Related-Key Secure Pseudorandom Functions: The Case of Additive Attacks

Benny Applebaum* Eyal Widder*

June 17, 2014

Abstract

In a related-key attack (RKA) an adversary attempts to break a cryptographic primitive by invoking the primitive with several secret keys which satisfy some known relation. The task of constructing provably RKA secure PRFs (for non-trivial relations) under a standard assumption has turned to be challenging. Currently, the only known provably-secure construction is due to Bellare and Cash [5]. This important feasibility result is restricted, however, to linear relations over relatively complicated groups (e.g., $\mathbb{Z}_q^*$ where q is a large prime) that arise from the algebraic structure of the underlying cryptographic assumption (DDH/DLIN). In contrast, applications typically require RKA-security with respect to simple additive relations such as XOR or addition modulo a power-of-two.

In this paper, we partially fill this gap by showing that it is possible to deal with simple additive relations at the expense of relaxing the model of the attack. We introduce several natural relaxations of RKA-security, study the relations between these notions, and describe efficient constructions either under lattice assumptions or under general assumptions. Our results enrich the landscape of RKA security and suggest useful trade-offs between the attack model and the family of possible relations.

*School of Electrical Engineering, Tel-Aviv University, {benny.applebaum,wieyal}@gmail.com. Supported by ISF grant 1155/11, Israel Ministry of Science and Technology (grant 3-9094), and GIF grant 1152/2011.

1 Introduction

In a related-key attack (RKA) an adversary attempts to break a cryptographic primitive by invoking the primitive with several secret keys which satisfy some known relation. For example, the adversary may query a pseudorandom function under a tuple of keys $(k_1, \ldots, k_t)$ whose differences $\Delta_i = k_i - k_1 \pmod{2^n}$ are known, or even chosen by the adversary during the attack. Apart from being theoretically interesting, the study of RKAs is motivated by several scenarios.

- (Side channel attacks) In some cases, an adversary can mount a related-key attack by modifying the bits of the secret key (e.g., by tampering the hardware) and observing the resulting behavior. (See [18] and references therein.)
- (RKA as a working hypothesis) In practice, security against RKA has become a de-facto standard for block-ciphers. (The design of Rijndael, for example, explicitly stated RKA-security as a goal [14].) Correspondingly, systems are often designed while implicitly relying on the RKA-security of the underlying block-cipher. (See [5] and references therein).
- (RKA-security as a resource) Security against RKA allows *cheap and structured* re-keying mechanism – a feature which turns to be extremely useful for higher-level applications (cf. [31, 2, 1]).

RKAs were originally considered by Biham [9] and Knudsen [25] in the early 1990's, and since then have become commonly used in the cryptanalysis of symmetric cryptography [10, 11, 17, 24, 32]. Motivated by this state of affairs, Bellare and Kohno [7] initiated a theoretical study of RKA security for block ciphers, theoretically modeled by pseudorandom functions (PRFs) and pseudorandom permutations (PRPs) [20]. They defined RKA security with respect to a class of related-key-deriving (RKD) functions Φ which specify the key-relations available to the adversary, and considered an active (and adaptive) adversary who can choose the relation from Φ during the attack. The notion of RKA security was further extended to many other cryptographic primitives, and several constructions were introduced (cf. [19, 2, 21, 6, 8, 1]).

The task of constructing provably RKA secure PRFs (for non-trivial relations) under a standard assumption has turned to be challenging. For a while, the only positive results were based on ideal models or non-standard assumptions [7, 26, 19]. The situation has changed with the beautiful work of Bellare and Cash [5] who showed that RKA secure block ciphers can be based on standard cryptographic assumptions (e.g., the hardness of the DDH/DLIN problem). This important feasibility result is restricted, however, to linear relations over relatively complicated groups (e.g., $\mathbb{Z}_q^*$ where q is a large prime) that arise from the algebraic structure of the underlying cryptographic assumption (DDH/DLIN).

From an application point of view, such relations are somewhat unnatural. It is hard to imagine, for example, a hardware-tampering attack which manipulates the key in a way that corresponds to multiplication modulo a prime. Similarly, in practice, a cipher's key is typically "tweaked" by XOR-ing it with some public value or by treating it as a counter and increasing it by 1. Indeed, Bellare and Kohno [7] suggested XOR and addition modulo 2^n as the canonical examples of useful relations. The existence of RKA secure PRFs under such simple relations has been left open by previous works. Interestingly, the situation is completely different for randomized encryption, for which RKA-security under additive relations can be achieved in a relatively simple way [2].

1.1 Our Contribution

In this paper, we partially fill this gap by showing that it is possible to deal with simple additive relations at the expense of relaxing the model of the attack. We introduce various relaxations of RKA-security by putting different natural restrictions on the set of legal RKA queries (Δ, x). This include "passive" adversaries which are restricted to query $F_{k+\Delta}(x)$ with respect to random points x's or random shifts Δ's, "distinct" adversaries which are not allowed to query the same point x twice, and "bounded" adversaries which can use only a bounded number of different keys. We study the relations between these notions and present generic transformations between them. We also describe efficient constructions either for modular addition (over any large modulus) or, in the case of bounded adversaries, for any linear relation (including XOR). The security of these constructions is based on lattice assumptions or on general one-wayness assumptions. (A detailed account of our results appears below; see also Figure 1 for a summary.)

In a sense, our study takes the one-dimensional RKA-security game (which is solely parameterized by the RKD family Φ) and turns it into a multidimensional game. This enriches the landscape of RKA security, and provides a useful trade-off between the attack model and the family of possible relations.

1.1.1 RKA Secure Weak PRF

A weak PRF (wPRF) [27] is a relaxation of standard PRF which remains indistinguishable from a truly random function as long as it is being queried on random points. We construct a wPRF which offers RKA security with respect to mod-p addition over any (sufficiently large) integer modulus (including the case of $p = 2^n$). Our construction relies on the Learning with Rounding (LWR) assumption, introduced by Banerjee et al. [3], whose security can be based on the worst-case hardness of lattice problems. The construction and its proof are quite simple and efficient.

In a high-level, the LWR-based wPRF $F_s(x)$ computes the inner-product of the key $s \in \mathbb{Z}_q^n$ and the point $x \in \mathbb{Z}_q^n$ and outputs the result rounded to some integer grid (i.e., q is divided to r equal intervals and the output is rounded to the starting point of the corresponding interval). This function has an almost linear form which provides an "approximate" key-homomorphism, namely, $F_s(x) + F'_s(x)$ is close to $F_{s+s'}(x)$. This property, which was also used in [13], is extremely useful for proving RKA-security. Indeed, if we had an exact homomorphism we could emulate the value of $F_{s+\Delta}(x)$ given $F_s(x)$. A natural way to turn the approximate key-homomorphism into an exact homomorphism is to further round the result according to a grid with larger intervals. This gives an efficient mapping h from $F_s(x)$ and Δ to $F'_{s+\Delta}(x)$ where F' is the LWR wPRF parameterized with different "rounding resolution". The mapping h is almost always correct with respect to a random key and a random point. However, in our context the adversary can shift the key *arbitrarily*, and when the modulus p is composite (e.g., $p = 2^k$ and rounding is applied with respect to multiples of $2^{k'}$) there are shift vectors Δ for which h fails miserably. Fortunately, we note that such a rounding error happens only when the output of h is close to the end of an interval, hence we can detect a potential failure. Using sufficiently large intervals we can make sure that when h is applied to a truly random function the result is unlikely to fall next to an end of an interval. Hence, the failure of h (which prevents us from emulating an RKA oracle) allows us to directly distinguish the wPRF from a truly random function.

We further demonstrate the usefulness of our LWR-based RKA-wPRF by constructing a simple and efficient message-authentication code (MAC). Our construction follows the outline suggested

in [15] which relies on a key-homomorphic wPRF. While our wPRF does not support a full key-homomorphism in the strict sense of [15], we show how to adopt the RKA-security proof to prove the security of the resulting MAC. (This result appears in Section A.)

1.1.2 Passive-RKA secure PRF

Passive-RKA (pRKA) is a weak form of RKA which was previously considered in the cryptanalytic literature (see discussion in [12]) and in the context of randomized encryption [2]. In such attacks the key-relations are chosen randomly and are not controlled by the adversary. For example, in the case of linear relations, an adversary who asks for an RKA query on a point x will get as a result the value of $(\Delta, F_{k+\Delta}(x))$ where Δ is a random group element and k is the target key. (In a sense this is dual to the case of RKA secure wPRF where the point x is chosen at random and the shift Δ is chosen by the adversary.) We formalize the notion of pRKA security for PRFs, and show how to upgrade an RKA wPRF into a pRKA secure pseudorandom function or pseudorandom permutations (PRP). Combining this with our LWR-based construction we derive a PRF which is pRKA-secure under modular addition.

1.1.3 Distinct-RKA secure PRF

Given the aforementioned results, it is natural to ask whether RKA-wPRF can be further upgraded into standard RKA-PRFs. Unfortunately, Bellare et al. [6] show that this is impossible in general as there are relations Φ for which RKA security is achievable for wPRF, while any PRF can be successfully attacked via Φ-RKA. In light of this negative result, we try to find the strongest notion of RKA-security which can be carried from the wPRF setting to the standard PRF setting. Looking closely at the attack of [6] we see that the PRF is applied to the same point x under related keys. This motivates the notion of *distinct*-RKA (dRKA) secure PRFs where the adversary can actively choose the key relations and the input points x as long as no input appears twice. Namely, the adversary is allowed to apply a standard RKA on the PRF except that she is not allowed to query the value of a point x under different keys.

We describe a transformation which maps an RKA-wPRF and a standard PRF into a new PRF, and prove that if the resulting PRF fails to achieve dRKA-security, then a key-agreement protocol can be established (whose security holds for infinitely-many input lengths). Thus, in "Minicrypt" – the hypothetical world in which private-key cryptography exists but public-key cryptography does not exist – the existence of RKA-wPRF implies the existence of dRKA-PRFs. (This is similar in spirit to the results of [28, 29, 4].) Our transformation is generic and works for any class of RKD functions Φ. We leave open the question of upgrading dRKA security to RKA-security for concrete relations.

1.1.4 Bounded-RKA secure PRF

Finally, we consider the notion of *bounded-RKA* (bRKA) where there exists an a-priory bound t on the number of different related keys that the adversary can generate. (Each related key k_i can be queried with respect to arbitrarily many different x's.) We show that any PRF F can be immunized against t-bRKA attack, where $t(n)$ can be an arbitrary (a-priory fixed) polynomial. Furthermore, this holds for an arbitrary linear relation over any group (including the case of XOR).

The idea is to use a long key s of length $\Omega(tn)$ and derive an n-bit key k for F via an appropriate (public) key-derivation mechanism H. An adversary that uses the shifts $\vec{\Delta} = (\Delta_1, \ldots, \Delta_t)$ gets an access to F keyed by the keys $k_1 = H(s + \Delta_1), \ldots, k_t = H(s + \Delta_t)$, and, in addition, sees F keyed under the master key $k_0 = H(s)$. We show that if H is chosen from a family of $\Omega(nt^2)$-wise independent hash functions, then, for any choice of $\vec{\Delta}$, the joint distribution of the keys $(k_0, \ldots, k_t)$ is statistically indistinguishable from uniform. Hence, the bRKA security of the scheme reduces to the security of F under t independent keys, which follows from standard PRF security.

