Concurrent Asynchronous Byzantine Agreement in Expected-Constant Rounds, Revisited

Ran Cohen* Pouyan Forghani† Juan Garay† Rutvik Patel† Vassilis Zikas‡

Abstract

It is well known that without randomization, Byzantine agreement (BA) requires a linear number of rounds in the synchronous setting, while it is flat out impossible in the asynchronous setting. The primitive which allows to bypass the above limitation is known as *oblivious common coin* (OCC). It allows parties to agree with constant probability on a random coin, where agreement is oblivious, i.e., players are not aware whether or not agreement has been achieved.

The starting point of our work is the observation that no known protocol exists for information-theoretic multi-valued OCC—i.e., OCC where the coin might take a value from a domain of cardinality larger than 2—with optimal resiliency in the asynchronous (with eventual message delivery) setting. This apparent hole in the literature is particularly problematic, as multi-valued OCC is implicitly or explicitly used in several constructions. (In fact, it is often falsely attributed to the asynchronous BA result by Canetti and Rabin [STOC '93], which, however, only achieves **binary** OCC and **does not** translate to a multi-valued OCC protocol.)

In this paper, we present the first information-theoretic multi-valued OCC protocol in the asynchronous setting with optimal resiliency, i.e., tolerating $t < n/3$ corruptions, thereby filling this important gap. Further, our protocol efficiently implements OCC with an exponential-size domain, a property which is not even achieved by known constructions in the simpler, synchronous setting.

We then turn to the problem of round-preserving parallel composition of asynchronous BA. A protocol for this task was proposed by Ben-Or and El-Yaniv [Distributed Computing '03]. Their construction, however, is flawed in several ways: For starters, it relies on multi-valued OCC instantiated by Canetti and Rabin's result (which, as mentioned above, only provides binary OCC). This shortcoming can be repaired by plugging in our above multi-valued OCC construction. However, as we show, even with this fix it remains unclear whether the protocol of Ben-Or and El-Yaniv achieves its goal of expected-constant-round parallel asynchronous BA, as the proof is incorrect. Thus, as a second contribution, we provide a simpler, more modular protocol for the above task. Finally, and as a contribution of independent interest, we provide proofs in Canetti's Universal Composability framework; this makes our work the first one offering composability guarantees, which are important as BA is a core building block of secure multi-party computation protocols.

*Efi Arazi School of Computer Science, Reichman University. E-mail: cohenran@runi.ac.il.

†Department of Computer Science and Engineering, Texas A&M University. E-mail: {pouyan.forghani,garay,rsp7}@tamu.edu.

‡Department of Computer Science, Purdue University. E-mail: vzikas@cs.purdue.edu.

Contents

1 Introduction

Byzantine agreement (BA) [PSL80, LSP82] enables n parties to reach agreement on one of their inputs in an adversarial setting, facing up to t colluding and cheating parties. The core properties require all honest parties to eventually terminate with the same output (*agreement*), which equals their input value in case they all begin with the same common input (*validity*). BA and its closely related single-sender variant, *broadcast*, are fundamental building blocks in the construction of cryptographic protocols, in particular for *secure multi-party computation* (MPC) [Yao82, GMW87, BGW88, CCD88], in which parties wish to privately compute a joint function over their inputs.

We consider a complete network of authenticated and private point-to-point (P2P) channels, which enables every pair of parties to communicate directly. The central settings in which BA has been studied are:

The *synchronous* setting. Here the protocol proceeds in a round-by-round fashion, and messages sent in a given round are guaranteed to be delivered by the start of the next round. The round structure can be achieved given synchronized clocks and a known bound on message delivery, and enables the use of *timeouts*. This clean abstraction allows for simpler analyses of protocols, but comes at the cost that parties must wait for the worst-case delay in each round before they can proceed.

The *asynchronous* setting. Here no assumptions are made on the clocks or on the bound of message delivery (other than that each message will be eventually delivered), and messages may be adversarially delayed by an arbitrary (yet finite) amount of time. The main challenge is that timeouts cannot be used, implying the inability to distinguish a slow honest party from a silent, noncooperative corrupted party. On the positive side, asynchronous protocols can advance as fast as the network allows, irrespectively of the worst-case delay, and each party can proceed to the next step as soon as it gets sufficiently many messages.

The *feasibility* of BA is inherently related to the synchrony assumptions of the system. Synchronous BA with *perfect* security is achievable with deterministic protocols if $t < n/3$ [PSL80, BGP89, GM98]; this bound is tight in the plain model[1] even when considering weaker, computational security [PSL80, FLM86, Bor96], but can be overcome with setup assumptions, yielding computationally secure BA [DS83], and even information-theoretically secure BA [PW92], for $t < n/2$.[2] On the other hand, deterministic asynchronous BA (A-BA) is impossible even facing a single crash failure [FLP85], and randomized solutions are a necessity. Following Ben-Or [Ben83] and Rabin [Rab83], information-theoretic randomized A-BA has been achieved with $t < n/3$ corruptions [Bra87, CR93, ADH08], which, as opposed to the synchronous case, is a tight bound even given setup and cryptographic assumptions [DLS88, BT85].

Round complexity of BA. In the synchronous setting, it is known that *deterministic* BA requires $t + 1$ rounds [FL82, DS83], a bound that is matched by early feasibility results [PSL80, DS83, GM98]. It is also known that t-secure randomized BA for $t = \Theta(n)$ cannot terminate in a *strict* constant number of rounds [CMS89, KY86, CPS19]; yet, *expected* constant-round protocols have been constructed both for $t < n/3$ in the plain model [FM97] and for $t < n/2$ in the PKI

[1] That is, without setup assumptions and without imposing resource restrictions on the adversary.

[2] The bound $t < n/2$ is tight for BA [Fit03]; however, under the same setup assumptions, broadcast can be solved for any number of corruptions.

model [FG03, KK09].[3] The latter protocols follow the approach of Rabin [Rab83] and rely on an *oblivious common coin* (OCC), that is, a distributed coin-tossing protocol over a domain V such that the output of every honest party is a common random value $v \in V$ with constant probability p, but with probability $1 - p$ is independently and adversarially chosen; the coin toss is "oblivious" since the parties cannot distinguish between a successful coin toss and an adversarial one.

Loosely speaking, the round complexity of asynchronous protocols is the number of times a party has to alternate between sending messages and reading messages from the network [CGHZ16]. In an unpublished manuscript, Feldman [Fel89] generalized the expected-constant-round synchronous protocol of [FM88] to asynchronous networks with $t < n/4$; at the core of the construction lies a **binary** (asynchronous) OCC protocol which actually has resiliency $\min(t', \lceil n/3 \rceil - 1)$, where t' is the corruption threshold of an *asynchronous verifiable secret sharing* (A-VSS) scheme.[4] Canetti and Rabin [CR93] constructed A-VSS for $t < n/3$, thereby obtaining A-BA in expected-constant rounds for the optimal threshold $t < n/3$.

Concurrent BA. All of the above constructions are for solving a *single* instance of BA. However, most applications, particularly MPC protocols, require composing multiple instances of BA: sequentially, in parallel, or concurrently. While the composition of synchronous, deterministic protocols is relatively simple (although care must be taken in the cryptographic setting [LLR06]), composing expected-constant-round protocols with probabilistic termination is a much more challenging task.

Indeed, Ben-Or and El-Yaniv [BE88, BE03] observed that running m instances of a probabilistic-termination protocol in parallel may incur a blow-up in the expected number of rounds until they all terminate. The technical reason is that the expectation of the maximum of m independent, identically distributed random variables does not necessarily equal the maximum of their expectations. In particular, for expected-constant-round BA with a geometric termination probability (which is the case in all known protocols), the parallel composition of m instances terminates after expected $\Theta(\log m)$ rounds [CCGZ19]. Further, even when all parties start the protocol together, simultaneous termination is not guaranteed as the adversary can force some honest parties to terminate after the others; although this gap can be reduced to a single round, inaccurate sequential re-synchronization of ℓ instances of BA may lead to an exponential blow up in ℓ if not done with care [LLR02]. Following [BE03, LLR02, LLR06, KK09], recent works have shown how to compose synchronous BA in a round-preserving way with simulation-based security in Canetti's framework for universal composability (UC) [Can20], with optimal resiliency and *perfect* security in the plain model for $t < n/3$ [CCGZ19], and with cryptographic security in the PKI model for $t < n/2$ [CCGZ21].

In the asynchronous setting, the parties are not assumed to begin the protocol at the same time, so intuitively, sequential composition is not problematic. However, running m instances of expected-constant-round A-BA concurrently would yield a $\Theta(\log m)$ blowup as in the synchronous case. Ben-Or and El-Yaniv [BE03] further showed how to execute m instances of A-BA in expected-constant rounds and with optimal resiliency $t < n/3$; however, their solution is more complicated than the synchronous one. In addition, they only prove a property-based security definition of A-BA that does not necessarily address modern security requirements such as security under composition, or facing adaptive adversaries.

[3] Fitzi and Garay [FG03] devised expected-constant-round BA for $t < n/2$ in the PKI model under number-theoretic assumptions. Katz and Koo [KK09] established a similar result from the minimal assumption of digital signatures, which yields an information-theoretic variant using pseudo-signatures [PW92].

[4] Feldman's A-VSS suffers from a negligible error probability. An *errorless* A-VSS scheme for $t < n/4$ is given in [BCG93] and used to construct a *perfectly* secure asynchronous MPC protocol with resiliency $t < n/4$.

1.1 Concurrent A-BA in Expected-Constant Rounds: Cracks in the Concrete

The underlying idea behind the synchronous protocol of Ben-Or and El-Yaniv [BE03] for parallel BA is to execute each BA instance multiple times over the same inputs, but only for a constant number of rounds. For a suitable choice of parameters, this ensures that with high probability each party will have obtained at least one output value in each such batch. To coordinate these outputs, the parties then run an *oblivious leader election* (OLE) protocol, which guarantees that with constant probability, a random leader is elected. In the event that the leader is honest and obtained an output in each batch (which, again, occurs with constant probability) the parties will terminate; otherwise they repeat the process.

The same general technique underlies Ben-Or and El-Yaniv's asynchronous protocol, but great care is needed to deal with the low message dispersion inherent in asynchronous networks while maintaining optimal resiliency $t < n/3$. A closer look at their security proof indeed raises a number of subtle issues. First, they point to [CR93] for instantiating the (asynchronous) OLE primitive used in their construction (called *A-Election()*). (Recall that Canetti and Rabin construct an OCC to obtain A-BA in expected-constant rounds; an n-valued OCC would indeed imply OLE.) As it turns out, the OCC construction in [CR93, Sec. 8] (as well as the more detailed versions [Can96, Sec. 5.7] and [CR98, Sec. 8]) is only *binary* (i.e., it only works for $V = \{0, 1\}$), and it does not seem straightforward to generalize to larger (non-constant-sized) domains. Further, running $\log n$ executions of a binary OCC in parallel to make it multi-valued yields only $1/\mathsf{poly}(n)$ probability of agreement, and as long as the coin is not *perfectly* fair (which is impossible in the asynchronous setting [dSKT22]), that would not imply OLE with constant success probability. We note that Patra *et al.* [PCR14] claim to construct a $(t + 1)$-bit asynchronous OCC, but their main focus is on communication complexity, and the agreement probability of their protocol is no better than would be obtained by running $t + 1$ executions of a binary OCC protocol (i.e., exponentially small). Techniques used to get OLE in the synchronous setting [FM88, KK09] do not seem to extend in asynchrony for $t < n/3$ (we elaborate on this in Section 1.2). Thus, to the best of our knowledge, no existing OCC construction is *simultaneously* optimally resilient, multi-valued, and asynchronous, without relying on computational assumptions (in Section 1.3 we discuss solutions in the cryptographic setting).

Second, there is a subtle issue in the logic of one of the proofs in [BE03]. This issue raises concerns about the validity of the proof claiming an expected-constant round complexity of one of the main subroutines—namely, the Π_{select} subroutine, which handles the shortcomings of their message-distribution mechanism. Specifically, in the analysis of Π_{select} it is claimed that if the leader is chosen from a certain set, the protocol will terminate. However, further examination reveals that there are scenarios in which the protocol may not terminate for certain leaders from that set. As a result, this issue casts doubt on the promised expected-constant round complexity of their concurrent A-BA protocol. (Refer to Appendix A for more details on this issue.)

Finally, the concurrent asynchronous (resp., synchronous) BA protocol in [BE03] relies on *multi-valued* asynchronous (resp., synchronous) BA in expected-constant rounds.[5] Recall that running the binary protocols in [FM97] or [CR93] $\omega(1)$ times in parallel would terminate in expected $\omega(1)$ rounds, so they cannot be naïvelyused for this task. In the synchronous setting, Turpin and Coan [TC84] extended binary BA to multi-valued BA for $t < n/3$ with an overhead of just two rounds. Ben-Or and El-Yaniv claim that this technique can be adapted for asynchronous networks by using Bracha's "A-Cast" primitive [Bra87] for message distribution. However, a closer look reveals that although the Turpin-Coan extension works (with appropriate modifications) in the

[5] This is true even if one is interested only in *binary* concurrent BA (i.e., when the input vectors consist of bits). Multi-valued BA is needed to agree on the leader's output vector.

asynchronous setting for $t < n/5$, it **provably does not work** when $t \geq n/5$, regardless of the specific choice of the underlying binary A-BA protocol and even when the adversary is limited to static corruptions (see Appendix B).

More recently, an optimally resilient multi-valued A-BA protocol with expected-constant round complexity was proposed by Patra [Pat11], but it relies on the *Agreement on a Common Subset* (ACS) protocol in [BKR94], which itself uses the concurrent A-BA protocol in [BE03]; in other words, using this approach would be **circular**. Fortunately, Mostéfaoui and Raynal [MR17] recently gave a black-box, constant-round reduction from multi-valued to binary A-BA for $t < n/3$,[6] using just one invocation of the underlying binary protocol as in [TC84].

We emphasize that the asynchronous protocol of Ben-Or and El-Yaniv [BE88, BE03] lies, either explicitly or implicitly, at the core of virtually every round-efficient asynchronous MPC construction [BCG93, BKR94, HNP05, BH07, HNP08, Coh16, CGHZ16, BZL20, LLM+20]. The concerns raised above regarding the result of [BE03] renders this extensive follow-up work unsound. In this paper, we revisit this seminal result and rectify these issues.

1.2 Overview of Our Results

We now present an overview of our results, which are three-fold, including a detailed exposition of our techniques.

Multi-valued and asynchronous oblivious common coin. As a starting point, we look at the *binary* asynchronous OCC protocol of Canetti and Rabin [CR93]. The idea (following the approach of Feldman and Micali [FM97] in the synchronous setting and [Fel89] in the asynchronous setting) is that each party secret-shares a random vote for each party, using an optimally resilient A-VSS scheme. Each party accepts $t + 1$ of the votes cast for him (at least one of which must have come from an honest party), and once it is determined that enough secrets have been fixed (based on several rounds of message exchange, using Bracha's A-Cast primitive [Bra87] for message distribution), the parties begin reconstructing the accepted votes. The sum or "tally" of these votes becomes the value associated with the corresponding party. After computing the values associated with an appropriate set of at least $n - t$ parties, an honest party outputs 0 if at least one of those tallies is 0, and outputs 1 otherwise. Note that each tally must be uniformly random, and the properties of A-Cast guarantee that no two honest parties can disagree on the value of any given tally (although up to t tallies may be "missing" in an honest party's local view); moreover, Canetti and Rabin show using a counting argument that at least $n/3$ of the tallies are known to all honest parties (i.e., common to their local views). This can be used to show that with probability at least $1/4$ all honest parties output 0, and similarly for 1.

In the conference version of Feldman and Micali's paper [FM88], there is a brief remark suggesting that the synchronous version of the above protocol can be modified to obtain (oblivious) leader election.[7] Rather than outputting a bit, parties output the index of the party whose tally is minimum; when the domain of secrets is large enough, with constant probability the same *honest* party is chosen. This approach was fully materialized by Katz and Koo [KK09] for $t < n/3$ in the information-theoretic setting and $t < n/2$ in the computational setting. We note that what is obtained is not exactly OLE as we have defined it, as the adversary can of course bias the index of the elected party, but nevertheless this is sufficient for the concurrent BA protocols of Ben-Or and

[6] They are also concerned with obtaining $O(n^2)$ message complexity. The novelty of their result, even without this more stringent requirement, does not seem to be acknowledged in the paper.

[7] This claim no longer appears in the ICALP [FM89] or journal [FM97] versions of the paper, or in Feldman's thesis [Fel88].

El-Yaniv [BE03]. Unfortunately, the same technique **cannot** be used in the asynchronous setting without giving up on optimal resiliency. The issue is that even when the globally minimum tally lies within the intersection of the honest parties' local views of the tallies, when $t < n/3$ there may be just *one* honest party whose associated tally is known to all honest parties, and thus the chosen index is likely to correspond to a corrupted party. On the other hand, the overlap increases to $5n/8$ when $t < n/4$ [Fel89].

In conclusion, no OLE construction—and therefore no concurrent A-BA protocol in expected-constant rounds—exists with optimal resiliency $t < n/3$ in asynchronous networks. We now describe our solution to this problem, which is based on the following simple combinatorial observation. If we work over a field of size $N \in \Theta(n^2)$, then with *constant* probability, at least one value will be repeated in the global view of tallies, and, moreover, all repeats will occur within the subset of indices known to all honest parties. The intuition for this fact is that when $N \in O(n^2)$ there is, due to the birthday paradox, at least one repeat in any constant fraction of the indices with constant probability, and when $N \in \Omega(n^2)$, there are no repeats at all with constant probability. There is a "sweet spot" between these extremes that can be leveraged to extract shared randomness: Honest parties output a value that is repeated in their local views of the tallies (if multiple values are repeated just take their sum, which is still uniformly random). With this modification of Canetti and Rabin's protocol [CR93], we obtain the first n^2-valued asynchronous OCC for $t < n/3$ in the information-theoretic setting. We remark that the above combinatorial observation at the heart of our construction may be of independent interest.

It is easy to generalize our OCC to work for other (larger or smaller) domains V. For example, one can work over a field of size $|V|$ (or n^2 if $|V| < n^2$), and then reduce the tallies modulo n^2 before looking for repeats. Then, instead of summing the repeated values, sum the original field elements corresponding to the indices of the repeats, reducing modulo $|V|$ if necessary. In particular, when $|V| = n$, we get an asynchronous OLE protocol with optimal resiliency.

Simplified concurrent A-BA. Ben-Or and El-Yaniv [BE03] devised an expected-constant-round concurrent A-BA protocol. However, in addition to relying on unspecified building blocks, as mentioned above, it suffers from logical issues in its proof. Although our new OCC protocol can instantiate the missing primitive, doubts remain about the expected-constant round complexity due to a lingering issue in the proof. This issue stems from the steps taken to address low message dispersion, and the possibility of resolving it without changing the protocol is unclear. To tackle this, we redesign the message-distribution phase, avoiding the problem in the proof and obtaining stronger guarantees. These guarantees simplify the protocol structure, achieving a level of simplicity comparable to the synchronous solution.

In more detail, we build on Ben-Or and El-Yaniv's work, where parties initiate multiple executions for each A-BA instance that are "truncated" after a fixed number of rounds. However, we adopt a different approach to message distribution, allowing us to establish the rest of the protocol based on the simpler structure of their synchronous solution. Similarly to [BE03], we set parameters to ensure that each party receives at least one output from each batch of truncated A-BA executions (for each instance) with constant probability. Based on their local results from those truncated A-BAs, parties create suggestions for the final output. Subsequently, the message-distribution phase begins with parties running a binary A-BA to verify a precondition, ensuring the ability to validate each other's suggestions. If they choose to proceed, they A-Cast their suggestions and only accept those they can validate using their local results from the truncated A-BAs. This validation relies on the property that honest parties terminate within two consecutive rounds in each A-BA execution, ensuring the validity of suggestions even when provided by corrupted parties. Once parties receive

$n - t$ suggestions, they proceed by A-Casting the set of the first $n - t$ suggestions they receive, along with the identity of their providers. The checked precondition guarantees that everyone can move on to the next step.

Parties then wait until they receive enough suggestions and enough sets, ensuring that at least $n - t$ sets are completely contained within the set of suggestions they received. By employing a counting argument similar to [Fel89, CR93], we can ensure the delivery of suggestions from at least $n/3$ parties to all honest participants. Moreover, the validation process applied to the suggestions guarantees that each honest party only accepts valid suggestions, even if they originate from corrupted sources. These robust guarantees in the distribution of suggested outputs establish that the $n/3$ suggestions commonly received by honest parties are legitimate outputs. This enables us to directly utilize the synchronous protocol in the asynchronous setting.

We employ our new asynchronous OCC protocol to elect a leader for party coordination. Every party adopts the leader's suggestion and runs a multi-valued A-BA to handle the obliviousness of the leader-election mechanism. If the leader is chosen from those $n/3$ commonly received suggestions, all honest parties initiate the A-BA protocol with the leader's suggestion and output the same value. If the leader is not among those $n/3$ parties, precautions are taken to ensure no malicious value is output. For this purpose, we utilize an "intrusion-tolerant" A-BA protocol that guarantees the output to be either a default value or one of the honest parties' inputs.[8] Finally, parties run a binary A-BA to determine if they have reached consensus on a non-default value and terminate.

By following the above approach, we overcome the issues in the proof and achieve a significantly simpler protocol structure for the asynchronous setting compared to the one presented in [BE03]. Somewhat surprisingly, the resulting protocol is conceptually as simple as its synchronous counterpart.

Composable treatment of expected-constant-round concurrent A-BA. We choose to work in Canetti's Universal Composability (UC) framework [Can20], and as such, we prove the security of our protocols in a *simulation-based* manner. (See Section 2.1 for a high-level overview.) The UC framework provides strong composability guarantees when secure protocols are run as a subroutine in higher-level protocols (this is absolutely critical in our context given that expected-constant-round concurrent A-BA is a key building block in many round-efficient cryptographic protocols, as mentioned above), and even in *a priori* unknown or highly adversarial environments (such as asynchronous networks). Moreover, it enables us to provide a modular, bottom-up security analysis. However, obtaining a composable and round-preserving treatment of "probabilistic-termination" BA is non-trivial, as pointed out by Cohen *et al.* [CCGZ19, CCGZ21] in the synchronous setting. In the following, we discuss some unique issues in asynchrony and how we address them.

