Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation

Geoffroy Couteau, Elette Boyle, Niv Gilboa, Yuval Ishai, Lisa Kohl, Peter Rindal, Peter Scholl, Idc Herzliya

Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation

Elette Boyle[1], Geoffroy Couteau[2], Niv Gilboa[3], Yuval Ishai[4], Lisa Kohl[5], Peter Rindal[6], and Peter Scholl[7]

[1] IDC Herzliya
[2] CNRS, IRIF, Université Paris-Diderot
[3] Ben-Gurion University of the Negev
[4] Technion
[5] Karlsruhe Institute of Technology
[6] Visa Research
[7] Aarhus University

Abstract. We consider the problem of securely generating useful instances of two-party correlations, such as many independent copies of a random oblivious transfer (OT) correlation, using a small amount of communication. This problem is motivated by the goal of secure computation with *silent preprocessing*, where a low-communication input-independent setup, followed by local ("silent") computation, enables a lightweight "non-cryptographic" online phase once the inputs are known.

Recent works of Boyle et al. (CCS 2018, Crypto 2019) achieve this goal with good concrete efficiency for useful kinds of two-party correlations, including OT correlations, under different variants of the Learning Parity with Noise (LPN) assumption, and using a small number of "base" oblivious transfers. The protocols of Boyle et al. have several limitations. First, they require a large number of communication rounds. Second, they are only secure against *semi-honest* parties. Finally, their concrete efficiency estimates are not backed by an actual implementation. In this work we address these limitations, making three main contributions:

- **Eliminating interaction.** Under the same assumption, we obtain the first concretely efficient *2-round* protocols for generating useful correlations, including OT correlations, in the semi-honest security model. This implies the first efficient 2-round OT extension protocol of any kind and, more generally, protocols for *non-interactive secure computation* (NISC) that are concretely efficient and have the silent preprocessing feature.
- **Malicious security.** We provide security against malicious parties (in the random oracle model) without additional interaction and with only a modest concrete overhead; prior to our work, no similar protocols were known with any number of rounds.
- **Implementation.** Finally, we implemented, optimized, and benchmarked our 2-round OT extension protocol, demonstrating that it offers a more attractive alternative to the OT extension protocol of Ishai et al. (Crypto 2003) in many realistic settings.

1 Introduction

There is a large body of work on optimizing the concrete efficiency of secure computation protocols via input-independent preprocessing. By securely generating many instances of simple correlations, one can dramatically reduce the online communication and computation costs of most existing protocols.

To give just one example, multiple independent instances of a random oblivious transfer[8] (OT) correlation can be used for secure two-party computation of Boolean circuits in the semi-honest model, with communication cost of only two bits per party per (nonlinear) gate, and with computation cost that is comparable to computing the circuit with no security requirements at all [GMW87, Kil88, Bea91]. Thus, assuming a fast communication network, protocols based on correlated randomness can achieve near-optimal performance.

The main challenge in applying this approach is the high concrete cost of securely generating the correlated randomness. Traditional solutions involve carefully optimized special-purpose

[8] In (a single instance of) a random OT correlation, one party obtains a pair of random bits (more generally, strings) (s_0, s_1) and the other obtains the pair (r, s_r) for a random bit r.

secure computation protocols that have a high communication cost for each instance of the desired correlation [BDOZ11, DPSZ12]. This holds even for the case of OT correlations, for which relatively fast OT extension techniques are known [IKNP03, ALSZ13, KOS15]. Moreover, even if offline communication is cheap, the cost of *storing* large amounts of correlated randomness for each party with whom a future interaction *might* take place can be significant.

Motivated by the limitations of traditional approaches for generating and storing correlated randomness, the notion of a *pseudorandom correlation generator* (PCG) was recently proposed and studied by Boyle et al. [BCGI18, BCG+19]. The goal of a PCG is to compress long sources of correlated randomness without violating security. More concretely, a (two-party) PCG replaces a target two-party correlation, say many independent OT correlation instances, by a pair of *short* correlated keys, which can be "silently" expanded *without any interaction*. The process of generating the correlated keys and locally expanding them should emulate an ideal process for generating the target correlation not only from the point of view of outsiders, but also from the point of view of *insiders* who can observe one of the two keys. Among other results, the aforementioned works of Boyle et al. [BCGI18, BCG+19] obtain concretely efficient constructions of PCGs for OT correlations and vector oblivious linear evaluation (VOLE) correlations [NP06, IPS09, ADI+17] based on variants of the Learning Parity with Noise assumption [BFKL93]. These PCG constructions are motivated by the goal of secure computation with *silent preprocessing*, where a low-communication input-independent setup, followed by local ("silent") computation, enables a lightweight "non-cryptographic" online phase once the inputs are known.

However, towards realizing this goal, one major challenge remains: how can the pair of keys be securely generated? While the keys are short, their sampling algorithm is quite complex and involves multiple invocations of cryptographic primitives. Thus, even applying the fastest general-purpose protocols for generating these keys (e.g., optimized protocols based on garbled circuits [KRRW18]) incurs a very significant overhead.

An alternative approach for distributing the PCG key generation, suggested in [BCGI18, BCG+19], relies on a recent special-purpose protocol of Doerner and shelat [Ds17] for secure key generation of a distributed point function (DPF) [GI14, BGI16]. This protocol only makes a black-box use of symmetric cryptography and a small number of oblivious transfers, and hence it is also concretely efficient. Using this protocol for distributing the key generation of a PCG for OT correlations, Boyle et al. [BCG+19] obtained a *silent OT extension* protocol that generates (without any trusted setup) a large number of pseudo-random OTs from a small number of base OTs, using a low-communication setup followed by silent key expansion [BCG+19].

While the silent OT extension protocol from [BCG+19] and other protocols obtained using this approach have good concrete efficiency, they also have several limitations. First, they require a large number of communication rounds that grows (at least) logarithmically with the output length. Second, they are only secure against *semi-honest* parties. Both of the above limitations are inherited from the DPF key generation protocol of [Ds17]. Finally, their concrete efficiency estimates are not backed by an actual implementation, and ignore possible cache-misses and other system- and network-related sources of slowdown.

1.1 Our Contribution

In this work, we address the above limitations by making the following contributions.

Two-Round Silent OT Extension. We present the first *concretely efficient* two-round OT extension protocol, based on a variant of the LPN assumption. The protocol has a silent preprocessing feature, allowing the parties to push the bulk of the computational work to an offline phase. It can be used in two modes: either a random-input mode, where the communication complexity is sublinear in the output length, or a chosen-input mode, where the communication is roughly equal to the total input length. This applies even to the more challenging case of 1-bit OT, for which standard OT extension techniques that make a black-box use of symmetric

cryptography [IKNP03, ALSZ13, KK13, KOS15] have a high communication overhead compared to the input length. A key idea that underlies this improvement is replacing the DPF primitive in the PCG for OT from [BCG+19] by the simpler puncturable pseudorandom function (PPRF) primitive [KPTZ13, BW13, BGI14]. We design a parallel version of the distributed key generation protocol from [Ds17] that applies to a PPRF instead of a DPF.

Our OT extension protocol bypasses a recent impossibility result of Garg et al. [GMMM18] on 2-round OT extension due to the use of the LPN assumption. While our construction (inevitably) does not fall into the standard black-box framework considered in [GMMM18], it still has a black-box flavor in that it only invokes a syndrome computation of *any* error-correcting code for which the LPN assumption holds. We remark that aside from its concrete efficiency, our 2-round OT extension protocol can be based on a conservative variant of (binary) LPN in a noise regime that is not known to imply public-key encryption, let alone oblivious transfer. Concretely, it can be instantiated by binary LPN in which the Hamming weight of the noise is higher than the $n^{1/2}$ bound required by the construction of Alekhnovich [Ale03] and its variants.

The technique we use for generating OT correlations in two rounds can also be applied to VOLE correlations, as well as general protocols for non-interactive secure computation (NISC) with silent preprocessing.

Malicious Security. We present simple, practical techniques for secure distributed setup of PPRF keys with a weak form of malicious security. This suffices to upgrade our semi-honest OT and VOLE protocols to malicious security, at a very low cost. Our main protocols in this setting have 4 rounds of interaction, but this can be reduced to 2 rounds using the Fiat-Shamir transform. We can also use this to obtain maliciously secure silent NISC or two-round OT extension on chosen inputs. These protocols are based on slightly stronger variants of LPN, where the adversary is allowed a single query to a one-bit leakage function on the error vector.

Implementation. We demonstrate the efficiency of our constructions with an implementation of our random OT extension protocol. The most costly part of the implementation is a large matrix-vector multiplication, which comes from applying the LPN assumption. We optimize this using a variant of LPN with quasi-cyclic codes, similarly to several recent, candidate post-quantum secure cryptosystems [ABB+19, MBD+18, AMAB+19], and present different tradeoffs with parameter choices. Our protocols have a very low communication overhead and perform significantly faster than previous, state-of-the-art protocols [IKNP03, ALSZ13, KOS15] in environments with restricted bandwidth. For instance, in a 100Mbps WAN setting, we are around 5x faster, and this improves to 47x in a 10MBps WAN. This is because, while our computational costs are around an order of magnitude higher, we need around 1000–2000 times less communication than the other protocols. We expect that additional optimizations of our implementation and the underlying error-correcting code will further improve the computational cost.

Applications. As well as the new application to NISC with silent preprocessing, our protocols can be applied to a range of traditional secure computation tasks. Below we mention just a few areas where we expect silent OT extension and VOLE to have an impact.

- *Semi-honest MPC for binary circuits.* In the semi-honest "GMW protocol" [GMW87], the correlated randomness needed to evaluate a Boolean circuit can be obtained from two random OTs per AND gate. Plugging in our random OT extension, we obtain a practical 2-PC protocol where each party communicates just 2 bits per AND gate on average. This is around 30x less communication than the state-of-the-art [DKS+17].
- *Malicious MPC for binary circuits.* Protocols based on authenticated garbling [WRK17a, WRK17b] and BMR [HSS17] are currently the state-of-the-art in maliciously secure MPC for binary circuits in a high-latency network. The main cost in these protocols comes from a preprocessing phase, where the parties use a large number of random, correlated oblivious

transfers to produce correlated randomness. Our protocol can produce the same kind of oblivious transfers with almost zero communication, and we estimate this could reduce the *overall* communication in these protocols by around an order of magnitude.
- *Malicious MPC for arithmetic circuits.* The "SPDZ" family of protocols [BDOZ11, DPSZ12, DKL+13, KOS16, KPR18] uses information-theoretic MACs to achieve malicious security in MPC based on secret sharing. A large batch of these MACs can be created using a single instance of a long, random VOLE correlation, with essentially optimal communication. Plugging in our maliciously secure VOLE construction will reduce the costs of previous works that use either homomorphic encryption or string-OT to create MACs.
- *Private set intersection (PSI).* In circuit-based PSI, a generic 2-PC protocol is used to first compute a secret-sharing of the intersection of two sets, and then perform some useful computation on the result [HEK12, PSSZ15, PSTY19]. With the improvements to GMW mentioned above, we can expect to obtain a similar reduction in communication for these families of PSI protocols.

Concurrent Work. In recent, concurrent work, Schoppmann et al. [SGRR19] presented optimizations and an implementation of the VOLE protocol by Boyle et al. [BCGI18]. Similarly to our work, they observe that the distributed setup procedure can be parallelized and performed in only two rounds, although they only apply this to VOLE correlations and not two-round OT extension. They also give a technique for efficient multi-point DPF evaluation, which allows batching t evaluations while avoiding the factor t overhead from a naive approach. This allows for an efficient implementation, without relying on the hardness of LPN for a regular error distribution as in our implementation. Finally, note that their protocols have semi-honest security, whilst we also give maliciously secure protocols with very low overhead.

1.2 Technical Overview

We now give an overview of our silent constructions in the semi-honest and malicious settings. For simplicity, we focus here on the case of 1-out-of-2 oblivious transfer.

We start by recalling the high-level idea of the pseudorandom correlation generators for vector-OLE (VOLE) and OT from [BCGI18, BCG+19]. These constructions distribute a pair of seeds to a sender and a receiver, who can then locally expand the seeds to produce many instances of pseudorandom OT or VOLE. To do so, they use two main ingredients: a variant of the LPN assumption, and a method for the two parties to obtain a *compressed* form of random secret shares $\boldsymbol{v}_0, \boldsymbol{v}_1$, satisfying

$$\boldsymbol{v}_1 = \boldsymbol{v}_0 + \boldsymbol{e} \cdot x \in \mathbb{F}_{2^\lambda}^N \tag{1}$$

where $\boldsymbol{e} \in \{0,1\}^N$ is a random, sparse vector held by one party, and $x \in \mathbb{F}_{2^\lambda}$ is a random field element held by the other party.

Given this, the shares can be randomized by taking a public, binary matrix H that compresses from N down to $n < N$ elements, and locally multiplying each share with H. This works because $\boldsymbol{u} = \boldsymbol{e} \cdot H$ is pseudorandom under a suitable variant of LPN. Writing $\boldsymbol{v} = \boldsymbol{v}_0 \cdot H$ and $\boldsymbol{w} = \boldsymbol{v}_1 \cdot H$, from (1) we then get $\boldsymbol{w} = \boldsymbol{v} + \boldsymbol{u}x$. This can be seen as a set of random *correlated OTs*, where $u_i \in \{0,1\}$ are the receiver's choice bits, and $(v_i, v_i + x)$ are the sender's strings, of which the receiver learns w_i. These can be locally converted into random string-OTs with a standard hashing technique [IKNP03].

To obtain a compressed form of the shares in (1), the constructions of [BCGI18, BCG+19] used a *distributed point function* (DPF) [GI14, BGI16]. Our first observation is that DPF is an overkill for this application,[9] and can be replaced with the simpler *puncturable pseudorandom*

[9] In contrast, we do not know how to replace DPF by PPRF in some of the other PCG constructions from [BCG+19], including the LPN-based constructions for low-degree correlations and the PRG-based constructions for one-time-truth-table correlations.

function (PPRF) primitive. A PPRF is a PRF F such that given an input x, and a PRF key k, one can generate a punctured key $\mathsf{k}\{x\}$ which allows evaluating F at every point except for x, and does not conceal any information about the value $F(\mathsf{k}, x)$. A PPRF can be built from any length-doubling pseudorandom generator, using a binary tree-based construction [KPTZ13, BW13, BGI14].

In the setup procedure, we will give the sender a random key k and x, and give to the receiver a random point $\alpha \in \{1, \ldots, N\}$, a punctured key $\mathsf{k}\{\alpha\}$, and the value $z = F(\mathsf{k}, \alpha) + x$. Given these seeds, the sender and receiver can now define the expanded outputs, for $i = 1, \ldots, n$:

$$\boldsymbol{v}_0[i] = F(\mathsf{k}, i), \quad \boldsymbol{v}_1[i] = \begin{cases} F(\mathsf{k}, i) & i \neq \alpha \\ z & \text{otherwise} \end{cases}$$

These immediately satisfy (1), with $\boldsymbol{e}$ as the α-th unit vector. To obtain sharings of sparse $\boldsymbol{e}$ with, say, t non-zero coordinates, as needed to use LPN, we repeat this t times and XOR together all t sets of outputs.

Conceptually, this construction is simpler than using a DPF, and moreover, as we now show, it brings several efficiency advantages.

Two-Round Setup of Puncturable PRF Keys. We present a simple, two-round protocol for distributed the above setup with semi-honest security, inspired by the DPF setup protocol of Doerner and shelat [Ds17]. The core of our protocol is the following procedure. For each of t secret LPN noise coordinates $\alpha_j \in [N]$ known to the receiver, the sender generates a fresh PRF key k_j, and wishes to obliviously communicate a punctured key $\mathsf{k}_j\{\alpha_j\}$ and hardcoded punctured output $z_j = PRF(\mathsf{k}_j, \alpha) + x$ to the receiver. Combined, this yields a secret sharing of the vector $x \cdot \boldsymbol{e}$, as required. To do so, for each $\mathsf{k}\{\alpha\}$, the parties made use of $\ell = \log N$ parallel OT executions: the sender's ℓ message pairs correspond to appropriate sums of partial evaluations from a consistent GGM PRF tree and his secret value x, and the receiver's ℓ selection bits correspond to the bits of his chosen path α.

Compared with previous works based on distributed point functions [BCGI18, BCG+19, Ds17], the number of rounds of interaction collapses from $O(\log N)$ to just two, given any two-round OT protocol. This is possible since the punctured point α is known to the receiver, whereas when α is secret-shared as in a DPF, the OTs in the setup procedure seem hard to parallelize.

Two-Round OT Extension and Silent NISC. We observe that in the two-round setup, the receiver can *already compute* part of its output before sending the first round message. In the case of OT, this part corresponds to its random vector of choice bits $\boldsymbol{u}$. This means that the receiver can already *derandomize* its OT outputs in the first round, by sending in parallel with its setup message the value $\boldsymbol{u} + \boldsymbol{c}$, where $\boldsymbol{c}$ is its *chosen* input vector. Since the sender can compute its random OT outputs after the first round, this leads to a two-round OT extension protocol that additionally enjoys the "silent preprocessing" feature of pushing the bulk of the computation to an offline phase, before the inputs are known. This can be generalized from OT to VOLE and other useful instances of *non-interactive secure computation* (NISC) [IKO+11], simultaneously inheriting the silent preprocessing feature from the PCG and the minimal interaction feature from an underlying NISC protocol. See Section 3 for a more detailed discussion of our new notion of NISC with silent preprocessing.

Maliciously Secure Setup. In the above semi-honest setup procedure, a malicious *receiver* has no cheating space; altered selection bits merely correspond to a different choice of noise coordinate $\alpha' \in [N]$. However, a malicious *sender* may generate message pairs inconsistent with any correct PRF evaluation tree, or use inconsistent inputs x across the t executions (in which case the outputs are not valid shares of $x \cdot \boldsymbol{u}$ for any single x). For example, by injecting errors into one of the two messages within an OT message pair, the sender can effectively "guess" and learn a bit of α, and will go unnoticed if his guess is correct.

We demonstrate that with small overhead, we can restrict a malicious sender to *only* such selective-failure attacks. This is formalized via an ideal functionality where the adversarial sender can send a guess range $I \subseteq [N]$ for α, a "getting caught" predicate is tested as a function of the receiver's true input, and the functionality either aborts or delivers the output accordingly. We then show that paired with an interactive leakage notion for LPN, this suffices to give us PCG setup protocols for VOLE and OT with malicious security.

Our basic maliciously secure protocols have 4 rounds, but this can be compressed to two rounds with the Fiat-Shamir transform, in the random oracle model. Just as in the semi-honest protocols, we can convert the setup protocols into NISC protocols, this time under a slightly stronger variant of LPN with one bit of *adaptive* leakage on the error vector. This leads to efficient two-round OT extension and VOLE protocols with malicious security.

2 Preliminaries

2.1 Puncturable Pseudorandom Function

Pseudorandom functions (PRF) are keyed functions which are indistinguishable from truly random functions, have been introduced in [GGM86]. A *puncturable pseudorandom function* (PPRF) is a PRF F such that given an input x, and a PRF key k, one can generate a *punctured* key, denoted $k\{x\}$, which allows evaluating F at every point except for x, and does not conceal any information about the value of F at x. PPRFs have been introduced in [KPTZ13,BW13,BGI14].

Definition 1 (t-Puncturable Pseudorandom Function). *A puncturable pseudorandom function (PPRF) with key space $\mathcal{K}$, domain $\mathcal{X}$, and range $\mathcal{Y}$, is a pseudorandom function F with an additional punctured key space $\mathcal{K}_p$ and three probabilistic polynomial-time algorithms (F.KeyGen, F.Puncture, F.Eval) such that*

- *F.KeyGen(1^λ) outputs a random key $K \in \mathcal{K}$,*
- *F.Puncture(K, S), on input a key $K \in \mathcal{K}$, and a subset $S \subset \mathcal{X}$ of size t, outputs a punctured key $K\{S\} \in \mathcal{K}_p$,*
- *F.Eval$(K\{S\}, x)$, on input a key $K\{S\}$ punctured at all points in S, and a point x, outputs $F(K, x)$ if $x \notin S$, and $\perp$ otherwise,*

such that no probabilistic polynomial-time adversary wins the experiment Exp-s-pPRF *represented on Figure 1 with non-negligible advantage over the random guess.*

By F.FullEval(K) we denote the algorithm that on input a key $K \in \mathcal{K}$ evaluates F on all inputs $\mathcal{X}$ and returns the vector of outputs.

Experiment Exp-s-pPRF

Setup Phase. The adversary $\mathcal{A}$ sends a size-t subset $S^* \in \mathcal{X}$ to the challenger. When it receives S^*, the challenger picks $K \xleftarrow{\$} F.\mathsf{KeyGen}(1^\lambda)$ and a random bit $b \xleftarrow{\$} \{0,1\}$.