Our usage of ℓ-wise independent hash function is inspired by the work of Faust et al. [16], who showed that such hash functions give rise to *non-malleable key derivation*. In this setting the adversary is restricted to *one-time* tampering with respect to a *large* family of tempering functions G. Namely, it is allowed to view the underlying primitive under the key $h(g(s))$ where $g \in G$. In contrast, we allow the adversary to access many keys but restrict it to linear relations. As a result, we have to overcome some non-trivial technicalities which do not appear in [16].

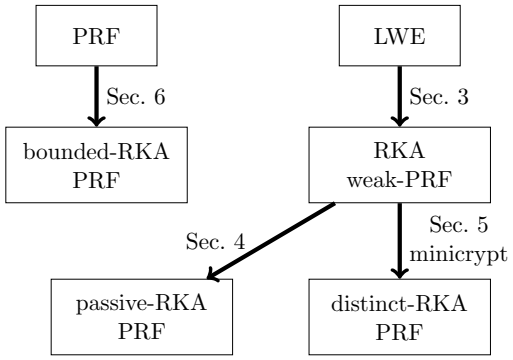

Figure 1: Results and Organization.

2 Preliminaries

Standard definitions. We say that a function $\mu : \mathbb{N} \to [0, 1]$ is *negligible* if for every positive polynomial p there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$, $\mu(n) \leq \frac{1}{p(n)}$. We let $\mathrm{neg}(n)$ denote some unspecified negligible function. A function $\mu : \mathbb{N} \to [0, 1]$ is noticeable if for some positive polynomial p there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$, $\mu(n) \geq \frac{1}{p(n)}$.

The statistical distance between two random variables X and Y over a domain Ω, denoted $\Delta(X; Y)$, is defined by

$$\Delta(X; Y) = \frac{1}{2} \cdot \sum_{u \in \Omega} \left| \Pr[X = u] - \Pr[Y = u] \right| .$$

We will say that X and Y are ε-close if $\Delta(X; Y) \leq \varepsilon$. Let $X = \{X_n\}_{n \in \mathbb{N}}$ and $Y = \{Y_n\}_{n \in \mathbb{N}}$ be sequences of probability distributions. Then X and Y are said to be *statistically indistinguishable* if $\Delta(X_n; Y_n) = \mathrm{neg}(n)$, and *computationally indistinguishable* if for every PPT distinguisher algorithm D, the distinguishing advantage $|\Pr[D(1^n, X_n) = 1] - \Pr[D(1^n, Y_n) = 1]|$ is negligible in n.

2.1 Pseudorandom Functions

Syntax. Let $X = \{X_n\}_{n\in\mathbb{N}}$, $Y = \{Y_n\}_{n\in\mathbb{N}}$, and $K = \{K_n\}_{n\in\mathbb{N}}$ be a sequence of finite sets. A function ensemble $\mathcal{F}$ from X to Y, indexed by keys from K, is a sequence of collections of functions $\{\mathcal{F}_n\}$ where for every n (security parameter) $\mathcal{F}_n = \{F_s : X_n \to Y_n\}_{s\in K_n}$. We always assume that the ensemble is efficiently computable and efficiently samplable. Namely, there exists an efficient sampler that given 1^n outputs a uniformly chosen element from K_n, and there exists an evaluation algorithm that given $s \in K_n$ and $x \in X_n$ outputs $y = F_s(x)$ in time polynomial in n. In the special case of *permutation* ensemble we assume that F_s forms a permutation over X_n and that there exists an efficient inversion algorithm which computes F_s^{-1}. Finally, we assume that the set of keys K_n is an additive Abelian group, and denote its group operation by $+$. By default, addition over K_n is assumed to be efficiently computable (in time poly(n)).

In the following, we define different security notions for PRFs. Since we mainly deal with linear relations, we will define RKA security explicitly for such relations. (All the following definitions can be extended to general related-key-deriving function families Φ as in [7].)

Weak PRF. An ensemble $\mathcal{F}$ is a *weak PRF* (wPRF) if for every PPT adversary A

$$\left| \Pr_{s\xleftarrow{R}K_n}[A^{\mathsf{Sam}F_s}(1^n) = 1] - \Pr[A^{\mathsf{R}(X_n,Y_n)}(1^n) = 1] \right| < \mathrm{neg}(n),$$

where the sampling oracle $\mathsf{Sam}F_s$ ignores its input and outputs a pair (x, y) where $x \xleftarrow{R} X_n$ and $y = F_s(x)$, and the random oracle $\mathsf{R}(X_n, Y_n)$ ignores its input and outputs a random pair $(x, y) \xleftarrow{R} (X_n \times Y_n)$.

RKA secure Weak PRF. An ensemble $\mathcal{F}$ is an *RKA weak PRF* (RKA-wPRF) if for every PPT adversary A

$$\left| \Pr_{s\xleftarrow{R}K_n}[A^{\mathsf{Sam}^+F_s}(1^n) = 1] - \Pr[A^{\mathsf{R}(X_n,Y_n)}(1^n) = 1] \right| < \mathrm{neg}(n),$$

where the related-key oracle Sam^+F_s takes $\Delta \in K_n$ as an input, and outputs a pair (x, y) where $x \xleftarrow{R} X_n$ and $y = F_{s+\Delta}(x)$.

Strong (standard) PRFs. An ensemble $\mathcal{F}$ is a *strong PRF* (or simply PRF) if for every PPT adversary A

$$\left| \Pr_{s\xleftarrow{R}K_n}[A^{F_s}(1^n) = 1] - \Pr[A^{\mathsf{R}(X_n\to Y_n)}(1^n) = 1] \right| < \mathrm{neg}(n),$$

where the (stateful) oracle $\mathsf{R}(X_n \to Y_n)$ initializes a random function $\rho : X_n \to Y_n$, and given a query $x \in X_n$ outputs the value $\rho(x)$. Without loss of generality, we may restrict our attention to adversaries A which do not repeat the same query twice, and in this case we may replace $\mathsf{R}(X_n \to Y_n)$ with the oracle $\mathsf{R}(Y_n)$ which ignores its query and outputs a random value in Y_n.

RKA secure PRFs. An ensemble $\mathcal{F}$ is a *RKA secure PRF* (RKA-PRF) if for every PPT adversary A

$$\left| \Pr_{s \xleftarrow{R} K_n} [A^{F_s^+}(1^n) = 1] - \Pr[A^{\mathsf{R}^+(X_n \to Y_n)}(1^n) = 1] \right| < \mathrm{neg}(n), \tag{1}$$

where the oracles are define as follows. The oracle F_s^+ takes $x \in X_n$ and $\Delta \in K_n$ as inputs, and outputs the value $y = F_{s+\Delta}(x)$. The stateful oracle $\mathsf{R}^+(X_n \to Y_n)$ initializes for each $s \in K_n$ a random function $\rho_s : X_n \to Y_n$, and, given a query $(x, \Delta) \in X_n \times K_n$ responds with $y = \rho_{s+\Delta}(x)$. Again, we may assume, without loss of generality, that a query (x, Δ) is never repeated twice, and in this case the oracle $\mathsf{R}^+(X_n \to Y_n)$ can be replaced with the oracle $\mathsf{R}(Y_n)$ which ignores its query and outputs a random value in Y_n.

Relaxations (bounded, passive and distinct RKA). We say that a PRF is $t(n)$-*bounded-RKA secure* (bRKA) if the above holds for adversaries that use at most t different shift vectors (but may apply the same shift vector more than once with different inputs.) We say that a PRF is *passive-RKA secure* (pRKA) if (1) holds for adversaries that each of their shift queries Δ_i is either set to zero or is chosen uniformly at random from K_n as part of the adversary's *public-coins*. Equivalently, we may assume that the random shift values are chosen by the oracle.

We say that a PRF is *distinct RKA secure* (dRKA) if Eq. 1 holds for adversaries that do not query the same point x twice. Namely, there are no two queries of the form (x, Δ) and (x, Δ').

Extensions. All the above definitions extend in the natural way to the case of pseudorandom permutations. In some cases, it is also useful to consider collections whose index consists of a *public-parameter* $p \in P_n$ in addition to a secret key $s \in K_n$. Namely, $\mathcal{F}_n = \{F_{s,p} : X_n \to Y_n\}_{s \in K_n . p \in P_n}$. In this case, we assume the existence of an efficient procedure which samples $p \xleftarrow{R} P_n$ in time $\mathrm{poly}(n)$. When defining security, we always assume that the public parameter p is chosen once and for all and is given to the adversary.

2.2 A weak-PRF based on Learning with Rounding

For any integer modulus $q \geq 2$ we let $\mathbb{Z}_q$ denote the quotient ring of integers modulo q. We let U_q denote the uniform distribution of $\mathbb{Z}_q$ and U_q^n denote the uniform distribution over $\mathbb{Z}_q^n$.

Learning with Errors and Learning with Rounding. For dimension n, modulus $q = q(n)$ and noise distribution $\chi = \chi(n)$ over $\mathbb{Z}_q$, the *(decisional) Learning With Errors* $\mathsf{LWE}_{n,q,\chi}$ [30] assumption asserts that the random oracle which outputs uniform samples from $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is computationally indistinguishable from the (stateful) LWE oracle T_s which is initialized with a random $s \xleftarrow{R} \mathbb{Z}_q$ and outputs samples $x \xleftarrow{R} \mathbb{Z}_q^n, y \xleftarrow{R} \langle s, x \rangle + \chi$. Namely, for every PPT A,

$$\left| \Pr_s[A^{T_s} = 1] - \Pr[A^{\mathsf{U}_q^n \times \mathsf{U}_q} = 1] \right| \leq \mathrm{neg}(n).$$

Following [3], we modify the LWE problem such that the noise distribution over $\mathbb{Z}_q$ is replaced with a deterministic rounding operation. The idea is to partition the elements $0, \ldots, q-1$ to

p consecutive intervals, and map an element to the starting point of its interval. Formally, for parameters $q > p$, we define the following mapping from $x \in \mathbb{Z}_q$ to an element in $\mathbb{Z}_p$ by

$$\lceil x \rfloor_{q/p} := \lfloor \bar{x} \cdot p/q \rfloor \bmod p,$$

where $\bar{x} \in \mathbb{Z}$ is any integer congruent to $x \bmod q$. Our notation slightly deviates from [3] as we would like to keep q explicit as part of the operation.

