Minicrypt Primitives with Algebraic Structure and Applications

Navid Alamati[1,2], Hart Montgomery[2], Sikhar Patranabis[2,3], Arnab Roy[2]

[1] University of Michigan
[2] Fujitsu Laboratories of America
[3] IIT Kharagpur

Abstract. Algebraic structure lies at the heart of Cryptomania as we know it. An interesting question is the following: instead of building (Cryptomania) primitives from concrete assumptions, can we build them from *simple* Minicrypt primitives endowed with some additional *algebraic* structure? In this work, we affirmatively answer this question by adding algebraic structure to the following Minicrypt primitives:

- One-Way Function (OWF)
- Weak Unpredictable Function (wUF)
- Weak Pseudorandom Function (wPRF)

The algebraic structure that we consider is group homomorphism over the input/output spaces of these primitives. We also consider a "bounded" notion of homomorphism where the primitive only supports an a priori bounded number of homomorphic operations in order to capture lattice-based and other "noisy" assumptions. We show that these structured primitives can be used to construct many cryptographic protocols. In particular, we prove that:

- (Bounded) *Homomorphic OWFs* (HOWFs) imply collision-resistant hash functions, Schnorr-style signatures and chameleon hash functions.
- (Bounded) *Input-Homomorphic weak UFs* (IHwUFs) imply CPA-secure PKE, non-interactive key exchange, trapdoor functions, blind batch encryption (which implies anonymous IBE, KDM-secure and leakage-resilient PKE), CCA2 deterministic PKE, and hinting PRGs (which in turn imply transformation of CPA to CCA security for ABE/1-sided PE).
- (Bounded) *Input-Homomorphic weak PRFs* (IHwPRFs) imply PIR, lossy trapdoor functions, OT and MPC (in the plain model).

In addition, we show how to realize any CDH/DDH-based protocol with certain properties in a generic manner using IHwUFs/IHwPRFs, and how to instantiate such a protocol from many concrete assumptions.
We also consider primitives with substantially richer structure, namely *Ring IHwPRFs* and *L-composable IHwPRFs*. In particular, we show the following:

- Ring IHwPRFs with certain properties imply FHE.
- 2-composable IHwPRFs imply (black-box) IBE, and L-composable IHwPRFs imply non-interactive $(L+1)$-party key exchange.

Our framework allows us to categorize many cryptographic protocols based on which structured Minicrypt primitive implies them. In addition, it potentially makes showing the *existence* of many cryptosystems from novel assumptions substantially easier in the future.

1 Introduction

An important question in the theory of cryptography is also one of the simplest to state: what implies public-key cryptography? Ever since the (public) invention of public-key encryption [DH76,RSA78], people have debated this important question.

The history of symmetric-key cryptography goes back millenia–the Caesar cipher is a classic example of old cryptography–and it has continued to evolve through the centuries in different ways. There is a long list of ciphers, notably including the Viginère cipher, the Enigma machine, and even modern ciphers like AES, that can be thought of as the output of an enormous amount of human effort to build secure symmetric-key encryption.

On the other hand, public-key cryptography is a very recent development compared to symmetric-key cryptography. Many people thought that public-key cryptography was impossible before the seminal work by Diffie and Hellman [DH76]. Although we can build symmetric-key ciphers from many different assumptions, including some very simple ones, the known methods for realizing public-key cryptography require at least some kind of mathematical structure. This has led many to conjecture that public-key cryptography does, in fact, require some mathematical structure.

Barak ruminated on this question in his recent work "The Complexity of Public Key Cryptography" [Bar17]. As he puts it, "... it seems that you can't throw a rock without hitting a one-way function" but public-key cryptography is somehow "special". Barak implicitly argues that there is some mathematical structure inherent in public-key cryptography: "One way to phrase the question we are asking is to understand what type of structure is needed for public-key cryptography."

But many cryptosystems that interest people today are substantially more complicated than basic public-key encryption (PKE). In recent years, primitives like identity-based encryption [Sha84], fully homomorphic encryption [Gen09], and functional encryption [BSW11] have captivated cryptographers. It is natural to ask: is there any sort of mathematical structure that is inherent to these primitives as well? While there has been a substantial amount of work relating relatively similar primitives, to our knowledge no one has attempted to comprehensively examine the relationship between a broader collection of these higher-level primitives.

In a celebrated work, Impagliazzo [Imp95] proposed "five worlds" of relative complexity, which range from *Algorithmica*–where "efficient" algorithms for all (worst-case) problems in NP exist and cryptography is essentially nonexistent–to *Cryptomania*, a world in which public-key cryptography exists. Only two of

these worlds allow for cryptography: *Minicrypt*, where symmetric cryptographic primitives exist but public-key cryptography does not, and the aforementioned *Cryptomania*.

It turns out that Minicrypt is a fairly simple world. A number of famous works have shown how to build the most commonly studied and used Minicrypt primitives from one-way functions in a generic manner. For instance, one-way functions imply pseudorandom generators [BM82,HILL99], which in turn can be used to build pseudorandom functions [GGM84]. From these primitives, it has long been known how to generically build symmetric-key encryption schemes and digital signature schemes [Rom90].

On the other hand, Cryptomania is a significantly more complicated class. It contains primitives that are very different, and it seems difficult to relate them in a generic manner. We cannot expect to, say, build FHE from PKE in a black-box manner, and there are many black-box separation results for cryptosystems in Cryptomania (we discuss this more in our related work section). In fact, recently it has even become popular to separate Cryptomania into two worlds: a world where indistinguishability obfuscation (iO) [BGI$^+$01,GGH$^+$13b] doesn't exist, and a world called Obfustopia [GPSZ17] where it does.

This, of course, raises a fundamental question in the complexity of public-key cryptography: can we construct classes of primitives within Cryptomania (i.e. "continents" of Cryptomania) that are tightly tied to each other through generic constructions? Ideally, we would want these "continents" to have strong relationships with a particular primitive (similar to the relationship between one-way functions and Minicrypt) where all of the cryptographic algorithms in the class could be built from the given primitive in a generic manner, and the given primitive would be conceptually the simplest function in the class.

The fact that most of the concrete assumptions that imply PKE (and also many other cryptographic primitives) have some algebraic structure seems to imply that perhaps we can classify cryptosystems by the algebraic structure necessary for them to function. This leads us to the following question:

Is it possible to construct Cryptomania primitives from simple Minicrypt primitives that are additionally equipped with some algebraic structure?

1.1 Our Contributions

In this work, we provide a constructive answer to the question of building PKE (and other primitives in Cryptomania) from Minicrypt primitives with algebraic structure. Let's start by considering the following Minicrypt primitives:

1. One-way Functions
2. Weak Unpredictable Functions
3. Weak Pseudorandom Functions

To add *algebraic structure* to the mentioned primitives, we assume that they are *(Input-)Homomorphic*: the input and output spaces of the primitive are groups,

and the primitive is (bounded) homomorphic with respect to an efficiently computable group homomorphism. We use the following primitives and abbreviations throughout the paper:

- *Homomorphic One-way Functions* (HOWFs)[4]
- *Input-Homomorphic Weak Unpredictable Functions* (IHwUFs)
- *Input-Homomorphic Weak Pseudorandom Functions* (IHwPRFs)[5]

In the body of the paper we also consider "bounded" homomorphisms, where the number of allowed homomorphisms is bounded by some function $\gamma = \gamma(\lambda)$ where λ is the security parameter, which lets us work with lattice-based and other "noisy" cryptographic assumptions.

At this point we can informally state our main contribution: we present a framework for building cryptographic primitives from HOWFs/IHwUFs/IHwPRFs (see Figure 1). This framework lets us categorize cryptographic primitives by the type of structured Minicrypt primitive that implies them. However, we need to be able to instantiate the above *general* primitives from *concrete* assumptions to have a useful framework. It turns out that we can instantiate our primitives (in most cases) from a wide variety of assumptions, typically including the assumptions that would be expected for such applications.

Instantiations from Concrete Assumptions. We show that "mainstream" cryptographic assumptions such as DDH and LWE naturally imply (bounded) HOWFs/IHwUFs/IHwPRFs. We also show that a (bounded) group-homomorphic PKE implies a (bounded) IHwPRF. This allows instantiating these primitives from any concrete assumption that implies a (bounded) homomorphic PKE (e.g. QR and DCR). Unfortunately, there is a caveat to this: the transformation from homomorphic PKE to IHwPRF comes with a disadvantage that the input space may *depend* on the key.[6] The reader may refer to Figure 2 for an overview of instantiations from concrete assumptions.[7]

Building Cryptosystems from New Assumptions. One of the benefits of our work is the implications for new assumptions. Rather than manually building lots of different cryptosystems from a new assumption, researchers only need to build one (or more) of our simple structured primitives, and the existence of a whole host of cryptosystems immediately follows.

[4] When the function does not have a key (i.e. a one-way function) we will drop the "I" and refer to the function as simply homomorphic.

[5] In case of IHwUFs/IHwPRFs we do not assume any homomorphism on the key space.

[6] This property is necessary to realize certain cryptographic primitives from IHwUFs or IHwPRFs.

[7] Notice that search to decision reductions are mostly for Gaussian-like distributions, and there are certain distributions for which search to decision reduction is not available.