To model eventual message delivery, we follow [KMTZ13, CGHZ16, Coh16] and require parties to repeatedly attempt fetching messages from the network. The first D such requests are ignored by the functionality, where D is a value provided by the adversary in unary so that it remains bounded by the adversary's running time (i.e., so that messages cannot be delayed *indefinitely*). It is straightforward then to derive a formal notion of asynchronous rounds in UC, based on this mechanism. We remark that unlike in the synchronous setting [KMTZ13], (asynchronous) rounds cannot be used by the environment to distinguish the real and ideal worlds in the asynchronous setting. Thus, as opposed to [CCGZ19, CCGZ21], our functionalities are round-unaware. Similarly, we do not need to deal with standard issues in sequential composition, namely, non-simultaneous

[8] Ben-Or and El-Yaniv [BE03] introduced and used a strengthened property for (A-)BA without naming it. This property was later called "non-intrusion" validity in [MR17]. Non-intrusion validity lies between standard validity and "strong" validity, as it requires that a value decided by an honest party is either an honest party's input or a special symbol $\perp$. In other words, the adversary cannot intrude malicious values into the output.

start/termination ("slack"), since asynchronous protocols are already robust to slack. Indeed, it is entirely possible that some parties receive output from a (secure) asynchronous protocol before other parties have even started the protocol!

On the other hand, the issue of *input incompleteness* is trickier to address. This refers to the problem that in the asynchronous setting, the inputs of up to t honest parties may not be considered in the result of the computation; the remaining $n - t$ parties form a "core set" of input providers. Note that in the worst case, the core set is adversarially chosen and includes all corrupted parties. Prior work [CGHZ16, Coh16] allowed the adversary to send an explicit core set to the functionality; however, this approach does not always accurately model what happens in the real world, and can cause difficulties in the simulation. Instead, our solution is to allow the adversary to define the core set *implicitly*, by delaying the submission of inputs to the functionality in the same way that it delays the release of outputs from the functionality. Using this novel modeling approach, we obtain updated functionalities for some standard asynchronous primitives that more accurately capture realizable security guarantees.

1.3 Additional Related Work

As mentioned earlier, the $t + 1$ lower bounds for deterministic BA [FL82, DS83] were extended to rule out *strict*-constant-round t-secure randomized BA for $t = \Theta(n)$ [CMS89, KY86, CPS19]; these bounds show that any such r-round BA must fail with probability at least $(c \cdot r)^{-r}$ for a constant c, a result that is matched by the protocol of [GGL22]. Cohen *et al.* [CHM+22] showed that for $t > n/3$, two-round BA are unlikely to reach agreement with constant probability, implying that the *expected* round complexity must be larger; this essentially matches Micali's BA [Mic17] that terminates in three rounds with probability 1/3. Attiya and Censor-Hillel [AC10] extended the results on worst-case round complexity for $t = \Theta(n)$ from [CMS89, KY86] to the asynchronous setting, showing that any r-round A-BA must fail with probability $1/c^r$ for some constant c.

In the dishonest-majority setting, expected-constant-round broadcast protocols were initially studied by Garay *et al.* [GKKO07], who established feasibility for $t = n/2 + O(1)$ as well as a negative result. A line of work [FN09, CPS20, WXDS20, WXSD20, SLM+23] established expected-constant-round broadcast for any constant fraction of corruptions under cryptographic assumptions.

Synchronous and (binary) asynchronous OCC protocols in the information-theoretic setting were discussed earlier. Using the synchronous protocol in [BE03], Micali and Rabin [MR90] showed how to realize a *perfectly unbiased* common coin in expected-constant rounds for $t < n/3$ over secure channels (recall that this task is impossible in asynchronous networks [dSKT22]). In the cryptographic setting, both synchronous and asynchronous OCC protocols with optimal resiliency are known, relying on various computational assumptions; we mention a few here. Beaver and So [BS93] gave two protocols tolerating $t < n/2$ corruptions in synchronous networks, which are secure under the quadratic residuosity assumption and the hardness of factoring, respectively. Cachin *et al.* [CKS05] presented two protocols for $t < n/3$ and asynchronous networks, which are secure in the random oracle model based on the RSA and Diffie-Hellman assumptions, respectively. Nielsen [Nie02] showed how to eliminate the random oracle and construct an asynchronous OCC protocol relying on standard assumptions alone (RSA and DDH). Although these constructions are for asynchronous networks, they can be readily extended to work in synchronous networks for $t < n/2$ (i.e., so that they can be used in the computationally secure BA protocol from [FG03]). We also note that while the resiliency bounds for asynchronous OCC protocols coincide in the information-theoretic and computational settings, working in the latter typically yields expected-constant-round A-BA protocols that are much more efficient in terms of communication complexity (i.e., *interaction*) than the unconditionally secure protocol of Canetti and Rabin [CR93].

Lastly, we discuss solutions to multi-valued A-BA in the computational setting. Cachin *et al.* [CKPS01] studied a more general version of this problem, in which the validity property is replaced with "external" validity, where the output domain can be arbitrarily large but the agreed-upon value must only satisfy an application-specific predicate. They gave a construction for multi-valued "validated" A-BA that runs in expected-constant rounds for $t < n/3$, assuming a PKI and a number of threshold cryptographic primitives (including an asynchronous OCC), and used it to obtain an efficient protocol for asynchronous *atomic* broadcast. Recently, Abraham *et al.* [AMS19] (and follow-ups, e.g., [LLTW20, AJM+21, GLL+22]) have improved the communication complexity. The work of Fitzi and Garay [FG03] also considered *strong* (A-)BA. Here we require "strong" validity: the common output must have been one of the honest parties' inputs (note that this is equivalent to standard validity in the binary case). When the size of the input domain is $m > 2$, neither a Turpin-Coan-style reduction [TC84] nor the obvious approach of running $\log m$ parallel executions of a binary protocol would suffice to realize this stronger notion of agreement; indeed, Fitzi and Garay showed that strong A-BA is possible if and only if $t < n/(m+1)$. This bound holds in both the information-theoretic and computational settings. Their unconditionally secure asynchronous protocol actually involves oblivious coin flipping on the domain, but $m > 2$ forces $t < n/4$ and the binary asynchronous OCC protocols in [Fel89, CR93] can be extended to multi-valued in this regime, as discussed in Section 1.2.

1.4 Organization of the Paper

The rest of the paper is organized as follows. We start in Section 2 with some preliminaries, including a brief overview of the UC framework. In Section 3, we discuss our model in greater depth, formally specifying the asynchronous primitives we use as building blocks and motivating our novel modeling choices along the way. Section 4 contains our multi-valued asynchronous OCC construction with optimal resiliency $t < n/3$, and its security proof. Finally, in Section 5 we present the impactful result that our OCC construction enables: a simplified and sound protocol for concurrent A-BA in expected-constant rounds. Appendix A contains our attack on the asynchronous construction in [BE03] (along with the required background material), and Appendix B demonstrates that an asynchronous version of the binary to multi-valued BA extension in [TC84] works **if and only if** $t < n/5$.

2 Model and Preliminaries

We will use $[m]$ to denote the set $\{1, \ldots, m\}$. Our protocols often use dynamically growing sets S; when $|S| \geq k$, we denote by $S^{(k)} \subseteq S$ the set containing the first k elements that were added to S. We also denote by $\mathbb{F}$ the field from which the protocols' messages come. Our statements (in particular, the ones about statistical security) assume an (often implicit) security parameter κ which is assumed to be linear in $\max\{\log |\mathbb{F}|, n\}$.

We write our protocols using a series of numbered steps. The interpretation is that a party repeatedly goes through them in sequential order, attempting each instruction. Of course, in the asynchronous setting, the necessary precondition for carrying out an instruction might only be met much later in the protocol, and furthermore messages may be delayed. We discuss the latter below, in Section 2.2. Regarding the former, we frequently use statements of the form "Wait until [condition]. Then, [instruction]," which is to be executed at most once, or "If [condition], then [instruction]," which can be executed multiple times.

2.1 UC Basics

We prove our constructions secure in the UC framework [Can20] and we briefly summarize it here. Protocol machines, ideal functionalities, the adversary, and the environment are all modeled as interactive Turing machine (ITM) instances, or ITIs. An execution of protocol Π consists of a series of activations of ITIs, starting with the environment $\mathcal{Z}$ who provides inputs to and collects outputs from the parties and the adversary $\mathcal{A}$; parties can also give input to and collect output from sub-parties (e.g., hybrid functionalities), and $\mathcal{A}$ can communicate with parties via "backdoor" messages. Although parties can send messages to one another, $\mathcal{A}$ is responsible for delivering them, making this model *completely* asynchronous (see Section 2.2 for the way we capture eventual-delivery channels). Protocol instances are delineated using a unique session identifier (SID).

Corruption of parties is modeled by a special `corrupt` message sent from $\mathcal{A}$ to the party; upon receipt of this message, the party sends its entire local state to $\mathcal{A}$, and in all future activations follows the instructions of $\mathcal{A}$. Note that a party P_i can only be corrupted once $\mathcal{A}$ receives a special (`corrupt` P_i) input from $\mathcal{Z}$. We emphasize, however, that corruptions can occur at any point during the protocol (i.e., $\mathcal{A}$ is assumed to be adaptive). Denote by $\text{EXEC}_{\Pi,\mathcal{A},\mathcal{Z}}$ the probability distribution ensemble corresponding to the (binary) output of $\mathcal{Z}$ at the end of an execution of Π with adversary $\mathcal{A}$.

The ideal-world process for functionality $\mathcal{F}$ is simply defined as an execution of the ideal protocol $\text{IDEAL}_{\mathcal{F}}$, in which the so-called "dummy" parties just forward inputs from $\mathcal{Z}$ to $\mathcal{F}$ and forward outputs from $\mathcal{F}$ to $\mathcal{Z}$ (in particular, the dummy parties do not communicate with the adversary, but rather the adversary is expected to send backdoor messages directly to $\mathcal{F}$, including corruption requests). Our functionalities implicitly respond to corruption requests in the standard way (e.g., all previous inputs of the newly corrupted party are leaked, and the adversary has the option to replace its output); we refer to [Can20] for further details. The adversary in the ideal world is also called the *simulator* and denoted $\mathcal{S}$; the corresponding ensemble is denoted by $\text{IDEAL}_{\mathcal{F},\mathcal{S},\mathcal{Z}}$.

We are interested in unconditional (aka information-theoretic) security. Thus, we say that a protocol Π (statistically) *UC-realizes* an ideal functionality $\mathcal{F}$ if for any computationally unbounded adversary $\mathcal{A}$, there exists a simulator $\mathcal{S}$ (which is polynomial in the complexity of $\mathcal{A}$), such that for any computationally unbounded environment $\mathcal{Z}$, we have $\text{EXEC}_{\Pi,\mathcal{A},\mathcal{Z}} \approx \text{IDEAL}_{\mathcal{F},\mathcal{S},\mathcal{Z}}$. In case the distribution ensembles are perfectly indistinguishable we say that Π UC-realizes $\mathcal{F}$ with *perfect* security.

When Π is a $(\mathcal{G}_1,\ldots,\mathcal{G}_n)$-hybrid protocol (i.e., making subroutine calls to $\text{IDEAL}_{\mathcal{G}_1},\ldots,\text{IDEAL}_{\mathcal{G}_n}$), we say that Π UC-realizes $\mathcal{F}$ in the $(\mathcal{G}_1,\ldots,\mathcal{G}_n)$-hybrid model.

2.2 Modeling Eventual Message Delivery in UC

As mentioned above, the base communication model in UC is completely unprotected. To capture asynchronous networks with eventual message delivery, we work in a hybrid model with access to the multi-use *asynchronous secure message transmission* functionality $\mathcal{F}_{\mathsf{a\text{-}smt}}$ shown in Figure 1, which was introduced in [CGHZ16] and is itself based on the (single-use) *eventual-delivery secure channel* functionality $\mathcal{F}_{\mathsf{ed\text{-}sec}}$ from [KMTZ13].

The functionality $\mathcal{F}_{\mathsf{a\text{-}smt}}$ models a *secure* eventual-delivery channel between a sender P_s and receiver P_r.[9] To reflect the adversary's ability to delay the message by an arbitrary finite duration (even when P_s and P_r are not corrupted), the functionality operates in a "pull" mode, managing a message buffer M and a counter D that represents the current message delay. This counter is decremented every time P_r tries to fetch a message, which is ultimately sent once the counter

[9] Recall that while (concurrent) A-BA is not a private task, secure channels are needed to construct an OCC.

Functionality $\mathcal{F}_{\text{a-smt}}$

The functionality proceeds as follows. At the first activation, verify that $\mathsf{sid} = (P_s, P_r, \mathsf{sid}')$, where P_s and P_r are player identities. Initialize the current delay $D := 0$ and the message buffer $M := (\texttt{eom})$, where $\texttt{eom}$ is a special "end-of-messages" symbol.

- Upon receiving $(\texttt{send}, \mathsf{sid}, m)$ from P_s, update $D := D + 1$ and $M := (m, \mathsf{mid}) \parallel M$ (i.e., insert (m, mid) at the beginning of M), where mid is a unique message ID, and send $(\texttt{leakage}, \mathsf{sid}, \mathsf{mid})$ to the adversary.
- Upon receiving $(\texttt{delay}, \mathsf{sid}, T)$ from the adversary for $T \in \mathbb{Z}$ represented in unary notation, update $D := \max(1, D + T)$ and send $(\texttt{delay-set}, \mathsf{sid})$ to the adversary.
- Upon receiving $(\texttt{fetch}, \mathsf{sid})$ from P_r, do:
  1. Update $D := \max(0, D - 1)$ and send $(\texttt{fetched}, \mathsf{sid})$ to the adversary.
  2. If $D = 0$ and $M = ((m_1, \mathsf{mid}_1), \ldots, (m_l, \mathsf{mid}_l), \texttt{eom})$, then update $M := ((m_2, \mathsf{mid}_2), \ldots, (m_l, \mathsf{mid}_l), \texttt{eom})$ and send $(\texttt{output}, \mathsf{sid}, m_1)$ to P_r.
- Upon receiving $(\texttt{permute}, \mathsf{sid}, \pi)$ from the adversary, if $M = ((m_1, \mathsf{mid}_1), \ldots, (m_l, \mathsf{mid}_l), \texttt{eom})$ and π is a permutation over $[l]$, then update $M := ((m_{\pi(1)}, \mathsf{mid}_{\pi(1)}), \ldots, (m_{\pi(l)}, \mathsf{mid}_{\pi(l)}), \texttt{eom})$.
- (Adaptive Message Replacement) Upon receiving $(\texttt{replace}, \mathsf{sid}, ((m_1, \mathsf{mid}_1), \ldots, (m_{l'}, \mathsf{mid}_{l'})), T')$ from the adversary: If P_s is corrupted, $D > 0$, and T' is a valid delay, then update $M := ((m_1, \mathsf{mid}_1), \ldots, (m_{l'}, \mathsf{mid}_{l'}), \texttt{eom})$ and $D := \max(1, T')$.

Figure 1: The asynchronous secure message transmission functionality.

hits 0. The adversary can at any time provide an additional integer delay T, and if it wishes to immediately release the messages, it needs only to submit a large negative value. It is important to note that T must be encoded in unary; this ensures that the delay, while arbitrary, remains bounded by the adversary's computational resources or running time.[10] Also, note that $\mathcal{F}_{\text{a-smt}}$ guarantees eventual message delivery assuming that the environment gives sufficient resources to the protocol, i.e., activates P_r sufficiently many times. We additionally allow the adversary to permute the messages in the buffer; see [CGHZ16] for a discussion.

Since $\mathcal{F}_{\text{a-smt}}$ (and our other asynchronous functionalities) may not provide output immediately, we must clarify what we mean when instructing a party to fetch the output from multiple instances of a hybrid (e.g., one per party), as repeatedly attempting to fetch from the first instance before continuing to the second instance might not make any progress. Accordingly, we require that parties fetch the output in a "round-robin fashion" across activations (i.e., after attempting to fetch from each instance, the party moves on to try the remaining steps in the protocol). It is implicit that the party stops making fetch requests to any given instance after it receives an output from that instance (of course, this behavior can be easily implemented using flags).

Finally, we note that while the UC framework has no notion of time, and we are in the asynchronous setting (with eventual message delivery) where parties may proceed at different rates, one can still formally define a notion of asynchronous rounds along the lines of [CGHZ16], which will be referred to in our statements. In a nutshell, the round complexity of asynchronous protocols is the number of times a party has to alternate between sending messages and reading messages from the network.

3 Ideal Functionalities for a Few Standard Primitives

In this section, we present ideal functionalities for asynchronous primitives used in our constructions. This seemingly simple task requires careful consideration of certain aspects, as the adversary's abil-

[10] We refer to [Can20] for a formal definition of running time in the UC framework.

ity to delay messages in the network has an upstream impact on the achievable security guarantees of distributed tasks. In particular, the adversary can obstruct the output release procedure and impede honest parties' participation. To model *delayed output release*, we extend the mechanism discussed in Section 2.2 (using per-party delay counters). However, to model *delayed participation*, we introduce a novel and more natural approach that addresses limitations of prior work and more closely captures the effects of asynchrony. We start by discussing in Section 3.1 our design choices for the latter, and proceed to describe a few ideal functionalities in Section 3.2.

3.1 Modeling Delayed Participation

In the asynchronous setting, it is impossible for an honest party to distinguish whether uncooperative parties are corrupted and intentionally withholding messages, or if they are honest parties whose messages have been delayed. Consequently, when the number of corruptions is upper-bounded by t, waiting for the participation of the last t parties can result in an indefinite wait. In ideal functionalities, this translates to expecting participation and/or input only from a subset of adversarially chosen parties, known as the "core set," with a size of $n-t$. Observe that the value of t is closely related to the behavior of the functionality. In this work, we specifically consider optimal resiliency, where $t = \lceil \frac{n}{3} \rceil - 1$. However, our functionalities can be easily adapted to accommodate other resiliency bounds.

In our modeling approach, the adversary implicitly determines the core set by strategically delaying participation (or input submission) to the functionality. If we instruct the ideal functionality to proceed once $n - t$ parties have participated, the adversary can precisely determine the core set by manipulating the order of participation (or input submissions). To accommodate arbitrary but finite delays for input submissions, we employ a technique similar to the one we use for the output-release mechanism. That is, in addition to a per-party *output delay counter*, there is an *input delay counter* (updatable by the adversary) which is decremented every time the party pings the functionality; once the counter reaches zero, the party is allowed to participate.

This approach contrasts with the work of Cohen [Coh16] and Coretti *et al.* [CGHZ16], wherein the adversary (simulator) **explicitly** sends a core set to the functionality. Obtaining the core set from the adversary all at once does not accurately mimic real-world executions and requires careful consideration to ensure the implementation works in all scenarios. For instance, a challenging case to model is when the simulator sets the core set, but the environment never activates some parties in that core set. If not handled properly, this situation can lead to either the ideal functionality stalling indefinitely while the real-world execution proceeds, or allowing for core sets of smaller sizes, neither of which is acceptable.

There are other aspects of modeling the core set that can potentially cause issues. If the simulator is required to set the core set early on, it may encounter issues during the simulation because in some real-world protocols, such as the asynchronous MPC protocol of Ben-Or *et al.* [BKR94], the core set is not fixed in the early stages of the execution. Similarly, if the functionality allows late submission of the core set, then when using the functionality as a hybrid, the adversary can potentially stall the functionality unless appropriate preventive mechanisms are in place. In contrast, implicitly defining the core set by delaying parties' participation aligns more closely with real-world executions, reducing the probability of errors. Additionally, it can potentially simplify the simulation process, as the simulator can gradually define the core set as the protocol progresses.

3.2 Ideal Functionalities for a Few Standard Primitives

We now cast a few standard asynchronous primitives as UC functionalities, following our novel modeling approach. We also present security statements showing how classical protocols can be used to realize these primitives.

Asynchronous Broadcast (A-Cast). The first essential primitive used in both our OCC and concurrent A-BA protocols, which also finds numerous applications in other asynchronous protocols, is *Bracha's Asynchronous Broadcast* (A-Cast) [Bra87]. A-Cast enables a distinguished sender to distribute its input, such that if an honest party outputs a value, then all honest parties must (eventually) output the same value. Moreover, if the sender is honest, then all honest parties must (eventually) output the sender's input. While these are essentially the agreement and validity properties required from regular (synchronous) broadcast, we stress that honest parties may not terminate when the sender is corrupted. We formulate A-Cast as the ideal functionality $\mathcal{F}_{\mathsf{a\text{-}cast}}$, shown in Figure 2.

Functionality $\mathcal{F}_{\mathsf{a\text{-}cast}}$

The functionality proceeds as follows. Start a session once a message of the form $(\texttt{send}, \mathsf{sid}, \cdot)$ with $\mathsf{sid} = (\mathcal{P}, P_s, \mathsf{sid}')$ is received from (the sender) $P_s \in \mathcal{P}$, where $\mathcal{P}$ is a player set of size n. For each $P_i \in \mathcal{P}$, initialize $\mathsf{participated}_i := 0$ and delay values $D_i^{\text{input}} = D_i^{\text{output}} := 1$. Also initialize y to a default value $\perp$ and $t := \lceil \frac{n}{3} \rceil - 1$.

- Upon receiving $(\texttt{delay}, \mathsf{sid}, P_i, \mathsf{type}, D)$ from the adversary for $P_i \in \mathcal{P}$, $\mathsf{type} \in \{\text{input}, \text{output}\}$, and $D \in \mathbb{Z}$ represented in unary notation, update $D_i^{\mathsf{type}} := \max(1, D_i^{\mathsf{type}} + D)$ and send $(\texttt{delay-set}, \mathsf{sid})$ to the adversary.
- Upon receiving $(\texttt{send}, \mathsf{sid}, v)$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i) run the Input Submission Procedure, and if $P_i = P_s$ then record $y := v$ and send $(\texttt{leakage}, \mathsf{sid}, P_s, v)$ to the adversary; else send $(\texttt{fetched}, \mathsf{sid}, P_i)$ to the adversary.
- Upon receiving $(\texttt{replace}, \mathsf{sid}, v)$ from the adversary (v can be $\perp$), if P_s is corrupted and no party has received their output yet, then update $y := v$.
- Upon receiving $(\texttt{fetch}, \mathsf{sid})$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i) run the Input Submission and Output Release Procedures, and send $(\texttt{fetched}, \mathsf{sid}, P_i)$ to the adversary and any messages set by the Output Release Procedure to P_i.

Input Submission Procedure: If $\mathsf{participated}_i = 0$ and $(\texttt{send}, \mathsf{sid}, v)$ was already received from P_i, then do:

1. Update $D_i^{\text{input}} := D_i^{\text{input}} - 1$.
2. If $D_i^{\text{input}} = 0$ then set $\mathsf{participated}_i := 1$.

Output Release Procedure: If $\sum_{j=1}^{n} \mathsf{participated}_j \geq n - t$ and $y \neq \perp$, then do:

1. Update $D_i^{\text{output}} := D_i^{\text{output}} - 1$.
2. If $D_i^{\text{output}} = 0$ then set $(\texttt{output}, \mathsf{sid}, y)$ to be sent to P_i.

