section 3.2).

4.1 Basic notions and notations

We start off with a collective (re)statement of all definitions and notations that are used throughout the rest of this paper.

Notation 1 (Finite sums of function values). Given a set T with finite subset $S \subseteq T$ and some mapping $g : T \to \mathbb{R}$, we set $g(S) := \sum_{\omega \in S} g(\omega)$. For functions with more arguments we use the canonical extension of this notation, e.g. $h(a, B, C, d) := \sum_{\beta \in B, \gamma \in C} h(a, \beta, \gamma, d)$.

Notation 2 (Spaces of probability mass functions). Given some finite alphabet Ω, we denote the set of all probability mass functions over Ω by $\mathrm{pmf}(\Omega)$, i.e. $\mathrm{pmf}(\Omega) = \big\{\rho : \Omega \to \mathbb{R}_{\geq 0} \bigm| \rho(\Omega) = 1\big\}$.

Notation 3 (Finite randomized 2-party functions). Let $\mathfrak{F}_{\mathsf{fin}}$ denote the set of all quintuples $(\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, \phi)$, where $\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}$ are non-empty finite alphabets and $\phi = \{\phi_{x,y}\}_{x \in \Upsilon_\mathrm{A}, y \in \Upsilon_\mathrm{B}}$ is a family of probability mass functions over $\Omega_\mathrm{A} \times \Omega_\mathrm{B}$, i.e. $\phi \subseteq \mathrm{pmf}(\Omega_\mathrm{A} \times \Omega_\mathrm{B})$.

Definition 4 (Redundancy). Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$. An input symbol $y' \in \Upsilon_\mathrm{B}$ is called *redundant*, if there exist some $\iota \in \mathrm{pmf}(\Upsilon_\mathrm{B})$ and a family of probability mass functions $\{\lambda_{y,b}\}_{y \in \Upsilon_\mathrm{B}, b \in \Omega_\mathrm{B}} \subseteq \mathrm{pmf}(\Omega_\mathrm{B})$, such that $\iota(y') = 0$ and for all $x \in \Upsilon_\mathrm{A}$, $a \in \Omega_\mathrm{A}$, $b' \in \Omega_\mathrm{B}$ it holds:

$$\phi_{x,y'}(a, b') = \sum\nolimits_{y \in \Upsilon_\mathrm{B},\, b \in \Omega_\mathrm{B}} \iota(y) \cdot \phi_{x,y}(a, b) \cdot \lambda_{y,b}(b')$$

For input symbols $x \in \Upsilon_\mathrm{A}$ redundancy is defined analogously. If neither Υ_A nor Υ_B contains any redundant input symbols, F is called *redundancy-free.*

Definition 5 (Cheating situations). For $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ let $\mathfrak{N}_\mathrm{B}^{(F)}$ denote the set of all probability mass functions $\eta \in \mathrm{pmf}\big((\Upsilon_\mathrm{A} \times \Omega_\mathrm{A}) \times (\Upsilon_\mathrm{B} \times \Omega_\mathrm{B})^2\big)$ that meet the following conditions.

1. For all $x \in \Upsilon_{\mathrm{A}}$ it holds that $\eta|_{\mathrm{A}}(x) := \eta\big((x, \Omega_{\mathrm{A}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) > 0$.
2. For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$, $b \in \Omega_{\mathrm{B}}$, with $\eta|_{\mathrm{B}}^{\mathsf{true}}(y) := \eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, \Omega_{\mathrm{B}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)$, it holds:
$$\eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) = \eta|_{\mathrm{A}}(x) \cdot \eta|_{\mathrm{B}}^{\mathsf{true}}(y) \cdot \phi_{x,y}(a,b)$$
3. For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y' \in \Upsilon_{\mathrm{B}}$, $b' \in \Omega_{\mathrm{B}}$, with $\eta|_{\mathrm{B}}^{\mathsf{fake}}(y') := \eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y', \Omega_{\mathrm{B}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)$, it holds:
$$\eta\big((x,a),(\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}),(y',b')\big) = \eta|_{\mathrm{A}}(x) \cdot \eta|_{\mathrm{B}}^{\mathsf{fake}}(y') \cdot \phi_{x,y'}(a,b')$$
4. For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$, $b, b' \in \Omega_{\mathrm{B}}$ with $\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y,b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) > 0$ it holds:
$$\eta\big((x,a),(y,b),(y',b')\big) = \eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}),(y,b),(y',b')\big) \cdot \frac{\eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)}{\eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)}$$

The mappings $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ are called *Bob's cheating situations for F*. The set $\mathfrak{N}_{\mathrm{A}}^{(F)}$ of *Alice's cheating situations for F* is defined analogously.

Definition 6 (Special cheating situations)**.** Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$. We define the following subsets of $\mathfrak{N}_{\mathrm{B}}^{(F)}$.

Normalized cheating situations: A cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ is called *normalized*, if $\eta|_{\mathrm{A}}(x) = \frac{1}{|\Upsilon_{\mathrm{A}}|}$ for all $x \in \Upsilon_{\mathrm{A}}$.

Trivial cheating situations: A cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ is called *trivial*, if for all $y, y' \in \Upsilon_{\mathrm{B}}$ and $b, b' \in \Omega_{\mathrm{B}}$ the following implication holds true:
$$(y,b) \neq (y',b') \quad \Rightarrow \quad \eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}),(y,b),(y',b')\big) = 0$$

Direct cheating situations: A cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ is called *direct*, if for each $(y,b) \in \Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}}$ at least one of the following two equalities holds true:
$$\eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) = \eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}),(y,b),(y,b)\big)$$
$$\eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}),(y,b)\big) = \eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}),(y,b),(y,b)\big)$$

Straight cheating situations: A cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ is called *straight*, if for each $y \in \Upsilon_{\mathrm{B}}$ at least one of the following two equalities holds true:
$$\hat{\eta}|_{\mathrm{B}}^{\mathsf{true}}(y) = 0 \qquad \text{or} \qquad \hat{\eta}|_{\mathrm{B}}^{\mathsf{fake}}(y) = 0$$

Definition 7 (Cheating characteristics)**.** For $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ let $\mathfrak{X}_{\mathrm{B}}^{(F)}$ denote the set of all mappings $\xi : \Upsilon_{\mathrm{B}} \to \mathbb{R}$ for that exist some cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ and some $\gamma \in \mathbb{R}_{>0}$, such that for all $y \in \Upsilon_{\mathrm{B}}$ it holds:
$$\gamma \cdot \xi(y) = \eta|_{\mathrm{B}}^{\mathsf{fake}}(y) - \eta|_{\mathrm{B}}^{\mathsf{true}}(y)$$

4.2 Linear properties of cheating situations

In this section we show that cheating situations can be considered independent from the honest party's input distribution, since they can be canonically rescaled (Lemma 8 and Corollary 9). Further, we show how the algebraic structures $\mathfrak{N}_{\mathrm{B}}^{(F)}$ and $\mathfrak{X}_{\mathrm{B}}^{(F)}$ allow for basic composition and/or decomposition of mixed strategies (Lemma 10 and Corollary 11).

Lemma 8 (Rescalability of cheating situations)**.** *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ and $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$. Further, let $\tau : \Upsilon_{\mathrm{A}} \to \mathbb{R}_{>0}$, such that $\sum_{x\in\Upsilon_{\mathrm{A}}} \tau(x) \cdot \eta|_{\mathrm{A}}(x) = 1$. Then, the following mapping is a cheating situation for F:*

$$\tilde{\eta} : (\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2 \to \mathbb{R}_{\geq 0},\ \big((x,a),(y,b),(y',b')\big) \mapsto \tau(x) \cdot \eta\big((x,a),(y,b),(y',b')\big)$$

Proof. We just have to check the conditions of Definition 5.

0. First note that $\tilde{\eta} \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, since $\mathrm{Image}(\tilde{\eta}) \subseteq \mathbb{R}_{\geq 0}$ and by construction we have:

$$\tilde{\eta}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = \sum\nolimits_{x\in\Upsilon_{\mathrm{A}}} \tau(x) \cdot \eta\big((x,\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = 1$$

1. For all $x \in \Upsilon_{\mathrm{A}}$ it holds that $\tilde{\eta}|_{\mathrm{A}}(x) = \tau(x) \cdot \eta|_{\mathrm{A}}(x) > 0$.

2. For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$, $b \in \Omega_{\mathrm{B}}$ it holds:

$$\tilde{\eta}\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = \tau(x) \cdot \eta|_{\mathrm{A}}(x) \cdot \eta|_{\mathrm{B}}^{\mathsf{true}}(y) \cdot \phi_{x,y}(a,b)$$

By taking the sum over x, a, b it follows that $\tilde{\eta}|_{\mathrm{B}}^{\mathsf{true}} = \eta|_{\mathrm{B}}^{\mathsf{true}}$. This yields:

$$\tilde{\eta}\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = \underbrace{\tau(x) \cdot \eta|_{\mathrm{A}}(x)}_{\tilde{\eta}|_{\mathrm{A}}(x)} \cdot \underbrace{\eta|_{\mathrm{B}}^{\mathsf{true}}(y)}_{\tilde{\eta}|_{\mathrm{B}}^{\mathsf{true}}(y)} \cdot \phi_{x,y}(a,b)$$

3. For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y' \in \Upsilon_{\mathrm{B}}$, $b' \in \Omega_{\mathrm{B}}$ it holds:

$$\tilde{\eta}\big((x,a),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(y',b')\big) = \tau(x) \cdot \eta|_{\mathrm{A}}(x) \cdot \eta|_{\mathrm{B}}^{\mathsf{fake}}(y) \cdot \phi_{x,y}(a,b)$$

By taking the sum over x, a, b' it follows that $\tilde{\eta}|_{\mathrm{B}}^{\mathsf{fake}} = \eta|_{\mathrm{B}}^{\mathsf{fake}}$. This yields:

$$\tilde{\eta}\big((x,a),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(y',b')\big) = \underbrace{\tau(x) \cdot \eta|_{\mathrm{A}}(x)}_{\tilde{\eta}|_{\mathrm{A}}(x)} \cdot \underbrace{\eta|_{\mathrm{B}}^{\mathsf{fake}}(y)}_{\tilde{\eta}|_{\mathrm{B}}^{\mathsf{fake}}(y)} \cdot \phi_{x,y}(a,b)$$

4. For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$, $b, b' \in \Omega_{\mathrm{B}}$ with $\eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) > 0$ it holds:

$$\frac{\eta\big((x,a),(y,b),(y',b')\big)}{\eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big)} = \frac{\eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y',b')\big)}{\eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big)}$$

Thereby for all $y, y' \in \Upsilon_{\mathrm{B}}$, $b, b' \in \Omega_{\mathrm{B}}$ we can conclude:

$$\begin{aligned}
&\eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y',b')\big) \cdot \sum\nolimits_{x\in\Upsilon_{\mathrm{A}},\, a\in\Omega_{\mathrm{A}}} \tau(x) \cdot \eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \\
&= \sum\nolimits_{x\in\Upsilon_{\mathrm{A}},\, a\in\Omega_{\mathrm{A}}} \tau(x) \cdot \eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y',b')\big) \cdot \eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \\
&= \sum\nolimits_{x\in\Upsilon_{\mathrm{A}},\, a\in\Omega_{\mathrm{A}}} \tau(x) \cdot \eta\big((x,a),(y,b),(y',b')\big) \cdot \eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \\
&= \eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \cdot \sum\nolimits_{x\in\Upsilon_{\mathrm{A}},\, a\in\Omega_{\mathrm{A}}} \tau(x) \cdot \eta\big((x,a),(y,b),(y',b')\big)
\end{aligned}$$

In other words, for all $y, y' \in \Upsilon_{\mathrm{B}}$, $b, b' \in \Omega_{\mathrm{B}}$ with $\eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) > 0$ it holds:

$$\frac{\eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, b), (y', b')\big)}{\eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)} = \frac{\sum_{x \in \Upsilon_{\mathrm{A}},\, a \in \Omega_{\mathrm{A}}} \tau(x) \cdot \eta\big((x, a), (y, b), (y', b')\big)}{\sum_{x \in \Upsilon_{\mathrm{A}},\, a \in \Omega_{\mathrm{A}}} \tau(x) \cdot \eta\big((x, a), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)}$$

For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$, $b, b' \in \Omega_{\mathrm{B}}$ with $\tilde{\eta}\big((x, a), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) > 0$ now follows:

$$\begin{aligned}
\frac{\tilde{\eta}\big((x, a), (y, b), (y', b')\big)}{\tilde{\eta}\big((x, a), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)} &= \frac{\tau(x) \cdot \eta\big((x, a), (y, b), (y', b')\big)}{\tau(x) \cdot \eta\big((x, a), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)} \\
&= \frac{\eta\big((x, a), (y, b), (y', b')\big)}{\eta\big((x, a), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)} \\
&= \frac{\eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, b), (y', b')\big)}{\eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)} \\
&= \frac{\sum_{x' \in \Upsilon_{\mathrm{A}},\, a' \in \Omega_{\mathrm{A}}} \tau(x') \cdot \eta\big((x', a'), (y, b), (y', b')\big)}{\sum_{x' \in \Upsilon_{\mathrm{A}},\, a' \in \Omega_{\mathrm{A}}} \tau(x') \cdot \eta\big((x', a'), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)} \\
&= \frac{\tilde{\eta}\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, b), (y', b')\big)}{\tilde{\eta}\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)}
\end{aligned}$$

□

Corollary 9 (Normalizability of cheating situations). *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ and let $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$. Then there exists a unique normalized cheating situation $\tilde{\eta} \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, such that for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$, $b, b' \in \Omega_{\mathrm{B}}$ it holds:*

$$\frac{\eta((x, a), (y, b), (y', b'))}{\eta|_{\mathrm{A}}(x)} = \frac{\tilde{\eta}((x, a), (y, b), (y', b'))}{\tilde{\eta}|_{\mathrm{A}}(x)}$$

Proof. This directly follows by Lemma 8, instantiated as follows:

$$\tau : \Upsilon_{\mathrm{A}} \to \mathbb{R}_{>0},\ x \mapsto \frac{1}{|\Upsilon_{\mathrm{A}}| \cdot \eta|_{\mathrm{A}}(x)}$$

□

Lemma 10 (Convex combinability of cheating situations). *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ and $\upsilon \in \mathrm{pmf}(\Upsilon_{\mathrm{A}})$, such that $\upsilon(x) > 0$ for all $x \in \Upsilon_{\mathrm{A}}$. Then the set of all cheating situations $\eta \in \mathfrak{N}_{\mathrm{B}}(F)$ with $\eta|_{\mathrm{A}} = \upsilon$ is the convex hull of some finite set of vertices in the affine space $\mathbb{R}^{(\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2}$. In particular, for all $\eta, \eta' \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ with $\eta|_{\mathrm{A}} = \eta'|_{\mathrm{A}} = \upsilon$ and each $s \in \mathbb{R}$ the mapping $\tilde{\eta} := s \cdot \eta + (1 - s) \cdot \eta'$ is a normalized cheating situation for F, if only* $\mathrm{Image}(\tilde{\eta}) \subseteq \mathbb{R}_{\geq 0}$.

Proof. It suffices to give a proof for the case that υ is the uniform distribution, i.e. $\upsilon(x) = \frac{1}{|\Upsilon_{\mathrm{A}}|}$ for all $x \in \Upsilon_{\mathrm{A}}$ and thus all considered cheating situations are normalize (q.v. Definition 6). Everything else then follows straightforwardly by Corollary 9.

We just have to adapt the four conditions of Definition 5 to normalized cheating situations. As one verifies quite straightforwardly, the set of all normalized cheating situations for F is the set of all $\eta \in \mathrm{pmf}\big((\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2\big)$ that meet the following conditions.

1. For all $x \in \Upsilon_{\mathrm{A}}$ it holds that $\eta\big((x, \Omega_{\mathrm{A}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) = \frac{1}{|\Upsilon_{\mathrm{A}}|}$.

2. For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$, $b \in \Omega_{\mathrm{B}}$ it holds:

$$\eta\big((x, a), (y, b), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) = \tfrac{1}{|\Upsilon_{\mathrm{A}}|} \cdot \eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, \Omega_{\mathrm{B}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) \cdot \phi_{x,y}(a, b)$$

3. For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y' \in \Upsilon_{\mathrm{B}}$, $b' \in \Omega_{\mathrm{B}}$ it holds:
$$\eta\big((x,a),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(y',b')\big) = \tfrac{1}{|\Upsilon_{\mathrm{A}}|}\cdot\eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(y',\Omega_{\mathrm{B}})\big)\cdot\phi_{x,y'}(a,b')$$

4. For all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y,y' \in \Upsilon_{\mathrm{B}}$, $b,b' \in \Omega_{\mathrm{B}}$ with $\phi_{\Upsilon_{\mathrm{A}},y}(\Omega_{\mathrm{A}},b) > 0$ it holds:
$$\eta\big((x,a),(y,b),(y',b')\big) = \eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y',b')\big)\cdot\frac{\phi_{x,y}(a,b)}{\phi_{\Upsilon_{\mathrm{A}},y}(\Omega_{\mathrm{A}},b)}$$

Since all these conditions are linear, they define a convex polytope in $\mathbb{R}^{(\Upsilon_{\mathrm{A}}\times\Omega_{\mathrm{A}})\times(\Upsilon_{\mathrm{B}}\times\Omega_{\mathrm{B}})^2}$. Note that this polytope is a subset of the bounded set $\mathrm{pmf}\big((\Upsilon_{\mathrm{A}}\times\Omega_{\mathrm{A}})\times(\Upsilon_{\mathrm{B}}\times\Omega_{\mathrm{B}})^2\big)$ and hence also is bounded. Further, as the polytope is described by a finite number of linear constraints, it is the convex hull of a finite set of vertices. Finally, the only inequation that normalized cheating situations must fulfill, is that they have non-negative image space. Thus, for all normalized $\eta,\eta' \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ and each $s \in \mathbb{R}$ the mapping $\tilde{\eta} := s\cdot\eta + (1-s)\cdot\eta'$ is a normalized cheating situation for F, if only $\mathrm{Image}(\tilde{\eta}) \subseteq \mathbb{R}_{\geq 0}$. □

Corollary 11 (Positive linearity of cheating characteristics)**.** *Let any $F \in \mathfrak{F}_{\mathsf{fin}}$ and $\xi,\xi' \in \mathfrak{X}_{\mathrm{B}}^{(F)}$, $\gamma,\gamma' \in \mathbb{R}_{>0}$ be given. Then it holds that $\gamma\cdot\xi + \gamma'\cdot\xi' \in \mathfrak{X}_{\mathrm{B}}^{(F)}$.*

Proof. This directly follows by Definition 7 and the combination of Corollary 9 and Lemma 10. □

4.3 Cheating situations for redundant input symbols

We expose now the inherent structure of cheating strategies by decomposing them into more easily understandable parts. This decomposition consists of two steps.