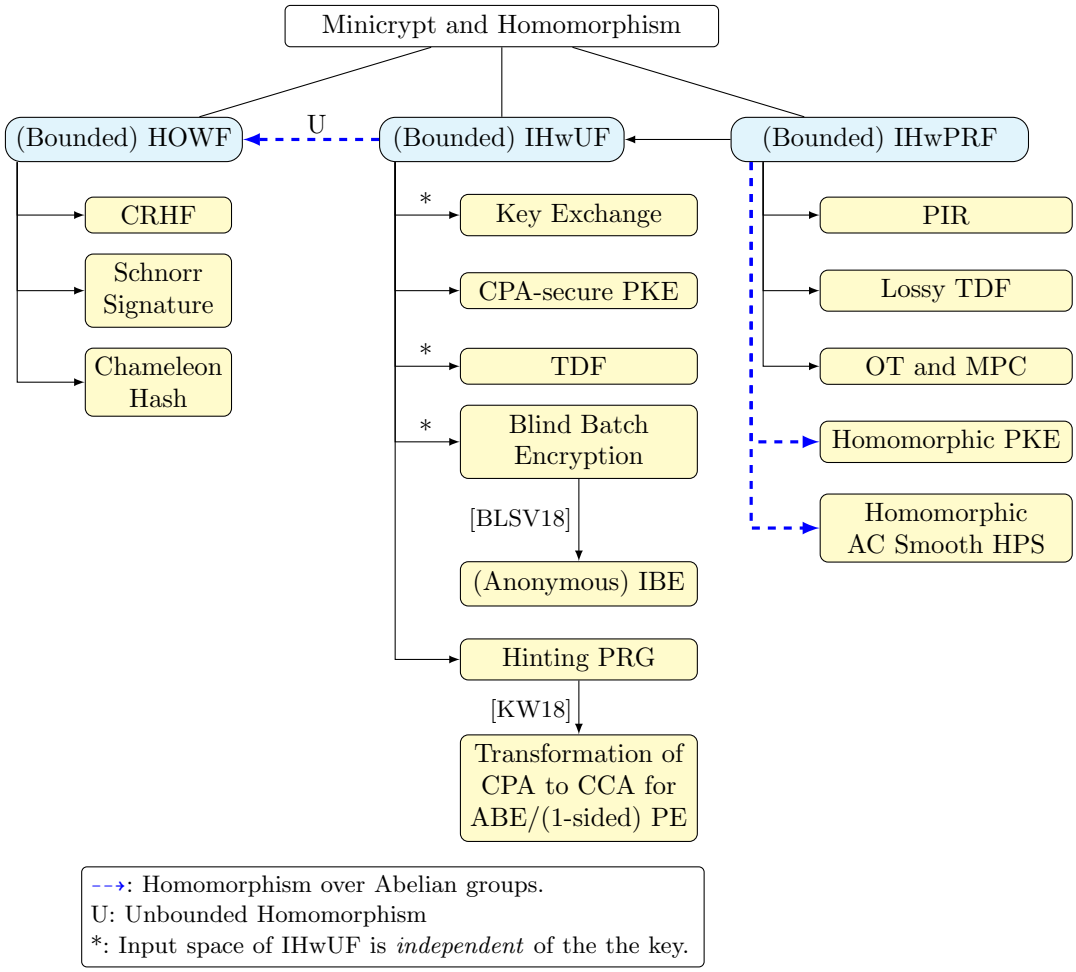

Fig. 1. Cryptographic primitives from Minicrypt and Homomorphism.

To illustrate how this might be useful, let's look at the history of lattice-based cryptography: Ajtai and Dwork [AD97] gave a lattice-based PKE (following Ajtai's worst-case to average-case reductions for lattice problems [Ajt96]), but lattice cryptography may have begun in earnest with Regev's LWE paper [Reg05] in 2005. This work, in addition to introducing the LWE problem, showed how to build a basic PKE scheme from LWE as well. However, it took a while for the cryptographic community to "catch up" to other group-based cryptosystems: for instance, the first private information retrieval scheme from lattices was presented in [AMG07], and the first identity-based encryption was given in [GPV08].

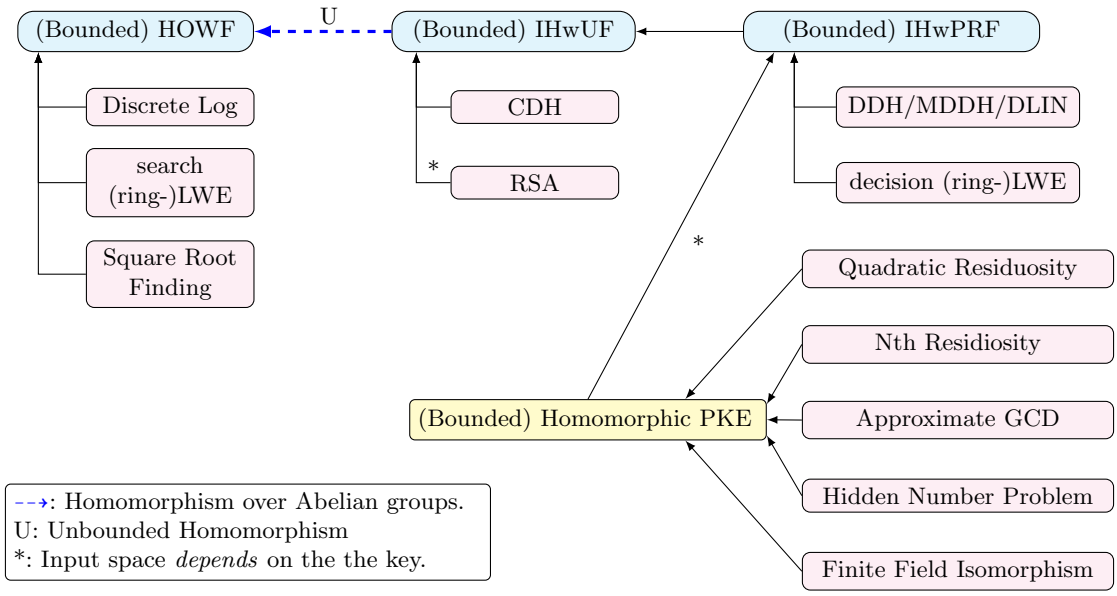

Fig. 2. Instantiations from Concrete Assumptions

These works used sophisticated techniques on lattices in order to extend the range of lattice-based cryptosystems. With our work, the existence of all of these types of cryptosystems based on the LWE assumption follows immediately from the simple observation that LWE implies a (bounded) IHwPRF. While the necessary tools for many of our constructions were not around in 2008 (particularly [DG17b] and the line of work following it), we do hope that this paper is useful for public-key cryptography assumptions in the future in terms of *feasibility* results. Ideally, it will be easy to show the existence of many types of cryptosystems for new assumptions using the tools from this paper.

More Primitives from Richer Structures. Although the main focus of this work is to construct many cryptographic primitives from IHwUFs/IHwPRFs, one might ask: what if we consider richer structures? For instance, what would happen if we have a *ring homomorphism* for an IHwPRF instead of just a group homomorphism? To partially answer this question, we consider two additional structures over wPRFs:

- *Ring Homomorphism*: We consider Ring IHwPRFs (RIHwPRFs) where the input and output spaces are rings, and the homomorphism is with respect to ring operations (instead of just group operations).

- *L-composability*: We consider L-composable IHwPRFs, where L levels of IHwPRF operations compose with each other under certain conditions.

We summarize our results for these richly structured primitives in Figure 3. We remark that "*" means the order of the output ring of RIHwPRF is polynomial in the security parameter.

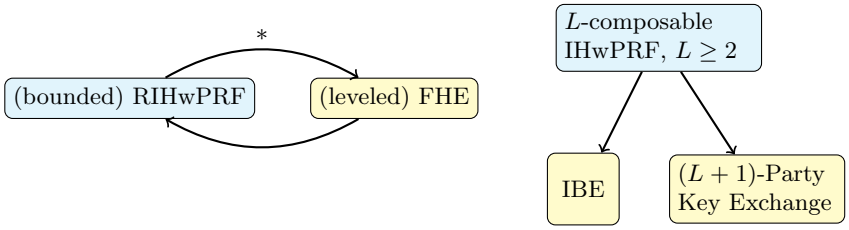

Fig. 3. Cryptographic primitives from richer structures.

While the structure of 2-composability appears similar to that of bilinear pairing groups, we partially explore a possible separation between the two. We argue that 2-composability suffices to achieve three-party non-interactive key exchange and simple black-box constructions of IBE. Subsequently, we also present a discussion on why this primitive does not naturally yield other cryptographic protocols implied by bilinear pairings. This leaves open the interesting question of whether there exists some concrete assumption that implies 2-composability but not bilinear pairings. The separation seemingly extends to the general L-composability setting, in the sense that the structure of L-composability appears to be weaker than that of a full-fledged multilinear map [GGH13a].

On the Categorization of Primitives. This work enables us to categorize different primitives based upon which structured Minicrypt primitive implies them. But it is also possible to ask whether a given cryptosystem may be constructed from some other structured Minicrypt primitive. For instance, is it possible to construct PKE from a HOWF? A positive answer would imply that one can base PKE on the discrete log problem, a long-standing (and potentially possible) goal in cryptography. We can build PKE from IHwUFs, but can we hope to do better? Our work gives rise to interesting questions like this for future work, and we discuss this more later in the paper.

It is easy to see that none of the three primitives HOWF/IHwUF/IHwPRF can be built from PKE in a *black-box* manner [HHRS07], as all of them imply collision-resistant hash functions. In addition to input homomorphisms, one may consider other structures on Minicrypt primitives.

One of the simplest structures is what we term *dual-computable*. This notion is certainly folklore, and some earlier works on PKE and key exchange implicitly constructed this primitive. A *dual-computable* primitive is a tuple of keyed functions (F_1, G_1, F_2, G_2) such that $G_1(k_1, F_2(k_2, x)) = G_2(k_2, F_1(k_1, x))$ where x

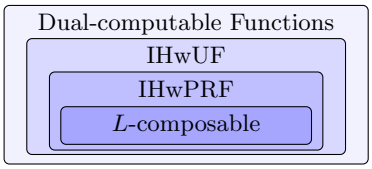

Fig. 4. Implication Landscape

represents the input and k_i represent keys. The reader may notice that this primitive is almost an abstraction of key exchange if the functions are unpredictable. It is not clear what kind of (minimal) structure over OWFs would imply dual-computable functions.

1.2 Related Works

Realizing public-key cryptography via some form of structure and hardness has been studied seemingly since its invention. However, several recent works have discussed this relationship in more detail. For instance, [BDV17] examined the relationship of structure and hardness through obfuscation lens, while a recent work by Berman *et al.* showed that laconic zero-knowledge protocols imply PKE [BDRV18]. Pietrzak and Sjdin [PS08] showed that a certain input property of weak PRFs implies PKE. A recent survey [BR17] briefly discusses structure and PKE through the lens of (strengthened) PRFs.