Figure 2: The A-Cast functionality.

Note that although A-Cast is a single-sender primitive, assuming it can proceed to the output generation phase without sufficient participation from other parties is too idealized. A realizable functionality should only proceed to the output generation phase when $n - t$ parties (which may include the sender) have participated. Parties demonstrate their participation by sending (dummy) input messages, followed by issuing fetch requests to the functionality. An important technicality here is that the participation of parties before the sender initiates the session should not contribute to the count. Therefore, $\mathcal{F}_{\mathsf{a\text{-}cast}}$ starts a session only once the input from the sender is received. Consequently, any efforts for participation before that point will not be taken into account. An implication of this design choice when using $\mathcal{F}_{\mathsf{a\text{-}cast}}$ as a hybrid is that parties other than the sender

will not know when the session has started. As a result, they should constantly switch between sending input messages and fetch requests until they receive the output.

Bracha's asynchronous broadcast protocol [Bra87] can be used to UC-realize $\mathcal{F}_{\mathsf{a\text{-}cast}}$ with perfect security. We formally state this result in the following proposition, whose proof is straightforward.

Proposition 1. *$\mathcal{F}_{\mathsf{a\text{-}cast}}$ can be UC-realized with perfect security in the $\mathcal{F}_{\mathsf{a\text{-}smt}}$-hybrid model, in constant rounds and against an adaptive and malicious t-adversary, provided $t < \frac{n}{3}$.*

Asynchronous Verifiable Secret Sharing (A-VSS). Another crucial primitive we require, mainly for our OCC protocol, is *Asynchronous Verifiable Secret Sharing* (A-VSS). A-VSS allows a dealer to secret-share a value among all parties, ensuring that no unauthorized subset of colluding parties can learn any information about the secret. However, any authorized subset of parties should be able to efficiently reconstruct the secret using their shares. The term "verifiable" reflects that the dealer cannot cheat, for example by causing the reconstruction to fail or by inducing inconsistent output values from honest parties. In particular, whenever the sharing phase succeeds, any authorized subset of parties should be able to efficiently complete the reconstruction phase, and all honest parties doing so must recover the same secret. Moreover, if the dealer is honest, the sharing phase must always succeed, and everyone should recover the value originally shared by the dealer. In our context, we consider only the threshold access structure, where a subset of parties can recover the secret if and only if it contains at least 1/3 of the parties. The formulation of A-VSS as an ideal functionality, $\mathcal{F}_{\mathsf{a\text{-}vss}}$, is shown in Figure 3. We denote this as the "plain" A-VSS functionality, as it does not allow homomorphic computation over shares; nonetheless, this basic functionality suffices for obtaining concurrent A-BA in expected-constant rounds.

A-VSS, being a single-sender primitive, also requires the participation of at least $n - t$ parties to be realizable. We adopt a similar approach to $\mathcal{F}_{\mathsf{a\text{-}cast}}$ in modeling this requirement. Parties other than the dealer demonstrate their participation by sending (dummy) input messages and issuing fetch requests, ensuring that the minimum participation threshold is met for the A-VSS protocol to proceed. Also, it is important to note that $\mathcal{F}_{\mathsf{a\text{-}vss}}$ only initiates a session once it receives the first input from the dealer. Any participation efforts made before that point are not taken into account.

The A-VSS protocol given by Canetti and Rabin in [CR93] can be used to UC-realize $\mathcal{F}_{\mathsf{a\text{-}vss}}$ with statistical security for $t < n/3$. This result is formally stated in the following proposition. It is worth noting that perfectly secure A-VSS is impossible for $t \geq n/4$ [BKR94].

Proposition 2. *For any finite field $\mathbb{F}$ (with $|\mathbb{F}| > n$), $\mathcal{F}^{\mathbb{F}}_{\mathsf{a\text{-}vss}}$ can be UC-realized with statistical security, in constant rounds and in the $\mathcal{F}_{\mathsf{a\text{-}smt}}$-hybrid model against an adaptive and malicious t-adversary, provided $t < \frac{n}{3}$.*

Asynchronous Byzantine Agreement (A-BA). We use A-BA for both binary and multi-valued domains V in our revised concurrent A-BA protocol. In this primitive, each party P_i has an input $v_i \in V$. The goal is for all parties to output the same value, such that if $n-2t$ input values are the same, that value is chosen as the output; otherwise, the adversary determines the output. We initially consider *corruption-unfair* A-BA, where the adversary learns the input of each party the moment it is provided. Corruption fairness, as introduced in [HZ10] and later coined in [CGZ23], essentially ensures that the (adaptive) adversary cannot corrupt a party and subsequently influence the input value of that party based on the original input value. It is worth noting that corruption-fair A-BA can easily be defined by avoiding leaking honest parties' inputs before the output is generated. We formulate A-BA as the ideal functionality $\mathcal{F}_{\mathsf{a\text{-}ba}}$, shown in Figure 4.

The functionality $\mathcal{F}_{\mathsf{a\text{-}ba}}$ encompasses an additional property known as "non-intrusion" validity (see Section 1.2). In a nutshell, this property guarantees that no malicious value can be present in

Functionality $\mathcal{F}_{\mathsf{a\text{-}vss}}^{V}$

The functionality is parameterized by a set V of possible secrets and proceeds as follows. Start a session once a message of the form $(\texttt{share}, \mathsf{sid}, v)$ with $\mathsf{sid} = (\mathcal{P}, P_d, \mathsf{sid}')$ and $v \in V$ is received from (the dealer) $P_d \in \mathcal{P}$, where $\mathcal{P}$ is a player set of size n. For each $P_i \in \mathcal{P}$, initialize $\mathsf{phase}_i := \text{share}$, $\mathsf{participated}_{i,\text{share}} = \mathsf{participated}_{i,\text{rec}} := 0$, and current delay values $D_i^{\text{share,input}} = D_i^{\text{share,output}} = D_i^{\text{rec,input}} = D_i^{\text{rec,output}} := 1$. Also initialize secret to a default value $\perp$ and $t := \lceil \frac{n}{3} \rceil - 1$.

- Upon receiving $(\texttt{delay}, \mathsf{sid}, P_i, \mathsf{phase}, \mathsf{type}, D)$ from the adversary for $P_i \in \mathcal{P}$, $\mathsf{phase} \in \{\text{share}, \text{rec}\}$, $\mathsf{type} \in \{\text{input}, \text{output}\}$, and $D \in \mathbb{Z}$ represented in unary notation, update $D_i^{\mathsf{phase,type}} := \max(1, D_i^{\mathsf{phase,type}} + D)$ and send $(\texttt{delay-set}, \mathsf{sid})$ to the adversary.
- Upon receiving $(\texttt{share}, \mathsf{sid}, v)$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i) run the Input Submission Procedure, and if $P_i = P_d$ and $v \in V$, then record $\mathsf{secret} := v$ and send $(\texttt{leakage}, \mathsf{sid}, P_d, |\mathsf{secret}|)$ to the adversary; else send $(\texttt{fetched}, \mathsf{sid}, P_i)$ to the adversary.
- Upon receiving $(\texttt{replace}, \mathsf{sid}, s)$ from the adversary, if P_d is corrupted, $s \in V \cup \{\perp\}$, and no honest party has received $(\texttt{shared}, \mathsf{sid})$ yet, then update $\mathsf{secret} := s$.
- Upon receiving $(\texttt{rec}, \mathsf{sid}, v)$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i) run the Input Submission Procedure, and if $\sum_{j=1}^{n} \mathsf{participated}_{j,\text{rec}} \geq n - t$ then send $(\texttt{leakage}, \mathsf{sid}, P_i, \mathsf{secret})$ to the adversary; else send $(\texttt{fetched}, \mathsf{sid}, P_i)$ to the adversary.
- Upon receiving $(\texttt{fetch}, \mathsf{sid})$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i) run the Input Submission and Output Release Procedures, and send $(\texttt{fetched}, \mathsf{sid}, P_i)$ to the adversary and any messages set by the Output Release Procedure to P_i.

Input Submission Procedure: If $\mathsf{participated}_{i,\mathsf{phase}_i} = 0$ and $(\mathsf{phase}_i, \mathsf{sid}, v)$ was already received from P_i, then do:

1. Update $D_i^{\mathsf{phase}_i,\text{input}} := D_i^{\mathsf{phase}_i,\text{input}} - 1$.
2. If $D_i^{\mathsf{phase}_i,\text{input}} = 0$, set $\mathsf{participated}_{i,\mathsf{phase}_i} := 1$.

Output Release Procedure: If $\sum_{j=1}^{n} \mathsf{participated}_{j,\mathsf{phase}_i} \geq n - t \wedge (\mathsf{phase}_i \neq \text{rec} \vee \mathsf{secret} \neq \perp)$ then do:

1. Update $D_i^{\mathsf{phase}_i,\text{output}} := D_i^{\mathsf{phase}_i,\text{output}} - 1$.
2. If $D_i^{\mathsf{phase}_i,\text{output}} = 0$, then if $\mathsf{phase}_i = \text{share}$, set $(\texttt{shared}, \mathsf{sid})$ to be sent to P_i and update $\mathsf{phase}_i := \text{rec}$; otherwise, set $(\texttt{opened}, \mathsf{sid}, \mathsf{secret})$ to be sent to P_i.

Figure 3: The plain A-VSS functionality.

the output. In other words, the output must be either an honest party's input or a default value $\perp$. This stronger notion of A-BA is vital for the security of our concurrent A-BA protocol.

The expected-constant-round binary A-BA protocol of Canetti and Rabin [CR93] can be used to UC-realize $\mathcal{F}_{\mathsf{a\text{-}ba}}^{V}$ with statistical security for binary domains ($|V| = 2$) and $t < n/3$. However, our concurrent A-BA protocol (and the one in [BE03]) require **multi-valued** A-BA, where $|V|$ is not constant (in fact, exponential), in expected-constant rounds. Ben-Or and El-Yaniv [BE03] claim that the constant-round reduction of multi-valued to binary BA proposed by Turpin and Coan [TC84], which works in the synchronous setting for $t < n/3$, can be extended to work in the asynchronous setting by using A-Cast for message distribution. However, we demonstrate that the asynchronous version of this reduction works if and only if $t < n/6$, even when using A-Cast and considering a static adversary (see Appendix B for details). Some additional modifications can improve this bound to $t < n/5$, but achieving optimal resiliency is not straightforward.

More recently, Mostéfaoui and Raynal [MR17] presented a constant-round transformation from binary to multi-valued A-BA that works for $t < n/3$. Furthermore, the resulting protocol satisfies the non-intrusion validity property mentioned above. By applying this transformation to the binary A-BA protocol of Canetti and Rabin [CR93], we can UC-realize $\mathcal{F}_{\mathsf{a\text{-}ba}}^{V}$ for arbitrary V with statistical security:

Functionality $\mathcal{F}_{\mathsf{a\text{-}ba}}^{V}$

The functionality is parameterized by a set V of values and proceeds as follows. At the first activation, verify that $\mathsf{sid} = (\mathcal{P}, \mathsf{sid}')$, where $\mathcal{P}$ is a player set of size n. For each $P_i \in \mathcal{P}$, initialize v_i to a default value $\perp$, $\mathsf{participated}_i := 0$, and delay values $D_i^{\text{input}} = D_i^{\text{output}} := 1$. Also initialize y to $\perp'$, a to $\perp$, and $t := \lceil \frac{n}{3} \rceil - 1$.

- Upon receiving $(\texttt{delay}, \mathsf{sid}, P_i, \mathsf{type}, D)$ from the adversary for $P_i \in \mathcal{P}$, $\mathsf{type} \in \{\text{input}, \text{output}\}$, and $D \in \mathbb{Z}$ represented in unary notation, update $D_i^{\mathsf{type}} := \max(1, D_i^{\mathsf{type}} + D)$ and send $(\texttt{delay-set}, \mathsf{sid})$ to the adversary.
- Upon receiving $(\texttt{input}, \mathsf{sid}, v)$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i), run the Input Submission Procedure and send $(\texttt{leakage}, \mathsf{sid}, P_i, v)$ to the adversary.
- Upon receiving $(\texttt{replace}, \mathsf{sid}, v)$ from the adversary, record $a := v$.
- Upon receiving $(\texttt{fetch}, \mathsf{sid})$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i) run the Input Submission and Output Release Procedures, and send $(\texttt{fetched}, \mathsf{sid}, P_i)$ to the adversary and any messages set by the Output Release Procedure to P_i.

Input Submission Procedure: If $\mathsf{participated}_i = 0$ and $(\texttt{input}, \mathsf{sid}, v)$ was already received from P_i, then do:

1. Update $D_i^{\text{input}} := D_i^{\text{input}} - 1$.
2. If $D_i^{\text{input}} = 0$, then set $\mathsf{participated}_i := 1$ and record $v_i := v$.

Output Release Procedure: If $\sum_{j=1}^{n} \mathsf{participated}_j \geq n - t$ then do:

1. Update $D_i^{\text{output}} := D_i^{\text{output}} - 1$.
2. If $D_i^{\text{output}} = 0$, if $y = \perp'$ then set $y := x$ if there exists $x \in V$ such that $x = v_k$ for at least $n - 2t$ input values v_k; else if $a = \perp$ or $a \in V$ was provided by at least one honest party, then set $y := a$; else set $y := \perp$. Additionally, set $(\texttt{output}, \mathsf{sid}, y)$ to be sent to P_i.

Figure 4: The intrusion-tolerant A-BA functionality.

Proposition 3. *For any domain V, $\mathcal{F}_{\mathsf{a\text{-}ba}}^{V}$ can be UC-realized with statistical security in the $\mathcal{F}_{\mathsf{a\text{-}smt}}$-hybrid model, in expected-constant rounds and against an adaptive and malicious t-adversary, provided $t < \frac{n}{3}$.*

4 Asynchronous Oblivious Common Coin

Oblivious Common Coin (OCC) is a crucial primitive, particularly in the asynchronous setting. As discussed in the Introduction, achieving even binary A-BA against a single fail-stop corruption becomes impossible without the use of randomization [FLP85], emphasizing the importance of randomization in the asynchronous setting. The OCC primitive allows parties to collectively agree on a random value with a constant probability. This property opens up possibilities for various higher-level asynchronous protocols, as OCC can potentially serve as the building block that provides the necessary randomization. To illustrate its significance, in the case of binary values, OCC enables binary A-BA in expected-constant rounds [Rab83], and when extended to domains with a size equal to the number of participants, it can be used for Oblivious Leader Election (OLE) and sets the stage for expected-constant-round concurrent BA in both synchronous and asynchronous networks [BE03]. Refer to Section 5 for a formal definition of asynchronous OLE (A-OLE) and its application toward expected-constant-round concurrent A-BA.

As highlighted in the Introduction, none of the existing OCC proposals is simultaneously information-theoretic, asynchronous, multi-valued, and optimally resilient. Furthermore, no straightforward adaptation of the existing schemes yields an OCC with all the aforementioned properties. In Section 4.1, we first formulate (multi-valued) OCC as an ideal functionality in the asynchronous setting with eventual delivery. Subsequently, in Section 4.2, we propose our own OCC protocol that aims to satisfy all the aforementioned properties. In Section 4.3, we provide

proof demonstrating that our protocol runs in constant time and UC-realizes the (multi-valued) OCC functionality with perfect security, even against an adaptive and malicious adversary who corrupts fewer than 1/3 of the parties in the asynchronous setting.

At a high level, our protocol is based on the binary OCC of Feldman [Fel89] and Canetti and Rabin [CR93], and incorporates a novel combinatorial technique derived from our observation stated in Lemma 4 below. By leveraging this lemma, we unveil interesting and powerful properties of the local views formed during the protocol's execution, leading to enhanced extraction capabilities. In fact, instead of extracting a single bit, by choosing appropriate parameters we can extract random values from any arbitrary domain still with a constant probability.

4.1 A-OCC Ideal Functionality

An oblivious common coin is parameterized by a set V and some constant probability p. Each party starts with an empty input λ and every party P_i outputs a value from V where with at least probability $p > 0$ every party output the same uniformly random value $x \in V$ and with probability $1 - p$ the adversary chooses each party's output.[11]

A natural translation of the above goal to a UC functionality is as follows: Initially, the functionality samples a "fairness bit" $b \leftarrow \text{Bernoulli}(p)$ and a value $y \xleftarrow{R} [m]$. Then, if $b = 1$ or no meaningful input from the adversary is received it outputs the same random value y to every party. However, if $b = 0$ and meaningful input is received from the adversary, it assigns each party the value provided by the adversary. The ideal functionality also informs the adversary about the fairness bit b and the random value once they have been sampled. Furthermore, the handling of asynchronous aspects, including delayed output release and participation, is discussed in Section 3.

Unfortunately, it is unclear if the above functionality can be realized by our protocol via an efficient straight-line simulator. The intuitive reason is that the simulator needs to come up with a view that is distributed according to the protocol view while inducing the above distribution on b (and matching the b received from the OCC functionality). To resolve this issue, we embed a sampling procedure in our OCC functionality that allows the simulator to choose (part of the) randomness, but only in a way that does not tweak the distribution of b.[12] The resulting functionality is described in Figure 5.

4.2 The A-OCC Protocol

We proceed to present our asynchronous and multi-valued OCC protocol. We begin by discussing all the essential building blocks employed in our protocol. Subsequently, we provide a high-level overview of the protocol, highlighting its key ideas, followed by a detailed description.

Building blocks. The basic building blocks of our A-OCC protocol are A-VSS and A-Cast. A-VSS enables parties to contribute by privately providing their local randomness and only revealing this randomness when the contributions to the output are determined. A-VSS ensures the secrecy and verifiability of the shared secrets in an asynchronous setting. The A-VSS primitive is formally modeled as the ideal functionality $\mathcal{F}_{\mathsf{a\text{-}vss}}$ in Figure 3. On the other hand, A-Cast facilitates communication among parties by providing stronger guarantees than simple message distribution. This is especially crucial in asynchronous settings where challenges such as low message dispersion can

[11] It is important to note that the term "oblivious" in this context refers to the fact that parties do not learn whether an agreement on a random coin value has been achieved or not, while the adversary does.

[12] For readers familiar with simulation issues in UC, this is an analogue to the need for a key-setup functionality to receive coins from its simulator so that it enables simulation.

Functionality $\mathcal{F}_{\text{a-occ}}^{V}$

The functionality is parameterized by a set V of possible outcomes and it proceeds as follows. At the first activation, verify that $\mathsf{sid} = (\mathcal{P}, \mathsf{sid}')$, where $\mathcal{P}$ is a player set of size n. For each $P_i \in \mathcal{P}$, initialize y_i to a default value $\perp$, $\mathsf{participated}_i := 0$, and delay values $D_i^{\text{input}} = D_i^{\text{output}} := 1$. Also initialize a, y, and b to $\perp$, the set S to $[\lceil \frac{n}{3} \rceil]$, and $t := \lceil \frac{n}{3} \rceil - 1$. Additionally, let $m = \text{lcm}(n^2, |V|)$ and sample $(w_1, \ldots, w_n) \xleftarrow{R} [m]^n$.

- Upon receiving $(\texttt{delay}, \mathsf{sid}, P_i, \mathsf{type}, D)$ from the adversary for $P_i \in \mathcal{P}$, $\mathsf{type} \in \{\text{input}, \text{output}\}$, and $D \in \mathbb{Z}$ represented in unary notation, update $D_i^{\mathsf{type}} := \max(1, D_i^{\mathsf{type}} + D)$ and send $(\texttt{delay-set}, \mathsf{sid})$ to the adversary.
- Upon receiving $(\texttt{set}, \mathsf{sid}, A)$ from the adversary for the first time, if $|A| \geq \frac{n}{3}$ record $S := A$ and send $(\texttt{vector}, \mathsf{sid}, (w_1, \ldots, w_n))$ to the adversary.
- Upon receiving $(\texttt{input}, \mathsf{sid})$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i), run the Input Submission Procedure and send $(\texttt{leakage}, \mathsf{sid}, P_i)$ to the adversary.
- Upon receiving $(\texttt{replace}, \mathsf{sid}, v)$ from the adversary, record $a := v$.
- Upon receiving $(\texttt{fetch}, \mathsf{sid})$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i) run the Input Submission and Output Release Procedures, and send $(\texttt{fetched}, \mathsf{sid}, P_i)$ to the adversary and any messages set by the Output Release Procedure to P_i.

Input Submission Procedure: If $\mathsf{participated}_i = 0$ and $(\texttt{input}, \mathsf{sid})$ was already received from P_i, then do:

1. Update $D_i^{\text{input}} := D_i^{\text{input}} - 1$.
2. If $D_i^{\text{input}} = 0$ then set $\mathsf{participated}_i := 1$.

Output Release Procedure: If $\sum_{j=1}^{n} \mathsf{participated}_j \geq n - t$ then do:

1. Update $D_i^{\text{output}} := D_i^{\text{output}} - 1$.
2. If $D_i^{\text{output}} = 0$, if $b = \perp$ then for each $j \in [n]$, calculate $w'_j := w_j \bmod n^2$ and form a set I that includes j and k if and only if $w'_j = w'_k$ and $j \neq k$. Then, set the "fairness bit" $b := 1$ if $I \subseteq S$ and $I \neq \emptyset$; otherwise set $b := 0$. Additionally, set $y := \Sigma_{j \in I} w_j \bmod |V|$ (if $I = \emptyset$ then set $y := \perp$), and do the following:
   - If $b = 1$ or a cannot be parsed as $(a_1, \ldots, a_n) \in (V \cup \{\perp\})^n$, set $y_j := y$ for each $P_j \in \mathcal{P}$.
   - If $b = 0$ and a can be parsed as $(a_1, \ldots, a_n) \in (V \cup \{\perp\})^n$, set $y_j := a_j$ for each $P_j \in \mathcal{P}$.

   Additionally, set $(\texttt{output}, \mathsf{sid}, y_i)$ to be sent to P_i.

Figure 5: The asynchronous OCC functionality.

occur. A-Cast helps overcoming these challenges and ensures reliable message dissemination among the parties. A-Cast is provided in the ideal functionality $\mathcal{F}_{\mathsf{a\text{-}cast}}$ in Figure 2.

The protocol. As previously mentioned, our multi-valued protocol is built upon the existing binary OCC [Fel89, CR93] and introduces a novel combinatorial technique for extracting values from arbitrary domains. In both the binary protocol and our proposed protocol, each party secret-shares n random elements from a field. It can be observed that at some point during the protocol execution, a vector of length n consisting of random elements from the same field is established (with up to t missing values due to asynchrony). For each coordinate of this vector, random elements shared by $t + 1$ parties are utilized to prevent the adversary, controlling up to t parties, from biasing any specific coordinate. Subsequently, each party starts reconstructing secrets shared by other parties to form the same vector locally. In the asynchronous setting, due to the low dispersion of messages, not all coordinates can be reconstructed by honest parties. This can result in different parties reconstructing different subsets of coordinates. However, by utilizing mechanisms to improve message dispersion, as demonstrated by Feldman [Fel89], it has been proven that when $t \leq n/3$, while the local vectors of honest parties may have up to t missing coordinates, they have an overlap

of size at least $n/3$.[13] This is significant because when allowing for t missing components when $n = 3t + 1$, the overlap of local vectors of even four parties could be empty.