Challenge Phase. The challenger sends $K\{S^*\} \leftarrow F.\mathsf{Puncture}(K, S^*)$ to $\mathcal{A}$. If $b = 0$, the challenger additionally sends $(F(K,x))_{x \in S^*}$ to $\mathcal{A}$; otherwise, if $b = 1$, the challenger picks t random values ($y_x \xleftarrow{\$} \mathcal{Y}$ for every $x \in S^*$) and sends them to $\mathcal{A}$.

Fig. 1. Selective security game for puncturable pseudorandom functions. At the end of the experiment, $\mathcal{A}$ sends a guess b' and wins if $b' = b$.

A PPRF can be constructed from any length-doubling pseudorandom generator, using the GGM tree-based construction [GGM86, KPTZ13, BW13, BGI14]. The construction proceeds as follows: On input a key K and a point x, set $K^{(0)} \leftarrow K$ and perform the following iterative

evaluation procedure: for $i = 1$ to $\ell \leftarrow \log |x|$, compute $(K_0^{(i)}, K_1^{(i)}) \leftarrow G(K^{(i-1)})$, and set $K^{(i)} \leftarrow K_{x_i}^{(i)}$. Output $K^{(\ell)}$. This procedure creates a complete binary tree with edges labeled by keys; the output of the PRF on an input x is the key labeling the leaf at the end of the path defined by x from the root of the tree.

- $F.\mathsf{KeyGen}(1^\lambda)$: output a random seed for G.
- $F.\mathsf{Puncture}(K, z)$: on input a key $K \in \{0,1\}^k$ and a point x, apply the above procedure and return $K\{x\} = (K_{1-x_1}^{(1)}, \ldots, K_{1-x_\ell}^{(\ell)})$.
- $F.\mathsf{Eval}(K\{x\}, x')$, on input a punctured key $K\{x\}$ and a point x, if $x = x'$, output $\perp$. Otherwise, parse $K\{x\}$ as $(K_{1-x_1}^{(1)}, \ldots, K_{1-x_\ell}^{(\ell)})$ and start the iterative evaluation procedure from the first $K_{1-x_i}^{(i)}$ such that $x'_i = 1 - x_i$.

To obtain a t-puncturable PRF with input domain $[n]$, one can simply run t instances of the above puncturable PRF and set the output of the PRF to be the bitwise xor of the output of each instance. With this construction, the length of a key punctured at t points is $t\lambda \log n$, where λ is the seed size of the PRG.

2.2 Learning Parity with Noise

In this work, we rely on variants of the Learning Parity with Noise (LPN) assumption [BFKL93] over either $\mathbb{F}_2$ or a large finite field $\mathbb{F}$, where the noise is assumed to have a small, fixed Hamming weight. In particular, our constructions use the *dual* form[10] of decisional LPN, defined below, where for efficiency reasons we choose the matrix from a family of codes that supports (nearly) linear-time matrix-vector multiplication.

In the following we define the LPN and dual-LPN assumptions over a general finite ring $\mathcal{R}$ with error distribution $\mathcal{D}(\mathcal{R})$. For the case of OT we will let $\mathcal{R} = \mathbb{F}_2$, and for the case of VOLE $\mathcal{R}$ will typically be a big finite field. [11]

Definition 2 (LPN). *Let $\mathcal{D}(\mathcal{R}) = \{\mathcal{D}_{k,N}(\mathcal{R})\}_{k,N\in\mathbb{N}}$ denote a family of distributions over a ring $\mathcal{R}$, such that for any $k, N \in \mathbb{N}$, $\mathsf{Im}(\mathcal{D}_{k,N}(\mathcal{R})) \subseteq \mathcal{R}^N$. Let $\mathbf{C}$ be a probabilistic code generation algorithm such that $\mathbf{C}(k, N, \mathcal{R})$ outputs a matrix $A \in \mathcal{R}^{k\times N}$. For dimension $k = k(\lambda)$, number of samples (or block length) $N = N(\lambda)$, and ring $\mathcal{R} = \mathcal{R}(\lambda)$, the $(\mathcal{D}, \mathbf{C}, \mathcal{R})$-$\mathsf{LPN}(k, N)$ assumption states that*

$$\{(A, \boldsymbol{b}) \mid A \xleftarrow{\$} \mathbf{C}(k, N, \mathcal{R}), \boldsymbol{e} \xleftarrow{\$} \mathcal{D}_{k,N}(\mathcal{R}), \boldsymbol{s} \xleftarrow{\$} \mathbb{F}^k, \boldsymbol{b} \leftarrow \boldsymbol{s} \cdot A + \boldsymbol{e}\}$$
$$\overset{c}{\approx} \{(A, \boldsymbol{b}) \mid A \xleftarrow{\$} \mathbf{C}(k, N, \mathcal{R}), \boldsymbol{b} \xleftarrow{\$} \mathcal{R}^N\}$$

Here and in the following, all parameters are functions of the security parameter λ and computational indistinguishability is defined with respect to λ. When $\mathcal{R} = \mathbb{F}_2$ and $\mathcal{D}$ is the Bernoulli distribution over $\mathbb{F}_2^N$, where each coordinate is 1 with probability r and 0 otherwise, this corresponds to the standard binary LPN assumption. Note that the search LPN problem, of finding the vector can be reduced to the decisional LPN assumption as defined above above when the code generator $\mathbf{C}$ outputs a uniform matrix A [BFKL93, AIK09]. However, this is less relevant for us as we are mainly interested in efficient variants with more structured codes. See [DI14] for further discussion of search-to-decision reductions in the general case.

[10] We could also use the standard primal form of LPN, but this leads to worse communication complexity in our constructions.

[11] While our current malicious VOLE protocol fails when applied over general non-field rings, the semi-honest variant is secure whenever the LPN assumption is secure. We leave the security analysis of LPN over non-field rings to future work.

LPN with Fixed Weight and Regular Noise. For a finite field $\mathbb{F}$, let $\mathcal{HW}_t(\mathbb{F})$ be the distribution of uniform, weight t vectors over $\mathbb{F}^N$; that is, a sample from $\mathcal{HW}_t(\mathbb{F})$ is a uniformly random non-zero field element in t random positions, and zero elsewhere. The corresponding assumption used in our constructions is denoted by $(\mathcal{HW}_t(\mathbb{F}), \mathbf{C}, \mathbb{F})$-$\mathsf{LPN}(k, N)$.

To increase efficiency in our constructions, we also consider a *regular* noise distribution. This is as in the fixed weight case, except the noise vector in $\mathbb{F}^n$ is divided into t consecutive sub-vectors of length $\lfloor n/t \rfloor$, where each sub-vector has a single noisy coordinate.

If the block length N and noise weight t are such that k random coordinates will be all noiseless with non-negligible probability (e.g., when t is constant and $N = \Omega(k^2)$), these structured variants can be broken via Gaussian elimination (cf. [AG11]). This attack does not apply to our constructions, which always have $N = O(k)$.

Definition 3 (dual LPN). *Let $\mathcal{D}(\mathcal{R})$ and $\mathbf{C}$ be as in Definition 2, $n, N \in \mathbb{N}$ with $N > n$, and define $\mathbf{C}^{\perp}(N, n, \mathcal{R}) = \{H \in \mathcal{R}^{N \times n} : A \cdot H = 0, A \in \mathbf{C}(N - n, N, \mathcal{R}), \mathsf{rank}(H) = n\}$.*

For $n = n(\lambda), N = N(\lambda)$ and $\mathcal{R} = \mathcal{R}(\lambda)$, the $(\mathcal{D}, \mathbf{C}, \mathcal{R})$-$\mathsf{dual\text{-}LPN}(N, n)$ assumption states that

$$\{(H, \boldsymbol{b}) \mid H \xleftarrow{\$} \mathbf{C}^{\perp}(N, n, \mathcal{R}), \boldsymbol{e} \xleftarrow{\$} \mathcal{D}(\mathcal{R}), \boldsymbol{b} \leftarrow \boldsymbol{e} \cdot H\}$$
$$\overset{c}{\approx} \{(H, \boldsymbol{b}) \mid H \xleftarrow{\$} \mathbf{C}^{\perp}(N, n, \mathcal{R}), \boldsymbol{b} \xleftarrow{\$} \mathcal{R}^n\}$$

We will slightly abuse our notations by omitting to explicitely mention the code $\mathbf{C}$ and writing $(\mathcal{D}, H, \mathcal{R})$-$\mathsf{dual\text{-}LPN}(N, n)$ for above dual-LPN assumption with a matrix $H \in \mathbf{C}^{\perp}(N, n, \mathcal{R})$.

The search version of the dual LPN problem is also known as syndrome decoding. For any fixed family of codes $\mathbf{C}$ and error distribution $\mathcal{D}$, the decisional version defined above is equivalent to the primal variant of LPN from Definition 2 with dimension $k = N - n$ and N samples. One direction (transforming an LPN instance into dual-LPN) follows from the simple fact that when H is the parity-check matrix of the code generated by A, we have $(\boldsymbol{s} \cdot A + \boldsymbol{e}) \cdot H = \boldsymbol{s} \cdot A \cdot H + \boldsymbol{e} \cdot H = \boldsymbol{e} \cdot H$. The reverse direction can be shown similarly to, e.g. [MM11, Lemma 4.9].

Attacks on LPN. We recall here the main attacks on LPN, following the analysis of [BCGI18]. We refer the reader to [EKM17] for a more comprehensive overview. We assume that $\mathcal{D}$ is a noise distribution with Hamming weight bounded by some integer t.

- **Gaussian elimination.** The most natural attack on LPN recovers $\boldsymbol{s}$ from $\boldsymbol{b} = \boldsymbol{s} \cdot A + \boldsymbol{e}$ by guessing n non-noisy coordinates of $\boldsymbol{b}$, and inverting the corresponding subsystem to verify whether the guess was correct. This approach recovers $\boldsymbol{s}$ in time at least $(1/(1-r))^n$ using at least $O(n/r)$ samples ($r = t/N$). For low-noise LPN, with noise rate $1/n^c$ for some constant $c \geq 1/2$, this translates to a bound on attacks of $O(e^{n^{1-c}})$ time using $O(n^{1+c})$ samples.
- **Information Set Decoding (ISD) [Pra62].** Breaking LPN is equivalent to solving its dual variant, which can be interpreted as the task of decoding a random linear code from its syndrome. The best algorithms for this task are improvements of Prange's ISD algorithm, which attempts to find a size-t subset of the rows of B (the parity-check matrix of the code) that spans $\boldsymbol{e} \cdot B$, where $t = rN$ is the number of noisy coordinates. The state of the art variant of Prange's information set decoding attack is the BJMM attack [BJMM12], which was analyzed in [TS16], and in the NIST candidate BIKE [ABB+19, Section 5.2], which also take into account the effect of the DOOM attack [Sen11] which applies to the specific case of LPN with quasi-cyclic codes.
- **The BKW algorithm [BKW00].** This algorithm is a variant of Gaussian elimination which achieves subexponential complexity even for high-noise LPN (e.g. constant noise rate), but requires a subexponential number of samples: the attack solves LPN over $\mathbb{F}_2$ in time $2^{O(n/\log(n/r))}$ using $2^{O(n/\log(n/r))}$ samples.

- **Combinations of the above [EKM17].** The authors of [EKM17] conducted an extended study of the security of LPN, and described combinations and refinements of the previous three attacks (called the *well-pooled Gauss attack*, the *hybrid attack*, and the *well-pooled MMT attack*). All these attacks achieve subexponential time complexity, but require as many sample as their time complexity.
- **Scaled-down BKW [Lyu05].** This algorithm is a variant of the BKW algorithm, tailored to LPN with polynomially-many samples. It solves LPN in time $2^{O(n/\log\log(n/r))}$, using $n^{1+\varepsilon}$ samples (for any constant $\varepsilon > 0$) and has worse performance in time and number of samples for larger fields.
- **Low-Weight Parity Check (cf. [ADI+17, Zic17]).** Eventually, all the previous attacks recover the secret $\boldsymbol{s}$. A more efficient attack (by a polynomial factor) can be used if one simply wants to distinguish $\boldsymbol{b} = \boldsymbol{s} \cdot A + \boldsymbol{e}$ from random: by the singleton bound, the minimal distance of the dual code of $\mathbf{C}$ is at most $n+1$, hence there must be a parity-check equation for $\mathbf{C}$ of weight $n+1$. Then, if $\boldsymbol{b}$ is random, it passes the check with probability at most $1/|\mathbb{F}|$, whereas if $\boldsymbol{b}$ is a noisy encoding, it passes the check with probability at least $((N-n-1)/N)^t$.

Example Instantiations. Our constructions will rely on dual-LPN with $N = s \cdot n$ and a fixed, small noise weight t, where s is a small constant and the dimension n is very large; for example, $n \approx 10^6, s = 2, t \approx 120$. We also use a regular error distribution to improve the efficiency of our implementation. Finally, we instantiate the code family with random, quasi-cyclic codes, which allow fast $\tilde{O}(n)$ time syndrome computation.

This leads an assumption that is almost the same as was recently used in code-based post-quantum cryptosystems [MBD+18, ABB+19, AMAB+19], the only differences being that we use a much larger dimension n and a regular error distribution, which as far as we know does not lead to significantly better attacks. For further discussion on our instantiation, security analysis and example parameters, see Section 7.1.

As discussed in [BCGI18], alternative choices of codes are possible, and can even be linear-time encodable based on [DI14] or LDPC codes. Optimizing and implementing such linear-time implementations is an interesting direction for future work.

2.3 Secure Computation and NISC

We use standard definitions of (composable) secure two-party computation. Our protocols can be analyzed and used either in a standalone setting, as formalized in [Can00, Gol04], or in a UC setting [Can01, PVW08, IKO+11]. It will be convenient to cast our protocols in a hybrid model that allows parallel calls to an ideal oblivious transfer functionality. These calls can be instantiated by any composable OT protocol (e.g., the "PVW protocol" [PVW08] when considering UC security against malicious adversaries in the CRS model). We use λ to denote a computational security parameter, which we view as a public parameter that is available to all algorithms even when not explicitly stated.

We will specifically be interested in 2-round protocols for "sender-receiver functionalities" that take an input x from a receiver R and input y from a sender S, and deliver an output $f(x, y)$ to R. The communication consists of a single message from the receiver to the sender followed by a single message from the receiver to the sender. Such protocols can be viewed as being *non-interactive* in that the receiver can publish its message $\hat{x}$ (which depends only on its input x) and then go offline, before even knowing who the sender will be. Then $\hat{x}$ can be used by any sender S (in fact, in some cases even multiple senders) by sending the encrypted output $\hat{z}$ to the receiver's mailbox. We use the term *non-interactive secure computation* from [IKO+11] (NISC for short) to highlight this qualitative advantage. When described in the OT-hybrid model, NISC protocols involve only one round of parallel OT calls. They can additionally involve a message from R to S and a message from S to R, as long as these messages (in an honest execution) do not depend on outputs of the OT oracle. Such NISC protocols in the OT-hybrid model can be

converted into NISC protocols in the plain model (or CRS model for malicious security) using any 2-round (parallel-)OT protocol.

2.4 Pseudorandom Correlation Generators

A (two-party) pseudorandom correlation generator (PCG) securely generates long correlated pseudo-randomness from a pair of correlated keys. Defining a PCG requires care, since the natural simulation-based definition is not realizable. Instead, the following relaxed definition has been proposed in [BCGI18, BCG+19].

The ideal output distribution of a PCG is specified by a (long) target correlation (R_0, R_1), e.g., n independent instances of an OT correlation. This target correlation is specified by PPT algorithm $\mathcal{C}$, called a *correlation generator*, where $\mathcal{C}(1^\lambda)$ outputs a pair of strings. We furthermore restrict $\mathcal{C}$ to be *reverse-samplable* in the following sense: there exists a PPT algorithm $\mathsf{RSample}$ such that for $\sigma \in \{0,1\}$, the correlation obtained via:

$$\{(R'_0, R'_1) \,|(R_0, R_1) \xleftarrow{\$} \mathcal{C}(1^\lambda), R'_\sigma := R_\sigma, R'_{1-\sigma} \xleftarrow{\$} \mathsf{RSample}(\sigma, R_\sigma)\}$$

is computationally indistinguishable from $\mathcal{C}(1^\lambda)$.

Examples for standard and useful correlations, all of which are reverse-samplable, include Oblivious Transfer (OT) correlation, where R_0 includes n independent pairs of bit-strings (s_0^i, s_1^i) and R_1 includes $(c_i, s_{c_i}^i$ for random bits c_i, and Vector-OLE (VOLE) correlation over a finite field $\mathbb{F}$, where $R_0 = (\boldsymbol{u}, \boldsymbol{v})$ for random $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}^n$, and $R_1 = (x, \boldsymbol{u}x + \boldsymbol{v})$ for random $x \in \mathbb{F}$.

Definition 4 (Pseudorandom Correlation Generator (PCG) [BCG+19]). *Let $\mathcal{C}$ be a reverse-samplable correlation generator. A* pseudorandom correlation generator (PCG) for $\mathcal{C}$ *is a pair of algorithms* $(\mathsf{PCG.Gen}, \mathsf{PCG.Expand})$ *with the following syntax:*

- $\mathsf{PCG.Gen}(1^\lambda)$ *is a PPT algorithm that given a security parameter λ, outputs a pair of seeds* $(\mathsf{k}_0, \mathsf{k}_1)$*;*
- $\mathsf{PCG.Expand}(\sigma, \mathsf{k}_\sigma)$ *is a polynomial-time algorithm that given party index $\sigma \in \{0,1\}$ and a seed k_σ, outputs a bit string $R_\sigma \in \{0,1\}^n$.*

The algorithms $(\mathsf{PCG.Gen}, \mathsf{PCG.Expand})$ *should satisfy:*

- **Correctness.** *The correlation obtained via:*

$$\{(R_0, R_1) \,|(\mathsf{k}_0, \mathsf{k}_1) \xleftarrow{\$} \mathsf{PCG.Gen}(1^\lambda), R_\sigma \leftarrow \mathsf{PCG.Expand}(\sigma, \mathsf{k}_\sigma)\}$$

  is computationally indistinguishable from $\mathcal{C}(1^\lambda)$.
- **Security.** *For corrupted party $\sigma \in \{0,1\}$, the following two distributions are computationally indistinguishable:*

$$\{(\mathsf{k}_\sigma, R_{\bar\sigma}) \mid (\mathsf{k}_0, \mathsf{k}_1) \xleftarrow{\$} \mathsf{PCG.Gen}(1^\lambda), R_{\bar\sigma} \leftarrow \mathsf{PCG.Expand}(\bar\sigma, \mathsf{k}_{\bar\sigma})\} \text{ and}$$
$$\{(\mathsf{k}_\sigma, R_{\bar\sigma}) \mid (\mathsf{k}_0, \mathsf{k}_1) \xleftarrow{\$} \mathsf{PCG.Gen}(1^\lambda), R_\sigma \leftarrow \mathsf{PCG.Expand}(\sigma, \mathsf{k}_\sigma), R_{\bar\sigma} \xleftarrow{\$} \mathsf{RSample}(\sigma, R_\sigma)\}$$

  where $\bar\sigma = 1 - \sigma$ and $\mathsf{RSample}$ *is the reverse sampling algorithm for $\mathcal{C}$.*

As shown in [BCG+19], a PCG as defined above can be used as a drop-in replacement for ideal correlated randomness generated by $\mathcal{C}$ in any application that remains secure even when $\mathcal{C}$ is replaced by the following corruptible version $\tilde{\mathcal{C}}$. In $\tilde{\mathcal{C}}$ the corrupted party can choose its own randomness, and the randomness of the honest party $R_{1-\sigma}$ is obtained by applying $\mathsf{RSample}$. It turns out that in most concretely efficient MPC protocols that consume correlated randomness, security still holds even with this corruptible variant. In particular, this holds for the simple protocols that implement standard (chosen-input) OT or VOLE from the corresponding correlations. However, applying PCGs, the pair of keys $(\mathsf{k}_0, \mathsf{k}_1)$ to be generated either by a trusted dealer or by a secure protocol realizing $\mathsf{PCG.Gen}$.

3 PCG Protocols and Silent NISC

We now define two new cryptographic primitives we introduce in this work: A *pseudorandom correlation generation protocol* (*PCG protocol* for short) and a *non-interactive secure computation protocol with silent preprocessing* (*silent NISC* for short).

3.1 PCG Protocols

The above notion of PCG gives a *deterministic* procedure for securely generating long sources of correlated randomness from short but *suitably correlated* seeds. It does not explicitly address the question of generating the seeds. In the following we formalize a natural generalization of PCGs to a *low-communication* protocol for securely generating long sources of correlated randomnness *from scratch*. By "low communication" we means that the total communication complexity is sublinear in the output length.[12]

We take the following natural definition approach: a PCG protocol for an ideal correlation $\mathcal{C}$ is a secure two-party protocol (in the usual sense) for the *corruptible* correlated randomness functionality $\tilde{\mathcal{C}}$ described below.