A number of works have shown how to build certain cryptosystems from cryptographic primitives with algebraic structure. These include commitment schemes, CRHF, IND-CCA secure PKE, PIR, and key-dependent message (KDM) secure PKE [IKO05,HO12,KO97,HKS16]. Of particular relevance to us is the work of Hajiabadi *et al.* [HKS16] on using homomorphic weak PRFs to build KDM secure PKE.[8]

There are other related black-box constructions (or implications in a non-black-box way) between cryptographic primitives, some of which we utilize in our work. For instance, Ishai *et al.* showed how to construct secure computation protocols from enhanced trapdoor functions (or homomorphic PKE) [IKLP06]. Rothblum [Rot11] showed a transformation of a secret-key encryption (SKE) scheme with some special form of weak homomorphism into a PKE that has similar properties. Black-box constructions have been shown for resettable zero-knowledge arguments [OSV15] and cryptographic accumulators [DHS15]. Many cryptographic primitives have been realized in a black-box manner from lossy trapdoor functions [PW08,BHY09,GPR16]. Very recently, Friolo *et al.* [FMV18] showed how to build secure multi-party computation from what they call strongly uniform key agreement and Fischlin and Harasser [FH18] showed the equivalence of invisible sanitizable signatures and PKE.

[8] As mentioned earlier, we refer to this primitive as Input-Homomorphic weak PRF (IHwPRF) to emphasize that the homomorphism is on the input space and not on the key space.

Understanding the complexity of various public-key primitives also requires knowledge of black-box separations, which have been extensively studied in the literature. This (non-exhaustively) includes studies separating IBE from CRHFs (and thus FHE) [MM16], separating indistinguishability obfuscation (iO) from certain primitives (for instance, CRHFs) [AS15,MMN+16], separating succinct non-interactive arguments from falsifiable assumptions [GW11], and showing that garbling of circuits having one-way function gates are not sufficient to realize PKE [GHMM18]. These separations (and related works) allow us to clearly see that some primitives are *not* equivalent, at least modulo certain assumptions. We refer the reader to [RTV04,Fis12,BBF13] for a survey on black-box reductions and separations.

2 Technical Overview

In this section, we aim to explain some of the intuition behind our results. We will start by focusing on one particular primitive–the input homomorphic weak PRF–and some of its applications. The results for other primitives are not exactly the same, but the general structure of how we build cryptosystems from these other primitives is relatively similar. We will discuss these other primitives later in this section.

2.1 PKE from IHwUFs/IHwPRFs

Let's start by considering the notion of a general input-homomorphic weak PRF, or, as we have been abbreviating, an IHwPRF, which we will define as a function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$. Recall that, informally speaking, a weak PRF is a function that is indistinguishable from a random function *with respect to uniformly sampled inputs*. This "weakness" as compared to a regular PRF will be critical.

We will also endow our weak PRF F with a homomorphism over the input. Suppose our input space $\mathcal{X}$ and our output space $\mathcal{Y}$ are groups with group operations $\oplus$ and $\otimes$, respectively. Roughly speaking, an IHwPRF is just a regular weak PRF with the following property:

$$F(k, x_1 \oplus x_2) = F(k, x_1) \otimes F(k, x_2).$$

We also consider what we call γ-bounded IHwPRFs. These IHwPRFs have a homomorphism that can only be computed a maximum of γ times, where γ is a pre-determined parameter. This concept lets us consider noisy assumptions like LWE, which are only approximately homomorphic. The notion is very similar to definitions of the *almost* key-homomorphic PRFs of [BLMR13]. γ-bounded IHwPRFs work for almost all of the applications that we consider in almost the same way that unbounded IHwPRFs do. For the rest of this technical overview, though, we will assume we have an unbounded IHwPRF. Also, we occasionally refer to an Input-Homomorphic weak Unpredictable Function (IHwUF), which has the same properties as IHwPRF except for the fact that its output on a uniformly random input is just *unpredictable* and not necessarily *pseudorandom*.

DDH-based Instantiation of IHwPRF. In general, it is simple to build IHwPRFs from assumptions that are widely used in cryptography. Here we show how to build an IHwPRF from the DDH assumption. Let $\mathbb{G}$ be a group of prime order q where the DDH problem is hard. For a uniformly sampled key $k \leftarrow \mathbb{Z}_q$ and an input $x \in \mathbb{G}$, consider the following function:

$$F(k, x) = x^k.$$

If we are only allowed to see the evaluation of F on random inputs x_i (as the weak PRF definition requires), then it is easy to see that F is a weak PRF based on the DDH assumption. Moreover, the homomorphism property is also satisfied:

$$x_1^k \cdot x_2^k = (x_1 \cdot x_2)^k.$$

Thus F is an IHwPRF. Building a *bounded* IHwPRF from LWE is similarly straightforward, but we defer this to later in the paper.

On the Input Space. It is useful to note that the "discrete logarithm problem" on the input space of an IHwPRF must be hard by its weak pseudorandomness property. Concretely, given two evaluations $(x_1, F(k, x_1))$ and $(x_2, F(k, x_2))$, an adversary can compute some value c such that $x_1^c = x_2$, then they can check if

$$F(k, x_1)^c = F(k, x_2)$$

and use this to break the (weak) pseudorandomness of F. In the context of (bounded) IHwPRFs over arbitrary groups, we note that there must exist an equivalent "discrete log" problem that allows us to capture the aforementioned property.[9] This property is crucial to the security of nearly all constructions presented in this paper.

PKE Construction. We now illustrate how to construct a CPA-secure PKE given an IHwPRF. To provide more intuition, we will present an instantiation of the encryption scheme using the DDH assumption in parallel. The construction from IHwPRF is highlighted for clarity.

Setup:

- **IHwPRF Construction:** Select an IHwPRF $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ over groups $(\mathcal{X}, \oplus)$ and $(\mathcal{Y}, \otimes)$ with key space $\mathcal{K}$, input space $\mathcal{X}$, and output space $\mathcal{Y}$ and some integer $n > 3\log(|\mathcal{X}|)$. Select a set X of $2n$ uniform "base elements" from $\mathcal{X}$ as

  $$\mathrm{X} = \{x_{j,b} \leftarrow \mathcal{X}\}_{j \in [n], b \in \{0,1\}}.$$

  Select a random key $k \leftarrow \mathcal{K}$. Create a tuple Y of $2n$ elements from $\mathcal{Y}$ as

  $$\mathrm{Y} = \{y_{j,b}\}_{j \in [n], b \in \{0,1\}}$$

[9] For our LWE-based bounded IHwPRF, the "discrete log" problem equivalent is the ISIS problem.

such that $y_{j,b} = F(k, x_{j,b})$. Output the secret key and public key as:[10]

$$\mathsf{sk} = k, \quad \mathsf{pk} = (\mathrm{X}, \mathrm{Y}).$$

- **DDH Instantiation:** Let $F : \mathbb{Z}_q \times \mathbb{G} \to \mathbb{G}$ be the function defined as $F(k \in \mathbb{Z}_q, g \in \mathbb{G}) = g^k$. Select a set G of $2n$ randomly sampled elements from $\mathbb{G}$ as
$$\mathrm{G} = \{g_{j,b} \leftarrow \mathbb{G}\}_{j\in[n],b\in\{0,1\}}.$$
Select a random key $k \leftarrow \mathbb{Z}_q$. Create a tuple H of $2n$ elements from $\mathbb{G}$ as
$$\mathrm{H} = \{h_{j,b}\}_{j\in[n],b\in\{0,1\}}$$
such that $h_{j,b} = g_{j,b}^k$. Output the secret key and the public key as
$$\mathsf{sk} = k, \quad \mathsf{pk} = (\mathrm{G}, \mathrm{H}).$$

Encrypt:

- **IHwPRF Construction:** On input a message $\mathsf{m} \in \mathcal{Y}$, sample a vector $\mathbf{s} = (s_1, \ldots, s_n) \leftarrow \{0,1\}^n$. Set
$$x^* = \bigoplus_{j\in[n]} x_{j,s_j}, \quad y^* = \bigotimes_{j\in[n]} y_{j,s_j}.$$
Output the ciphertext $\mathsf{ct} = (x^*, y^* \otimes \mathsf{m})$.

- **DDH Instantiation:** On input a message $\mathsf{m} \in \mathbb{G}$, sample a vector $\mathbf{s} = (s_1, \ldots, s_n) \leftarrow \{0,1\}^n$. Set
$$g^* = \prod_{j=1}^{n} g_{j,s_j}, \quad h^* = \prod_{j=1}^{n} h_{j,s_j}.$$
Output the ciphertext $\mathsf{ct} = (g^*, h^* \cdot \mathsf{m})$.

By the leftover hash lemma, our "subset sum" process gives us outputs that are statistically close to uniform for arbitrary groups. This may be viewed as a generalization of the "exponentiation" operation to arbitrary groups.

Decrypt:

- **IHwPRF Construction:** On input a ciphertext $\mathsf{ct} = (\mathsf{ct}_1, \mathsf{ct}_2) \in \mathcal{X} \times \mathcal{Y}$, output
$$\mathsf{m}' = [F(k, \mathsf{ct}_1)]^{-1} \otimes \mathsf{ct}_2.$$
If $(\mathsf{ct}_1, \mathsf{ct}_2) = (x^*, y^* \otimes \mathsf{m})$, we have
$$\mathsf{m}' = [F(k, \mathsf{ct}_1)]^{-1} \otimes \mathsf{ct}_2 = (y^*)^{-1} \otimes (y^* \otimes \mathsf{m}) = \mathsf{m}.$$

[10] We implicitly assume that the description of IHwPRF is publicly available. This is similar to the assumption that in a DDH-based encryption scheme like ElGamal, the description of the cyclic group $\mathbb{G}$ is public.