Definition 2.1 (The LWR Function)**.** *For integers $q > p$ and n, and a key $s \in \mathbb{Z}_q^n$ we let $F_s^{q,p} : \mathbb{Z}_q^n \to \mathbb{Z}_p$ be the mapping*

$$F_s^{q,p} : x \mapsto \lceil \langle s, x \rangle \rfloor_{q/p},$$

where $\langle x, s \rangle$ denotes inner-product, i.e., $\sum_i x_i \cdot s_i \bmod q$. For integer functions $q(n) > p(n)$, we define the function ensemble $\mathcal{F}^{q,p}$ over the domain/key-space $\mathbb{Z}_{q(n)}^n$ and range set $\mathbb{Z}_{p(n)}$, which for every n, consists of the functions $\left\{ F_s^{q(n),p(n)} : s \in \mathbb{Z}_{q(n)}^n \right\}$.

For ease of notation, we typically omit the dependency in the security parameter and write $F_s^{q,p}$.

In [3] it is proven that under the LWE assumption, $\mathcal{F}^{q,p}$ is a weak PRF. In the following, we say that a noise distribution $\chi = \chi_n$ over $\mathbb{Z}$ is $B(n)$-bounded if $\Pr[|\chi_n| > B(n)] < \mathrm{neg}(n)$.

Proposition 2.2 ([3])**.** *Assume that $\mathsf{LWE}_{n,q,\chi}$ holds for some B-bounded noise distribution χ and $q(n) > p(n) \cdot B(n) \cdot n^{\omega(1)}$. Then the collection $\mathcal{F}^{q,p}$ is a weak-PRF.*

The proposition does not impose any restriction regarding the structure of p and q (except for their size) and, in particular, holds for the case where p and q are powers of two.

The following proposition shows that when a uniformly chosen element from $\mathbb{Z}_q$ is projected down to $\mathbb{Z}_p$, either by taking modulo or by the rounding operation, the resulting element is almost uniformly distributed over $\mathbb{Z}_p$.

Proposition 2.3. *Let $p < q$ and let $\delta(p, q)$ be zero if p divides q, and $\frac{p}{2q}$ otherwise. Then, the random variable $\mathsf{U}_q \bmod p$ (resp., $\lceil \mathsf{U}_q \rfloor_{q/p}$) is $\delta(p, q)$-close to the uniform distribution over $\mathbb{Z}_p$.*

Proof. Observe that the modulo operation and the rounding operation are both "almost balanced" in the sense that each element in $\mathbb{Z}_p$ has either $\lceil q/p \rceil$ preimages or $\lfloor q/p \rfloor$ preimages. Assume that we have r values of the first type and $p - r$ values of the second type. Then, the statistical distance between the two distributions is

$$\frac{1}{2} \left| r \cdot \frac{\lceil q/p \rceil - q/p}{q} + (p - r) \cdot \frac{q/p - \lfloor q/p \rfloor}{q} \right|,$$

which is zero when p divides q, and is upper-bounded by $\frac{p}{2q}$, otherwise. □

3 RKA secure Weak-PRF

In this section we show that if the collection $\mathcal{F}^{q,r}$ is a weak PRF then, for a proper choice of parameters $q > r > p$, the collection $\mathcal{F}^{q,p}$ is a weak PRF which is secure under related-key attacks. The key idea is to map a random input/output pair (x, y) of $F_s^{q,r}$ and an RKA query Δ into a random input/output pair (x, y') of $F_{s+\Delta}^{q,p}$. The transformation is based on the following mapping.

The mapping h. For integers $q > r > p$ and n, we define the mapping $h : \mathbb{Z}_q^n \times \mathbb{Z}_r \times \mathbb{Z}_q^n \to \mathbb{Z}_p$ as follows:

$$h : (x, y, \Delta) \mapsto \lceil y + F_\Delta^{q,r}(x) \pmod r \rfloor_{r/p}. \tag{2}$$

Before we prove our main theorem, we collect several useful facts regarding the property of the mapping h. We begin by showing that when h is applied to a random pair $(x, y) \xleftarrow{R} \mathbb{Z}_q^n \times \mathbb{Z}_r$ then, regardless of Δ, the result is almost uniform over $\mathbb{Z}_p$ and independent of x.

Claim 3.1. *For $(x, y) \xleftarrow{R} \mathbb{Z}_q^n \times \mathbb{Z}_r$ and every $\Delta \in \mathbb{Z}_q^n$ the pair $(x, h(x, y, \Delta))$ is $\delta(p, r)$-close to $\mathsf{U}_q^n \times \mathsf{U}_p$, where $\delta(p, r)$ is zero if p divides r, and $\frac{p}{2r}$ otherwise.*

Proof. Since y is uniform and independent of x, the random variable $y + F_\Delta^{q,r}(x)$ is uniform (over $\mathbb{Z}_r$) and independent of x and so, by Proposition 2.3, the random variable $h(x, y, \Delta) = \lceil y + F_\Delta^{q,r}(x) \pmod r \rfloor_{r/p}$ is $\delta(p, r)$-close to uniform over $\mathbb{Z}_p$. □

Next we would like to show that when (x, y) is an input/output pair of $F_s^{q,r}$ then, whp, the output $h(x, y, \Delta)$ equals to $F_{s+\Delta}^{q,p}(x)$. Unfortunately, this claim does not hold for a non-prime modulus q. (See the discussion in the introduction.) Instead, we define an (efficiently recognizable) event that guarantees that h succeeds. Specifically, we will need the following claim.

Claim 3.2. *Let $p < r < q$. For every $s, \Delta, x \in \mathbb{Z}_q^n$, if the difference between $(F_s^{q,r}(x) + F_\Delta^{q,r}(x))$ to any multiple of r/p is at least 2, then $h(x, F_s^{q,r}(x), \Delta) = F_{s+\Delta}^{q,p}(x)$.*

Proof. First, we claim that the difference between $F_s^{q,r}(x) + F_\Delta^{q,r}(x)$ and $F_{s+\Delta}^{q,r}(x)$ is at most 2. Indeed,

$$\begin{aligned} F_s^{q,r}(x) + F_\Delta^{q,r}(x) &= \left\lfloor \langle x, s \rangle \cdot \frac{r}{q} \right\rfloor + \left\lfloor \langle x, \Delta \rangle \cdot \frac{r}{q} \right\rfloor \\ &= \langle x, s \rangle \cdot \frac{r}{q} + \langle x, \Delta \rangle \cdot \frac{r}{q} + e_1 + e_2 \\ &= \left\lfloor \langle x, s + \Delta \rangle \cdot \frac{r}{q} \right\rfloor + e_1 + e_2 + e_3 \\ &= F_{s+\Delta}^{q,r}(x) + e \end{aligned}$$

where the "error" terms $e_1, e_2 \in [-1, 0]$ and $e_3 \in [0, 1]$ compensate the omission/addition of the floor operation, and $e = e_1 + e_2 + e_3 \in [\pm 2]$ denotes the accumulated error.

Since $F_s^{q,r}(x) + F_\Delta^{q,r}(x)$ is 2-close to $F_{s+\Delta}^{q,r}(x)$, it follows, by our hypothesis, that both elements reside in the same r/p-interval. We can therefore write:

$$h(x, F_s^{q,r}(x), \Delta) = \lceil F_s^{q,r}(x) + F_\Delta^{q,r}(x) \rfloor_{r/p} = \lceil F_{s+\Delta}^{q,r}(x) \rfloor_{r/p} = F_{s+\Delta}^{q,p}(x)$$

and the claim follows. □

We can now prove the main theorem of this section.

Theorem 3.3. *Let $p < r < q$ such that $r/q < \mathrm{neg}(n)$, $p/r < \mathrm{neg}(n)$ and $1/p < \mathrm{neg}(n)$. Then if the collection $\mathcal{F}^{q,r}$ is a weak PRF then the collection $\mathcal{F}^{q,p}$ is RKA secure weak PRF.*

Proof. Fix some p, r, and q that satisfy the hypothesis. Assume, towards a contradiction, that A is an adversary that breaks the security of function $F_s^{q,p}$ as an RKA wPRF. Namely,

$$\Pr_s[A^{\mathsf{Sam}^+ F_s^{q,p}}(1^n) = 1] - \Pr_s[A^{\mathsf{R}(\mathbb{Z}_q^n, \mathbb{Z}_p)}(1^n) = 1] > \varepsilon(n),$$

for some non-negligible ε. We derive a contradiction by constructing an adversary B which distinguishes the oracle $\mathsf{Sam}F_s^{q,r}$ from the oracle $\mathsf{R}(\mathbb{Z}_q^n, \mathbb{Z}_r)$ with advantage $\varepsilon - \mathrm{neg}(n)$. The algorithm $B^{\mathcal{O}}$ emulates A, if A makes a query Δ to its oracle, the algorithm B asks for a sample $(x, y) \xleftarrow{R} \mathcal{O}$, and continues as follows:

- If the difference between $y + F_\Delta^{q,r}(x)$ to some multiple of r/p is smaller or equal to 2, then B quits with the output 1.
- Otherwise, B answers A with $(x, h(x, y, \Delta))$, where h is the mapping defined in Eq. (2).
- When reached the end of the emulation B halts with the same output as A.

Let us analyze the distinguishing advantage of B assuming that A makes $t = \mathrm{poly}(n)$ queries. First, observe that when $\mathcal{O}$ is the uniform oracle $\mathsf{R}(\mathbb{Z}_q^n, \mathbb{Z}_r)$, the probability that B quits is $t \cdot (4r/p)/r = \mathrm{neg}(n)$. Also, by Claim 3.1, conditioned on not quitting, the view of A in the emulation is within statistical distance of $t \cdot \delta(p, r) = \mathrm{neg}(n)$ from the view of A when the oracle is $\mathsf{R}(\mathbb{Z}_q^n, \mathbb{Z}_p)$. It, therefore, follows that

$$\Pr[B^{\mathsf{R}(\mathbb{Z}_q^n, \mathbb{Z}_r)}(1^n) = 1] \leq \Pr[A^{\mathsf{R}(\mathbb{Z}_q^n, \mathbb{Z}_p)}(1^n) = 1] + \mathrm{neg}(n).$$

We move on to the case where the oracle $\mathcal{O}$ is $\mathsf{Sam}F_s^{q,r}$. By Claim 3.2, if $B^{\mathsf{Sam}F_s^{q,r}}$ does not quit, the emulation is perfect. Letting $\delta = \Pr_s[B^{\mathsf{Sam}F_s^{q,r}}(1^n)$ quits], and recalling that when B quits it always outputs 1, we can write

$$\Pr_s[B^{\mathsf{Sam}F_s^{q,r}}(1^n) = 1] = \delta + \Pr_s[B^{\mathsf{Sam}F_s^{q,r}}(1^n) = 1| \text{ not quitting}] \cdot (1 - \delta) \geq \Pr_s[A^{\mathsf{Sam}^+ F_s^{q,p}}(1^n) = 1].$$

Overall, it follows that

$$\Pr_s[B^{\mathsf{Sam}F_s^{q,r}}(1^n) = 1] - \Pr_s[B^{\mathsf{R}(\mathbb{Z}_q^n, \mathbb{Z}_r)}(1^n) = 1] > \varepsilon(n) - \mathrm{neg}(n),$$

as required. □

4 Passive-RKA secure PRF and PRP

In this section we show how to convert any RKA-wPRF $\mathcal{F}$ (such as the one constructed in Section 3) into a strong PRF $\mathcal{G}$ with Passive-RKA security. The idea is similar to the one proposed in [19] (See also [5, 6]). Essentially, $\mathcal{F}$ is used as a key derivation mechanism for a standard PRF PRF. That is, our new PRF $\mathcal{G}$ will be keyed by pairs (k_1, k_2) and $\mathcal{G}_{k_1,k_2}(x) = \mathsf{PRF}_k(x)$ where the pseudorandom key k is taken to be $\mathcal{F}_{k_1}(k_2)$. A passive-RKA adversary that applies random shifts (Δ_1, Δ_2) to (k_1, k_2) will get an access to the function $\mathsf{PRF}_{k'}$ keyed under $k' = \mathcal{F}_{k_1+\Delta_1}(k_2 + \Delta_2)$. Due to the RKA-security of $\mathcal{F}$, the key k' will still be pseudorandom, and so, intuitively, $\mathsf{PRF}_{k'}$ remains secure. Furthermore, if PRF is a *pseudorandom permutation* (PRP), the resulting construction yields a passive-RKA secure PRP. We move on to a formal definition of our construction.