Definition 5 (PCG protocol). *Let $\mathcal{C}$ be a reverse-samplable correlation generator. Define a randomized functionality $\tilde{\mathcal{C}}$ that takes from a corrupted party σ a string $\tilde{r}_\sigma$ as input, and outputs to the honest party $\bar{\sigma}$ a string $r_{\bar{\sigma}}$ sampled by $\mathsf{RSample}(\sigma, \tilde{r}_\sigma)$. If no party is corrupted, $\tilde{\mathcal{C}}$ outputs to both parties a fresh pair of outputs generated by $\mathcal{C}$. A (two-party) PCG protocol is a two-party protocol realizing $\tilde{\mathcal{C}}$ in which the communication complexity grows sublinearly with the output length. In the case of security against* semi-honest adversaries*, we still allow the ideal-model corrupted party (if any) to pick its input $\tilde{r}_\sigma$ for $\tilde{\mathcal{C}}$ arbitrarily, whereas the real-model adversary must follow the protocol.*

As a simple corollary of an MPC composition theorem, a PCG protocol for $\mathcal{C}$ can serve as a substitute for ideal correlated randomness $\mathcal{C}$ in any higher-level application that remains secure even when $\mathcal{C}$ is replaced by $\tilde{C}$. Indeed, this is the case for standard MPC protocols that rely on OT correlations or other types of simple correlations, both for semi-honest and malicious security.

A general way of obtaining a PCG protocol is by distributing the randomized key generation functionality $\mathsf{PCG.Gen}$ of a PCG (as in Definition 4) via a secure two-party computation protocol, and then locally applying $\mathsf{PCG.Expand}$. Indeed, this is the approach suggested in [BCG+19] for the purpose of applying PCGs in the context of "MPC with silent preprocessing." However, our notion of a PCG protocol is less stringent than an alternative definition that requires securely emulating $\mathsf{PCG.Gen}$ for some PCG, while at the same time being as good for applications. We make use of this extra degree of freedom in our PCG protocols for the malicious model.

A central contribution of this work is the construction of *two-round* PCG protocols, namely ones involving only a message from R to S followed by a message from S to R. We refer to such a protocol as a *non-interactive PCG* protocol. We use the following syntax to highlight the fact that the message of R can be published as a "public key" before the sender(s) are known.

Definition 6 (Non-interactive PCG protocol). *A* non-interactive PCG protocol *is defined by 4 algorithms with the following syntax:*

- $\mathsf{R.Gen}(1^\lambda) \to (sk_\mathsf{R}, pk_\mathsf{R})$
- $\mathsf{S.Gen}(pk_\mathsf{R}) \to (sk_\mathsf{S}, m_\mathsf{S})$
- $\mathsf{R.Expand}(sk_\mathsf{R}, m_\mathsf{S}) \to r_\mathsf{R}$
- $\mathsf{S.Expand}(sk_\mathsf{S}) \to r_\mathsf{S}$

[12] In fact, in all protocols presented in this paper, the communication complexity only grows *polylogarithmically* with the output length, under widely believed variants of the LPN assumption.

We say that the above algorithms define a non-interactive PCG protocol for a reverse-samplable correlation $\mathcal{C}$ if the two-round protocol they naturally define (where each party outputs the output of Expand*) is a PCG protocol for $\mathcal{C}$ as in Definition 5.*

In a non-interactive PCG protocol as above, the two Gen algorithms can be viewed as defining a cheap setup that results in short, correlated keys. The two Expand algorithms are used to locally perform "silent preprocessing" that generates useful correlated randomness (e.g., many instances of an OT correlation, or few instances of a long VOLE correlation). In the most useful special case of OT correlations, we will refer to a non-interactive PCG that makes a small number of parallel OT calls as a non-interactive (or 2-round) *silent OT extension protocol*.

3.2 Silent NISC

In this section we define our new notion of *non-interactive secure computation with silent preprocessing*, or *silent NISC* for short. A silent NISC protocol for f can be viewed as a "best-of-both-worlds" combination of a non-interactive PCG protocol (see Definition 6) and a NISC protocol (see Section 2.3). That is, a 2-round (chosen-input) secure computation protocol that supports "silent preprocessing" followed by a light-weight (and often "non-cryptographic") online phase, without additional interaction.

Combining non-interactive PCG and NISC protocols in a generic way does not achieve the above goal, since it involves 4 rounds: two to generate the correlated randomness, and two to use it. To collapse these 4 rounds into two, we rely on the following feature of our concrete non-interactive PCG constructions. For useful NISC correlations such as OT and VOLE, the receiver's piece of the correlated randomness r_{R} can be split into two parts: $r^{\mathsf{in}}_{\mathsf{R}}$, which is used to mask its input, and $r^{\mathsf{out}}_{\mathsf{R}}$, used to unmask the output. The key feature is that the construction allows R to locally generate $r^{\mathsf{in}}_{\mathsf{R}}$ from its public key pk_{R} alone, independently of the sender. This enables R to prepare to a future NISC before the sender is even known.

More concretely, let $f(x, y)$ be a sender-receiver functionality with receiver input x and sender input y. Useful examples for which we get efficient solutions include: (1) n instances of string-OT; (2) bitwise-AND of two n-bit strings; (3) inner product of two length-n vectors over $\mathbb{F}$; (4) a general function f represented by a Boolean circuit, which can be efficiently and non-interactively reduced to (1) via garbled circuits (see [IKO+11, AMPR14, MR17] for such black-box reductions for the malicious model).

A *NISC protocol with silent preprocessing* (or silent NISC) for f is defined by 8 algorithms:

- $\mathsf{R.Gen}(1^\lambda) \to (sk_{\mathsf{R}}, pk_{\mathsf{R}})$
- $\mathsf{R.Expand}^{\mathsf{in}}(sk_{\mathsf{R}}) \to r^{\mathsf{in}}_{\mathsf{R}}$
- $\mathsf{S.Gen}(pk_{\mathsf{R}}) \to (sk_{\mathsf{S}}, pk_{\mathsf{S}})$
- $\mathsf{R.Expand}^{\mathsf{out}}(sk_{\mathsf{R}}, pk_{\mathsf{S}}) \to r^{\mathsf{out}}_{\mathsf{R}}$
- $\mathsf{S.Expand}(sk_{\mathsf{S}}) \to r_{\mathsf{S}}$
- $\mathsf{R.Msg}(r^{\mathsf{in}}_{\mathsf{R}}, x) \to \hat{x}$
- $\mathsf{S.Msg}(r_{\mathsf{S}}, \hat{x}, y) \to \hat{z}$
- $\mathsf{R.Dec}(r^{\mathsf{out}}_{\mathsf{R}}, x, \hat{z}) \to z$

The security requirement is that the 2-round protocol obtained by executing the above algorithms in any consistent order satisfies the security requirement of a (standard) NISC protocol for f.

To clarify the intended use and the features of our model for non-interactive secure computation protocols with silent preprocessing, we provide on Figure 2 a pictural representation of the protocol flow, illustrating the interdependencies between the algorithms, and we identify the main features of each of the algorithms (whether they require small communication, or only silent computation; whether they require cryptographic or non-cryptographic computation).

The 3 Expand algorithms define the "silent preprocessing" phase, that can be executed before the inputs are known. The last 3 algorithms define the online part of the NISC protocol, which

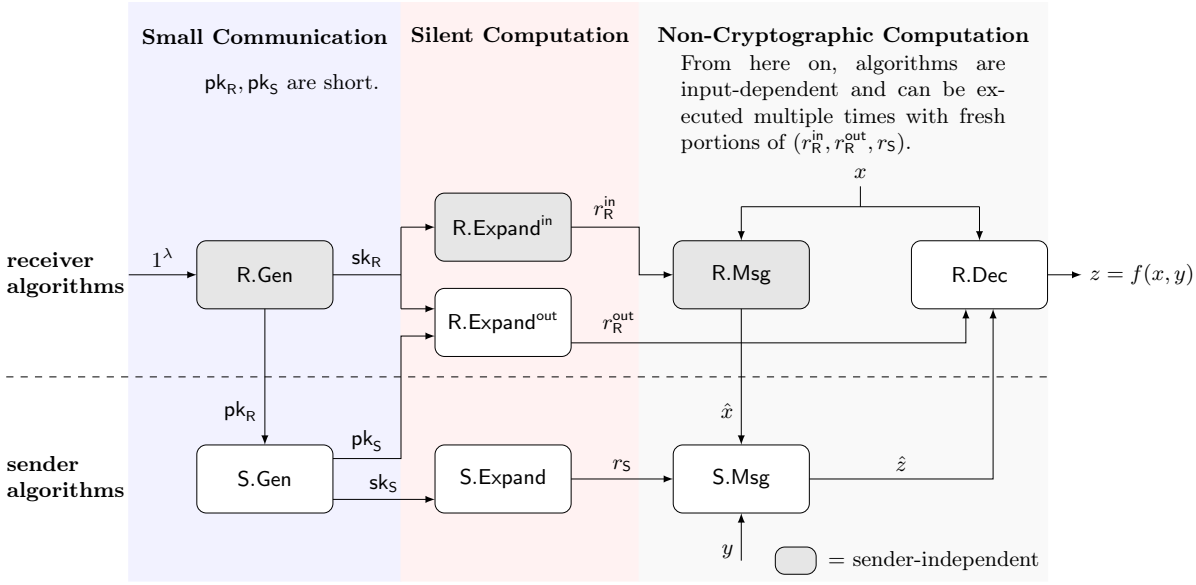

Fig. 2. Pictural representation of the protocol flow for non-interactive secure computation with silent preprocessing. The receiver input is y, the sender input is x, and the target output is $z = f(x, y)$.

is carried out once the inputs are known. Among the four examples given above, this part is "non-cryptographic" in the first three cases, and makes a black-box use of symmetric crypto in the last one.

We will be particularly interested in silent NISC realizing many parallel OTs using few parallel OTs, which can be viewed as a non-interactive, chosen-input variant of silent OT extension. While here one cannot make the communication complexity sublinear in the input length, our goal (which we achieve both in theorem and in practice) to make the communication very close to the total input length. This is the case even for the more challenging case of 1-bit OT, for which standard OT extension techniques that make a black-box use of cryptography [IKNP03, ALSZ13, KK13, KOS15] have a high communication overhead compared to the input length.

4 Improved PCGs for VOLE and OT

4.1 Simplified subfield VOLE generator

We provide a construction of a PCG for subfield-VOLE correlations in Fig. 3. Recall that in subfield-VOLE, one party receives random vectors $\boldsymbol{u} \in \mathbb{F}_p^N$ and $\boldsymbol{v} \in \mathbb{F}_{p^r}^N$, while the other party gets a random $x \in \mathbb{F}_{p^r}$, and $\boldsymbol{w} = \boldsymbol{u}x + \boldsymbol{v}$. The construction follows the informal description from Section 1.2 (where we described the special case $p = 2$, which is equivalent to correlated OT), and is essentially the same as the construction in [BCG+19], with a puncturable PRF instead of a DPF. Likewise, the security analysis is essentially identical to the analysis of [BCG+19].

4.2 Instantiating the puncturable PRF

We use a simple puncturable PRF based on the GGM approach [GGM86] (as defined in Section 2). To build a PPRF supporting t punctured points, we simply create t independent GGM PRFs, each punctured once. Evaluation of the final PPRF is defined by adding the evaluations of all t GGM-based PRFs.

More Efficient Puncturing Strategy. The key size for the above t-puncturable PRF is $t \cdot \lambda \log(N)$. It is possible to reduce this size to $t \cdot \lambda \log(N/t)$ with a more optimized puncturing strategy; however, this alternative construction is not compatible with our optimized distributed generation

Construction G_{sVOLE}

PARAMETERS: $1^\lambda, n, N, t, p, r \in \mathbb{N}$, where $N > n$. A matrix $H \in \mathbb{F}_p^{N\times n}$ and a weight-t error distribution $\mathcal{D}_{t,N}$ over $\mathbb{F}_p^N$.
CORRELATION: After expansion, outputs $(\boldsymbol{u}, \boldsymbol{v}) \in \mathbb{F}_p^n \times \mathbb{F}_{p^r}^n$ and $(x, \boldsymbol{w}) \in \mathbb{F}_{p^r} \times \mathbb{F}_{p^r}^N$, where $\boldsymbol{w} = \boldsymbol{u}x + \boldsymbol{v}$. We view $\mathbb{F}_p$ as a subfield of $\mathbb{F}_{p^r}$, via some fixed embedding and representation of field elements.
PPRF is a puncturable PRF with domain $[N]$ and range $\mathbb{F}_{p^r}$.
Gen: On input 1^λ:

1. Sample $\boldsymbol{e} \xleftarrow{\$} \mathcal{D}_{t,N}$. Let $S = \{\alpha_1, \ldots, \alpha_t\} \in [N]^t$ be the sorted indices of non-zero entries in $\boldsymbol{e}$, and $y_i = e_{\alpha_i} \in \mathbb{F}_p^*$.
2. Sample $x \xleftarrow{\$} \mathbb{F}_{p^r}$.
3. Sample $\mathsf{k}_{\mathsf{pprf}} \xleftarrow{\$} \mathsf{PPRF.Gen}(1^\lambda)$, and $\mathsf{k}^*_{\mathsf{pprf}} \leftarrow \mathsf{PPRF.Puncture}(\mathsf{k}_{\mathsf{pprf}}, S)$.
4. For $i = 1, \ldots, t$, let $z_i \leftarrow x \cdot y_i - \mathsf{PPRF.Eval}(\mathsf{k}_{\mathsf{pprf}}, \alpha_i)$
5. Let $\mathsf{k}_0 \leftarrow (\mathsf{k}^*_{\mathsf{pprf}}, S, \boldsymbol{y}, \{z_i\}_{i\in[t]})$ and $\mathsf{k}_1 \leftarrow (\mathsf{k}_{\mathsf{pprf}}, x)$.
6. Output $(\mathsf{k}_0, \mathsf{k}_1)$.

Expand: On input $(\sigma, \mathsf{k}_\sigma)$:

1. If $\sigma = 0$, parse k_0 as $(\mathsf{k}^*_{\mathsf{pprf}}, S, \boldsymbol{y}, \{z_i\}_i)$ and do as follows:
   (a) Define $\boldsymbol{e} \in \mathbb{F}_{p^m}^N$ using $\boldsymbol{y}, \{z_i\}_i$ as above.
   (b) For $j \in [N]$, define the j-th entry of vector $\boldsymbol{v}_0$ as

$$\boldsymbol{v}_0[j] = \begin{cases} z_i & \text{if } j = \alpha_i \in S \\ -\mathsf{PPRF.Eval}(\mathsf{k}^*_{\mathsf{pprf}}, j) & \text{if } j \notin S \end{cases}$$

   (c) Output $(\boldsymbol{u}, \boldsymbol{v}) \leftarrow (\boldsymbol{e} \cdot H, -\boldsymbol{v}_0 \cdot H)$.
2. If $\sigma = 1$, parse k_1 as $(\mathsf{k}_{\mathsf{pprf}}, x)$ and do as follows:
   (a) Compute $\boldsymbol{v}_1 \leftarrow \mathsf{PPRF.FullEval}(\mathsf{k}_{\mathsf{pprf}})$ in $\mathbb{F}_{p^r}^N$.
   (b) Output $(x, \boldsymbol{w} \leftarrow \boldsymbol{v}_1 \cdot H)$.

Fig. 3. PPRF-based PCG for subfield vector-OLE

protocols of Section 5 and Section 6. It is nonetheless useful in a setting where a trusted dealer is available to distribute the PCG seeds, or where computation is not a bottleneck compared to long-term storage. For a formal treatment, see Appendix B.

4.3 PCG for OT Correlation from Subfield-VOLE

In Fig. 4, we recall the construction of a PCG for OT correlations from a PCG for subfield-VOLE, introduced in [BCG+19]. The PCG produces a set of n random 1-out-of-p OTs based on a correlation robust hash function and the LPN assumption over $\mathbb{F}_p$ (where p is any prime power, not necessarily prime).

5 Semi-Honest PCG Protocols and Two-Round OT Extension

In this section, we show how to securely compute the Gen algorithm from Fig. 3, in just 2 rounds (assuming any 2-round OT). Using the construction of Fig. 4, this also leads to a distributed protocol for generating random OT correlations, assuming in addition a correlation-robust hash function. Then, we observe that our protocols satisfy a specific feature, which allows them to be derandomized into chosen-input VOLEs and OTs, without increasing their round complexity; this leads to 2-round OT extension and VOLE extension protocols, with silent preprocessing. Our construction relies on the GGM puncturable PRF [GGM86] constructed from any length-doubling pseudorandom generator G (Section 2.1).

On VOLE and reverse VOLE. Note that in a typical (chosen-input) VOLE, the sender inputs $(\boldsymbol{u}, \boldsymbol{v})$, while the receiver inputs x and gets $\boldsymbol{w} = \boldsymbol{u}x + \boldsymbol{v}$. In our two-round protocols, however,

Construction G_{OT}

Parameters:

- Security parameter 1^λ, integers n, r and prime power p with $p^r = O(2^\lambda)$.
- An $\mathbb{F}_p$-correlation-robust function $\mathsf{H} : \{0,1\}^\lambda \times \mathbb{F}_{p^r} \to \{0,1\}^\lambda$.
- The subfield-VOLE PCG $(G_{\mathsf{sVOLE}}.\mathsf{Gen}, G_{\mathsf{sVOLE}}.\mathsf{Expand})$ with parameters (n, p, r).

Correlation: Outputs $(R_0, R_1) = \big(\{(u_i, w_{i,u_i})\}_{i\in[n]}, \{w_{i,j}\}_{i\in[n],j\in[p]}\big)$, where $w_{i,j} \xleftarrow{\$} \{0,1\}^\lambda$ and $u_i \xleftarrow{\$} \{1,\ldots,p\}$, for $i \in [n], j \in [p]$.

Gen: On input 1^λ, output $(\mathsf{k}_0, \mathsf{k}_1) \leftarrow G_{\mathsf{sVOLE}}.\mathsf{Gen}(1^\lambda)$.

Expand: On input $(\sigma, \mathsf{k}_\sigma)$:

1. If $\sigma = 0$: compute $(\boldsymbol{u}, \boldsymbol{v}') \leftarrow G_{\mathsf{sVOLE}}.\mathsf{Expand}(\sigma, \mathsf{k}_\sigma)$, where $\boldsymbol{u} \in \mathbb{F}_p^n, \boldsymbol{v}' \in \mathbb{F}_q^n$. Compute
$$v_i \leftarrow \mathsf{H}(i, v_i') \quad \text{for } i = 1,\ldots,n$$
and output (u_i, v_i).
2. If $\sigma = 1$: compute $(x, \boldsymbol{w}') \leftarrow G_{\mathsf{sVOLE}}.\mathsf{Expand}(\sigma, \mathsf{k}_\sigma)$, where $x \in \mathbb{F}_q, \boldsymbol{w}' \in \mathbb{F}_q^n$. Compute
$$w_{i,j} \leftarrow \mathsf{H}(i, w_i' - j \cdot x) \quad \text{for } i = 1,\ldots,n, \forall j \in \mathbb{F}_p$$
and output $\{w_{i,j}\}_{i,j}$.

Fig. 4. PCG for n sets of 1-out-of-p random OT

we obtain a variant called *reverse VOLE* [ADI+17], where the *sender* inputs $(x, \boldsymbol{w})$, while the receiver inputs $\boldsymbol{u}$ and learns $\boldsymbol{v} = \boldsymbol{w} - \boldsymbol{u}x$. These two variants are equivalent when the inputs are random, so the distinction does not matter when constructing a PCG. In the chosen-input case, a reverse VOLE can be used to construct standard VOLE with one additional message (as observed in [ADI+17]), so our protocols give rise to 3-round chosen-input VOLE.

5.1 Distributed GGM-PPRF Correlation

We first consider a functionality where a party R holds a PPRF key $\mathsf{k}_{\mathsf{pprf}} \in \{0,1\}^\lambda$ for the GGM PPRF [GGM86], and a point $\alpha = \alpha_1 \cdots \alpha_\ell$ where $\ell = \ell(\lambda)$ is logarithmic in λ, and a party S holds a value $\beta \in \{0,1\}^\lambda$. The functionality computes and gives $k\{\alpha\}, \beta - \mathsf{PPRF.Eval}(k, \alpha)$ to R. The functionality is represented on Figure 5.