- **DDH Instantiation:** On input a ciphertext $\mathsf{ct} = (\mathsf{ct}_1, \mathsf{ct}_2) \in \mathbb{G} \times \mathbb{G}$, output

$$\mathsf{m}' = \left(\mathsf{ct}_1^k\right)^{-1} \cdot \mathsf{ct}_2.$$

  If $(\mathsf{ct}_1, \mathsf{ct}_2) = (g^*, h^* \cdot \mathsf{m})$, we have

$$\mathsf{m}' = \left(\mathsf{ct}_1^k\right)^{-1} \cdot \mathsf{ct}_2 = (h^*)^{-1} \cdot (h^* \cdot \mathsf{m}) = \mathsf{m}.$$

Note that the decryption in the IHwPRF construction works even when $\mathcal{X}$ and $\mathcal{Y}$ are non-abelian groups.

We summarize the main steps in the construction of PKE from IHwPRF in Figure 5, and compare it with the DDH-instantiation over cyclic groups of prime order. Observe that the DDH-based PKE described above is very similar to ElGamal encryption [ElG84]. In fact, it can be viewed as a form of ElGamal encryption where we use a less efficient method to create the group elements (g, h) and (g^*, h^*): namely, in order to get a random element, we take a subset product of many public elements rather than just raising a single element to a random power.

This leads us to the following question: how far can we go if we take traditional DDH-based schemes and write them as IHwPRFs? For schemes that require two exponentiations, we could write the first exponentiation as a "subset sum", and then the second as a IHwPRF evaluation. This is essentially how our DDH-based instantiation of PKE from IHwPRF works. In what follows, we illustrate this comparison via a non-interactive key exchange protocol.

We show a non-interactive key exchange protocol from IHwPRFs in Figure 6. For illustration, we compare it with the Diffie-Hellman key exchange protocol. In the IHwPRF setting, the (randomly sampled) "base elements" $\{x_{j,b}\}_{j\in[n],b\in\{0,1\}}$ are publicly available to both parties at the beginning of the protocol. Given the "base elements", there are two ways to arrive at the final secret y^*. The first way is to apply the IHwPRF on the "base elements", followed by applying a "subset product" in the output space of the IHwPRF. The second way is to first do a "subset sum" on the base elements, and then apply the IHwPRF. The two parties involved in the protocol each use one of these strategies. Security of the protocol follows from the weak pseudorandomness of F and one-wayness of "subset sums" in its input space, where the latter is also implied by the weak pseudorandomness of F.

Finally, the reader may observe that the protocol is secure even if the function F is an IHwUF instead of an IHwPRF, provided that both parties extract a "hardcore bit" from the secret y^* and use it as the key.[11] Similarly, one can construct a CPA-secure PKE from IHwUF by using the hardcore bit of the secret y^* to mask the message bit.

[11] Note that the protocol assumes that the input space of the IHwUF/IHwPRF is independent of the choice of key.

Setup:

$$
\begin{array}{lcl}
F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y} & \leftrightsquigarrow & (\mathbb{G}, q) \\
\mathrm{X} = \{x_{j,b} \leftarrow \mathcal{X}\}_{j\in[n],b\in\{0,1\}} & \leftrightsquigarrow & \mathrm{G} = \{g_{j,b} \leftarrow \mathbb{G}\}_{j\in[n],b\in\{0,1\}} \\
k \leftarrow \mathcal{K} & \leftrightsquigarrow & k \leftarrow \mathbb{Z}_q \\
\mathrm{Y} = \{y_{j,b} = F(k, x_{j,b})\}_{j\in[n],b\in\{0,1\}} & \leftrightsquigarrow & \mathrm{H} = \left\{h_{j,b} = g_{j,b}^{k}\right\}_{j\in[n],b\in\{0,1\}} \\
\boxed{\mathsf{sk} = k, \quad \mathsf{pk} = (\mathrm{X}, \mathrm{Y})} & \leftrightsquigarrow & \boxed{\mathsf{sk} = k, \quad \mathsf{pk} = (\mathrm{G}, \mathrm{H})}
\end{array}
$$

Encrypt:

$$
\begin{array}{lcl}
\mathsf{m} \in \mathcal{Y} & \leftrightsquigarrow & \mathsf{m} \in \mathbb{G} \\
\mathsf{s} \leftarrow \{0,1\}^n & \leftrightsquigarrow & \mathsf{s} \leftarrow \{0,1\}^n \\
x^* = \bigoplus_{j\in[n]} x_{j,s_j} & \leftrightsquigarrow & g^* = \prod_{j=1}^{n} g_{j,s_j} \\
y^* = \bigotimes_{j\in[n]} y_{j,s_j} & \leftrightsquigarrow & h^* = \prod_{j=1}^{n} h_{j,s_j} \\
\boxed{\mathsf{ct} = (x^*, y^* \otimes \mathsf{m})} & \leftrightsquigarrow & \boxed{\mathsf{ct} = (g^*, h^* \cdot \mathsf{m})}
\end{array}
$$

Decrypt:

$$
\begin{array}{lcl}
\mathsf{ct} = (\mathsf{ct}_1, \mathsf{ct}_2) & \leftrightsquigarrow & \mathsf{ct} = (\mathsf{ct}_1, \mathsf{ct}_2) \\
\boxed{\mathsf{m}' = \left[F\left(k, \mathsf{ct}_1\right)\right]^{-1} \otimes \mathsf{ct}_2} & \leftrightsquigarrow & \boxed{\mathsf{m}' = \left(\mathsf{ct}_1^{k}\right)^{-1} \cdot \mathsf{ct}_2}
\end{array}
$$

Fig. 5. PKE from IHwPRF and DDH Instantiation

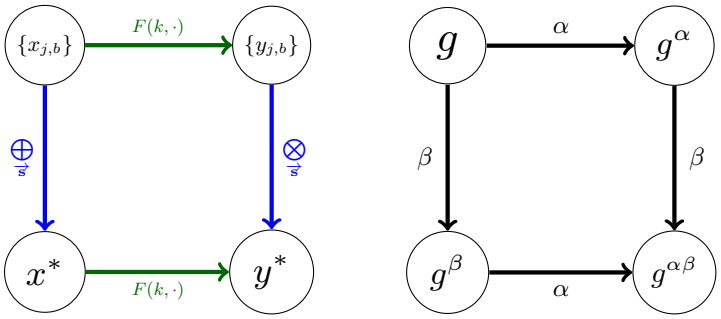

Fig. 6. Visualization of Non-Interactive Key Exchange from IHwPRF

2.2 Extending the Scheme with a General Protocol

It turns out that we can do substantially more than just PKE, as an examination of the above protocol might suggest. It turns out we can take *any* one-round[12]

[12] Informally, in our context this means a protocol that can be "played" by two parties with a simple out-and-back communication flow, along with any PPT computation the parties choose to do before, during, or after the communication.

CDH/DDH-based protocol and convert it into a (less efficient) protocol using a general IHwUF/IHwPRF. The basic idea is the following: visualize one-round CDH/DDH schemes as protocols played by two parties with the following four phases. Below is a rough description of this protocol:

- **Initialization**: Setting up the group and any random elements needed for the protocol.
- **Pre-Evaluation**: The first party exponentiates some (or all) of the random elements from the initialization stage and sends some (or all) of these to the second player.
- **Evaluation**: The second party exponentiates some of the elements from the first player and potentially some of the elements from initialization as well. The second player potentially publishes some of these elements as well.
- **Post-Evaluation**: Either party can multiply/invert/process the elements, and may publish some outputs of these.

It turns out that the vast majority of CDH/DDH-based cryptosystems fall into this archetype, and thus we can build them using an IHwUF/IHwPRF. Among other implications, this approach encompasses recent constructions such as (anonymous) IBE from CDH/DDH and a number of other works in the same vein [DG17b,DG17a,BLSV18,DGHM18,GH18,KW18,GGH18]. Although these works use many novel techniques, we show that the CDH/DDH-related portion of the constructions can be boiled down to something that fits within the above framework. The few protocols that cannot be handled involve at least three exponentiations (and cannot be rewritten as less efficient protocols with two or less exponentiations).

We can use our general protocol and the ideas around it to build many cryptosystems. In the following subsection, we outline some of the constructions that we consider interesting.

2.3 Batch Encryption from IHwUFs

In a recent work, Brakerski *et al.* [BLSV18] introduced and formalized a powerful cryptographic primitive called *batch encryption*. Roughly speaking, the basic idea of batch encryption is the following: a user encrypts a $2 \times N$ matrix of bits, and decryption *selectively* reveals only N of these bits–one in each column. For a given column, which bit is revealed depends on the value of the secret key used for decryption.

Brakerski *et al.* showed that batch encryption can be used in conjunction with garbled circuits to construct identity-based encryption (IBE).[13] In fact, when equipped with a stronger property called "blinding", batch encryption was shown to imply anonymous IBE, KDM-CPA secure PKE, and leakage resilient PKE [BLSV18]. The authors of [BLSV18] showed how to construct batch

[13] An equivalent cryptosystem, named as *hash encryption*, was introduced by Döttling *et al.*in [DGHM18].

encryption from concrete assumptions, so it is natural to ask the following question: is there a generic primitive that implies batch encryption?

In this subsection, we answer this question in the affirmative by showing that IHwUFs are sufficient to construct blind batch encryption. This in turn implies that IHwUFs are sufficient to construct anonymous IBE, KDM-secure PKE and leakage-resilient PKE as well.[14] We begin by defining blind batch encryption informally, and then illustrate how to construct the same from any IHwUF family. [15]

Batch Encryption. A batch encryption scheme is a public-key encryption scheme in which the key generation algorithm Gen "projects" a secret string $\mathbf{s} \in \{0,1\}^n$ onto a corresponding hash value $h \in \{0,1\}^\ell$, such that $\ell < n$. Corresponding to this "projection" function, there should exist encryption and decryption algorithms such that:

- The encryption algorithm $\mathsf{Enc}(\mathsf{pp}, h, i, (\mathsf{m}_0, \mathsf{m}_1))$ takes as input the public parameter pp associated with the projection function, a hash $h \in \{0,1\}^\ell$, a position index $i \in [n]$ and a pair of message-bits $(\mathsf{m}_0, \mathsf{m}_1) \in \{0,1\}^2$, and outputs a ciphertext ct.
- The decryption algorithm $\mathsf{Dec}\,(\mathsf{pp}, \mathbf{s}, i, \mathsf{ct})$ takes as input a ciphertext ct and a secret string $\mathbf{s}$, and then recovers m_{s_i} where s_i is the value of the i^{th}-bit of $\mathbf{s}$, provided that ct was generated using $h = \mathsf{Gen}(\mathsf{pp}, \mathbf{s})$.

