Correlated Pseudorandom Functions from Variable-Density LPN

Elette Boyle*, Geoffroy Couteau†, Niv Gilboa‡, Yuval Ishai§, Lisa Kohl§ and Peter Scholl¶
*IDC Herzliya, Herzliya, Israel
†IRIF, Paris, France
‡Ben-Gurion University, Be'er Sheva, Israel
§Technion, Haifa, Israel
¶Aarhus University, Aarhus, Denmark
Email: eboyle@alum.mit.edu, couteau@irif.fr, niv.gilboa@gmail.com, yuvali@cs.technion.ac.il, lisamariakohl@gmail.com, peter.scholl@cs.au.dk

***Abstract*—Correlated secret randomness is a useful resource for many cryptographic applications. We initiate the study of *pseudorandom correlation functions* (PCFs) that offer the ability to securely generate virtually unbounded sources of correlated randomness using only local computation. Concretely, a PCF is a keyed function F_k such that for a suitable joint key distribution (k_0, k_1), the outputs $(f_{k_0}(x), f_{k_1}(x))$ are indistinguishable from instances of a given target correlation. An essential security requirement is that indistinguishability hold not only for outsiders, who observe the pairs of outputs, but also for *insiders* who know one of the two keys.**

We present efficient constructions of PCFs for a broad class of useful correlations, including oblivious transfer and multiplication triple correlations, from a *variable-density* variant of the Learning Parity with Noise assumption (VDLPN). We also present several cryptographic applications that motivate our efficient PCF constructions.

The VDLPN assumption is independently motivated by two additional applications. First, different flavors of this assumption give rise to weak pseudorandom function candidates in depth-2 $\mathsf{AC}^0[\oplus]$ that can be conjectured to have subexponential security, matching the best known learning algorithms for this class. This is contrasted with the quasipolynomial security of previous (higher-depth) $\mathsf{AC}^0[\oplus]$ candidates. We support our conjectures by proving resilience to several classes of attacks. Second, VDLPN implies simple constructions of pseudorandom generators and weak pseudorandom functions with security against XOR related-key attacks.

I. Introduction

Correlated secret randomness is a ubiquitous resource in cryptography. A one-time pad, namely a pair of identical random keys, enables perfectly secure communication. Kilian [1] and Beaver [2], [3] showed that more complex forms of correlated randomness can similarly facilitate *secure multiparty computation* (MPC)—protocols that enable two or more parties to jointly compute a function of secret inputs revealing nothing beyond the output. A useful example is an *oblivious transfer* (OT) correlation, where one party is given two random bits (s_0, s_1) and another party gets (b, s_b) for a random bit b. Cryptographic power stems from the fact that the correlation forms a *non-product distribution* in which neither party can determine the secret of the other party.

Such correlations not only provide feasibility results, but are a central tool in essentially all concretely efficient instantiations of MPC in the setting of a dishonest majority. For example, two honest-but-curious parties can securely evaluate any Boolean circuit with s AND gates (and an arbitrary number of XOR/NOT gates) using $2s$ independent instances of an OT correlation, and communicating $2s$ bits per party. Moreover, the local computation of both parties involves just a small constant number of bit-operations per gate [4], [5]. The efficiency and simplicity of MPC protocols based on correlated randomness gives rise to the following common paradigm. In an *offline preprocessing phase*, before the inputs are known, the parties use a dedicated protocol to securely generate correlated randomness. Then, once the inputs are available, the parties use a (typically very efficient) *online protocol* to to securely evaluate the target function by consuming the correlated randomness. The main challenge, and the core bottleneck of almost all practically oriented protocols, is to design efficient methods to securely generate correlated randomness, without revealing more information than prescribed by the joint distribution.

A sequence of recent works [6]–[9] put forth a new technique for securely generating correlated randomness via *pseudorandom correlation generators* (PCGs). In the two-party case, a PCG provides a means for locally expanding a short correlated pair of seeds to a longer instance of a pseudorandom correlation. PCGs enable secure computation with "silent" preprocessing, where parties use a small amount of communication to securely generate the correlated seeds and then expand them to the target correlation without any interaction. Moreover, recent PCG constructions achieve this for useful correlations and with good concrete efficiency.

However, PCGs come with a major limitation: The expansion of the correlated seeds is an "all-or-nothing" procedure, where the target correlation is produced *all at once* without enabling fast random access to the long output. This is similar to the limitation of a standard pseudorandom generator (PRG), except that existing PCG constructions do not even support the type of (stateful) *incremental* evaluation enabled by standard PRGs in a "stream-cipher mode." This limits the

2575-8454/20/$31.00 ©2020 IEEE
DOI 10.1109/FOCS46700.2020.00103

use of PCGs to a monolithic form of silent preprocessing that requires parties to generate and store big amounts of correlated randomness they *might* want to use in the future.

In this work, we initiate the study of the natural desired target: a *pseudorandom correlation function*[1] (PCF), which extends a PCG analogously to the way a *pseudorandom function* (PRF) [10] extends a PRG. Concretely, we seek to design short correlations of keys that can be expanded "on the fly" to a *virtually unbounded* number of pseudorandom correlation instances, and which further enable fast random access to these instances.

A bit more precisely, recall that a PRF is a keyed function $f_k : \{0,1\}^n \to \{0,1\}^{\ell(n)}$, such that for a secret random key k, the outputs of f_k are computationally indistinguishable from those of a random function. A *strong PRF* (or just PRF) is secure against distinguishers that query the function on arbitrary inputs x, while for a *weak PRF* (WPRF) the distinguisher is only given *samples* $(x_i, f_k(x_i))$ for uniformly random inputs x_i. Generalizing this notion, a (two-party) PCF is a keyed function f_k such that for a suitable joint key distribution (k_0, k_1), the outputs $(f_{k_0}(x_i), f_{k_1}(x_i))$ are indistinguishable from instances of a given target correlation. An essential security requirement is that indistinguishability hold not only for outsiders, who observe the pairs of outputs, but also for *insiders* who know one of the two keys. Here too, one can consider both a strong PCF and a weak PCF. We use the weak notion by default, since it is easier to construct and it suffices for our motivating applications.

Traditional techniques for upgrading a PRG to a PRF in the standard setting, such as the tree-based GGM construction [10], do not apply here. The challenge lies in the requirement of security against insiders. Applying a GGM-style approach would require a PCG that expands its seeds to two instances of its own seed correlation. This seems infeasible for current PCG constructions and calls for a different approach to PCF design.

A. *Overview of Contributions*

In this work, we initiate a systematic study of pseudorandom correlation functions, and investigate related primitives and assumptions. We make the following main contributions.

Definition and generic construction. We start by formally defining (weak and strong) PCFs and put forth a natural general template for constructing them. The construction combines a (weak) PRF f_k with a *function secret sharing* (FSS) [11] scheme for either the PRF class itself or closely related function classes. A (two-party) FSS scheme for a function class $\mathcal{F}$ enables splitting any function $f \in \mathcal{F}$ into two succinctly described functions (f_0, f_1), such that $f = f_0 + f_1$ and each share f_i hides f. We show how our template can be instantiated using known FSS schemes for circuits [12], [13] together with any PRF. This leads to a general PCF construction for a useful class of "additive" correlations, which includes most of the useful correlations for MPC, under a standard cryptographic assumption, namely the *Learning With Errors* (LWE) assumption [14].

PCFs from VDLPN. While the above LWE-based construction provides a theoretical feasibility result, it has poor asymptotic and concrete efficiency. Moreover, the construction uses the heavy machinery of fully homomorphic encryption and leaves open the possibility of constructing useful PCF instances from other, seemingly weaker, assumptions. We show how to efficiently construct PCFs for a broad class of useful correlations, including oblivious transfer (OT), vector oblivious linear-function evaluation (VOLE) [6], [15], and "multiplication triple" correlations [2], from a natural *variable-density* variant of the Learning Parity with Noise (LPN) assumption [16], or VDLPN for short, that we introduce and study in this work. These efficient PCF constructions are motivated by applications to MPC and non-interactive zero knowledge.