Traditionally, existing protocols extract a single bit from the local views of the random vector by instructing parties to take all existing coordinates modulo n and output 0 if any coordinate is 0 or output 1 otherwise. In contrast, our protocol represents a significant improvement by going beyond the extraction of a single bit from the local views of the random vector. This enhanced randomness extraction is through a combinatorial observation regarding vectors of random values, as formulated in Lemma 4. This observation, allows parties to agree non-interactively on certain coordinates of the random vector with a constant probability, while also ensuring that these agreed-upon coordinates lie within their overlap section. They can then compute the sum of all distinct values among those coordinates to generate the output.

Another important observation regarding existing binary A-OCC protocols is the lack of a proper termination mechanism. This poses significant challenges as network delays can cause parties to operate out of sync. In such cases, some parties may receive the output before completing their role in the execution, and if they stop, others may not be able to generate the output at all. This directly affects the simulator's ability to accurately simulate the protocol, especially in managing input and output delays in the ideal functionality. This is mainly because, unlike the protocol, the ideal functionality ensures that once a party receives the output, sufficient participation has occurred, and any other party, regardless of others' participation, can fetch the output if sufficiently activated. One potential solution could be invoking A-BA on the output at the end; however, this would create a circular dependency since A-OCC itself is used in A-BA. Instead, we chose to adopt a simpler approach inspired by Bracha's termination mechanism. This approach resolves the participation issue without causing deadlocks and ensures agreement once all parties initiate the procedure with the same value. The formal description of our asynchronous OCC protocol $\Pi_{\mathsf{a\text{-}occ}}$ appears in Figure 6.

Here, we aim to highlight a technical aspect concerning the descriptions of our protocols. The $\mathcal{F}_{\mathsf{a\text{-}cast}}$ and $\mathcal{F}_{\mathsf{a\text{-}vss}}$ functionalities incorporate the requirement for non-sender/non-dealer parties to send (dummy) input messages, demonstrating their participation in the input phase. These functionalities can generate an output only when $n - t$ parties, including the main sender, participate in the input phase. However, the participation of parties is considered only upon receipt of the input message from the main sender or the dealer (refer to Section 3 for further elaboration).

When employing these ideal functionalities as hybrids, it becomes challenging for parties to determine when the main input provider initiates the session, ensuring their participation is duly accounted for. As a result, we implement a strategy wherein the party alternates between sending the input message and the fetch message each time it is instructed to fetch the output.

This approach is employed in our protocols, including $\Pi_{\mathsf{a\text{-}occ}}$. To clarify further, the term "fetch X from $\mathcal{F}_{\mathsf{y}}$" implies that the party continually switches between sending the relevant input message for X and the fetch message to $\mathcal{F}_{\mathsf{y}}$ whenever is asked to fetch during the execution.

4.3 Security Proof

After describing our A-OCC protocol, we proceed to present and prove the formal security statement that demonstrates how our A-OCC protocol UC-realizes $\mathcal{F}_{\mathsf{a\text{-}occ}}$. Next, we prove a combinatorial observation regarding vectors of random values. Finally, we utilize this combinatorial observation

[13] Feldman [Fel89] calculated the size of the overlap, denoted as x, based on the number of participants n and the maximum number of corruptions t. The general relation is $x \geq n - t - \frac{t^2}{n-2t}$, which yields $x \geq n/3$ and $x \geq 5n/8$ when $t \leq n/3$ and $t \leq n/4$, respectively.

Protocol $\Pi^V_{\mathsf{a\text{-}occ}}$

The protocol is parameterized by a set V of possible outcomes. Let $m = \mathrm{lcm}(n^2, |V|)$.

- Upon receiving input $(\mathtt{input}, \mathsf{sid})$ from the environment, where $\mathsf{sid} = (\mathcal{P}, \mathsf{sid}')$ for a player set $\mathcal{P}$ of size n, and its following activations, party $P_i \in \mathcal{P}$ proceeds as follows.
  1. Initialize sets C_i, G_i, Z_i, and R_i to $\emptyset$, flag $\mathsf{finished}$ to 0, and variable y_i to $\perp$. Also initialize $C'_j := \perp$, $G'_j := \perp$, $b_{j,k} := 0$, $r_{k,j} := \perp$, $v_j := \perp$, and $z'_j := \perp$ for all $j, k \in [n]$.
  2. For each $j \in [n]$, choose $x_{i,j} \xleftarrow{\mathrm{R}} [m]$ and send $(\mathtt{share}, \mathsf{sid}_i^{\mathrm{share},j}, x_{i,j})$ to an instance of $\mathcal{F}^{\mathbb{F}}_{\mathsf{a\text{-}vss}}$ ($\mathbb{F}$ is the smallest prime field with size at least m) with SID $\mathsf{sid}_i^{\mathrm{share},j} := (\mathcal{P}, P_i, \mathsf{sid}', \mathtt{share}, j)$.
- Upon later activations from the environment, if $\mathsf{finished} = 0$ then do:
  1. For each $j, k \in [n]$ such that $b_{j,k} = 0$, in a round-robin fashion (across activations) fetch the share from the instance of $\mathcal{F}^{\mathbb{F}}_{\mathsf{a\text{-}vss}}$ with SID $\mathsf{sid}_j^{\mathrm{share},k}$. Upon receiving back $(\mathtt{shared}, \mathsf{sid}_j^{\mathrm{share},k})$ set $b_{j,k} := 1$, and if $b_{j,l} = 1$ for all $l \in [n]$ then update $C_i := C_i \cup \{P_j\}$.
  2. Wait until $|C_i| \geq t{+}1$. Then, send $(\mathtt{send}, \mathsf{sid}_i^{\mathrm{attach}}, C_i^{(t+1)})$ to an instance of $\mathcal{F}_{\mathsf{a\text{-}cast}}$ with SID $\mathsf{sid}_i^{\mathrm{attach}} := (\mathcal{P}, P_i, \mathsf{sid}', \mathtt{attach})$.
  3. For each $j \in [n]$ such that $C'_j = \perp$, in a round-robin fashion fetch the output from the instance of $\mathcal{F}_{\mathsf{a\text{-}cast}}$ with SID $\mathsf{sid}_j^{\mathrm{attach}}$. Upon receiving back $(\mathtt{output}, \mathsf{sid}_j^{\mathrm{attach}}, Y)$, record $C'_j := Y$, and if $C'_j \subseteq C_i$ then update $G_i := G_i \cup \{P_j\}$. Additionally, for each party newly added to C_i, repeat the last part for any previously received C'_j if $P_j \notin G_i$.
  4. Wait until $|G_i| \geq n{-}t$. Then, send $(\mathtt{send}, \mathsf{sid}_i^{\mathrm{ready}}, G_i^{(n-t)})$ to an instance of $\mathcal{F}_{\mathsf{a\text{-}cast}}$ with SID $\mathsf{sid}_i^{\mathrm{ready}} := (\mathcal{P}, P_i, \mathsf{sid}', \mathtt{ready})$.
  5. For each $j \in [n]$ such that $G'_j = \perp$, in a round-robin fashion fetch the output from the instance of $\mathcal{F}_{\mathsf{a\text{-}cast}}$ with SID $\mathsf{sid}_j^{\mathrm{ready}}$. Upon receiving back $(\mathtt{output}, \mathsf{sid}_j^{\mathrm{ready}}, Y)$, record $G'_j := Y$, and if $G'_j \subseteq G_i$ then update $R_i := R_i \cup \{P_j\}$; once $|R_i| \geq n - t$ record $Z_i := G_i$. Additionally, for each newly added party to G_i, repeat the last part for any previously received G'_j if $P_j \notin R_i$.
  6. If $|R_i| \geq n - t$, then for each $P_k \in C'_j$ such that $P_j \in G_i$ and $r_{k,j} = \perp$, in a round-robin fashion fetch the secret from the instance of $\mathcal{F}^{\mathbb{F}}_{\mathsf{a\text{-}vss}}$ with SID $\mathsf{sid}_k^{\mathrm{share},j}$. Upon receiving back $(\mathtt{opened}, \mathsf{sid}_k^{\mathrm{share},j}, s)$, record $r_{k,j} := s$, and if $r_{l,j} \neq \perp$ for all $P_l \in C'_j$ then set $v_j := \sum_{P_l \in C'_j} r_{l,j} \bmod m$.
  7. Wait until $v_j \neq \perp$ for all $P_j \in Z_i$. Then, for each $v_j \neq \perp$, calculate $v'_j := v_j \bmod n^2$ and form a set I that includes j and k if and only if $v'_j = v'_k$ and $j \neq k$. Then, set $z_i := \Sigma_{j \in I} v_j \bmod |V|$ (if $I = \emptyset$ then set z_i to be an arbitrary value from V) and send $(\mathtt{send}, \mathsf{sid}_i^{\mathrm{term}}, z_i)$ to an instance of $\mathcal{F}_{\mathsf{a\text{-}cast}}$ with SID $\mathsf{sid}_i^{\mathrm{term}} := (\mathcal{P}, P_i, \mathsf{sid}', \mathtt{term})$.
  8. For each $j \in [n]$ such that $z'_j = \perp$, in a round-robin fashion fetch the output from the instance of $\mathcal{F}_{\mathsf{a\text{-}cast}}$ with SID $\mathsf{sid}_j^{\mathrm{term}}$. Upon receiving back $(\mathtt{output}, \mathsf{sid}_j^{\mathrm{term}}, x)$ record $z'_j := x$. Continue this process until for $n - t$ different indices $k \in [n]$ we have $z'_k \neq \perp$. Once this condition is satisfied, set $\mathsf{finished} := 1$ and y_i to the mode (most repeated value) among the received (non-default) z'_k values for $k \in [n]$.
- Upon receiving input $(\mathtt{fetch}, \mathsf{sid})$ from the environment, if $\mathsf{finished} = 1$ then output $(\mathtt{output}, \mathsf{sid}, y_i)$ to the environment.

Figure 6: The multi-valued asynchronous OCC protocol.

to argue that the sampling procedure embedded in $\mathcal{F}_{\mathsf{a\text{-}occ}}$, which receives parts of its randomness from the adversary, results in a uniformly random common coin with a constant probability.

Theorem 1. *For any integer domain V, protocol $\Pi^V_{\mathsf{a\text{-}occ}}$ UC-realizes $\mathcal{F}^V_{\mathsf{a\text{-}occ}}$ with perfect security in the $(\mathcal{F}_{\mathsf{a\text{-}cast}}, \mathcal{F}^{\mathbb{F}}_{\mathsf{a\text{-}vss}})$-hybrid model where $\mathbb{F}$ is the smallest prime field of size at least $\mathrm{lcm}(|V|, n^2)$, in constant rounds and in the presence of an adaptive and malicious t-adversary, provided $t < \frac{n}{3}$.*

Proof. Let $\mathcal{A}$ be an adversary in the real world. We construct a simulator $\mathcal{S}$ in the ideal world, such that no environment $\mathcal{Z}$ can distinguish whether it is interacting with $\Pi^V_{\mathsf{a\text{-}occ}}$ and $\mathcal{A}$, or with

$\mathcal{F}_{\mathsf{a\text{-}occ}}^{V}$ and $\mathcal{S}$.

The simulator internally runs a copy of $\mathcal{A}$, and plays the roles of $\mathcal{F}_{\mathsf{a\text{-}cast}}$, $\mathcal{F}_{\mathsf{a\text{-}vss}}^{\mathbb{F}}$, and the parties in a simulated execution of the protocol. All inputs from $\mathcal{Z}$ are forwarded to $\mathcal{A}$, and all outputs from $\mathcal{A}$ are forwarded to $\mathcal{Z}$. Moreover, whenever $\mathcal{A}$ corrupts a party in the simulation, $\mathcal{S}$ corrupts the same party in the ideal world by interacting with $\mathcal{F}_{\mathsf{a\text{-}occ}}^{V}$, and if the corruption was direct (i.e., not via either of the aiding functionalities), then $\mathcal{S}$ sends $\mathcal{A}$ the party's state and thereafter follows $\mathcal{A}$'s instructions for that party. Moreover, $\mathcal{S}$ manages delays in the ideal functionality based on the delays that $\mathcal{A}$ sets on the hybrids.

The simulated execution begins when $\mathcal{S}$ receives the message $(\texttt{leakage}, \mathsf{sid}, P_i)$ from $\mathcal{F}_{\mathsf{a\text{-}occ}}$. During the internal execution, $\mathcal{S}$ simulates $\mathcal{F}_{\mathsf{a\text{-}cast}}$ honestly. As for $\mathcal{F}_{\mathsf{a\text{-}vss}}^{\mathbb{F}}$, $\mathcal{S}$ simulates the sharing phase without explicitly assigning any random secrets to honest parties. The actual values of these secrets will be determined by $\mathcal{S}$ later in order to ensure that the output matches that of $\mathcal{F}_{\mathsf{a\text{-}occ}}$, while maintaining indistinguishability between the real and ideal world views.

By employing the same counting argument as in [Fel89, CR93], we can demonstrate that once the first honest party P_i reaches the stage where $|R_i| = n - t$, a subset A of indices, with a size of at least $\frac{n}{3}$, becomes fixed such that all the honest parties could eventually recover all the tallies in $\{v_j \mid j \in A\}$.

Once the first honest party P_i reaches the condition $|R_i| = n - t$, the simulator $\mathcal{S}$, being aware of message delivery, can easily determine the set A and send $(\texttt{set}, \mathsf{sid}, A)$ to $\mathcal{F}_{\mathsf{a\text{-}occ}}$. Basically, parties whose messages appear in at least $t + 1$ of the sets G'_j received by P_i from the set A (for more details, refer to the counting argument in [CR93]). Since A is a valid set of indices with a size of at least $\frac{n}{3}$, $\mathcal{F}_{\mathsf{a\text{-}occ}}$ will respond with a random vector $(w_1, \ldots, w_n) \in [m]^n$. At this point, $\mathcal{S}$ can initiate the opening of secrets through the reconstruction phase of $\mathcal{F}_{\mathsf{a\text{-}vss}}$ in such a way that if an honest party recovers the k^{th} tally v_k, it will correspond to $v_k = w_k$. This can be achieved because each tally is composed of secrets from $t + 1$ parties that must include some honest parties. By adjusting the secret of honest parties, $\mathcal{S}$ ensures that the tally adds up to the desired value. Importantly, opening the tallies to match the uniformly random vector $(w_1, \ldots, w_n)$ received from $\mathcal{F}_{\mathsf{a\text{-}occ}}$ is indistinguishable from the real-world execution. In the real-world execution, secrets from $t + 1$ parties, which must include at least one honest party, contribute to each tally. Since honest parties independently and uniformly choose their secrets, and the set of contributors is fixed before revealing secrets and the same for all parties (can be shown using properties of A-Cast), each tally will eventually open to a uniformly random value, exactly matching the vector $(w_1, \ldots, w_n)$.

Correctness. To ensure that the approach generates the correct output in the simulated execution, we need to consider two cases.

First, let us assume that there are repeats among the tallies $(w_1, \ldots, w_n)$, and all of these repeats lie within the set A. In this scenario, all honest parties observe all the repeats since all of them can recover all the tallies in A. Consequently, all the honest parties extract the same random value from the repeats, which then will serve as the final output. This is due to the fact that any set of $n-t$ parties contains a majority of honest parties. Therefore, the output of any honest party, which is determined by taking the mode of the $n - t$ extracted values they received via $\mathcal{F}_{\mathsf{a\text{-}cast}}$, will be equal to r. Furthermore, since there are no repeats outside of A, the ideal functionality, which performs the same extraction procedure on the entire vector $(w_1, \ldots, w_n)$ (rather than on local views), will also output the exact same value r.

Second, let us consider the case where there are no repeats or the repeats are not entirely contained within A. In this situation, $\mathcal{F}_{\mathsf{a\text{-}occ}}$ sets the fairness bit $b := 0$, indicating the possibility of adversarial influence on the output. The simulator $\mathcal{S}$, who observes the simulated execution, can

seize this opportunity and exert influence to ensure that the output of $\mathcal{F}_{\mathsf{a\text{-}occ}}$ matches the output of the simulated execution. This ensures that the output in the simulated execution matches the output of $\mathcal{F}_{\mathsf{a\text{-}occ}}$ while maintaining the indistinguishability of the real and ideal worlds.

Termination. To ensure the termination of the protocol and maintain the indistinguishability of the real and ideal worlds, we need to demonstrate that the protocol will eventually terminate.

When an honest party P_i has $P_h \in C_i$, then any honest party P_j will also have $P_h \in C_j$ which means that eventually $C_i \subseteq C_j$. This is because once an honest party receives a $(\texttt{shared}, \mathsf{sid})$ message from $\mathcal{F}_{\mathsf{a\text{-}vss}}$, all other honest parties will eventually receive it as well. Therefore, for any pair of honest parties P_i and P_j, we can eventually observe $C_i^{(t+1)} \subseteq C_j$. As a result, every honest party P_i will pass the threshold $|G_i| \geq n - t$ and A-Cast $G_i^{(n-t)}$.

Now, if an honest party P_i has $P_h \in G_i^{(n-t)}$, it means that $C'_h \subseteq C_i$. As mentioned earlier, for any pair of honest parties P_i and P_j, we eventually have $C_i \subseteq C_j$, which indicates that eventually $C'_h \subseteq C_j$. Therefore, any $P_h \in G_i^{(n-t)}$ will eventually be in G_j, leading to $G'_i \subseteq G_j$. This implies that for any honest party P_i, R_i will eventually contain all the honest parties.

Consequently, for any honest party P_i, the condition $|R_i| \geq n - t$ will eventually be satisfied, allowing them to proceed to the reconstruction phase of $\mathcal{F}_{\mathsf{a\text{-}vss}}$. Since all honest parties will eventually start the reconstruction phase, they will receive the necessary secrets and can generate the output without encountering any deadlocks.

In summary, the protocol $\Pi_{\mathsf{a\text{-}occ}}$ ensures termination by guaranteeing that each honest party eventually satisfies the required thresholds and proceeds to the necessary phases of $\mathcal{F}_{\mathsf{a\text{-}vss}}$. This guarantees the eventual output generation without any deadlocks, preserving the perfect indistinguishability of the real and ideal worlds.

We claim that the overall round complexity of the protocol $\Pi_{\mathsf{a\text{-}occ}}$ is constant. The protocol consists of a constant number of steps, each involving constant-round operations. The constant round complexity of the protocol $\Pi_{\mathsf{a\text{-}occ}}$ is achieved by utilizing underlying building blocks such as $\mathcal{F}_{\mathsf{a\text{-}cast}}$ and $\mathcal{F}_{\mathsf{a\text{-}vss}}$. By ensuring that these building blocks have constant-round realizations, we are able to preserve the overall constant round complexity of the protocol $\Pi_{\mathsf{a\text{-}occ}}$ even after replacing $\mathcal{F}_{\mathsf{a\text{-}cast}}$ and $\mathcal{F}_{\mathsf{a\text{-}vss}}$ with actual protocols realizing them.

We can conclude that, the execution of $\Pi^V_{\mathsf{a\text{-}occ}}$ with $\mathcal{A}$ and $\mathcal{F}^V_{\mathsf{a\text{-}occ}}$ with $\mathcal{S}$ are perfectly indistinguishable to any environment $\mathcal{Z}$. This ensures that $\Pi^V_{\mathsf{a\text{-}occ}}$ UC-realizes $\mathcal{F}^V_{\mathsf{a\text{-}occ}}$ with perfect security. □

Lemma 4. *Let V be a vector of n values chosen independently and uniformly at random from a set S of size $N \in \Theta(n^2)$, and let α be a constant satisfying $0 < \alpha \leq 1$. Then for any subset of indices $I \subseteq [n]$ such that $|I| \geq \alpha n$, with constant probability p there is at least one repeated value in V; moreover, all of the repeated values are constrained to the indices in I.*

Proof. It suffices to consider the case $|I| = \lceil \alpha n \rceil$. We first define the following events. Denote by V_J the restriction of V to the indices in $J \subseteq [n]$.