1. Every cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ is *equivalent* to a *direct* cheating situation $\tilde{\eta} \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, in the sense that $\eta|_{\mathrm{B}}^{\mathsf{true}}(y) = \tilde{\eta}|_{\mathrm{B}}^{\mathsf{true}}(y)$ and $\eta|_{\mathrm{B}}^{\mathsf{fake}}(y') = \tilde{\eta}|_{\mathrm{B}}^{\mathsf{fake}}(y')$ for all $y,y' \in \Upsilon_{\mathrm{B}}$, and for each $(y,b) \in \Upsilon_{\mathrm{B}}\times\Omega_{\mathrm{B}}$ at least one of the following two equalities holds true:
$$\tilde{\eta}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = \tilde{\eta}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y,b)\big)$$
$$\tilde{\eta}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(y,b)\big) = \tilde{\eta}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y,b)\big)$$

   The intuition behind calling a cheating situation "direct" is that Bob does not sometimes claim an actual input-output tuple (y,b) to be (y',b') and also sometimes claim an actual input-output tuple (y',b') to be (y'',b''), but instead always goes the direct way: He claims (y,b) to be (y'',b'') in the first place and is just honest about (y',b').

2. Every direct cheating situation $\tilde{\eta} \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ is a convex combination of a *trivial* and a *straight* cheating situation $\bar{\eta},\hat{\eta} \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, in the sense that $\bar{\eta}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y',b')\big) = 0$ for all distinct $(y,b),(y',b') \in \Upsilon_{\mathrm{B}}\times\Omega_{\mathrm{B}}$, and for each $y \in \Upsilon$ at least one of the following two equalities holds true:
$$\hat{\eta}|_{\mathrm{B}}^{\mathsf{true}}(y) = 0 \qquad \text{or} \qquad \hat{\eta}|_{\mathrm{B}}^{\mathsf{fake}}(y) = 0$$

   The intuition behind trivial cheating situations is that Bob is simply always honest, and the intuition behind straight cheating situations is that Bob always claims to have used some input symbol that he actually did never use at all.

This yields a more abstract redundancy criterion (Corollary 18), which plays a major role in proving existence of appropriate OT-cores for secure generation of correlated data. Moreover, this insight also helps proving that the redundancy-free version of any $F \in \mathfrak{F}_{\mathsf{fin}}$ is unique up to isomorphism (Corollary 19).

Notation 12 (Equivalent cheating situations). Let any $F \in \mathfrak{F}_{\mathsf{fin}}$ be given and $\eta, \eta' \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, such that $\eta|_{\mathrm{B}}^{\mathsf{true}} = \eta'|_{\mathrm{B}}^{\mathsf{true}}$ and $\eta|_{\mathrm{B}}^{\mathsf{fake}} = \eta'|_{\mathrm{B}}^{\mathsf{fake}}$. Then η and η' are called *equivalent*, what we denote by $\eta \sim \eta'$.

Remark 13. As a direct consequence of the conditions 2 and 3 of Definition 5, every cheating situation is equivalent to its normalized version (cf. Corollary 9).

Notation 14 (Containedness). Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ and let $\eta, \eta' \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, such that for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$, $b, b' \in \Omega_{\mathrm{B}}$ the following implication holds true:

$$\eta'\big((x,a),(y,b),(y',b')\big) > 0 \quad \Rightarrow \quad \eta\big((x,a),(y,b),(y',b')\big) > 0$$

Then we say that η *contains* η' and we denote that by $\eta \sqsupseteq \eta'$. Let $\eta \sqsupset \eta'$ denote that $\eta \sqsupseteq \eta' \not\sqsupseteq \eta$.

Lemma 15 (Generality of direct cheating situations)**.** *Let any $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ and $\tilde{\eta} \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ be given. Then there exists a direct cheating situation $\hat{\eta} \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, such that $\hat{\eta} \sim \tilde{\eta}$.*

Proof. First note that by Remark 13, w.l.o.g. η is normalized. Since otherwise we just can set $\hat{\eta} := \tilde{\eta}$, w.l.o.g. we find some $\tilde{y}, \tilde{y}' \in \Upsilon_{\mathrm{B}}$, $\tilde{b}, \tilde{b}' \in \Omega_{\mathrm{B}}$, such that $(\tilde{y}, \tilde{b}) \neq (\tilde{y}', \tilde{b}')$ and:

$$\begin{aligned} \tilde{\eta}\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (\tilde{y}, \tilde{b})\big) &> \tilde{\eta}\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\tilde{y}, \tilde{b}), (\tilde{y}, \tilde{b})\big) \\ \tilde{\eta}\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\tilde{y}, \tilde{b}), (\tilde{y}', \tilde{b}')\big) &> 0 \end{aligned}$$

We will now construct a normalized cheating situation $\tilde{\eta}' \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ with the following properties.

(**a**) It holds that $\tilde{\eta}' \sim \tilde{\eta}$.

(**b**) At least one of the following two equalities does hold true:

$$\begin{aligned} \tilde{\eta}'\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (\tilde{y}, \tilde{b})\big) &= \tilde{\eta}'\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\tilde{y}, \tilde{b}), (\tilde{y}, \tilde{b})\big) \\ \tilde{\eta}'\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\tilde{y}, \tilde{b}), (\tilde{y}', \tilde{b}')\big) &= 0 \end{aligned}$$

(**c**) For all $y' \in \Upsilon_{\mathrm{B}}$, $b' \in \Omega_{\mathrm{B}}$ with $(\tilde{y}, \tilde{b}) \neq (y', b')$ and $\tilde{\eta}\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\tilde{y}, \tilde{b}), (y', b')\big) = 0$ it still does hold that $\tilde{\eta}'\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\tilde{y}, \tilde{b}), (y', b')\big) = 0$.

(**d**) For all $y \in \Upsilon_{\mathrm{B}}$, $b \in \Omega_{\mathrm{B}}$ with $\tilde{\eta}\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (y, b)\big) = \tilde{\eta}\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, b), (y, b)\big)$ it still does hold that $\tilde{\eta}'\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (y, b)\big) = \tilde{\eta}'\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (y, b), (y, b)\big)$.

Our lemma then follows by induction. For our construction of $\tilde{\eta}'$ we first define the auxiliary values $\gamma, \gamma', \delta \in \mathbb{R}_{>0}$ as follows:

$$\begin{aligned} \gamma &:= \tilde{\eta}\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (\tilde{y}, \tilde{b})\big) - \tilde{\eta}\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\tilde{y}, \tilde{b}), (\tilde{y}, \tilde{b})\big) \\ \gamma' &:= \tilde{\eta}\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}), (\tilde{y}, \tilde{b}), (\tilde{y}', \tilde{b}')\big) \\ \delta &:= \min(\gamma, \gamma') \end{aligned}$$

Now we define the mapping $\Delta : \Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}} \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2 \to \mathbb{R}$ by:

$$\Delta\big((x,a),(y,b),(y',b')\big) := \begin{cases} -\frac{\delta \cdot \tilde{\eta}((x,a),(y,b),(\tilde{y},\tilde{b}))}{\gamma} & \text{if } (y,b) \neq (\tilde{y},\tilde{b}) \text{ and } (y',b') = (\tilde{y},\tilde{b}) \\ \frac{\delta \cdot \tilde{\eta}((x,a),(y,b),(\tilde{y},\tilde{b}))}{\gamma} & \text{if } (y,b) \neq (\tilde{y},\tilde{b}) \text{ and } (y',b') = (\tilde{y}',\tilde{b}') \\ -\frac{\delta \cdot \tilde{\eta}((x,a),(\tilde{y},\tilde{b}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}))}{\tilde{\eta}((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\tilde{y},\tilde{b}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}))} & \text{if } (y,b) = (\tilde{y},\tilde{b}) \text{ and } (y',b') = (\tilde{y}',\tilde{b}') \\ \frac{\delta \cdot \tilde{\eta}((x,a),(\tilde{y},\tilde{b}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}))}{\tilde{\eta}((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\tilde{y},\tilde{b}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}))} & \text{if } (y,b) = (\tilde{y},\tilde{b}) \text{ and } (y',b') = (\tilde{y},\tilde{b}) \\ 0 & \text{else} \end{cases}$$

Since $\tilde{\eta}$ is normalized, it is straightforward to verify that $\Delta\big((x,a),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(y',b')\big) = 0$ and $\Delta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = 0$ for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y,y' \in \Upsilon_{\mathrm{B}}$, $b,b' \in \Omega_{\mathrm{B}}$. Hence, the mapping $\tilde{\eta}' := \tilde{\eta} + \Delta$ fulfills the conditions 1–3 of Definition 5, and $\tilde{\eta}' \sim \tilde{\eta}$. Further, by Condition 4 of Definition 5 one can conclude quite easily that $\Delta\big((x,a),(y,b),(y',b')\big) \geq -\tilde{\eta}\big((x,a),(y,b),(y',b')\big)$ for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y,y' \in \Upsilon_{\mathrm{B}}$, $b,b' \in \Omega_{\mathrm{B}}$ and therefore $\tilde{\eta}'\big((x,a),(y,b),(y',b')\big) \geq 0$. Finally, by a simple case analysis one can show that for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y,y' \in \Upsilon_{\mathrm{B}}$, $b,b' \in \Omega_{\mathrm{B}}$ with $\tilde{\eta}\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) > 0$ it holds:

$$\frac{\Delta\big((x,a),(y,b),(y',b')\big)}{\tilde{\eta}\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big)} = \frac{\Delta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y',b')\big)}{\tilde{\eta}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big)}$$

Thereby, since $\Delta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = 0$, for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y,y' \in \Upsilon_{\mathrm{B}}$, $b,b' \in \Omega_{\mathrm{B}}$ with $\tilde{\eta}'\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) > 0$ follows:

$$\frac{\tilde{\eta}'\big((x,a),(y,b),(y',b')\big)}{\tilde{\eta}'\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big)} = \frac{\tilde{\eta}'\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y',b')\big)}{\tilde{\eta}'\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big)}$$

Thus, $\tilde{\eta}'$ is a normalized cheating situation for F with $\tilde{\eta}' \sim \tilde{\eta}$. Yet, there are just the properties (**b**), (**c**) and (**d**) left to prove.

*Proof for (**b**):* The property (**b**) follows by our choice of δ. In the case that $\delta = \gamma$, we have that $\Delta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(\tilde{y},\tilde{b})\big) = -\tilde{\eta}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(\tilde{y},\tilde{b})\big)$ for all $(y,b) \in (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}}) \setminus \big\{(\tilde{y},\tilde{b})\big\}$, whereby follows that $\tilde{\eta}'\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(\tilde{y},\tilde{b})\big) = \tilde{\eta}'\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\tilde{y},\tilde{b}),(\tilde{y},\tilde{b})\big)$. In the case that $\delta = \gamma'$, we have that $\Delta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\tilde{y},\tilde{b}),(\tilde{y}',\tilde{b}')\big) = -\tilde{\eta}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\tilde{y},\tilde{b}),(\tilde{y}',\tilde{b}')\big)$, whereby follows that $\tilde{\eta}'\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\tilde{y},\tilde{b}),(\tilde{y}',\tilde{b}')\big) = 0$.

*Proof for (**c**):* By construction of Δ, for all $x \in \Upsilon_{\mathrm{B}}$, $a \in \Omega_{\mathrm{B}}$, $y' \in \Upsilon_{\mathrm{B}}$, $b' \in \Omega_{\mathrm{B}}$ with $(y',b') \neq (\tilde{y},\tilde{b})$ it holds that $\Delta\big((x,a),(\tilde{y},\tilde{b}),(y',b')\big) \leq 0$, what yields:

$$\tilde{\eta}'\big((x,a),(\tilde{y},\tilde{b}),(y',b')\big) \leq \tilde{\eta}\big((x,a),(\tilde{y},\tilde{b}),(y',b')\big)$$

*Proof for (**d**):* Let us assume that we could find some $y \in \Upsilon_{\mathrm{B}}$, $b \in \Omega_{\mathrm{B}}$ with:

$$\begin{aligned}\tilde{\eta}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) &= \tilde{\eta}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y,b)\big)\\ \tilde{\eta}'\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) &> \tilde{\eta}'\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y,b)\big)\end{aligned}$$

This would directly yield that $\Delta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) > \Delta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y,b)\big)$, but by construction of Δ for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$, $b \in \Omega_{\mathrm{B}}$ it holds:

$$\begin{aligned}\Delta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) &= 0\\ \Delta\big((x,a),(y,b),(y,b)\big) &\geq 0\end{aligned}$$

□

Lemma 16 (Decomposition of direct cheating situations)**.** *Let $F := (\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},\Omega_{\mathrm{A}},\Omega_{\mathrm{B}},\phi) \in \mathfrak{F}_{\mathsf{fin}}$ and let $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ be direct. Then η is straight or it contains a trivial cheating situation for F.*

Proof. W.l.o.g. we assume that η is not straight, i.e. we find some $\tilde{y} \in \Upsilon_{\mathrm{B}}$, such that $\eta|^{\mathsf{true}}(\tilde{y}) > 0$ and $\eta|^{\mathsf{fake}}(\tilde{y}) > 0$. We now construct a trivial cheating situation $\tilde{\eta}$, such that $\tilde{\eta} \sqsubseteq \eta$. We define the following mapping:

$$\tilde{\eta} : (\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2 \to \mathbb{R}_{\geq 0},\ \big((x,a),(y,b),(y',b')\big) \mapsto \begin{cases} \frac{\phi_{x,\tilde{y}}(a,b)}{|\Upsilon_{\mathrm{A}}|} & \text{if } y = y' = \tilde{y} \text{ and } b = b' \\ 0 & \text{else} \end{cases}$$

It is pretty obvious that $\tilde{\eta}$ is a trivial cheating situation for F. So there is just left to show that $\tilde{\eta} \sqsubseteq \eta$. So, let some arbitrary $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$, $b, b' \in \Omega_{\mathrm{B}}$ be given with:

$$\tilde{\eta}\big((x,a),(y,b),(y',b')\big) > 0$$

By construction of $\tilde{\eta}$ this means that $y = y' = \tilde{y}$ and $b = b'$ and $\phi_{x,\tilde{y}}(a,b) > 0$. By our choice of $\tilde{y}$ and the conditions 2 and 3 of Definition 5 follows:

$$\eta\big((x,a),(\tilde{y},b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) > 0$$
$$\eta\big((x,a),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(\tilde{y},b)\big) > 0$$

Since η is direct by assumption, this implies that $\eta\big((x,a),(\tilde{y},b),(\tilde{y},b)\big) > 0$. Since $y = y' = \tilde{y}$ and $b = b'$, this means that $\eta\big((x,a),(y,b),(y',b')\big) > 0$. This is what we had to show. □

Corollary 17 (General decomposition of cheating situations)**.** *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ and let $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$. Then η is equivalent to a trivial cheating situation for F or there exists a convex combination $\eta' := t \cdot \bar{\eta} + (1-t) \cdot \hat{\eta}$ of a trivial cheating situation $\bar{\eta} \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ and a straight cheating situation $\hat{\eta} \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, such that $\eta \sim \eta'$.*

Proof. W.l.o.g. we assume that η is a direct cheating situation (cf. Lemma 15). Further, w.l.o.g. we assume that η is neither trivial nor straight. We will now construct some cheating situations $\bar{\eta}', \hat{\eta}' \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ meeting the following four conditions:

$\bar{\eta}' \sqsubseteq \eta$ $\qquad$ $\hat{\eta}' \sqsubset \eta$ $\qquad$ $\bar{\eta}'$ is trivial $\qquad$ η is a convex combination of $\bar{\eta}'$ and $\hat{\eta}'$

Since every convex combination of trivial cheating situations for F itself is a trivial cheating situation, our lemma then follows by induction.

By Lemma 16, we find some trivial cheating situation $\bar{\eta}' \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, such that $\bar{\eta}' \sqsubseteq \eta$. Now, let $t := \max\big\{s \in \mathbb{R} \mid \mathrm{Image}(\eta - s \cdot \bar{\eta}') \subseteq \mathbb{R}_{\geq 0}\big\}$. Note that $0 < t < 1$ by our choice of η and $\bar{\eta}'$. We set $\hat{\eta}' := (1-t)^{-1} \cdot (\eta - t \cdot \bar{\eta}')$. By Lemma 10, it follows that $\hat{\eta}' \in \mathfrak{N}_{\mathrm{B}}^{(F)}$. Moreover, by our choice of t we have that $\hat{\eta}' \sqsubset \eta$. □

Corollary 18 (Characteristic-based redundancy criterion)**.** *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ and let $y' \in \Upsilon_{\mathrm{B}}$, $\xi \in \mathfrak{X}_{\mathrm{B}}^{(F)}$, such that $\xi(y) \leq 0$ for all $y \in \Upsilon_{\mathrm{B}} \setminus \{y'\}$ and $\xi(y') > 0$. Then y' is redundant.*

Proof. By Definition 7 we find some normalized cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, such that for all $y \in \Upsilon_{\mathrm{B}}$ it holds:

$$\eta|_{\mathrm{B}}^{\mathsf{fake}}(y) > \eta|_{\mathrm{B}}^{\mathsf{true}}(y) \ \text{ if } y = y'$$
$$\eta|_{\mathrm{B}}^{\mathsf{fake}}(y) \leq \eta|_{\mathrm{B}}^{\mathsf{true}}(y) \ \text{ else}$$

By Corollary 17 we can choose η to be straight (we just discard the trivial part), whereby it follows:

$$\eta|_{\mathrm{B}}^{\mathsf{fake}}(y') = 1 \qquad \text{and} \qquad \eta|_{\mathrm{B}}^{\mathsf{true}}(y') = 0$$

Now, let $\iota := \eta|_{\mathrm{B}}^{\mathsf{true}}$. We also find some family of probability mass functions $\lambda := (\lambda_{y,b})_{y \in \Upsilon_{\mathrm{B}}, b \in \Omega_{\mathrm{B}}} \subseteq \mathrm{pmf}(\Omega_{\mathrm{B}})$, such that for all $y \in \Upsilon_{\mathrm{B}}$, $b, b' \in \Omega_{\mathrm{B}}$ with $\eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) > 0$ we have:

$$\lambda_{y,b}(b') = \frac{\eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}),(y,b),(y',b')\big)}{\eta\big((\Upsilon_{\mathrm{A}}, \Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big)}$$

Exploiting the conditions 2, 4 and 3 of Definition 5, we get for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $b' \in \Omega_{\mathrm{B}}$:

$$\sum\nolimits_{y\in\Upsilon_{\mathrm{B}},\, b\in\Omega_{\mathrm{B}}} \iota(y)\cdot\phi_{x,y}(a,b)\cdot\lambda_{y,b}(b') \;=\; \sum\nolimits_{y\in\Upsilon_{\mathrm{B}},\, b\in\Omega_{\mathrm{B}}} \frac{\eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big)\cdot\lambda_{y,b}(b')}{\eta|_{\mathrm{A}}(x)}$$
$$=\; \sum\nolimits_{y\in\Upsilon_{\mathrm{B}},\, b\in\Omega_{\mathrm{B}}} \frac{\eta\big((x,a),(y,b),(y',b')\big)}{\eta|_{\mathrm{A}}(x)} \;=\; \eta|_{\mathrm{B}}^{\mathsf{fake}}(y')\cdot\phi_{x,y'}(a,b') \;=\; \phi_{x,y'}(a,b') \qquad \square$$

Corollary 19 (Uniqueness of redundancy-free versions)**.** *Let any $F := (\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},\Omega_{\mathrm{A}},\Omega_{\mathrm{B}},\phi) \in \mathfrak{F}_{\mathsf{fin}}$ be given. Then the redundancy-free version of F is unique up to isomorphism.*

Proof. We have to show: For any two redundant input symbols $\tilde{y}',\tilde{y}'' \in \Upsilon_{\mathrm{B}}$, such that after removing one of them the other is not redundant any more, the respective block columns in the condensed canonical representation are equal up to internal permutation of columns. This implies that it does not matter in which order redundant input symbols are removed from Υ_{B} (or Υ_{A} respectively).