Construction 4.1. *Let* $\mathsf{PRF} = \{\mathsf{PRF}_k\}$ *be a function ensemble with key space* K*, domain* X *and range* Y*, and let* $\mathcal{F} = \{F_{k_1}\}$ *be a function ensemble with key space* K_1*, domain* K_2*, and range* K*. We define a new function ensemble* $\mathcal{G}$ *with key space* $K_1 \times K_2$ *domain* X *and range* Y *via the mapping:*

$$G_{(k_1,k_2)} : x \mapsto \mathsf{PRF}_k(x), \qquad \text{where } k = F_{k_1}(k_2).$$

Theorem 4.2. *If* PRF *is a PRF and* $\mathcal{F}$ *is an RKA secure wPRF, then* $\mathcal{G}$ *is a passive-RKA secure PRF. Moreover, if* PRF *is a PRP then* $\mathcal{G}$ *is a passive-RKA secure PRP.*

Proof. The proof relies on a hybrid argument. We define four sampling oracles which support standard PRF queries and passive-RKA (pRKA) queries. Syntactically, a PRF query $x \in X$ should be answered with $y \in Y$, and pRKA query $x \in X$ should be answered with $(\Delta_1, \Delta_2, y) \in K_1 \times K_2 \times Y$. The oracles are defined as follows. (For simplicity we omit the dependencies on n.)

- $\mathcal{O}^0_{(k_1,k_2)}$ is the passive-RKA oracle for the original G construction:
  - pRKA query $x \in X$ is answered with $(\Delta_1, \Delta_2) \xleftarrow{R} K_1 \times K_2$ and $y = \mathsf{PRF}_{k'}(x)$ where $k' = F_{k_1+\Delta_1}(k_2 + \Delta_2)$.
  - PRF query $x \in X$ is answered with $y = \mathsf{PRF}_k(x)$ where $k = F_{k_1}(k_2)$.
- $\mathcal{O}^1_k$ is a hybrid oracle:
  - pRKA query $x \in X$ is answered with $(\Delta_1, \Delta_2) \xleftarrow{R} K_1 \times K_2$ and $y = \mathsf{PRF}_{k'}(x)$ where $k' \xleftarrow{R} K$ is a fresh random key.
  - PRF query $x \in X$ is answered with $y = \mathsf{PRF}_k(x)$.
- $\mathcal{O}^2_k$ is a hybrid oracle:
  - pRKA query $x \in X$ is answered with $(\Delta_1, \Delta_2) \xleftarrow{R} K_1 \times K_2$ and $y \xleftarrow{R} Y$.
  - PRF query $x \in X$ is answered with $y = \mathsf{PRF}_k(x)$.
- $\mathcal{O}^3$ is the random sampling oracle:
  - pRKA query $x \in X$ is answered with $(\Delta_1, \Delta_2) \xleftarrow{R} K_1 \times K_2$ and $y \xleftarrow{R} Y$.
  - New PRF query $x \in X$ is answered with $y \xleftarrow{R} Y$, old PRF query is answered consistently with the previous answers.

Our goal is to show that the oracles $\mathcal{O}^0$ and $\mathcal{O}^3$ are indistinguishable. We begin by showing that the oracle $\mathcal{O}^0$ is indistinguishable from the oracle $\mathcal{O}^1$.

Claim 4.3. *For every PPT adversary* A*,*

$$\left| \Pr_{k_1,k_2}[A^{\mathcal{O}^0_{k_1,k_2}}(1^n) = 1] - \Pr_k[A^{\mathcal{O}^1_k}(1^n) = 1] \right| \leq \varepsilon(n),$$

for some negligible function $\varepsilon(n)$*.*

Proof. Assume, towards contradiction, that A has a non-negligible distinguishing advantage $\varepsilon(n)$. We construct an efficient PPT $B^{\mathcal{O}}$ that breaks the RKA wPRF security of $\mathcal{F}$. Namely, B distinguishes between the random oracle $\mathsf{R}(K_2, K)$ to the RKA wPRF oracle $\mathsf{Sam}^+F_{k_1}$ where $k_1 \xleftarrow{R} K_1$. The idea is to emulate A as follow:

1. B initially queries $\mathcal{O}$ with $\Delta = \mathbf{0}$ and obtains a random input/output pair $(k_2, k) \in K_2 \times K$.
2. If A makes a PRF query $x \in X$, then B returns the value $y = \mathsf{PRF}_k(x)$.
3. If A makes pRKA query $x \in X$, then B computes the answer (Δ_1, Δ_2, y) as follows. B chooses a random shift $\Delta_1 \xleftarrow{R} K_1$, uses the oracle to compute $(k_2', k') = \mathcal{O}(\Delta_1)$ and sets $\Delta_2 = k_2' - k_2$ and $y = \mathsf{PRF}_{k'}(x)$.
4. At the end of the emulation B terminates with the same output as A.

It is not hard to verify that if $\mathcal{O} = \mathsf{R}(K_2, K)$ then B perfectly emulates the oracle $\mathcal{O}_k^1$. On the other hand, when $\mathcal{O}$ is $\mathsf{Sam}^+F_{k_1}$ we obtain a perfect emulation of $\mathcal{O}^0_{(k_1,k_2)}$ for a randomly chosen $k_2 \xleftarrow{R} \mathcal{K}_2$. Indeed, since $k = F_{k_1}(k_2)$, PRF queries are answered properly by $\mathsf{PRF}_k(x)$. Similarly, the answer (Δ_1, Δ_2, y) to a pRKA query x, is computed properly as the shifts are random $(\Delta_1, \Delta_2) \xleftarrow{R} K_1 \times K_2$ and $y = \mathsf{PRF}_{k'}(x)$ for $k' = F_{k_1+\Delta_1}(k_2 + \Delta_2)$, as required. It follows that B breaks the RKA wPRF security of $\mathcal{F}$ in contraction to our assumption. □

We proceed by showing that $\mathcal{O}^1$ is indistinguishable from the oracle $\mathcal{O}^2$.

Claim 4.4. *For every PPT adversary A,*

$$\left| \Pr_k[A^{\mathcal{O}_k^1}(1^n) = 1] - \Pr_k[A^{\mathcal{O}_k^2}(1^n) = 1] \right| \leq \varepsilon(n),$$

for some negligible function $\varepsilon(n)$.

Proof. The security is reduced to the security of the PRF via a standard hybrid argument. Assume, towards contradiction, that A has a non-negligible distinguishing advantage $\varepsilon(n)$. Let $t(n) = \text{poly}(n)$ denote an upper bound on the number of queries that A performs, and assume, wlog, that A never repeats the same PRF query twice. Fix some n

We construct an efficient PPT $B^{\mathcal{O}}(1^n)$ that breaks the security of PRF, where its oracle $\mathcal{O}$ is either PRF_{k_1} or $\mathsf{R}(Y_n)$.

1. B samples a random key $k \xleftarrow{R} K_n$.
2. B chooses a random hybrid index $i \in \{1, \ldots, t(n)\}$, and emulates A as follows.
   (a) For the first $i - 1$ queries B ignores its oracle and answers as in $\mathcal{O}_k^2$:
      - If x is a pRKA query then B outputs $(\Delta_1, \Delta_2) \xleftarrow{R} K_1 \times K_2$ and $y \xleftarrow{R} Y$.
      - If x is a PRF query then B answers with $\mathsf{PRF}_k(x)$.

   (b) On the i-th query B answers as follows:
      - If x is a pRKA query then B outputs $(\Delta_1, \Delta_2) \xleftarrow{R} K_1 \times K_2$ and $y = \mathcal{O}(x)$.

- If x is a PRF query then B answers with $\mathsf{PRF}_k(x)$.

(c) For the remaining queries B ignores its oracle and answers as in $\mathcal{O}_k^1$:

- If x is a pRKA query then B outputs $(\Delta_1, \Delta_2) \xleftarrow{R} K_1 \times K_2$ and $y = PRF_{k'}(x)$ for a randomly sampled $k' \xleftarrow{R} K$.
- If x is a PRF query then B answers with $\mathsf{PRF}_k(x)$.

3. When A terminates B outputs the same output of A.

For $j \in \{1, \ldots, t\}$, let

$$\alpha_j(n) = \Pr_{k_1 \xleftarrow{R} K_n}[B^{\mathsf{PRF}_{k_1}}(1^n) = 1 | i = j] \qquad \text{and} \qquad \beta_j(n) = \Pr[B^{\mathsf{R}(Y_n)}(1^n) = 1 | i = j].$$

It is not hard to verify that $\alpha_1 = \Pr_k[A^{\mathcal{O}_k^1}(1^n) = 1]$ and that $\beta_t = \Pr_k[A^{\mathcal{O}_k^2}(1^n) = 1]$. Also, by definition, for every j, $\beta_j(n) = \alpha_{j+1}(n)$. Therefore, the distinguishing advantage of B (for a randomly chosen i) is $1/t \sum_j \alpha_j(n) - \beta_j(n) = (\alpha_1(n) - \beta_t(n))/t$ and so B breaks the security of PRF with noticeable advantage of $\varepsilon(n)/t(n)$, and we derive a contradiction. □

We proceed by showing that $\mathcal{O}^2$ is indistinguishable from the oracle $\mathcal{O}^3$.

Claim 4.5. *For every PPT adversary A,*

$$\left| \Pr_{k_1}[A^{\mathcal{O}_{k_1}^2}(1^n) = 1] - \Pr[A^{\mathcal{O}^3}(1^n) = 1] \right| \leq \varepsilon(n),$$

for some negligible function $\varepsilon(n)$.

Proof. Assume, towards contradiction, that A has a non-negligible distinguishing advantage $\varepsilon(n)$, and assume without loss of generality that A does not repeat the same query twice. We construct an efficient PPT $B^{\mathcal{O}}$ which distinguishes with advantage ε, between the oracle $\mathsf{R}(Y)$ to the oracle PRF_k for a randomly chosen $k \xleftarrow{R} K$.