Applications of VDLPN. The VDLPN assumption is independently motivated by two additional applications. First, different flavors of this assumption give rise to WPRF candidates in depth-2 $\mathsf{AC}^0[\oplus]$ (concretely, XOR of conjunctions of input variables and their negations) that can be conjectured to have subexponential security, matching the best known learning algorithms for this class [17]. This is contrasted with the quasipolynomial security of previous (higher-depth) $\mathsf{AC}^0[\oplus]$ candidates [18], [19]. We support the VDLPN assumption and related conjectures by proving resilience to several classes of attacks, including *linear attacks* that use the input samples to find a biased linear combination of the outputs, and *algebraic* attacks that exploit low rational degree. Finally, we observe that VDLPN implies simple constructions of PRGs and WPRFs with security against XOR related-key attacks. Previous constructions are either heuristic or rely on strong assumptions such as multilinear maps [20].

The following sections give a more detailed account of the the new WPRF candidates, the PCF constructions that build on them, and different kinds of applications. Most of the technical details are deferred to the full version.

B. *Low-Complexity WPRF Candidates*

Motivated by the goals of improving the efficiency of PCFs and diversifying the underlying assumptions, we put forth a new kind of WPRF candidates that are "FSS-friendly" in the sense of being compatible with existing PRG-based FSS schemes. Our candidates are in a very low complexity class: the class $\mathsf{XOR} \circ \mathsf{AND}$ of polynomial-size, depth-2 boolean circuits with one layer of AND gates at

[1] One could alternatively view a PCF as a pair of *correlated pseudorandom functions*. The term *pseudorandom correlation function* (similarly to a pseudorandom correlation *generator*) refers to a single function f_k that samples from a pseudorandom correlation given suitably correlated keys.

the bottom and a single XOR gate at the top (both of arbitrary fan-in).[2] We also refer to such a circuit as an *XNF formula* (for Xor Normal Form). We conjecture our candidates to have *subexponential* security in both the key length and the input length. Concretely, our main candidate $f_k : \{0,1\}^n \to \{0,1\}$ is of the form

$$f_k(x) = \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{m} \bigwedge_{h=1}^{j} (x_{i,j,h} \oplus k_{i,j,h}). \qquad (1)$$

(Other variants of this candidate are given in Section II and the full version.) The security of this WPRF candidate is based on a natural *variable-density* flavor of the well-studied *learning parity with noise* (LPN) assumption that we will discuss below. A slightly different candidate is plausibly secure against $2^{o(\sqrt{n})}$-time distinguishers, matching the best known learning algorithm for this class [17]. (Restricting the distinguisher to a smaller number of samples, say $2^{n^{o(1)}}$, we get plausible security against $2^{o(n/\log n)}$-time distinguishers.) Subexponential security is good enough to support λ bits of security (against 2^λ-bounded adversaries) in poly(λ) time, and is typically the strongest level of security one can hope to obtain from standard cryptographic assumptions.

In contrast to our candidates, previous WPRF candidates in $\mathsf{AC}^0[\oplus]$ (namely, of constant-depth polynomial-size circuits with AND/OR/XOR gates of unbounded fan-in) were restricted to *quasipolynomial* security, which is considered "borderline insecure" and cannot support λ bits of security in poly(λ) time. Thus, our candidates fill a gap in the current landscape of (weak) PRF candidates in low complexity classes. See Section II below for related work.

We support the conjectured security of our candidates by analysis that proves their security against several classes of natural attacks, capturing essentially any relevant class of attacks we are aware of. This includes, for instance, *linear* attacks that try to correlate the outputs via an input-dependent linear combination, as well as *algebraic* attacks that exploit a low *rational degree*. The latter yielded a quasipolynomial-time distinguisher for a previous WPRF candidate in $\mathsf{AC}^0[\oplus]$ [18], [19].

Assuming our conjectures, the complexity class $\mathsf{AC}^0[\oplus]$ does not admit a $2^{n^{o(1)}}$-time learning algorithm, even under the uniform distribution. In fact, the same holds for the class of XNF formulas that can be alternatively viewed as sparse $\mathbb{F}_2$-polynomials in inputs and their negations. This also implies similar hardness for learning sparse $\mathbb{F}_2$-polynomials (without negations) in the standard PAC model, which allows for arbitrary input distributions. Our analysis and conjectured hardness assumptions complement the $2^{\tilde{O}(\sqrt{n})}$-time PAC learning algorithm from [17] for sparse polynomials, which also applies to XNF formulas by changing the input distribution. The conjectured hardness should be contrasted with efficient learning algorithms when *membership queries* are allowed [21], [22]. This corresponds to our WPRF candidates not being strong PRFs.

C. Variable-Density LPN

The security hypothesis for our main WPRF candidate from Eq. (1) can be cast as a new natural variant of the standard *Learning Parity with Noise* (LPN) assumption [16]. We explain this below.

In its dual formulation, LPN asserts that for suitably chosen parity-check matrix $H \in \mathbb{F}_2^{N \times M}$ and noise vector $e \in \mathbb{F}_2^M$, the distribution (H, He) is pseudorandom, namely it is indistinguishable from (H, r) for a uniform vector $r \in \mathbb{F}_2^N$ chosen independently of H. Here H is typically chosen to be a uniformly random matrix and e an i.i.d. noise vector in which each entry is set to 1 with probability $0 < p < 1/2$. Many other flavors of LPN have been used for different cryptographic applications. For instance, H can be structured [23], [24] or even of "medium density" [25]. The noise vector e is sometimes chosen to have a fixed weight or even a *regular* structure [26], where e consist of disjoint blocks and each block contains a single nonzero entry in a random position.

In the context of our WPRF candidates, each of the N rows H_i of H is determined by a corresponding random random input sample x_i, and the secret noise vector e by the secret key k. This means that N is super-polynomial in the input length n, and hence also M. (Indeed, if $M \leq \mathsf{poly}(n)$ and $M < N$, one can efficiently find a linear dependency between any $N+1$ rows of H and use this to break the WPRF.) In this setting, we need to set probability distributions for H and e such that the (dual) LPN assumption holds and yet $H_i \cdot e$ is computable in $\mathsf{poly}(n)$ time. This rules out all of the typical choices of H and e mentioned above.

A natural solution is to make e a uniformly random *sparse* vector, say of Hamming weight n. However, this requires the rows of H to be dense, or else the outputs $H_i \cdot e$ will be biased towards 0. The latter means that either each row of H has too much entropy, and thus cannot be determined by a sample x_i, or otherwise has a lot of structure that we would like to avoid.

Our way to balance between the different constraints is by using *variable density* H and e, which start with a dense part and quickly become sparse, so that the overall entropy is small. Concretely, the matrix H and the LPN secret e are picked from the following "regular" variable-density distribution: Each row of H, as well as e, is divided into m blocks, where block j ($1 \leq j \leq m$) is the concatenation of m random weight-1 vectors of length 2^j. Note that the length of each such vector is $M = O(m2^m)$ and each block has twice the size and half the density of the previous block.

[2] As is common in the study of constant-depth PRFs, we consider the complexity of mapping the input to the output when the key is fixed, where inputs can be negated without counting towards the depth. The latter is consistent with, for instance, a DNF formula having depth 2. Viewed as a function of both the input and the key, the depth increases to 3.

We refer to the conjectured security of this flavor of variable-density LPN as the *VDLPN assumption*. This assumption is equivalent to the security of the WPRF candidate in Eq. (1). In Section II we further motivate this choice and discuss its provable security against a variety of relevant attacks. We also discuss other flavors of the VDLPN assumption that correspond to alternative WPRF candidates.