So, let any such $\tilde{y}',\tilde{y}'' \in \Upsilon_{\mathrm{B}}$ be given. Since $\tilde{y}'$ is redundant, we find some $\iota \in \mathrm{pmf}(\Upsilon_{\mathrm{B}})$ and $\{\lambda_{y,b}\}_{y\in\Upsilon_{\mathrm{B}},b\in\Omega_{\mathrm{B}}} \subseteq \mathrm{pmf}(\Omega_{\mathrm{B}})$, such that $\iota(\tilde{y}') = 0$ and for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $b' \in \Omega_{\mathrm{B}}$ it holds:

$$\phi_{x,\tilde{y}'}(a,b') = \sum\nolimits_{y\in\Upsilon_{\mathrm{B}},\, b\in\Omega_{\mathrm{B}}} \iota(y)\cdot\phi_{x,y}(a,b)\cdot\lambda_{y,b}(b')$$

Thus, we can construct a (normalized) cheating situation as follows:

$$\eta'\big((x,a),(y,b),(y',b')\big) := \begin{cases} \frac{1}{|\Upsilon_{\mathrm{A}}|}\cdot\iota(y)\cdot\phi_{x,y}(a,b)\cdot\lambda_{y,b}(b') & \text{if } y\neq\tilde{y}' \text{ and } y'=\tilde{y}' \\ 0 & \text{else} \end{cases}$$

Note that by construction η' is straight and $\eta'|_{\mathrm{B}}^{\mathsf{fake}}(\tilde{y}') = 1$. Further note that $\eta'|_{\mathrm{B}}^{\mathsf{true}}(\tilde{y}'') > 0$ by our choice of $\tilde{y}',\tilde{y}''$. Analogously, we find some straight cheating situation $\eta'' \in \mathfrak{B}_{\mathrm{B}}^{(F)}$, such that $\eta''|_{\mathrm{B}}^{\mathsf{fake}}(\tilde{y}'') = 1$ and $\eta''|_{\mathrm{B}}^{\mathsf{true}}(\tilde{y}') > 0$. Let $t := \eta''|_{\mathrm{B}}^{\mathsf{true}}(\tilde{y}')$. Now, by Lemma 10, we can construct a new cheating strategy η as follows:

$$\eta := \tfrac{1}{1+t}\cdot\eta'' + \tfrac{t}{1+t}\cdot\eta'$$

By construction we have that $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\{\tilde{y}',\tilde{y}''\}) = 1$ and $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\tilde{y}') = \eta|_{\mathrm{B}}^{\mathsf{true}}(\tilde{y}') = \frac{t}{1+t}$. By Corollary 17 we can conclude that η is either equivalent to a trivial cheating situation, or there exists a straight cheating situation $\hat{\eta} \in \mathfrak{B}_{\mathrm{B}}^{(F)}$ such that $\hat{\eta}|_{\mathrm{B}}^{\mathsf{fake}}(\tilde{y}'') = 1$ and $\hat{\eta}|_{\mathrm{B}}^{\mathsf{fake}}(\tilde{y}') = \hat{\eta}|_{\mathrm{B}}^{\mathsf{true}}(\tilde{y}') = 0$. Since the latter is ruled out by our choice of $\tilde{y}',\tilde{y}''$, we have that $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\tilde{y}'') = \eta|_{\mathrm{B}}^{\mathsf{true}}(\tilde{y}'') = \frac{1}{1+t}$, whereby it follows:

$$\eta'|_{\mathrm{B}}^{\mathsf{fake}}(\tilde{y}') = \eta'|_{\mathrm{B}}^{\mathsf{true}}(\tilde{y}'') = 1 \qquad \text{and} \qquad \eta''|_{\mathrm{B}}^{\mathsf{fake}}(\tilde{y}'') = \eta''|_{\mathrm{B}}^{\mathsf{true}}(\tilde{y}') = 1$$

Intuitively speaking, a corrupted Bob can replace the input symbols $\tilde{y}'$ and $\tilde{y}''$ just by each other. It is straightforward now to verify that in the condensed canonical representation of F the block columns belonging to $\tilde{y}'$ and $\tilde{y}''$ are equal up to internal permutation of columns. □

4.4 Existence of robust OT-cores

In this section we show for every redundancy-free 2-party function $F \in \mathfrak{F}_{\mathsf{fin}}$ that it has some OT-core useful for us, if it has any OT-core at all. This is the core argumentation of the algebraic part of our security proof.

Definition 20 (OT-cores)**.** Let $F := (\Upsilon_{\mathrm{A}},\Upsilon_{\mathrm{B}},\Omega_{\mathrm{A}},\Omega_{\mathrm{B}},\phi) \in \mathfrak{F}_{\mathsf{fin}}$ and some $(x,a),(x',a') \in \Upsilon_{\mathrm{A}}\times\Omega_{\mathrm{A}}$, $(y,b),(y',b') \in \Upsilon_{\mathrm{B}}\times\Omega_{\mathrm{B}}$ be given. We call $\big\{(x,a),(x',a')\big\}\times\big\{(y,b),(y',b')\big\}$ an *OT-core* of F, if $\phi_{x,y}(a,b)\cdot\phi_{x',y'}(a',b') \neq \phi_{x',y}(a',b)\cdot\phi_{x,y}(a,b')$ and at most one of the factors is zero.

Notation 21 (Hideable inputs). Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$. For $Y \subseteq \Upsilon_{\mathrm{B}}$ we define:

$$\Psi_F(Y) \ := \ \big\{ y \in \Upsilon_{\mathrm{B}} \ \big| \ \exists\, \eta \in \mathfrak{N}_{\mathrm{B}}^{(F)} : \ \eta|_{\mathrm{B}}^{\mathsf{true}}(y) > 0 \ \wedge \ \eta|_{\mathrm{B}}^{\mathsf{fake}}(Y) = 1 \big\}$$

Given any $y, y' \in \Upsilon_{\mathrm{B}}$, we write $\Psi_F(y, y')$ instead of $\Psi_F(\{y, y'\})$ for convenience.

Remark 22. Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$. Then for all $Y \subseteq \Upsilon_{\mathrm{B}}$ it holds:

$$\Psi_F(Y) = Y \cup \big\{ y \in \Upsilon_{\mathrm{B}} \ \big| \ \exists\, \xi \in \mathfrak{X}_{\mathrm{B}}^{(F)} : \ \xi(y) < 0 \ \wedge \ \forall y' \in \Upsilon_{\mathrm{B}} \backslash Y : \xi(y') \leq 0 \big\}$$

Lemma 23 (Monotonicity of Ψ_F)**.** *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ and let $Y' \subseteq \Upsilon_{\mathrm{B}}$. Then for all $Y \subseteq \Psi_F(Y')$ we have that $\Psi_F(Y) \subseteq \Psi_F(Y')$.*

Proof. Let $Y \subseteq \Psi_F(Y')$. By Remark 22 and Corollary 11 we find some cheating characteristics $\xi', \xi'' \in \mathfrak{X}_{\mathrm{B}}^{(F)}$, such that for all $y \in \Upsilon_{\mathrm{B}}$ it holds:

$$\begin{aligned} &\xi'(y) < 0 \ \text{ if } y \in \Psi_F(Y) \backslash Y && \xi''(y) < 0 \ \text{ if } y \in \Psi_F(Y') \backslash Y' \\ &\xi'(y) \leq 0 \ \text{ if } y \in \Upsilon_{\mathrm{B}} \backslash \Psi_F(Y) && \xi''(y) \leq 0 \ \text{ if } y \in \Upsilon_{\mathrm{B}} \backslash \Psi_F(Y') \end{aligned}$$

Now we find some $\gamma \in \mathbb{R}_{>0}$, such that $\gamma \cdot \xi''(y) < -\xi'(y)$ for all $y \in \Psi_F(Y') \backslash Y'$. Since $Y \subseteq \Psi_F(Y')$ by assumption, we especially have that $\gamma \cdot \xi''(y) + \xi'(y) < 0$ for all $y \in Y \backslash Y'$. Let $\xi := \xi' + \gamma \cdot \xi''$ (cf. Corollary 11). Thereby, for all $y \in \Upsilon_{\mathrm{B}}$ we can conclude:

$$\begin{aligned} &\xi(y) < 0 \ \text{ if } y \in \Psi_F(Y) \backslash Y' \\ &\xi(y) \leq 0 \ \text{ if } y \notin Y' \end{aligned}$$

Hence, by Remark 22 it must hold that $\Psi_F(Y) \subseteq \Psi_F(Y')$. □

Lemma 24. *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$, such that Υ_{B} does not contain any redundant input symbols. Further let $\tilde{y}, \tilde{y}' \in \Upsilon_{\mathrm{B}}$ and $\tilde{Y}, \tilde{Y}' \subseteq \Psi_F(\tilde{y}, \tilde{y}')$, such that $\Psi_F(\tilde{y}, \tilde{y}') \supsetneq \{\tilde{y}, \tilde{y}'\}$ and for all $\hat{y} \in \tilde{Y}$, $\hat{y}' \in \tilde{Y}'$ it holds that $\Psi_F(\hat{y}, \hat{y}') = \Psi_F(\tilde{y}, \tilde{y}')$. Then for all $\hat{y} \in \tilde{Y}$, $\hat{y}' \in \tilde{Y}'$, $Y \subseteq \tilde{Y} \cup \tilde{Y}'$ with $\hat{y}, \hat{y}' \notin Y$ there exists some $\xi \in \mathfrak{X}_{\mathrm{B}}^{(F)}$, such that for all $y \in \Upsilon_{\mathrm{B}}$ it holds:*

$$\begin{aligned} &\xi(y) > 0 \ \text{ if } y \in \{\hat{y}, \hat{y}'\} \\ &\xi(y) = 0 \ \text{ if } y \in Y \text{ or } y \notin \Psi_F(\tilde{y}, \tilde{y}') \\ &\xi(y) < 0 \ \text{ else} \end{aligned}$$

Proof. Our proof is by induction on $|Y|$. So in the first instance we assume that $Y = \emptyset$. Let $\hat{y} \in \tilde{Y}$ and $\hat{y}' \in \tilde{Y}'$ be arbitrary. Since $\Psi_F(\hat{y}, \hat{y}') = \Psi_F(\tilde{y}, \tilde{y}')$ by assumption, we find some $\xi \in \mathfrak{X}_{\mathrm{B}}^{(F)}$ by Remark 22 and Corollary 11, such that for all $y \in \Upsilon_{\mathrm{B}}$ it holds:

$$\begin{aligned} &\xi(y) = 0 \ \text{ if } y \notin \Psi_F(\tilde{y}, \tilde{y}') \\ &\xi(y) < 0 \ \text{ if } y \in \Psi_F(\tilde{y}, \tilde{y}') \backslash \{\hat{y}, \hat{y}'\} \end{aligned}$$

Moreover, since $\Psi_F(\tilde{y}, \tilde{y}') \backslash \{\hat{y}, \hat{y}'\} \neq \emptyset$ by assumption and $\xi(\Upsilon_{\mathrm{B}}) = 0$ by definition, it must hold that $\xi(\hat{y}) > 0$; else $\hat{y}'$ would be redundant by Corollary 18. Analogously it follows that $\xi(\hat{y}') > 0$. Thereby we have proven our lemma for the case that $|Y| = 0$.

Now, let $Y \subseteq \tilde{Y} \cup \tilde{Y}'$ with $Y \neq \emptyset$ and let $\hat{y} \in \tilde{Y}$, $\hat{y}' \in \tilde{Y}'$, such that $\hat{y}, \hat{y}' \notin Y$. Furthermore, let $y' \in Y$. There are two cases to be considered: $y' \in \tilde{Y}$ and $y' \in \tilde{Y}'$. Since both cases can be handled analogously, we just consider the latter. By induction hypothesis we find some $\xi', \xi'' \in \mathfrak{X}_{\mathrm{B}}^{(F)}$, such that for all $y \in \Upsilon_{\mathrm{B}}$ it holds:

$$\begin{array}{ll} \xi'(y) > 0 \text{ if } y \in \{\hat{y}, y'\} & \xi''(y) > 0 \text{ if } y \in \{\hat{y}, \hat{y}'\} \\ \xi'(y) = 0 \text{ if } y \in Y \backslash \{y'\} \text{ or } y \notin \Psi_F(\tilde{y}, \tilde{y}') & \xi''(y) = 0 \text{ if } y \in Y \backslash \{y'\} \text{ or } y \notin \Psi_F(\tilde{y}, \tilde{y}') \\ \xi'(y) < 0 \text{ else} & \xi''(y) < 0 \text{ else} \end{array}$$

We set $\xi := \xi'(y') \cdot \xi'' - \xi''(y') \cdot \xi'$; note that $\xi \in \mathfrak{X}_{\mathrm{B}}^{(F)}$ by Corollary 11, since $\xi'(y') > 0$ and $\xi''(y') < 0$. By construction, for all $y \in \Upsilon_{\mathrm{B}}$ it follows:

$$\begin{aligned} &\xi(y) > 0 \text{ if } y = \hat{y} \\ &\xi(y) = 0 \text{ if } y \in Y \text{ or } y \notin \Psi_F(\tilde{y}, \tilde{y}') \\ &\xi(y) < 0 \text{ if } y \in \Psi_F(\tilde{y}, \tilde{y}') \text{ and } y \notin Y \cup \{\hat{y}, \hat{y}'\} \end{aligned}$$

Finally, we still must have that $\xi(\hat{y}') > 0$, since otherwise $\hat{y}$ would be redundant by Corollary 18. □

Lemma 25. *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$, such that Υ_{B} does not contain any redundant input symbols. Further let $\{(\tilde{x}, \tilde{a}), (\tilde{x}', \tilde{a}')\} \times \{(\tilde{y}, \tilde{b}), (\tilde{y}', \tilde{b}')\} \subseteq (\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}})^2 \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2$ be an OT-core of F. Then there exist some $(\bar{y}, \bar{b}), (\bar{y}', \bar{b}') \in \Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}}$, such that $\{(\tilde{x}, \tilde{a}), (\tilde{x}', \tilde{a}')\} \times \{(\bar{y}, \bar{b}), (\bar{y}', \bar{b}')\}$ also is an OT-core of F and $\Psi_F(\bar{y}, \bar{y}') = \{\bar{y}, \bar{y}'\}$.*

Proof. W.l.o.g., $\phi_{\tilde{x},\tilde{y}}(\tilde{a}, \tilde{b}) > 0$ and $\phi_{\tilde{x}',\tilde{y}}(\tilde{a}', \tilde{b}) > 0$, i.e. we can write $\frac{\phi_{\tilde{x},\tilde{y}'}(\tilde{a},\tilde{b}')}{\phi_{\tilde{x},\tilde{y}}(\tilde{a},\tilde{b})} \neq \frac{\phi_{\tilde{x}',\tilde{y}'}(\tilde{a}',\tilde{b}')}{\phi_{\tilde{x}',\tilde{y}}(\tilde{a}',\tilde{b})}$; else we interchange $(\tilde{y}, \tilde{b})$ and $(\tilde{y}', \tilde{b}')$. We define the following input sets:

$$\begin{aligned} \hat{Y}' &:= \big\{ y' \in \Upsilon_{\mathrm{B}} \;\big|\; \text{for some } b' \in \Omega_{\mathrm{B}},\ \{(\tilde{x}, \tilde{a}), (\tilde{x}', \tilde{a}')\} \times \{(\tilde{y}, \tilde{b}), (y', b')\} \text{ is an OT-core of } F \big\} \\ \hat{Y} &:= \big\{ y \in \Upsilon_{\mathrm{B}} \backslash \hat{Y}' \;\big|\; \text{for some } b \in \Omega_{\mathrm{B}},\ \{(\tilde{x}, \tilde{a}), (\tilde{x}', \tilde{a}')\} \times \{(y, b), (\tilde{y}', \tilde{b}')\} \text{ is an OT-core of } F \big\} \\ \hat{Y}_0 &:= \big\{ y_0 \in \Upsilon_{\mathrm{B}} \;\big|\; \phi_{\tilde{x},y_0}(\tilde{a}, \Omega_{\mathrm{B}}) = \phi_{\tilde{x}',y_0}(\tilde{a}', \Omega_{\mathrm{B}}) = 0 \big\} \end{aligned}$$

Further we set $\tilde{Y} := \hat{Y} \cap \Psi_F(\tilde{y}, \tilde{y}')$ and $\tilde{Y}' := \hat{Y}' \cap \Psi_F(\tilde{y}, \tilde{y}')$ and $\tilde{Y}_0 := \hat{Y}_0 \cap \Psi_F(\tilde{y}, \tilde{y}')$. Note that $\hat{Y} \cup \hat{Y}' \cup \hat{Y}_0 = \Upsilon_{\mathrm{B}}$ and thereby $\tilde{Y} \cup \tilde{Y}' \cup \tilde{Y}_0 = \Psi_F(\tilde{y}, \tilde{y}')$. Further note that $\tilde{y} \in \tilde{Y}$ and $\tilde{y}' \in \tilde{Y}'$.