Functionality $\mathcal{F}_{\mathsf{PPRF\text{-}GGM}}$:

Parameters: $1^\lambda, \ell, p, r \in \mathbb{N}$. PPRF is the GGM puncturable PRF with domain $\{0,1\}^\ell$, key space $\{0,1\}^\lambda$, and range $\mathbb{F}_{p^r}$.

Inputs:

- S inputs $\beta \in \mathbb{F}_{p^r}$ and a PPRF key $\mathsf{k}_{\mathsf{pprf}} \in \{0,1\}^\lambda$.
- R inputs $\alpha \in \{0,1\}^\ell$.

Functionality:

- Compute $\mathsf{k}^*_{\mathsf{pprf}} = \mathsf{PPRF.Puncture}(\mathsf{k}_{\mathsf{pprf}}, \alpha)$.
- Send $\mathsf{k}^*_{\mathsf{pprf}}$ and $t = \beta - \mathsf{PPRF.Eval}(\mathsf{k}_{\mathsf{pprf}}, \alpha)$ to R.

Fig. 5. Functionality for distributing a PPRF correlation

Theorem 7. *Assuming a black-box access to a PRG, there exists a 2-party protocol for $\mathcal{F}_{\mathsf{PPRF\text{-}GGM}}$, with semi-honest security in the OT-hybrid model, and the following efficiency features. The computational complexity is dominated by $O(2^\ell)$ calls to a length-doubling PRG $G : \{0,1\}^\lambda \mapsto \{0,1\}^{2\lambda}$. The interaction consists of ℓ* parallel *calls to $\mathcal{F}_{\mathsf{OT}}$ and has communication complexity $\lambda + (3\lambda + 1)\ell$.*

Proof. We represent the protocol $\Pi_{\mathsf{PPRF\text{-}GGM}}$ satisfying the requirements of Theorem 7 on Figure 6. At a high-level, our protocol proceeds as follows: at each level i of the GGM tree, the holder of the PRF key k computes the XOR i^i_R of all odd-numbered nodes, and the XOR t^i_L of all even-numbered nodes. Using a single 1-out-of-2 OT, the receiver obtains one of (t^i_L, t^i_R). The protocol maintains the invariant that at the level $i-1$, the receiver can compute (from the previously stored information) all node values except one, implying that at level i, the receiver can compute all node values except two; recovering one of (t^i_L, t^i_R) allows him to compute exactly one of those two values, maintaining the invariant. At the end of the protocol, the receiver has stored ℓ intermediate keys (ℓ being the depth of the tree) which allow to compute all PRF outputs, except one. Transmitting a single additional value allow the sender to reveal him this value up to an offset β.

Correctness. We first show that the $s^i_{\alpha^*_i}$ values form a correct PRF key punctured at α. We need that for each i, $s^i_{\alpha^*_i}$ equals the GGM tree value that is sibling to the unique node on level i lying on the path to leaf α. This clearly holds for the first level, $i = 1$. On subsequent levels, R first computes the $2^i - 2$ values at level i that it can obtain from the previous values it knows, and then uses these to compute the final missing value $s^i_{\alpha^*_i}$. It does this by XORing (resp. summing over $\mathbb{F}_{p^r}$, for the last level) with the i-th OT output all-but-one of the odd-indexed, or even-indexed, values, depending on the choice $\overline{\alpha_i}$. Since the sender's OT inputs contain the XOR (resp. sum over $\mathbb{F}_{p^r}$, for the last level) of every odd- or even-indexed value, the receiver ends up with the value of the sibling node to $s^i_{\alpha_i}$. To see correctness of the final correction value t, a similar reasoning as above shows that $t = \beta - \mathsf{PPRF.Eval}(k, \alpha)$, as required.

Security. We exhibit a simulator Sim that generates a view indistinguishable from an honest run of the protocol as long as a single party is corrupted.

Case 1: S is corrupted. The simulation of R is straightforward, since R does not send any message directly to S in the protocol; R only send inputs to $\mathcal{F}_{\mathsf{OT}}$.

Case 2: R is corrupted. Sim receives the input α and the target output $(\{s^i_{\alpha^*_i}\}_{i\in[\ell]}, t)$ of R. Sim defines $t^1 \cdots t^\ell$ and the values $(s^i_j)_{i,j}$ inductively, starting with $t^1 \leftarrow s^1_{\overline{\alpha_1}}$ and following the output procedure of R (see Figure 6). Eventually, Sim computes

$$c' = t - \left(t^\ell + \sum_{j=0, j\neq\alpha}^{2^{\ell-1}} s^\ell_{2j+\alpha_\ell} \right).$$

Then, Sim simulates the OT sender using input (t^i, d_i) as input if $\overline{\alpha_i} = 0$, and (d_i, t^i) as input otherwise, where d_i is an arbitrary dummy value; Sim also sends c' in parallel to the OTs. The indistinguishability of the simulation follows directly from the definition of $\mathcal{F}_{\mathsf{OT}}$ and by construction of c'.

5.2 Semi-Honest Non-Interactive PCG Protocol for Subfield-VOLE Correlations

We now construct a semi-honest non-interactive PCG protocol for the subfield-VOLE correlation in the $\mathcal{F}_{\mathsf{PPRF\text{-}GGM}}$-hybrid model, by describing a 2-message, 2-party protocol to distributively execute the procedure $G_{\mathsf{sVOLE}}.\mathsf{Gen}$. This is modelled by the functionality $\mathcal{F}_{\mathsf{Gen}}$ in Figure 7. When $p > 2$, the implementation requires in addition a single (subfield-) reverse VOLE on vectors of length t. Reverse VOLE can be implemented in two rounds under an appropriate variant

Protocol $\Pi_{\mathsf{PPRF\text{-}GGM}}$:

PARAMETERS: $1^\lambda, \ell, p, r \in \mathbb{N}$. PPRF is the GGM puncturable PRF with domain $\{0,1\}^\ell$, key space $\{0,1\}^\lambda$, and range $\mathbb{F}_{p^r}$, constructed from a length-doubling PRG $G : \{0,1\}^\lambda \mapsto \{0,1\}^{2\lambda}$, and a second PRG $G' : \{0,1\}^\lambda \mapsto (\mathbb{F}_{p^r})^2$ used to compute the PRF outputs on the last level of the tree.

INPUTS:

- R inputs $\alpha \in \{0,1\}^\ell$.
- S inputs $\beta \in \mathbb{F}_{p^r}$ and a PPRF key $\mathsf{k}_{\mathsf{pprf}} \in \{0,1\}^\lambda$.

PROTOCOL:

1. R and S execute in parallel ℓ calls to $\mathcal{F}_{\mathsf{OT}}$, where for $i = 1$ to $\ell - 1$:
   - R uses as input the choice bit $\overline{\alpha_i}$;
   - S computes the 2^i partial evaluations at level i of the GGM tree defined by k, denoted $s^i_0, \ldots, s^i_{2^i-1}$ (in left-to-right order) and uses the two OT inputs

$$t^i_L = \bigoplus_{j \in [0, 2^{i-1})} s^i_{2j}, \quad t^i_R = \bigoplus_{j \in [0, 2^{i-1})} s^i_{2j+1}.$$

   and for the last OT,
   - R uses as input the choice bit $\overline{\alpha_\ell}$;
   - S computes the 2^ℓ evaluations of the GGM tree defined by k, denoted $s^\ell_0, \ldots, s^\ell_{2^i-1} \in (\mathbb{F}_{p^r})^{2^\ell}$ (in left-to-right order) and uses the two OT inputs

$$t^\ell_L = \sum_{j=0}^{2^{\ell-1}} s^\ell_{2j}, \quad t^\ell_R = \sum_{j=0}^{2^{\ell-1}} s^\ell_{2j+1}.$$

2. In parallel to the OT calls, S sends $c = \beta - (t^\ell_L + t^\ell_R)$ to R.

OUTPUT: R computes its output as follows:

1. Let t^1 be R's output in the first OT. Define $s^1_{\overline{\alpha_1}} = t^1$.
2. For $i = 2, \ldots, \ell - 1$:
   (a) Compute $(s^i_{2j}, s^i_{2j+1}) = G(s^{i-1}_j)$, for $j \in [0, \ldots, 2^{i-1}), j \neq \alpha_1 \cdots \alpha_{i-1}$.
   (b) Let t^i be the output from the i-th OT.
   (c) Define $\alpha^*_i = \alpha_1 \cdots \alpha_{i-1}\overline{\alpha_i}$. Compute

$$s^i_{\alpha^*_i} = t^i \oplus \bigoplus_{\substack{j \in [0, 2^{i-1}), \\ j \neq \alpha^*_i}} s^i_{2j+\overline{\alpha_i}}$$

3. Compute $(s^\ell_{2j}, s^\ell_{2j+1}) = G'(s^{i-1}_j)$, for $j \in [0, \ldots, 2^{\ell-1}), j \neq \alpha_1 \cdots \alpha_{\ell-1}$.
4. R receives c, and computes

$$t = c + t^\ell + \sum_{j=0, j \neq \alpha}^{2^{\ell-1}} s^\ell_{2j+\alpha_\ell}$$

5. R outputs the punctured key $\{s^i_{\alpha^*_i}\}_{i \in [\ell]}$, and the final correction value t.

Fig. 6. Protocol $\Pi_{\mathsf{PPRF\text{-}GGM}}$ for distributing a GGM-based PPRF correlation with semi-honest security in the $\mathcal{F}_{\mathsf{OT}}$-hybrid model

of LPN [ADI+17] or using linearly homomorphic encryption. We represent the functionality $\mathcal{F}_{\mathsf{rev\text{-}VOLE}}$ on Figure 8. Note that in a reverse VOLE protocol, the sender is the one holding the input x (while in a standard VOLE, x is held by the receiver).

Functionality $\mathcal{F}_{\mathsf{sVOLE\text{-}Gen}}$

PARAMETERS: $1^\lambda, N, t, p, r \in \mathbb{N}$. PPRF is a puncturable PRF with domain $[N]$, key space $\{0,1\}^\lambda$, and range $\mathbb{F}_{p^r}$.

INPUTS:

- R inputs a weight-t vector $\boldsymbol{e} \in \mathbb{F}_p^N$. Let $\mathcal{S} = \{\alpha_1, \ldots, \alpha_t\} \in [N]^t$ be the sorted indices of non-zero entries in $\boldsymbol{e}$, and $y_i = e_{\alpha_i} \in \mathbb{F}_p^*$.
- S inputs $x \in \mathbb{F}_{p^r}$ and a PPRF key $\mathsf{k}_{\mathsf{pprf}} \in \{0,1\}^\lambda$.

FUNCTIONALITY:

1. Compute $\mathsf{k}^*_{\mathsf{pprf}} \leftarrow \mathsf{PPRF.Puncture}(\mathsf{k}_{\mathsf{pprf}}, \mathcal{S})$.
2. For $i = 1, \ldots, t$, let $z_i \leftarrow x \cdot y_i - \mathsf{PPRF.Eval}(\mathsf{k}_{\mathsf{pprf}}, \alpha_i)$
3. Let $\mathsf{k}_0 \leftarrow (\mathsf{k}^*_{\mathsf{pprf}}, \mathcal{S}, \boldsymbol{y}, \{z_i\}_{i\in[t]})$ and $\mathsf{k}_1 \leftarrow (\mathsf{k}_{\mathsf{pprf}}, x)$.
4. Output k_0 to R and k_1 to S.

Fig. 7. Functionality for the Generation Procedure of the Subfield-VOLE Generator

Functionality $\mathcal{F}_{\mathsf{rev\text{-}VOLE}}$

PARAMETERS: $t, p, r \in \mathbb{N}$.

INPUT: The sender S inputs a pair $(\boldsymbol{b}, x) \in \mathbb{F}_{p^r}^t \times \mathbb{F}_{p^r}$. The receiver R inputs a vector $\boldsymbol{y} \in \mathbb{F}_p$.

FUNCTIONALITY: Compute $\boldsymbol{c} \leftarrow \boldsymbol{y}x - \boldsymbol{b}$ and output $\boldsymbol{c}$ to R.

Fig. 8. Reverse Vector-OLE Functionality over a Field $\mathbb{F}_p$

Theorem 8. *There exists a 2-message protocol $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ which realizes the functionality $\mathcal{F}_{\mathsf{sVOLE\text{-}Gen}}(1^\lambda, N, t, p, r)$, with semi-honest security in the $(\mathcal{F}_{\mathsf{PPRF\text{-}GGM}}, \mathcal{F}_{\mathsf{rev\text{-}VOLE}})$-hybrid model, using t calls to $\mathcal{F}_{\mathsf{PPRF\text{-}GGM}}$, a single call to $\mathcal{F}_{\mathsf{rev\text{-}VOLE}}(t, p)$, and no further communication. Furthermore, when $p = 2$, the functionality can be implemented directly using t calls to $\mathcal{F}_{\mathsf{PPRF\text{-}GGM}}$, and no call to $\mathcal{F}_{\mathsf{rev\text{-}VOLE}}$.*

We present the protocol $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ in Figure 9. Correctness follows easily by inspection: for $i = 1$ to t, we have $z_i = w_i + c_i = (b_i - \mathsf{PPRF.Eval}(\mathsf{k}_{\mathsf{pprf}}, \alpha_i)) + c_i = x \cdot y_i - \mathsf{PPRF.Eval}(\mathsf{k}_{\mathsf{pprf}}, \alpha_i)$. Security is straightforward. We note that when $p = 2$, since $\boldsymbol{y}$ is a weight-t vector, it always hold that $y_i = 1$, hence computing a share of $x \cdot y_i = x$ is trivial and does not require a call to the VOLE functionality.

Implementing $\mathcal{F}_{\mathsf{PPRF\text{-}GGM}}$ with the protocol $\Pi_{\mathsf{PPRF\text{-}GGM}}$ and $\mathcal{F}_{\mathsf{OT}}$ with any 2-round semi-honest OT protocol, this immediately leads to a semi-honest non-interactive PCG protocol $\Pi_{\mathsf{sVOLE}}(\mathbb{F}_q)$ for the subfield-VOLE correlation:

- $\mathsf{R.Gen}(1^\lambda)$: sets pk_R to be the first message of $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ and sk_R to be the secret state of R.
- $\mathsf{S.Gen}(\mathsf{pk}_\mathsf{R})$: sets m_S to be the second message of $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ on first message pk_R, and sk_S to be the sender output in $\Pi_{\mathsf{sVOLE\text{-}Gen}}$.

- $\mathsf{R.Expand}(\mathsf{sk}_\mathsf{R}, m_\mathsf{S})$: computes the output k_0 of the receiver from the state sk_R and the second message m_S, and outputs $G_{\mathsf{sVOLE}}.\mathsf{Expand}(0, \mathsf{k}_0)$.
- $\mathsf{S.Expand}(\mathsf{sk}_\mathsf{S})$: outputs $G_{\mathsf{sVOLE}}.\mathsf{Expand}(1, \mathsf{sk}_\mathsf{S})$.

Corollary 9. *Assuming the* $(\mathcal{HW}_t, H, \mathbb{F}_q)$-dual-LPN$(N, n)$ *assumption,* $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ *is a semi-honest non-interactive PCG protocol for subfield-VOLE correlations over an arbitrary extension field* $\mathbb{F}_q$ *of* $\mathbb{F}_2$*, which only makes a black-box use of a* 1*-out-of-*2 *semi-honest 2-message OT and a length-doubling PRG* $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$*. By making additionally a single black-box use of a 2-message length-*t *semi-honest reverse VOLE, this can be generalized to arbitrary fields.*

In the above corollary, $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ makes $t \cdot \lceil \log N \rceil$ black-box accesses to the 1-out-of-2 semi-honest 2-message OT, $t \cdot N$ black-box accesses to a length-doubling PRG, and additionally computes one matrix-vector multiplication with H. Regarding communication, the size of pk_R is $t \cdot \lceil \log N \rceil \cdot N_\mathsf{R}$ and the size of m_S is $t \cdot (\lambda + \lceil \log N \rceil \cdot N_\mathsf{S})$, where N_R (resp. N_S) denote the receiver communication (resp. the sender communication) in the underlying OT protocol; over general fields, there is an additional $+M_\mathsf{R}(t, q, r)$ term in the size of pk_R and $+t \cdot M_\mathsf{S}(t, q, r)$ in the size of m_S, where $M_\mathsf{R}(t, q, r)$ (resp. $M_\mathsf{S}(t, q, r)$) denote the receiver communication (resp. the sender communication) in the underlying length-t reverse subfield-VOLE protocol over $\mathbb{F}_{q^r}$.

Protocol $\Pi_{\mathsf{sVOLE\text{-}Gen}}$

PARAMETERS: $1^\lambda, N = 2^\ell, t, p, r \in \mathbb{N}$. PPRF is a puncturable PRF with domain $[N]$ and range $\mathbb{F}_{p^r}$.

INPUTS:

- R inputs a weight-t vector $\boldsymbol{e} \in \mathbb{F}_p^N$. Let $\mathcal{S} = \{\alpha_1, \ldots, \alpha_t\} \in [N]^t$ be the sorted indices of non-zero entries in $\boldsymbol{e}$, and $y_i = e_{\alpha_i} \in \mathbb{F}_p^*$.
- S inputs $x \in \mathbb{F}_{p^r}$ and a PPRF key $\mathsf{k}_{\mathsf{pprf}} \in \{0,1\}^\lambda$.

PROTOCOL:

1. S picks $\boldsymbol{b} \xleftarrow{\$} \mathbb{F}_p^t$.
2. R and S call $\mathcal{F}_{\mathsf{rev\text{-}VOLE}}(t, p)$ on respective inputs $(\boldsymbol{y}, (\boldsymbol{b}, x))$. R receives an output $\boldsymbol{c}$.
3. For $i = 1$ to t, R and S call $\mathcal{F}_{\mathsf{PPRF\text{-}GGM}}(1^\lambda, \ell, p, r)$ on respective inputs α_i and $(b_i, \mathsf{k}_{\mathsf{pprf}})$. R receives an output $(\mathsf{k}^*_{\mathsf{pprf}}, w_i)$.
4. For $i = 1$ to t, R computes $z_i \leftarrow w_i + c_i$. R outputs $(\mathsf{k}^*_{\mathsf{pprf}}, \mathcal{S}, \boldsymbol{y}, \{z_i\}_{i \in [t]})$ and S outputs $(\mathsf{k}_{\mathsf{pprf}}, x)$.

Fig. 9. Protocol for the Generation Procedure of the Subfield-VOLE Generator

5.3 Semi-Honest Non-Interactive Secure Computation with Silent Preprocessing

While the non-interactive PCG protocols of the previous section are interesting in their own right, we observe that they satisfy the features outlined in Section 3.2, and therefore lead to 2-round protocols, and even *silent NISC*, for the OT and the VOLE functionalities.

Semi-Honest Two-Round OT with Silent Preprocessing As observed in [BCG+19] (and shown in Fig. 4), a PCG for subfield-VOLE together with a correlation-robust hash function lead to a PCG G_{OT} for the ROT correlation. Using our distributed setup protocol $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ (which can be implemented in two rounds, given any two-round OT and two-round subfield-VOLE), together with the standard protocol for chosen-input OT from ROT, directly leads to a two-round OT extension protocol, which performs n OTs on s-bit strings with communication $(2s + 1) \cdot n + o(n)$ (for any s).

Theorem 10. *Assuming the* $(\mathcal{HW}_t, H, \mathbb{F}_p)$-dual-LPN$(N, n)$ *assumption,* Π_{OT} *is a* semi-honest 2-round OT extension with silent preprocessing *for generating* n 1*-out-of-*2 *OTs, which makes* $o(n)$ *black-box uses of a 2-round semi-honest* 1*-out-of-*2 *OT, and* $O(n)$ *black-box uses to a length-doubling PRG and an* $\mathbb{F}_p$*-correlation robust hash function.*

Assuming further any 2-round semi-honest reverse VOLE, there is a 2-round OT extension with silent preprocessing for 1*-out-of-*p *OT with comparable costs, using additionnally one black-box execution of a reverse-VOLE on length-*$o(n)$ *inputs.*

Proof. In the above theorem, Π_{OT} additionally requires the computation of one matrix-vector multiplication with H. It has total communication $(2s+1) \cdot n + o(n)$, where s is the bit-length of the sender messages. We represent the protocol for 2-round OT extension on Figure 10.

Correctness. By the correctness of $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ and G_{OT}, it holds that $v_i = w_{i,u_i}$ for $i = 1$ to n. Therefore, $m'_{i,s_i} - v_i = m_{i,s_i} + w_{i,t_i - s_i} - w_{i,u_i} = m_{i,s_i}$ since $t_i - s_i = u_i$.

Security. We exhibit a simulator Sim that generates a view indistinguishable from an honest run of the protocol as long as a single party is corrupted.