In other words, a decryptor can use the knowledge of the preimage $\mathbf{s}$ of a hash output string $h \in \{0,1\}^\ell$ to decrypt *exactly one* of the two encrypted messages, depending on the i^{th}-bit of $\mathbf{s}$. The security requirement is roughly that the distributions

$$\{\mathsf{pp}, \mathbf{s}, \mathsf{Enc}(\mathsf{pp}, h = \mathsf{Gen}(\mathsf{pp}, \mathbf{s}), i, (\mathsf{m}_{s_i}, \mathsf{m}_{1-s_i}))\}_{\mathbf{s} \in \{0,1\}^n} \quad \text{and}$$
$$\{\mathsf{pp}, \mathbf{s}, \mathsf{Enc}(\mathsf{pp}, h = \mathsf{Gen}(\mathsf{pp}, \mathbf{s}), i, (\mathsf{m}_{s_i}, \mathsf{m}^*))\}_{\mathbf{s} \in \{0,1\}^n, \mathsf{m}^* \leftarrow \{0,1\}}$$

are computationally indistinguishable. In fact, as Brakerski et al. pointed out in [BLSV18], a weaker *selective* notion of security suffices, where the adversary commits to a string $\mathbf{s} \in \{0,1\}^n$ and an index $i \in [n]$ before the public parameter pp is published.

Note that the adaptive security guarantee implicitly requires the projection function to be collision-resistant; otherwise, a PPT adversary could distinguish an encryption of m_{1-s_i} from random with non-negligible probability simply by generating a different preimage $\mathbf{s}'$ of h such that $s'_i \neq s_i$.

An additional security requirement, called "blindness" was formalized with respect to batch encryption in [BLSV18]. Roughly, a batch encryption scheme is

[14] The construction of anonymous IBE requires an additional primitive - "blind garbled circuits" besides blind batch encryption. However, blind garbled circuits are implied by any one-way function, and are hence also implied by IHwUFs.

[15] We can analogously construct blind batch encryption from γ-bounded IHwUFs. For simplicity, we show the construction from an "unbounded" IHwUF here.

said to be blind if the ciphertext ct can be decomposed into parts $(\mathsf{ct}_1, \mathsf{ct}_2)$ such that the marginal distribution of ct_1 is independent of both the image string h and the message pair $(\mathsf{m}_0, \mathsf{m}_1)$, while the marginal distribution of ct_2 is uniform whenever the message pair $(\mathsf{m}_0, \mathsf{m}_1)$ is uniform in $\{0,1\}^2$.

Projection Function from IHwUF. The first step in instantiating a batch encryption scheme is to realize the projection function. Given an IHwUF $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$, we define $\mathsf{Gen}_{\mathrm{IHwUF}}(\mathsf{pp}, \mathbf{s})$ to output

$$h = \bigoplus_{j \in [n]} x_{j,s_j},$$

where $\{x_{j,b}\}_{j\in[n],b\in\{0,1\}}$ is a set of uniformly random elements in the input group of the IHwUF, published as part of the public parameter pp. We claim that this function is both one-way and collision resistant, provided that $n > 3\log|\mathcal{X}|$.[16]

One-wayness. To see that this function is one-way, consider a PPT adversary $\mathcal{A}$ that, given uniformly random group elements $\{x_{j,b}\}_{j\in[n],b\in\{0,1\}}$ and a "target" element x^*, outputs a vector $\mathbf{s} \in \{0,1\}^n$ such that

$$x^* = \bigoplus_{j \in [n]} x_{j,s_j}.$$

One can then construct a PPT algorithm $\mathcal{B}$ that on input $\{x_{j,b}, F(k, x_{j,b})\}_{j\in[n],b\in\{0,1\}}$ (where each $x_{j,b}$ is uniformly random) and a uniformly random target element x^*, invokes $\mathcal{A}$ as a subroutine on the tuple $\left\{x^*, \{x_{j,b}\}_{j\in[n],b\in\{0,1\}}\right\}$ to obtain $\mathbf{s} \in \{0,1\}^n$ and outputs

$$F(k, x^*) = \bigotimes_{j \in [n]} F\left(k, x_{j,s_j}\right),$$

which violates the weak unpredictability of the function F. We note that the reduction is valid because for $n > 3\log|\mathcal{X}|$, the distribution of $\bigoplus_{j\in[n]} x_{j,s_j}$ is statistically indistinguishable from uniform by the leftover hash lemma [IZ89].

Collision-Resistance. To see that this function is collision-resistant, consider a PPT adversary $\mathcal{A}$ that, given uniformly random group elements $\{x_{j,b}\}_{j\in[n],b\in\{0,1\}}$, outputs $(\mathbf{s}, \mathbf{s}') \in \{0,1\}^n \times \{0,1\}^n$ such that $\mathbf{s} \neq \mathbf{s}'$ and

$$\bigoplus_{j \in [n]} x_{j,s_j} = \bigoplus_{j \in [n]} x_{j,s'_j}.$$

[16] We note that it is possible to use a smaller constant, but we use 3 through the whole paper for the sake of simplicity.

One can then construct a PPT algorithm $\mathcal{B}$ that on input $\{x_{j,b}, F(k, x_{j,b})\}_{j\in[n],b\in\{0,1\}}$ (where each $x_{j,b}$ is uniformly random) and a random target element x^*, uniformly guesses $i \leftarrow [n]$, resets $x_{i,0} := x^*$ and invokes $\mathcal{A}$ as a subroutine on the modified set $\{x_{j,b}\}_{j\in[n],b\in\{0,1\}}$ to obtain a collision $(\mathbf{s}, \mathbf{s}')$. If $s_i = s'_i$, it aborts. Otherwise, it exploits the homomorphism of the function F to output $F(k, x^*)$. Since the probability that $\mathbf{s}$ and $\mathbf{s}'$ differ in the i^{th} bit is at least $1/n$, $\mathcal{B}$ breaks the weak unpredictability of F.

Encryption and Decryption. Corresponding to the projection function as described above, we realize our encryption procedure $\mathsf{Enc}_{\text{IHwUF}}(\mathsf{pp}, h, i, (\mathsf{m}_0, \mathsf{m}_1))$ as follows: sample $k_0, k_1 \leftarrow \mathcal{K}$ and set the following

$$\begin{aligned} y^{(0)}_{j,0} &= F(k_0, x_{j,b}), \quad y^{(1)}_{j,1} = F(k_1, x_{j,b}) \quad \text{for } j \in [n] \setminus \{i\}, b \in \{0,1\} \\ y^{(0)}_{i,0} &= F(k_0, x_{i,0}), \quad y^{(1)}_{i,0} = \perp, \\ y^{(0)}_{i,1} &= \perp, \quad y^{(1)}_{i,1} = F(k_1, x_{i,1}). \end{aligned}$$

Next, mask the messages $(\mathsf{m}_0, \mathsf{m}_1) \in \{0,1\} \times \{0,1\}$ as follows:[17]

$$\begin{aligned} \mathsf{e}_0 &= \text{XOR}(\text{HardCore}(F(k_0, h)), \mathsf{m}_0) \\ \mathsf{e}_1 &= \text{XOR}(\text{HardCore}(F(k_1, h)), \mathsf{m}_1). \end{aligned}$$

Output the ciphertext as

$$\mathsf{ct} = \left(\mathsf{ct}_1 = \left\{y^{(0)}_{j,b}, y^{(1)}_{j,b}\right\}_{j\in[n],b\in\{0,1\}}, \mathsf{ct}_2 = (\mathsf{e}_0, \mathsf{e}_1)\right).$$

Given a preimage string $\mathbf{s}$, our decryption algorithm $\mathsf{Dec}_{\text{IHwUF}}(\mathsf{pp}, \mathbf{s}, i, \mathsf{ct})$ now recovers m_{s_i} as

$$\mathsf{m}_{s_i} = \text{XOR}\left(\text{HardCore}\left(\bigotimes_{j\in[n]} y^{(s_i)}_{j,s_j}\right), \mathsf{e}_{s_i}\right).$$

Correctness follows from the homomorphic property of the function F. Observe that irrespective of the value of the bit s_i, m_{s_i} can always be recovered as the decryptor has access to $y^{(b)}_{i,b}$ for each $b \in \{0,1\}$. However, it cannot recover m_{1-s_i} since it does not have access to $y^{(b)}_{i,1-b}$ for either $b = 0$ or $b = 1$. In addition, we note that, unlike existing constructions, our construction does not require the groups $(\mathcal{X}, \oplus)$ and $(\mathcal{Y}, \otimes)$ to be abelian for correctness to hold.

[17] We assume that each group element $y \in \mathcal{Y}$ has a deterministic hardcore bit, denoted as HardCore(y). If a deterministic hardcore bit is not known then we can use the Goldreich-Levin [GL89] construction.

Security. We now sketch our security proof. Suppose we are given an adversary $\mathcal{A}$ that breaks the security of this scheme. We construct a PPT algorithm $\mathcal{B}$ that breaks the weak unpredictability of the function F. We assume that $\mathcal{B}$ has oracle access to an IHwUF F with key k.

In our security game, $\mathcal{B}$ receives a uniformly random challenge element x^* and a bit $\mathsf{e}^* \in \{0,1\}$ such that $\mathsf{e}^* = \text{HardCore}\left(F\left(k, x^*\right)\right)$ (the "real" case) or e^* is a uniform bit (the "random" case). The goal of $\mathcal{B}$ is to output a bit b, such that

$$b = \begin{cases} 0 & \text{if } \mathsf{e}^* = \text{HardCore}\left(F\left(k, x^*\right)\right) \\ 1 & \text{if } \mathsf{e}^* \leftarrow \{0,1\} \end{cases}$$

In other words, $\mathcal{B}$ must distinguish the hardcore bit associated with the output of $F\left(k, x^*\right)$ from random (which is equivalent to constructing the entire output $F\left(k, x^*\right)$)[18] using the adversary $\mathcal{A}$.