E_V :	At least two components of V have the same value
E_{V_I} :	At least two components of V_I have the same value
$E_{V_{I^c}}$:	At least two components of V_{I^c} have the same value
$E_{(V_I, V_{I^c})}$:	At least one component of V_I has the same value as a component of V_{I^c}

We now compute

$$
\begin{aligned}
p &= \Pr[E_{V_I} \cap E^{\mathsf{c}}_{V_{I^{\mathsf{c}}}} \cap E^{\mathsf{c}}_{(V_I,V_{I^{\mathsf{c}}})}] \\
&= \Pr[E_{V_I} \mid E^{\mathsf{c}}_{V_{I^{\mathsf{c}}}} \cap E^{\mathsf{c}}_{(V_I,V_{I^{\mathsf{c}}})}] \Pr[E^{\mathsf{c}}_{V_{I^{\mathsf{c}}}} \cap E^{\mathsf{c}}_{(V_I,V_{I^{\mathsf{c}}})}] \\
&\geq \Pr[E_{V_I} \mid E^{\mathsf{c}}_{V_{I^{\mathsf{c}}}} \cap E^{\mathsf{c}}_{(V_I,V_{I^{\mathsf{c}}})}] \Pr[E^{\mathsf{c}}_{V}] && (E^{\mathsf{c}}_{V} \subseteq E^{\mathsf{c}}_{V_{I^{\mathsf{c}}}} \cap E^{\mathsf{c}}_{(V_I,V_{I^{\mathsf{c}}})}) \\
&= \left(1 - \Pr[E^{\mathsf{c}}_{V_I} \mid E^{\mathsf{c}}_{V_{I^{\mathsf{c}}}} \cap E^{\mathsf{c}}_{(V_I,V_{I^{\mathsf{c}}})}]\right) \Pr[E^{\mathsf{c}}_{V}] \\
&= \left(1 - \prod_{i=0}^{\lceil \alpha n \rceil - 1} \left(1 - \frac{(n - \lceil \alpha n \rceil) + i}{N}\right)\right) \left(\prod_{i=0}^{n-1} \left(1 - \frac{i}{N}\right)\right) \\
&\geq \left(1 - \prod_{i=0}^{\lceil \alpha n \rceil - 1} \left(1 - \frac{i}{N}\right)\right) \left(\prod_{i=0}^{n-1} \left(1 - \frac{i}{N}\right)\right) && (n - \lceil \alpha n \rceil \geq 0) \\
&\approx \left(1 - \prod_{i=0}^{\lceil \alpha n \rceil - 1} e^{-\frac{i}{N}}\right) \left(\prod_{i=0}^{n-1} e^{-\frac{i}{N}}\right) && \left(\frac{n-1}{N} \ll 1 \text{ implies } 1 - \frac{i}{N} \approx e^{-\frac{i}{N}}\right) \\
&= \left(1 - e^{-\frac{1}{N}\sum_{i=0}^{\lceil \alpha n \rceil - 1} i}\right) \left(e^{-\frac{1}{N}\sum_{i=0}^{n-1} i}\right) \\
&= \left(1 - e^{-\frac{\lceil \alpha n \rceil^2 - \lceil \alpha n \rceil}{2N}}\right) \left(e^{-\frac{n^2-n}{2N}}\right) \\
&\in \Theta(1). && (\text{since } N \in \Theta(n^2))
\end{aligned}
$$

□

Remark 5. In the ideal functionality $\mathcal{F}_{\mathsf{a\text{-}occ}}$, a vector $(w_1, \ldots, w_n)$ of independent and uniformly random elements from $[m]^n$, where $m = \mathrm{lcm}(n^2, |V|)$, is chosen. Since m is a multiple of n^2, taking $(w_1, \ldots, w_n)$ modulo n^2 gives us $(w'_1, \ldots, w'_n)$, which are still independent and uniformly random over the range $[n^2]$. Additionally, the adversarially selected set S, with a size of $\frac{n}{3}$, has to be fixed before the random vector is leaked. This ensures that S is independent of the vector $(w'_1, \ldots, w'_n)$. Now, since $(w'_1, \ldots, w'_n)$ is a vector of n values independently and uniformly chosen from the set $[n^2]$, and $S \subseteq [n]$ is a set of indices with a size of $\frac{n}{3}$, Lemma 4 guarantees that with a constant probability, there is at least one repeated value in $(w'_1, \ldots, w'_n)$. Furthermore, all the repeated values are constrained to the indices in S. This implies that $\mathcal{F}_{\mathsf{a\text{-}occ}}$ sets the fairness bit $b := 1$ with a constant probability, indicating that no adversarial influence on the output is accepted. Moreover, once $b = 1$, it means that there is at least one repeated value in $(w'_1, \ldots, w'_n)$, which implies $I \neq \emptyset$. In this case, $\mathcal{F}_{\mathsf{a\text{-}occ}}$ outputs $y := \sum_{j \in I} w_j \bmod |V|$, which is a uniformly random value over the set $|V|$. This holds because the w_i's are randomly and independently chosen from $[m]$ and m is a multiple of $|V|$.

5 Concurrent A-BA in Expected-Constant Rounds

Concurrent A-BA plays a significant role in existing asynchronous MPC protocols, including those described in [BCG93, BKR94, HNP05, BH07, HNP08, Coh16, CGHZ16, BZL20, LLM+20]. Its primary purpose is to address the lack of coordination among the parties, which is amplified in the asynchronous setting. Specifically, it enables parties to reach agreement on a common subset of input providers (the "core set" [BCG93]). This capability is essential in various applications within asynchronous networks, where the different delays experienced by each party can lead to discrepancies in their respective views.

In this section, we dive into the important problem of achieving concurrent A-BA in an expected-constant number of rounds. As discussed in the Introduction, Ben-Or and El-Yaniv [BE03] high-

lighted the potential issue of running multiple executions of a probabilistic-termination protocol in parallel, which could lead to an increase in the expected number of rounds required for *all* executions to terminate. The concurrent A-BA protocol proposed in [BE03] relies on A-OLE and multi-valued A-BA, both of which can be instantiated using our A-OCC protocol from Section 4 and the A-BA protocol from [MR17], respectively. However, during our analysis, we identified certain issues in their analysis that cast doubt on the expected-constant round complexity of one of their main building blocks and, consequently, their concurrent A-BA protocol. For a more comprehensive presentation of these issues, see Appendix A. It is unclear how to address these issues without modifying the protocol itself.

To rectify these concerns, we modify the underlying message distribution mechanism and incorporate an additional layer of message validation. These changes not only resolve the identified issues, but also significantly simplify the protocol. It is worth emphasizing that our revised concurrent A-BA protocol achieves a level of simplicity that is comparable to the synchronous version proposed in [BE03]. This accomplishment is significant because when designing an asynchronous counterpart to a synchronous protocol, achieving a level of simplicity on par with the synchronous version is often considered the ideal outcome. In the following, we present an ideal functionality for concurrent A-BA, describe our protocol and its required building blocks, and provide a security proof.

5.1 Concurrent A-BA Ideal Functionality

Concurrent A-BA, as the name suggests, refers to a primitive that enables parties to solve N instances of A-BA concurrently. We are primarily interested in the case $N = n$, corresponding to the emulation of an ideal A-BA primitive, but we study the more general version. In this setting, each party P_i initiates the concurrent A-BA by providing N values, namely $v_{i,1}, \ldots, v_{i,N}$. Subsequently, all parties receive the same set of N output values, denoted as $y_1, \ldots, y_N$. Each individual output value y_j is computed based on the input values $v_{1,j}, \ldots, v_{n,j}$, following the prescribed procedure outlined in the standard A-BA primitive. Specifically, if $n - 2t$ input values are identical, that common value is selected as the output; otherwise, the output is determined by the adversary. We capture the task of concurrent A-BA using the ideal functionality $\mathcal{F}_{\mathsf{conc\text{-}a\text{-}ba}}$, shown in Figure 7.

5.2 The Simplified Concurrent A-BA Protocol

Building blocks. Our concurrent A-BA protocol relies on A-Cast as the fundamental communication primitive due to its enhanced guarantees compared to basic message distribution mechanisms. The ideal functionality $\mathcal{F}_{\mathsf{a\text{-}cast}}$, which models the A-Cast primitive, was given in Figure 2.

As another crucial building block, our protocol incorporates asynchronous oblivious leader election (A-OLE) as a coordination mechanism among the parties. A-OLE enables parties to randomly elect a leader from among themselves. The term "oblivious" indicates that parties are unaware of whether an agreement on a random leader has occurred or not. In our concurrent A-BA protocol, similar to the approach described in [BE03], there comes a point where all parties suggest outputs, and A-OLE assists them in reaching an agreement by adopting the suggestion of the elected leader. To capture the functionality of A-OLE, we parameterize the A-OCC functionality $\mathcal{F}_{\mathsf{a\text{-}occ}}$ (Figure 5) by a domain with a size equal to the number of parties. This yields an ideal functionality for A-OLE, denoted as $\mathcal{F}_{\mathsf{a\text{-}ole}}$, which is defined as $\mathcal{F}_{\mathsf{a\text{-}occ}}^{[n]}$. Recall from Theorem 1 that $\mathcal{F}_{\mathsf{a\text{-}ole}}$ can be realized using protocol $\Pi_{\mathsf{a\text{-}occ}}^{[n]}$. The specific details and proofs can be referred to in the respective theorem. Moreover, according to Remark 5, $\mathcal{F}_{\mathsf{a\text{-}ole}}$ outputs a uniformly random index $i \in [n]$ that indicates a leader P_i with a constant probability.

Functionality $\mathcal{F}_{\text{conc-a-ba}}^{V,N}$

The functionality is parameterized by a set V of values and a positive integer N representing the number of concurrent instances, and proceeds as follows. At the first activation, verify that $\mathsf{sid} = (\mathcal{P}, \mathsf{sid}')$, where $\mathcal{P}$ is a player set of size n. For each $P_i \in \mathcal{P}$, initialize $v_{i,1}, \ldots, v_{i,N}$ to a default value $\perp$, $\mathsf{participated}_i := 0$, and delay values $D_i^{\text{input}} = D_i^{\text{output}} := 1$. Also initialize $y_1, \ldots, y_N$ and $a_1, \ldots, a_N$ to $\perp$, and $t := \lceil \frac{n}{3} \rceil - 1$.

- Upon receiving $(\texttt{delay}, \mathsf{sid}, P_i, \mathsf{type}, D)$ from the adversary for $P_i \in \mathcal{P}$, $\mathsf{type} \in \{\text{input}, \text{output}\}$, and $D \in \mathbb{Z}$ represented in unary notation, update $D_i^{\mathsf{type}} := \max(1, D_i^{\mathsf{type}} + D)$ and send $(\texttt{delay-set}, \mathsf{sid})$ to the adversary.
- Upon receiving $(\texttt{input}, \mathsf{sid}, (v_1, \ldots, v_N))$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i), run the Input Submission Procedure and send $(\texttt{leakage}, \mathsf{sid}, P_i, (v_1, \ldots, v_N))$ to the adversary.
- Upon receiving $(\texttt{replace}, \mathsf{sid}, (v_1, \ldots, v_N))$ from the adversary, record $(a_1, \ldots, a_N) := (v_1, \ldots, v_N)$.
- Upon receiving $(\texttt{fetch}, \mathsf{sid})$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i) run the Input Submission and Output Release Procedures, and send $(\texttt{fetched}, \mathsf{sid}, P_i)$ to the adversary and any messages set by the Output Release Procedure to P_i.

Input Submission Procedure: If $\mathsf{participated}_i = 0$ and $(\texttt{input}, \mathsf{sid}, (v_1, \ldots, v_N))$ was already received from P_i, then do:

1. Update $D_i^{\text{input}} := D_i^{\text{input}} - 1$.
2. If $D_i^{\text{input}} = 0$, then set $\mathsf{participated}_i = 1$ and record $(v_{i,1}, \ldots, v_{i,N}) := (v_1, \ldots, v_N)$.

Output Release Procedure: If $\sum_{j=1}^{n} \mathsf{participated}_j \geq n - t$ then do:

1. Update $D_i^{\text{output}} := D_i^{\text{output}} - 1$.
2. If $D_i^{\text{output}} = 0$, for each $j \in [N]$, if $y_j = \perp$ then set $y_j := x$ if there exists $x \in V$ such that $x = v_{k,j}$ for at least $n - 2t$ input values $v_{k,j}$; else, if $a_j = \perp$ or $a_j \in V$ was provided by at least one honest party, then set $y_j := a_j$; else, set $y_j := \perp'$. Additionally, set $(\texttt{output}, \mathsf{sid}, (y_1, \ldots, y_N))$ to be sent to P_i.

Figure 7: The concurrent intrusion-tolerant A-BA functionality.

Our concurrent A-BA protocol leverages both binary and multi-valued A-BA functionalities. Binary A-BA is employed to achieve agreement on critical decisions within the protocol, such as whether to continue a particular iteration or even terminate the protocol. On the other hand, the utilization of multi-valued A-BA addresses the inherent obliviousness of the A-OLE primitive by providing a means for parties to reach an agreement. Ideal functionality for A-BA can be found in Figure 4.

Similar to [BE03], another essential component in our concurrent A-BA protocol is *truncated* executions of an A-BA protocol up to a fixed number of rounds. In the spirit of [CCGZ19], we model those executions with the ideal functionality $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ defined in Figure 8. $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ is parameterized with V, p, and rnd, where V denotes the domain, p represents the termination probability in each round, and rnd indicates the maximum number of rounds in the execution.

This ideal functionality captures Bracha's technique for termination [Bra84], which ensures that all honest parties will terminate within two consecutive rounds, and allows the adversary to specify which parties terminate first. Unlike a traditional A-BA functionality that outputs a single value, $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ produces a vector of values that includes the output of each round of execution. Modeling Bracha's termination technique and providing outputs for all rounds is crucial since our concurrent A-BA protocol relies on those properties of truncated executions of A-BA.

It is worth mentioning that $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}^{V,p,\mathsf{rnd}}$ can be implemented by executing any intrusion-tolerant A-BA protocol with a termination probability of p in each round, precisely for rnd rounds, and considering the output of all rounds in the final output (with λ representing rounds without output). Fortunately, both Canetti and Rabin's binary A-BA protocol [CR93] and Mostéfaoui and Raynal's multi-valued A-BA protocol [MR17] possess the desired properties of intrusion-tolerance

Functionality $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}^{V,p,\mathsf{rnd}}$

The functionality is parameterized by a set V of values, a probability p, and an integer rnd representing the number of rounds to run for, and proceeds as follows. At the first activation, verify that $\mathsf{sid} = (\mathcal{P}, \mathsf{sid}')$, where $\mathcal{P}$ is a player set of size n. For each $P_i \in \mathcal{P}$, initialize value v_i and vector y_i to a default value $\perp$, $\mathsf{participated}_i := 0$, and delay values $D_i^{\text{input}} = D_i^{\text{output}} := 1$. Also initialize values y, a, and r to $\perp$, the set $\mathcal{E}$ of parties receiving output earlier to $\mathcal{P}$, and $t := \lceil \frac{n}{3} \rceil - 1$.

- Upon receiving $(\texttt{delay}, \mathsf{sid}, P_i, \mathsf{type}, D)$ from the adversary for $P_i \in \mathcal{P}$, $\mathsf{type} \in \{\text{input}, \text{output}\}$, and $D \in \mathbb{Z}$ represented in unary notation, update $D_i^{\mathsf{type}} = \max(1, D_i^{\mathsf{type}} + D)$ and send $(\texttt{delay-set}, \mathsf{sid}, P_i)$ to the adversary.
- Upon receiving $(\texttt{early}, \mathsf{sid}, \mathcal{R})$ from the adversary, update $\mathcal{E} := \mathcal{R}$.
- Upon receiving $(\texttt{input}, \mathsf{sid}, v)$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i), run the Input Submission Procedure and send $(\texttt{leakage}, \mathsf{sid}, P_i, v)$ to the adversary.
- Upon receiving $(\texttt{replace}, \mathsf{sid}, v)$ from the adversary, record $a := v$.
- Upon receiving $(\texttt{fetch}, \mathsf{sid})$ from $P_i \in \mathcal{P}$ (or the adversary on behalf of corrupted P_i) run the Input Submission and Output Release Procedures, and send $(\texttt{fetched}, \mathsf{sid}, P_i)$ to the adversary and any messages set by the Output Release Procedure to P_i.

Input Submission Procedure: If $\mathsf{participated}_i = 0$ and $(\texttt{send}, \mathsf{sid}, v)$ was already received from P_i, then do:

1. Update $D_i^{\text{input}} := D_i^{\text{input}} - 1$.
2. If $D_i^{\text{input}} = 0$, then set $\mathsf{participated}_i = 1$ and record $v_i := v$.

Output Release Procedure: If $\sum_{j=1}^{n} \mathsf{participated}_j \geq n - t$ then do:

1. Update $D_i^{\text{output}} := D_i^{\text{output}} - 1$.
2. If $D_i^{\text{output}} = 0$, then if $r = \perp$ sample $r \leftarrow \text{Geometric}(p)$[a] and set $y := x$ if there exists a value $x \in V$ such that $x = v_k$ for at least $n - 2t$ input values v_k; else, if $a = \perp$ or $a \in V$ was provided by at least one honest party, then set $y := a$; else, set $y := \perp$. If $y_i = \perp$ then proceed as follows.
   - If $P_i \in \mathcal{E}$, then for $k < r$ let $y_{i,k} := \lambda$ (λ refers to empty string) and for $r \leq k \leq \mathsf{rnd}$ let $y_{i,k} := y$.
   - If $P_i \notin \mathcal{E}$, then for $k \leq r$ let $y_{i,k} := \lambda$ and for $r < k \leq \mathsf{rnd}$ let $y_{i,k} := y$.
   - Set $y_i := (y_{i,1}, \ldots, y_{i,\mathsf{rnd}})$.

   Additionally, set $(\texttt{output}, \mathsf{sid}, y_i)$ to be sent to P_i.

[a] Recall that the geometric distribution corresponds to the termination probability in expected-constant-round A-BA protocols. Moreover, by adjusting this distribution, the functionality can be generalized to accommodate other A-BA protocols.

Figure 8: The intrusion-tolerant truncated A-BA functionality with Bracha's termination.

and terminating with a constant probability in each round. Thus, we can formulate the following proposition about realizing $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}^{V,p,\mathsf{rnd}}$.

Proposition 6. *For some constant probability p, any domain V, and any integer* rnd, $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}^{V,p,\mathsf{rnd}}$ *can be UC-realized with statistical security in the $\mathcal{F}_{\mathsf{a\text{-}smt}}$-hybrid model, in constant rounds and in the presence of an adaptive and malicious t-adversary, provided $t < n/3$.*

The above statement guarantees statistical security since the A-BA protocols we consider rely on the A-VSS primitive, which can only be realized with statistical security when $t < n/3$. In fact, by working in the $\mathcal{F}_{\mathsf{a\text{-}vss}}$-hybrid model, we can achieve perfect $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$. We remark that the intrusion tolerance of $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ is not a requirement in our concurrent A-BA protocol; however, employing a non-intrusion-tolerant version of truncated A-BA will naturally lead to a non-intrusion-tolerant concurrent A-BA protocol.

The new concurrent A-BA protocol. Our protocol builds on the core idea presented in [BE03]. In addition to instantiating the missing OLE building block using our OCC protocol from Section 4, we address the issue in the analysis by redesigning the message distribution phase. Our revised message distribution mechanism not only resolves the issue in the proof but also provides stronger guarantees, which in turn simplifies the final protocol design. In fact, apart from the message distribution phase, the overall structure of our protocol closely resembles the synchronous version of the protocol described in [BE03].

Before diving into the high-level description of our protocol, we highlight the choices we made in the message distribution mechanism and discuss some alternative approaches that fail to meet our requirements. In the eventual-delivery model, at least $n - t$ parties will receive each other's messages if they wait for a sufficient duration, as messages from honest parties will eventually be delivered to one another, but determining the exact waiting time required is not straightforward. One possible approach is to instruct parties to A-Cast the identities of the parties from which they have received messages. By constructing a graph with parties as vertices and adding edges between parties that have reported message receipts from each other, we can look for a clique of size $n - t$ in the graph; however, finding a maximum clique is known to be NP-complete and also difficult to approximate [FGL+91]. To overcome this challenge, one possible approach is to explore alternative structures that can be efficiently identified, even if they provide weaker guarantees in terms of message dispersion [BCG93, BKR94, Can96, Pat11]; this approach does not guarantee the desired message dispersion required for our specific application. In our analysis, it is crucial that *all* honest parties receive messages from a linear fraction of other parties. Even finding a clique of size $n - t$ does not guarantee this level of message dispersion, rendering this approach not suitable for our protocol. Thus, we adopt another approach that has been used in prior works [Fel89, CR93], and extend it by incorporating a precondition check before the process and introducing a validation layer during the execution. These additions enhance the guarantees, making them more suitable and effective for our specific purpose. We proceed to explain our protocol.

Similar to the (synchronous) protocol described in [BE03], in our concurrent A-BA protocol, each party initiates for every A-BA instance a batch of m executions of the A-BA protocol (over the same inputs) for a fixed number of rounds, denoted as rnd. If the A-BA protocol has a termination probability of at least a constant value p in each round, which is the case for most existing A-BA protocols, suitable values of m and rnd can be determined so that each party obtains at least one output value for each batch. Each party then selects an output for each instance and forms a suggestion for the final output. The next paragraph, which explains the mechanism for distributing suggestions among parties, is our main modification to the protocol. Then, for the remaining part, we can use a similar structure as the synchronous version of the protocol.

Firstly, parties initiate a binary A-BA protocol to determine a specific condition that allows for choosing and validating suggested outputs later in the execution. Based on the outcome of this binary A-BA, parties decide whether to continue or start over. In the case of continuation, parties perform A-Cast operations to distribute their suggestions and wait to receive suggestions from other parties. Each party only accepts an A-Cast message containing a suggested output if the value is consistent with the outputs obtained from their own truncated A-BA executions. This validation step is crucial as it ensures that even corrupted parties provide acceptable (correct) suggestions. The validation is based on the property of A-BA that ensures all honest parties terminate within two consecutive rounds, which is achieved using Bracha's termination technique [Bra84]. Parties wait to accept A-Casts of suggested outputs from at least $n-t$ parties and then A-Cast the set of all these $n-t$ suggestions along with the identities of the corresponding senders. They continue accepting A-Casts of suggestions and sets until they receive at least $n-t$ sets that are fully contained within their accepted suggestions. At this point, a sufficient number of messages have been exchanged, and using a counting argument similar to the one in [Fel89, CR93], it can be deduced that at least $n/3$ parties have their suggested outputs received by all honest parties.

After the message distribution phase described above, our protocol proceeds similarly to the synchronous protocol presented in [BE03]. Specifically, parties execute OLE to elect a random leader to adopt its suggested output. Subsequently, a multi-valued A-BA is performed on the adopted output to address the oblivious nature of OLE. Finally, a binary A-BA is executed to determine whether an agreement on the output has been reached, resulting in the termination or restarting of the protocol. The intrusion-tolerance property of multi-valued A-BA is crucial to make sure that the result of the agreement on the output is not provided by a corrupted party. It is worth noting that the favorable scenario occurs when the leader is among the $n/3$ parties whose suggested outputs have been accepted by all honest parties. If the leader is elected randomly, this event happens with a probability of $1/3$. In this case, all parties adopt the same output, leading to termination in the subsequent A-BA calls.

It is worth noting that the set of $n/3$ parties whose suggested outputs have been accepted by all honest parties may only contain a single honest party. This single honest party can only be elected with a probability of $O(1/n)$ by the OLE. However, due to the validation step in the message-distribution phase, there is no longer a need to ensure that an honest leader is elected, as the suggested values from corrupted parties are considered valid outputs. Refer to Figure 9 for a formal description of protocol $\Pi_{\mathsf{conc\text{-}a\text{-}ba}}$.

5.3 Security Proof

We now present the security proof for our concurrent A-BA protocol. Before stating the theorem, it is worth noting that the specific parameters of the hybrid model, which combine the different ideal functionalities, are not explicitly specified in the theorem statement. However, they can be determined from the protocol's parameters and are integral to the overall security guarantees of the protocol. Now, let us state the theorem formally:

Theorem 2. *For any domain V, integer N, constant $0 < p < 1$, and constant integer $\mathsf{rnd} > 1$, setting $m := \log_{\frac{1}{1-p}} N$, the protocol $\Pi^{V,N,m,p,\mathsf{rnd}}_{\mathsf{conc\text{-}a\text{-}ba}}$ UC-realizes $\mathcal{F}^{V,N}_{\mathsf{conc\text{-}a\text{-}ba}}$ with statistical security in the $(\mathcal{F}_{\mathsf{a\text{-}cast}}, \mathcal{F}_{\mathsf{a\text{-}ba}}, \mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}, \mathcal{F}_{\mathsf{a\text{-}ole}})$-hybrid model, in expected-constant rounds and in the presence of an adaptive and malicious t-adversary, provided $t < n/3$.*

Proof. Let $\mathcal{A}$ be an adversary in the real world. We construct a simulator $\mathcal{S}$ in the ideal world, such that no environment $\mathcal{Z}$ can distinguish whether it is interacting with $\Pi^{V,N,m,p,\mathsf{rnd}}_{\mathsf{conc\text{-}a\text{-}ba}}$ and $\mathcal{A}$, or with $\mathcal{F}^{V,N}_{\mathsf{conc\text{-}a\text{-}ba}}$ and $\mathcal{S}$. Here, V and N are given parameters of the problem, and p is the parameter

Protocol $\Pi^{V,N,m,p,\mathsf{rnd}}_{\mathsf{conc\text{-}a\text{-}ba}}$

The protocol is parameterized by a set V of possible inputs (for each instance), positive integers N and m representing respectively the number of instances and the number of redundant executions to run per instance, a termination probability p, and the number rnd of rounds after which to truncate the executions.