Case 1: S is corrupted. Sim simulates R by constructing $(\boldsymbol{e}, \boldsymbol{u})$ honestly, participating to $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ as R does (note that this does not require any input of R). Sim simulates $\boldsymbol{t}$ by sending $\boldsymbol{t}' \xleftarrow{\$} \mathbb{F}_p^n$. Since $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ securely emulates $\mathbb{F}_{\mathsf{Gen}}$, no information about $\boldsymbol{u}$ leaks to S during the execution of $\Pi_{\mathsf{sVOLE\text{-}Gen}}$. By the security of G_{OT}, $\boldsymbol{u}$ is computationally indistinguishable from random from the viewpoint of S, hence so is $\boldsymbol{t} = \boldsymbol{u} + \boldsymbol{s}$; therefore, the simulation is indistinguishable from an honest run of the protocol.

Case 2: R is corrupted. Sim receives R's input $(s_i)_{i \le n}$, R's random tape, and the corresponding target output $(m_{i,s_i})_i$ from the OT functionality. Sim simulates S by sampling k_1 and computing the $w_{i,j}$ honestly (this does not require the input of S). Sim computes the random noise vector $\boldsymbol{e}$ of R using R's random tape, from which he can compute R's output $\mathsf{k}_0 = (\boldsymbol{u}, \boldsymbol{v})$. For $i = 1$ to n, Sim computes m'_{i,s_i} as $m_{i,s_i} + v_i$, and picks $m'_{i,j} \xleftarrow{\$} \{0,1\}^\lambda$ for each $j \neq s_i$. Sim sends $(m'_{i,j})_{i,j}$ to R. By the security of $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ and G_{OT}, the $m'_{i,j}$ for $j \neq s_i$ are indistinguishable from random from the viewpoint of R, hence the simulation is indistinguishable from an honest run of the protocol.

Protocol Π_{OT}

Parameters: $1^\lambda, n, N = 2^\ell, t, p, r \in \mathbb{N}$. $H \in \mathbb{F}_p^{N \times n}$. PPRF is a puncturable PRF with domain $[N]$ and range $\mathbb{F}_{p^r}$. $\mathcal{D}_{t,N}$ is a weight-t error distribution over $\mathbb{F}_p^N$.

Inputs:

- R inputs n field elements $(s_i)_{i \le n} \in \mathbb{F}_p^n$.
- S inputs n length-p vectors $(\boldsymbol{m}_i)_{i \le n}$ where each $\boldsymbol{m}_i$ is over $(\{0,1\}^\lambda)^p$.

Protocol:

1. R picks $\boldsymbol{e} \xleftarrow{\$} \mathcal{D}_{t,N}$. Let $\mathcal{S} = \{\alpha_1, \ldots, \alpha_t\} \in [N]^t$ be the sorted indices of non-zero entries in $\boldsymbol{e}$, and $y_i = e_{\alpha_i} \in \mathbb{F}_p^*$. R computes the first part $\boldsymbol{u}$ of $G_{\mathsf{OT}}.\mathsf{Expand}(0, \mathsf{k}_0)$ (note that $\boldsymbol{u}$ is computed as $\boldsymbol{e} \cdot H$ where $\boldsymbol{e}$ depends solely on $\boldsymbol{e}$). R sets $\boldsymbol{t} \leftarrow \boldsymbol{u} + \boldsymbol{s}$
2. S samples $x \xleftarrow{\$} \mathbb{F}_{p^r}$ and $\mathsf{k}_{\mathsf{pprf}} \xleftarrow{\$} \mathsf{PPRF.Gen}(1^\lambda)$. He sets $\mathsf{k}_1 \leftarrow (\mathsf{k}_{\mathsf{pprf}}, x)$ and computes $\{w_{i,j}\}_{i \le n, j \le p} \leftarrow G_{\mathsf{OT}}.\mathsf{Expand}(1, \mathsf{k}_1)$.
3. R computes and sends to S the first round of $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ on input $\boldsymbol{e}$, together with $\boldsymbol{t}$.
4. S computes and sends to R the second round of $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ on input $(x, \mathsf{k}_{\mathsf{pprf}})$ together with $m'_{i,j} \leftarrow m_{i,j} + w_{i,t_i - j}$ for $i = 1$ to n and $j = 1$ to p; R gets an output k_0.
5. R computes $(\boldsymbol{u}, \boldsymbol{v}) \leftarrow G_{\mathsf{OT}}.\mathsf{Expand}(0, \mathsf{k}_0)$ and outputs $(m'_{i,s_i} - v_i)_{i \le n}$.

Fig. 10. Two-Round OT Extension

NISC for OT with Silent Preprocessing. Our 2-round OT extension protocol directly gives rise to a non-interactive secure computation protocol for the oblivious transfer functionality, with silent preprocessing, as defined in Section 3.2. For the sake of concreteness, we frame our OT extension protocol into the language of NISC with silent preprocessing on Figure 11.

Protocol $\mathsf{NISC}_{\mathsf{OT}}$

PARAMETERS: $1^\lambda, n, N = 2^\ell, t, p, r \in \mathbb{N}$. $H \in \mathbb{F}_p^{N \times n}$. PPRF is a puncturable PRF with domain $[N]$ and range $\mathbb{F}_{p^r}$. $\mathcal{D}_{t,N}$ is a weight-t error distribution over $\mathbb{F}_p^N$.
$\mathsf{par} \leftarrow (1^\lambda, n, N, t, p, r, H)$.

INPUTS:

- R inputs n field elements $(s_i)_{i \le n} \in \mathbb{F}_p^n$.
- S inputs n length-p vectors $(\boldsymbol{m}_i)_{i \le n}$ where each $\boldsymbol{m}_i$ is over $(\{0,1\}^\lambda)^p$.

PROTOCOL:

- $\mathsf{R.Gen}(\mathsf{par})$: pick $\boldsymbol{e} \xleftarrow{\$} \mathcal{D}_{t,N}$. Compute the first round of $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ on input $\boldsymbol{e}$. Set $\mathsf{sk_R}$ to be the secret state of R after computing the first round of $\Pi_{\mathsf{sVOLE\text{-}Gen}}$, and $\mathsf{pk_R}$ be the message computed by R in $\Pi_{\mathsf{sVOLE\text{-}Gen}}$.
- $\mathsf{R.Expand}^{\mathsf{in}}(\mathsf{sk_R})$: compute the first part $\boldsymbol{u}$ of $G_{\mathsf{OT}}.\mathsf{Expand}(0, \mathsf{k}_0)$ (note that $\boldsymbol{u}$ is computed as $\boldsymbol{e} \cdot H$ where $\boldsymbol{e}$ depends solely on $\boldsymbol{e}$). Output $r^{\mathsf{in}}_{\mathsf{R}} \leftarrow \boldsymbol{u}$.
- $\mathsf{S.Gen}(\mathsf{pk_R})$: sample $x \xleftarrow{\$} \mathbb{F}_{p^r}$ and $\mathsf{k_{pprf}} \xleftarrow{\$} \mathsf{PPRF.Gen}(1^\lambda)$. Set $\mathsf{sk_S} \leftarrow (\mathsf{k_{pprf}}, x)$. Define $\mathsf{pk_S}$ to be the second round message of S in $\Pi_{\mathsf{sVOLE\text{-}Gen}}$ on input $(x, \mathsf{k_{pprf}})$ after receiving the message $\mathsf{pk_R}$ from R.
- $\mathsf{R.Expand}^{\mathsf{out}}(\mathsf{sk_R}, \mathsf{pk_S})$: compute the output $r^{\mathsf{out}}_{\mathsf{R}}$ obtained by R with state $\mathsf{sk_R}$ upon receiving the message $\mathsf{pk_S}$ from S in $\Pi_{\mathsf{sVOLE\text{-}Gen}}$.
- $\mathsf{S.Expand}(\mathsf{sk_S})$: compute $r_{\mathsf{S}} = \{w_{i,j}\}_{i \le n, j \le p} \leftarrow G_{\mathsf{OT}}.\mathsf{Expand}(1, \mathsf{sk_S})$.
- $\mathsf{R.Msg}(r^{\mathsf{in}}_{\mathsf{R}}, \boldsymbol{s})$: output $\hat{s} \leftarrow r^{\mathsf{in}}_{\mathsf{R}} + \boldsymbol{s}$.
- $\mathsf{S.Msg}(r_{\mathsf{S}}, \hat{s}, (\boldsymbol{m}_i)_i)$: parse r_{S} as $\{w_{i,j}\}_{i \le n, j \le p}$. Compute $m'_{i,j} \leftarrow m_{i,j} + w_{i,\hat{s}_i - j}$ for $i = 1$ to n and $j = 1$ to p and output $\hat{z} = (m'_{i,j})_{i,j}$.
- $\mathsf{R.Dec}(r^{\mathsf{out}}_{\mathsf{R}}, \boldsymbol{s}, \hat{z})$: parse $\hat{z}$ as $(m'_{i,j})_{i,j}$. Compute $(\boldsymbol{u}, \boldsymbol{v}) \leftarrow G_{\mathsf{OT}}.\mathsf{Expand}(0, r^{\mathsf{out}}_{\mathsf{R}})$ and output $z = (m'_{i,s_i} - v_i)_{i \le n}$.

Fig. 11. Non-interactive secure computation with silent preprocessing for oblivious transfer

Semi-Honest NISC for Reverse Subfield-VOLE The same derandomization strategy as above directly implies, starting from the non-interactive PCG protocol for subfield-VOLE of Section 5.2, a NISC protocol for reverse subfield-VOLE with silent preprocessing, with features comparable to that of the NISC for OT extension. We omit the details.

Theorem 11. *Suppose the $(\mathcal{HW}_t, H, \mathbb{F}_p)$-dual-LPN$(N, n)$ assumption holds. Then there is a* semi-honest NISC protocol for reverse subfield-VOLE with silent preprocessing *for generating length-n reverse subfield-VOLEs over an arbitrary field $\mathbb{F}_p$, which uses $o(n)$ black-box executions of a 2-message semi-honest* 1*-out-of-*2 *OT, $O(n)$ black-box calls to a length-doubling PRG, one black-box call to a 2-message semi-honest reverse VOLE, and additionally computes one matrix-vector multiplication with H. It has total communication $(2s+1) \cdot n + o(n)$.*

6 Maliciously Secure PCG Protocols

In this section, we present protocols for VOLE, OT extension and NISC with security against *malicious* parties. Our final protocol for OT extension takes place in four rounds, and can be compressed to two rounds via Fiat-Shamir.

We begin in Section 6.1 by formalizing and describing an augmented PPRF primitive with a "malicious key verification" procedure, corresponding to the event of when a selective-failure attack will (or not) be identified. In Sections 6.2 and 6.3, we describe simple consistency checks that achieve the selective-failure-only security notion for a single GGM PPRF and for a batch of t PPRFs (with consistent x), respectively. Then, in Section 6.4, we build atop this functionality to obtain a PCG protocol for subfield VOLE with standard *malicious* security. In Section 6.5, we explain how the PCG protocol for subfield VOLE can be converted into a four round PCG protocol for random 1-out-of-p OT correlation. Finally, in Section 6.6 we show how to apply the Fiat-Shamir heuristic to compress the protocol down to just 2 rounds, relying on a slightly stronger assumption and the random oracle model. To obtain silent NISC for the OT functionality, which implies two-round OT extension on chosen inputs, we use the observation (as in our semi-honest protocol) that the receiver and sender can derandomize their inputs in parallel with their protocol messages.

6.1 Puncturable PRF with Malicious Keys

In the following sections we will realize a relaxed form of distributed PPRF setup functionality, where a corrupt sender may choose its own "master key," defining a PRF evaluation that need not coincide with any honest GGM tree, provided that it is consistent with the receiver's punctured point. The consistency of the keys will serve as the "getting caught" predicate in our ideal functionality. In this section, we introduce necessary terminology in order for the consistency check to be formulated.

To check consistency of the punctured key, we modify both the range and domain of the GGM construction used previously. We extend the domain from $[N]$ to $[2N]$, and the range so that the values of even-indexed leaves lie in $(\mathbb{F}_{p^r})^2$, whilst those of odd-indexed leaves are in $\{0,1\}^\lambda$. We will use a pair of PPRF consecutive outputs $((\omega, w), \gamma) \in (\mathbb{F}_{p^r})^2 \times \{0,1\}^\lambda$ as follows: The value w will correspond to the actual output of the PPRF. The value γ will be used to ensure consistency *within a single PPRF keys*. The value ω will be used to ensure consistency *across t PPRF keys*. To verify a single PPRF key, the punctured point $\alpha \in [N]$ is mapped to an even index in $[2N]$, so that an honest receiver can verify correctness of a punctured key by computing a hash of all the γ values. The sender computes the same hash and sends this to the receiver to check.

Formally, we can apply this technique to any PPRF which has the following key verification property for a maliciously generated key.

Definition 12 (Verification of malicious PPRF keys). *Let* $(\mathsf{PPRF.Gen}, \mathsf{PPRF.Puncture}, \mathsf{PPRF.Eval})$ *be a PPRF with keyspace* $\{0,1\}^\lambda$*, domain* $\mathcal{X}$ *and range* $\mathcal{Y}$*. We say that* PPRF *allows* verification of malicious keys *for a set* $\mathcal{K}$*, the malicious keyspace, if there exist efficient algorithms* $(\mathsf{Ver}, \mathsf{Puncture}^*, \mathsf{Eval}^*)$*, such that;*

- Ver *takes as input a malicious key* $K \in \mathcal{K}$ *and a set* $I \subseteq \mathcal{X}$ *and outputs* $0/1$*.*
- $\mathsf{Puncture}^*$ *takes as input a malicious key* K *and an index* $\alpha \in \mathcal{X}$ *and outputs a key* $\mathsf{k}^*_{\mathsf{pprf}}$ *punctured at* α*.*
- Eval^* *takes as input a malicious key* K^**, a set* $I \subseteq \mathcal{X}$ *and an index in* $x \in \mathcal{X}$*, and outputs a value in* $\mathcal{Y}$ *or* $\perp$*.*

Futher, we require for all $I \subseteq \mathcal{X}$ *and* $K^* \in \mathcal{K}$*:*

Consistency check. *If* $\mathsf{Ver}(K^*, I) = 1$ *then for all* $\alpha \in I, x \in \mathcal{X} \setminus \{\alpha\}$*:* $\mathsf{PPRF.PuncEval}(\mathsf{k}^*, x) = \mathsf{Eval}^*(K^*, I, \alpha)$*, where* $\mathsf{k}^* \leftarrow \mathsf{Puncture}^*(K^*, \alpha)$*.*
If this holds then we say that K^* *is* consistent *with the set* I*.*

GGM instantiation. In Appendix C.1, we show that the GGM puncturable PRF allows for verification of malicious keys. The malicious keyspace $\mathcal{K}$ will correspond to malicious choices of the sender's ℓ OT message pairs, while the malicious puncturing algorithm $\mathsf{Puncture}^*$ computes the same punctured key that an honest receiver would, for some maliciously chosen sender key. For a given malicious key K and subset of the PRF domain $I \subset [N]$, $\mathsf{Ver}(K, I)$ evaluates to 1 if the full-domain evaluation vector $\boldsymbol{s} = (s_0, \ldots, s_{N-1})$ of K (as defined by Eval^*) is "well formed" for I: namely, for any possible choice of the receiver's input $\alpha \in I$, then the sender's string $\boldsymbol{s}$ agrees with the corresponding receiver full-domain evaluation string, defined by the received key k^* derived from puncturing K (via $\mathsf{Puncture}^*$) at α.

6.2 Malicious Setup for Single-Point PPRF

As mentioned in the previous section, in order to achieve malicious security of a single PPRF evaluation, we use the redundancy introduced via the domain extension for checking consistent behaviour, by letting the sender provide a hash of all right leaves of the fully evaluated GGM tree. The idea is that a sender computing the correct hash value (relative to the receiver's input α), either behaved honestly, or guessed a set I such that $\alpha \in I$. This is captured in the functionality in Figure 12. The functionality is similar to the semi-honest functionality given in Figure 12, but the adversary is additionally allowed to give a set $I \subseteq [N]$ as guess. If indeed $\alpha \in I$, the sender will successfully finish the protocol and learn some partial information about α (namely, whether $\alpha \in I$). Otherwise, the functionality will abort.

In order for the right leaves of the GGM tree to fix a *unique* tree, we require the PRG of the last level $G' \colon \{0,1\}^\lambda \to (\mathbb{F}_{p^r})^2 \times \{0,1\}^\lambda$ to satisfy the *right-half injectivity* property below.

Definition 13 (Right-half injectivity). *We say a function $f = (f_0, f_1) \colon \{0,1\}^\lambda \to \mathcal{Y} \times \{0,1\}^\lambda, x \mapsto (f_0(x), f_1(x))$ is* right-half injective*, if its restriction to the right-half of the output space $f_1 \colon \{0,1\}^\lambda \to \{0,1\}^\lambda$ is injective.*

Remark 14. Note that the standard construction of a PRG from any one-way permutation is right-half injective [GPS16]. To avoid using a one-way permutation when implementing G', we can relax the half injectivity requirement to just *right-half collision resistance*, if G' is sampled at random from a family of hash functions that are collision-resistant in their right-half output. In practice, if $p^r = 2^\lambda$, we can define $G' : \{0,1\}^\lambda \to \mathbb{F}_{2^\lambda}^2 \times \{0,1\}^{2\lambda}$ and instantiate it with a standard counter mode PRG based on any block cipher, under the assumption that it is infeasible to find a collision in the latter 2λ bits of output. Note that here, we extended the latter part of its output from λ to 2λ bits, for 2^λ concrete security against birthday attacks.

Note that the protocol we present implements the functionality for the function PPRF_1, defined as the GGM PPRF used in the protocol, but where evaluation drops the final λ bits of output (which were used in the consistency check, so are no longer pseudorandom).

We give the protocol for distributed setup of PPRF_1 with security against malicious adversaries in Figure 13. First, in steps 1–6 the parties run the semi-honest protocol, such that the receiver holds a key k^* punctured at $\alpha \| 0$ and the sender a possibly malicious key K. As the tree is always punctured at an even value, both parties can compute all the right leaves of the GGM tree. The sender additionally sends a hash of all these leaves to the receiver. The receiver checks if this hash is consistent with his view and aborts otherwise.

The following theorem is proven in Appendix C.2.

Theorem 15. *Assuming a black-box access to a PRG $G : \{0,1\}^\lambda \mapsto \{0,1\}^{2\lambda}$, a right-half injective PRG $G' : \{0,1\}^\lambda \mapsto (\mathbb{F}_{p^r})^2 \times \{0,1\}^\lambda$, and a collision resistant hash function $h \colon \{0,1\}^{\lambda N} \to \{0,1\}^\lambda$, there exists a 2-party protocol implementing $\mathcal{F}_{\mathsf{mal\text{-}PPRF}}$ (see Fig. 12) for the puncturable PRF PPRF_1, with malicious security in the parallel OT-hybrid model, and the following efficiency features. The interaction consists of ℓ* parallel *calls to $\mathcal{F}_{\mathsf{OT}}$, and uses additional communication of $r \log p + \lambda$. The computational complexity is dominated by $O(2^\ell)$ calls each to G and G'.*

Functionality $\mathcal{F}_{\mathsf{mal\text{-}PPRF}}$:

PARAMETERS: $1^\lambda, N = 2^\ell, p, r \in \mathbb{N}$. PPRF is a puncturable PRF with domain $[N] = \{0,1\}^\ell$, key space $\{0,1\}^\lambda$, and range $(\mathbb{F}_{p^r})^2$, supporting verification of malicious keys.

INPUTS:

- R inputs $\alpha \in \{0,1\}^\ell$.
- S inputs $\beta \in (\mathbb{F}_{p^r})^2$ and a PPRF key $\mathsf{k}_{\mathsf{pprf}} \in \{0,1\}^\lambda$.

FUNCTIONALITY:

- If S is honest:
  1. Compute $\mathsf{k}^*_{\mathsf{pprf}} = \mathsf{PPRF.Puncture}(\mathsf{k}_{\mathsf{pprf}}, \alpha)$.
  2. Send $\mathsf{k}^*_{\mathsf{pprf}}$ and $w = -\mathsf{PPRF.Eval}(\mathsf{k}_{\mathsf{pprf}}, \alpha) + \beta$ to R, and $\mathsf{k}_{\mathsf{pprf}}$ to S.
- If S is corrupted:
  1. Wait for $\mathcal{A}$ to send a guess $I \subseteq [N]$ and a key $K^* \in \mathcal{K}$.
  2. Check that $\alpha \in I$ and that $\mathsf{Ver}(K^*, I) = 1$. If either check fails, send *abort* to R and wait for a response from R. When R responds with *abort*, forward this to S and halt.
  3. Compute $\mathsf{k}^*_{\mathsf{pprf}} = \mathsf{Puncture}^*(K^*, \alpha)$ and
  $$w = -\mathsf{Eval}^*(K^*, I, \alpha) + \beta.$$
  4. Send $\mathsf{k}^*_{\mathsf{pprf}}$ and w to R, and *success* to S.