We note here that the exact value of n is typically chosen by the adversary $\mathcal{A}$ at the beginning of the game, subject to the restriction that $n > 3\log|\mathcal{X}|$. For simplicity, we describe the interaction between $\mathcal{B}$ and $\mathcal{A}$ after the value of n has been chosen.

- The adversary $\mathcal{A}$ chooses an arbitrary preimage string $\mathbf{s} \in \{0,1\}^n$ and an index $i \in [n]$, and provides $(\mathbf{s}, i)$ to $\mathcal{B}$.

- $\mathcal{B}$ queries the IHwUF F a total of $2n$ times, getting a tuple of the form

$$\left\{x_{j,b}, F\left(k, x_{j,b}\right)\right\}_{j\in[n], b\in\{0,1\}}.$$

- $\mathcal{B}$ now resets

$$x_{i,s_i} := \left(\bigoplus_{j\in[i-1]} x_{j,s_j}\right)^{-1} \oplus x^* \oplus \left(\bigoplus_{j\in[i+1,n]} x_{j,s_j}\right)^{-1},$$

  and provides $\mathsf{pp} = \left\{x_{j,b}\right\}_{j\in[n],b\in\{0,1\}}$ to $\mathcal{A}$. In other words, $\mathcal{B}$ fixes x^* to be the image of $\mathbf{s}$ under the projection function parameterized by pp.

- The adversary $\mathcal{A}$ generates $\mathbf{m}^{(0)} = \left(\mathsf{m}_0^{(0)}, \mathsf{m}_1^{(0)}\right)$ and $\mathbf{m}^{(1)} = \left(\mathsf{m}_0^{(1)}, \mathsf{m}_1^{(1)}\right)$ such that $\mathsf{m}_{s_i}^{(0)} = \mathsf{m}_{s_i}^{(1)}$, and sends them to $\mathcal{B}$.

- In response, $\mathcal{B}$ samples $k' \leftarrow \mathcal{K}$, and implicitly fixes $k_{s_i} := k'$ and $k_{1-s_i} := k$. It then sets the following

$$\begin{aligned} y_{j,s_j}^{(s_i)} &= F\left(k', x_{j,s_j}\right), \quad & y_{j,s_j}^{(1-s_i)} &= F\left(k, x_{j,s_j}\right) \quad \text{for } j \in [n]\setminus\{i\}, b \in \{0,1\}, \\ y_{i,s_i}^{(s_i)} &= F\left(k', x_{i,s_i}\right), \quad & y_{i,s_i}^{(1-s_i)} &= \perp, \\ y_{i,1-s_i}^{(s_i)} &= \perp, \quad & y_{i,1-s_i}^{(1-s_i)} &= F\left(k, x_{i,1-s_i}\right). \end{aligned}$$

[18] By the Goldreich-Levin Theorem [GL89], this can be used to build an algorithm that constructs $F\left(k, x^*\right)$ with only polynomial loss in advantage.

To mask the messages, $\mathcal{B}$ sets the following

$$\mathsf{e}_{s_i}^{(0)} = \mathrm{XOR}\left(\mathrm{HardCore}\left(F\left(k', x^*\right)\right), \mathsf{m}_{s_i}^{(0)}\right), \quad \mathsf{e}_{1-s_i}^{(0)} = \mathrm{XOR}\left(\mathsf{e}^*, \mathsf{m}_{1-s_i}^{(0)}\right),$$
$$\mathsf{e}_{s_i}^{(1)} = \mathrm{XOR}\left(\mathrm{HardCore}\left(F\left(k', x^*\right)\right), \mathsf{m}_{s_i}^{(1)}\right), \quad \mathsf{e}_{1-s_i}^{(1)} = \mathrm{XOR}\left(\mathsf{e}^*, \mathsf{m}_{1-s_i}^{(1)}\right).$$

Finally, $\mathcal{B}$ samples $b^* \leftarrow \{0,1\}$ and sends ct to $\mathcal{A}$ where

$$\mathsf{ct} = \left(\mathsf{ct}_1 = \left\{y_{j,b}^{(0)}, y_{j,b}^{(1)}\right\}_{j\in[n], b\in\{0,1\}}, \mathsf{ct}_2 = \left(\mathsf{e}_0^{(b^*)}, \mathsf{e}_1^{(b^*)}\right)\right).$$

- $\mathcal{A}$ outputs a bit b'. If $b^* = b'$, $\mathcal{B}$ outputs 1. Otherwise it outputs 0.

Note that when $\mathsf{e}^* = \mathrm{HardCore}\left(F\left(k, x^*\right)\right)$, the challenge ciphertext is generated perfectly. On the other hand, when e^* is a uniform bit, the adversary $\mathcal{A}$ has no advantage since $\mathsf{m}_{s_i}^{(0)} = \mathsf{m}_{s_i}^{(1)}$ by definition. Hence, the advantage of $\mathcal{B}$ is negligibly different from the advantage of $\mathcal{A}$.

Blindness. The aforementioned batch encryption scheme is additionally "blind". This follows from the fact that the ciphertext component ct_1 is independent of both the image string h and the message-pair $(\mathsf{m}_0, \mathsf{m}_1)$. Additionally, if $(\mathsf{m}_0, \mathsf{m}_1)$ is uniform in $\{0,1\}^2$, then the distribution of ct_2 is also uniform.

2.4 More Primitives

Recyclable OWFE. In a recent work, Garg and Hajiabadi [GH18] introduced a cryptographic primitive called recyclable *one-way function with encryption* (OWFE), and showed that recyclable OWFEs imply trapdoor functions (TDFs) with negligibly small inversion error. They also showed how to construct recyclable OWFE from the CDH assumption, which in turn gave the first TDF construction from the CDH assumption. In a more recent follow-up, Garg *et al.* [GGH18] introduced a strengthened version of recyclable OWFE called *smooth* recyclable OWFE, and showed how to realize the same from CDH assumption. They showed that this strengthened primitive implies TDFs with almost-perfect correctness and CCA2-secure deterministic encryption, where the CCA2-security holds with respect to plaintexts sampled from distributions with super-logarithmic min-entropy.

We show that IHwUFs imply smooth recyclable OWFE, thereby answering the question of whether this cryptosystem can be constructed from a generic primitive. This shows that IHwUFs also imply TDFs with almost-perfect correctness and CCA2-secure deterministic encryption for plaintexts sampled from distributions with super-logarithmic min-entropy. The techniques for this construction are similar to those presented for batch encryption.

Hinting PRG. A "hinting PRG" is a stronger variant of traditional PRGs introduced by Koppula and Waters in [KW18], who show that hinting PRGs can be used to generically transform any CPA-secure attribute-based encryption scheme or one-sided predicate encryption scheme into a CCA-secure counterpart. Informally, a hinting PRG takes n bits as input and outputs $n \cdot \ell$ output bits with the restriction that no PPT adversary can distinguish between $2n$ uniformly random strings and $2n$ strings such that half the strings are output by the PRG, and the remaining half are uniformly random, where the strings are arranged as a $2 \times n$ matrix as follows: in the i^{th} column of this matrix, the top entry is pseudorandom and the bottom entry is random if the i^{th} bit of the seed is 0; otherwise the bottom entry is pseudorandom and top entry is random.

Koppula and Waters [KW18] showed explicit constructions of hinting PRG families from the CDH and LWE assumptions. We show that any IHwUF family can be used to construct a hinting PRG, thereby answering the question of whether hinting PRGs can be constructed from a generic primitive. The techniques for our construction are also similar to those presented for batch encryption.

CRHF and More from HOWF. Informally, a HOWF is just a one-way function $f : \mathcal{X} \to \mathcal{Y}$ with the following additional properties: the input space $\mathcal{X}$ and the output space $\mathcal{Y}$ are groups with group operations $\oplus$ and $\otimes$, respectively, and

$$f(x_1 \oplus x_2) = f(x_1) \otimes f(x_2).$$

In this paper, we show that any HOWF can used to construct a collision-resistant hash function (CRHF) family that maps bit strings to elements in the output space of the HOWF. In addition, we show constructions of Schnorr signatures and chameleon hash functions from HOWFs. [19]

Richer Structures. As mentioned earlier, we can also consider richer structures than just a group homomorphism over a Minicrypt primitive. In this section, we provide more details for two of these more structured primitives, namely Ring IHwPRFs and L-composable IHwPRFs.

Ring IHwPRFs. We first informally define a Ring Input-Homomorphic weak PRF (RIHwPRF). Let $(R, +, \times)$ and $(\boxed{R}, \boxplus, \boxtimes)$ be two efficiently samplable rings such that the ring operations are efficiently computable. An RIHwPRF is a weak PRF

$$F : \mathcal{K} \times \boxed{R} \to R$$

[19] Here we use "unbounded" HOWF for simplicity. We also consider "bounded" HOWFs for which only a bounded number of homomorphic operations is allowed. The notion of bounded HOWFs works for all of the applications that we consider in almost the same way that unbounded HOWFs do.