We prove our lemma by contradiction. So, we assume that our initially given OT-core is a minimal counterexample in the sense that $\Psi_F(\tilde{y}, \tilde{y}') \supsetneq \{\tilde{y}, \tilde{y}'\}$ and for all $y \in \tilde{Y}$, $y' \in \tilde{Y}'$ it holds that $\Psi_F(y, y') = \Psi_F(\tilde{y}, \tilde{y}')$ (cf. Lemma 23). Now, by Lemma 24 instantiated with $Y := (\tilde{Y} \cup \tilde{Y}') \backslash \{\tilde{y}, \tilde{y}'\}$, we find some $\xi \in \mathfrak{X}_{\mathrm{B}}^{(F)}$, such that for all $y \in \Upsilon_{\mathrm{B}}$ it holds:

$$\begin{aligned} &\xi(y) > 0 \text{ if } y \in \{\tilde{y}, \tilde{y}'\} \\ &\xi(y) = 0 \text{ if } y \in Y \text{ or } y \notin \Psi_F(\tilde{y}, \tilde{y}') \\ &\xi(y) < 0 \text{ else} \end{aligned}$$

In other words, since $\Psi_F(\tilde{y}, \tilde{y}') = \tilde{Y} \cup \tilde{Y}' \cup \tilde{Y}_0$ and $\tilde{Y}_0 \cap \tilde{Y} = \tilde{Y}_0 \cap \tilde{Y}' = \emptyset$, for all $y \in \Upsilon_{\mathrm{B}}$ it holds:

$$\begin{aligned} &\xi(y) > 0 \text{ if } y \in \{\tilde{y}, \tilde{y}'\} \\ &\xi(y) < 0 \text{ if } y \in \tilde{Y}_0 \\ &\xi(y) = 0 \text{ else} \end{aligned}$$

Thereby we find a cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$, such that for all $y \in \Upsilon_{\mathrm{B}}$ it holds:

$$\begin{aligned} \eta|_{\mathrm{B}}^{\mathsf{fake}}(y) > \eta|_{\mathrm{B}}^{\mathsf{true}}(y) &\text{ if } y \in \{\tilde{y}, \tilde{y}'\} \\ \eta|_{\mathrm{B}}^{\mathsf{fake}}(y) < \eta|_{\mathrm{B}}^{\mathsf{true}}(y) &\text{ if } y \in \tilde{Y}_0 \\ \eta|_{\mathrm{B}}^{\mathsf{fake}}(y) = \eta|_{\mathrm{B}}^{\mathsf{true}}(y) &\text{ else} \end{aligned}$$

By Corollary 17 we can decompose η into a trivial and a straight part. Let $\hat{\eta}$ denote the straight part. By construction it holds:

$$\begin{aligned} \hat{\eta}|_{\mathrm{B}}^{\mathsf{true}}(\tilde{Y}_0) &= 1 \\ \hat{\eta}|_{\mathrm{B}}^{\mathsf{fake}}(\tilde{y}) &> 0 \end{aligned}$$

However, by our choice of $\hat{Y}_0$ we have:

$$0 \;=\; \hat{\eta}|_{\mathrm{A}}(\tilde{x}) \cdot \sum\nolimits_{y \in \hat{Y}_0} \hat{\eta}|_{\mathrm{B}}^{\mathsf{true}}(y) \cdot \phi_{\tilde{x},y}(\tilde{a}, \Omega_{\mathrm{B}}) \;\geq\; \hat{\eta}|_{\mathrm{A}}(\tilde{x}) \cdot \sum\nolimits_{y \in \tilde{Y}_0} \hat{\eta}|_{\mathrm{B}}^{\mathsf{true}}(y) \cdot \phi_{\tilde{x},y}(\tilde{a}, \Omega_{\mathrm{B}})$$

Hence, by Condition 2 of Definition 5 we can conclude that $0 \geq \eta\big((\tilde{x}, \tilde{a}), (\tilde{Y}_0, \Omega_{\mathrm{B}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big)$. Because $\hat{\eta}|_{\mathrm{B}}^{\mathsf{true}}(\tilde{Y}_0) = 1$ and thus $\hat{\eta}\big((\tilde{x}, \tilde{a}), (\Upsilon_{\mathrm{B}} \backslash \tilde{Y}_0, \Omega_{\mathrm{B}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) = 0$, we also have:

$$\hat{\eta}\big((\tilde{x}, \tilde{a}), (\tilde{Y}_0, \Omega_{\mathrm{B}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) \;=\; \hat{\eta}\big((\tilde{x}, \tilde{a}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}})\big) \;\geq\; \hat{\eta}\big((\tilde{x}, \tilde{a}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (\tilde{y}, \tilde{b})\big)$$

Now, since $\phi_{\tilde{x},\tilde{y}}(\tilde{a}, \tilde{b}) > 0$ by assumption and we found $\hat{\eta}|_{\mathrm{B}}^{\mathsf{fake}}(\tilde{y}) > 0$, we can finally estimate by the conditions 1 and 2 of Definition 5:

$$\hat{\eta}\big((\tilde{x}, \tilde{a}), (\Upsilon_{\mathrm{B}}, \Omega_{\mathrm{B}}), (\tilde{y}, \tilde{b})\big) = \hat{\eta}|_{\mathrm{A}}(\tilde{x}) \cdot \hat{\eta}|_{\mathrm{B}}^{\mathsf{fake}}(\tilde{y}) \cdot \phi_{\tilde{x},\tilde{y}}(\tilde{a}, \tilde{b}) > 0$$

Putting things together, we get the contradiction that $0 > 0$, what concludes our proof. □

Corollary 26 (Existence of robust OT-cores)**.** *Let $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$, such that Υ_{B} does not contain any redundant input symbols. Further let $\{(\tilde{x}, \tilde{a}), (\tilde{x}', \tilde{a}')\} \times \{(\tilde{y}, \tilde{b}), (\tilde{y}', \tilde{b}')\} \subseteq (\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}})^2 \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2$ be an OT-core of F. Then there exist some $(\bar{y}, \bar{b}), (\bar{y}', \bar{b}') \in \Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}}$, such that $\{(\tilde{x}, \tilde{a}), (\tilde{x}', \tilde{a}')\} \times \{(\bar{y}, \bar{b}), (\bar{y}', \bar{b}')\}$ also is an OT-core of F and for every cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ with $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\{\bar{y}, \bar{y}'\}) = 1$ and all $y \in \Upsilon_{\mathrm{B}}$ it holds:*

$$\eta|_{\mathrm{B}}^{\mathsf{fake}}(y) \;=\; \eta|_{\mathrm{B}}^{\mathsf{true}}(y)$$

Proof. By Lemma 25 we find some $(\bar{y}, \bar{b}), (\bar{y}', \bar{b}') \in \Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}}$, such that $\{(\tilde{x}, \tilde{a}), (\tilde{x}', \tilde{a}')\} \times \{(\bar{y}, \bar{b}), (\bar{y}', \bar{b}')\}$ also is an OT-core of F and $\Psi_F(\bar{y}, \bar{y}') = \{\bar{y}, \bar{y}'\}$. Now, let any $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ with $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\{\bar{y}, \bar{y}'\}) = 1$ be given. We just have to show:

$$\begin{aligned} \eta|_{\mathrm{B}}^{\mathsf{fake}}(\bar{y}) &= \eta|_{\mathrm{B}}^{\mathsf{true}}(\bar{y}) \\ \eta|_{\mathrm{B}}^{\mathsf{fake}}(\bar{y}') &= \eta|_{\mathrm{B}}^{\mathsf{true}}(\bar{y}') \end{aligned}$$

We pick the following cheating characteristic (q.v. Definition 7):

$$\xi : \Upsilon_{\mathrm{B}} \to \mathbb{R},\; y \mapsto \eta|_{\mathrm{B}}^{\mathsf{fake}}(y) - \eta|_{\mathrm{B}}^{\mathsf{true}}(y)$$

Since $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\{\bar{y}, \bar{y}'\}) = 1$ and thus $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\Upsilon_{\mathrm{B}} \backslash \{\bar{y}, \bar{y}'\}) = 0$, for all $y \in \Upsilon_{\mathrm{B}} \backslash \{\bar{y}, \bar{y}'\}$ it must hold that $\xi(y) \leq 0$. Moreover, since $\Psi_F(\bar{y}, \bar{y}') = \{\bar{y}, \bar{y}'\}$, for all $y \in \Upsilon_{\mathrm{B}} \backslash \{\bar{y}, \bar{y}'\}$ we actually have that $\xi(y) = 0$ by Remark 22. Since $\xi(\Upsilon_{\mathrm{B}}) = 0$, it follows that $\xi(\bar{y}) = -\xi(\bar{y}')$. Now, if $\xi(\bar{y}) \neq 0$, this would render either $\bar{y}$ or $\bar{y}'$ redundant by Corollary 18. Thus, it must hold that $\xi(\bar{y}) = \xi(\bar{y}') = 0$. □

Protocol $\pi_F(X, Y, \alpha, \beta, \gamma)$

Parametrized by a 2-party function $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ and $(X, Y, \alpha, \beta, \gamma) \in \Pi_F$. Let k denote the security parameter and let $K := \{1, \dots, k\}$. The protocol proceeds as follows.

0. **Initialization:** Alice initializes two empty strings $s_{\mathrm{A}}^{\mathsf{in}}, s_{\mathrm{A}}^{\mathsf{out}}$ and an index set $K_{\mathrm{A}} \leftarrow K$. Bob analogously initializes $s_{\mathrm{B}}^{\mathsf{in}}, s_{\mathrm{B}}^{\mathsf{out}}, K_{\mathrm{B}}$. Let the probability mass functions $\tilde{n}_{\mathrm{A}}, \tilde{n}_{\mathrm{B}}$ be defined by:

$$\tilde{n}_{\mathrm{A}} : \Upsilon_{\mathrm{A}} \to \mathbb{R}_{>0},\, x \mapsto \begin{cases} (1 - k^{-\alpha}) \cdot |X|^{-1} + k^{-\alpha} \cdot |\Upsilon_{\mathrm{A}}|^{-1} & \text{if } x \in X \\ k^{-\alpha} \cdot |\Upsilon_{\mathrm{A}}|^{-1} & \text{else} \end{cases}$$

$$\tilde{n}_{\mathrm{B}} : \Upsilon_{\mathrm{B}} \to \mathbb{R}_{>0},\, y \mapsto \begin{cases} (1 - k^{-\alpha}) \cdot |Y|^{-1} + k^{-\alpha} \cdot |\Upsilon_{\mathrm{B}}|^{-1} & \text{if } y \in Y \\ k^{-\alpha} \cdot |\Upsilon_{\mathrm{B}}|^{-1} & \text{else} \end{cases}$$

1. **Invocation of F:** According to $\tilde{n}_{\mathrm{A}}$ Alice randomly chooses some input symbol $x \in \Upsilon_{\mathrm{A}}$; Bob randomly chooses some $y \in \Upsilon_{\mathrm{B}}$ according to $\tilde{n}_{\mathrm{B}}$. Then F is invoked with the input tuple (x, y), i.e. Alice learns some $a \in \Omega_{\mathrm{A}}$ and Bob learns some $b \in \Omega_{\mathrm{B}}$ with (a, b) distributed according to $\phi_{x,y}$. Alice concatenates x to $s_{\mathrm{A}}^{\mathsf{in}}$ and a to $s_{\mathrm{A}}^{\mathsf{out}}$ respectively; Bob concatenates y to $s_{\mathrm{B}}^{\mathsf{in}}$ and b to $s_{\mathrm{B}}^{\mathsf{out}}$.

   This protocol step is executed for k times.

2. **Check A:** Alice picks some uniformly random index set $\bar{K}_{\mathrm{A}} \subseteq K_{\mathrm{A}}$ with[a] $|\bar{K}_{\mathrm{A}}| = k^{\frac{1}{2}+\beta}$ and sends $\bar{K}_{\mathrm{A}}$ to Bob, who announces $\big(\hat{s}_{\mathrm{B}}^{\mathsf{in}}[\bar{K}_{\mathrm{A}}], \hat{s}_{\mathrm{B}}^{\mathsf{out}}[\bar{K}_{\mathrm{A}}]\big) := \big(s_{\mathrm{B}}^{\mathsf{in}}[\bar{K}_{\mathrm{A}}], s_{\mathrm{B}}^{\mathsf{out}}[\bar{K}_{\mathrm{A}}]\big)$. Alice aborts the protocol, if she finds some $x \in \Upsilon_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$, $a \in \Omega_{\mathrm{A}}$, $b \in \Omega_{\mathrm{B}}$ with:

$$\big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times \hat{s}_{\mathrm{B}}^{\mathsf{in}} \times \hat{s}_{\mathrm{B}}^{\mathsf{out}}[\bar{K}_{\mathrm{A}}]\big|_{(x,a,y,b)} \neq k^{\frac{1}{2}+\beta} \cdot \tilde{n}_{\mathrm{A}}(x) \cdot \tilde{n}_{\mathrm{B}}(y) \cdot \phi_{x,y}(a, b) \pm k^{\frac{1}{4}+\beta}$$

   At the end of this protocol step, Alice sets $K_{\mathrm{A}} \leftarrow K_{\mathrm{A}} \setminus \bar{K}_{\mathrm{A}}$ and Bob sets $K_{\mathrm{B}} \leftarrow K_{\mathrm{B}} \setminus \bar{K}_{\mathrm{A}}$.

3. **Check B:** This protocol step proceeds analogously to Check A with interchanged roles of Alice and Bob.

4. **Output:** Alice announces the index set $K'_{\mathrm{A}} := \big\{i \in K_{\mathrm{A}} \bigm| s_{\mathrm{A}}^{\mathsf{in}}[i] \in X\big\}$, then Bob announces $K'_{\mathrm{B}} := \big\{i \in K_{\mathrm{B}} \bigm| s_{\mathrm{B}}^{\mathsf{in}}[i] \in Y\big\}$; let $K' := K'_{\mathrm{A}} \cap K'_{\mathrm{B}}$. If $|K'| < k - k^{1-\gamma}$, the protocol is aborted; else Alice outputs the compound string $s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}}[K']$ and Bob outputs $s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}[K']$.

[a] W.l.o.g. we have that $k^{\frac{1}{2}+\beta} \in \mathbb{N}$, since $\beta \in \mathbb{Q}$ and w.l.o.g. $k \in \big\{l^{\zeta} \bigm| l, \zeta \in \mathbb{N}, \text{ such that } \zeta \cdot (\frac{1}{2} + \beta) \in \mathbb{N}\big\}$.

Figure 8: Our protocol scheme for secure generation of correlated data from a given 2-party function.

4.5 Protocol for generation of correlated data

Now we give the formal description of our generic protocol scheme for generation of correlated data (q.v. Figure 8). For convenience, we use the following quite self-suggesting notations.

Notation 27. Let "$a = b \pm c$" denote that $|a - b| < |c|$, i.e. the value a differs from b at most by c.

Notation 28. Let s be a finite string over some alphabet Ω. By $|s|$ we denote the length of s. By $|s|_\alpha$ with $\alpha \in \Omega$ we denote the number of appearances of α in s. We canonically extend this notation to subalphabets $T \subseteq \Omega$ by $|s|_T := \sum_{\alpha \in T} |s|_\alpha$. By $s[i]$ with $i \in \{1, \dots, |s|\}$ we denote the i-th element of s. For $n \in \mathbb{N}$ and a given index set $K = \{k_1, \dots, k_n\} \subset \mathbb{N}$ with $0 < k_1 < \ldots < k_n \leq |s|$, we denote the string $s[k_1]\, s[k_2] \ldots s[k_n]$ by $s[k_1, \dots, k_n]$, or simply by $s[K]$. Further, for some given strings s_{A} and s_{B} of the same length, we define the *compound string* $s_{\mathrm{A}} \times s_{\mathrm{B}}$, whose i-th element is just the tuple $\big(s_{\mathrm{A}}[i], s_{\mathrm{B}}[i]\big)$. We denote the i-th element of such a compound string by $s_{\mathrm{A}} \times s_{\mathrm{B}}[i]$.

Notation 29. Given any $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$, let Π_F denote the set of all quintuples $(X, Y, \alpha, \beta, \gamma)$, where $X \subseteq \Upsilon_{\mathrm{A}}$, $Y \subseteq \Upsilon_{\mathrm{B}}$, $\alpha, \beta, \gamma \in \mathbb{R}_{>0}$, such that $X, Y \neq \emptyset$ and $\beta \in \mathbb{Q}$ with $\beta < \frac{1}{6}$.