Fig. 12. Functionality for malicious distributed setup of single-point PPRF

6.3 Malicious Setup of t PPRFs with Consistent Offset

For the VOLE setup with malicious security, we require a protocol for distributed setup of t PPRFs, where the inputs β_j of the sender are *consistent* across all evaluations. By consistent, we mean that each β_j is an additive share of $x \cdot y_j$, where the receiver knows the other share and the noise value $y_j \in \mathbb{F}_p^*$. To this end, we introduce a second consistency check, where the sender has to provide a linear combination of the outputs of each PPRF. We show that a cheating sender will fail this final check, unless he managed to guess part of the receiver's input. This guessing is modelled by the functionality $\mathcal{F}_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$ (Fig. 15), which is parameterized by a 1-puncturable PRF with verification of malicious keys.

To carry out this check, we exploit the extended range of the PPRF given by the functionality $\mathcal{F}_{\mathsf{mal\text{-}PPRF}}$. The extra $\mathbb{F}_{p^r}$ element from each evaluation serves to check consistency, by taking a random linear combination of all these outputs (for each PPRF), together with a linear combination of the original outputs, and sending these to the receiver to check. Note that without the extended range, sending a linear combination of PPRF outputs to the receiver would leak the sender's input x; with the extra outputs, however, the sender can use a random value χ which serves to mask x.

Since we sacrifice the extended outputs in the consistency check, the functionality $\mathcal{F}_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$ which we realize gives us a PPRF with range $\mathbb{F}_{p^r}$, as required, which is defined by simply ignoring the first element output from the one with range $\mathbb{F}_{p^r}^2$.

To create the shares of $x \cdot y_j$, when $p > 2$ we again need a slightly stronger flavor of reverse VOLE, presented in Figure 14. Here, we require the functionality to take two inputs by the sender $((\boldsymbol{\beta}, \chi), (\boldsymbol{b}, x))$, and only one input $\boldsymbol{y}$ by the receiver, and return to the sender values $\boldsymbol{\gamma}, \boldsymbol{c}$, such that $(\boldsymbol{\beta}, \boldsymbol{\gamma})$ constitute sharings of $x \times \boldsymbol{y}$ (and similar for $\boldsymbol{c}$). Note that it is not enough for our protocol to instead call the basic reverse VOLE functionality twice, as a receiver providing inconsistent inputs in the two calls can learn the input x of the sender in the protocol $\Pi_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$ (Figure 16).

For a proof of the following theorem we refer to Appendix C.3.

Protocol $\Pi_{\mathsf{mal\text{-}PPRF}}$:

PARAMETERS: $1^\lambda, \ell, N = 2^\ell, p, r \in \mathbb{N}$. $\mathsf{PPRF}_{\mathsf{GGM}}$ is the GGM puncturable PRF with domain $\{0,1\}^{\ell+1} = [2N]$, key space $\{0,1\}^\lambda$, and range $(\mathbb{F}_{p^r})^2 \times \{0,1\}^\lambda$, constructed from a length-doubling PRG $G : \{0,1\}^\lambda \mapsto \{0,1\}^{2\lambda}$, and a second PRG $G' : \{0,1\}^\lambda \mapsto (\mathbb{F}_{p^r})^2 \times \{0,1\}^\lambda$ used to compute the PRF outputs on the last level of the tree.

INPUTS:

- R inputs $\alpha \in \{0,1\}^\ell$.
- S inputs $\beta \in (\mathbb{F}_{p^r})^2$ and a PPRF key $\mathsf{k}_{\mathsf{pprf}} \in \{0,1\}^\lambda$.

PROTOCOL:

1. S samples a random seed $\mathsf{k}_{\mathsf{pprf}} \in \{0,1\}^\lambda$.
2. S computes the 2^i partial evaluations at level i of the GGM tree:
   (a) S sets $s_0^0 = \mathsf{k}_{\mathsf{pprf}}$.
   (b) For $i \in \{1,\dots,\ell\}, j \in [0,\dots,2^{i-1})$: S computes $(s_{2j}^i, s_{2j+1}^i) = G(s_j^{i-1})$.
   (c) For $j \in \{0,1\}^\ell$: S computes $(s_{2j}^{\ell+1}, s_{2j+1}^{\ell+1}) = G'(s_j^\ell) \in (\mathbb{F}_{p^r})^2 \times \{0,1\}^\ell$.
3. S computes the "left" and "right" halves for $i \in \{1,\dots,\ell\}$:
$$K_0^i = \bigoplus_{j \in [0,2^{i-1})} s_{2j}^i, \quad K_1^i = \bigoplus_{j \in [0,2^{i-1})} s_{2j+1}^i$$
4. S computes the "right" half for $i = \ell + 1$:
$$K_1^{\ell+1} = \bigoplus_{j \in \{0,1\}^\ell} s_{2j+1}^{\ell+1}$$
5. For $i = 1,\dots,\ell = \log N$ (in parallel) the parties run OT where in the i-th OT:
   (a) R inputs the choice bit $\overline{\alpha_i}$.
   (b) S inputs the pair (K_0^i, K_1^i).
6. S sends to R the key $K_1^{\ell+1}$ and the correction value
$$c = \beta - \sum_{j \in [N]} s_{2j}^{\ell+1}.$$
7. For the consistency check, S sets $\gamma_j = s_{2j+1}^{\ell+1}$ for all $j \in [N]$ and sends to R the value $\Gamma = h(\gamma_0,\dots,\gamma_{N-1})$.
8. Let $\{K^i\}_{i=1}^{\ell+1}$ denote the OT outputs received by R together with the key of the $(\ell+1)$-st level. Then, R proceeds as follows.
   (a) $\mathsf{k}^*_{\mathsf{pprf}} \leftarrow \mathsf{Puncture}^*(\{K^i\}_{i=1}^{\ell+1}, \alpha)$.
   (b) $\{s_j\}_{j \neq \alpha\|0} \leftarrow \mathsf{PPRF}_{\mathsf{GGM}}.\mathsf{FullEval}(\mathsf{k}^*_{\mathsf{pprf}}, \alpha\|0)$.
   (c) R receives c, and computes
$$w = c - \sum_{j \in [N] \setminus \{\alpha\}} s_{2j}$$
   (d) To verify consistency, R sets $\gamma_j = s_{2j+1}$ for all $j \in [N]$, and computes $\Gamma' = h(\gamma_0,\dots,\gamma_{N-1})$.
9. If $\Gamma = \Gamma'$, R outputs the punctured key $\mathsf{k}^*_{\mathsf{pprf}}$, and the final correction value w. Otherwise, R aborts.

Fig. 13. Protocol for distributed setup of single-point PPRF with consistency check

Functionality $\mathcal{F}_{\mathsf{g\text{-}rev\text{-}VOLE}}$

PARAMETERS: $t, p, r \in \mathbb{N}$.

INPUT: The sender S inputs a pair $((\boldsymbol{\beta}, \chi), (\boldsymbol{b}, x)) \in (\mathbb{F}_{p^r}^t \times \mathbb{F}_{p^r})^2$. The receiver R inputs a vector $\boldsymbol{y} \in \mathbb{F}_p^t$.

FUNCTIONALITY: Compute $\boldsymbol{\gamma} \leftarrow \boldsymbol{y}\chi - \boldsymbol{\beta}$ and $\boldsymbol{c} \leftarrow \boldsymbol{y}x - \boldsymbol{b}$ and output $(\boldsymbol{\gamma}, \boldsymbol{c})$ to R.

Fig. 14. Generalized Reverse Vector-OLE Functionality over a Field $\mathbb{F}_p$

Functionality $\mathcal{F}_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$:

PARAMETERS: $1^\lambda, N = 2^\ell, t, p, r \in \mathbb{N}$. PPRF is a puncturable PRF with domain $[N]$, key space $\{0,1\}^\lambda$, and range $\mathbb{F}_{p^r}$, supporting verification of malicious keys.

INPUTS:

- R inputs indices $\alpha_1, \ldots, \alpha_t \in [N]$ and weights $y_1, \ldots, y_t \in \mathbb{F}_p^*$. We define $\mathcal{S} = \{\alpha_1, \ldots, \alpha_t\}$.
- S inputs $\mathsf{k}_1 = (\{\mathsf{k}_j\}_{j\in[t]}, x)$, where $x \in \mathbb{F}_{p^r}$ and $\mathsf{k}_j \in \{0,1\}^\lambda$.

FUNCTIONALITY:

- If S is honest:
  1. Compute $\mathsf{k}_j^* \leftarrow \mathsf{PPRF.Puncture}(\mathsf{k}_j, \alpha_j)$, for $j \in \{1, \ldots, t\}$.
  2. Let $z_j \leftarrow x \cdot y_j - \mathsf{PPRF.Eval}(\mathsf{k}_j, \alpha_j)$ for $j \in \{1, \ldots, t\}$.
  3. Let $\mathsf{k}_0 \leftarrow (\{\mathsf{k}_j^*, z_j\}_{j\in[t]}, \mathcal{S}, \boldsymbol{y})$.
  4. Output k_0 to R.
- If S is corrupted:
  1. Receive from $\mathcal{A}$ t subsets $I_1, \ldots, I_t \subseteq [N]$ and a set of keys $K_1^*, \ldots, K_t^* \in \mathcal{K}$.
  2. For each $j \in \{1, \ldots, t\}$ check that $\alpha_j \in I_j$ and that $\mathsf{Ver}(K_j^*, I_j) = 1$. If any check fails, abort.
  3. Compute $k_j^* = \mathsf{PPRF.Puncture}^*(K_j^*, \alpha_j)$ for each $j \in \{1, \ldots, t\}$.
  4. Let $z_j \leftarrow x \cdot y_j - \mathsf{PPRF.Eval}^*(K_j^*, I_j, \alpha_j)$ for $j \in \{1, \ldots, t\}$.
  5. Output $\mathsf{k}_0 \leftarrow (\mathsf{k}_{\mathsf{pprf}}^*, \mathcal{S}, \boldsymbol{y}, \{z_j\}_{j\in[t]})$ to R and *success* to S.

Fig. 15. Functionality for malicious distributed setup of t puncturable PRFs

Protocol $\Pi_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$:

PARAMETERS: $1^\lambda, N = 2^\ell, t, p, r \in \mathbb{N}$. PPRF is a puncturable PRF with domain $[N]$, key space $\{0,1\}^\lambda$ and range $(\mathbb{F}_{p^r})^2$.

INPUTS:

- R inputs distinct indices $\alpha_1, \ldots, \alpha_t \in [N]$ and weights $y_1, \ldots, y_t \in \mathbb{F}_p^*$. We define $\mathcal{S} = \{\alpha_1, \ldots, \alpha_t\}$ and $\boldsymbol{y} = (y_1, \ldots, y_t) \in (\mathbb{F}_p^*)^t$.
- S inputs $x \in \mathbb{F}_{p^r}$.

PROTOCOL:

1. S picks $\boldsymbol{\beta}, \boldsymbol{b} \xleftarrow{\$} \mathbb{F}_{p^r}^t$ and $\chi \xleftarrow{\$} \mathbb{F}_{p^r}$.
2. R and S call $\mathcal{F}_{\mathsf{g\text{-}rev\text{-}VOLE}}(t, p, r)$ on respective inputs $\boldsymbol{y}$ and $((\boldsymbol{\beta}, \chi), (\boldsymbol{b}, x))$. R receives $(\boldsymbol{\gamma}, \boldsymbol{c}) \in \mathbb{F}_{p^r}^t \times \mathbb{F}_{p^r}^t$.
3. R and S call $\mathcal{F}_{\mathsf{mal}\text{-}\mathsf{PPRF}}(1^\lambda, N, p, r)$ t times on respective inputs α_j and (β_j, b_j). R receives k_j^* and (ω_j, w_j) for each $j \in \{1, \ldots, t\}$. If any of the runs is not successful, R receives *abort* from the functionality.
4. R samples $\tau, \tau_0, \ldots, \tau_{N-1} \xleftarrow{\$} \mathbb{F}_{p^r}$ and sends these to S.
5. S computes $(v_{S,2i}^j, v_{S,2i+1}^j) \leftarrow \mathsf{PPRF.Eval}(\mathsf{k}_j, i)$ for $i \in [N], j \in \{1, \ldots, t\}$, and sends $X = \chi + \tau \cdot x$ and $V_{S,j} = \sum_{i=0}^{N-1} \tau_i \cdot (v_{S,2i}^j + \tau \cdot v_{S,2i+1}^j)$ for $j \in \{1, \ldots, t\}$ to R.
6. R computes $(v_{R,2i}^j, v_{R,2i+1}^j) \leftarrow \mathsf{PPRF.Eval}'(\mathsf{k}_j^*, i)$ for $i \in [N], j \in \{1, \ldots, t\}$, where $\mathsf{PPRF.Eval}'$ is an algorithm that outputs $(\omega_j, w_j) + (\gamma_j, c_j)$ on input $(\mathsf{k}_j^*, \alpha_j)$, and $-\mathsf{PPRF.Eval}(\mathsf{k}_j^*, i)$ else.
7. R checks if $V_{S,j} + \sum_{i=0}^{N-1} \tau_i \cdot (v_{R,2i}^j + \tau \cdot v_{R,2i+1}^j) = X \cdot \tau_{\alpha_j} \cdot y_j$ for $j \in \{1, \ldots, t\}$. If any of these checks fail or R received *abort* from $\mathcal{F}_{\mathsf{mal}\text{-}\mathsf{PPRF}}$ in step 3, R aborts. Otherwise, R sends *ok* to $\mathcal{F}_{\mathsf{mal}\text{-}\mathsf{PPRF}}$ and outputs $\mathsf{k}_0 = (\{\mathsf{k}_j^*, z_j\}_j, \mathcal{S}, \boldsymbol{y})$.

Fig. 16. Protocol for malicious distributed setup of t puncturable PRFs

Theorem 16. *There exists a 4-message 2-party protocol $\Pi_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$ which securely implements the functionality $\mathcal{F}_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}(1^\lambda, N, p, r)$ for the puncturable PRF PPRF in the $\mathcal{F}_{\mathsf{g\text{-}rev\text{-}VOLE}}$-, parallel $\mathcal{F}_{\mathsf{mal}\text{-}\mathsf{PPRF}}$-hybrid model, with malicious security, using t parallel calls to $\mathcal{F}_{\mathsf{mal}\text{-}\mathsf{PPRF}}$, and only one call to $\mathcal{F}_{\mathsf{g\text{-}rev\text{-}VOLE}}$, and further communication of $(N+t+2)r\log p$ bits. Furthermore, when $p=2$, the functionality can be implemented in the parallel $\mathcal{F}_{\mathsf{mal}\text{-}\mathsf{PPRF}}$-hybrid model, using no call to $\mathcal{F}_{\mathsf{g\text{-}rev\text{-}VOLE}}$.*

Using an additional pseudorandom generator $\mathsf{PRG} : \{0,1\}^\lambda \to \mathbb{F}_{p^r}^{N+1}$, the communication can be reduced to just $(t+1)r\log p + \lambda$ bits, by sampling τ, τ_i using a random seed for PRG. We did not include this in the protocol, to simplify its description and proof of security.

6.4 4-Round VOLE and OT Setup with Malicious Security

The $\mathcal{F}_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$ functionality can be immediately used to distribute the setup of the subfield-VOLE PCG from Section 4. To prove this gives secure subfield-VOLE, however, we now need to assume that the dual-LPN assumption remains secure when an adversary is allowed to query (on average) one bit of information on the error vector. This reflects the fact that a malicious sender in $\mathcal{F}_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$ can try to guess subsets containing the receiver's α_j inputs, which correspond to non-zero coordinates of the error vector. This assumption with leakage is essentially the same as an assumption recently used for maliciously secure MPC based on syndrome decoding [HOSS18a]. For a formal definition, complete protocol and proof of the following theorem, we refer to Appendix C.4.

Theorem 17. *Let PPRF be a t-puncturable PRF, and suppose that $(\mathcal{HW}_t, \mathbf{C}, \mathbb{F}_p)$-$\mathsf{dual\text{-}LPN}(N, n)$ with static leakage holds. The protocol in Fig. 20 securely realizes the functionality $\mathcal{F}_{\mathsf{sVOLE}}$ (Fig. 19).*

Corollary 18. *Suppose that $(\mathcal{HW}_t, \mathbf{C}, \mathbb{F}_p)$-$\mathsf{dual\text{-}LPN}(N, n)$ with static leakage holds, where $N = O(n)$ and $t = o(n/(\lambda \log n))$. Then there exists a 4-message, maliciously secure PCG protocol for the subfield VOLE correlation, which makes $o(n)$ parallel calls to an oblivious transfer functionality, with communication complexity $o(n)$ bits.*

6.5 4-Round Random OT PCG Protocol with Malicious Security

Given the PCG protocol for the subfield VOLE correlation, we can easily convert this a PCG protocol for random oblivious transfer using a correlation robust hash function, as in construction G_{OT} (Fig. 4). To perform 1-out-of-2 OT, the parties run subfield VOLE over $\mathbb{F}_{2^\lambda}$, where the OT receiver, who acts as VOLE sender, obtains $\boldsymbol{u} \in \mathbb{F}_2^n$ and $\boldsymbol{v} = \boldsymbol{w} + \boldsymbol{u}x \in \mathbb{F}_{2^\lambda}^n$, while the OT sender / VOLE receiver gets $x \in \mathbb{F}_{2^\lambda}, \boldsymbol{w} \in \mathbb{F}_{2^\lambda}^n$. This can be seen as a correlated OT, where the receiver has choice bits u_i and messages v_i, which equal either w_i or $w_i + x$. To convert these to random OTs, the parties use a hash function H, and output respectively

$$(u_i, \mathsf{H}(i, v_i)), \quad (\mathsf{H}(i, w_i), \mathsf{H}(i, w_i + x))$$

We require the hash function to be correlation robust, namely, for any choices of w_i, the pairs $(w_i, \mathsf{H}(i, w_i + x))_i$ are indistinguishable from pairs $(w_i, U)_i$, where U is the uniform distribution [IKNP03, BCG+19]. This then gives a protocol that realizes the corruptible random OT functionality, where corrupt parties may influence their random outputs, in the $\mathcal{F}_{\mathsf{sVOLE}}$-hybrid model.

Notice that, as observed in [GKWY19], in order to prove security the index i must be included as an input to H, since otherwise a malicious receiver can break security by choosing its outputs of the corruptible $\mathcal{F}_{\mathsf{sVOLE}}$ functionality (where it is VOLE sender).[13]

The theorem below can be proven similarly to the proof of Theorem 17.

[13] In practice, however, we do not know of an attack on our concrete protocol if this is omitted, since a malicious VOLE sender cannot actually choose its $\boldsymbol{v}$ outputs; this is only needed for the security proof.

Theorem 19. *Suppose that there exists an $\mathbb{F}_p$-correlation-robust hash function, and $(\mathcal{HW}_t, \mathbf{C}, \mathbb{F}_p)$-dual-LPN$(N, n)$ with static leakage holds for $N = O(n)$ and $t = o(n/(\lambda \log n))$. Then there exists a 4-message, maliciously secure PCG protocol for the random 1-out-of-p OT correlation, which makes $o(n)$ parallel calls to an oblivious transfer functionality and communicates $o(n)$ bits.*

6.6 2-Round OT Extension and Silent NISC with Malicious Security

We now show how to compress the above protocols down to just two rounds, by applying the Fiat-Shamir heuristic. Additionally, under a slightly stronger version of the dual-LPN assumption with one bit of *adaptive* leakage (see Definition 23 in Section C.4), we can convert the random OTs/VOLEs into ones on chosen inputs in parallel with the setup messages. This gives a two-round OT extension protocol with malicious security.

First, observe that the only interaction in the malicious secure protocol for distributing t puncturable PRF keys (Fig. 16), besides the parallel calls to $\mathcal{F}_{\mathsf{mal\text{-}PPRF}}$ and $\mathcal{F}_{\mathsf{g\text{-}rev\text{-}VOLE}}$, is the random challenges $(\tau, \tau_0, \ldots, \tau_{N-1})$ from the receiver, and response from the sender. Using the Fiat-Shamir heuristic in the random oracle model, the sender can instead compute the challenges by hashing the transcript. From Theorem 15, $\mathcal{F}_{\mathsf{mal\text{-}PPRF}}$ can be realized with $o(n)$ parallel calls to OT; also, note that $\mathcal{F}_{\mathsf{g\text{-}rev\text{-}VOLE}}$ can be efficiently realized using any semi-homomorphic encryption scheme which supports zero-knowledge proofs of knowledge for ciphertext generation and homomorphic multiplication. For instance, [BDOZ11] shows how to instantiate this under the Paillier or LWE assumption. In the random oracle model, the zero-knowledge proofs can be made non-interactive, leading to a two round protocol overall.