- Upon receiving input $(\mathtt{input}, \mathsf{sid}, (v_{i,1}, \ldots, v_{i,N}))$ from the environment, where $\mathsf{sid} = (\mathcal{P}, \mathsf{sid}')$ for a player set $\mathcal{P}$ of size n and $v_{i,1}, \ldots, v_{i,N} \in V$, party $P_i \in \mathcal{P}$ proceeds as follows.
  1. For all $h \in [n]$, $j \in [N]$, $k \in [m]$, and $\mathsf{rnd} \leq r \leq \mathsf{rnd} + 3$, initialize flags $b_h := 0$ and $b_{j,k} := 0$, variables $c_{i,j} := \perp$ and $y_{i,j} := \perp$, and sets $S^r_{i,j} := \emptyset$, $Q_{i,1} := \emptyset$, $Q_{i,2} := \emptyset$, and $Q'_{h,1} := \perp$. Also initialize a counter $\varphi := 1$, and a flag $\mathsf{finished} := 0$.
  2. For all $j \in [N]$ and $k \in [m]$, send $(\mathtt{input}, \mathsf{sid}^{j,k}, v_{i,j})$ to an instance of $\mathcal{F}^{V,p,\mathsf{rnd}+3}_{\mathsf{trunc\text{-}a\text{-}ba}}$ with SID $\mathsf{sid}^{j,k}_\varphi := (\mathsf{sid}, \varphi, j, k)$.
- Upon later activations, if $\mathsf{finished} = 0$ then do:
  1. For each $j \in [N]$ and $k \in [m]$ such that $b_{j,k} = 0$, fetch the output from the instance of $\mathcal{F}^{V,p,\mathsf{rnd}+3}_{\mathsf{trunc\text{-}a\text{-}ba}}$ with SID $\mathsf{sid}^{j,k}_\varphi$. Upon receiving back $(\mathtt{output}, \mathsf{sid}^{j,k}_\varphi, (z_{i,1}, \ldots, z_{i,\mathsf{rnd}+3}))$, update $S^r_{i,j} := S^r_{i,j} \cup \{z_{i,r}\} \setminus \{\lambda\}$ for $\mathsf{rnd} \leq r \leq \mathsf{rnd} + 3$, and also set $b_{j,k} := 1$.
  2. Wait until $b_{j,k} = 1$ for all $j \in [N]$ and $k \in [m]$. Then, let $\mathsf{cont}_i := 1$ if for all $j \in [N]$ it holds that $S^{\mathsf{rnd}}_{i,j} \neq \emptyset$, and $\mathsf{cont}_i := 0$ otherwise. Send $(\mathtt{input}, \mathsf{sid}^{\mathrm{cont}}_\varphi, \mathsf{cont}_i)$ to an instance of $\mathcal{F}^{\{0,1\}}_{\mathsf{a\text{-}ba}}$ with SID $\mathsf{sid}^{\mathrm{cont}}_\varphi := (\mathsf{sid}, \varphi, \mathtt{cont})$.
  3. Fetch the output from the instance of $\mathcal{F}^{\{0,1\}}_{\mathsf{a\text{-}ba}}$ with SID $\mathsf{sid}^{\mathrm{cont}}_\varphi$. Upon receiving back $(\mathtt{output}, \mathsf{sid}^{\mathrm{cont}}_\varphi, \mathsf{continue})$, if $\mathsf{continue} = 0$ then start over (i.e., increment φ, re-initialize all other local variables, and run truncated A-BA for mN times again); else, for each $j \in [N]$ set $c_{i,j}$ to be an arbitrary element in $S^{\mathsf{rnd}}_{i,j} \cup S^{\mathsf{rnd}+1}_{i,j}$, and send $(\mathtt{send}, \mathsf{sid}^{\mathrm{vector}}_{i,\varphi}, (c_{i,1}, \ldots, c_{i,N}))$ to an instance of $\mathcal{F}_{\mathsf{a\text{-}cast}}$ with SID $\mathsf{sid}^{\mathrm{vector}}_{i,\varphi} := (\mathcal{P}, P_i, \mathsf{sid}', \varphi, \mathtt{vector})$.
  4. For each $h \in [n]$ such that $b_h = 0$, fetch the output from the instance of $\mathcal{F}_{\mathsf{a\text{-}cast}}$ with SID $\mathsf{sid}^{\mathrm{vector}}_{h,\varphi}$. Upon receiving back $(\mathtt{output}, \mathsf{sid}^{\mathrm{vector}}_{h,\varphi}, (c'_{h,1}, \ldots, c'_{h,N}))$, for each $b \in \{1,2\}$ update $Q_{i,b} := Q_{i,b} \cup \{(P_h, (c'_{h,1}, \ldots, c'_{h,N}))\}$ if for all $j \in [N]$ it holds that $c'_{h,j} \in S^{\mathsf{rnd}+1+b}_{i,j}$, and also set $b_h := 1$.
  5. Wait until $|Q_{i,1}| \geq n - t$. Then send $(\mathtt{send}, \mathsf{sid}^{\mathrm{set}}_{i,\varphi}, Q^{(n-t)}_{i,1})$ to an instance of $\mathcal{F}_{\mathsf{a\text{-}cast}}$ with SID $\mathsf{sid}^{\mathrm{set}}_{i,\varphi} := (\mathcal{P}, P_i, \mathsf{sid}', \varphi, \mathtt{set})$.
  6. For each $h \in [n]$ such that $Q'_{h,1} = \perp$, fetch the output from the instance of $\mathcal{F}_{\mathsf{a\text{-}cast}}$ with SID $\mathsf{sid}^{\mathrm{set}}_{h,\varphi}$. Upon receiving back $(\mathtt{output}, \mathsf{sid}^{\mathrm{set}}_{h,\varphi}, Y)$, record $Q'_{h,1} := Y$.
  7. Wait until $Q'_{h,1} \subseteq Q_{i,2}$ for at least $n - t$ values of $h \in [n]$. Then send $(\mathtt{input}, \mathsf{sid}^{\mathrm{elect}}_\varphi)$ to an instance of $\mathcal{F}_{\mathsf{a\text{-}ole}}$ with SID $\mathsf{sid}^{\mathrm{elect}}_\varphi := (\mathsf{sid}, \varphi, \mathtt{elect})$.
  8. Fetch the output from the instance of $\mathcal{F}_{\mathsf{a\text{-}ole}}$ with SID $\mathsf{sid}^{\mathrm{elect}}_\varphi$. Upon receiving back $(\mathtt{output}, \mathsf{sid}^{\mathrm{elect}}_\varphi, l_i)$, if there is a pair $(P_{l_i}, (c'_{l_i,1}, \ldots, c'_{l_i,N})) \in Q_{i,2}$, then let $C'_{l_i} := (c'_{l_i,1}, \ldots, c'_{l_i,N})$; else, let $C'_{l_i} := \perp$. Send $(\mathtt{input}, \mathsf{sid}^{\mathrm{vector}}_\varphi, C'_{l_i})$ to an instance of $\mathcal{F}^{V^N}_{\mathsf{a\text{-}ba}}$ with SID $\mathsf{sid}^{\mathrm{vector}}_\varphi := (\mathsf{sid}, \varphi, \mathtt{vector})$.
  9. Fetch the output from the instance of $\mathcal{F}_{\mathsf{a\text{-}ba}}$ with SID $\mathsf{sid}^{\mathrm{vector}}_\varphi$. Upon receiving back $(\mathtt{output}, \mathsf{sid}^{\mathrm{vector}}_\varphi, Y_i)$, if $Y_i \neq \perp$, then let $\mathsf{term}_i := 1$ and record $(y_{i,1}, \ldots, y_{i,N}) := Y_i$; else, let $\mathsf{term}_i := 0$. Send $(\mathtt{input}, \mathsf{sid}^{\mathrm{term}}_\varphi, \mathsf{term}_i)$ to an instance of $\mathcal{F}^{\{0,1\}}_{\mathsf{a\text{-}ba}}$ with SID $\mathsf{sid}^{\mathrm{term}}_\varphi := (\mathsf{sid}, \varphi, \mathtt{term})$.
  10. Fetch the output from the instance of $\mathcal{F}^{\{0,1\}}_{\mathsf{a\text{-}ba}}$ with SID $\mathsf{sid}^{\mathrm{term}}_\varphi$. Upon receiving back $(\mathtt{output}, \mathsf{sid}^{\mathrm{term}}_\varphi, \mathsf{terminate})$, if $\mathsf{terminate} = 0$ then start over; else, set $\mathsf{finished} := 1$.
- Upon receiving input $(\mathtt{fetch}, \mathsf{sid})$ from the environment, if $\mathsf{finished} = 1$ then output $(\mathtt{output}, \mathsf{sid}, (y_{i,1}, \ldots, y_{i,N}))$ to the environment.

Figure 9: The concurrent A-BA protocol.

for the $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ hybrid, which is determined based on the specific protocol used to realize it. The parameters m and rnd need to be appropriately adjusted based on the other parameters to ensure an expected-constant round complexity for $\Pi^{V,N,m,p,\mathsf{rnd}}_{\mathsf{conc\text{-}a\text{-}ba}}$. As discussed below, setting $m := \log_{\frac{1}{1-p}} N$

for any constant integer $\mathsf{rnd} > 1$ suffices.

The simulator internally runs a copy of $\mathcal{A}$, and plays the roles of all the hybrids and the parties in a simulated execution of the protocol. All inputs from $\mathcal{Z}$ are forwarded to $\mathcal{A}$, and all outputs from $\mathcal{A}$ are forwarded to $\mathcal{Z}$. Moreover, whenever $\mathcal{A}$ corrupts a party in the simulation, $\mathcal{S}$ corrupts the same party in the ideal world by interacting with $\mathcal{F}_{\mathsf{conc\text{-}a\text{-}ba}}^{V,N}$, and if the corruption was direct (i.e., not via either of the aiding functionalities), then $\mathcal{S}$ sends $\mathcal{A}$ the party's state and thereafter follows $\mathcal{A}$'s instructions for that party. Moreover, $\mathcal{S}$ manages delays in the ideal functionality based on the delays that $\mathcal{A}$ sets on the hybrids.

The simulated execution begins when $\mathcal{S}$ receives messages of the form $(\mathtt{leakage}, \mathsf{sid}, \cdot, \cdot)$ from $\mathcal{F}_{\mathsf{conc\text{-}a\text{-}ba}}^{V,N}$. These messages contain the values that party P_i receives as input from the environment. $\mathcal{S}$ can derive these input values from the leakage message $(\mathtt{leakage}, \mathsf{sid}, P_i, (v_1, \ldots, v_N))$ by setting $v_{i,j} = v_j$ for all $j \in [N]$. The set $\{v_{1,j}, v_{2,j}, \ldots, v_{n,j}\}$ represents the inputs for the j^{th} instance of the (concurrent) A-BA that the parties are supposed to solve.

Upon receiving these leakage messages, $\mathcal{S}$ can initiate sessions of $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ with the actual inputs. For each instance $j \in [N]$, $\mathcal{S}$ invokes m sessions of $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ with the inputs $v_{1,j}, v_{2,j}, \ldots, v_{n,j}$. After this point, $\mathcal{S}$ continues the simulation by honestly playing the roles of other ideal functionalities and honest parties involved in the protocol. Since there are no private states that $\mathcal{S}$ needs to guess or fake in order to provide a consistent view, the rest of the simulation proceeds straightforwardly.

Now, this internal execution generates a transcript that is perfectly indistinguishable from a real-world execution. Therefore, it remains to show that the protocol execution indeed results in the same output as $\mathcal{F}_{\mathsf{conc\text{-}a\text{-}ba}}^{V,N}$. To demonstrate this, we first establish that with probability 1 the execution will eventually terminate. Additionally, we show that if at least $n - 2t$ parties have the same value for any instance, everyone will receive that value as the output; otherwise, the output will be either one of the inputs provided by some honest parties for that instance or a special value $\perp$.

Termination. After initializing some variables, the parties collectively initiate m sessions of $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ for each of the N instances. Since the maximum number of corrupted parties is t and $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ only requires the participation of $n - t$ parties, all instances of $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ will eventually terminate upon receiving a sufficient number of activations from the environment.

If, for all N instances, the integer r sampled in any of the m invocations of $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ for that instance is at most $\mathsf{rnd} - 1$, then every honest party P_i sets $\mathsf{cont}_i := 1$. Here, r is sampled from the geometric distribution Geometric(p) (that corresponds to expected-constant-round A-BA as in [Fel89, CR93]). We define E as the event where for all instances at least one of the m sessions of $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ has $r \leq \mathsf{rnd} - 1$. The probability of event E occurring can be calculated as follows, using similar logic as presented in [BE03].

Define A_{r_0} as the event where $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ does not sample $r = r_0$ given $r \geq r_0$. Then

$$\Pr[A_{r_0}] = 1 - p.$$

Therefore, for the event B_{r_0}, in which at least one of the m $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$'s for an instance samples $r = r_0$ given $r \geq r_0$, we have

$$\Pr[B_{r_0}] = 1 - \Pr[A_{r_0}]^m = 1 - (1 - p)^m.$$

This implies that for the event C_{r_0} in which for some of the N instances, none of the m $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$'s sample $r = r_0$ given $r \geq r_0$, the following holds:

$$\Pr[C_{r_0}] = 1 - \Pr[B_{r_0}]^N = 1 - (1 - (1 - p)^m)^N$$

Now we can calculate the probability of E^{c}, which represents the event where for some of the N instances, none of the m $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$'s sample $r \leq \mathsf{rnd}-1$:

$$\Pr[E^{\mathrm{c}}] = \prod_{i=1}^{\mathsf{rnd}-1} \Pr[C_i] = \left(1-(1-(1-p)^m)^N\right)^{\mathsf{rnd}-1}$$

Therefore, the complementary probability is

$$\Pr[E] = 1 - \Pr[E^{\mathrm{c}}] = 1 - \left(1-(1-(1-p)^m)^N\right)^{\mathsf{rnd}-1}.$$

By setting $m := \log_{\frac{1}{1-p}} N$ it holds that

$$\Pr[E] = 1 - \left(1-\left(1-\frac{1}{N}\right)^N\right)^{\mathsf{rnd}-1}.$$

Then considering $\left(1-\frac{1}{N}\right)^N \approx \frac{1}{e}$ we have

$$\Pr[E] \approx 1 - \left(1-\frac{1}{e}\right)^{\mathsf{rnd}-1}.$$

So, for a constant value of $\mathsf{rnd} > 1$, the probability $\Pr[E]$ is a non-zero constant. This implies that, with appropriate parameter choices, every honest party P_i sets $\mathsf{cont}_i := 1$ with a constant probability. In other words, the output of the binary $\mathcal{F}_{\mathsf{a\text{-}ba}}$ protocol on the cont_i values results in 1 with a constant probability, indicating continuation.

When the binary $\mathcal{F}_{\mathsf{a\text{-}ba}}$ on cont_i values outputs 1, it guarantees that at least one honest party has provided 1. In this case, at least one honest party P_i sets $\mathsf{cont}_i := 1$, which implies that for all $j \in [N]$, $S_{i,j}^{\mathsf{rnd}} \neq \emptyset$. As $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ models Bracha's termination, it follows that for any honest party P_k, we have $S_{k,j}^{\mathsf{rnd}} \cup S_{k,j}^{\mathsf{rnd}+1} \neq \emptyset$, allowing them to set $c_{k,j}$ values without any issues (deadlocks).

Then, honest party P_k can A-Cast $(c_{k,1}, c_{k,2}, \ldots, c_{k,N})$ and wait for the other parties. Again, utilizing the property of Bracha's termination in $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$, for any pair of honest parties P_k and P_i, for all $j \in [N]$, $c_{k,j} \in S_{i,j}^{\mathsf{rnd}+2}$ (because P_k chooses $c_{k,j} \in S_{k,j}^{\mathsf{rnd}} \cup S_{k,j}^{\mathsf{rnd}+1}$). Therefore, upon receiving the A-Cast of $(c'_{k,1}, \ldots, c'_{k,N})$ from P_k, honest party P_i will update $Q_{i,1} := Q_{i,1} \cup (P_k, (c'_{k,1}, \ldots, c'_{k,N}))$ if P_k is honest.

Since there are at most t corruptions, for any honest party P_i, we eventually have $|Q_{i,1}| \geq n-t$. This ensures that there is no deadlock in forming and A-Casting $Q_{i,1}^{(n-t)}$. Furthermore, using the property of Bracha's termination in $\mathcal{F}_{\mathsf{trunc\text{-}a\text{-}ba}}$ again, we can see that for any pair of honest parties P_k and P_i, it holds that $Q_{k,1}^{(n-t)} \subseteq Q_{i,2}$. This can be verified easily because for any $(P_h, (c_{h,1}, \ldots, c_{h,N})) \in Q_{k,1}^{(n-t)}$ and for all $j \in [N]$, it holds that $c_{h,j} \in S_{k,j}^{\mathsf{rnd}+2}$. This implies that for any honest party P_i, we eventually have $c_{h,j} \in S_{i,j}^{\mathsf{rnd}+3}$, which means $(P_h, (c_{h,1}, \ldots, c_{h,N})) \in Q_{i,2}$.

Since there are at least $n-t$ honest parties, each honest party P_i will eventually receive enough A-Casts $Q'_{h,1} \subseteq Q_{i,2}$ to proceed with $\mathcal{F}_{\mathsf{a\text{-}ole}}$.

Before proceeding, it is important to note that by using a similar counting argument as in [Fel89, CR93], we can guarantee that messages (suggestions) from at least $\frac{n}{3}$ parties will eventually be received by all honest parties. In more detail, let us consider the scenario where an honest party P_i receives $s$sets $Q'_{h,1} \subseteq Q_{i,2}$. We can construct an $s \times n$ table T, where $T_{l,k} = 1$ if and only if P_i has received $Q'_{l,1} \subseteq Q_{i,2}$ and $(P_k, (c'_{k,1}, \ldots, c'_{k,N})) \in Q'_{l,1}$. Each row of the table contains $n-t$ entries equal to one, indicating that there are a total of $s(n-t)$ one entries in T. Let q be the

minimum number of columns in T that have at least $t+1$ one entries. We can express the following inequality:

$$qs + (n-q)t \geq s(n-t).$$

Simplifying this inequality, we have

$$q \geq \frac{s(n-t) - nt}{s-t}.$$

We also know that $n \geq 3t+1$ and each will eventually reach the state where $s \geq n-t$ (before starting $\mathcal{F}_{\mathsf{a\text{-}ole}}$); by plugging in those relations we have

$$\begin{aligned} q &\geq \frac{(n-t)^2 - nt}{n-2t} \\ &= \frac{(n-2t)^2 + nt - 3t^2}{n-2t} \\ &= n - 2t + \frac{nt - 3t^2}{n-2t} \\ &\geq n - 2t + \frac{t}{n-2t} \\ &\geq \frac{n}{3}. \end{aligned}$$

Therefore, we can conclude that at least $q \geq \frac{n}{3}$ columns in the table contain at least $t+1$ one entries. As mentioned earlier, each honest party P_j will eventually receive $n-t$ sets $Q'_{h,1} \subseteq Q_{j,2}$, meaning that in their respective table, they will have at least one entry with a value of one in each of those q columns. Consequently, they will have all the parties and their suggestions corresponding to those q columns in their $Q_{j,2}$ set. Hence, we can infer that suggestions from at least $\frac{n}{3}$ parties will be delivered to all honest parties.

Since all honest parties eventually participate in $\mathcal{F}_{\mathsf{a\text{-}ole}}$, there is no deadlock in completing that phase. With a constant probability, the parties agree on a random leader. Conditioned on agreeing on a random leader, there is a probability of at least $\frac{1}{3}$ that the leader is among the parties whose inputs will eventually be delivered to all honest parties. In this case, all honest parties start the $\mathcal{F}_{\mathsf{a\text{-}ba}}$ after $\mathcal{F}_{\mathsf{a\text{-}ole}}$ with the same non-default input, which is the agreed-upon leader's value. Therefore, any honest party P_i receives the leader's output (which is not $\perp$) and sets $\mathsf{term}_i := 1$. Since all honest parties start the final binary $\mathcal{F}_{\mathsf{a\text{-}ba}}$ with 1, they all receive 1 as the output and terminate with the leader's value.

Therefore, the execution of the protocol $\Pi_{\mathsf{conc\text{-}a\text{-}ba}}$ does not encounter any deadlocks. Furthermore, by choosing appropriate parameters, specifically $m := \log_{\frac{1}{1-p}} N$, the protocol $\Pi_{\mathsf{conc\text{-}a\text{-}ba}}$ can achieve termination with a constant probability in each iteration. This implies that the protocol $\Pi_{\mathsf{conc\text{-}a\text{-}ba}}$ will eventually terminate with probability 1, and the expected number of iterations is constant.

Correctness. Now we demonstrate that once the protocol terminates, all honest parties output the same value as the ideal functionality. This part of the proof requires the intrusion-tolerance property of A-BA, which guarantees that the output is either $\perp$ or a value provided by an honest party.

Since we assumed termination, the last binary $\mathcal{F}_{\mathsf{a\text{-}ba}}$ on term_i must return 1. This occurs only when at least one honest party P_i has $\mathsf{term}_i = 1$, indicating that it receives a non-empty vector

$Y_i = (y_{i,1}, \ldots, y_{i,N})$ from the $\mathcal{F}_{\text{a-ba}}$ after $\mathcal{F}_{\text{a-ole}}$. According to the intrusion tolerance property of $\mathcal{F}_{\text{a-ba}}$, it returns $Y_i \neq \perp$ only when Y_i is provided by an honest party P_j. Therefore, honest party P_j can find an element $(P_{l_i}, (y_{i,1}, \ldots, y_{i,N})) \in Q_{j,2}$. Hence, for every $1 \leq k \leq N$, P_j has confirmed that $y_{i,k} \in S_{j,k}^{\text{rnd}+3}$. This implies that $y_{i,k}$ is a valid and non-empty output from one of the $\mathcal{F}_{\text{trunc-a-ba}}$ executions for the k^{th} instance. Thus, according to the description of $\mathcal{F}_{\text{trunc-a-ba}}$, if at least $n - 2t$ parties have the same value for any instance, everyone will receive that value as the output; otherwise, the output will be either one of the inputs provided by some honest parties for that instance or a special value $\perp$.