Notation 30. Given any $F \in \mathfrak{F}_{\mathsf{fin}}$ and $(X, Y, \alpha, \beta, \gamma) \in \Pi_F$, we define the following characteristics for non-aborted protocol runs of $\pi_F(X, Y, \alpha, \beta, \gamma)$:

$$\nu_{\mathrm{B}}\big((x,a),(y,b),(y',b')\big) := \frac{\big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}} \times \hat{s}_{\mathrm{B}}^{\mathsf{in}} \times \hat{s}_{\mathrm{B}}^{\mathsf{out}}[\bar{K}_{\mathrm{A}}]\big|_{(x,a,y,b,y',b')}}{\big|\bar{K}_{\mathrm{A}}\big|}$$

$$\nu_{\mathrm{A}}\big((x,a),(x',a'),(y,b)\big) := \frac{\big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times \hat{s}_{\mathrm{A}}^{\mathsf{in}} \times \hat{s}_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}[\bar{K}_{\mathrm{B}}]\big|_{(x,a,x',a'y,b)}}{\big|\bar{K}_{\mathrm{B}}\big|}$$

For convenience, we also write:

$$\begin{aligned}
\nu_{\mathrm{B}}|_{\mathrm{A}}(x) &:= \nu_{\mathrm{B}}\big((x,\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) & \nu_{\mathrm{A}}|_{\mathrm{B}}(y) &:= \nu_{\mathrm{A}}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(y,\Omega_{\mathrm{B}})\big) \\
\nu_{\mathrm{B}}|_{\mathrm{B}}^{\mathsf{true}}(y) &:= \nu_{\mathrm{B}}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,\Omega_{\mathrm{B}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) & \nu_{\mathrm{A}}|_{\mathrm{A}}^{\mathsf{true}}(x) &:= \nu_{\mathrm{A}}\big((x,\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \\
\nu_{\mathrm{B}}|_{\mathrm{B}}^{\mathsf{fake}}(y') &:= \nu_{\mathrm{B}}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(y',\Omega_{\mathrm{B}})\big) & \nu_{\mathrm{A}}|_{\mathrm{A}}^{\mathsf{fake}}(x') &:= \nu_{\mathrm{A}}\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(x',\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big)
\end{aligned}$$

4.6 Real protocol runs versus idealized cheating situations

We show now that our notion of cheating situations is close to what may ever happen during real protocol runs. Therefor, we utilize some powerful tools from probability theory (Lemma 31 and Corollary 32) and real algebraic geometry (Lemma 35 and Corollary 36). The former are borrowed from [KMQ10], but the latter are completely novel tools, which were necessary because our notion of cheating situations is more complex than that of [KMQ10, KMQ11]. In particular, normalized cheating situations in [KMQ10] can be described by linear constraints, which is not true in our case due to Condition 4 of Definition 5.

Lemma 31 (Stability of random distributions, [KMQ10, Lemma 15])**.** *Let some sequence $(X_k)_{k\in\mathbb{N}}$ of binomially and/or hypergeometrically distributed random variables X_k be given, such that $\mathbf{P}[0 \le X_k \le k] = 1$ for all $k \in \mathbb{N}$. Further let $\Delta > \frac{1}{2}$. Then the probability $\mathbf{P}\big[|X_k - \mathbf{E}(X_k)| \ge k^{\Delta}\big]$ is negligible in k.*

Proof. By [Hoe63, Theorem 2], for all $n \in \mathbb{N}$, $c \in \mathbb{R}_{>0}$ and every binomially distributed random variable X with $\mathbf{P}[0 \le X \le n] = 1$ it holds that $\mathbf{P}\big[|X - \mathbf{E}(X)| \ge c\big] \le 2 \cdot \exp\big(-2c^2 \cdot n^{-1}\big)$. In [Hoe63, Section 6] it was shown that this estimation holds for hypergeometrically distributed X, too. For all $k \in \mathbb{N}$, we can conclude:

$$\mathbf{P}\big[|X_k - \mathbf{E}(X_k)| \ge k^{\Delta}\big] \;\le\; 2 \cdot \exp\big(-2k^{2\Delta-1}\big) \qquad \square$$

Corollary 32 ([KMQ10, Corollary 16])**.** *Let $\mathcal{H}$ be some memoryless random source that samples from some finite alphabet Ω. Let $p : \Omega \to \mathbb{R}$, $x \mapsto \mathbf{P}[\mathcal{H}$ outputs $x]$. Further let $\mathcal{A}$ be some arbitrary algorithm that on input $k \in \mathbb{N}$ sequentially samples up to k random symbols $X_1, \ldots, X_N \overset{\mathrm{r}}{\leftarrow} \mathcal{H}$, i.e. N is a random variable with $\mathbf{P}[1 \le N \le k] = 1$ and N may be correlated with $(X_1, \ldots, X_N)$. Then for all constants $\Delta > \frac{1}{2}$ and all $S \subseteq \Omega$ the probability $\mathbf{P}\left[\big||X_1 \ldots X_N|_S - N \cdot p(S)\big| \ge k^{\Delta}\right]$ is negligible in k.*

Proof. For our proof we make $\mathcal{A}$ a bit more powerful: $\mathcal{A}$ always samples exactly k random symbols $X_1, \ldots, X_k \overset{\mathrm{r}}{\leftarrow} \mathcal{H}$ and then computes and outputs N.

Now, for $n \in \{1, \ldots, k\}$, $S \subseteq \Omega$ let $\mathcal{X}_n(S) := |X_1 \ldots X_n|_S$. Analogously to the proof of Lemma 31, for all $n \in \{0, \ldots, k\}$ and $S \subseteq \Omega$ it always holds:

$$\mathbf{P}\big[|\mathcal{X}_n(S) - n \cdot p(S)| \ge k^{\Delta}\big] \;\le\; \mathbf{P}\big[|\mathcal{X}_n(S) - n \cdot p(S)| \ge n^{\Delta}\big] \;\le\; 2 \cdot \exp\big(-2n^{2\Delta-1}\big)$$

Further, for $n < k^{\Delta}$ it trivially holds that $\mathbf{P}\big[|\mathcal{X}_n(S) - n \cdot p(S)| \geq k^{\Delta}\big] = 0$. Hence follows:

$$\mathbf{P}\big[|\mathcal{X}_N(S) - N \cdot p(S)| \geq k^{\Delta}\big] \;\leq\; \sum_{n=\lceil k^{\Delta}\rceil}^{k} \mathbf{P}\big[|\mathcal{X}_n(S) - n \cdot p(S)| \geq k^{\Delta}\big] \;\leq\; \frac{2(k-k^{\Delta})}{\exp\big(2k^{\Delta(2\Delta-1)}\big)} \qquad \square$$

Corollary 33. *Let some arbitrary* $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ *and* $(X, Y, \alpha, \beta, \gamma) \in \Pi_F$ *be given, as well as some constant* $\Delta > \frac{1}{2}$. *Let* $\pi := \pi_F(X, Y, \alpha, \beta, \gamma)$ *and let* k *denote the security parameter. Then, if Alice is honest, a protocol run of* π *with overwhelming probability is either aborted or for all* $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$ *and* $b \in \Omega_{\mathrm{B}}$ *we have that* $\nu_{\mathrm{B}}\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = k^{-1}\big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}\big|_{(x,a,y,b)} \pm k^{\Delta-(\frac{1}{2}+\beta)}$. *If Bob is honest, the analog holds for* ν_{A}.

Proof. Let us consider some arbitrary but fixed $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$ and $b \in \Omega_{\mathrm{B}}$. Once the compound string $s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}$ is generated by Alice and Bob calling F in the protocol step Invocation of F, we can consider an honest Alice's random choice of $\bar{K}_{\mathrm{A}}$ as a random experiment with hypergeometrically distributed outcome $\big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}[\bar{K}_{\mathrm{A}}]\big|_{(x,a,y,b)}$. Now, by Lemma 31 we have with overwhelming probability:

$$\big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}[\bar{K}_{\mathrm{A}}]\big|_{(x,a,y,b)} \;=\; k^{\frac{1}{2}+\beta} \cdot \frac{\big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}\big|_{(x,a,y,b)}}{k} \pm k^{\Delta}$$

As $\nu_{\mathrm{B}}\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = k^{-(\frac{1}{2}+\beta)}\big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}[\bar{K}_{\mathrm{A}}]\big|_{(x,a,y,b)}$ by definition (cf. Notation 30), we can conclude:

$$\nu_{\mathrm{B}}\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \;=\; k^{-1}\big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}\big|_{(x,a,y,b)} \pm k^{\Delta-(\frac{1}{2}+\beta)}$$

If Bob is honest, we have to take into account that a corrupted Alice might choose $\bar{K}_{\mathrm{A}}$ maliciously and thereby introduce an additional error of at most $k^{\beta-\frac{1}{2}}$ into our estimation, i.e.:

$$\nu_{\mathrm{A}}\big((x,a),(\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b)\big) \;=\; k^{-1}\big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}\big|_{(x,a,y,b)} \pm \big(k^{\Delta-(\frac{1}{2}+\beta)} + k^{\beta-\frac{1}{2}}\big)$$

However, since $\beta < \frac{1}{6}$ by definition (cf. Notation 29) and the estimation also holds for any Δ' with $\frac{1}{2} < \Delta' < \Delta$, we can argue:

$$k^{\Delta'-(\frac{1}{2}+\beta)} + k^{\beta-\frac{1}{2}} \quad=\quad k^{\Delta-(\frac{1}{2}+\beta)} \cdot k^{\Delta'-\Delta} \cdot \big(1 + k^{-\Delta'+2\beta}\big) \quad<\quad k^{\Delta-(\frac{1}{2}+\beta)} \cdot \underbrace{k^{\Delta'-\Delta} \cdot \big(1 + k^{-\frac{1}{6}}\big)}_{\leq 1 \text{ for almost all } k}$$

Hence, if Bob is honest, a protocol run of π with overwhelming probability is either aborted or for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$ and $b \in \Omega_{\mathrm{B}}$ we have:

$$\nu_{\mathrm{A}}\big((x,a),(\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b)\big) = k^{-1}\big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}\big|_{(x,a,y,b)} \pm k^{\Delta-(\frac{1}{2}+\beta)} \qquad \square$$

Lemma 34. *Let some arbitrary* $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ *and* $(X, Y, \alpha, \beta, \gamma) \in \Pi_F$ *be given, as well as some constant* $\Delta > \frac{1}{2}$. *Let* $\pi := \pi_F(X, Y, \alpha, \beta, \gamma)$ *and let* k *denote the security parameter. Then, if Alice is honest, a protocol run of* π *with overwhelming probability is either aborted or we have:*

1. *For all* $x \in \Upsilon_{\mathrm{A}}$ *it holds that* $\nu_{\mathrm{B}}|_{\mathrm{A}}(x) = \tilde{n}_A(x) \pm k^{(\frac{1}{2}+\beta)(\Delta-1)}$.

2. *For all $x \in \Upsilon_\mathrm{A}$, $a \in \Omega_\mathrm{A}$, $y \in \Upsilon_\mathrm{B}$, $b \in \Omega_\mathrm{B}$ it holds:*

$$\nu_\mathrm{B}\big((x,a),(y,b),(\Upsilon_\mathrm{B},\Omega_\mathrm{B})\big) = \nu_\mathrm{B}|_\mathrm{A}(x) \cdot \nu_\mathrm{B}|_\mathrm{B}^{\mathsf{true}}(y) \cdot \phi_{x,y}(a,b) \pm k^{(\frac{1}{2}+\beta)(\Delta-1)}$$

3. *For all $x \in \Upsilon_\mathrm{A}$, $a \in \Omega_\mathrm{A}$, $y' \in \Upsilon_\mathrm{B}$, $b' \in \Omega_\mathrm{B}$ it holds:*

$$\nu_\mathrm{B}\big((x,a),(\Upsilon_\mathrm{B},\Omega_\mathrm{B}),(y',b')\big) = \nu_\mathrm{B}|_\mathrm{A}(x) \cdot \nu_\mathrm{B}|_\mathrm{B}^{\mathsf{fake}}(y') \cdot \phi_{x,y}(a,b) \pm k^{\frac{\Delta-1}{2}}$$

4. *For all $x \in \Upsilon_\mathrm{A}$, $a \in \Omega_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$, $b, b' \in \Omega_\mathrm{B}$ with $\nu_\mathrm{B}\big((\Upsilon_\mathrm{A},\Omega_\mathrm{A}),(y,b),(\Upsilon_\mathrm{B},\Omega_\mathrm{B})\big) > 0$ it holds:*

$$\nu_\mathrm{B}\big((x,a),(y,b),(y',b')\big) = \nu_\mathrm{B}\big((\Upsilon_\mathrm{A},\Omega_\mathrm{A}),(y,b),(y',b')\big) \cdot \tfrac{\nu_\mathrm{B}((x,a),(y,b),(\Upsilon_\mathrm{B},\Omega_\mathrm{B}))}{\nu_\mathrm{B}((\Upsilon_\mathrm{A},\Omega_\mathrm{A}),(y,b),(\Upsilon_\mathrm{B},\Omega_\mathrm{B}))} \pm k^{(\frac{1}{2}+\beta)(\Delta-1)}$$

If Bob is honest, the analog holds for ν_A.

Proof. The techniques needed here are pretty much the same as for the proof of Corollary 33. The assertions 1 and 4 are direct consequences of Lemma 31, as we can consider $k^{\frac{1}{2}+\beta} \cdot \nu_\mathrm{B}|_\mathrm{A}(x)$ a binomially distributed random variable and $k^{\frac{1}{2}+\beta} \cdot \nu_\mathrm{B}\big((x,a),(y,b),(y',b')\big)$ a hypergeometrically distributed random variable in the respective context. Assertion 2 can be derived from Corollary 32, as a corrupted Bob's view in the protocol step Invocation of F can be seen as maliciously sampling from $|\Upsilon_\mathrm{B}|$ mutually independent memoryless random sources. Finally, an honest Alice enforces assertion 3 in the protocol step Check A, what can be shown as follows. Alice directly enforces that $\nu_\mathrm{B}\big((x,a),(\Upsilon_\mathrm{B},\Omega_\mathrm{B}),(y',b')\big) = \tilde{n}_\mathrm{A}(x) \cdot \tilde{n}_\mathrm{B}(y') \cdot \phi_{x,y'}(a,b') \pm k^{-\frac{1}{4}}$ for all $x \in \Upsilon_\mathrm{A}$, $a \in \Omega_\mathrm{A}$, $y' \in \Upsilon_\mathrm{B}$, $b' \in \Omega_\mathrm{B}$, whereby especially follows:

$$\nu_\mathrm{B}|_\mathrm{A}(x) = \tilde{n}_\mathrm{A}(x) \pm |\Omega_\mathrm{A} \times \Omega_\mathrm{B}| \cdot k^{-\frac{1}{4}}$$
$$\nu_\mathrm{B}|_\mathrm{B}^{\mathsf{fake}}(y') = \tilde{n}_\mathrm{B}(y') \pm |\Omega_\mathrm{A} \times \Omega_\mathrm{B}| \cdot k^{-\frac{1}{4}}$$

Thereby, we already have:

$$\nu_\mathrm{B}\big((x,a),(\Upsilon_\mathrm{B},\Omega_\mathrm{B}),(y',b')\big) = \nu_\mathrm{B}|_\mathrm{A}(x) \cdot \nu_\mathrm{B}|_\mathrm{B}^{\mathsf{fake}}(y') \cdot \phi_{x,y'}(a,b') \pm \big(2 \cdot |\Omega_\mathrm{A} \times \Omega_\mathrm{B}| + 1\big)k^{-\frac{1}{4}}$$

Furthermore, we can estimate the error term $\big(2 \cdot |\Omega_\mathrm{A} \times \Omega_\mathrm{B}| + 1\big)k^{-\frac{1}{4}}$ from above by $k^{\frac{\Delta-1}{2}}$ for almost all $k \in \mathbb{N}$, since $\Delta > \frac{1}{2}$ by assumption.

If Bob is honest, we have to take into account that a corrupted Alice might choose $\bar{K}_\mathrm{A}$ maliciously. This will only introduce an additional error of at most $k^{\beta-\frac{1}{2}}$ in the analog of our estimations for the assertions 1 and 2, i.e. there we formally have to replace the error term $k^{(\frac{1}{2}+\beta)(\Delta-1)}$ by $\big(k^{(\frac{1}{2}+\beta)(\Delta-1)} + k^{\beta-\frac{1}{2}}\big)$. However, since $\beta < \frac{1}{6}$ by definition (cf. Notation 29) and our estimations also hold for any Δ' with $\frac{1}{2} < \Delta' < \Delta$, we can argue:

$$\begin{aligned} k^{(\frac{1}{2}+\beta)(\Delta'-1)} + k^{\beta-\frac{1}{2}} &= k^{(\frac{1}{2}+\beta)(\Delta-1)} \cdot \big(k^{(\frac{1}{2}+\beta)(\Delta'-\Delta)} + k^{-\frac{\Delta}{2}+(2-\Delta)\beta}\big) \\ &< k^{(\frac{1}{2}+\beta)(\Delta-1)} \cdot \underbrace{\big(k^{\frac{1}{3}(\Delta'-\Delta)} + k^{-\frac{\Delta}{2}+\frac{1}{4}}\big)}_{\leq 1 \text{ for almost all } k} \end{aligned}$$ □

Lemma 35. *Let $n \in \mathbb{N}$ and some polynomial $f \in \mathbb{R}[X_1, \ldots, X_n]$ be given, such that the variety $V := \{x \in \mathbb{R}^n \mid f(x) = 0\}$ is not empty. Furthermore, let a bounded convex polytope $P \subset \mathbb{R}^n$ be given, such that $V \cap P \neq \emptyset$. Then for every norm there exist some constants $c, \delta \in \mathbb{R}_{>0}$, such that for all $x \in P$ it holds:*

$$\min\nolimits_{y \in V \cap P} \|x - y\| \;\leq\; c \cdot \big|f(x)\big|^\delta$$

Proof. Our proof is based on the Łojasiewicz Inequality [Łoj59, Theorem 17], by which for every open set $U \subseteq \mathbb{R}^n$, every real analytic function $h : U \to \mathbb{R}$ with non-empty zero locus Z and every compact set $K \subset U$ there exist some constants $c, \delta \in \mathbb{R}_{>0}$, such that for all $x \in K$ it holds:

$$\inf_{z \in Z} \|x - z\| \;\leq\; c \cdot \big|h(x)\big|^{\delta}$$

Note that we do not need to specify the norm used, since all norms on $\mathbb{R}^n$ are equivalent. In the following, for any $x \in \mathbb{R}^n$ and $S \subseteq \mathbb{R}^n$ let $\operatorname{dist}(x, S) := \inf_{y \in S} \|x - y\|$.