Theorem 20. *Suppose that $(\mathcal{HW}_t, \mathbf{C}, \mathbb{F}_p)$-dual-LPN$(N, n)$ with static leakage holds, where $N = O(n)$ and $t = o(n/(\lambda \log n))$, and a semi-homomorphic encryption scheme exists. Then in the random oracle model, there is a non-interactive, maliciously secure PCG protocol for the subfield VOLE correlation, which makes $o(n)$ parallel calls to an oblivious transfer functionality and communicates $o(n)$ bits.*

Additionally assuming an $\mathbb{F}_p$-correlation robust hash function, there is a non-interactive PCG protocol for random 1-out-of-p OT with the same complexity.

To obtain silent NISC for the OT functionality, which implies two-round OT extension on chosen inputs, we use the observation (as in our semi-honest protocol) that the receiver and sender can derandomize their inputs in parallel with their protocol messages. In the malicious setting, this requires an *adaptive* variant of the dual-LPN with leakage assumption (Definition 23), since a corrupt sender can see the masked receiver's inputs before attempting to guess a few of the LPN error positions. We present the complete protocol for 1-out-of-2 OT in Figure 17.

Theorem 21. *Suppose that there exists a correlation-robust hash function, and $(\mathcal{HW}_t, \mathbf{C}, \mathbb{F}_2)$-dual-LPN$(N, n)$ with adaptive leakage holds for $N = O(n)$ and $t = o(n/(\lambda \log n))$. Then in the random oracle model, there exists a maliciously secure 2-message protocol for realizing n 1-out-of-2 oblivious transfers, which makes $o(n)$ parallel calls to an oblivious transfer functionality and communicates $o(n)$ bits.*

The above theorem also extends to 1-out-of-p OT for prime $p > 2$, by additionally assuming a semi-homomorphic encryption scheme as in Theorem 20.

7 Implementation

7.1 Instantiating LPN with Quasi-Cyclic Codes

Recall that our constructions use the dual-LPN assumption (Def. 3), which requires that given a parity-check matrix H, the syndrome $\boldsymbol{e} \cdot H$ is indistinguishable from random, where $\boldsymbol{e}$ is

Protocol $\Pi_{\mathsf{m\text{-}OT}}$

PARAMETERS: $1^\lambda, n, N = 2^\ell, t, 2, r \in \mathbb{N}$. PPRF is a puncturable PRF with domain $[N]$ and range $\mathbb{F}_{2^r}$, supporting verification of malicious keys. $H \in \mathbb{F}_2^{N \times n}$ is a matrix for which dual-LPN is hard. $\mathcal{D}_{t,N}$ is a weight-t error distribution over $\mathbb{F}_2^N$. RO is a random oracle with output space $(\mathbb{F}_{2^r})^{N+1}$. H is a correlation robust hash function.

- R inputs n field elements $(s_i)_{i \le n} \in \mathbb{F}_2^n$.
- S inputs n length-2 vectors $(\boldsymbol{m}_i)_{i \le n}$ where each $\boldsymbol{m}_i$ is over $(\{0,1\}^\lambda)^2$.

PROTOCOL:

1. R picks $\boldsymbol{e} \xleftarrow{\$} \mathcal{D}_{t,N}$. Let $\mathcal{S} = \{\alpha_1, \ldots, \alpha_t\} \in [N]^t$ be the sorted indices of non-zero entries in $\boldsymbol{e}$. R computes the first part $\boldsymbol{u}$ of $G_{\mathsf{sVOLE}}.\mathsf{Expand}(0, \{\mathsf{k}_j^*, z_j\}_{j=1}^t, \boldsymbol{e})$ (note that $\boldsymbol{u}$ is computed as $\boldsymbol{\mu} \cdot H$ where $\boldsymbol{\mu}$ depends solely on $\boldsymbol{e}$). R sets $\boldsymbol{t} \leftarrow \boldsymbol{u} + \boldsymbol{s}$.
2. R sends the first message for the protocol $\Pi_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$ with input $(\alpha_1, \ldots, \alpha_t)$. Simultaneously to the first message, R sends $\boldsymbol{t}$ to S. Let m_R denote the accumulation of receiver messages.
3. S samples $x \xleftarrow{\$} \mathbb{F}_{2^r}$ and $\mathsf{k}_j \xleftarrow{\$} \{0,1\}^\lambda$ for $j \in \{1, \ldots, t\}$, and uses $(x, \mathsf{k}_1, \ldots, \mathsf{k}_t)$ as input to $\Pi_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$. Let m_S denote the corresponding accumulation of messages of S in the protocol execution.
   - To replace the second message of R, S calls $\tau, \tau_1, \ldots, \tau_N \leftarrow \mathsf{RO}(m_\mathsf{R}, m_\mathsf{S})$ and computes the last message of $\Pi_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$ with these challenges.
   - S computes $(x, \boldsymbol{w}') \leftarrow G_{\mathsf{sVOLE}}.\mathsf{Expand}(1, \mathsf{k})$, where $\mathsf{k} = \{\mathsf{k}_1, \ldots, \mathsf{k}_t\}$.
   - S computes $w_{i,j} \leftarrow \mathsf{H}(i, w'_i - j \cdot x)$ for $i \in \{1, \ldots, n\}, j \in \{0,1\}$,
   - S sets $m'_{i,j} \leftarrow m_{i,j} + w_{i,t_i - j}$ for $i \in \{1, \ldots, n\}, j \in \{0,1\}$.
   - S sends $m_\mathsf{S}, X, V_{S,1}, \ldots, V_{S,j}, \{m'_{i,j}\}_{i \le n, j \le 2}$ to R.
4. R receives m_S containing k_j^*, (ζ_j, z_j) for each $j \in \{1, \ldots, t\}$ and further $X, V_{S,1}, \ldots, V_{S,j}$, and $\{m'_{i,j}\}_{i \in \{1,\ldots,n\}, j \in \{1,2\}}$.
   - R verifies all checks in $\Pi_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$ with $\tau, \tau_1, \ldots, \tau_N = \mathsf{RO}(m_\mathsf{R}, m_\mathsf{S})$. If any fails, abort.
   - R computes the second message $\boldsymbol{v}'$ of $G_{\mathsf{sVOLE}}.\mathsf{Expand}(0, \{\mathsf{k}_j^*, z_j\}_{j=1}^t, \boldsymbol{e})$.
   - R computes $v_i \leftarrow \mathsf{H}(i, v'_i)$ for $i \in \{1, \ldots, n\}$.
   - R outputs $(m'_{i,s_i} - v_i)_{i \le n}$.

Fig. 17. Two-Round 1-out-of-2 OT Extension with Malicious Security

sampled from some error distribution. Below, we describe how we instantiate the matrix and error distribution to achieve good concrete efficiency, and how we choose parameters for security.

Family of codes. We construct H based on quasi-cyclic codes. Recall that *cyclic codes* admit a parity-check matrix where every row is a cyclic shift of the previous row. In a *quasi-cyclic code*, the parity-check matrix can be written as a block matrix composed of several cyclic matrices.

Let $H' \in \mathbb{F}_2^{N \times n}$ be the parity-check matrix of a random, quasi-cyclic code in systematic form. Writing $N = s \cdot n$, where in our case we always choose $s \in \mathbb{Z}$, we have

$$H' = \left(I_n \ \mathsf{rot}(h_1) \cdots \mathsf{rot}(h_{s-1})\right)^\top$$

where I_n is the $n \times n$ identity, and $\mathsf{rot}(h_i)$ is the circulant matrix consisting of all n rotations of the random vector $h_i \in \mathbb{F}_2^n$. Note that multiplication of a vector with $\mathsf{rot}(h_i)$ is equivalent to a polynomial multiplication in $\mathbb{Z}_2[X]/(X^n - 1)$).

We then define H to be H' with its final row removed (see *Security* below). Computation of the syndrome of a vector $\boldsymbol{e} \in \mathbb{F}_2^{s \cdot n}$, viewed as the coefficients of degree-$(n-1)$ polynomials $e_0(X), \ldots, e_{s-1}(X) \in \mathbb{Z}_2[X]$, can now be written as

$$\boldsymbol{e} \cdot H = \mathsf{trunc}\left(e_0(X) + \sum_{i=1}^{s-1} e_i(X) \cdot h_i(X) \mod (X^n - 1)\right)$$

where $\mathsf{trunc}(\cdot)$ drops the last coefficient from its input.

Table 1. Dual-LPN parameters for estimated κ-bit security, counted as the minimum logarithm of the number of arithmetic operations for each of the ISD attack [Pra62, BJMM12], the low-weight parity check attack [Zic17] and the Gaussian elimination attack [EKM17]. The attacks take into account a $\sqrt{N}$ speedup from the DOOM attack [Sen11] which is enabled by our use of quasi-cyclic codes.

n	t	N/n	κ	n	t	N/n	κ
10^4	73	2	80	10^4	126	2	128
10^5	72	2	80	10^5	120	2	128
10^6	70	2	80	10^6	118	2	128
10^7	68	2	80	10^7	116	2	128
10^4	37	4	80	10^4	80	4	128
10^5	36	4	80	10^5	72	4	128
10^6	35	4	80	10^6	63	4	128
10^7	34	4	80	10^7	54	4	128

Fast quasi-cyclic encoding. To efficiently implement multiplication by H, we used the library `bitpolymul` [CCK+18] for fast multiplication in $\mathbb{Z}_2[X]$. Multiplying two degree n polynomials has complexity $\tilde{O}(n)$ using additive fast Fourier transforms, with an algorithm following the standard $\mathsf{FFT} \to \mathsf{PointwiseMult} \to \mathsf{FFT}^{-1}$ structure. We optimize this by preprocessing $\mathsf{FFT}(h_i)$, since the h_i values are fixed, and postponing FFT^{-1} until after summing up the s terms in the multiplication. This reduces computation by around 30–50%.

Noise distribution. To improve the efficiency of the puncturable PRF full-domain evaluation, we use a *regular* error vector $\boldsymbol{e} \in \mathbb{F}_2^N$, which is the concatenation of t random unit vectors, each of length N/t. This means we need to compute t full evaluations of PPRFs of domain size N/t, instead of size N, reducing the computational costs of this step by a factor t.

Security. Recall that for our dual-LPN variant, we require that given H, $\boldsymbol{e} \cdot H$ is indistinguishable from a uniform vector, where $\boldsymbol{e}$ is a weight-t, regular error vector. The reason we truncated the parity-check matrix H' to form H, is that with quasi-cyclic codes the parity bit of $\boldsymbol{e} \cdot H'$ only depends on H and t, so there is a trivial distinguisher [LP19] which truncating avoids. We also choose n to be prime to ensure that $X^n - 1$ does not have any non-trivial factors over $\mathbb{Z}_2$, apart from $X - 1$, avoiding attacks expoiting the quasi-cyclic structure [LJKS+16]. As also observed in [HOSS18b], we are not aware of any attacks that exploit a regular error distribution and perform significantly better than usual.

Note that quasi-cyclic codes have been used to construct optimized variants of the LPN-based cryptosystem of Alekhnovich and the code-based cryptosystem of McEliece [ABD+16,MBD+18], including several candidates in the ongoing NIST standardization process. Our assumption seems more conservative than these schemes, which need to embed a trapdoor into H that allows efficient decoding.

Choosing Parameters. We evaluate the concrete security of dual-LPN for various parameters (n, N, t), calculating the minimal number of noisy coordinates t such that dual-LPN with dimension n, number of samples N, and noise rate t/N requires 2^κ arithmetic operations to be broken using state-of-the-art attacks, for $\kappa \in \{80, 128\}$. The main attacks on LPN which apply in our setting (where the number of samples N is strongly restricted and the noise rate t/N is very low) are the low-weight parity check attack [Zic17], the Gaussian elimination attack and its variants [EKM17], and information set decoding (ISD) [Pra62] and its variants, especially BJMM [BJMM12]. We evaluated the concrete resistance of our LPN instances against all these attacks. For ISD [BJMM12], we relied on the analysis of [TS16] and of the NIST candidate BIKE [ABB+19, Section 5.2], which identify the BJMM attack as the most efficient, and provide a closed formula. Since we rely on quasi-cyclic codes to improve the computational efficiency, we also take into account the effect of the DOOM (Decoding One Out of Many) attack [Sen11]

which provides a $\sqrt{N}$ computational speedup against variants of LPN relying on quasi-cyclic codes. The results are summarized in Table 1.

Alternative Codes. Our choice of quasi-cyclic codes over alternative fast codes is mainly motivated by the fact that they are well studied, and fast implementations are available. However, as discussed in [BCGI18], we note that alternatives such as Druk-Ishai codes [DI14] or LDPC codes [Ale03, LM10] may be better. Both of these would allow for a *linear time* syndrome computation (instead of quasilinear), with small constants (less than $3d$ in the case of LDPC codes, where d is the row-weight of the sparse parity-check matrix). Moreover, these codes are not sensitive to the DOOM attack [Sen11], so might provide stronger resistance to standard attacks on LPN. Therefore, using such codes could potentially improve the efficiency of our implementation; we leave this to future work.

				LAN (10Gbps) times				WAN (100Mbps) times				WAN (10Mbps) times			
				n				n				n			
Protocol	Base type	λ	τ	10^7	10^6	10^5	10^4	10^7	10^6	10^5	10^4	10^7	10^6	10^5	10^4
This (SH)	hybrid	128	4	2,441	208	**76**	**67**	**2,726**	**513**	**422**	**425**	**2,756**	**518**	**454**	**422**
IKNP	base	128	4	**268**	**125**	94	91	13,728	1,850	493	459	128,954	13,332	1,756	445
This (SH)	hybrid	128	1	7,990	533	130	100	**8,252**	**808**	**451**	422	**8,291**	**815**	**467**	**422**
IKNP	base	128	1	**573**	**157**	**108**	**98**	15,622	2,030	613	**341**	129,011	13,285	1,672	429
This (Mal)	hybrid	128	4	2,659	280	**84**	**78**	**2,872**	**479**	**457**	**424**	**2,846**	**515**	**438**	**422**
KOS	base	128	4	**333**	**121**	110	111	13,722	1,933	589	426	129,052	13,391	1,804	536
This (Mal)	hybrid	128	1	8,765	584	141	**104**	**9,055**	**828**	**460**	**423**	**8,929**	**831**	**467**	**433**
KOS	base	128	1	**674**	**170**	**113**	106	15,741	2088	702	433	129,771	13,389	1,772	518

Table 2. The running time in milliseconds of our implementation compared to [ALSZ13] in both the LAN (0ms latency) and WAN (40ms one-way latency) settings, with security parameter $\lambda = 128$. λ is the computational security parameter. We set the compression N/n to 2. τ denotes the number of threads. Hybrid refers to doing 128 base OTs followed by IKNP to derive the total required base OTs.

		Total Comm. (bytes)				Comm./OT (bits)			
		n				n			
Protocol	Base type	10^7	10^6	10^5	10^4	10^7	10^6	10^5	10^4
This (SH/Mal)	hybrid	126,658	98,754	83,394	57,806	0.101	0.790	6.672	46.245
IKNP/KOS	base	160,056,360	16,011,518	1,655,784	168,186	128.045	128.092	132.463	134.549

Table 3. The communication overhead of our implementation compared to [IKNP03, KOS15], with $N/n = 2$ and $\lambda = 4$. See Table 2.

7.2 Results

We implement our semi-honest and malicious secure protocols and report their performance in several different settings. The source code can be found at `https://github.com/osu-crypto/libOTe`. The benchmark was performed on a single AWS c4.4xLarge instance with network latency artificially limited to emulate a LAN or WAN settings. Specifically, we consider a LAN setting with bandwidth of 10Gbps and 0ms latency and two WAN settings with 100, 10 Mbps & 40ms one-way latency. We compare with the semi-honest OT extension protocol of Ishai et al. [IKNP03] (IKNP) and the malicious secure protocol of Keller et al. [KOS15] (KOS) as implemented by a state-of-the-art library. Both our implementations and that of [IKNP03, KOS15] use the same three round malicious secure base OT protocol of Naor & Pinkas [NP05]. We

note that our protocols can be composed with a two round base OT protocol to give a two round OT extension. In the WAN setting this optimization would reduce the running times by approximately 40ms for all protocols.

The functionality we realize is to produce $n \in \{10^4, 10^5, 10^6, 10^7\}$ uniformly random OTs of length 128 bits. One distinction between our protocol and [IKNP03,KOS15] is that the choice bits of the receiver are uniformly chosen by our protocol, while [IKNP03, KOS15] allows the receiver to specify them. These random OTs can then be de-randomized with additional communication.

Table 2 contains the running time of our protocol. A fuller table, with alternative choices of parameters (security parameter λ, compression parameter N/n, method for computing the base OTs) is available in Appendix A.1. The primary takeaway is that both of our protocols achieve extremely low communication while the total running time remains competitive with or superior to KOS and IKNP. We report running times with each party having 1 or 4 threads, along with a background IO thread. In the LAN setting with sub-millisecond latency & 10Gbps we observe that the IKNP and KOS protocols achieve significant performance, requiring just 0.26 or 0.33 seconds to compute 10 million OTs with a single thread. While the computational cost of IKNP and KOS does outperform our implementation by roughly one order of magnitude, it also requires between 1000 and 2000 times more communication. This difference means that for more realistic network settings, such as 100Mbps, our implementation achieves a faster running time. With 4 threads and a limit of 100Mbps our implementation is up to 5 times faster (counting total running time, including both local computation and communication costs) and remains faster even for small n where our communication overheads are asymptotically closer together.

For the constrained setting of 10Mbps our protocol truly stands out with a 47 times speedup compared to IKNP with $n = 10^7$ and $t = 4$. We see a similar 46 times speedup in the malicious setting compared to KOS. Moreover, when comparing between the across the different network settings our protocol incurs minimal to no perform impact from decreasing bandwidth. For instance, with a 10Gbps connection our semi-honest protocol processes $n = 10^7$ OTs in 2.4 seconds while with 1000 times less bandwidth the protocol still just requires 2.8 seconds.

This scalability is explained in Table 3 which contains the communication overhead of our protocol. A fuller table, with alternative choices of parameters (security parameter λ, compression parameter N/n, method for computing the base OTs) is available in Appendix A.1. We parameterize our protocols by the desired security level $\lambda \in \{80, 128\}$ and a tunable parameter $s = N/n$. The latter controls a trade-off between the number of PPRF evaluations and length of the resulting vectors. To maintain security level of λ bits, increasing s results in fewer PPRF evaluations and less communication. However, it also increases the computational overhead. Our smallest running times were achieved with $s = 2$. However, we also consider $s = 4$ which decreases our total communication from 126KB to 80KB for $n = 10^7$. In contrast, the IKNP protocol requires 160MB for the same security level. This represents as much as a 2000 times reduction in communication. This low communication overhead results in our protocol requiring as little as 0.038 bits per OT for $n = 10^7$ and $\lambda = 80$. In our worst case of $n = 10^4$ our protocol still requires between 3 and 6 times less communication than IKNP. Another compelling property of our protocol is that we incur near constant additive communication overhead when comparing our malicious and semi-honest protocols.

8 Acknowledgements

E. Boyle, N. Gilboa, and Y. Ishai 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 1638/15, ERC grant 876110, and a grant by the BGU Cyber Center. Y. Ishai additionally supported by ISF grant 1709/14, NSF-BSF grant 2015782, DARPA SPAWAR contract N66001-15-C-4065, and a grant from the Ministry of Science and Technology, Israel and Department

of Science and Technology, Government of India. L. Kohl supported by ERC Project PREP-CRYPTO (724307) and by DFG grant HO 4534/2-2. This work was done in part while visiting the FACT Center at IDC Herzliya, Israel. P. Scholl supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 731583 (SODA), and the Danish Independent Research Council under Grant-ID DFF-6108-00169 (FoCC).

References

ABB+19. Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar Melchor, et al. Bike: Bit flipping key encapsulation. 2019. URL: https://bikesuite.org/files/round2/spec/BIKE-Spec-2019.06.30.1.pdf.

ABD+16. Carlos Aguilar, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor. Efficient encryption from random quasi-cyclic codes. Cryptology ePrint Archive, Report 2016/1194, 2016. http://eprint.iacr.org/2016/1194.

ADI+17. Benny Applebaum, Ivan Damgård, Yuval Ishai, Michael Nielsen, and Lior Zichron. Secure arithmetic computation with constant computational overhead. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 223–254. Springer, Heidelberg, August 2017. doi:10.1007/978-3-319-63688-7_8.

AG11. Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors. In Luca Aceto, Monika Henzinger, and Jiri Sgall, editors, *ICALP 2011, Part I*, volume 6755 of *LNCS*, pages 403–415. Springer, Heidelberg, July 2011. doi:10.1007/978-3-642-22006-7_34.