(with input space $\boxed{R}$ and output space R) such that for every key $k \in \mathcal{K}$ the mapping $F(k,\cdot) : \boxed{R} \to R$ is a ring homomorphism from $\boxed{R}$ to R.[20]

We outline a simple construction of symmetric-key FHE from an RIHwPRF F provided that the size of output space of F is polynomial in the security parameter, i.e., $|R| \leq \text{poly}(\lambda)$. Using the generic transformation in [Rot11], one can obtain a public-key FHE from a symmetric-key FHE. The construction is as follows:

- Given an RIHwPRF $F : \mathcal{K} \times \boxed{R} \to R$, publish its description as the public parameters. To generate a secret key sample a key $k \leftarrow \mathcal{K}$.
- To encrypt a bit $\mathsf{m} \in \{0,1\}$ under key k, sample a preimage $\mathsf{ct} \leftarrow \boxed{R}$ such that $F(k,\mathsf{ct}) = \mathsf{m}_R$ and publish ct as the ciphertext.[21] (Notice that 0_R and 1_R are the multiplicative and the additive identity elements of R, respectively.)
- To decrypt a ciphertext $\mathsf{ct} \in \boxed{R}$ under key k, output m' where

$$\mathsf{m}' = \begin{cases} 0 & \text{if } F(k,\boxed{r}) = 0_R \\ 1 & \text{if } F(k,\boxed{r}) = 1_R \\ \perp & \text{otherwise.} \end{cases}$$

- To evaluate a (homomorphic) $\mathsf{NAND}(\mathsf{ct},\mathsf{ct}')$ operation, output $\boxed{1} \boxminus \mathsf{ct} \boxtimes \mathsf{ct}'$ where $\boxed{1}$ is the identity element of $\boxed{R}$ with respect to addition, and $\boxminus$ is the subtraction in the ring $\boxed{R}$.

The security of the scheme follows from a standard hybrid argument. Observe that by ring-homomorphism of F, if ct and ct' are valid ciphertexts encrypting m and m' respectively, decrypting $\boxed{1} \boxminus \mathsf{ct} \boxtimes \mathsf{ct}'$ gives $\mathsf{NAND}(\mathsf{m},\mathsf{m}')$.

***L*-Composable IHwPRFs.** We first describe 2-Composable IHwPRFs before generalizing to $L \geq 2$. Informally, a two-composable IHwPRF is a collection of two functions and two "composers"

$$F_1 : \mathcal{K} \times \mathcal{X}_1 \to \mathcal{Y}_1\,, \quad F_2 : \mathcal{K} \times \mathcal{X}_2 \to \mathcal{Y}_2,$$
$$C_1 : \mathcal{Y}_1 \times \mathcal{X}_2 \to \mathcal{Z}\,, \quad C_2 : \mathcal{Y}_2 \times \mathcal{X}_1 \to \mathcal{Z}.$$

such that the functions are IHwPRFs and the composers are weak PRFs. Additionally, the following composition property holds: for every $k \in \mathcal{K}$ and for every $x_1, x_2 \in \mathcal{X}$, we have:

$$C_1\left(F_1\left(k,x_1\right),x_2\right) = C_2\left(F_2\left(k,x_2\right),x_1\right), \text{ both denoted } F_T(k,(x_1,x_2)).$$

[20] It is also possible to define (bounded) RIHwPRFs similar to IHwPRFs, but we only consider unbounded homomorphism here for the sake of simplicity.

[21] Such a preimage can be efficiently sampled by weak pseudorandomness of F and the fact that the order of the ring is polynomial.

This primitive gives us 3-party non-interactive key exchange (NIKE) in the following way: the public key includes vectors $\mathbf{x}^{(1)}$ and $\mathbf{x}^{(2)}$. Two of the parties generate secret subsets $\mathbf{s}_1$ and $\mathbf{s}_2$, and publish the group elements

$$\bigoplus_{j\in[n]} x^{(1)}_{j,s_{1,j}}, \quad \bigoplus_{j\in[n]} x^{(2)}_{j,s_{2,j}},$$

respectively. The 3rd party generates a secret key k and publishes $F_1(k, \mathbf{x}^{(1)})$ and $F_2(k, \mathbf{x}^{(2)})$. Each party computes the shared key:

$$F_T\Big(k, \Big(\bigoplus_{j\in[n]} x^{(1)}_{j,s_{1,j}}, \bigoplus_{j\in[n]} x^{(2)}_{j,s_{2,j}}\Big)\Big),$$

which can be computed from any party's secret and the other parties' outputs, using the composition property and input homomorphism of F_1 and F_2. Security follows by the weak PRF properties and LHL.

We argue that 2-composable IHwPRFs are seemingly much weaker than bilinear pairing groups. Specifically, we argue that the general abstraction of dual system groups (DSG [CGW15]) is hard to capture in the 2-Composable IHwPRF setting due to the following limitations:

1. DSG seems to require properties that translate to the requirement of key homomorphism in the 2-composable IHwPRF setting.
2. DSG also requires algebraic interaction on both of the coordinates. Realizing this in the IHwPRF setting forces both the coordinate domains $\mathcal{X}_1$ and $\mathcal{X}_2$ to be *ring homomorphic* on a single ring, where all the algebra can take place.

The currently known constructions of rich ABEs like fuzzy IBEs [SW05], spatial encryption [BH08] and monotone span program ABEs [GPSW06] from bilinear groups all require at least one of the properties just described. Since the only instantiation of 2-composable IHwPRFs we know of are bilinear groups, it seems difficult to achieve these rich ABEs without restricting 2-composable IHwPRFs to almost traditional bilinear groups.

Thus we see a seeming separation in the amount of structure that we need for 3-party NIKE and simple IBE (in RO) from that seemingly necessary for NIZKs (without RO) and rich ABEs. This poses a tantalizing question: *Can we construct a 3-party NIKE protocol from a weaker primitive than bilinear pairing groups?* In other words, can we achieve the structure of 2-composability from concrete assumptions, e.g., lattice-based assumptions, that do not naturally imply bilinear pairings?

Generalizing to $\mathbf{L \geq 2}$. In the general setting, we consider L inner IHwPRFs F_i and L different composers which satisfy an analogous composition property as the 2-composable setting. By a straightforward generalization, we get an $(L+1)$-party non-interactive key exchange from an L-Composable IHwPRF, which is not known from any $(< L)$-Composable IHwPRFs. We also do not know how

to construct such a protocol from any hard ($< L$)-multilinear group. We still observe an analogous seeming separation in the amount of structure that we need for multi-party non-interactive key exchange from that seemingly necessary for circuit ABEs and iOs. The corresponding open question is whether we can build the former from weaker primitives that may lack the structure needed for the latter.

2.5 Conclusion and Future Work

In this paper, we presented a framework to build many cryptosystems from Minicrypt primitives with structure. Our framework allows us to categorize many cryptosystems based on which structured Minicrypt primitive implies them, and potentially makes showing the *existence* of many cryptosystems from novel assumptions substantially easier in the future. In addition, some of our constructions are novel in their own right. Although our framework yields new constructions from less studied assumptions, the main focus of this work is to investigate what kind of structure, when added to simple and natural Minicrypt primitives, implies advanced cryptosystems like IBE. Hence, we are not explicitly examining new constructions from a mainstream assumption. We believe that our work opens up a substantial number of questions, some of which we mention here.

Primitives from Weaker Assumptions. A pertinent open question is: can we build some of the Cryptomania primitives discussed in this paper from weaker Minicrypt primitives with structure. For instance, can we build PKE from HOWFs (which would imply PKE from discrete log)? Can we build PIR/lossy TDFs from IHwUFs (which would imply the first PIR/lossy TDFs from CDH)? Is it possible to build round-optimal OT and MPC in the plain model from IHwUFs/IHwPRFs?

More Primitives. While we constructed many popularly used Cryptomania primitives from our framework, we could not encompass many others. These (non-exhaustively) include primitives implied by bilinear pairings such as NIZK, unique signatures, VRFs, ABE and PE, and primitives known from specific assumptions such as worst-case smooth hash proof systems, KDM-CCA secure PKE and dual-mode cryptosystems. It is open to construct one or more of these primitives from simple Minicrypt primitives with structure.

New Assumptions. One of the nicest aspects of our work is the implications for new assumptions. If a new assumption implies one of the Minicrypt primitives with structure discussed in this paper, then it immediately implies a whole host of cryptographic primitives. We leave it open to build HOWFs/IHwUFs/IHwPRFs from new concrete assumptions, which in conjunction with our framework would allow building a large number of Cryptomania primitives from such assumptions.

"Continents" of Cryptomania. We leave it open to explore if there are even weaker forms of structure that, when endowed upon Minicrypt primitives, lead to interesting implications in Cryptomania. It is also interesting to explore non-trivial separations between these structured primitives, e.g., between HOWFs and IHwUFs. Such separations would potentially allow us to divide the world of Cryptomania into many "continents" of primitives, where each "continent" is entirely implied by some simple Minicrypt primitive with structure.

References

[AD97] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *29th ACM STOC*, pages 284–293. ACM Press, May 1997.

[Ajt96] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *28th ACM STOC*, pages 99–108. ACM Press, May 1996.

[AMG07] C. Aguilar-Melchor and P. Gaborit. A lattice-based computationally-efficient private information retrieval protocol. In *Western European Workshop on Research in Cryptology*. Citeseer, 2007.

[AS15] G. Asharov and G. Segev. Limits on the power of indistinguishability obfuscation and functional encryption. In V. Guruswami, editor, *56th FOCS*, pages 191–209. IEEE Computer Society Press, October 2015.

[Bar17] B. Barak. The complexity of public-key cryptography. Cryptology ePrint Archive, Report 2017/365, 2017. `https://eprint.iacr.org/2017/365`.

[BBF13] P. Baecher, C. Brzuska, and M. Fischlin. Notions of black-box reductions, revisited. In K. Sako and P. Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 296–315. Springer, Heidelberg, December 2013.

[BDRV18] I. Berman, A. Degwekar, R. D. Rothblum, and P. N. Vasudevan. From laconic zero-knowledge to public-key cryptography - extended abstract. In H. Shacham and A. Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 674–697. Springer, Heidelberg, August 2018.

[BDV17] N. Bitansky, A. Degwekar, and V. Vaikuntanathan. Structure vs. hardness through the obfuscation lens. In J. Katz and H. Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 696–723. Springer, Heidelberg, August 2017.

[BGI+01] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. P. Vadhan, and K. Yang. On the (im)possibility of obfuscating programs. In J. Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 1–18. Springer, Heidelberg, August 2001.

[BH08] D. Boneh and M. Hamburg. Generalized identity based and broadcast encryption schemes. In J. Pieprzyk, editor, *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 455–470. Springer, Heidelberg, December 2008.