We want to prove our lemma by contradiction, i.e. we assume that for all $c, \delta \in \mathbb{R}_{>0}$ there exists some $x \in P$, such that $\operatorname{dist}(x, V \cap P) > c \cdot |f(x)|^{\delta}$. In particular, we find some sequence $(x_i)_{i \in \mathbb{N}} \subseteq P$, such that $\operatorname{dist}(x_i, V \cap P) > i \cdot \sqrt[i]{|f(x)|}$ for all $i \in \mathbb{N}$. Since P is closed and bounded and thus compact, the sequence $(x_i)_{i \in \mathbb{N}}$ has some limit point $\hat{x} \in P$. Moreover, we can choose $\hat{x}$ such that $f(\hat{x}) = 0$ and thus $\hat{x} \in V$, since otherwise we had the following contradiction:

$$\infty \;=\; \liminf_{i \in \mathbb{N}} i \cdot \sqrt[i]{|f(x_i)|} \;\leq\; \liminf_{i \in \mathbb{N}} \operatorname{dist}(x_i, V \cap P) \;\leq\; \operatorname{dist}(\hat{x}, V \cap P)$$

Hence, we have that $|f(x_i)| \leq 1$ for infinitely many $i \in \mathbb{N}$ and can discard all other members of the sequence $(x_i)_{i \in \mathbb{N}}$, while preserving the property that $\operatorname{dist}(x_i, V \cap P) > i \cdot \sqrt[i]{|f(x_i)|}$ for all $i \in \mathbb{N}$. Moreover, we can now discard *any* members of the sequence $(x_i)_{i \in \mathbb{N}}$ and still preserve that property. We will exploit this extensively. In the first instance, w.l.o.g. the whole sequence $(x_i)_{i \in \mathbb{N}}$ does converge to $\hat{x}$. Further, we find the following sequences:

- $(z_i)_{i \in \mathbb{N}} \subseteq V$, such that $\operatorname{dist}(x_i, z_i) = \operatorname{dist}(x_i, V)$
- $(w_i)_{i \in \mathbb{N}} \subseteq P$, such that w_i is a convex combination of x_i and z_i, and $\operatorname{dist}(w_i, z_i)$ is minimized

We also find some finite set of degree-one polynomials $T \subset \mathbb{R}[X_1, \ldots, X_n]$, such that we can write:

$$P \;=\; \big\{ x \in \mathbb{R}^n \;\big|\; \max_{g \in T} g(x) \leq 0 \big\}$$

Note that $\lim_{i \to \infty} w_i = \hat{x}$ and hence for almost all (w.l.o.g. all) $i \in \mathbb{N}$ it holds:

$$\forall\, g \in T : \qquad g(w_i) = 0 \quad \Rightarrow \quad g(\hat{x}) = 0$$

Moreover, by the Łojasiewicz Inequality there exist some constants $c', \delta' \in \mathbb{R}_{>0}$, such that for all $x \in P$ it holds:

$$\operatorname{dist}(x, V) \;\leq\; c' \cdot \big|f(x)\big|^{\delta'}$$

Hence, it must hold that $z_i \notin P$ and thus $\max_{g \in T} g(w_i) = 0$ for almost all (w.l.o.g. all) $i \in \mathbb{N}$, since otherwise we had a contradiction to our choice of $(x_i)_{i \in \mathbb{N}}$. Now, as $\max_{g \in T} g(w_i) = 0$ for all $i \in \mathbb{N}$, by a pigeonhole argument there must exist some $g \in T$, such that $g(w_i) = 0$ for infinitely many (w.l.o.g. all) $i \in \mathbb{N}$. Let $\hat{g}$ be such a polynomial. We define the affine subspace $A := \big\{ x \in \mathbb{R}^n \;\big|\; \hat{g}(x) = 0 \;\big\}$ and the polytope $Q := P \cap A$. Note that $V \cap Q \neq \emptyset$, as $\hat{x} \in V \cap Q$. Now we can utilize induction on the dimension n; or to be more precise, w.l.o.g. we may assume that n is minimal in the sense that for smaller n there would not exist any counterexample for our lemma. In particular, since for $n = 0$ our lemma is trivially true, we must have that $n > 0$. By the Triangle Inequality we can estimate:

$$\forall\, i \in \mathbb{N} : \quad \operatorname{dist}(x_i, V \cap P) \;\leq\; \operatorname{dist}(x_i, w_i) + \operatorname{dist}(w_i, V \cap Q)$$

However, since $(w_i)_{i \in \mathbb{N}} \subseteq Q \subset A$ by construction, we have that estimating $\operatorname{dist}(w_i, V \cap Q)$ is the original problem with dimension $n - 1$. Since by assumption there cannot be a counterexample for our lemma with dimension $n - 1$, we find $c'', \delta'' \in \mathbb{R}_{>0}$, such that for all $w \in Q$ it holds:

$$\operatorname{dist}(w, V \cap Q) \;\leq\; c'' \cdot \big|f(w)\big|^{\delta''}$$

Let $b := \max_{a \in P} \|\nabla f(a)\|$. For all $i \in \mathbb{N}$ it holds:

$$\begin{aligned} \operatorname{dist}(x_i, V \cap P) &\leq \operatorname{dist}(x_i, w_i) + \operatorname{dist}(w_i, V \cap Q) \\ &\leq \operatorname{dist}(x_i, w_i) + c'' \cdot \big|f(w_i)\big|^{\delta''} \\ &\leq \operatorname{dist}(x_i, w_i) + c'' \cdot \big(|f(x_i)| + \operatorname{dist}(x_i, w_i) \cdot \max_{a \in P} \|\nabla f(a)\|\big)^{\delta''} \\ &= \operatorname{dist}(x_i, w_i) + c'' \cdot \big(|f(x_i)| + b \cdot \operatorname{dist}(x_i, w_i)\big)^{\delta''} \end{aligned}$$

Now we can put things together. Since each w_i is a convex combination of the respective x_i and z_i, we can estimate:

$$\operatorname{dist}(x_i, w_i) \;\leq\; \operatorname{dist}(x_i, z_i) \;=\; \operatorname{dist}(x_i, V) \;\leq\; c' \cdot \big|f(x_i)\big|^{\delta'}$$

Thus, for all $i \in \mathbb{N}$ we have:

$$\operatorname{dist}(x_i, V \cap P) \;\leq\; c' \cdot \big|f(x_i)\big|^{\delta'} + c'' \cdot \Big(\big|f(x_i)\big| + b \cdot c' \cdot \big|f(x_i)\big|^{\delta'}\Big)^{\delta''}$$

We set $\delta := \min\{1, \delta', \delta''\}$ and $c := (c' + c'') \cdot (1 + b \cdot c')^{\delta}$. Since $\lim_{i \to \infty} f(x_i) = f(\hat{x}) = 0$, we have for almost all (w.l.o.g. all) $i \in \mathbb{N}$ that $|f(x_i)|$ is sufficiently small, so that we can estimate:

$$c' \cdot \big|f(x_i)\big|^{\delta'} + c'' \cdot \Big(\big|f(x_i)\big| + b \cdot c' \cdot \big|f(x_i)\big|^{\delta'}\Big)^{\delta''} \;\leq\; c' \cdot \big|f(x_i)\big|^{\delta} + c'' \cdot \Big(\big|f(x_i)\big| + b \cdot c' \cdot \big|f(x_i)\big|^{\delta}\Big)^{\delta}$$

In conclusion, we have for all $i \in \mathbb{N}$:

$$\begin{aligned} \operatorname{dist}(x_i, V \cap P) &\leq c' \cdot \big|f(x_i)\big|^{\delta} + c'' \cdot \Big(\big|f(x_i)\big| + b \cdot c' \cdot \big|f(x_i)\big|^{\delta}\Big)^{\delta} \\ &\leq (c' + c'') \cdot \Big(\big|f(x_i)\big| + b \cdot c' \cdot \big|f(x_i)\big|^{\delta}\Big)^{\delta} \\ &\leq (c' + c'') \cdot \Big((1 + b \cdot c') \cdot \big|f(x_i)\big|^{\delta}\Big)^{\delta} \\ &= c \cdot \big|f(x_i)\big|^{\delta^2} \end{aligned}$$

This contradicts our choice of the sequence $(x_i)_{i \in \mathbb{N}}$ and thus concludes this proof. □

Corollary 36. *Let $n \in \mathbb{N}$ and some finite set of polynomials $S \subset \mathbb{R}[X_1, \dots, X_n]$ be given, such that the variety $V := \{x \in \mathbb{R}^n \mid \forall f \in S : f(x) = 0\}$ is not empty. Furthermore, let a bounded convex polytope $P \subset \mathbb{R}^n$ be given, such that $V \cap P \neq \emptyset$. Then for every norm there exist some constants $c, \delta \in \mathbb{R}_{>0}$, such that for all $x \in P$ it holds:*

$$\min_{y \in V \cap P} \|x - y\| \;\leq\; c \cdot \max_{f \in S} \big|f(x)\big|^{\delta}$$

Proof. We define the polynomial $g := \sum_{f \in S} f^2$, whereby we get that $V = \{x \in \mathbb{R}^n \mid g(x) = 0\}$. Now, by Lemma 35 we find some constants $c', \delta' \in \mathbb{R}_{>0}$, such that for all $x \in P$ it holds:

$$\min_{y \in V \cap P} \|x - y\| \;\leq\; c' \cdot \big|g(x)\big|^{\delta'}$$

Thus, our proof is concluded by the observation that for all $x \in \mathbb{R}^n$ we have:

$$c' \cdot \big|g(x)\big|^{\delta'} \;\leq\; c' \cdot |S| \cdot \max_{f \in S} \big|f(x)\big|^{2\delta'}$$ □

Lemma 37. *Let any* $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ *be given. Then, if Alice is honest, there exist some constants* $\varepsilon, \varepsilon' \in \mathbb{R}_{>0}$*, such that for any* $\pi := \pi_F(X, Y, \alpha, \beta, \gamma)$ *with* $(X, Y, \alpha, \beta, \gamma) \in \Pi_F$ *and* $\alpha < \varepsilon'$ *a protocol run of* π *with overwhelming probability is either aborted or we have:*

$$\exists\, \eta \in \mathfrak{N}_{\mathrm{B}}^{(F)} :\ \sum\nolimits_{x \in \Upsilon_{\mathrm{A}},\, a \in \Omega_{\mathrm{A}},\, y, y' \in \Upsilon_{\mathrm{B}},\, b, b' \in \Omega_{\mathrm{B}}} \big| \eta\big((x,a),(y,b),(y',b')\big) - \nu_{\mathrm{B}}\big((x,a),(y,b),(y',b')\big) \big| \ \leq\ \tfrac{1}{k^{\varepsilon}}$$

If Bob is honest, the analog holds for ν_{A}*.*

Proof. For symmetry reasons it suffices to consider the case of an honest Alice.

First note that $P := \mathrm{pmf}\big((\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2\big)$ is a bounded convex polytope in the linear space $\mathbb{R}^{(\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2}$. Moreover, consider the variety $V \subseteq \mathbb{R}^{(\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2}$ defined by the following polynomial equations:

$$\begin{aligned}
&\eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = \eta\big((x,\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \cdot \eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,\Omega_{\mathrm{B}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \cdot \phi_{x,y}(a,b)\\
&\eta\big((x,a),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(y',b')\big) = \eta\big((x,\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \cdot \eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(y',\Omega_{\mathrm{B}})\big) \cdot \phi_{x,y'}(a,b')\\
&\eta\big((x,a),(y,b),(y',b')\big) \cdot \eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = \eta\big((\Upsilon_{\mathrm{A}},\Omega_{\mathrm{A}}),(y,b),(y',b')\big) \cdot \eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big)
\end{aligned}$$

Note that Bob's cheating situations for F (q.v. Definition 5) are just the mappings $\eta \in V \cap P$ with $\min_{x \in \Omega_{\mathrm{A}}} \eta\big((x,\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) > 0$, i.e. we have:

$$\mathfrak{N}_{\mathrm{B}}^{(F)} \ =\ \big\{\eta \in V \cap P \ \big|\ \forall\, x \in \Omega_{\mathrm{A}} : \eta\big((x,\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) > 0\big\} \tag{1}$$

Now, by Corollary 36 instantiated with the L^1-norm we find some constants $c, \delta \in \mathbb{R}_{>0}$, such that for *every* probability mass function $\tilde{\eta} \in P$ that fulfills our polynomial equations stated above up to some error ρ it holds:

$$\min\nolimits_{\eta \in V \cap P} \|\eta - \tilde{\eta}\|_1 \ \leq\ c \cdot \rho^{\delta}$$

Hence by Lemma 34, with some arbitrary but constant $\Delta > \frac{1}{2}$, a protocol run of π with overwhelming probability is either aborted or there exists a mapping $\eta \in V \cap P$ with:

$$\sum\nolimits_{x \in \Upsilon_{\mathrm{A}},\, a \in \Omega_{\mathrm{A}},\, y, y' \in \Upsilon_{\mathrm{B}},\, b, b' \in \Omega_{\mathrm{B}}} \big| \eta\big((x,a),(y,b),(y',b')\big) - \nu_{\mathrm{B}}\big((x,a),(y,b),(y',b')\big) \big| \ \leq\ c \cdot k^{\delta(\frac{1}{2}+\beta)(\Delta-1)}$$

Further, by Lemma 34 we still have that a protocol run of π with overwhelming probability is either aborted or for all $x \in \Upsilon_{\mathrm{A}}$ it holds:

$$\nu_{\mathrm{B}}\big((x,\Omega_{\mathrm{A}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \ \geq\ \tilde{n}_{\mathrm{A}}(x) - k^{(\frac{1}{2}+\beta)(\Delta-1)} \ \geq\ k^{-\alpha} \cdot |\Upsilon_{\mathrm{A}}|^{-1} - k^{(\frac{1}{2}+\beta)(\Delta-1)}$$

Now, if $k^{-\alpha} \cdot |\Upsilon_{\mathrm{A}}|^{-1} - k^{(\frac{1}{2}+\beta)(\Delta-1)} > c \cdot k^{\delta(\frac{1}{2}+\beta)(\Delta-1)}$, we can by (1) conclude that a protocol run of π with overwhelming probability is either aborted or there exists a *cheating situation* $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ with:

$$\sum\nolimits_{x \in \Upsilon_{\mathrm{A}},\, a \in \Omega_{\mathrm{A}},\, y, y' \in \Upsilon_{\mathrm{B}},\, b, b' \in \Omega_{\mathrm{B}}} \big| \eta\big((x,a),(y,b),(y',b')\big) - \nu_{\mathrm{B}}\big((x,a),(y,b),(y',b')\big) \big| \ \leq\ c \cdot k^{\delta(\frac{1}{2}+\beta)(\Delta-1)}$$

Note that w.l.o.g. $\delta \leq 1$, i.e. it suffices that $\alpha < \omega' := \delta(\frac{1}{2}+\beta)(1-\Delta)$ and hence $k^{-\alpha} \cdot |\Upsilon_{\mathrm{A}}|^{-1} > (c+1)k^{\delta(\frac{1}{2}+\beta)(\Delta-1)}$ for almost all $k \in \mathbb{N}$. Moreover, we could have chosen $\Delta < 1$, so that finally we can set $\varepsilon := \delta(\frac{1}{2}+\beta)(1-\Delta')$ with $\Delta < \Delta' < 1$. Thereby, we have that $c \cdot k^{\delta(\frac{1}{2}+\beta)(\Delta-1)} \leq k^{-\varepsilon}$ for almost all $k \in \mathbb{N}$ and it follows:

$$\sum\nolimits_{x \in \Upsilon_{\mathrm{A}},\, a \in \Omega_{\mathrm{A}},\, y, y' \in \Upsilon_{\mathrm{B}},\, b, b' \in \Omega_{\mathrm{B}}} \big| \eta\big((x,a),(y,b),(y',b')\big) - \nu_{\mathrm{B}}\big((x,a),(y,b),(y',b')\big) \big| \ \leq\ k^{-\varepsilon} \qquad \square$$

Lemma 38. *Let any $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ be given. Then, if Alice is honest, there exist some constants $\varepsilon, \varepsilon' \in \mathbb{R}_{>0}$, such that for any $\pi := \pi_F(X, Y, \alpha, \beta, \gamma)$ with $(X, Y, \alpha, \beta, \gamma) \in \Pi_F$ and $\alpha < \varepsilon'$ a protocol run of π with overwhelming probability is either aborted or there exists a cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ with the following properties:*

1. *We have that $\eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = \big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}\big|_{(x,a,y,b)} \cdot k^{-1} \pm k^{-\varepsilon}$ for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$, $b \in \Omega_{\mathrm{B}}$.*
2. *We have that $\eta|_{\mathrm{A}}(x) = \frac{1}{|X|} \pm k^{-\varepsilon}$ for all $x \in X$.*
3. *We have that $\eta|_{\mathrm{B}}^{\mathsf{fake}}(y) = \frac{1}{|Y|} \pm k^{-\varepsilon}$ for all $y \in Y$.*
4. *We have that $\eta|_{\mathrm{B}}^{\mathsf{fake}}(y) \leq k^{-\varepsilon}$ for all $y \in \Upsilon_{\mathrm{B}} \backslash Y$.*

If Bob is honest, the analog holds with $\eta \in \mathfrak{N}_{\mathrm{A}}^{(F)}$.

Proof. We just consider the case that Alice is honest; the analogous assertions for an honest Bob follow by symmetry reasons.