D. From VDLPN to XOR-RKA security

Independently of the PCF motivation, our new WPRF candidates are motivated by another cryptographic application: achieving security against *related-key attacks* (RKA) with respect to XOR functions. RKA security captures a model in which the attacker is allowed to see several instances of a primitive where the keys are not independent, but instead satisfy a relation of its choice. XOR-RKA security captures the setting where the adversary has access to the primitive with keys $k, k \oplus \Delta_1, k \oplus \Delta_2, \cdots$, for fixed offsets of his choice. The VDLPN assumption that implies the security of our main WPRF candidate actually implies the stronger XOR-RKA security for free. This follows from the fact that the WPRF can be written in the form $f_k(x) = h(k \oplus x)$, and so tampering with the key bits is equivalent to tampering with the (random) inputs.

XOR-RKA is arguably the most natural flavor of RKA security, capturing fault injection attacks where an adversary can induce bit flips in cryptographic hardware and other forms of tampering (see [27] and references therein). However, it is typically very hard to prove — the only "provable" XOR-RKA secure PRF is based on the very strong cryptographic assumption of multilinear maps [20]. Our main WPRF candidate implies simple PRGs and WPRFs whose XOR-RKA security follows from the VDLPN assumption. These can in turn be used for constructing other types of XOR-RKA secure variants of primitives that can be based on standard WPRF. These include identification and authentication schemes, semantically secure encryption schemes [28], and passive XOR-RKA secure strong PRFs [29]. Finally, since our WPRF candidate has the form $f_k(x) = h(k \oplus x)$, its security implies that the function h is *correlation-robust* in the sense of [30].

We stress that these XOR-RKA primitives depend on a new security assumption that is yet to withstand the test of time. This follows previous theory-oriented works that introduce new simple PRF candidates and study their resistance to concrete classes of attacks [18], [19], [31], [32].

E. From FSS-friendly WPRF to PCF

Our WPRF candidates are designed to be *FSS-friendly*, in the sense that they can be evaluated by lightweight function secret sharing schemes based on the existence of one-way functions. The primitive we use is a *distributed point function* (DPF) [33], namely an FSS scheme for the class of *point functions* $\{P_\alpha\}_{\alpha \in \{0,1\}^*}$. The point function $P_\alpha : \{0,1\}^{|\alpha|} \rightarrow \mathbb{F}_2$ evaluate to 1 on input α, and to 0 on all other inputs. Our main WPRF candidate, described in Eq. (1), can be seen as a sum of m^2 point functions, since each AND term in the summation performs an equality test of public input bits $(x_{i,j,1}, \ldots, x_{i,j,j})$ with (the negation of) the corresponding secret key bits $(k_{i,j,1}, \ldots, k_{i,j,j})$. Here we make a crucial use of the fact that the identity of the variables in each term of Eq. (1) is public and only whether each variable is negated or not is secret. Concretely efficient DPF schemes from any PRG were given in [11], [34]. We propose alternative low-complexity WPRF candidates that are even more FSS-friendly than our main VDLPN-based candidate. These exploit the fact that in the best known DPF constructions [34], sharing the point function P_α directly gives a sharing of all $P_{\alpha'}$ for α' a prefix of α.

Given FSS for a WPRF, or slight extensions thereof, we show direct constructions of several useful instances of a PCF. In some cases we need to extend the output of the WPRF from $\mathbb{F}_2$ to a bigger output ring; our concrete WPRF constructions can be extended in a natural way to this more general case. Our PCF constructions include PCFs for useful "low-degree" correlations such as *vector oblivious linear evaluation* (VOLE) and random *oblivious transfer* (OT), based on FSS for a WPRF, and in the case of OT, additionally a correlation-robust hash function [30]. (In fact, as discussed in Section I-D, this primitive is implied by the VDLPN assumption, so no extra assumption is needed.) To give a simple example, a PCF for a VOLE correlation is obtained by applying FSS to a random WPRF f_k, known to one party, and then to $c \cdot f_k$, where c is a random ring element known to the other party. For the above simple correlations, one can in fact replace the FSS primitive by the simpler *puncturable pseudorandom function* primitive [35]–[37].

We further construct PCF for *multiplication triples*, given FSS for both the WPRF class $\mathcal{F}$ and the *square* of $\mathcal{F}$, namely $\mathcal{F}^2 = \{f \cdot f' \,:\, f, f' \in \mathcal{F}\}$. For all of our WPRF candidates $\mathcal{F}$, their square is also FSS-friendly. The above correlations are useful for a wide variety of secure computation tasks. Other PCF constructions are deferred to the full version.

The above constructions only realize our default notion of *weak* PCF, where inputs are chosen at random. This is good enough in applications where a common source of public randomness is available. Moreover, in the random oracle model, one can easily obtain a strong PCF from a weak one by applying the random oracle to the input.

Compared to the generic LWE-based construction of PCFs, the LPN-style assumptions that underly our specialized constructions seem qualitatively weaker. For instance, they are not known to imply additively homomorphic encryption or even collision-resistant hashing. VDLPN-based PCFs also have attractive efficiency features that beat the generic alternative both asymptotically and concretely (by several orders of magnitude). Finally, they achieve *perfect correctness* whereas LWE-based constructions have negligible error probability that we do not know how to remove. See Section I-G for a more detailed comparison.

F. Applications of PCFs

PCFs give rise to a number of interesting cryptographic applications, which we briefly outline here, and in more detail in the full version.

Secure computation with correlated randomness. The most natural use-case, as already mentioned, is their ability to produce a practically unlimited amount of correlated randomness for use in secure computation protocols. Similar to the case of PCGs, this application is not entirely immediate — a PCF cannot substitute for an ideal source of correlated randomness in *every* protocol, since knowing a short representation of this randomness can in some cases contradict security. We can show, however, that PCFs *can* be plugged directly into a large class of natural, practical protocols in a secure manner; this holds for any protocol that is secure even when a corrupt party can influence its own correlated randomness. In particular, this property is satisfied by many, standard secure multi-party computation (MPC) protocols in the preprocessing model, so PCFs allow us to transform these protocols to have *reusable preprocessing*. Here, a one-time setup protocol is first performed to distribute the keys for a PCF. After this setup, the PCF can be used for as many instances of the MPC protocol as is needed, without having to re-run the setup.

Two-round MPC. A special class of multi-party computation protocols that have been developed recently [38]–[40] is those with just *two rounds* of interaction, the minimum that is possible. The two-round protocol of Garg et al. [41] uses a setup phase for producing a large number of random oblivious transfers, after which the entire protocols makes only black-box use of a pseudorandom generator. Replacing this oblivious transfer setup with PCFs, we obtain a fully reusable preprocessing phase, which after its setup, can be used for any number of two-round MPC protocols.

Non-interactive zero knowledge with fully reusable preprocessing. Non-interactive zero knowledge (NIZK) allows a prover to convince a verifier of the truth of some statement, by just sending a single message. NIZK with preprocessing allows a setup phase with a trusted third party, who generates secret proving and verification keys, which are given to the prover and verifier, respectively. Preprocessing NIZK can have information-theoretic security given OT or VOLE correlations [42], [43]. This motivated the use of a PCG-based approach in this context [6], [7], [44]. Using PCFs, we can obtain preprocessing NIZKs with fully reusable preprocessing, where a single setup consisting of PCF keys can be used to prove an arbitrary number of statements. Compared with other recent NIZK constructions in the designated verifier setting [45], which can be based on LPN, the PCF approach requires a stronger preprocessing setup, but leads to simpler constructions with better concrete efficiency. These constructions do not require any cryptographic operations after expanding the PCF outputs.

Multi-party PCFs. Some of our two-party PCF constructions can be extended to the *multi-party setting*, where m parties can obtain correlated randomness, which remains secure even when up to $m-1$ keys have been corrupted. These extensions are possible by exploiting a *programmability* feature of the two-party PCFs, which means that some portion of the PCF outputs can be reused as outputs in a separate PCF instance. This allows generically constructing multi-party PCFs, in a similar way to previous constructions of multi-party PCGs [7].