1. B emulates A and answers its queries as follows:

   - If x is a pRKA query then B outputs $(\Delta_1, \Delta_2) \xleftarrow{R} K_1 \times K_2$ and $y \xleftarrow{R} Y$.
   - If x is a PRF query then B answers with a sample from the oracle $\mathcal{O}(x)$.

2. When A terminates B outputs the same output of A.

It is not hard to verify that when $\mathcal{O}$ is PRF_k we perfectly emulate $\mathcal{O}_k^2$ and when $\mathcal{O} = \mathsf{R}(Y)$ we perfectly emulate $\mathcal{O}^3$ and so the claim follows. □

By combining the three claims we complete the proof of the theorem. The proof naturally extends to the special case where PRF is a permutation since both claims still hold, and so, in this case. a pRKA secure PRP is obtained. □

5 Constructing dRKA secure PRFs in Minicrypt

In this section, we show that in Minicrypt one can transform an RKA secure wPRF $\mathcal{F}$ into a distinct-RKA secure PRF. That is, we transform RKA wPRF $\mathcal{F}$ (as provided in Section 3) and a standard PRF PRF into a function ensemble $\mathcal{H}$, and show that if $\mathcal{H}$ is not a dRKA-PRF, then an (infinitely-often) secure bit-agreement protocol exists.

Definition 5.1 (Bit-Agreement)**.** *Bit-agreement is a protocol between two efficient parties, Alice A and Bob B. At the beginning of the protocol the parties are given the security parameter 1^n as a common input, and at the end of the interaction, Alice and Bob both output a single bit $a \in \{0,1\}$ and $b \in \{0,1\}$, respectively. The protocol is ε-correct secure bit-agreement if the following holds:*

- *ε-Correctness:* $\Pr_{(a,b)\xleftarrow{R}(A,B)(1^n)}[a = b] \geq (1 + \varepsilon(n))/2$, *for all n's.*
- *Security: For every efficient adversary (eavesdropper) E and for all n*

$$\Pr[E(1^n, \tau_n) = b] \leq \frac{1}{2} + \mathrm{neg}(n),$$

where τ_n denotes the random variable representing the messages exchanged by Alice and Bob on a security parameter 1^n.

By default, we require that for every polynomial $p(n)$, $\varepsilon > 1 - 1/p(n)$ for all sufficiently large n's. If the above holds for infinitely many n's, then the protocol is called an infinitely-often bit-agreement.

Construction 5.2. *For function ensembles $\mathsf{PRF} : K \times X \to Y$ and $F : S \times Y \to Z$, define the ensemble H with key-space S, domain X, range Y and public parameter space K via the mapping*

$$H_{s,k} : x \mapsto F_s(\mathsf{PRF}_k(x)), \qquad \text{where } s \in S_n, x \in X_n, \text{ and } k \in K_n \text{ is a public parameter.}$$

Theorem 5.3. *Assume that F is an RKA wPRF and PRF is a (standard) PRF. Then, either H is a dRKA-PRF or there exists an infinitely-often bit-agreement protocol.*

Proof. Assume, towards a contradiction, that the construction H is not dRKA secure then there exists an efficient distinguisher D and a non-negligible function $\varepsilon(n)$ such that:

$$\Pr_{k\xleftarrow{R}K_n, s\xleftarrow{R}S_n}[D^{H^+_{s,k}}(1^n, k) = 1] - \Pr_{k\xleftarrow{R}K_n}[D^{\mathsf{R}(Z_n)}(1^n, k) = 1] \geq \varepsilon(n),$$

where D does not query a point x more than once. We define a bit-agreement protocol as follows. (See also Figure 5.)

Bit-agreement: Given security parameter 1^n the parties do the following:

- Initially, Bob selects a secret key $s \xleftarrow{R} S_n$ and a random bit $b \xleftarrow{R} \{0,1\}$.
- Alice chooses $k \xleftarrow{R} K_n$ and emulates $D(1^n, k)$.
- If D asks a query $(\Delta, x) \in S_n \times X_n$, Alice does the following:

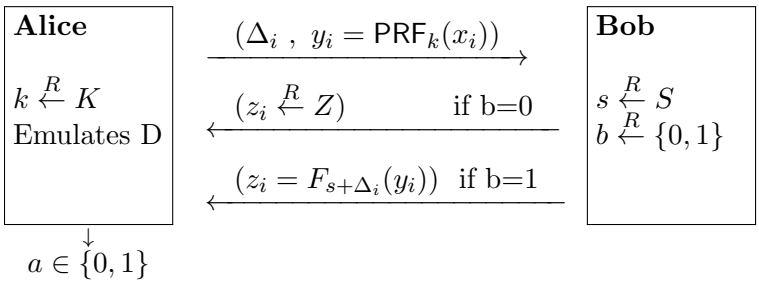

Figure 2: A two party bit-agreement based on a distinguisher D.

- Alice sends to Bob the message $(\Delta, y = \mathsf{PRF}_k(x))$.
- Bob responds with the value

$$z \leftarrow \begin{cases} H^k_{s+\Delta}(x) = F_{s+\Delta}(y) & \text{if } b = 1 \\ \mathsf{R}(Z_n) & \text{if } b = 0. \end{cases}$$

- Alice passes to D the answer z.

- Alice terminates with the output of D denoted by $a \in \{0,1\}$

Correctness. It is not hard to see that the parties agree with probability $\frac{1}{2} + \varepsilon/2$. Indeed,

$$\begin{aligned} \Pr[a = b] &= \Pr[b = 1] \cdot \Pr[a = 1 | b = 1] + \Pr[b = 0] \cdot \Pr[a = 0 | b = 0] \\ &= \frac{1}{2} \cdot (\Pr[a = 1 | b = 1] + 1 - \Pr[a = 1 | b = 0]) \\ &= \frac{1}{2} + \frac{1}{2} \cdot \left(\Pr_{s,k}[D^{H^+_s}(1^n, k) = 1] - \Pr_{k}[D^{\mathsf{R}(Z)}(1^n, k) = 1] \right) \geq \frac{1+\varepsilon}{2}. \end{aligned}$$

where the last equality follows by noting that when $b = 1$ the queries of D are answered according to $H^+_{s,k}$, and when $b = 0$ they are being answered according to $\mathsf{R}(Z)$.

Security. Next we show that our bit-agreement protocol is secure. Intuitively, an external adversary E who listens to the transcript just sees F_k evaluated on a pseudorandom points y_i (without knowing k), and therefore it should not be able to guess b due to the security of F_s as an RKA wPRF. We formalize this intuition below. Let $t = \text{poly}(n)$ denote the query complexity of D. Assume that E is an efficient adversary which guesses the bit b with probability $\frac{1}{2} + \delta(n)$ given the transcript

$$\tau_n = (\Delta_i, y_i, z_i)_{i=1}^t,$$

which is distributed according to the above protocol with security parameter 1^n. Observe that Alice can be implemented given an oracle access to PRF_k. It follows, by the security of the PRF, that

when the oracle to PRF_k is replaced with a random oracle $\mathsf{R}(X \to Y)$, the guessing probability of E does not change by more than negligible quantity. Hence, E guesses the bit b with probability at least $\frac{1}{2}+\delta(n)-\mathrm{neg}(n)$ even when the protocol is modified and the values of y_i are chosen uniformly at random. Let $\tau'_n(0)$ (resp., $\tau'_n(1)$) denote the distribution of the modified protocol conditioned on $b=0$ (resp., $b=1$). Then, we can write

$$\Pr[E(\tau'_n(b))=b] \geq \frac{1}{2}+\delta(n)-\mathrm{neg}(n),$$

where b is a random bit (the probability is also taken over the randomness used in the modified protocol and over the randomness of E). Equivalently, we can write

$$\Pr[E(\tau'_n(1))=1]-\Pr[E(\tau'_n(0))=1] \geq 2\delta(n)-\mathrm{neg}(n). \tag{3}$$

We can now combine E and D into an adversary $\mathcal{A}$ which violates the RKA security of F as a wPRF. Indeed, let $\mathcal{A}^{\mathcal{O}}$ be the adversary which distinguishes the RKA wPRF oracle Sam^+F_s from the random oracle $\mathsf{R}(Y,Z)$ as follows. Emulate $D(1^n)$, upon a query (Δ_i, x_i), the adversary $\mathcal{A}$ calls its oracle with Δ_i and obtains the value $(y_i, z_i) = \mathcal{O}(\Delta_i)$, and passes z_i to D. At the end of the emulation, apply E to the transcript $(\Delta_i, y_i, z_i)_{i=1}^t$ and output the result. It is not hard to verify that if $\mathcal{O} = \mathsf{Sam}^+F_s$ then E receives a transcript which is distributed exactly as in $\tau'_n(1)$, and if $\mathcal{O} = \mathsf{R}(Y,Z)$ then the transcript is distributed exactly as in $\tau'_n(0)$. It follows, by Eq. 3, that E breaks the RKA security of F as a wPRF, and we derive a contradiction.

Note that the above argument fails if D is allowed to query the same point x twice, as in this case we cannot replace the value $y = \mathsf{PRF}_k(x)$ with a random point, and so we cannot switch the PRF oracle PRF_k with a random oracle $\mathsf{R}(X \to Y)$.

We conclude that the bit-agreement is secure and that the honest parties agree on the bit with probability $\frac{1}{2} + 1/\mathrm{poly}(n)$ for infinitely many n's. Such a bit-agreement can be amplified into to standard (infinitely-often) key-agreement protocol with negligible error probability via the use of error-correcting codes, e.g., by repetition. (See also [23] for a more general transformation). □

6 Bounded-RKA secure PRF

In this section we show how to immunize any standard PRF (or PRP) $\mathsf{PRF} : K \times X \to Y$ against a bounded related-key attack which makes use of at most t related keys, where $t(n)$ is an arbitrary (a-priory fixed) polynomial in the security parameter. (This will hold for any arbitrary additive relation, including XOR, and addition modulo 2^n.) The idea is to use a long key s taken from a large key-space S (larger than K^t) and use some public hash function h to derive a shorter key $h(s) \in K$ for PRF.

Let us say that h is t-good if for any t-tuple of distinct shifts $(\Delta_1, \ldots, \Delta_t)$, the joint distribution of all the keys

$$(h(s), h(s+\Delta_1), \ldots, h(s+\Delta_t)), \tag{4}$$

induced by a random choice of $s \stackrel{R}{\leftarrow} S_n$, is ε-close in statistical distance to the uniform distribution over K_n^{t+1} for some negligible function $\varepsilon(n)$. It is not hard to verify that if h is t-good, then the resulting PRF is t-bounded RKA secure. In fact, it will be useful to consider a collection of hash function $H = \{H_z\}$ such that, with all but negligible probability, $H_z \stackrel{R}{\leftarrow} H$ is t-good. We refer to such an ensemble as t-good.