Let $\Delta > \frac{1}{2}$. Corollary 33 states that a protocol run of π is either aborted or for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}, y \in \Upsilon_{\mathrm{B}}, b \in \Omega_{\mathrm{B}}$ it holds:

$$\nu_{\mathrm{B}}\big((x,a),(y,a),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \;=\; \big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}\big|_{(x,a,y,b)} \cdot k^{-1} \pm k^{\Delta-(\frac{1}{2}+\beta)}$$

Further, by Lemma 37 we find some constants $\tilde{\varepsilon}, \varepsilon' \in \mathbb{R}_{>0}$, such that for any $\pi = \pi_F(X, Y, \alpha, \beta, \gamma)$ with $(X, Y, \alpha, \beta, \gamma) \in \Pi_F$ and $\alpha < \varepsilon'$ a protocol run of π with overwhelming probability is either aborted or we have:

$$\exists\, \eta \in \mathfrak{N}_{\mathrm{B}}^{(F)} : \; \sum\nolimits_{x\in\Upsilon_{\mathrm{A}},\, a\in\Omega_{\mathrm{A}},\, y,y'\in\Upsilon_{\mathrm{B}},\, b,b'\in\Omega_{\mathrm{B}}} \big|\eta\big((x,a),(y,b),(y',b')\big) - \nu_{\mathrm{B}}\big((x,a),(y,b),(y',b')\big)\big| \;\leq\; \tfrac{1}{k^{\tilde{\varepsilon}}}$$

Now, all we have to do is looking for some $\varepsilon > 0$, such that the four assertions of our proposition hold true for such an η. Assertion 1 directly follows by our considerations so far and the fact that we could have chosen $\Delta < \frac{1}{2} + \beta$. In particular, for all $x \in \Upsilon_{\mathrm{A}}, a \in \Omega_{\mathrm{A}}, y \in \Upsilon_{\mathrm{B}}, b \in \Omega_{\mathrm{B}}$ we have:

$$\eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \;=\; \big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}\big|_{(x,a,y,b)} \cdot k^{-1} \pm \big(k^{\Delta-(\frac{1}{2}+\beta)} + k^{-\tilde{\varepsilon}}\big)$$

I.e., we just need that $\varepsilon < \frac{1}{2} + \beta - \Delta$ and $\varepsilon < \tilde{\varepsilon}$. The remaining three assertions follow by the observation that in the protocol step Check A (q.v. Figure 8) an honest Alice for all $x \in \Upsilon_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$ enforces the following inequality:

$$\big|s_{\mathrm{A}}^{\mathsf{in}} \times \hat{s}_{\mathrm{B}}^{\mathsf{in}}[\bar{K}_{\mathrm{A}}]\big|_{(x,y)} \;=\; k^{\frac{1}{2}+\beta} \cdot \tilde{n}_{\mathrm{A}}(x) \cdot \tilde{n}_{\mathrm{B}}(y) \pm k^{\frac{1}{4}+\beta} \cdot |\Omega_{\mathrm{A}} \times \Omega_{\mathrm{B}}|$$

By definition of ν_{B} (q.v. Notation 30) this expression is equivalent to the following:

$$\nu_{\mathrm{B}}\big((x,\Omega_{\mathrm{A}}),(y,\Omega_{\mathrm{B}}),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \;=\; \tilde{n}_{\mathrm{A}}(x) \cdot \tilde{n}_{\mathrm{B}}(y) \pm k^{-\frac{1}{4}} \cdot |\Omega_{\mathrm{A}} \times \Omega_{\mathrm{B}}|$$

Thus, by construction of $\tilde{n}_{\mathrm{A}}$ and $\tilde{n}_{\mathrm{B}}$ (q.v. Figure 8) it follows for our η:

$$\begin{aligned}
\eta|_{\mathrm{A}}(x) &= \tfrac{1}{|X|} \pm \big(\tfrac{k^{-\alpha}}{|X|} - \tfrac{k^{-\alpha}}{|\Upsilon_{\mathrm{A}}|} + k^{-\frac{1}{4}} \cdot |\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{A}} \times \Omega_{\mathrm{B}}| + k^{-\varepsilon}\big) && \text{for all } x \in X \\
\eta|_{\mathrm{B}}^{\mathsf{fake}}(y) &= \tfrac{1}{|Y|} \pm \big(\tfrac{k^{-\alpha}}{|Y|} - \tfrac{k^{-\alpha}}{|\Upsilon_{\mathrm{B}}|} + k^{-\frac{1}{4}} \cdot |\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}} \times \Omega_{\mathrm{B}}| + k^{-\varepsilon}\big) && \text{for all } y \in Y \\
\eta|_{\mathrm{B}}^{\mathsf{fake}}(y) &\leq \tfrac{k^{-\alpha}}{|\Upsilon_{\mathrm{B}}|} + k^{-\frac{1}{4}} \cdot |\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}} \times \Omega_{\mathrm{B}}| + k^{-\varepsilon} && \text{for all } y \in \Upsilon_{\mathrm{B}} \backslash Y
\end{aligned}$$

So, we only additionally need that $\varepsilon < \alpha$ and $\varepsilon < \frac{1}{4}$ and we are done. □

4.7 Secure generation of correlated data

In this section we put things together by combining the results of Section 4.4 and Section 4.6. In particular, we show that our generic protocol scheme from Section 4.5 can always be instantiated such that no corrupted party can deviate from the prescribed input probabilities too much, and thus the generated data is non-trivially correlated. This suffices for implementation of OT as described in Section 3.2.

Notation 39 (Cheating quantum). For $F = (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$, with $\dot{\mathfrak{N}}_F$ denoting the minimal spanning set of all normalized cheating situations for F (q.v. Lemma 10), we define:

$$\vartheta_F \;:=\; \min\bigl\{\eta|_\mathrm{B}^{\mathsf{fake}}(y') \bigm| y' \in \Upsilon_\mathrm{B},\, \eta \in \dot{\mathfrak{N}}_F : \eta|_\mathrm{B}^{\mathsf{fake}}(y') > 0\bigr\}$$

Lemma 40 (Quantizability of cheating situations)**.** *Let $F := (\Upsilon_\mathrm{A}, \Upsilon_\mathrm{B}, \Omega_\mathrm{A}, \Omega_\mathrm{B}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$. Further, let $\eta \in \mathfrak{N}_\mathrm{B}^{(F)}$, $\omega \in \mathbb{R}_{\geq 0}$, such that $\omega < \frac{1}{|\Upsilon_\mathrm{B}|}$. Then there exists some $\eta' \in \mathfrak{N}_\mathrm{B}^{(F)}$ that fulfills the following two conditions:*

1. *For all $y' \in \Upsilon_\mathrm{B}$ we have the following implication:*

$$\eta|_\mathrm{B}^{\mathsf{fake}}(y') \leq \omega \cdot \vartheta_F \quad \Rightarrow \quad \eta'|_\mathrm{B}^{\mathsf{fake}}(y') = 0$$

2. *For all $x \in \Upsilon_\mathrm{A}$, $a \in \Omega_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$, $b, b' \in \Omega_\mathrm{B}$ we have:*

$$\bigl|\eta\bigl((x,a),(y,b),(y',b')\bigr) - \eta'\bigl((x,a),(y,b),(y',b')\bigr)\bigr| \;\leq\; 2\omega \cdot |\Upsilon_\mathrm{A} \times \Upsilon_\mathrm{B}|$$

Proof. As stated in Lemma 10, the set of all normalized cheating situations for F is the convex hull of a finte set of vertices, say $\{\dot\eta_1, \ldots, \dot\eta_n\}$. Note that for all $i \in \{1, \ldots, n\}$ and all $y' \in \Upsilon_\mathrm{B}$ we have that either $0 < \vartheta_F \leq \dot\eta_i|_\mathrm{B}^{\mathsf{fake}}(y')$ or $\dot\eta_i|_\mathrm{B}^{\mathsf{fake}}(y') = 0$ by definition of ϑ_F (q.v. Notation 39). Now, let $\tilde\eta$ denote the normalized version of η (cf. Corollary 9). We define:

$$Y' := \bigl\{y' \in \Upsilon_\mathrm{B} \bigm| 0 < \tilde\eta|_\mathrm{B}^{\mathsf{fake}}(y') \leq \omega \cdot \vartheta_F\bigr\}$$

W.l.o.g., we assume that $Y' \neq \emptyset$, as otherwise we could just set $\eta' := \eta$ (cf. Remark 13). Moreover, we find some $a_1, \ldots, a_n \in \mathbb{R}_{\geq 0}$, such that $\sum_{i=1}^n a_i \cdot \dot\eta_i = \tilde\eta$ and especially $\sum_{i=1}^n a_i = 1$. We define the index set $I := \bigl\{i \in \{1, \ldots, n\} \bigm| \dot\eta_i|_\mathrm{B}^{\mathsf{fake}}(y') > 0\bigr\}$, whereby we get:

$$\sum\nolimits_{i\in I} a_i \cdot \vartheta_F \;\leq\; \sum\nolimits_{i\in I} a_i \cdot \dot\eta_i|_\mathrm{B}^{\mathsf{fake}}(Y') \;\leq\; \tilde\eta|_\mathrm{B}^{\mathsf{fake}}(Y') \;\leq\; \omega \cdot \vartheta_F \cdot |Y'|$$

Since $\omega < \frac{1}{|\Upsilon_\mathrm{B}|}$ by assumption, this especially yields that $\sum_{i\in I} a_i \leq \omega \cdot |Y'| < 1$. So, we can set $J := \{1, \ldots, n\} \backslash I$ and $\tilde\eta' := (\sum_{i\in J} a_i)^{-1} \cdot \sum_{i\in J} a_i \cdot \dot\eta_i$, whereby for all $x \in \Upsilon_\mathrm{A}$, $a \in \Omega_\mathrm{A}$, $y, y' \in \Upsilon_\mathrm{B}$, $b, b' \in \Omega_\mathrm{B}$ we get:

$$\begin{aligned}
&\bigl|\tilde\eta\bigl((x,a),(y,b),(y',b')\bigr) - \tilde\eta'\bigl((x,a),(y,b),(y',b')\bigr)\bigr| \\
&= \left|\sum_{i=1}^n a_i \cdot \dot\eta_i\bigl((x,a),(y,b),(y',b')\bigr) - \frac{\sum_{i\in J} a_i \cdot \dot\eta_i\bigl((x,a),(y,b),(y',b')\bigr)}{\sum_{i\in J} a_i}\right| \\
&\leq \left|\sum_{i\in I} a_i \cdot \dot\eta_i\bigl((x,a),(y,b),(y',b')\bigr)\right| + \left|\left(1 - \frac{1}{\sum_{i\in J} a_i}\right) \cdot \sum_{i\in J} a_i \cdot \dot\eta_i\bigl((x,a),(y,b),(y',b')\bigr)\right| \\
&\leq \left|\sum_{i\in I} a_i\right| + \left|\left(1 - \frac{1}{\sum_{i\in J} a_i}\right) \cdot \sum_{i\in J} a_i\right| \;=\; 2\sum_{i\in I} a_i \;\leq\; 2\omega \cdot |Y'| \;\leq\; 2\omega \cdot |\Upsilon_\mathrm{B}|
\end{aligned}$$

Finally, we define the mapping $\eta' : (\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}}) \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2 \to \mathbb{R}_{\geq 0}$ by:

$$\eta'\big((x,a),(y,b),(y',b')\big) := |\Upsilon_{\mathrm{A}}| \cdot \eta|_{\mathrm{A}}(x) \cdot \tilde{\eta}'\big((x,a),(y,b),(y',b')\big)$$

Since $\tilde{\eta}'$ is normalized, by Lemma 8 it follows that $\eta' \in \mathfrak{N}_{\mathrm{B}}^{(F)}$. Now we can put things together. On the one hand, by our choice of $\tilde{\eta}$ for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y' \in \Upsilon_{\mathrm{B}}$, $b' \in \Omega_{\mathrm{B}}$ we have (q.v. Corollary 9):

$$\frac{\eta((x,a),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(y',b'))}{\eta|_{\mathrm{A}}(x)} = \frac{\tilde{\eta}((x,a),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}}),(y',b'))}{\tilde{\eta}|_{\mathrm{A}}(x)}$$

Thus, by Condition 3 of Definition 5, for all $y' \in \Upsilon_{\mathrm{B}}$ it follows:

$$\eta|_{\mathrm{B}}^{\mathsf{fake}}(y') = \tilde{\eta}|_{\mathrm{B}}^{\mathsf{fake}}(y')$$

So, for all $y' \in \Upsilon_{\mathrm{B}}$ with $\eta|_{\mathrm{B}}^{\mathsf{fake}}(y') \leq \omega \cdot \vartheta_F$ it holds that $y' \in Y'$ and hence $\eta'|_{\mathrm{B}}^{\mathsf{fake}}(y') = \tilde{\eta}'|_{\mathrm{B}}^{\mathsf{fake}}(y') = 0$ by construction. On the other hand, for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y, y' \in \Upsilon_{\mathrm{B}}$, $b, b' \in \Omega_{\mathrm{B}}$ we can rewrite the distance $\big|\eta\big((x,a),(y,b),(y',b')\big) - \eta'\big((x,a),(y,b),(y',b')\big)\big|$ as follows:

$$|\Upsilon_{\mathrm{A}}| \cdot \underbrace{\eta|_{\mathrm{A}}(x)}_{\leq 1} \cdot \underbrace{\big|\tilde{\eta}\big((x,a),(y,b),(y',b')\big) - \tilde{\eta}'\big((x,a),(y,b),(y',b')\big)\big|}_{\leq 2\omega \cdot |\Upsilon_{\mathrm{B}}|}$$ □

Corollary 41. *Let any $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ be given. Then, if Alice is honest, there exist some constants $\varepsilon, \varepsilon' \in \mathbb{R}_{>0}$, such that for any $\pi := \pi_F(X, Y, \alpha, \beta, \gamma)$ with $(X, Y, \alpha, \beta, \gamma) \in \Pi_F$ and $\alpha < \varepsilon'$ a protocol run of π with overwhelming probability is either aborted or there exists a cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ with the following properties:*

1. *It holds that $\eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = \big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}\big|_{(x,a,y,b)} \cdot k^{-1} \pm k^{-\varepsilon}$ for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$, $b \in \Omega_{\mathrm{B}}$.*
2. *It holds that $\eta|_{\mathrm{A}}(x) = \frac{1}{|X|} \pm k^{-\varepsilon}$ for all $x \in X$.*
3. *It holds that $\eta|_{\mathrm{B}}^{\mathsf{fake}}(y) = \frac{1}{|Y|} \pm k^{-\varepsilon}$ for all $y \in Y$.*
4. *It holds that $\eta|_{\mathrm{B}}^{\mathsf{fake}}(y) = 0$ for all $y \in \Upsilon_{\mathrm{B}} \backslash Y$.*

If Bob is honest, the analog holds with $\eta \in \mathfrak{N}_{\mathrm{A}}^{(F)}$.

Proof. The proof is straightforward; we just need to combine Lemma 38 and Lemma 40. □

Lemma 42. *Let some redundancy-free $F := (\Upsilon_{\mathrm{A}}, \Upsilon_{\mathrm{B}}, \Omega_{\mathrm{A}}, \Omega_{\mathrm{B}}, \phi) \in \mathfrak{F}_{\mathsf{fin}}$ be given that has some OT-core. Then there also exist an OT-core $\{(\bar{x},\bar{a}),(\bar{x}',\bar{a}')\} \times \{(\bar{y},\bar{b}),(\bar{y}',\bar{b}')\} \subseteq (\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}})^2 \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2$, a protocol $\pi := \pi_F(\{\bar{x},\bar{x}'\},\{\bar{y},\bar{y}'\},\alpha,\beta,\gamma)$ with $(\{\bar{x},\bar{x}'\},\{\bar{y},\bar{y}'\},\alpha,\beta,\gamma) \in \Pi_F$ and a constant $\varepsilon \in \mathbb{R}_{>0}$ with the following property: If at least one party (Alice or Bob) is honest, a protocol run of π with overwhelming probability is either aborted or in the end for all $x \in \{\bar{x},\bar{x}'\}$, $a \in \Omega_{\mathrm{A}}$, $y \in \{\bar{y},\bar{y}'\}$, $b \in \Omega_{\mathrm{B}}$ it holds:*

$$\tfrac{1}{k} \cdot \big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}[K']\big|_{(x,a,y,b)} \;=\; \tfrac{1}{|\{\bar{x},\bar{x}'\} \times \{\bar{y},\bar{y}'\}|} \cdot \phi_{x,y}(a,b) \pm k^{-\varepsilon}$$

Proof. By assumption we have an OT-core $\{(\tilde{x},\tilde{a}),(\tilde{x}',\tilde{a}')\} \times \{(\tilde{y},\tilde{b}),(\tilde{y}',\tilde{b}')\} \subseteq (\Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{A}})^2 \times (\Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}})^2$. By Corollary 26 we find some $(\bar{y},\bar{b}),(\bar{y}',\bar{b}') \in \Upsilon_{\mathrm{B}} \times \Omega_{\mathrm{B}}$, such that $\{(\tilde{x},\tilde{a}),(\tilde{x}',\tilde{a}')\} \times \{(\bar{y},\bar{b}),(\bar{y}',\bar{b}')\}$ also is an OT-core and every cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ with $\eta|^{\mathsf{fake}}(\{\bar{y},\bar{y}'\}) = 1$ is equivalent to a trivial cheating situation (cf. Definition 6). Analogously, we find some $(\bar{x},\bar{a}),(\bar{x}',\bar{a}') \in \Upsilon_{\mathrm{A}} \times \Omega_{\mathrm{a}}$, such that $\{(\bar{x},\bar{a}),(\bar{x}',\bar{a}')\} \times \{(\bar{y},\bar{b}),(\bar{y}',\bar{b}')\}$ is still an OT-core and for every $\eta \in \mathfrak{N}_{\mathrm{A}}^{(F)}$ with $\eta|_{\mathrm{A}}^{\mathsf{fake}}(\{\bar{x},\bar{x}'\}) = 1$ and all $x \in \Upsilon_{\mathrm{A}}$ we also have:

$$\eta|_{\mathrm{A}}^{\mathsf{fake}}(x) \;=\; \eta|_{\mathrm{A}}^{\mathsf{true}}(x)$$

Now, let $\pi := \pi_F(\{\bar{x},\bar{x}'\},\{\bar{y},\bar{y}'\},\alpha,\beta,\gamma)$ with $(\{\bar{x},\bar{x}'\},\{\bar{y},\bar{y}'\},\alpha,\beta,\gamma) \in \Pi_F$ and let α be sufficiently small, so that we can apply Corollary 41. Henceforth, for symmetry reasons it suffices to consider the case that Alice is honest. In this case, we find by Corollary 41 some constant $\tilde{\varepsilon} \in \mathbb{R}_{>0}$, such that a protocol run of π with overwhelming probability is either aborted or there exists a cheating situation $\eta \in \mathfrak{N}_{\mathrm{B}}^{(F)}$ fulfilling the following conditions for all $x \in \Upsilon_{\mathrm{A}}$, $a \in \Omega_{\mathrm{A}}$, $y \in \Upsilon_{\mathrm{B}}$, $b \in \Omega_{\mathrm{B}}$:

$$\eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) = \big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}\big|_{(x,a,y,b)} \cdot k^{-1} \pm k^{-\tilde{\varepsilon}} \tag{2}$$

$$\eta|_{\mathrm{A}}(x) = \tfrac{1}{|\{\bar{x},\bar{x}'\}|} \pm k^{-\tilde{\varepsilon}} \qquad \text{if } x \in \{\bar{x},\bar{x}'\} \tag{3}$$

$$\eta|_{\mathrm{B}}^{\mathsf{fake}}(y) = \tfrac{1}{|\{\bar{y},\bar{y}'\}|} \pm k^{-\tilde{\varepsilon}} \qquad \text{if } y \in \{\bar{y},\bar{y}'\} \tag{4}$$

$$\eta|_{\mathrm{B}}^{\mathsf{fake}}(y) = 0 \qquad \text{if } y \in \Upsilon_{\mathrm{B}} \backslash \{\bar{y},\bar{y}'\} \tag{5}$$