G. Advantages of the VDLPN-Based PCF Construction

PCFs can be constructed by instantiating the generic framework we present in the full version with different WPRF and suitable Function Secret Sharing schemes. In addition to our main WPRF candidate presented in Equation 1 we propose a second candidate in Equation 2. This second candidate is has more aggressive parameters compared to the main candidate, with reuse of input bits enabling shorter input.

$$f_k(x) = \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{m} \bigwedge_{h=1}^{j} (x_{j,h} \oplus k_{i,j,h}). \tag{2}$$

Without an FSS-friendly WPRF such as ours, it seems necessary to rely on more general forms of FSS such as for polynomial-size circuits. This can be constructed based on certain fully homomorphic encryption (FHE) schemes from the LWE assumption [12]. One can also obtain FSS for branching programs from the decisional Diffie-Hellman assumption, however, this suffers from an inverse polynomial correctness error which requires high computational costs to keep small [46].

Below, we analyze the properties of LWE-based constructions, and compare these with our approach. Specifically, we will consider an FSS construction based on the more efficient ring-LWE assumption, and instantiate this with an exponential ring-LWE modulus q; this allows to obtain FSS and PCFs with an exponentially small error probability [12], which is comparable to our constructions with perfect correctness.

Asymptotic efficiency. We first analyze an optimistic variant of a ring-LWE-based PCF, based on a WPRF which can be computed by a circuit of size $\tilde{O}(\lambda)$; note that the only candidates we are aware of satisfying this are our WPRF from VDLPN, and a permutation-based candidate PRF by Miles and Viola [31]. Fully homomorphic encryption from the ring-LWE assumption can be carried out with polylogarithmic overhead on top of the cleartext computation [47].

However, this does not directly translate to FSS with polylogarithmic overhead, since in our case the modulus q is exponential in the security parameter rather than polynomial as in FHE; this adds a multiplicative overhead of $\tilde{O}(\lambda)$ to the homomorphic evaluation procedure translating to a computational overhead of $\tilde{O}(\lambda^2)$ for PCF evaluation. Regarding storage costs, the PCF key in this construction consists of $\tilde{O}(\lambda)$ ring-LWE ciphertexts, giving a total key size of $\tilde{O}(\lambda^3)$ bits.[3]

Moreover, the above computation cost requires an additional hardness assumption for the WPRF with $\tilde{O}(\lambda)$ size circuits. PRF constructions from standard assumptions such as LWE, ring-LWE [48], number-theoretic assumptions [49] or a natural generalization of AES [31], require a circuit of size $\tilde{O}(\lambda^2)$, and result in $\tilde{O}(\lambda^4)$ computation for PCF.

In contrast, our candidate has key size $\tilde{O}(\lambda^2)$ bits and computational cost $\tilde{O}(\lambda)$ PRG operations, clearly improving over the alternatives in both complexity measures.

Concrete efficiency. Thanks to its simplicity, our constructions should in practice be more concretely efficient than LWE-based approaches. For example, we estimate that in our PCFs for VOLE or OT, each party's PCF key can be around 200kB, or 4MB based on our most conservative assumption (the parameters were chosen to achieve 100 bits of security against natural linear attacks such as BKW or the learning algorithm of [17]). For comparison, Boyle et al. [7] considered building a PCG from ring-LWE-based function secret sharing (or homomorphic secret sharing) and a suitable pseudorandom generator. To obtain a reasonable computation time, the resulting PCG keys were larger than 3GB, and the stretch of the PCG was still sub-quadratic. Since a single FHE ciphertext is typically the order of several megabytes, and a PCF key will need many such ciphertexts, it seems inherent that LWE-based PCFs will suffer similarly in terms of concrete key size and/or computational cost.

Conceptually weaker assumption. LWE is a powerful assumption that implies, amongst other things, the existence of (leveled) fully homomorphic encryption. On the other hand, LPN-type assumptions, even in a low-noise regime such as VDLPN, are not known to imply additively homomorphic encryption or even collision-resistant hashing. Despite recent progress towards the latter [50], [51], it is still unknown whether we can construct collision-resistant hashing based on the polynomial hardness of LPN. For additively homomorphic encryption, there are negative results showing that any LPN-based construction must make non-black-box use of the underlying ring, which seems to require techniques going beyond existing constructions [52]. Therefore, our constructions show that PCFs, although a powerful primitive, can plausibly be realized under much weaker assumptions than before.

Zero correctness error. Our constructions satisfy perfect correctness for all parameter choices. With LWE, a negligible correctness error requires a superpolynomial modulus, which is a stronger assumption than standard LWE. It is not known how to obtain perfectly correct HSS under LWE, and when the modulus is restricted to be polynomial, current constructions have an inverse polynomial correctness error which seems to require fundamentally different techniques.

H. *Related Work*

The study of secure computation with silent preprocessing is a recent but active research area [6]–[8], [53]–[55]. There is a long line of work which studied constructions of low-bias PRGs and PRFs in low complexity classes [56]–[63]. In particular, the work of [64] gives an ε-biased strong PRF in $\mathsf{AC}^0[\oplus]$; while it only achieves bias $\varepsilon \geq 1/\mathsf{superpoly}(\lambda)$, it was strengthened in [65] to achieve exponentially small bias. Our result is incomparable: we only construct a *weak* low-bias PRF family, but in the much smaller class $\mathsf{XOR} \circ \mathsf{AND}$. Heuristic constructions of PRFs and weak PRFs with provable security against classes of attacks have been studied in several previous work [18], [32], [66].

The combination PRFs and FSS (or the dual of homomorphic secret sharing) has been used before in different contexts. In particular, Boyle et al. used it to establish barriers for FSS [11] and to obtain low-communication MPC protocols [46], and Bartusek et al. [67] used it to obtain two-round MPC protocols with reusable first round.

II. FSS-Friendly Weak Pseudorandom Functions

In this section we give a more detailed technical overview of our new WPRF candidates, their design choices, and security analysis. We start with some general background.

The study of low-complexity cryptography has a long and rich history (see e.g. [18], [32], [68]–[73] and references therein). Beyond the direct goal of minimizing the complexity of useful cryptographic primitives, this line of work is motivated by its relevance to hardness results and barriers in computational complexity theory and learning theory. Another, more recent, motivation stems from the fact that many advanced primitives, such as secure computation, zero-knowledge proofs, fully homomorphic encryption (FHE), and indistinguishability obfuscation can induce their own efficiency metrics that motivate new designs of low-complexity primitives. Some relevant works in this direction include [72], [74]–[77].

Our work gives yet another example of this kind: we efficiently realize PCFs by relying on WPRFs with a specific "FSS-friendly" structure. To instantiate this framework, we can use a "heavy hammer" approach, by relying on advanced constructions of FSS for all circuits [11], [12]. However,

[3] The number of ciphertexts could be reduced using packing techniques [47], but this requires storing additional 'key-switching' material, and would not change the overall key size.

while such an approach is interesting for establishing feasibility (which we do in the full version), it is unsatisfactory for several reasons. First, it is unlikely to lead to any concretely efficient candidate (in the same way that hybrid FHE can be achieved by combining any FHE scheme with any standard block cipher, but the resulting scheme will be highly inefficient, hence motivating the design of FHE-friendly ciphers [74]–[76]). Second, it requires a strong flavor of "homomorphic cryptography," which implies a severe limitation on the type of assumptions we can realistically hope to rely on and the level of concrete efficiency. Finally, a curious limitation of all known constructions of FSS of circuits is that they cannot achieve perfect correctness.

Therefore, we take the opposite road: rather than starting from advanced FSS for all circuits based of FHE-style assumptions, we ask whether the simplest and most efficient known FSS schemes [34], which can be based on any one-way function, are already sufficiently powerful to instantiate our framework. Namely, we ask:

Is there a weak PRF in the complexity class captured by known FSS schemes based on one-way functions?

The FSS schemes of [34] capture point functions (which are equal to 0 everywhere except on a single point) and other classes of functions, interval functions (which take a fixed value for all inputs from an interval, and 0 otherwise), multi-dimensional generalizations of the latter, decision trees with fixed topology, as well as all linear combinations of the above. All these classes can be expressed as sums of point functions applied to different projections of the inputs. The schemes from [34] achieve better efficiency than that obtained via independent instances of DPF. But from a feasibility point of view, all these functions can be expressed as depth-2 $\mathsf{AC}^0[\oplus]$ circuits.