Lemma 6.1. *For a pseudorandom function* $\mathsf{PRF} : K \times X \to Y$ *and* t*-good ensemble* $H : Z \times S \to K$*, define the ensemble* G *with key-space* S*, domain* X*, range* Y *and public parameter space* Z *via the mapping*

$$G_{s,z} : x \mapsto \mathsf{PRF}_k(x), \qquad \text{where } k = H_z(s), s \in S_n, x \in X_n, \text{ and } z \in Z_n \text{ is a public parameter.}$$

Then, the PRF G *is secure against* t*-bounded RKA.*

Proof. Let A be a PPT RKA-adversary that uses at most t-distinct shifts and ε-breaks G, namely,

$$\Pr_{s \xleftarrow{R} K_n, z \xleftarrow{R} Z_n}[A^{G^+_{s,z}}(1^n, z) = 1] - \Pr_{z \xleftarrow{R} Z_n}[A^{\mathsf{R}^+(X_n \to Y_n)}(1^n, z) = 1] > \varepsilon(n),$$

for some non-negligible function $\varepsilon(n)$. For $\vec{k} = (k_0, \ldots, k_t) \in K_n^{t(n)+1}$, define the following (stateful) oracle $\mathcal{O}_{\vec{k}}$. Given a standard (non-RKA) query x, the oracle $\mathcal{O}_{\vec{k}}$ answers with $\mathsf{PRF}_{k_0}(x)$. To deal with RKA queries the oracle keeps track of the t different shifts $(\Delta_1, \ldots, \Delta_t)$ used by the adversary, and answers an RKA query (Δ_i, x) with $\mathsf{PRF}_{k_i}(x)$. (The oracle dynamically builds the list of seen Δ's.) Since H is t-good, we have that

$$\Pr_{\vec{k} \xleftarrow{R} K_n^{t(n)+1}}[A^{\mathcal{O}_{\vec{k}}}(1^n, z) = 1] > \Pr_{s \xleftarrow{R} K_n, z \xleftarrow{R} Z_n}[A^{G^+_s}(1^n, z) = 1] - \mathrm{neg}(n).$$

Assume (without loss of generality) that A does not repeat the same query (Δ, x) twice. Then, A distinguishes with non-negligible advantages between $\mathcal{O}_{\vec{k}}$, for a random key-vector $\vec{k}$, to a random oracle $\mathsf{R}(Y_n)$. It is not hard to show (via a standard hybrid argument) that this violates the security of the PRF PRF. □

The following lemma shows that an $\Omega(t^2 \log(|K|))$-wise independent hash function with a sufficiently large domain is t-good.

Lemma 6.2. *Let* $t = \mathrm{poly}(n)$*, and let* H *be an ensemble of* ℓ*-wise independent hash function with domain* $S = \{S_n\}$ *and range* $K = \{K_n\}$ *where* $\ell \geq n(2t+2)(t+1)$*,* $|K_n| = 2^n$ *and* $|S_n| = 2^{(2t+6)n}$*. Then* H *is* t*-good. In particular, for all but a* 2^{-n} *fraction of the functions in* H*, the distribution (4) is* $2^{-0.99n}$*-close to uniform.*

Proof. Fix a sequence of distinct non-zero shifts $(\Delta_1, \ldots, \Delta_t)$. It will be convenient to let $\Delta_0 = 0$ and set $\vec{\Delta} = (\Delta_0, \Delta_1, \ldots, \Delta_t)$. To simplify notation, we use lower-case h to denote a function H_z from the collection H. We say that $h \in H$ is ε-good for $\vec{\Delta}$ if for a random s, the distribution $(h(s + \Delta_i))_{0 \leq i \leq t}$ is ε-close to the uniform distribution over K^{t+1}. In order to bound the statistical distance, we prove the following claim.

Claim 6.3. *For all but* $2^{-n(t+1))}$*-fraction of the* h*'s the following holds. For every vector of (not necessarily distinct) keys* $\vec{k} = (k_0, \ldots, k^t) \in K^{t+1}$*,*

$$\Pr_s\left[\bigwedge_{i=0}^{t} h(s + \Delta_i) = k_i\right] \in \left(\frac{1}{|K|^{t+1}} \cdot (1 \pm 2^{-0.99n})\right).$$

Proof. Fix some vector of keys $\vec{k} \in K^{t+1}$. For every $s \in S$ define a random variable χ_s which takes the value 1 if $h(s+\Delta_i) = k_i$ for every $0 \le i \le t$, where $h \xleftarrow{R} H$. Observe that the random variable (induced by a choice of h) $\Pr_s[\bigwedge_{i=0}^{t} h(s+\Delta_i) = k_i]$ can be written as $\bar{\chi} = \sum_{s\in S} \chi_s/|S|$. We will show that

$$\Pr_h\left[\bar{\chi} \notin \left(\frac{1}{|K|^{t+1}}(1 \pm 2^{-0.99n})\right)\right] \le 2^{-n(2t+2)}. \tag{5}$$

Note that Claim 6.3 follows from (5) by applying a union-bound over all $2^{(t+1)n}$ possible $\vec{k} \in K^{t+1}$.

To prove (5) we make the following observations. First, since H is ℓ-wise independent and $\ell > t+1$, we have that $E[\chi_s] = 1/|K|^{t+1}$ for every s, and, so, by the linearity of expectation, $\mathsf{E}(\bar{\chi}) = 1/|K|^{t+1}$. We would like to show that the average of χ_s is concentrated around its expectation. Note that the random variables χ_s's are not even pair-wise independent. Indeed, consider s and s' for which $s+\Delta_i = s'+\Delta_j$ for some $i \neq j$. Then, the i-th coordinate of the random variable $(h(s+\Delta_0), \ldots, h(s+\Delta_t))$ equals to the j-th coordinate of the random variable $(h(s'+\Delta_0), \ldots, h(s'+\Delta_t))$ and as a result χ_s is not statistically independent from $\chi_{s'}$. Fortunately, we can show that, apart from these local dependencies, the χ's are r-wise independent, for $r = (\ell/(t+1)) \ge 2t+2$, which still yield a strong concentration (cf. [22]). We proceed with a formal proof.

Define a simple graph G over $s \in S$ by putting an edge between s and s' if $s+\Delta_i = s'+\Delta_j$ for some $i \neq j$. Observe that the degree of each node in the graph is at most $d = (t+1)^2$. We claim that for every independent set I in the graph, the random variables $\{\chi_s : s \in I\}$ are r-wise independent. In the terminology of [22], the random variables *r-agree* with G. Indeed, for any independent set I, and for any r-subset $(s_1, \ldots, s_r) \subseteq I$, the value of each of the the random variables $\chi_{s_1}, \ldots, \chi_{s_r}$ solely depends on the value of h on a set of $t+1$ distinct points $\{s_j+\Delta_0, \ldots, s_j+\Delta_{t+1}\}$. These sets of points are distinct (since I is an independent set) and so their images under h are statistically independent since h is ℓ-wise independent for $\ell = r \cdot (t+1)$. It therefore, follows that $\chi_{s_1}, \ldots, \chi_{s_r}$ are statistically independent.

Having shown that the χ_s's agree with G, we can apply Corollary 3.2 of [22] and conclude that

$$\Pr_h[\bar{\chi} \notin \frac{1}{|K|^{t+1}}(1 \pm \delta)] \le 4\sqrt{\pi r}\left(\frac{|K|^{t+1}\sqrt{(d+1)r}}{\delta\sqrt{|S|}}\right)^r.$$

For $\delta = 2^{-0.99n}$, $|K| = 2^n$, $|S| = 2^{(2t+6)n}$, and $r, t \in \mathrm{poly}(n)$, the RHS is upper-bounded by $2^{-nr} \le 2^{-n(2t+2)}$, for all sufficiently large n's, and (5) follows. □

We can now complete the proof of the lemma. First, observe that any h that satisfies the lemma is $2^{-0.99n}$-good for $\vec{\Delta}$. Indeed, for such an h, the probability distribution $(h(s+\Delta_i))_{0\le i\le t}$ assigns to each outcome $\vec{k}$ a weight which corresponds to its weight under the uniform distribution up to a multiplicative factor of $1 \pm 2^{-0.99n}$. It is not hard to show that in this case the statistical distance is at most $2^{-0.99n}$. Therefore, all but $2^{-n(t+1))}$-fraction of the h's are $2^{-0.99n}$-good for $\vec{\Delta}$. By applying a union bound over all possible 2^{nt} shift vectors, we conclude that all but 2^{-n}-fraction of the h's are $2^{-0.99n}$-good, and the lemma follows. □

By combining Lemmas 6.1, 6.2 with any efficient construction of ℓ-wise independent hash function (e.g., based on Reed-Solomon codes), we obtain the following theorem.

Theorem 6.4. *Let $K = \{(K_n, +_n)\}$ be a sequence of efficiently computable additive groups, and let $t(n)$ be an arbitrary poynomial. Then, assuming the existence of a PRF $\mathsf{PRF} : K \times X \to Y$, there exists a t-bounded-RKA secure PRF with respect to addition over K.*

Specifically, assuming the existence of a one-way function, we can achieve bounded-RKA security with respect to XOR or addition modolu 2^n.

Acknowledgement. We thank Daniel Wichs for a detailed discussion about [16].

References

[1] Benny Applebaum. Garbling XOR gates "for free" in the standard model. In Amit Sahai, editor, *TCC 2013*, volume 7785 of *LNCS*, pages 162–181, Tokyo, Japan, March 3–6, 2013. Springer, Berlin, Germany.

[2] Benny Applebaum, Danny Harnik, and Yuval Ishai. Semantic security under related-key attacks and applications. In Bernard Chazelle, editor, *ICS 2011*, pages 45–60, Tsinghua University, Beijing, China, January 7–9, 2011. Tsinghua University Press.

[3] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 719–737, Cambridge, UK, April 15–19, 2012. Springer, Berlin, Germany.

[4] Boaz Barak, Yevgeniy Dodis, Hugo Krawczyk, Olivier Pereira, Krzysztof Pietrzak, François-Xavier Standaert, and Yu Yu. Leftover hash lemma, revisited. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 1–20, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Berlin, Germany.

[5] Mihir Bellare and David Cash. Pseudorandom functions and permutations provably secure against related-key attacks. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 666–684, Santa Barbara, CA, USA, August 15–19, 2010. Springer, Berlin, Germany.

[6] Mihir Bellare, David Cash, and Rachel Miller. Cryptography secure against related-key attacks and tampering. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 486–503, Seoul, South Korea, December 4–8, 2011. Springer, Berlin, Germany.

[7] Mihir Bellare and Tadayoshi Kohno. A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 491–506, Warsaw, Poland, May 4–8, 2003. Springer, Berlin, Germany.

[8] Mihir Bellare, Kenneth G. Paterson, and Susan Thomson. RKA security beyond the linear barrier: IBE, encryption and signatures. In Xiaoyun Wang and Kazue Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 331–348, Beijing, China, December 2–6, 2012. Springer, Berlin, Germany.

[9] Eli Biham. New types of cryptoanalytic attacks using related keys (extended abstract). In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 398–409, Lofthus, Norway, May 23–27, 1993. Springer, Berlin, Germany.