Note that (5) can be reformulated as $\eta|_{\mathrm{B}}^{\mathsf{fake}}(\{\bar{y},\bar{y}'\}) = 1$, and thus our choice of $\bar{y},\bar{y}'$ yields that (4) is equivalent to the following:

$$\eta|_{\mathrm{B}}^{\mathsf{true}}(y) = \tfrac{1}{|\{\bar{y},\bar{y}'\}|} \pm k^{-\tilde{\varepsilon}} \quad \text{for all } y \in \{\bar{y},\bar{y}'\}$$

Hence, by (3) and Condition 2 of Definition 5 we have for all $x \in \{\bar{x},\bar{x}'\}$, $a \in \Omega_{\mathrm{A}}$, $y \in \{\bar{y},\bar{y}'\}$, $b \in \Omega_{\mathrm{B}}$:

$$\eta\big((x,a),(y,b),(\Upsilon_{\mathrm{B}},\Omega_{\mathrm{B}})\big) \;=\; \frac{\phi_{x,y}(a,b)}{|\{\bar{x},\bar{x}'\} \times \{\bar{y},\bar{y}'\}|} \pm k^{-\tilde{\varepsilon}} \left(\frac{1}{|\{\bar{x},\bar{x}'\}|} + \frac{1}{|\{\bar{y},\bar{y}'\}|} + k^{-\tilde{\varepsilon}}\right)$$

By (2), this yields for all $x \in \{\bar{x},\bar{x}'\}$, $a \in \Omega_{\mathrm{A}}$, $y \in \{\bar{y},\bar{y}'\}$, $b \in \Omega_{\mathrm{B}}$:

$$\tfrac{1}{k} \cdot \big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}\big|_{(x,a,y,b)} \;=\; \frac{\phi_{x,y}(a,b)}{|\{\bar{x},\bar{x}'\} \times \{\bar{y},\bar{y}'\}|} \pm k^{-\tilde{\varepsilon}} \left(1 + \frac{1}{|\{\bar{x},\bar{x}'\}|} + \frac{1}{|\{\bar{y},\bar{y}'\}|} + k^{-\tilde{\varepsilon}}\right)$$

Since in the protocol step Output of π every honest party enforces that $|K'| \geq k - k^{1-\gamma}$ (q.v. Figure 8), we finally have for all $x \in \{\bar{x},\bar{x}'\}$, $a \in \Omega_{\mathrm{A}}$, $y \in \{\bar{y},\bar{y}'\}$, $b \in \Omega_{\mathrm{B}}$:

$$\tfrac{1}{k} \cdot \big|s_{\mathrm{A}}^{\mathsf{in}} \times s_{\mathrm{A}}^{\mathsf{out}} \times s_{\mathrm{B}}^{\mathsf{in}} \times s_{\mathrm{B}}^{\mathsf{out}}[K']\big|_{(x,a,y,b)} \;=\; \frac{\phi_{x,y}(a,b)}{|\{\bar{x},\bar{x}'\} \times \{\bar{y},\bar{y}'\}|} \pm \left(k^{-\tilde{\varepsilon}} \left(1 + \frac{1}{|\{\bar{x},\bar{x}'\}|} + \frac{1}{|\{\bar{y},\bar{y}'\}|} + k^{-\tilde{\varepsilon}}\right) + k^{-\gamma}\right)$$

This concludes our proof, since we can choose an arbitrary constant $\varepsilon > 0$ with $\varepsilon < \min\{\tilde{\varepsilon},\gamma\}$ and then for almost all $k \in \mathbb{N}$ estimate the error term by $k^{-\varepsilon}$. □

4.8 Conclusion of the formal part

By Lemma 42, one can now show quite straightforwardly our final theorem. This final theorem just states that we can implement the functionality $\mathcal{F}_{\mathrm{SMCD}}^{(G,\varepsilon)}$ (q.v. Figure 6), instantiated such that G has some OT-core, from any redundancy-free 2-party function $F \in \mathfrak{F}_{\mathsf{fin}}$ that has some OT-core itself. Since OT can be implemented from such instantiations of $\mathcal{F}_{\mathrm{SMCD}}^{(G,\varepsilon)}$ by standard techniques (q.v. Section 3.2), this concludes our work.

Theorem. *Let any redundancy-free 2-party function $F \in \mathfrak{F}_{\mathsf{fin}}$ be given that has some OT-core. Then there exist a constant $\varepsilon \in \mathbb{R}_{>0}$ and a tuple of protocol parameters $(X, Y, \alpha, \beta, \gamma) \in \Pi_F$, such that the protocol $\pi := \pi_F(X, Y, \alpha, \beta, \gamma)$ implements UC-securely the functionality $\mathcal{F}^{(G,\varepsilon)}_{\mathrm{SMCD}}$ (q.v. Figure 6) with some G that also has an OT-core.*

Proof. We instantiate ε and the protocol parameters $(X, Y, \alpha, \beta, \gamma)$ as needed for Lemma 42, with $X = \{\bar{x}, \bar{x}'\}$ and $Y = \{\bar{y}, \bar{y}'\}$. In particular, there exist $\bar{a}, \bar{a}' \in \Omega_{\mathrm{A}}$, $\bar{b}, \bar{b}' \in \Omega_{\mathrm{B}}$, such that $\{(\bar{x}, \bar{a}), (\bar{x}', \bar{a}')\} \times \{(\bar{y}, \bar{b}), (\bar{y}', \bar{b}')\}$ is an OT-core. Further, we define $G := (\Lambda_{\mathrm{A}}, \Lambda_{\mathrm{B}}, \psi)$ as follows:

$$\Lambda_{\mathrm{A}} := \big\{(x, a) \in X \times \Omega_{\mathrm{A}} \bigm| \phi_{X,Y}(a, \Omega_{\mathrm{B}}) > 0\big\} \qquad \psi\big((x, a), (y, b)\big) := \frac{\phi_{x,y}(a, b)}{|X \times Y|}$$
$$\Lambda_{\mathrm{B}} := \big\{(y, b) \in Y \times \Omega_{\mathrm{B}} \bigm| \phi_{X,Y}(\Omega_{\mathrm{A}}, b) > 0\big\}$$

Note that G has some OT-core by construction. Furthermore, w.l.o.g. we have that $\varepsilon \leq \gamma$. Now we have to show that $\pi := \pi_F(X, Y, \alpha, \beta, \gamma)$ implements UC-securely $\mathcal{F}^{(G,\varepsilon)}_{\mathrm{SMCD}}$.

If no party is corrupted, it follows straightforwardly by Lemma 31 that π is aborted only with some negligible probability. Further, the simulator in the ideal model just has to send a compound string $t_{\mathrm{A}} \times t_{\mathrm{B}}$ of right length to the ideal functionality $\mathcal{F}^{(G,\varepsilon)}_{\mathrm{SMCD}}$, so that the joint output distribution of non-aborted protocol runs in the real model is identical to the joint output distribution in the ideal model. Thus, simulation in a totally uncorrupted setting is just straightforward.

If Alice (and only Alice) or Bob (and only Bob) is corrupted, we need only a slightly more sophisticated simulator program. For symmetry reasons it suffices to consider a corrupted Bob. In this case, our simulator works as follows: He lets the corrupted Bob play with a simulated version of the honest Alice and a simulated version of the hybrid functionality $\mathcal{F}^{(F)}_{\mathrm{SFE}}$, thus generating some joint output string $(s^{\mathsf{in}}_{\mathrm{A}} \times s^{\mathsf{out}}_{\mathrm{A}}) \times (s^{\mathsf{in}}_{\mathrm{B}} \times s^{\mathsf{out}}_{\mathrm{B}})[K']$ with $k - k^{1-\gamma} < |K'| \leq k$ (if the protocol is not aborted). By Lemma 42, this simulated protocol run of π with overwhelming probability is either aborted or in the end for all $x \in \{\bar{x}, \bar{x}'\}$, $a \in \Omega_{\mathrm{A}}$, $y \in \{\bar{y}, \bar{y}'\}$, $b \in \Omega_{\mathrm{B}}$ it holds:

$$\tfrac{1}{k} \cdot \big|s^{\mathsf{in}}_{\mathrm{A}} \times s^{\mathsf{out}}_{\mathrm{A}} \times s^{\mathsf{in}}_{\mathrm{B}} \times s^{\mathsf{out}}_{\mathrm{B}}[K']\big|_{(x,a,y,b)} \;=\; \tfrac{1}{|\{\bar{x},\bar{x}'\} \times \{\bar{y},\bar{y}'\}|} \cdot \phi_{x,y}(a, b) \pm k^{-\varepsilon}$$

Thus, if the simulated protocol run is not aborted, the simulator can just set $t_{\mathrm{A}} := s^{\mathsf{in}}_{\mathrm{A}} \times s^{\mathsf{out}}_{\mathrm{A}}[K']$ and $t_{\mathrm{B}} := s^{\mathsf{in}}_{\mathrm{B}} \times s^{\mathsf{out}}_{\mathrm{B}}[K']$ and then send $t_{\mathrm{A}} \times t_{\mathrm{B}}$ to the ideal functionality $\mathcal{F}^{(G,\varepsilon)}_{\mathrm{SMCD}}$. Else, i.e. if the simulated protocol run is aborted, the simulator just needs to terminate, too. Again, it is straightforward to verify that the ideal model is statistically indistinguishable from the real model.

If both parties are corrupted, there is nothing to prove, since the simulator can just perfectly simulate the complete real model. □

Acknowledgements

The author wants to heartly thank Felipe Voloch from the mathoverflow community for pointing him to the Łojasiewicz Inequality.

References

[BMM99] Amos Beimel, Tal Malkin, and Silvio Micali. The all-or-nothing nature of two-party secure computation. In Michael J. Wiener, editor, *Advances in Cryptology, Proceedings of CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 80–97. Springer, 1999.

[BOGKW88] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of STOC 1988*, pages 113–131. ACM, 1988.

[Can01] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings of FOCS 2001*, pages 136–145, 2001. Revised full version online available at `http://eprint.iacr.org/2000/067`.

[CCM98] Christian Cachin, Claude Crépeau, and Julien Marcil. Oblivious transfer with a memory-bounded receiver. In *Proceedings of FOCS 1998*, pages 493–502, 1998.

[CGS08] Nishanth Chandran, Vipul Goyal, and Amit Sahai. New constructions for UC secure computation using tamper-proof hardware. In Nigel P. Smart, editor, *Advances in Cryptology, Proceedings of EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 545–562. Springer, 2008.

[CGT95] Claude Crépeau, Jeroen van de Graaf, and Alain Tapp. Committed oblivious transfer and private multi-party computation. In Don Coppersmith, editor, *Advances in Cryptology, Proceedings of CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 110–123. Springer, 1995.

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *Proceedings of FOCS 1988*, pages 42–52. IEEE Computer Society, 1988.

[CK90] Claude Crépeau and Joe Kilian. Weakening security assumptions and oblivious transfer (abstract). In Shafi Goldwasser, editor, *Advances in Cryptology, Proceedings of CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 2–7. Springer, 1990.

[CKS$^+$11] Seung Geol Choi, Jonathan Katz, Dominique Schröder, Arkady Yerukhimovich, and Hong-Sheng Zhou. (Efficient) universally composable two-party computation using a minimal number of stateless tokens. *IACR Cryptology ePrint Archive*, 2011:689, 2011.

[CMW05] Claude Crépeau, Kirill Morozov, and Stefan Wolf. Efficient unconditional oblivious transfer from almost any noisy channel. In Carlo Blundo and Stelvio Cimato, editors, *SCN 2004*, volume 3352 of *Lecture Notes in Computer Science*, pages 47–59. Springer, 2005.

[Cré88] Claude Crépeau. Equivalence between two flavours of oblivious transfers. In Carl Pomerance, editor, *Advances in Cryptology, Proceedings of CRYPTO '87*, volume 293 of *Lecture Notes in Computer Science*, pages 350–354. Springer, 1988.

[DFMS04] Ivan Damgård, Serge Fehr, Kirill Morozov, and Louis Salvail. Unfair noisy channels and oblivious transfer. In Moni Naor, editor, *Theory of Cryptography, Proceedings of TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 355–373. Springer, 2004.

[DFR$^+$07] Ivan Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In Alfred Menezes, editor, *Advances in Cryptology, Proceedings of CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 360–378. Springer, 2007.

[DKMQ11] Nico Döttling, Daniel Kraschewski, and Jörn Müller-Quade. Unconditional and composable security using a single stateful tamper-proof hardware token. In Yuval Ishai, editor, *Theory of Cryptography, Proceedings of TCC 2011*, volume 6597 of *Lecture Notes in Computer Science*, pages 164–181. Springer, 2011. Extended full version online available at `http://eprint.iacr.org/2012/135`.

[DKS99] Ivan Damgård, Joe Kilian, and Louis Salvail. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In *Advances in Cryptology, Proceedings of EUROCRYPT '99*, pages 56–73, 1999.

[GIMS10] Vipul Goyal, Yuval Ishai, Mohammad Mahmoody, and Amit Sahai. Interactive locking, zero-knowledge PCPs, and unconditional cryptography. In Tal Rabin, editor, *Advances in Cryptology, Proceedings of CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 173–190. Springer, 2010.

[GIS$^+$10] Vipul Goyal, Yuval Ishai, Amit Sahai, Ramarathnam Venkatesan, and Akshay Wadia. Founding cryptography on tamper-proof hardware tokens. In Daniele Micciancio, editor, *Theory of Cryptography, Proceedings of TCC 2010*, volume 5978 of *Lecture Notes in Computer Science*, pages 308–326. Springer, 2010.

[GKR08] Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum. One-time programs. In David Wagner, editor, *Advances in Cryptology, Proceedings of CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 39–56. Springer, 2008.

[GL91] Shafi Goldwasser and Leonid A. Levin. Fair computation of general functions in presence of immoral majority. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology, Proceedings of CRYPTO '90*, volume 537 of *Lecture Notes in Computer Science*, pages 77–93. Springer, 1991.

[HIKN08] Danny Harnik, Yuval Ishai, Eyal Kushilevitz, and Jesper Buus Nielsen. OT-combiners via secure computation. In Ran Canetti, editor, *Theory of Cryptography, Proceedings of TCC 2008*, volume 4948 of *Lecture Notes in Computer Science*, pages 393–411. Springer, 2008.

[HNRR06] Danny Harnik, Moni Naor, Omer Reingold, and Alon Rosen. Completeness in two-party secure computation: A computational view. *Journal of Cryptology*, 19(4):521–552, 2006.

[Hoe63] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963.

[IKO$^+$11] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai, and Jürg Wullschleger. Constant-rate oblivious transfer from noisy channels. In Phillip Rogaway, editor, *Advances in Cryptology, Proceedings of CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 667–684. Springer, 2011.

[IPS08] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In David Wagner, editor, *Advances in Cryptology, Proceedings of CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 572–591. Springer, 2008.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *Proceedings of STOC 1988*, pages 20–31. ACM, 1988.

[Kil91] Joe Kilian. A general completeness theorem for two-party games. In *Proceedings of STOC 1991*, pages 553–560. ACM, 1991.

[Kil00] Joe Kilian. More general completeness theorems for secure two-party computation. In *Proceedings of STOC 2000*, pages 316–324. ACM, 2000.

[KMQ10] Daniel Kraschewski and Jörn Müller-Quade. Completeness theorems with constructive proofs for finite deterministic 2-party functions (full version). *IACR Cryptology ePrint Archive*, 2010:654, 2010. Full version of [KMQ11].

[KMQ11] Daniel Kraschewski and Jörn Müller-Quade. Completeness theorems with constructive proofs for finite deterministic 2-party functions. In Yuval Ishai, editor, *Theory of Cryptography, Proceedings of TCC 2011*, volume 6597 of *Lecture Notes in Computer Science*, pages 364–381. Springer, 2011. Full version online available at `http://eprint.iacr.org/2010/654`.

[Kol10] Vladimir Kolesnikov. Truly efficient string oblivious transfer using resettable tamper-proof tokens. In Daniele Micciancio, editor, *Theory of Cryptography, Proceedings of TCC 2010*, volume 5978 of *Lecture Notes in Computer Science*, pages 327–342. Springer, 2010.

[Łoj59] Stanisław Łojasiewicz. Sur le problème de la division. *Polska Akademia Nauk. Instytut Matematyczny. Studia Mathematica*, 18:87–136, 1959.

[May95] Dominic Mayers. On the security of the quantum oblivious transfer and key distribution protocols. In Don Coppersmith, editor, *Advances in Cryptology, Proceedings of CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 124–135. Springer, 1995.

[May96] Dominic Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In Neal Koblitz, editor, *Advances in Cryptology, Proceedings of CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 343–357. Springer, 1996.

[MPR10] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. A zero-one law for cryptographic complexity with respect to computational UC security. In Tal Rabin, editor, *Advances in Cryptology, Proceedings of CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 595–612. Springer, 2010.

[MPR12] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. A unified characterization of completeness and triviality for secure function evaluation. In Steven D. Galbraith and Mridul Nandi, editors, *Progress in Cryptology, Proceedings of INDOCRYPT 2012*, volume 7668 of *Lecture Notes in Computer Science*, pages 40–59. Springer, 2012.

[MPW07] Remo Meier, Bartosz Przydatek, and Jürg Wullschleger. Robuster combiners for oblivious transfer. In Salil P. Vadhan, editor, *Theory of Cryptography, Proceedings of TCC 2007*, volume 4392 of *Lecture Notes in Computer Science*, pages 404–418. Springer, 2007.

[Rab81] Michael O. Rabin. How to exchange secrets by oblivious transfer. Technical report, Aiken Computation Laboratory, Harvard University, 1981.

[Wul07] Jürg Wullschleger. Oblivious-transfer amplification. In Moni Naor, editor, *Advances in Cryptology, Proceedings of EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 555–572. Springer, 2007.

[Wul09] Jürg Wullschleger. Oblivious transfer from weak noisy channels. In Omer Reingold, editor, *Theory of Cryptography, Proceedings of TCC 2009*, volume 5444 of *Lecture Notes in Computer Science*, pages 332–349. Springer, 2009.

[WW06] Stefan Wolf and Jürg Wullschleger. Oblivious transfer is symmetric. In Serge Vaudenay, editor, *Advances in Cryptology, Proceedings of EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 222–232. Springer, 2006.

[Yao95] Andrew Chi-Chih Yao. Security of quantum protocols against coherent measurements. In Frank Thomson Leighton and Allan Borodin, editors, *Proceedings of STOC 1995*, pages 67–75. ACM, 1995.