On Weak PRFs in $\mathsf{AC}^0[\oplus]$. WPRFs with quasipolynomial security are known to exist in complexity classes as low as AC^0, the class of polysize constant-depth circuits with arbitrary fan-in $\vee, \wedge$ gates, under standard cryptographic assumptions such as factoring and DDH [68]–[70] or assuming the existence of random local functions [73]. Furthermore, no weak PRF with better than quasipolynomial security can exist in AC^0 [78]. Strong PRFs with quasipolynomial security are known to exist in $\mathsf{AC}^0[\oplus]$ under standard cryptographic assumptions [79], and quasipolynomial security is the best one can hope for in this class [80], [81]. Finally, strong PRFs with exponential security are known in TC^0 [48] and in the "almost constant-depth" variant of $\mathsf{AC}^0[\oplus]$ [82] under standard cryptographic assumptions, and heuristic constructions (with provable resistance against some classes of attacks) of strong PRFs in ACC^0 have been proposed in [32]. Our work proposes conceptually simple WPRF candidates in $\mathsf{AC}^0[\oplus]$ that have depth 2 (the best possible) and are FSS-friendly. See Table I for comparison with related work.

A Natural Approach. A natural approach to building weak pseudorandom functions in a low complexity class, which was the starting point of most prior works [18], [32], [48], [82], is to start from (variants of) the learning parity with noise assumption. The LPN assumption postulates that the function family $f_{s,B}(x) = \langle s, x\rangle + B(x)$ is a weak PRF, where $s \in \{0,1\}^n$ is a secret random vector, and $B(x)$ is a noise function which associates to each x a random noise coordinate that is biased towards zero. In spite of its low complexity, this weak PRF family is not efficient: the standard formulation of LPN requires entropy for each noise term, which is too much for storing B in the key, unless the number of samples is restricted to some fixed polynomial.

A. Our Approach – the LPN Viewpoint

As discussed in Section I-C, our approach is to instead start from the dual form of LPN, with suitable modifications to the distributions from which both the error and the public matrix are sampled. Concretely, fix some parameter D, and for $i = 1$ to D, let x_i, e_i be random sparse vectors of density $1/2^i$, such that each x_i, e_i is twice as long as x_{i-1}, e_{i-1}. Our main candidate WPRF can be defined by the function family:

$$f_{e_1,\cdots,e_D}(x_1,\cdots,x_D) = \bigoplus_{i=1}^{D}\langle x_i, e_i\rangle.$$

Given many samples from f, for each i we can define a sparse matrix H_i of density $1/2^i$, where each row contains one sample x_i. Distinguish a set of samples from random is therefore equivalent to distinguishing $\bigoplus_{i=1}^{D} H_i \cdot e_i$, when given $(H_1, \cdots, H_D)$. This gives rise to a *variable density* variant of the dual-LPN assumption, which states that $H \cdot e$ is indistinguishable from random when given H; in our case, H and e are defined from horizontal and vertical concatenation of H_i and e_i, respectively. This variable density structure is the key to allow simultaneously for exponentially many samples (in some security parameter), while maintaining a polynomial-size compressed representation of the exponentially long vectors. We call this assumption the *variable-density learning parity with noise assumption* (VDLPN), and initiate its study in this paper.

B. Our Approach – the Low-Bias Function Viewpoint

For an alternative perspective, we can view our candidate as a methodology for obtaining a family of functions in a simple complexity class and with *low bias*, meaning that it provably resists a class of linear attacks. Below, we give some background on this approach, as well as some intuition behind why our candidate has low bias.

A large body of work has been dedicated to the construction of pseudorandom *generators* in low complexity

Circuit Depth	**Complexity Class** AC^0	 $\mathsf{AC}^0[\oplus]$	 $\mathsf{ACC}^{0\dagger}$
Depth 2	Weak PRF [16] (quasipolynomial*)	**Weak PRF** **(subexponential*)**‡	Weak PRF [32] (exponential*)
Depth 3	Weak PRF [73] (quasipolynomial)	Weak PRF [18], [19] (quasipolynomial*)	Strong PRF [32] (exponential*)
Depth > 3	Weak PRF [68] (quasipolynomial)	Strong PRF [69], [79] (quasipolynomial)	–
Negative Results	No weak PRF with better than quasipolynomial security [78]	No strong PRF with better than quasipolynomial security [80], [81]	–

* Starred entries refer to (provable or heuristic) security against known classes of attacks, as opposed to security proofs via reductions to well-studied cryptographic assumptions.

† For entries in ACC^0, it suffices to consider $\mathsf{AC}^0[6]$, that is, the class AC^0 augmented with mod_6 gates.

‡ Subexponential security means that there exists $\epsilon > 0$ such that the candidate is secure against all distinguishers of size 2^{n^ϵ}.

Table I

COMPARISON OF POSITIVE AND NEGATIVE RESULTS FOR CONSTANT-DEPTH PRFS. When measuring depth, we consider the complexity of mapping the input to the output when the key is fixed, and do not count negations of the input. For each candidate, we denote in parenthesis its conjectured level of security. Different constructions in the same class rely on incomparable assumptions. The entry shown in **bold** is from this work.

classes. A common strategy is to PRGs which *unconditionally* resist restricted class of attacks, and to use them as plausible heuristic candidates for cryptographically secure PRGs. Perhaps the most representative example is the design of ε-*biased* PRGs, which unconditionally resist all linear distinguishers (see e.g. [56]–[63] and references therein). For the reader familiar with the literature on ε-biased PRG, we find it useful to provide an alternative interpretation of our approach as a natural approach to design an unconditionally secure low-bias weak pseudorandom function family (which we then conjecture to be also a cryptographically secure weak PRF family).

An ε-biased PRG is a function $G : \{0,1\}^n \mapsto \{0,1\}^m$ which maps a short seed $s \in \{0,1\}^n$ to a longer string $G(s)$, such that no linear function L has advantage more than ε in distinguishing $G(U_n)$ from U_m (U_n, U_m denote the uniform distributions over $\{0,1\}^n$ and $\{0,1\}^m$ respectively). A standard strategy to build a low-bias PRG, used for example in [57], [59], is to design two generators, one secure against "light tests" (linear tests of small Hamming weight), and one secure against "heavy tests" (linear tests of large Hamming weight). Then, the PRG G is constructed as

$$G(x,y) = G_{\mathsf{light}}(x) \oplus G_{\mathsf{heavy}}(y);$$

it is relatively easy to show that this gives a low-bias PRG since G inherits the security against all possible linear tests from its components.

Our candidate WPRF can be seen as following a generalization of this approach. We define an (ε, N)-biased WPRF to be a family $\{f_k : \{0,1\}^n \mapsto \{0,1\}\}_k$ of functions such that the restriction of the function $k \to (f_k(x))_{x\in\{0,1\}^n}$ to a random size-N subet of its outputs is an ε-biased pseudorandom generator with very high probability.