[10] Eli Biham, Orr Dunkelman, and Nathan Keller. New cryptanalytic results on IDEA. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 412–427, Shanghai, China, December 3–7, 2006. Springer, Berlin, Germany.

[11] Eli Biham, Orr Dunkelman, and Nathan Keller. A unified approach to related-key attacks. In Kaisa Nyberg, editor, *FSE 2008*, volume 5086 of *LNCS*, pages 73–96, Lausanne, Switzerland, February 10–13, 2008. Springer, Berlin, Germany.

[12] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir. Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 299–319, French Riviera, May 30 – June 3, 2010. Springer, Berlin, Germany.

[13] Dan Boneh, Kevin Lewi, Hart William Montgomery, and Ananth Raghunathan. Key homomorphic PRFs and their applications. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 410–428, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Berlin, Germany.

[14] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[15] Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, and Daniel Wichs. Message authentication, revisited. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 355–374, Cambridge, UK, April 15–19, 2012. Springer, Berlin, Germany.

[16] Sebastian Faust, Pratyay Mukherjee, Daniele Venturi, and Daniel Wichs. Efficient non-malleable codes and key-derivation for poly-size tampering circuits. In *EUROCRYPT 2014*, LNCS, pages 111–128. Springer, Berlin, Germany, 2014.

[17] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 213–230, New York, NY, USA, April 10–12, 2000. Springer, Berlin, Germany.

[18] Rosario Gennaro, Anna Lysyanskaya, Tal Malkin, Silvio Micali, and Tal Rabin. Algorithmic tamper-proof (ATP) security: Theoretical foundations for security against hardware tampering. In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 258–277, Cambridge, MA, USA, February 19–21, 2004. Springer, Berlin, Germany.

[19] David Goldenberg and Moses Liskov. On related-secret pseudorandomness. In Daniele Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 255–272, Zurich, Switzerland, February 9–11, 2010. Springer, Berlin, Germany.

[20] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33:792–807, 1986.

[21] Vipul Goyal, Adam O'Neill, and Vanishree Rao. Correlated-input secure hash functions. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 182–200, Providence, RI, USA, March 28–30, 2011. Springer, Berlin, Germany.

[22] Ronen Gradwohl and Amir Yehudayoff. t-wise independence with local dependencies. *Information Processing Letters*, 106(5):208–212, 2008.

[23] Thomas Holenstein. Key agreement from weak bit agreement. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 664–673, Baltimore, Maryland, USA, May 22–24, 2005. ACM Press.

[24] Goce Jakimoski and Yvo Desmedt. Related-key differential cryptanalysis of 192-bit key AES variants. In Mitsuru Matsui and Robert J. Zuccherato, editors, *SAC 2003*, volume 3006 of *LNCS*, pages 208–221, Ottawa, Ontario, Canada, August 14–15, 2003. Springer, Berlin, Germany.

[25] Lars R. Knudsen. Cryptanalysis of LOKI. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, *ASIACRYPT'91*, volume 739 of *LNCS*, pages 22–35, Fujiyoshida, Japan, November 11–14, 1991. Springer, Berlin, Germany.

[26] Stefan Lucks. Ciphers secure against related-key attacks. In Bimal K. Roy and Willi Meier, editors, *FSE 2004*, volume 3017 of *LNCS*, pages 359–370, New Delhi, India, February 5–7, 2004. Springer, Berlin, Germany.

[27] Moni Naor and Omer Reingold. Synthesizers and their application to the parallel construction of pseudo-random functions. In *36th FOCS*, pages 170–181, Milwaukee, Wisconsin, October 23–25, 1995. IEEE Computer Society Press.

[28] Krzysztof Pietrzak. Composition implies adaptive security in minicrypt. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 328–338, St. Petersburg, Russia, May 28 – June 1, 2006. Springer, Berlin, Germany.

[29] Krzysztof Pietrzak and Johan Sjödin. Weak pseudorandom functions in minicrypt. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *ICALP 2008, Part II*, volume 5126 of *LNCS*, pages 423–436, Reykjavik, Iceland, July 7–11, 2008. Springer, Berlin, Germany.

[30] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93, Baltimore, Maryland, USA, May 22–24, 2005. ACM Press.

[31] Liting Zhang, Wenling Wu, Peng Wang, Lei Zhang, Shuang Wu, and Bo Liang. Constructing rate-1 MACs from related-key unpredictable block ciphers: PGV model revisited. In Seokhie Hong and Tetsu Iwata, editors, *FSE 2010*, volume 6147 of *LNCS*, pages 250–269, Seoul, Korea, February 7–10, 2010. Springer, Berlin, Germany.

[32] Wentao Zhang, Lei Zhang, Wenling Wu, and Dengguo Feng. Related-key differential-linear attacks on reduced AES-192. In K. Srinathan, C. Pandu Rangan, and Moti Yung, editors, *INDOCRYPT 2007*, volume 4859 of *LNCS*, pages 73–85, Chennai, India, December 9–13, 2007. Springer, Berlin, Germany.

A Simple Message Authentication Code

In [15] it is shown how to construct an efficient MAC based a key-homomorphic wPRF. While our wPRF does not support a full key-homomorphism in the strict sense of [15], we show how to adopt

the RKA-security proof from Section 3 to prove the security of the resulting MAC. The result is a very simple MAC based on the hardness of lattices.

A.1 Definitions

Syntax. A message authentication code $\mathsf{MAC} = (\mathsf{KG}, \mathsf{TAG}, \mathsf{VRFY})$ is a triple of algorithms associated with key space $\mathcal{K}$, message space $\mathcal{M}$ and tag space $\mathcal{T}$:

- KG is a probabilistic algorithm which takes as input the security parameter 1^n and outputs a secret key $k \in \mathcal{K}$.
- $\mathsf{TAG} : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ is a probabilistic authentication algorithm which takes as input a secret key and a message and outputs a corresponding tagging. (Since the algorithm is probabilistic the tag may not be unique.)
- $\mathsf{VRFY} : \mathcal{K} \times \mathcal{M} \times \mathcal{T} \to \{\mathsf{accept}, \mathsf{reject}\}$ is a deterministic verification algorithm which receives a key, a message and an authentication tag triplet and returns accept or reject. We require that for every $k \in \mathcal{K}$,$m \in \mathcal{M}$

$$\Pr[\mathsf{VRFY}_k(m, \mathsf{TAG}_k(m)) = \mathsf{accept}] = 1.$$

Security. We consider two models of forgery attacks: *universal forgery under chosen message and verification attacks* (ufcmva) and *selective universal-forgeability under chosen message attacks* (sufcma). For an adversary A and message authentication code $\mathsf{MAC} = (\mathsf{KG}, \mathsf{TAG}, \mathsf{VRFY})$, we define the following games.

- Game $G^{\mathsf{ufcmva}}_{\mathsf{MAC}}(1^n, A)$:
  1. Set $k \leftarrow \mathsf{KG}(1^n)$.
  2. Invoke $A^{\mathsf{TAG}_k(\cdot),\mathsf{VRFY}_k(\cdot,\cdot)}$ and answer its TAG and VRFY queries.
  3. Output 1 iff A queries (m^*, σ^*) such that $\mathsf{VRFY}_k(m^*, \sigma^*) = \mathsf{accept}$ and A did not receive $\mathsf{TAG}_k(m^*)$ as a query answer.
- Game $G^{\mathsf{sufcma}}_{\mathsf{MAC}}(1^n, A)$:
  1. Set $k \leftarrow \mathsf{KG}(1^n)$.
  2. A announces a target message $m^* \in \mathcal{M}$.
  3. Invoke $A^{\mathsf{TAG}_k(\cdot)}$ and answer only queries $m \neq m^*$.
  4. At the end of the game A outputs σ^*, the value of the game is 1 iff $\mathsf{VRFY}_k(m^*, \sigma^*) = \mathsf{accept}$.

Definition A.1 (ufcmva and sufcma security)**.** *We say that a* $\mathsf{MAC} = (\mathsf{KG}, \mathsf{TAG}, \mathsf{VRFY})$ *is* ufcmva *secure (resp.,* sufcma *secure) if for every PPT adversary A the winning probability* $\Pr[G^{\mathsf{ufcmva}}_{\mathsf{MAC}}(1^n, A)$ *(resp.,* $\Pr[G^{\mathsf{sufcma}}_{\mathsf{MAC}}(1^n, A) = 1]$*) is negligible in n.*

It is not hard to see that ufcmva security implies sufcma security. In [15] it is shown that if a sufcma secure MAC is also "message-hiding" (as our construction will be) then it can be efficiently converted to a ufcmva secure MAC.

A.2 Construction

Let $\ell < p < q$ be integer-valued functions such that $\ell(n)/p(n) < \mathrm{neg}(n)$, and let $F^{q,p}$ be the LWR-based weak-PRF function (See Definition 2.1).

Construction A.2 (MAC)**.** *Define* $\mathsf{MAC} = (\mathsf{KG}, \mathsf{TAG}, \mathsf{VRFY})$ *with key-space* $\mathbb{Z}_q^n \times \mathbb{Z}_q^n$ *and message space* $\left\{-\frac{\ell-1}{2}, \ldots, \frac{\ell+1}{2}\right\} \subseteq \mathbb{Z}_q$ *as follows.*

- *Key Generation:* $\mathsf{KG}(1^n)$ *chooses* $k_1, k_2 \xleftarrow{R} \mathbb{Z}_q^n$ *uniformly at random and outputs* $k = (k_1, k_2)$.
- *Tagging:* $\mathsf{TAG}_{(k_1,k_2)}(m)$ *chooses* $x \xleftarrow{R} \mathbb{Z}_q^n$ *uniformly at random and sets* $y = F_{m\cdot k_1+k_2}(x) = \lceil \langle m \cdot k_1 + k_2, x \rangle \rfloor_{q/p}$. *Output* $\sigma = (x, y)$.
- *Verification:* $\mathsf{VRFY}_{(k_1,k_2)}(m, \sigma)$ *parses* $\sigma = (x, y)$ *and accepts iff* $F_{m\cdot k_1+k_2}(x) = \lceil \langle m \cdot k_1 + k_2, x \rangle \rfloor_{q/p} = y$.

To prove the security of our construction we rely on the following mapping. For $\ell < p < r < q$, let

$$h : (\Delta, x, \alpha, y) \mapsto \alpha \cdot y + F_{\Delta}^{q,r}(x) \pmod{r}, \tag{6}$$

where $\alpha \in \left\{-\frac{\ell-1}{2}, \ldots, \frac{\ell+1}{2}\right\}, \Delta, x \in \mathbb{Z}_q^n$ and $y \in \mathbb{Z}_r$.