Therefore, with probability 1, no environment can distinguish between the execution of $\Pi_{\text{conc-a-ba}}^{V,N,m,p,\text{rnd}}$ with $\mathcal{A}$ and $\mathcal{F}_{\text{conc-a-ba}}^{V,N}$ with $\mathcal{S}$, assuming expected-PPT machines. However, in order to apply UC composition guarantees, we need to introduce a stopping point for our expected-PPT machines and make them strict PPT. In doing so, the distinguishing probability of the environment would become a non-zero value which can be arbitrarily small, depending on the duration for which we allow the machines to run. This ensures that the *strict* PPT protocol $\Pi_{\text{conc-a-ba}}^{V,N,m,p,\text{rnd}}$ UC-realizes $\mathcal{F}_{\text{conc-a-ba}}^{V,N}$ with statistical security. □

Acknowledgements

Our original motivation for this project was to provide a simulation-based treatment of concurrent A-BA protocols, such as Ben-Or and El-Yaniv's [BE03], but the search for building blocks, in particular of an optimally resilient asynchronous OCC protocol became a bit of a "detective story," as many references pointed to an unpublished manuscript by Feldman [Fel89], which was nowhere to be found. We thank Michael Ben-Or for providing it to us, which corroborated its in-existence.

Bibliography

[AC10] Hagit Attiya and Keren Censor-Hillel. Lower bounds for randomized consensus under a weak adversary. *SIAM Journal on Computing*, 39(8):3885–3904, 2010.

[ADH08] Ittai Abraham, Danny Dolev, and Joseph Y. Halpern. An almost-surely terminating polynomial protocol for asynchronous byzantine agreement with optimal resilience. In *27th ACM PODC*, pages 405–414. ACM, 2008.

[AJM+21] Ittai Abraham, Philipp Jovanovic, Mary Maller, Sarah Meiklejohn, Gilad Stern, and Alin Tomescu. Reaching consensus for asynchronous distributed key generation. In *40th ACM PODC*, pages 363–373. ACM, 2021.

[AMS19] Ittai Abraham, Dahlia Malkhi, and Alexander Spiegelman. Asymptotically optimal validated asynchronous byzantine agreement. In *38th ACM PODC*, pages 337–346. ACM, 2019.

[BCG93] Michael Ben-Or, Ran Canetti, and Oded Goldreich. Asynchronous secure computation. In *25th ACM STOC*, pages 52–61. ACM Press, 1993.

[BE88] Michael Ben-Or and Ran El-Yaniv. Interactive consistency in constant expected time. Technical report, Inst. of Math. and Comp. Sci., Hebrew University, Jerusalem, 1988.

[BE03] Michael Ben-Or and Ran El-Yaniv. Resilient-optimal interactive consistency in constant time. *Distributed Computing*, 16(4):249–262, 2003.

[Ben83] Michael Ben-Or. Another advantage of free choice: Completely asynchronous agreement protocols (extended abstract). In *2nd ACM PODC*, pages 27–30. ACM, 1983.

[BGP89] Piotr Berman, Juan A. Garay, and Kenneth J. Perry. Towards optimal distributed consensus (extended abstract). In *30th FOCS*, pages 410–415. IEEE Computer Society Press, 1989.

[BGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *20th ACM STOC*, pages 1–10. ACM Press, 1988.

[BH07] Zuzana Beerliová-Trubíniová and Martin Hirt. Simple and efficient perfectly-secure asynchronous MPC. In *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 376–392. Springer, Heidelberg, 2007.

[BKR94] Michael Ben-Or, Boaz Kelmer, and Tal Rabin. Asynchronous secure computations with optimal resilience (extended abstract). In *13th ACM PODC*, pages 183–192. ACM, 1994.

[Bor96] Malte Borcherding. Levels of authentication in distributed agreement. In *10th International Workshop on Distributed Algorithms WDAG*, pages 40–55. Springer, Berlin, Heidelberg, 1996.

[Bra84] Gabriel Bracha. An asynchronous [(n-1)/3]-resilient consensus protocol. In *3rd ACM PODC*, pages 154–162. ACM, 1984.

[Bra87] Gabriel Bracha. Asynchronous byzantine agreement protocols. *Inf. Comput.*, 75(2):130–143, 1987.

[BS93] Donald Beaver and Nicol So. Global, unpredictable bit generation without broadcast. In *EUROCRYPT'93*, volume 765 of *LNCS*, pages 424–434. Springer, Heidelberg, 1993.

[BT85] Gabriel Bracha and Sam Toueg. Asynchronous consensus and broadcast protocols. *Journal of the ACM*, 32(4):824–840, 1985.

[BZL20] Erica Blum, Chen-Da Liu Zhang, and Julian Loss. Always have a backup plan: Fully secure synchronous MPC with asynchronous fallback. In *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 707–731. Springer, Heidelberg, 2020.

[Can96] Ran Canetti. *Studies in secure multiparty computation and applications*. PhD thesis, Weizmann Institute of Science, 1996.

[Can20] Ran Canetti. Universally composable security. *Journal of the ACM*, 67(5):1–94, 2020.

[CCD88] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In *20th ACM STOC*, pages 11–19. ACM Press, 1988.

[CCGZ19] Ran Cohen, Sandro Coretti, Juan Garay, and Vassilis Zikas. Probabilistic termination and composability of cryptographic protocols. *Journal of Cryptology*, 32(3):690–741, 2019.

[CCGZ21] Ran Cohen, Sandro Coretti, Juan A. Garay, and Vassilis Zikas. Round-preserving parallel composition of probabilistic-termination cryptographic protocols. *Journal of Cryptology*, 34(2):12, 2021.

[CGHZ16] Sandro Coretti, Juan Garay, Martin Hirt, and Vassilis Zikas. Constant-round asynchronous multi-party computation based on one-way functions. In *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 998–1021. Springer, Heidelberg, 2016.

[CGZ23] Ran Cohen, Juan Garay, and Vassilis Zikas. Completeness theorems for adaptively secure broadcast. CRYPTO '23 (to appear), 2023.

[CHM+22] Ran Cohen, Iftach Haitner, Nikolaos Makriyannis, Matan Orland, and Alex Samorodnitsky. On the round complexity of randomized byzantine agreement. *Journal of Cryptology*, 35(2):10, 2022.

[CKPS01] Christian Cachin, Klaus Kursawe, Frank Petzold, and Victor Shoup. Secure and efficient asynchronous broadcast protocols. In *CRYPTO 2001*, volume 2139 of *LNCS*, pages 524–541. Springer, Heidelberg, 2001.

[CKS05] Christian Cachin, Klaus Kursawe, and Victor Shoup. Random oracles in constantinople: Practical asynchronous byzantine agreement using cryptography. *Journal of Cryptology*, 18(3):219–246, 2005.

[CMS89] Benny Chor, Michael Merritt, and David B. Shmoys. Simple constant-time consensus protocols in realistic failure models. *Journal of the ACM*, 36(3):591–614, 1989.

[Coh16] Ran Cohen. Asynchronous secure multiparty computation in constant time. In *PKC 2016, Part II*, volume 9615 of *LNCS*, pages 183–207. Springer, Heidelberg, 2016.

[CPS19] T.-H. Hubert Chan, Rafael Pass, and Elaine Shi. Round complexity of Byzantine agreement, revisited. IACR Cryptology ePrint Archive, Report 2019/886, 2019. https://eprint.iacr.org/2019/886.

[CPS20] T.-H. Hubert Chan, Rafael Pass, and Elaine Shi. Sublinear-round byzantine agreement under corrupt majority. In *PKC 2020, Part II*, volume 12111 of *LNCS*, pages 246–265. Springer, Heidelberg, 2020.

[CR93] Ran Canetti and Tal Rabin. Fast asynchronous byzantine agreement with optimal resilience. In *25th ACM STOC*, pages 42–51. ACM Press, 1993. Full version available at https://www.cs.tau.ac.il/~canetti/materials/cr93.ps.

[CR98] Ran Canetti and Tal Rabin. Fast asynchronous byzantine agreement with optimal resilience. Full version of [CR93], 1998. https://www.cs.tau.ac.il/~canetti/materials/cr93.ps.

[DLS88] Cynthia Dwork, Nancy A. Lynch, and Larry J. Stockmeyer. Consensus in the presence of partial synchrony. *Journal of the ACM*, 35(2):288–323, 1988.

[DS83] Danny Dolev and H. Raymond Strong. Authenticated algorithms for byzantine agreement. *SIAM Journal on Computing*, 12(4):656–666, 1983.

[dSKT22] Luciano Freitas de Souza, Petr Kuznetsov, and Andrei Tonkikh. Distributed randomness from approximate agreement. In *36th DISC*, volume 246 of *LIPIcs*, pages 24:1–24:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[Fel88] Paul Neil Feldman. *Optimal Algorithms for Byzantine Agreement*. PhD thesis, Massachusetts Institute of Technology, 1988.

[Fel89] Paul Feldman. Asynchronous byzantine agreement in constant expected time. Unpublished manuscript, 1989.

[FG03] Matthias Fitzi and Juan A. Garay. Efficient player-optimal protocols for strong and differential consensus. In *22nd ACM PODC*, pages 211–220. ACM, 2003.

[FGL+91] Uriel Feige, Shafi Goldwasser, László Lovász, Shmuel Safra, and Mario Szegedy. Approximating clique is almost NP-complete (preliminary version). In *32nd FOCS*, pages 2–12. IEEE Computer Society Press, 1991.

[Fit03] Matthias Fitzi. *Generalized communication and security models in Byzantine agreement*. PhD thesis, ETH Zurich, Zürich, Switzerland, 2003.

[FL82] Michael J. Fischer and Nancy A. Lynch. A lower bound for the time to assure interactive consistency. *Information Processing Letters*, 14(4):183–186, 1982.

[FLM86] Michael J. Fischer, Nancy A. Lynch, and Michael Merritt. Easy impossibility proofs for distributed consensus problems. *Distributed Computing*, 1(1):26–39, 1986.

[FLP85] Michael J. Fischer, Nancy A. Lynch, and Mike Paterson. Impossibility of distributed consensus with one faulty process. *Journal of the ACM*, 32(2):374–382, 1985.

[FM88] Paul Feldman and Silvio Micali. Optimal algorithms for byzantine agreement. In *20th ACM STOC*, pages 148–161. ACM Press, 1988.

[FM89] Paul Feldman and Silvio Micali. An optimal probabilistic algorithm for synchronous byzantine agreement. In *ICALP 89*, volume 372 of *LNCS*, pages 341–378. Springer, Heidelberg, 1989.

[FM97] Pesech Feldman and Silvio Micali. An optimal probabilistic protocol for synchronous byzantine agreement. *SIAM J. Comput.*, 26(4):873–933, 1997.

[FN09] Matthias Fitzi and Jesper Buus Nielsen. On the number of synchronous rounds sufficient for authenticated byzantine agreement. In *23rd DISC*, volume 5805 of *LNCS*, pages 449–463. Springer, Heidelberg, 2009.

[GGL22] Diana Ghinea, Vipul Goyal, and Chen-Da Liu-Zhang. Round-optimal byzantine agreement. In *EUROCRYPT 2022, Part I*, volume 13275 of *LNCS*, pages 96–119. Springer, Heidelberg, 2022.

[GKKO07] Juan A. Garay, Jonathan Katz, Chiu-Yuen Koo, and Rafail Ostrovsky. Round complexity of authenticated broadcast with a dishonest majority. In *48th FOCS*, pages 658–668. IEEE Computer Society Press, 2007.

[GLL+22] Yingzi Gao, Yuan Lu, Zhenliang Lu, Qiang Tang, Jing Xu, and Zhenfeng Zhang. Efficient asynchronous byzantine agreement without private setups. In *42nd ICDCS*, pages 246–257. IEEE, 2022.

[GM98] Juan A. Garay and Yoram Moses. Fully polynomial byzantine agreement for $n > 3$t processors in $t + 1$ rounds. *SIAM J. Comput.*, 27(1):247–290, 1998.

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In *19th ACM STOC*, pages 218–229. ACM Press, 1987.

[HNP05] Martin Hirt, Jesper Buus Nielsen, and Bartosz Przydatek. Cryptographic asynchronous multi-party computation with optimal resilience (extended abstract). In *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 322–340. Springer, Heidelberg, 2005.

[HNP08] Martin Hirt, Jesper Buus Nielsen, and Bartosz Przydatek. Asynchronous multi-party computation with quadratic communication. In *ICALP 2008, Part II*, volume 5126 of *LNCS*, pages 473–485. Springer, Heidelberg, 2008.

[HZ10] Martin Hirt and Vassilis Zikas. Adaptively secure broadcast. In *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 466–485. Springer, Heidelberg, 2010.

[KK09] Jonathan Katz and Chiu-Yuen Koo. On expected constant-round protocols for byzantine agreement. *Journal of Computer and System Sciences*, 75(2):91–112, 2009.

[KMTZ13] Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas. Universally composable synchronous computation. In *TCC 2013*, volume 7785 of *LNCS*, pages 477–498. Springer, Heidelberg, 2013.

[KY86] Anna R. Karlin and Andrew Chi-Chih Yao. Probabilistic lower bounds for Byzantine agreement and clock synchronization. Unpublished manuscript, 1986.

[LLM+20] Chen-Da Liu-Zhang, Julian Loss, Ueli Maurer, Tal Moran, and Daniel Tschudi. MPC with synchronous security and asynchronous responsiveness. In *ASIACRYPT 2020, Part III*, volume 12493 of *LNCS*, pages 92–119. Springer, Heidelberg, 2020.

[LLR02] Yehuda Lindell, Anna Lysyanskaya, and Tal Rabin. Sequential composition of protocols without simultaneous termination. In *21st ACM PODC*, pages 203–212. ACM, 2002.

[LLR06] Yehuda Lindell, Anna Lysyanskaya, and Tal Rabin. On the composition of authenticated byzantine agreement. *Journal of the ACM*, 53(6):881–917, 2006.

[LLTW20] Yuan Lu, Zhenliang Lu, Qiang Tang, and Guiling Wang. Dumbo-mvba: Optimal multi-valued validated asynchronous byzantine agreement, revisited. In *39th ACM PODC*, pages 129–138. ACM, 2020.

[LSP82] Leslie Lamport, Robert E. Shostak, and Marshall C. Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, 1982.

[Mic17] Silvio Micali. Very simple and efficient byzantine agreement. In *ITCS 2017*, volume 4266 of *LIPIcs*, pages 6:1–6:1. Schloss Dagstuhl, 2017.

[MR90] Silvio Micali and Tal Rabin. Collective coin tossing without assumptions nor broadcasting. In *CRYPTO'90*, volume 537 of *LNCS*, pages 253–266. Springer, Heidelberg, 1990.

[MR17] Achour Mostéfaoui and Michel Raynal. Signature-free asynchronous byzantine systems: from multivalued to binary consensus with t< n/3, $O(n^2)$ messages, and constant time. *Acta Informatica*, 54(5):501–520, 2017.

[Nie02] Jesper Buus Nielsen. A threshold pseudorandom function construction and its applications. In *CRYPTO 2002*, volume 2442 of *LNCS*, pages 401–416. Springer, Heidelberg, 2002.

[Pat11] Arpita Patra. Error-free multi-valued broadcast and byzantine agreement with optimal communication complexity. In *15th OPODIS*, volume 7109 of *LNCS*, pages 34–49. Springer, 2011.

[PCR14] Arpita Patra, Ashish Choudhury, and C. Pandu Rangan. Asynchronous byzantine agreement with optimal resilience. *Distributed Computing*, 27(2):111–146, 2014.

[PSL80] Marshall C. Pease, Robert E. Shostak, and Leslie Lamport. Reaching agreement in the presence of faults. *Journal of the ACM*, 27(2):228–234, 1980.

[PW92] Birgit Pfitzmann and Michael Waidner. Unconditional byzantine agreement for any number of faulty processors. In *9th STACS*, volume 577 of *LNCS*, pages 339–350. Springer, 1992.

[Rab83] Michael O. Rabin. Randomized byzantine generals. In *24th FOCS*, pages 403–409. IEEE Computer Society Press, 1983.

[SLM+23] Shravan Srinivasan, Julian Loss, Giulio Malavolta, Kartik Nayak, Charalampos Papamanthou, and Sri Aravinda Krishnan Thyagarajan. Transparent batchable time-lock puzzles and applications to byzantine consensus. In *PKC 2023, Part I*, LNCS, pages 554–584. Springer, Heidelberg, 2023.

[TC84] Russell Turpin and Brian A. Coan. Extending binary byzantine agreement to multivalued byzantine agreement. *Information Processing Letters*, 18(2):73–76, 1984.

[WXDS20] Jun Wan, Hanshen Xiao, Srinivas Devadas, and Elaine Shi. Round-efficient byzantine broadcast under strongly adaptive and majority corruptions. In *TCC 2020, Part I*, volume 12550 of *LNCS*, pages 412–456. Springer, Heidelberg, 2020.

[WXSD20] Jun Wan, Hanshen Xiao, Elaine Shi, and Srinivas Devadas. Expected constant round byzantine broadcast under dishonest majority. In *TCC 2020, Part I*, volume 12550 of *LNCS*, pages 381–411. Springer, Heidelberg, 2020.

[Yao82] Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In *23rd FOCS*, pages 160–164. IEEE Computer Society Press, 1982.

A Attack on Ben-Or and El-Yaniv's Select Protocol

In this section, we begin by presenting a static adversary that disproves an important claim regarding the expected-constant round complexity for one of the main subroutines in Ben-Or and El-Yaniv's concurrent A-BA protocol [BE03]. Consequently, the assured expected-constant round complexity of their concurrent A-BA protocol is no longer valid. Furthermore, we demonstrate that when considering adaptive adversaries, attempting to argue even for weaker claims becomes futile. The attacks we present here consider a simple case with only four parties, one of which can be corrupted (respecting the bound $t < n/3$). To provide essential context for our attacks, we present some of the protocols nearly verbatim from [BE03] in Figures 10, 11, and 12.

Protocol $\Pi_{\text{a-cast}+}$

Common inputs: n, $t \leq (n-1)/3$; k (the identity of the transmitter)
Local input for processor p_i: none
Additional local input for processor p_k: V
Local output for processor p_i: $Value_i$, $Relay_i$

Epoch 1: (p_k only)

- A-Cast V.

Epoch 2: (Every processor p_i)

- Upon accepting a value v from a transmitter p, A-Cast ["*commit*", p, v].

Epoch 3: (Every processor p_i)

- Upon accepting $2t+1$ ["*commit*", p', v'] A-Casts from a set S of processors (transmitters), $Value_i \leftarrow v'$, $Relay_i \leftarrow S$, and return $Value_i, Relay_i$.

Figure 10: The A-Cast$^+$ protocol from [BE03, Fig. 3].

Next, we highlight that certain aspects of the attacks do not necessitate any corruption and can be executed solely by imposing appropriate delays. These aspects are common to both the static and adaptive attacks; thus, they form the initial focus of our analysis before we dive into the separate subsections for the static and adaptive attacks. Claims 7 and 8 formulate capabilities of adversaries only imposing delays maliciously.

Claim 7. *In any invocation of the $\Pi_{\text{a-cast}+}$ protocol, the adversary can arbitrarily assign different sets of participants of size $n-t$ to the Relay sets of honest parties' outputs by imposing appropriate delays. No corruption is necessary for this manipulation.*

Proof. To assign a set S of participants to the *Relay* set of an honest party p_i, the adversary can allow all the honest parties to accept the A-Cast initiated in Epoch 1 of $\Pi_{\text{a-cast}+}$. However, the adversary selectively delivers ["*commit*", $\cdot, \cdot$] messages from parties in set S to p_i before delivering any other ["*commit*", $\cdot, \cdot$] messages. □

Claim 8. *Let $P = \{p_1, p_2, p_3, p_4\}$ be the set of participants, v_i for $i \in [4]$ be the input of p_i, and $Relay_{i,j}$ for $i, j \in [4]$ be arbitrary subsets of P with size 3. The adversary can manipulate the output of the Π_{spread} protocol as follows solely through message scheduling. No corruption is necessary.*

$$p_1 \colon \langle (v_1, Relay_{1,1}), (v_2, Relay_{1,2}), (v_3, Relay_{1,3}), (v_4, Relay_{1,4}) \rangle$$
$$p_2 \colon \langle (v_1, Relay_{2,1}), (v_2, Relay_{2,2}), (v_3, Relay_{2,3}), (v_4, Relay_{2,4}) \rangle$$
$$p_3 \colon \langle (v_1, Relay_{3,1}), (v_3, Relay_{3,3}), (v_4, Relay_{3,4}) \rangle$$
$$p_4 \colon \langle (v_2, Relay_{4,2}), (v_3, Relay_{4,3}), (v_4, Relay_{4,4}) \rangle$$

Protocol Π_{spread}

Common inputs: n, $t \leq (n-1)/3$
Local input for processor p_i: V_i
Local output for processor p_i: $\langle X_1, X_2, \ldots, X_n \rangle$

Epoch 1:

- A-Cast$^+$ V_i.

Epoch 2:

- Wait until $2t+1$ values $V_{i_1}, \ldots, V_{i_{2t+1}}$ accepted (from $p_{i_1}, \ldots, p_{i_{2t+1}}$).
- A-Cast $\langle (p_{i_1}, V_{i_1}), \ldots, (p_{i_{2t+1}}, V_{i_{2t+1}}) \rangle$.
  Participate in the A-Cast of a vector $u = \langle (p_{j_1}, U_{j_1}), \ldots, (p_{j_{2t+1}}, U_{j_{2t+1}}) \rangle$ only if for every $1 \leq k \leq 2t+1$, U_{j_k} accepted from p_{j_k}.

Epoch 3:

- Wait until $t+1$ vectors $u_{l_1}, \ldots, u_{l_{2t+1}}$ [sic] accepted (from $p_{l_1}, \ldots, p_{l_{t+1}}$) such that for every $1 \leq k \leq t+1$ if $u_{l_k} = \langle (p_{k_1}, U_{k_1}), \ldots, (p_{k_{2t+1}}, U_{k_{2t+1}}) \rangle$, and for every $1 \leq r \leq 2t+1$, U_{k_r} accepted from p_{k_r}'s A-Cast$^+$.
- For every $1 \leq l \leq n$:
  - If a value V was accepted from p_l via A-Cast$^+$ then $X_l \leftarrow (V, \mathit{Relay}_{i,l})$ (where $(V, \mathit{Relay}_{i,l})$ is the output of A-Cast$^+$).
  - Else $X_l := \emptyset$.
- Return $\langle X_1, X_2, \ldots, X_n \rangle$.