The work of Naor and Naor [56] shows that to build low-bias sample spaces, it is useful to restrict our attention to tests whose weight belongs to an interval of the form $[2^i, 2^{i+1}]$, because such tests are provably fooled by random sparse vectors of density $1/2^i$. Building upon this observation, we show how to get a low-complexity weak PRF that fools linear tests with weight in $[2^i, 2^{i+1}]$: we let the random inputs to the PRF define the rows of a random matrix H_i of density $1/2^i$. Using a Chernoff-type concentration bound for random variables with limited dependency, we prove that any given test with weight in $[2^i, 2^{i+1}]$ is fooled by a constant fraction c of the columns of H_i. Therefore, the distribution induced by $H_i \cdot e_i$ for a random sparse vector e_i of weight w (i.e., a random subset-sum of columns of H_i) fools any given test with weight in $[2^i, 2^{i+1}]$ with probability at least c^w. We let f_{i,e_i} be the function which, on input x, samples a $1/2^i$-dense row h of H_i using randomness x, and outputs $h^\intercal \cdot e_i$ (by our argument, f_{i,e_i} has low bias against all tests with weight in $[2^i, 2^{i+1}]$). Finally, to get a 2^D-sample WPRF which has low bias with respect to all possible linear tests, we define

$$f_{e_1\cdots e_D}(x_1,\cdots,x_D) = f_{1,e_1}(x_1) \oplus \cdots \oplus f_{D,e_D}(x_D).$$

1) Boolean circuit formulation: As presented earlier in (1), we can also obtain the equivalent Boolean circuit formulation:

$$f_k(x) = \bigoplus_{i=1}^{D} \bigoplus_{j=1}^{w} \bigwedge_{h=1}^{i} (x_{i,j,h} \oplus k_{i,j,h}), \qquad (3)$$

where $x, k \in \{0,1\}^{wD(D-1)/2}$ are parsed as D sequences such that the i-th sequence, $1 \le i \le D$ is made up of i

blocks of i bits. To see that this is equivalent to the VDLPN formulation above, observe that each block of i bits defines a binary unit vector of length 2^i and $\bigwedge_{h=1}^{i}(x_{i,j,h} \oplus k_{i,j,h}) = 1$ exactly when the inner product of the associated binary vectors in the key and in the input is 1.

This formulation is conceptually simpler, and highlights that for a fixed key k, it corresponds to an XNF formula, namely a depth-2 circuit computing a single XOR of ANDs of literals (inputs or their negations). In the section below, we also mention several variants of the construction based on this boolean circuit perspective.

C. On the Security of our Candidate and Variants

We conjecture that a $2^{O(\lambda)}$-size adversary, given 2^λ samples, breaks our candidates instantiated with $w, D = O(\lambda)$ with probability at most $2^{-O(\lambda)}$. Since our main candidate has inputs of size $n = O(wD^2) = O(\lambda^3)$, this corresponds to subexponential security against $2^{O(n^{1/3})}$-size attackers. For our variant, which has inputs of size $n = O(wD) = O(\lambda^2)$, this corresponds to subexponential security against $2^{O(n^{1/2})}$, which is essentially optimal due to the existence of a $2^{\tilde{O}(n^{1/2})}$-time learning algorithm for XNF with arbitrary distributions [17]. When restricting the adversary to a quasipolynomial number $n^{\mathsf{polylog}(\lambda)}$ (i.e. $D = \mathsf{polylog}(\lambda)$) of samples, we conjecture quasiexponential security $2^{\tilde{O}(n)}$.

Of course, when defining low-complexity cryptographic building blocks, one must be especially careful with security analysis. For example — despite conjectured to yield security against algebraic attacks — the candidate WPRF construction in $\mathsf{AC}^0[\oplus]$ by Akavia et al. [18] turned out to be broken (in quasipolynomial time) via an algebraic relinearization attack, as observed by Bogdanov and Rosen [19].

On the other hand, we *prove* resistance against a wide range of attacks considered in the literature. In particular, we identify a large variety of attacks on LPN as special cases of *linear distinguishers*, as described above (Section II-B), and provably rule them out for our candidate. We observe that Gaussian elimination attacks [83], statistical decoding attacks [84]–[88], information set decoding attacks [89]–[95], BKW and variants [96], [97] all fall under this umbrella of a linear attack. We also rule out general algebraic attacks, which covers the attack on the Akavia et al. [18] candidate, and statistical query attacks based on the learning algorithm of Linial, Mansour and Nisan [78], and prove resistance to linear cryptanalysis as formalized by Miles and Viola [66].

For all of the classes of attacks above, we prove that no $2^{O(w)}$-size adversary mounting an attack from one of these classes can have advantage more than $2^{-O(w)}$ in distinguishing our candidates from random functions given 2^D samples. Further, we show our construction is (w/D)-wise independent , so resists all AC^0 tests of size $2^{(w/D)^c}$ for some constant c.

1) Generalization to arbitrary rings: The VDLPN candidate can be generalized to work over larger rings than $\mathbb{Z}_2$. Here, we simply modify the two sparse, VDLPN distributions by replacing ones with random, non-zero elements from a ring R, which gives a candidate that is still FSS-friendly, and can be used for PCFs that output correlations over R. For an appropriate choice of parameters, our proof of resistance to linear attacks also extends to this arithmetic setting, and we conjecture its security against general attacks for an arbitrary choice of the ring R.

2) Variants with smaller inputs and smaller keys: Taking the boolean function definition seen in equation (3), we can consider several variants of the construction by making simplifications. For instance, our first variant reduces the input size from $O(wD^2)$ to $O(wD)$ bits by reusing inputs, replacing the variable $x_{i,j,h}$ with $x_{j,h}$. This modified candidate still provably resists linear attacks, and we conjecture it also resists the other attacks we have considered. We can further modify this variant by XORing an additional triangular function to the weak PRF. Since triangular functions have high algebraic immunity, this allows us to prove resistance to algebraic attacks whilst retaining the benefit of the reduced $O(wD)$ input size.

Finally, we present an aggressive variation which reduces the key size from $O(wD^2)$ down to $O(wD)$ bits. Here, the proofs of resistance for linear and algebraic attacks break down, however, we have not found any attacks, and put forward the security of this variant as an interesting direction for future study.

III. Acknowledgements

We would like to thank Nader Bshouty, Rocco Servedio, Jean-Pierre Tillich, Nicolas Sendrier, and Thomas Debris for useful discussions and pointers, and the anonymous FOCS reviewers for helpful suggestions.

E. Boyle, N. Gilboa, and Y. Ishai, and L. Kohl supported by ERC Project NTSC (742754). E. Boyle additionally supported by ISF grant 1861/16 and AFOSR Award FA9550-17-1-0069. G. Couteau supported by ERC Project PREP-CRYPTO (724307). N. Gilboa additionally supported by ISF grant 2951/20, ERC grant 876110, and a grant by the BGU Cyber Center. Y. Ishai additionally supported by NSF-BSF grant 2015782, BSF grant 2018393, ISF grant 2774/20, and a grant from the Ministry of Science and Technology, Israel and Department of Science and Technology, Government of India. Work of L. Kohl was done in part while at Karlsruhe Institute of Technology, supported by ERC Project PREP-CRYPTO (724307) and DFG grant HO 4534/2-2. P. Scholl supported by the Danish Independent Research Council under Grant-ID DFF-6108-00169 (FoCC) and an Aarhus University Research Foundation starting grant.

References

[1] J. Kilian, "Founding cryptography on oblivious transfer," in *20th ACM STOC*. ACM Press, May 1988.

[2] D. Beaver, "Efficient multiparty protocols using circuit randomization," in *CRYPTO '91*, 1991, pp. 420–432.

[3] ——, "Precomputing oblivious transfer," in *CRYPTO'95*, ser. LNCS. Springer, Aug. 1995.

[4] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game or A completeness theorem for protocols with honest majority," in *19th ACM STOC*. ACM Press, May 1987.

[5] O. Goldreich, *Foundations of Cryptography: Volume 2, Basic Applications*. New York, NY, USA: Cambridge University Press, 2004.

[6] E. Boyle, G. Couteau, N. Gilboa, and Y. Ishai, "Compressing vector OLE," in *ACM CCS 18*. ACM Press, 2018.

[7] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, and P. Scholl, "Efficient pseudorandom correlation generators: Silent OT extension and more," ser. LNCS. Springer, 2019.

[8] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, P. Rindal, and P. Scholl, "Efficient two-round OT extension and silent non-interactive secure computation," in *ACM CCS 19*. ACM Press, 2019.

[9] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, and P. Scholl, "Efficient pseudorandom correlation generators from ring-lpn," 2020, to appear on eprint.

[10] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," *J. ACM*, vol. 33, no. 4, pp. 792–807, 1986.

[11] E. Boyle, N. Gilboa, and Y. Ishai, "Function secret sharing," ser. LNCS. Springer, 2015.