[BHY09] M. Bellare, D. Hofheinz, and S. Yilek. Possibility and impossibility results for encryption and commitment secure under selective opening. In *EUROCRYPT*, pages 1–35. 2009.

[BLMR13] D. Boneh, K. Lewi, H. W. Montgomery, and A. Raghunathan. Key homomorphic PRFs and their applications. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 410–428. Springer, Heidelberg, August 2013.

[BLSV18] Z. Brakerski, A. Lombardi, G. Segev, and V. Vaikuntanathan. Anonymous IBE, leakage resilience and circular security from new assumptions. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 535–564. Springer, Heidelberg, April / May 2018.

[BM82] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudo random bits. In *23rd FOCS*, pages 112–117. IEEE Computer Society Press, November 1982.

[BR17] A. Bogdanov and A. Rosen. Pseudorandom functions: Three decades later. Cryptology ePrint Archive, Report 2017/652, 2017. `https://eprint.iacr.org/2017/652`.

[BSW11] D. Boneh, A. Sahai, and B. Waters. Functional encryption: Definitions and challenges. In Y. Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 253–273. Springer, Heidelberg, March 2011.

[CGW15] J. Chen, R. Gay, and H. Wee. Improved dual system ABE in prime-order groups via predicate encodings. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 595–624. Springer, Heidelberg, April 2015.

[DG17a] N. Döttling and S. Garg. From selective IBE to full IBE and selective HIBE. In Y. Kalai and L. Reyzin, editors, *TCC 2017, Part I*, volume 10677 of *LNCS*, pages 372–408. Springer, Heidelberg, November 2017.

[DG17b] N. Döttling and S. Garg. Identity-based encryption from the Diffie-Hellman assumption. In J. Katz and H. Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 537–569. Springer, Heidelberg, August 2017.

[DGHM18] N. Döttling, S. Garg, M. Hajiabadi, and D. Masny. New constructions of identity-based and key-dependent message secure encryption schemes. In M. Abdalla and R. Dahab, editors, *PKC 2018, Part I*, volume 10769 of *LNCS*, pages 3–31. Springer, Heidelberg, March 2018.

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[DHS15] D. Derler, C. Hanser, and D. Slamanig. Revisiting cryptographic accumulators, additional properties and relations to other primitives. In K. Nyberg, editor, *CT-RSA 2015*, volume 9048 of *LNCS*, pages 127–144. Springer, Heidelberg, April 2015.

[ElG84] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and D. Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 10–18. Springer, Heidelberg, August 1984.

[FH18] M. Fischlin and P. Harasser. Invisible sanitizable signatures and public-key encryption are equivalent. In B. Preneel and F. Vercauteren, editors, *ACNS 18*, volume 10892 of *LNCS*, pages 202–220. Springer, Heidelberg, July 2018.

[Fis12] M. Fischlin. Black-box reductions and separations in cryptography (invited talk). In A. Mitrokotsa and S. Vaudenay, editors, *AFRICACRYPT 12*, volume 7374 of *LNCS*, pages 413–422. Springer, Heidelberg, July 2012.

[FMV18] D. Friolo, D. Masny, and D. Venturi. Secure multi-party computation from strongly uniform key agreement. Cryptology ePrint Archive, Report 2018/473, 2018. `http://eprint.iacr.org/`.

[Gen09] C. Gentry. Fully homomorphic encryption using ideal lattices. In M. Mitzenmacher, editor, *41st ACM STOC*, pages 169–178. ACM Press, May / June 2009.

[GGH13a] S. Garg, C. Gentry, and S. Halevi. Candidate multilinear maps from ideal lattices. In T. Johansson and P. Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 1–17. Springer, Heidelberg, May 2013.

[GGH+13b] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *54th FOCS*, pages 40–49. IEEE Computer Society Press, October 2013.

[GGH18] S. Garg, R. Gay, and M. Hajiabadi. New techniques for efficient trapdoor functions and applications. Cryptology ePrint Archive, Report 2018/872, 2018. `http://eprint.iacr.org/`.

[GGM84] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions (extended abstract). In *25th FOCS*, pages 464–479. IEEE Computer Society Press, October 1984.

[GH18] S. Garg and M. Hajiabadi. Trapdoor functions from the computational diffie-hellman assumption. In *CRYPTO*, pages 362–391. 2018.

[GHMM18] S. Garg, M. Hajiabadi, M. Mahmoody, and A. Mohammed. Limits on the power of garbling techniques for public-key encryption. In H. Shacham and A. Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 335–364. Springer, Heidelberg, August 2018.

[GL89] O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In *21st ACM STOC*, pages 25–32. ACM Press, May 1989.

[GPR16] V. Goyal, O. Pandey, and S. Richelson. Textbook non-malleable commitments. In *STOC*. 2016.

[GPSW06] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In A. Juels, R. N. Wright, and S. Vimercati, editors, *ACM CCS 06*, pages 89–98. ACM Press, October / November 2006. Available as Cryptology ePrint Archive Report 2006/309.

[GPSZ17] S. Garg, O. Pandey, A. Srinivasan, and M. Zhandry. Breaking the subexponential barrier in obfustopia. In J. Coron and J. B. Nielsen, editors, *EUROCRYPT 2017, Part III*, volume 10212 of *LNCS*, pages 156–181. Springer, Heidelberg, April / May 2017.

[GPV08] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In R. E. Ladner and C. Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.

[GW11] C. Gentry and D. Wichs. Separating succinct non-interactive arguments from all falsifiable assumptions. In L. Fortnow and S. P. Vadhan, editors, *43rd ACM STOC*, pages 99–108. ACM Press, June 2011.

[HHRS07] I. Haitner, J. J. Hoch, O. Reingold, and G. Segev. Finding collisions in interactive protocols - a tight lower bound on the round complexity of statistically-hiding commitments. In *48th FOCS*, pages 669–679. IEEE Computer Society Press, October 2007.

[HILL99] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.

[HKS16] M. Hajiabadi, B. M. Kapron, and V. Srinivasan. On generic constructions of circularly-secure, leakage-resilient public-key encryption schemes. In C.-M. Cheng, K.-M. Chung, G. Persiano, and B.-Y. Yang, editors, *PKC 2016, Part II*, volume 9615 of *LNCS*, pages 129–158. Springer, Heidelberg, March 2016.

[HO12] B. Hemenway and R. Ostrovsky. On homomorphic encryption and chosen-ciphertext security. In M. Fischlin, J. Buchmann, and M. Manulis, editors, *PKC 2012*, volume 7293 of *LNCS*, pages 52–65. Springer, Heidelberg, May 2012.

[IKLP06] Y. Ishai, E. Kushilevitz, Y. Lindell, and E. Petrank. Black-box constructions for secure computation. In J. M. Kleinberg, editor, *38th ACM STOC*, pages 99–108. ACM Press, May 2006.

[IKO05] Y. Ishai, E. Kushilevitz, and R. Ostrovsky. Sufficient conditions for collision-resistant hashing. In J. Kilian, editor, *TCC 2005*, volume 3378 of *LNCS*, pages 445–456. Springer, Heidelberg, February 2005.

[Imp95] R. Impagliazzo. A personal view of average-case complexity. In *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*, pages 134–147. June 1995. ISSN 1063-6870.

[IZ89] R. Impagliazzo and D. Zuckerman. How to recycle random bits. In *30th FOCS*, pages 248–253. IEEE Computer Society Press, October / November 1989.

[KO97] E. Kushilevitz and R. Ostrovsky. Replication is NOT needed: SINGLE database, computationally-private information retrieval. In *FOCS*, pages 364–373. 1997.

[KW18] V. Koppula and B. Waters. Realizing chosen ciphertext security generically in attribute-based encryption and predicate encryption. Cryptology ePrint Archive, Report 2018/847, 2018. `http://eprint.iacr.org/`.

[MM16] M. Mahmoody and A. Mohammed. On the power of hierarchical identity-based encryption. In M. Fischlin and J.-S. Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 243–272. Springer, Heidelberg, May 2016.

[MMN+16] M. Mahmoody, A. Mohammed, S. Nematihaji, R. Pass, and A. Shelat. Lower bounds on assumptions behind indistinguishability obfuscation. In E. Kushilevitz and T. Malkin, editors, *TCC 2016-A, Part I*, volume 9562 of *LNCS*, pages 49–66. Springer, Heidelberg, January 2016.

[OSV15] R. Ostrovsky, A. Scafuro, and M. Venkitasubramaniam. Resettably sound zero-knowledge arguments from OWFs - the (semi) black-box way. In Y. Dodis and J. B. Nielsen, editors, *TCC 2015, Part I*, volume 9014 of *LNCS*, pages 345–374. Springer, Heidelberg, March 2015.

[PS08] K. Pietrzak and J. Sjödin. Weak pseudorandom functions in minicrypt. In L. Aceto, I. Damgård, L. A. Goldberg, M. M. Halldórsson, A. Ingólfsdóttir, and I. Walukiewicz, editors, *ICALP 2008, Part II*, volume 5126 of *LNCS*, pages 423–436. Springer, Heidelberg, July 2008.

[PW08] C. Peikert and B. Waters. Lossy trapdoor functions and their applications. In R. E. Ladner and C. Dwork, editors, *40th ACM STOC*, pages 187–196. ACM Press, May 2008.

[Reg05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In H. N. Gabow and R. Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.

[Rom90] J. Rompel. One-way functions are necessary and sufficient for secure signatures. In *22nd ACM STOC*, pages 387–394. ACM Press, May 1990.

[Rot11] R. Rothblum. Homomorphic encryption: From private-key to public-key. In Y. Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 219–234. Springer, Heidelberg, March 2011.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[RTV04] O. Reingold, L. Trevisan, and S. P. Vadhan. Notions of reducibility between cryptographic primitives. In M. Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 1–20. Springer, Heidelberg, February 2004.

[Sha84] A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and D. Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 47–53. Springer, Heidelberg, August 1984.

[SW05] A. Sahai and B. R. Waters. Fuzzy identity-based encryption. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473. Springer, Heidelberg, May 2005.