Figure 11: The Spread protocol from [BE03, Fig. 4].

Proof. According to the description of Π_{spread}, for any $i, j \in [4]$, the j^{th} component of the output of p_i is either $\perp$ or is the output of $\Pi_{\mathsf{a\text{-}cast}^+}$ accepted from p_j (from Epoch 1). Since in each party's output all the available values corresponding to other parties are correct, the adversary does not need to make any changes to them. Moreover, based on Claim 7, the adversary can set the *Relay* set in the output of $\Pi_{\mathsf{a\text{-}cast}^+}$ to any arbitrary subset of participants as long as it has the correct size, which is 3. Since all the $\mathit{Relay}_{i,j}$ sets are of size 3, the adversary will not face any challenges setting them. Now we only need to demonstrate how the adversary can include and exclude inputs from different parties in each party's output to achieve the desired event. The adversary can accomplish this by carefully designing the order in which the parties accept the $\Pi_{\mathsf{a\text{-}cast}^+}$ messages from Epoch 1. The following steps outline the message delivery order:

- The adversary delivers the $\Pi_{\mathsf{a\text{-}cast}^+}$ messages to p_1 in the order: p_1, p_3, p_4, p_2.
- The adversary delivers the $\Pi_{\mathsf{a\text{-}cast}^+}$ messages to p_2 in the order: p_2, p_3, p_4, p_1.
- The adversary delivers the $\Pi_{\mathsf{a\text{-}cast}^+}$ messages to p_3 in the order: p_1, p_3, p_4, and delays the $\Pi_{\mathsf{a\text{-}cast}^+}$ message from p_2 until p_3 terminates.
- The adversary delivers the $\Pi_{\mathsf{a\text{-}cast}^+}$ messages to p_4 in the order: p_2, p_3, p_4, and delays the $\Pi_{\mathsf{a\text{-}cast}^+}$ message from p_1 until p_4 terminates.

By using this scheduling and delivering all the A-Cast$^+$ messages initiated in Epoch 2, the following outcomes occur:

- Parties p_1 and p_3 accept the vector $\langle (p_1, v_1), (p_3, v_3), (p_4, v_4) \rangle$ twice (once from p_1 and once from p_3 by the participation of p_1, p_2, p_3).

Protocol Π_{select}

Common inputs: n, $t \leq (n-1)/3$
Local input for processor p_i: V_i - an arbitrary value; $Pred_i(x)$ - a predicate
Local output for processor p_i: D_i

Epoch 1:

- $U_i \leftarrow V_i$ and run Spread on input U_i and let $View_i$ denote the local output.

Epoch 2:

- Run A-OLE. Let k be the output denoting the identity of the leader, p_k.

Epoch 3:

- $U \leftarrow View_i[k]$ (i.e., the value "related" to p_k upon termination of Spread).
- If U was accepted during the run of Spread and $\models Pred_i(U)$, then $R_i \leftarrow U$ and $U_i \leftarrow$ ["$deflected$", U, $Relay_i$], where $Relay_i$ is obtained by Spread (via A-Cast$^+$) for the accepted broadcast of the leader p_k.
- Else $R_i \leftarrow \emptyset$.
- Run A-BA on input R_i. Let D_i denote the local output.
- If $D_i \neq \emptyset$ then return D_i.

Epoch 4:

- A-Cast $View_i$ ($View_i$ defined in Epoch 1).
  Participate in admissible A-Casts only.

Epoch 5:

- Wait until $2t+1$ views, $View_{i_1}, \ldots, View_{i_{2t+1}}$ accepted.
- A-Cast U_i.

Epoch 6:

- Wait until $2t+1$ values accepted.
- If a ["$deflected$", U', $Relay$]-message was accepted and $p_k \in Relay$ (p_k is the leader from Epoch 2) and there are $t+1$ processors in $Relay$ which have a non-null value related to p_k in their accepted Views with the same value U' (if several such messages were accepted with different U' values take an arbitrary one), then $R_i \leftarrow U'$.
- Else $R_i := \emptyset$.

Epoch 7:

- Run A-BA on input R_i and let D_i denote the local output.
- If $D_i \neq \emptyset$ then return D_i.
- Else $U_i \leftarrow V_i$ and go to Epoch 1.

Figure 12: The Select protocol from [BE03, Fig. 5].

- Parties p_2 and p_4 accept the vector $\langle (p_2, v_2), (p_3, v_3), (p_4, v_4) \rangle$ twice (once from p_2 and once from p_4 by the participation of p_1, p_2, p_4).

Therefore, all parties terminate with the given output as stated in the claim. □

A.1 Static Attack

Π_{select} may involve multiple iterations, where parties either agree on a value and terminate, or restart the protocol. In the proof of the Π_{select} protocol, an event E is defined, which is claimed to occur with a constant probability. It is argued that when E happens in an iteration, all parties terminate. However, we demonstrate that this claim is not valid, resulting in uncertainty regarding the expected-constant round complexity guarantee of the Π_{select} protocol.

Assuming the preconditions for the Π_{select} protocol hold (i.e., for every non-faulty parties p_i and p_j, $\models Pred_j(V_i)$ and $V_i \neq \emptyset$), we will demonstrate that the argument regarding the round complexity is not valid. Let the static adversary $\mathcal{A}$ corrupt p_1 before the protocol begins. According to Claim 8, $\mathcal{A}$ can make parties terminate Π_{spread} in Epoch 1 of Π_{select} with the following outputs where $Relay_{1,2} = Relay_{4,2} = \{p_1, p_2, p_3\}$ (no corruption is required):

$$
\begin{aligned}
p_1 &: \langle (v_1, Relay_{1,1}), (v_2, Relay_{1,2}), (v_3, Relay_{1,3}), (v_4, Relay_{1,4}) \rangle \\
p_2 &: \langle (v_1, Relay_{2,1}), (v_2, Relay_{2,2}), (v_3, Relay_{2,3}), (v_4, Relay_{2,4}) \rangle \\
p_3 &: \langle (v_1, Relay_{3,1}), (v_3, Relay_{3,3}), (v_4, Relay_{3,4}) \rangle \\
p_4 &: \langle (v_2, Relay_{4,2}), (v_3, Relay_{4,3}), (v_4, Relay_{4,4}) \rangle
\end{aligned}
$$

Remark 9. Based on the properties of the Π_{spread} protocol, after the termination of the first honest party, there exist two subsets of participants, P_1 and P_2, satisfying the following conditions: P_1 only contains honest parties, $|P_1| = t + 1$, $|P_2| = 2t + 1$, and all the values from parties in P_2 are included in the output vector of all the parties in P_1.

Now let us assume that $\mathcal{A}$ allows p_4 to be the first to terminate Π_{spread} in Epoch 1 of the Π_{select} protocol. In this case, P_1 and P_2 could be $\{p_2, p_4\}$ and $\{p_2, p_3, p_4\}$, respectively.

In Epoch 2 of the Π_{select} protocol, a leader p_k is randomly chosen. The event E is defined as $p_k \in P_2 \cap (P - T)$ and it is claimed that if E occurs, the protocol terminates with the correct output. Since p_k is chosen randomly and $|P_2 \cap (P - T)| = t + 1$, the probability of the event E is at least $\frac{1}{3}$. Therefore, this claim suggests an expected-constant number of iterations (or asynchronous rounds).

However, we claim that when $p_k = p_2$, which satisfies E (since p_2 is honest and is in P_2), the protocol will start over instead of terminating. In the following, we explain the adversary's behavior in Epoch 3 to Epoch 7 of the Π_{select} protocol and provide a proof for our claim.

In Epoch 3 of Π_{select}, $\mathcal{A}$ can delay p_2 and assign a malicious value $v_2' \neq v_2$ to R_1. However, $\mathcal{A}$ allows p_1 to follow the protocol for the rest of its actions. As a result, the following state is observed:

- p_1: $R_1 = v_2'$ and $U_1 = (v_2, \{p_1, p_2, p_3\})$
- p_2: Delayed
- p_3: $R_3 = \perp$ and $U_3 = v_3$
- p_4: $R_4 = v_2$ and $U_4 = (v_2, \{p_1, p_2, p_3\})$

Consequently, the parties initiate the A-BA protocol with the inputs $(v_2', \text{delayed}, \perp, v_2)$. However, since there is no majority in the input values, we have no guarantee on the output of this A-BA protocol. In fact, as formulated in the A-BA ideal functionality, the adversary $\mathcal{A}$ can manipulate the protocol execution to make it output $\perp$ and prevent the termination of Π_{select}. Therefore, it is necessary to proceed to the next epoch, as the protocol cannot terminate at this stage.

In Epoch 4 of Π_{select}, $\mathcal{A}$ allows p_1 to follow the protocol. It should be noted that all the views in this epoch are admissible to everyone, as the components of all the views are either $\perp$ or the correct values. Therefore, all the views can be received by the honest parties. The only control that $\mathcal{A}$ has is over the order in which the views are received by the parties in the next epoch.

In Epoch 5 of Π_{select}, $\mathcal{A}$ allows p_1 to follow the protocol and strategically manages delays to achieve the following:

- Delivers $view_1, view_3, view_4$ to p_1 as its first $2t+1$ views.
- Delays the acceptance of any view for p_2 until the A-BA in Epoch 7 of Π_{select} is terminated.
- Delivers $view_1, view_3, view_4$ to p_3 as its first $2t+1$ views.
- Delivers $view_1, view_3, view_4$ to p_4 as its first $2t+1$ views.

Then, parties A-Cast values as follows based on the output they received from the Π_{spread} protocol in Epoch 1 of Π_{select}:

- p_1: $U_1 = (v_2, \{p_1, p_2, p_3\})$
- p_2: Still waiting from the previous epoch
- p_3: $U_3 = v_3$
- p_4: $U_4 = (v_2, \{p_1, p_2, p_3\})$

In Epoch 6 of Π_{select}, $\mathcal{A}$ lets p_1 follow the protocol, keeps p_2 waiting, and allows the remaining parties to receive each other's A-Cast messages. As a result, the following situation arises:

- p_1, p_3, p_4: Receive $(v_2, \{p_1, p_2, p_3\})$ from p_1, p_4, and v_3 from p_3.
- p_2: Still waiting from previous epochs

However, the "if" condition in Epoch 6 is not satisfied because only p_1 among $\{p_1, p_2, p_3\}$ has an accepted view that includes a value associated with p_2. Therefore, the following assignments are made:

- p_1, p_3, p_4: Assign $R_1 = R_3 = R_4 = \perp$.
- p_2: Still waiting from previous epochs

In Epoch 7 of Π_{select}, $\mathcal{A}$ allows p_1 to follow the protocol. Consequently, parties initiate the A-BA protocol with the following inputs:

- p_1, p_3, p_4: $\perp$
- p_2: Still waiting from previous epochs

As a result, parties complete the A-BA protocol and obtain the output $\perp$. Since the output is $\perp$, they have to start over, completing our attack.

A.2 Adaptive Attack

In the static attack, we demonstrated that the claim "for all possibilities for the set P_2, if the leader is an honest party in P_2, then the protocol terminates with the correct value" is not valid. We provided specific choices of the leader within certain possibilities for P_2 where the claim does not hold. This shows that the claim is incorrect in those cases.

In the adaptive attack, we further illustrate the difficulty in finding an argument for the weaker claim "there exists a possibility for P_2 such that if the leader is an honest party in P_2, then the protocol terminates with the correct values." We use the same setup with four parties, namely p_1, p_2, p_3, and p_4, and demonstrate that if either p_1 or p_2 is chosen as the leader, the adversary $\mathcal{A}$ can manipulate the protocol to start over instead of terminating. Since any legitimate set P_2 consists of three parties, it must include at least one of p_1 and p_2. Therefore, in any possible set P_2, there is an honest party whose selection as the leader does not guarantee termination. This shows the hopelessness of finding a valid argument for the weaker claim.

Assuming the preconditions for the Π_{select} protocol hold, we now consider adaptive corruption in this subsection. The adversary $\mathcal{A}$ does not corrupt any party before the leader is selected. If the chosen leader is p_2, then $\mathcal{A}$ follows the description of the static attack by corrupting p_1 and executing the attack as previously described.

However, if party p_1 is chosen as the leader, we can leverage symmetry and modify the adversary's description accordingly. We rename the parties as follows: $p'_1 := p_2$, $p'_2 := p_1$, $p'_3 := p_4$, and $p'_4 := p_3$. The adversary $\mathcal{A}$ corrupts p'_1 and runs the same static adversary code on the participant set $\{p'_1, p'_2, p'_3, p'_4\}$. Furthermore, it is important to note that in the static attack, we previously specified that $Relay_{1,2} = Relay_{4,2} := \{p_1, p_2, p_3\}$, while allowing $Relay_{2,1}$ and $Relay_{3,1}$ to be arbitrary since they were not essential to the attack and could take any value. However, in order to achieve full symmetry in the static attack and apply the aforementioned approach, $\mathcal{A}$ should now set $Relay_{2,1} = Relay_{3,1} := \{p_1, p_2, p_4\}$ in the description of the static attack.

With these adjustments, our adaptive adversary is complete.

B The Asynchronous Turpin-Coan Extension

Here, we investigate when the generic extension of binary to multi-valued synchronous BA (for $t < n/3$) given by Turpin and Coan [TC84] works in the asynchronous setting with eventual delivery. It turns out that an asynchronous version of the extension—with appropriate modifications—is secure when $t < n/5$, but is provably insecure for any $t \geq n/5$ regardless of which binary A-BA protocol is used. We remark that while our negative result is not exactly a lower bound, as the attack that we present is on a specific extension protocol, the fact that we lose two additive factors of t in resiliency (and even three, with a more naïveapproach) gives some evidence that more sophisticated techniques are needed to maintain optimal resiliency, as in [MR17]. Since our primary goal is to show that the Turpin-Coan extension cannot be used to get optimally resilient, multi-valued A-BA in expected-constant rounds, we choose to work with simpler, property-based definitions in this section.

We start by reviewing the original extension in [TC84], which requires just two additional rounds. Parties first distribute their inputs amongst one another, over P2P channels. An honest party, based on how many of the received values disagree with his own, considers himself either "perplexed" or "content," and announces this information. If enough parties claim to be perplexed, the honest party becomes "alert." The parties now run a binary BA protocol to agree on this last state (effectively, to determine if they all started with the same input), and depending on the

outcome they either output a default value, or are able to recover a common value from their local transcripts of the protocol.

Protocol $\Pi^V_{\mathsf{a\text{-}tc}}$

Local input of party p_i: $v_i \in V$, $|V| \geq 2$
Local output of party p_i: $v \in V$
Code for party p_i:

0. Initialize arrays $v[1..n]$ and $x[1..n]$ by filling them with a default value $\perp$.
1. **A-Cast** v_i.
2. Whenever v'_j is accepted from party p_j, record $v[j] := v'_j$.
3. Wait until $n - t$ values are accepted. Then, let $x_i := 1$ ("perplexed") if $v[j] \neq \perp$ and $v[j] \neq v_i$ for at least $t + 1$ different indices j, and otherwise let $x_i := 0$ ("content"). **A-Cast** (v_i, x_i).
4. Whenever (v'_j, x'_j) is accepted from party p_j, record $x[j] := x'_j$. If $v[j] = \perp$, then additionally record $v[j] := v'_j$.
5. Wait until $n - t$ pairs are accepted. Then, let $a_i := 1$ ("alert") if $x[j] = 1$ for at least $t + 1$ different indices j, and otherwise let $a_i := 0$. Run **binary A-BA** with input a_i.
6. If the binary computation agrees 1, then set v to be a predefined default value from V. Otherwise, if content set $v := v_i$, and if perplexed set v to be the majority value from the non-bottom entries in $v[]$ at indices j for which $x[j] = 0$. **Output** v.

Figure 13: The asynchronous Turpin-Coan extension.

Our asynchronous version of this extension, $\Pi_{\mathsf{a\text{-}tc}}$, is shown in Figure 13. We simply replace the basic message distribution mechanism with A-Cast, and account for the fact that adversarial A-Cast's may never terminate (i.e., honest parties should only expect to receive $n - t$ values). To avoid a somewhat artificial attack wherein the adversary can manipulate delays so that t entries are missing in an honest party's $v[]$ array and a *different* set of t entries are missing in the $x[]$ array, we require parties to re-send their input value in the second A-Cast. Note that this additional modification cannot *decrease* security, since honest parties will always use their actual input. In the following proposition, we prove the security of $\Pi_{\mathsf{a\text{-}tc}}$ for $t < n/5$. We emphasize that in the asynchronous setting we must impose relaxed termination requirements. However, since the modified extension is still deterministic and constant-round, any termination guarantees provided by the underlying binary A-BA protocol should be preserved; accordingly, we only prove the agreement and validity properties.

Proposition 10. *For any input domain V, protocol $\Pi^V_{\mathsf{a\text{-}tc}}$ securely implements multi-valued A-BA from A-Cast and binary A-BA, in constant rounds and in the presence of an adaptive and malicious t-adversary, provided $t < n/5$.*

Proof. The round complexity is easily established by inspection (considering A-Cast and binary A-BA to be ideal primitives). We now prove correctness:

Validity. If all honest parties begin with the same initial value v, then no honest party is perplexed and all honest parties are not alert. The binary computation agrees 0 and all honest parties (which are content) output v.

Agreement. There are two cases: the binary computation agrees either 1 or 0. In the former case, all honest parties output a common default value. For the latter case, we show that all content

parties have the same initial value, and that this value is correctly deduced by all the perplexed parties.

Note that each content party's input appears in at least $n - t - t = n - 2t$ positions in its $v[]$ array. Since at most t of these positions correspond to corrupted parties, we have that each content party has the same initial value as at least $n - 3t$ honest parties, which represent a majority of the honest parties when $n > 5t$. Of course there cannot be two distinct majorities, so all content parties must have the same initial value.

Furthermore, since the binary computation agrees 0, there must be at least $2t+1$ honest content parties, for otherwise there would be at least $n-3t$ honest perplexed parties and all honest parties would be alert (at least $n - 4t \geq t + 1$ of the corresponding entries in any honest party's $x[]$ array would not be $\perp$) and agreement would be on 1. Each perplexed party has $x[j] = 0$ or $x[j] = \perp$ for all honest content parties and possibly for some corrupted parties. Even in the worst case, when $x[j] = \perp$ for t of the honest content parties, there are still at least $2t + 1 - t = t + 1$ honest content parties left but at most t corrupted parties, so the content parties are a majority of those for which $x[j] = 0$ and $v[j] \neq \perp$. □

It is not difficult to see that when the predefined default value comes from outside of V, the resulting multi-valued A-BA protocol is actually *intrusion-tolerant* (see Section 1.2). We now show that $\Pi_{\mathsf{a\text{-}tc}}$ is insecure when $t \geq n/5$ (i.e., that the analysis above is tight). Our attack does not make any assumptions regarding the underlying binary A-BA protocol, other than that it satisfies the properties of A-BA. Moreover, we require only static corruptions, and somewhat surprisingly the attack considers only binary inputs (i.e., using the extension when $|V| = 2$ actually breaks the security of the binary protocol for $n/5 \leq t < n/3$).

Proposition 11. *For all input domains V, protocol $\Pi^V_{\mathsf{a\text{-}tc}}$ does NOT securely implement multi-valued A-BA from A-Cast and binary A-BA, in the presence of a static and malicious t-adversary, for any $t \geq n/5$.*

Proof. It suffices to consider the case $n = 5t$. We construct a distribution of inputs, a static adversary $\mathcal{A}$, and a message scheduling such that agreement is broken.

Let $\{p_1, \ldots, p_{5t}\}$ be the set of parties. Define four sets $A := \{p_1, \ldots, p_{2t}\}$, $B := \{p_{2t+1}, \ldots, p_{3t}\}$, $T := \{p_{3t+1}, \ldots, p_{4t}\}$, and $C := \{p_{4t+1}, \ldots, p_{5t}\}$. The parties in T are statically corrupted by $\mathcal{A}$ and instructed to start the protocol with input 0. Suppose the parties in A and B start with input 1, and parties in C with input 0. Now consider a message scheduling in which: 1) both A-Casts from parties in C get delayed for parties in A, 2) the A-Casted input values from $p_1, \ldots, p_t \in A$ get delayed for parties in B and C, 3) the A-Casted pairs from parties in C get delayed for parties in B, and 4) the A-Casted pairs from $p_{t+1}, \ldots, p_{2t} \in A$ get delayed for parties in C.

Observe that all parties in A will A-Cast that they are content. $\mathcal{A}$ also instructs parties in T to maliciously A-Cast that they are content. On the other hand, the parties in both B and C will A-Cast that they are perplexed. Then, no party in A or B will be alert, whereas all parties in C will be alert. We summarize all this information in Figure 14.

Consequently, if $\mathcal{A}$ instructs parties in T to run the binary A-BA protocol with input 0 (not alert), and delays messages from parties in C during the computation, then agreement will be on 0. Therefore, parties in A will output their initial value 1, while the parties in B and C will try to deduce the correct output from their arrays. All parties in B can do this successfully ($2t$ of the $3t$ relevant entries in the $v[]$ array will be 1). However, for parties in C, t of the $2t$ relevant entries will be 1 while the other t will be 0. □

It is possible to show that without the small modification in which parties A-Cast their input twice, the protocol is secure if and only if $t < n/6$. We have a method to extend binary to

	A_1	A_2	B	T	C	
A	1 $(1, \text{c})$	1 $(1, \text{c})$	1 $(1, \text{p})$	0 $(0, \text{c})$	$\perp$ $\perp$	not alert
B	$\perp$ $(1, \text{c})$	1 $(1, \text{c})$	1 $(1, \text{p})$	0 $(0, \text{c})$	0 $\perp$	not alert
C	$\perp$ $(1, \text{c})$	1 $\perp$	1 $(1, \text{p})$	0 $(0, \text{c})$	0 $(0, \text{p})$	alert

Figure 14: Summary of the A-Casts received by parties in A, B, and C, and their resulting alert status. The content and perplexed values are denoted by "c" and "p," respectively. Note that each column corresponds to a set of t parties (A_1 and A_2 denote $\{p_1, \ldots, p_t\}$ and $\{p_{t+1}, \ldots, p_{2t}\}$, respectively).

multi-valued A-BA in constant rounds for $t < n/4$, which is not much more complicated than the synchronous extension in [TC84] (although it requires *two* invocations of the binary protocol). However, as discussed in Section 3.2, to re-gain optimal resiliency $t < n/3$ we use the asynchronous extension of Mostéfaoui and Raynal [MR17]. We leave open the possibility of obtaining expected-constant-round multi-valued A-BA via other approaches, such as substituting our multi-valued OCC in the binary A-BA protocol from [CR93] (and making appropriate changes). In any case, we prefer the solution in [MR17] as it is a *black-box* reduction.