[12] Y. Dodis, S. Halevi, R. D. Rothblum, and D. Wichs, "Spooky encryption and its applications," ser. LNCS. Springer, Aug. 2016.

[13] E. Boyle, N. Gilboa, Y. Ishai, H. Lin, and S. Tessaro, "Foundations of homomorphic secret sharing," 2018.

[14] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *37th ACM STOC*. ACM Press, May 2005.

[15] B. Applebaum, I. Damgård, Y. Ishai, M. Nielsen, and L. Zichron, "Secure arithmetic computation with constant computational overhead," ser. LNCS. Springer, 2017.

[16] A. Blum, M. L. Furst, M. J. Kearns, and R. J. Lipton, "Cryptographic primitives based on hard learning problems," in *CRYPTO'93*, ser. LNCS. Springer, Aug. 1994.

[17] L. Hellerstein and R. A. Servedio, "On PAC learning algorithms for rich boolean function classes," *Theor. Comput. Sci.*, vol. 384, no. 1, pp. 66–76, 2007. [Online]. Available: https://doi.org/10.1016/j.tcs.2007.05.018

[18] A. Akavia, A. Bogdanov, S. Guo, A. Kamath, and A. Rosen, "Candidate weak pseudorandom functions in AC^0 o MOD_2," in *ITCS 2014*. ACM, 2014.

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

[20] M. Abdalla, F. Benhamouda, and A. Passelègue, "Algebraic XOR-RKA-secure pseudorandom functions from post-zeroizing multilinear maps," ser. LNCS. Springer, Dec. 2019.

[21] R. E. Schapire and L. Sellie, "Learning sparse multivariate polynomials over a field with queries and counterexamples," *J. Comput. Syst. Sci.*, vol. 52, no. 2, pp. 201–213, 1996. [Online]. Available: https://doi.org/10.1006/jcss.1996.0017

[22] N. H. Bshouty, "On learning multivariate polynomials under the uniform distribution," *Inf. Process. Lett.*, vol. 61, no. 6, pp. 303–309, 1997. [Online]. Available: https://doi.org/10.1016/S0020-0190(97)00021-5

[23] S. Heyse, E. Kiltz, V. Lyubashevsky, C. Paar, and K. Pietrzak, "Lapin: An efficient authentication protocol based on ring-LPN," in *FSE 2012*, ser. LNCS. Springer, Mar. 2012.

[24] C. A. Melchor, O. Blazy, J. Deneuville, P. Gaborit, and G. Zémor, "Efficient encryption from random quasi-cyclic codes," *IEEE Trans. Information Theory*, vol. 64, no. 5, pp. 3927–3943, 2018. [Online]. Available: https://doi.org/10.1109/TIT.2018.2804444

[25] R. Misoczki, J. Tillich, N. Sendrier, and P. S. L. M. Barreto, "Mdpc-mceliece: New mceliece variants from moderate density parity-check codes," in *2013 IEEE International Symposium on Information Theory*, 2013, pp. 2069–2073.

[26] D. Augot, M. Finiasz, and N. Sendrier, "A fast provably secure cryptographic hash function," Cryptology ePrint Archive, Report 2003/230, 2003, http://eprint.iacr.org/2003/230.

[27] R. Gennaro, A. Lysyanskaya, T. Malkin, S. Micali, and T. Rabin, "Algorithmic tamper-proof (ATP) security: Theoretical foundations for security against hardware tampering," in *TCC 2004*, ser. LNCS. Springer, Feb. 2004.

[28] B. Applebaum, D. Harnik, and Y. Ishai, "Semantic security under related-key attacks and applications," in *ICS 2011*. Tsinghua University Press, Jan. 2011.

[29] B. Applebaum and E. Widder, "Related-key secure pseudorandom functions: The case of additive attacks," Cryptology ePrint Archive, Report 2014/478, 2014, http://eprint.iacr.org/2014/478.

[30] Y. Ishai, J. Kilian, K. Nissim, and E. Petrank, "Extending oblivious transfers efficiently," in *CRYPTO 2003*, ser. LNCS. Springer, Aug. 2003.

[31] E. Miles and E. Viola, "Substitution-permutation networks, pseudorandom functions, and natural proofs," in *CRYPTO 2012*, ser. LNCS. Springer, Aug. 2012.

[32] D. Boneh, Y. Ishai, A. Passelègue, A. Sahai, and D. J. Wu, "Exploring crypto dark matter: New simple PRF candidates and their applications," ser. LNCS. Springer, 2018.

[33] N. Gilboa and Y. Ishai, "Distributed point functions and their applications," in *EUROCRYPT 2014*, ser. LNCS. Springer, 2014.

[34] E. Boyle, N. Gilboa, and Y. Ishai, "Function secret sharing: Improvements and extensions," in *ACM CCS 16*. ACM Press, 2016.

[35] A. Kiayias, S. Papadopoulos, N. Triandopoulos, and T. Zacharias, "Delegatable pseudorandom functions and applications," in *ACM CCS 13*. ACM Press, Nov. 2013.

[36] D. Boneh and B. Waters, "Constrained pseudorandom functions and their applications," in *ASIACRYPT 2013, Part II*, ser. LNCS. Springer, Dec. 2013.

[37] E. Boyle, S. Goldwasser, and I. Ivan, "Functional signatures and pseudorandom functions," in *PKC 2014*, ser. LNCS. Springer, 2014.

[38] S. Garg, C. Gentry, S. Halevi, and M. Raykova, "Two-round secure MPC from indistinguishability obfuscation," in *TCC 2014*, ser. LNCS. Springer, Feb. 2014.

[39] F. Benhamouda and H. Lin, "k-round multiparty computation from k-round oblivious transfer via garbled interactive circuits," ser. LNCS. Springer, 2018.

[40] S. Garg and A. Srinivasan, "Two-round multiparty secure computation from minimal assumptions," ser. LNCS. Springer, 2018.

[41] S. Garg, Y. Ishai, and A. Srinivasan, "Two-round MPC: Information-theoretic and black-box," ser. LNCS. Springer, 2018.

[42] J. Kilian, S. Micali, and R. Ostrovsky, "Minimum resource zero-knowledge proofs (extended abstract)," in *30th FOCS*. IEEE Computer Society Press, Oct. / Nov. 1989.

[43] M. Chase, Y. Dodis, Y. Ishai, D. Kraschewski, T. Liu, R. Ostrovsky, and V. Vaikuntanathan, "Reusable non-interactive secure computation," ser. LNCS. Springer, 2019.

[44] C. Weng, K. Yang, J. Katz, and X. Wang, "Fast, scalable, and communication-efficient zero-knowledge proofs for boolean and arithmetic circuits," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 925, 2020. [Online]. Available: https://eprint.iacr.org/2020/925

[45] A. Lombardi, W. Quach, R. D. Rothblum, D. Wichs, and D. J. Wu, "New constructions of reusable designated-verifier NIZKs," ser. LNCS. Springer, 2019.

[46] E. Boyle, N. Gilboa, and Y. Ishai, "Breaking the circuit size barrier for secure computation under DDH," in *CRYPTO 2016, Part I*, ser. LNCS. Springer, Aug. 2016.

[47] C. Gentry, S. Halevi, and N. P. Smart, "Fully homomorphic encryption with polylog overhead," in *EUROCRYPT 2012*, ser. LNCS. Springer, Apr. 2012.

[48] A. Banerjee, C. Peikert, and A. Rosen, "Pseudorandom functions and lattices," in *EUROCRYPT 2012*, ser. LNCS. Springer, Apr. 2012.

[49] M. Naor and O. Reingold, "Number-theoretic constructions of efficient pseudo-random functions," *Journal of the ACM*, no. 2, 2004.

[50] Z. Brakerski, V. Lyubashevsky, V. Vaikuntanathan, and D. Wichs, "Worst-case hardness for LPN and cryptographic hashing via code smoothing," ser. LNCS. Springer, 2019.

[51] Y. Yu, J. Zhang, J. Weng, C. Guo, and X. Li, "Collision resistant hashing from sub-exponential learning parity with noise," ser. LNCS. Springer, Dec. 2019.