Claim A.3. *For every* $s, \Delta, x \in \mathbb{Z}_q^n$ *and every* $\alpha \in \left\{-\frac{\ell-1}{2}, \ldots, \frac{\ell+1}{2}\right\}$*, if the integer* $h(\Delta, x, \alpha, F_s^{q,r}(x))$ *is at least* $\frac{\ell+3}{2}$*-far from a multiple of* r/p *then*

$$\lceil h(\Delta, x, \alpha, F_s^{q,r}(x)) \rfloor_{r/p} = F_{\alpha\cdot s+\Delta}^{q,p}(x).$$

Proof.

$$\begin{aligned}
\alpha \cdot F_s^{q,r}(x) + F_{\Delta}^{q,r}(x) &= \alpha \cdot \left\lfloor \langle x, s \rangle \cdot \frac{r}{q} \right\rfloor + \left\lfloor \langle x, \Delta \rangle \cdot \frac{r}{q} \right\rfloor \\
&= \alpha \cdot \langle x, s \rangle \cdot \frac{r}{q} + \langle x, \Delta \rangle \cdot \frac{r}{q} + \alpha \cdot e_1 + e_2 \\
&= \left\lfloor \langle x, \alpha \cdot s + \Delta \rangle \cdot \frac{r}{q} \right\rfloor + \alpha \cdot e_1 + e_2 + e_3 \\
&= F_{\alpha\cdot s+\Delta}^{q,r}(x) + e
\end{aligned}$$

where the "error" terms $e_1, e_2 \in [-1, 0]$ and $e_3 \in [0, 1]$ compensate the omission/addition of the floor operation, and $e = \alpha \cdot e_1 + e_2 + e_3 \in [\pm(\alpha - 1)]$ denotes the accumulated error.

Since $|\alpha - 1| \leq \frac{\ell+3}{2}$, $\alpha \cdot F_s^{q,r}(x) + F_{\Delta}^{q,r}(x)$ is $\frac{\ell+3}{2}$-close to $F_{s+\Delta}^{q,r}(x)$, it follows, by our hypothesis, that both elements reside in the same r/p-interval. We can therefore write:

$$\lceil h(\Delta, x, \alpha, F_s^{q,r}(x)) \rfloor_{r/p} = \lceil \alpha \cdot F_s^{q,r}(x) + F_{\Delta}^{q,r}(x) \rfloor_{r/p} = \lceil F_{\alpha\cdot s+\Delta}^{q,r}(x) \rfloor_{r/p} = F_{\alpha\cdot s+\Delta}^{q,p}(x)$$

and the claim follows. □

In the following we let $\varphi(p)$ denote Euler's phi function that counts the totatives of p, i.e., $\varphi(p) = |\mathbb{Z}_p^*|$. Also, recall that $\delta(p, q)$ is zero if p divides q, and $\frac{p}{2q}$ otherwise.

Theorem A.4. *Let $\ell < p < r < q$ be integer valued functions such that $r(n)$ is a prime and all the following quantities are negligible in n:*

$$\ell(n)p(n)/r(n), \qquad 1/p(n), \qquad \text{and } \left(1 - \frac{\varphi(q(n))}{q(n)}\right)^n.$$

Then, if $F^{q,r}$ is a weak PRF, then Construction A.2 is a sufcma-MAC.

For example, one can let $\ell = p = 2^n$, r be a prime of magnitude 2^{3n}, and $q = 2^{4n}$.

Proof. Fix some ℓ, p, r, q that satisfy the hypothesis. Assume, towards a contradiction, that A is an adversary that breaks the security of the construction above as sufcma-MAC. Namely, the adversary A forges a successful tag on a predeclared message m^* with a non negligible probability ε. We construct an adversary B that distinguishes the oracle $\mathsf{Sam}F_s^{q,r}$ from the oracle $\mathsf{R}(\mathbb{Z}_q^n, \mathbb{Z}_r)$ with advantage $\varepsilon - \mathrm{neg}(n)$. We begin with a high-level description.

Let us think of B's oracle as $\mathsf{Sam}F_s^{q,r}$. The key idea is to emulate A's attack against $\mathsf{MAC}_{k_1=s,k_2=\Delta-m^*\cdot s}$ where $\Delta \xleftarrow{R} \mathsf{U}_q^n$ is chosen at random by B and m^* is the forgery target message of A. To answer A's queries we use the (approximate) homomorphism h defined in (6). We will show that the emulation is close to the real game, and so the adversary A forges a tag y^* on m^* with non-negligible probability. Note that B can compute the forged tag by herself as it is equal to

$$\sigma = (x^*, y^*) = (x^*, F^{q,r}_{m^*\cdot s+\Delta-m^*\cdot s}(x^*)) = (x^*, F^{q,r}_{\Delta}(x^*)).$$

Therefore, B can identify a successful forgery. On the other hand, if the oracle $\mathcal{O}$ is a random oracle, then A is supplied with random tags which are almost independent of the correct tag, and so it cannot win the game with more than negligible probability. Therefore, B can distinguish the wPRF from a random oracle by checking if A's attack succeeds. In fact, the above description is not fully accurate as the emulation itself may fail (since the homomorphism is not perfect), however, we show that failure is unlikely to happen when $\mathcal{O}$ is a random oracle, and so failure allows to break the wPRF as well.

We move on to a formal description of $B^{\mathcal{O}}(1^n)$.

1. B chooses at random $\Delta \xleftarrow{R} \mathsf{U}_q^n$.
2. B emulates A, which announces $m^* \in \left\{-\frac{\ell-1}{2}, \ldots, \frac{\ell+1}{2}\right\}$ as its forgery target message.
3. If A makes a query $m \in \left\{-\frac{\ell-1}{2}, \ldots, \frac{\ell+1}{2}\right\}$ to its tagging oracle, B asks for a sample $(x, y) \xleftarrow{R} \mathcal{O}$, and continues as follows:
   - If $h(\Delta, x, \alpha = (m - m^*), y)$ is $\frac{\ell+3}{2}$-close to a multiple of r/p then B quits with the output 1.
   - Otherwise, B computes $y' = \lceil h(\Delta, x, \alpha = (m - m^*), y) \rfloor_{r/p}$ and returns the tag (x, y').
   - When reached the end of the emulation B intercepts the forged pair (x^*, y^*), B checks and outputs 1 iff $y^* = F^{q,p}_{\Delta}(x^*) = \lceil \langle x^*, \Delta \rangle \rfloor_{q/p}$.

Let us analyze the distinguishing advantage of B assuming that A makes $t = \mathrm{poly}(n)$ queries.

Claim A.5. $\Pr[B^{\mathsf{R}(\mathbb{Z}_q^n, \mathbb{Z}_r)}(1^n) = 1] \leq t(\ell + 3)p/r + t\delta(p, r) + \left(1 - \frac{\varphi(q)}{q}\right)^n + 1/p + \delta(p, q) = \mathrm{neg}(n)$.

Proof. For each query, y is uniform over $\mathbb{Z}_r$ and since $(m-m^*)$ is non-zero, the product $(m-m^*)\cdot y$ is also uniform over $\mathbb{Z}_r$ (recall that r is a prime). It follows that the value $h(\Delta, x, (m-m^*), y) = (m-m^*)\cdot y + F_\Delta^{q,r}(x)$ is uniform over $\mathbb{Z}_r$. We therefore conclude that, for each query, the probability that B halts is at most $\frac{(\ell+3)p}{r}$, and the overall halting probability is

$$\Pr[B^{\mathsf{R}(\mathbb{Z}_q^n,\mathbb{Z}_r)}(1^n) \text{ halts}] \leq t\frac{(\ell+3)p}{r}.$$

Conditioned on not halting, A is simulated with the tags (x, y') where $y' = \lceil h(\Delta, x, (m-m^*), y)\rfloor_{q/p}$. Since $h(\Delta, x, (m-m^*), y)$ is uniform over $\mathbb{Z}_r$, by Proposition 2.3, y' is $\delta(p,r)$-close to uniform over $\mathbb{Z}_p$. Therefore, by Claim 3.1, we have that

$$\Pr[B^{\mathsf{R}(\mathbb{Z}_q^n,\mathbb{Z}_r)}(1^n) = 1| \text{ not halting}] \leq \Pr[B'(1^n) = 1] + t\delta(p,r),$$

where B' is similar to B except that A's queries are answered with random values $\mathsf{R}(\mathbb{Z}_q^n, \mathbb{Z}_p)$. Finally, we claim that

$$\Pr[B'(1^n) = 1] \leq \left(1 - \frac{\varphi(q)}{q}\right)^n + 1/p + \delta(q,p).$$

Indeed, let us further condition on the event that $\Delta \in \mathbb{Z}_q^n$ has at least one invertible element, which happens with probability $1-(1-\frac{\varphi(q)}{q})^n$. In this case, $F_\Delta^{q,p}(x^*) = \lceil\langle x^*, \Delta\rangle\rfloor_{q/p}$ is $\delta(p,q)$-close to uniform (and independent of A's view) and so the probability that A guesses $F_\Delta^{q,p}(x^*)$ is at most $(1/p + \delta(p,q))$. By applying a union bound over all the above terms, we conclude that $\Pr[B^{\mathsf{R}(\mathbb{Z}_q^n,\mathbb{Z}_r)}(1^n) = 1]$ is upper-bounded by

$$t(\ell+3)p/r + t\delta(p,r) + \left(1-\frac{\varphi(q)}{q}\right)^n + 1/p + \delta(p,q) \leq t(\ell+3)p/r + 2tp/r + \left(1-\frac{\varphi(q)}{q}\right)^n + 1/p + 2p/q,$$

which, by our choice of the parameters, is negligible in n. □

We move on to the case where the oracle $\mathcal{O}$ is $\mathsf{Sam}F_s^{q,r}$.

Claim A.6. $\Pr[B^{\mathsf{Sam}F_s^{q,r}}(1^n) = 1] \geq \varepsilon$.

Proof. Let $\delta = \Pr_s[B^{\mathsf{Sam}F_s^{q,r}}(1^n) \text{ quits}]$. Since B outputs 1 when it quits we have that

$$\begin{aligned}\Pr_s[B^{\mathsf{Sam}F_s^{q,r}}(1^n) = 1] &= \delta + \Pr_s[B^{\mathsf{Sam}F_s^{q,r}}(1^n) = 1| \text{ not quitting}]\cdot(1-\delta)\\ &\geq \Pr_s[B^{\mathsf{Sam}F_s^{q,r}}(1^n) = 1| \text{ not quitting}].\end{aligned}$$

Let us condition on the event that all the queries that A made were answered by B without quitting. Then, A receives tags of the form (x, y') where $y' = \lceil (m-m^*)\cdot y + F_\Delta^{q,r}(x)\rfloor_{q/p}$ and where $(m-m^*)\cdot y + F_\Delta^{q,r}(x)$ is at least $\frac{\ell+3}{2}$ far from a multiple of r/p. By Claim A.3 it follows that B perfectly emulates the attack of A against MAC_{k_1,k_2} where $(k_1 = s, k_2 = \Delta - m^*\cdot s)$ is a random pair. It therefore follows that

$$\Pr_s[B^{\mathsf{Sam}F_s^{q,r}}(1^n) = 1| \text{ not quitting}] = \varepsilon,$$

and the claim follows. □

The theorem follows by combining Claim A.5 and A.6. □