[52] B. Applebaum, J. Avron, and C. Brzuska, "Arithmetic cryptography: Extended abstract," in *ITCS 2015*. ACM, 2015.

[53] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, and M. Orrù, "Homomorphic secret sharing: Optimizations and applications," in *ACM CCS 17*. ACM Press, 2017.

[54] P. Scholl, "Extending oblivious transfer with low communication via key-homomorphic PRFs," ser. LNCS. Springer, 2018.

[55] P. Schoppmann, A. Gascón, L. Reichert, and M. Raykova, "Distributed vector-OLE: Improved constructions and implementation," in *ACM CCS 19*. ACM Press, 2019.

[56] J. Naor and M. Naor, "Small-bias probability spaces: Efficient constructions and applications," in *22nd ACM STOC*. ACM Press, May 1990.

[57] E. Mossel, A. Shpilka, and L. Trevisan, "On e-biased generators in NC0," in *44th FOCS*. IEEE Computer Society Press, Oct. 2003.

[58] S. Lovett, O. Reingold, L. Trevisan, and S. Vadhan, "Pseudorandom bit generators that fool modular sums," in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*. Springer, 2009, pp. 615–630.

[59] A. Shpilka, "Constructions of low-degree and error-correcting ε-biased generators," *computational complexity*, vol. 18, no. 4, p. 495, 2009.

[60] E. Viola, "The complexity of distributions," in *51st FOCS*. IEEE Computer Society Press, Oct. 2010.

[61] R. Meka, O. Reingold, G. N. Rothblum, and R. D. Rothblum, "Fast pseudorandomness for independence and load balancing," in *International Colloquium on Automata, Languages, and Programming*. Springer, 2014, pp. 859–870.

[62] C. H. Lee and E. Viola, "Some limitations of the sum of small-bias distributions," *Theory of Computing*, vol. 13, no. 1, pp. 1–23, 2017.

[63] B. Applebaum and E. Kachlon, "Sampling graphs without forbidden subgraphs and unbalanced expanders with negligible error," in *FOCS 2019*, 2019, pp. 171–179.

[64] D. Gutfreund and E. Viola, "Fooling parity tests with parity gates," in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*. Springer, 2004, pp. 381–392.

[65] A. D. Healy, "Randomness-efficient sampling within nc," *Computational Complexity*, vol. 17, no. 1, pp. 3–37, 2008.

[66] E. Miles and E. Viola, "On the complexity of non-adaptively increasing the stretch of pseudorandom generators," in *TCC 2011*, ser. LNCS. Springer, Mar. 2011.

[67] J. Bartusek, S. Garg, D. Masny, and P. Mukherjee, "Reusable two-round MPC from DDH," 2020, https://eprint.iacr.org/2020/170.

[68] M. Kharitonov, "Cryptographic hardness of distribution-specific learning," in *25th ACM STOC*. ACM Press, May 1993.

[69] M. Naor and O. Reingold, "Number-theoretic constructions of efficient pseudo-random functions," in *38th FOCS*. IEEE Computer Society Press, Oct. 1997.

[70] M. Naor, O. Reingold, and A. Rosen, "Pseudo-random functions and factoring (extended abstract)," in *32nd ACM STOC*. ACM Press, May 2000.

[71] B. Applebaum, Y. Ishai, and E. Kushilevitz, "Cryptography in NC^0," in *45th FOCS*. IEEE Computer Society Press, Oct. 2004.

[72] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Cryptography with constant computational overhead," in *40th ACM STOC*. ACM Press, May 2008.

[73] B. Applebaum and P. Raykov, "Fast pseudorandom functions based on expander graphs," ser. LNCS. Springer, 2016.

[74] M. R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, and M. Zohner, "Ciphers for MPC and FHE," ser. LNCS. Springer, 2015.

[75] A. Canteaut, S. Carpov, C. Fontaine, T. Lepoint, M. Naya-Plasencia, P. Paillier, and R. Sirdey, "Stream ciphers: A practical solution for efficient homomorphic-ciphertext compression," in *FSE 2016*, ser. LNCS. Springer, 2016.

[76] P. Méaux, A. Journault, F.-X. Standaert, and C. Carlet, "Towards stream ciphers for efficient FHE with low-noise ciphertexts," ser. LNCS. Springer, 2016.

[77] H. Lin and S. Tessaro, "Indistinguishability obfuscation from trilinear maps and block-wise local PRGs," ser. LNCS. Springer, 2017.

[78] N. Linial, Y. Mansour, and N. Nisan, "Constant depth circuits, Fourier transform, and learnability," in *30th FOCS*. IEEE Computer Society Press, Oct. / Nov. 1989.

[79] E. Viola, "The communication complexity of addition," in *24th SODA*. ACM-SIAM, Jan. 2013.

[80] A. A. Razborov and S. Rudich, "Natural proofs," *J. Comput. Syst. Sci.*, vol. 55, no. 1, pp. 24–35, 1997.

[81] M. L. Carmosino, R. Impagliazzo, V. Kabanets, and A. Kolokolova, "Learning algorithms from natural proofs," in *CCC 2016*, 2016, pp. 10:1–10:24.

[82] Y. Yu and J. P. Steinberger, "Pseudorandom functions in almost constant depth from low-noise LPN," ser. LNCS. Springer, 2016.

[83] A. Esser, R. Kübler, and A. May, "LPN decoded," ser. LNCS. Springer, 2017.

[84] A. Al Jabri, "A statistical decoding algorithm for general linear block codes," in *IMA International Conference on Cryptography and Coding*. Springer, 2001, pp. 1–8.

[85] R. Overbeck, "Statistical decoding revisited," in *ACISP 06*, ser. LNCS. Springer, Jul. 2006.

[86] M. P. Fossorier, K. Kobara, and H. Imai, "Modeling bit flipping decoding based on nonorthogonal check sums with application to iterative decoding attack of mceliece cryptosystem," *IEEE Transactions on Information Theory*, vol. 53, no. 1, pp. 402–411, 2006.

[87] T. Debris-Alazard and J.-P. Tillich, "Statistical decoding," in *2017 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2017, pp. 1798–1802.

[88] L. Zichron, "Locally computable arithmetic pseudorandom generators," Master's thesis, School of Electrical Engineering, Tel Aviv University, 2017. [Online]. Available: http://www.eng.tau.ac.il/~bennyap/pubs/Zichron.pdf

[89] E. Prange, "The use of information sets in decoding cyclic codes," *IRE Transactions on Information Theory*, vol. 8, no. 5, pp. 5–9, 1962.

[90] J. Stern, "A method for finding codewords of small weight," in *International Colloquium on Coding Theory and Applications*. Springer, 1988, pp. 106–113.

[91] M. Finiasz and N. Sendrier, "Security bounds for the design of code-based cryptosystems," in *ASIACRYPT 2009*, ser. LNCS. Springer, Dec. 2009.

[92] D. J. Bernstein, T. Lange, and C. Peters, "Smaller decoding exponents: Ball-collision decoding," in *CRYPTO 2011*, ser. LNCS. Springer, Aug. 2011.

[93] A. May, A. Meurer, and E. Thomae, "Decoding random linear codes in $\tilde{\mathcal{O}}(2^{0.054n})$," in *ASIACRYPT 2011*, ser. LNCS. Springer, Dec. 2011.

[94] A. Becker, A. Joux, A. May, and A. Meurer, "Decoding random binary linear codes in $2^{n/20}$: How 1 + 1 = 0 improves information set decoding," in *EUROCRYPT 2012*, ser. LNCS. Springer, Apr. 2012.

[95] A. May and I. Ozerov, "On computing nearest neighbors with applications to decoding of binary linear codes," ser. LNCS. Springer, 2015.

[96] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," in *32nd ACM STOC*. ACM Press, May 2000.

[97] V. Lyubashevsky, "The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem," in *Approximation, randomization and combinatorial optimization. Algorithms and techniques*. Springer, 2005, pp. 378–389.