AIK09. Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography with constant input locality. *Journal of Cryptology*, 22(4):429–469, October 2009. doi:10.1007/s00145-009-9039-0.

Ale03. Michael Alekhnovich. More on average case vs approximation complexity. In *44th FOCS*, pages 298–307. IEEE Computer Society Press, October 2003. doi:10.1109/SFCS.2003.1238204.

ALSZ13. Gilad Asharov, Yehuda Lindell, Thomas Schneider, and Michael Zohner. More efficient oblivious transfer and extensions for faster secure computation. In Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors, *ACM CCS 2013*, pages 535–548. ACM Press, November 2013. doi:10.1145/2508859.2516738.

AMAB+19. Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, and Gilles Zémor. Hamming quasi-cyclic (HQC). 2019. URL: https://pqc-hqc.org/doc/hqc-specification_2018-12-14.pdf.

AMPR14. Arash Afshar, Payman Mohassel, Benny Pinkas, and Ben Riva. Non-interactive secure computation based on cut-and-choose. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 387–404. Springer, Heidelberg, May 2014. doi:10.1007/978-3-642-55220-5_22.

BCG+19. Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Efficient pseudorandom correlation generators: Silent OT extension and more. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part III*, volume 11694 of *LNCS*, pages 489–518. Springer, Heidelberg, August 2019. doi:10.1007/978-3-030-26954-8_16.

BCGI18. Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai. Compressing vector OLE. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018*, pages 896–912. ACM Press, October 2018. doi:10.1145/3243734.3243868.

BDOZ11. Rikke Bendlin, Ivan Damgård, Claudio Orlandi, and Sarah Zakarias. Semi-homomorphic encryption and multiparty computation. In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 169–188. Springer, Heidelberg, May 2011. doi:10.1007/978-3-642-20465-4_11.

Bea91. Donald Beaver. Efficient multiparty protocols using circuit randomization. In *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, pages 420–432, 1991. URL: https://doi.org/10.1007/3-540-46766-1_34, doi:10.1007/3-540-46766-1_34.

Bea95. Donald Beaver. Precomputing oblivious transfer. In Don Coppersmith, editor, *CRYPTO'95*, volume 963 of *LNCS*, pages 97–109. Springer, Heidelberg, August 1995. doi:10.1007/3-540-44750-4_8.

BFKL93. Avrim Blum, Merrick L. Furst, Michael J. Kearns, and Richard J. Lipton. Cryptographic primitives based on hard learning problems. In *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*, pages 278–291, 1993. URL: https://doi.org/10.1007/3-540-48329-2_24, doi:10.1007/3-540-48329-2_24.

BGI14. Elette Boyle, Shafi Goldwasser, and Ioana Ivan. Functional signatures and pseudorandom functions. In Hugo Krawczyk, editor, *PKC 2014*, volume 8383 of *LNCS*, pages 501–519. Springer, Heidelberg, March 2014. doi:10.1007/978-3-642-54631-0_29.

BGI16. Elette Boyle, Niv Gilboa, and Yuval Ishai. Function secret sharing: Improvements and extensions. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *ACM CCS 2016*, pages 1292–1303. ACM Press, October 2016. doi:10.1145/2976749.2978429.

BJMM12. Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 520–536. Springer, Heidelberg, April 2012. doi:10.1007/978-3-642-29011-4_31.

BKW00. Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. In *32nd ACM STOC*, pages 435–440. ACM Press, May 2000. doi:10.1145/335305.335355.

BW13. Dan Boneh and Brent Waters. Constrained pseudorandom functions and their applications. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part II*, volume 8270 of *LNCS*, pages 280–300. Springer, Heidelberg, December 2013. doi:10.1007/978-3-642-42045-0_15.

Can00. Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 13(1):143–202, January 2000. doi:10.1007/s001459910006.

Can01. Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd FOCS*, pages 136–145. IEEE Computer Society Press, October 2001. doi:10.1109/SFCS.2001.959888.

CCK+18. Ming-Shing Chen, Chen-Mou Cheng, Po-Chun Kuo, Wen-Ding Li, and Bo-Yin Yang. Multiplying boolean polynomials with frobenius partitions in additive fast fourier transform. *CoRR*, abs/1803.11301, 2018.

DI14. Erez Druk and Yuval Ishai. Linear-time encodable codes meeting the gilbert-varshamov bound and their cryptographic applications. In Moni Naor, editor, *ITCS 2014*, pages 169–182. ACM, January 2014. doi:10.1145/2554797.2554815.

DKL+13. Ivan Damgård, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, and Nigel P. Smart. Practical covertly secure MPC for dishonest majority - or: Breaking the SPDZ limits. In Jason Crampton, Sushil Jajodia, and Keith Mayes, editors, *ESORICS 2013*, volume 8134 of *LNCS*, pages 1–18. Springer, Heidelberg, September 2013. doi:10.1007/978-3-642-40203-6_1.

DKS+17. Ghada Dessouky, Farinaz Koushanfar, Ahmad-Reza Sadeghi, Thomas Schneider, Shaza Zeitouni, and Michael Zohner. Pushing the communication barrier in secure computation using lookup tables. In *NDSS 2017*. The Internet Society, February / March 2017.

DPSZ12. Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 643–662. Springer, Heidelberg, August 2012. doi:10.1007/978-3-642-32009-5_38.

Ds17. Jack Doerner and abhi shelat. Scaling ORAM for secure computation. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017*, pages 523–535. ACM Press, October / November 2017. doi:10.1145/3133956.3133967.

EKM17. Andre Esser, Robert Kübler, and Alexander May. LPN decoded. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 486–514. Springer, Heidelberg, August 2017. doi:10.1007/978-3-319-63715-0_17.

GGM86. Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, October 1986.

GI14. Niv Gilboa and Yuval Ishai. Distributed point functions and their applications. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 640–658. Springer, Heidelberg, May 2014. doi:10.1007/978-3-642-55220-5_35.

GKWY19. Chun Guo, Jonathan Katz, Xiao Wang, and Yu Yu. Efficient and secure multiparty computation from fixed-key block ciphers. Cryptology ePrint Archive, Report 2019/074, 2019. https://eprint.iacr.org/2019/074.

GMMM18. Sanjam Garg, Mohammad Mahmoody, Daniel Masny, and Izaak Meckler. On the round complexity of OT extension. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 545–574. Springer, Heidelberg, August 2018. doi:10.1007/978-3-319-96878-0_19.

GMW87. Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th ACM STOC*, pages 218–229. ACM Press, May 1987. doi:10.1145/28395.28420.

Gol04. Oded Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, New York, NY, USA, 2004.

GPS16. Sanjam Garg, Omkant Pandey, and Akshayaram Srinivasan. Revisiting the cryptographic hardness of finding a nash equilibrium. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 579–604. Springer, Heidelberg, August 2016. doi:10.1007/978-3-662-53008-5_20.

HEK12. Yan Huang, David Evans, and Jonathan Katz. Private set intersection: Are garbled circuits better than custom protocols? In *NDSS 2012*. The Internet Society, February 2012.

HOSS18a. Carmit Hazay, Emmanuela Orsini, Peter Scholl, and Eduardo Soria-Vazquez. Concretely efficient large-scale MPC with active security (or, TinyKeys for TinyOT). In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 86–117. Springer, Heidelberg, December 2018. doi:10.1007/978-3-030-03332-3_4.

HOSS18b. Carmit Hazay, Emmanuela Orsini, Peter Scholl, and Eduardo Soria-Vazquez. TinyKeys: A new approach to efficient multi-party computation. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 3–33. Springer, Heidelberg, August 2018. doi:10.1007/978-3-319-96878-0_1.

HSS17. Carmit Hazay, Peter Scholl, and Eduardo Soria-Vazquez. Low cost constant round MPC combining BMR and oblivious transfer. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 598–628. Springer, Heidelberg, December 2017. doi:10.1007/978-3-319-70694-8_21.

IKNP03. Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. Extending oblivious transfers efficiently. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 145–161. Springer, Heidelberg, August 2003. doi:10.1007/978-3-540-45146-4_9.

IKO+11. Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, and Amit Sahai. Efficient non-interactive secure computation. In Kenneth G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 406–425. Springer, Heidelberg, May 2011. doi:10.1007/978-3-642-20465-4_23.

IPS09. Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Secure arithmetic computation with no honest majority. In Omer Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 294–314. Springer, Heidelberg, March 2009. doi:10.1007/978-3-642-00457-5_18.

Kil88. Joe Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 20–31, 1988. URL: https://doi.org/10.1145/62212.62215, doi:10.1145/62212.62215.

KK13. Vladimir Kolesnikov and Ranjit Kumaresan. Improved OT extension for transferring short secrets. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 54–70. Springer, Heidelberg, August 2013. doi:10.1007/978-3-642-40084-1_4.

KOS15. Marcel Keller, Emmanuela Orsini, and Peter Scholl. Actively secure OT extension with optimal overhead. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 724–741. Springer, Heidelberg, August 2015. doi:10.1007/978-3-662-47989-6_35.

KOS16. Marcel Keller, Emmanuela Orsini, and Peter Scholl. MASCOT: Faster malicious arithmetic secure computation with oblivious transfer. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *ACM CCS 2016*, pages 830–842. ACM Press, October 2016. doi:10.1145/2976749.2978357.

KPR18. Marcel Keller, Valerio Pastro, and Dragos Rotaru. Overdrive: Making SPDZ great again. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 158–189. Springer, Heidelberg, April / May 2018. doi:10.1007/978-3-319-78372-7_6.

KPTZ13. Aggelos Kiayias, Stavros Papadopoulos, Nikos Triandopoulos, and Thomas Zacharias. Delegatable pseudorandom functions and applications. In Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors, *ACM CCS 2013*, pages 669–684. ACM Press, November 2013. doi:10.1145/2508859.2516668.

KRRW18. Jonathan Katz, Samuel Ranellucci, Mike Rosulek, and Xiao Wang. Optimizing authenticated garbling for faster secure two-party computation. In *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*, pages 365–391, 2018. URL: https://doi.org/10.1007/978-3-319-96878-0_13, doi:10.1007/978-3-319-96878-0_13.

LJKS+16. Carl Löndahl, Thomas Johansson, Masoumeh Koochak Shooshtari, Mahmoud Ahmadian-Attari, and Mohammad Reza Aref. Squaring attacks on mceliece public-key cryptosystems using quasi-cyclic codes of even dimension. *Des. Codes Cryptography*, 80(2):359–377, August 2016. URL: http://dx.doi.org/10.1007/s10623-015-0099-x, doi:10.1007/s10623-015-0099-x.

LM10. Jin Lu and José MF Moura. Linear time encoding of ldpc codes. *IEEE Transactions on Information Theory*, 56(1):233–249, 2010.

LP19. Zhen Liu and Yanbin Pan. NIST official comment – HQC. NIST Post-Quantum Cryptography Project, 2019. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/HQC-official-comment.pdf.

Lyu05. Vadim 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*, pages 378–389. Springer, 2005.

MBD+18. Carlos Aguilar Melchor, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor. Efficient encryption from random quasi-cyclic codes. *IEEE Trans. Information Theory*, 64(5):3927–3943, 2018. URL: https://doi.org/10.1109/TIT.2018.2804444, doi:10.1109/TIT.2018.2804444.

MM11. Daniele Micciancio and Petros Mol. Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 465–484. Springer, Heidelberg, August 2011. doi:10.1007/978-3-642-22792-9_26.

MR17. Payman Mohassel and Mike Rosulek. Non-interactive secure 2PC in the offline/online and batch settings. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part III*, volume 10212 of *LNCS*, pages 425–455. Springer, Heidelberg, April / May 2017. doi:10.1007/978-3-319-56617-7_15.

NP05. Moni Naor and Benny Pinkas. Computationally secure oblivious transfer. *Journal of Cryptology*, 18(1):1–35, January 2005. doi:10.1007/s00145-004-0102-6.

NP06. Moni Naor and Benny Pinkas. Oblivious polynomial evaluation. *SIAM J. Comput.*, 35(5):1254–1281, 2006.

Pra62. Eugene Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5):5–9, 1962.

PSSZ15. Benny Pinkas, Thomas Schneider, Gil Segev, and Michael Zohner. Phasing: Private set intersection using permutation-based hashing. In Jaeyeon Jung and Thorsten Holz, editors, *USENIX Security 2015*, pages 515–530. USENIX Association, August 2015.

PSTY19. Benny Pinkas, Thomas Schneider, Oleksandr Tkachenko, and Avishay Yanai. Efficient circuit-based psi with linear communication. 2019. https://eprint.iacr.org/2019/241.

PVW08. Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 554–571. Springer, Heidelberg, August 2008. doi:10.1007/978-3-540-85174-5_31.

Sen11. Nicolas Sendrier. Decoding one out of many. In Bo-Yin Yang, editor, *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011*, pages 51–67. Springer, Heidelberg, November / December 2011. doi:10.1007/978-3-642-25405-5_4.

SGRR19. Phillipp Schoppmann, Adrià Gascón, Leonie Reichert, and Mariana Raykova. Distributed vector-ole: Improved constructions and implementation. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019. https://eprint.iacr.org/2019/1084.

TS16. Rodolfo Canto Torres and Nicolas Sendrier. Analysis of information set decoding for a sub-linear error weight. In Tsuyoshi Takagi, editor, *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016*, pages 144–161. Springer, Heidelberg, 2016. doi:10.1007/978-3-319-29360-8_10.

WRK17a. Xiao Wang, Samuel Ranellucci, and Jonathan Katz. Authenticated garbling and efficient maliciously secure two-party computation. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017*, pages 21–37. ACM Press, October / November 2017. doi:10.1145/3133956.3134053.

WRK17b. Xiao Wang, Samuel Ranellucci, and Jonathan Katz. Global-scale secure multiparty computation. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017*, pages 39–56. ACM Press, October / November 2017. doi:10.1145/3133956.3133979.

Zic17. Lior Zichron. Locally computable arithmetic pseudorandom generators. Master's thesis, School of Electrical Engineering, Tel Aviv University, 2017. URL: http://www.eng.tau.ac.il/~bennyap/pubs/Zichron.pdf.

A Details on Implementation

A.1 Detailed Performance Figures

In this section, we provide more extensive numbers regarding the running time and communication complexity of our implementation, with alternative choices of parameters (security parameter λ, scaling parameter N/n, method for computing the base OTs). Table 4 contains the running time of our protocol. Table 5 contains the communication overhead of our protocol.

B An Improved PPRF for G_{sVOLE}

We describe in this section an improved (yet still relatively simple) puncturing strategy for constructing a t-puncturable PRF from the GGM PRF. This construction is somewhat folklore; it was explicitely presented in [BCG+19]. Unlike the simple construction presented in Section 4, however, this construction is not compatible with our distributed generation protocol. Still, it is useful in setting where computation is not an issue (hence a more costly distributed generation protocol can be used) but long-term storage is (hence it is important to reduce the size of the PCG keys), or in settings where a trusted dealer is available to distribute the PCG keys (like in the commodity-based model of Beaver [Bea95]).

					LAN (10Gbps) times				WAN (100Mbps) times				WAN (10Mbps) times			
					n				n				n			
Protocol	Base type	λ	s	τ	10^7	10^6	10^5	10^4	10^7	10^6	10^5	10^4	10^7	10^6	10^5	10^4
This	base	80	4	4	4,507	548	301	227	4,721	780	487	403	4,662	815	543	463
(SH)	hybrid	80	4	4	4,261	344	118	65	4,598	616	366	337	4,517	600	375	346
	base	128	4	4	4,861	766	421	357	4,932	938	616	539	5,018	929	646	516
	hybrid	128	4	4	4,233	276	85	90	4,595	551	391	337	4,615	552	408	352
	base	128	2	4	3,373	975	634	528	3,675	1,221	875	687	3,603	1,188	851	747
	hybrid	128	2	4	2,441	208	**76**	**67**	**2,726**	**513**	**422**	**425**	**2,756**	**518**	**454**	**422**
IKNP	base	128	-	4	**268**	**125**	94	91	13,728	1,850	493	459	128,954	13,332	1,756	445
This	base	80	4	1	14,127	1,204	479	305	14,467	1,408	682	505	14,385	1,416	716	534
(SH)	hybrid	80	4	1	13,772	812	164	102	13,987	1,067	406	344	13,962	1,060	407	353
	base	128	4	1	14,701	1,445	678	480	15,079	1,642	886	681	14,994	1,649	885	685
	hybrid	128	4	1	13,996	787	163	101	14,344	1,061	474	346	14,156	1,056	471	361
	base	128	2	1	9,414	1,747	1,008	761	9,694	1,973	1,220	964	9,750	1,980	1,226	980
	hybrid	128	2	1	7,990	533	130	100	**8,252**	**808**	**451**	422	**8,291**	**815**	**467**	**422**
IKNP	base	128	-	1	**573**	**157**	**108**	**98**	15,622	2,030	613	**341**	129,011	13,285	1,672	429
This	base	128	4	4	5286	879	463	358	5589	1127	787	670	5624	1123	801	670
(Mal)	hybrid	128	4	4	5030	344	116	69	5141	622	387	339	5292	699	372	354
	base	128	2	4	3674	1018	643	528	3897	1252	891	726	3836	1217	858	777
	hybrid	128	2	4	2659	280	**84**	**78**	**2872**	**479**	**457**	**424**	**2846**	**515**	**438**	**422**
KOS	base	128	-	4	**333**	**121**	110	111	13722	1933	589	426	129052	13391	1804	536
This	base	128	4	1	16096	1632	707	490	16499	1947	1033	811	16616	1958	1045	813
(Mal)	hybrid	128	4	1	15656	968	185	110	15999	1205	489	426	15889	1207	490	426
	base	128	2	1	10475	1833	1028	773	10585	2026	1278	1051	10449	2033	1286	1048
	hybrid	128	2	1	8765	584	141	**104**	**9055**	**828**	**460**	**423**	**8929**	**831**	**467**	**433**
KOS	base	128	-	1	**674**	**170**	**113**	106	15741	2088	702	433	129771	13389	1772	518

Table 4. The running time in milliseconds of our implementation compared to [ALSZ13] in both the LAN (0ms latency) and WAN (40ms one-way latency) settings. λ is the computational security parameter. $s = N/n$ denotes the compression parameter such that the PPRF output strings are of length N. τ denotes the number of threads. Hybrid refers to doing 128 base OTs followed by IKNP to derive the total required base OTs.

				Total Comm. (bytes)				Comm./OT (bits)			
				n				n			
Protocol	Base type	λ	s	10^7	10^6	10^5	10^4	10^7	10^6	10^5	10^4
This	base	80	4	53,478	45,678	37,878	27,478	0.043	0.365	3.030	21.982
(SH/Mal)	hybrid	80	4	**47,690**	**43,850**	**40,010**	**34,890**	**0.038**	**0.351**	**3.201**	**27.912**
	base	128	4	85,482	68,842	56,362	43,882	0.068	0.551	4.509	35.106
	hybrid	128	4	**80,238**	**55,662**	**49,518**	**43,374**	**0.064**	**0.445**	**3.961**	**34.699**
	base	80	2	91,470	72,750	58,710	44,418	0.073	0.582	4.697	35.534
	hybrid	80	2	83,322	74,106	50,810	43,910	0.067	0.593	4.065	35.128
	base	128	2	144,558	121,158	89,958	70,986	0.116	0.969	7.197	56.789
	hybrid	128	2	126,658	98,754	83,394	57,806	0.101	0.790	6.672	46.245
IKNP/KOS	base	128	-	160,056,360	16,011,518	1,655,784	168,186	128.045	128.092	132.463	134.549

Table 5. The communication overhead of our implementation compared to [ALSZ13]. λ stands for the computational security parameter. See Figure 2.

Intuitively, to obtain a t-puncturable PRF out of the GGM PRF, it suffices to define a key punctured at a subset S of leaves to be the smallest set of intermediate PRG values that allows to reconstruct all leaf values indexed by $[n] \setminus S$, and does not allow to reconstruct the leaf values indexed by S. We represent on Figure 18 a labelling algorithm which finds the indices of such a subset of the keys. The correctness of the algorithm follows easily by inspection; with a little more effort, one can also show that this algorithm is optimal (i.e., it produces the smallest possible punctured key satisfying the constraints). The worst-case scenario is easily seen to happen when all the punctured leaves are regularly spaces, with a distance of n/t between every two punctured leaves. This observation allows to upper bound the length of a key punctured at t points by $t\lambda \log(n/t)$, improving over the cost $t\lambda \log n$ of the naive approach.

Algorithm **Puncture-Label**

Input. A complete binary tree T with n leaves (indexed by $[n]$), and a size-t subset S of $[n]$. We denote by $s_1 < s_2 < \cdots < s_t$ the indices of the leaves in S.
Output. A labelling L_t of all nodes of T, such that all nodes of $[n] \setminus S$, and only them, belong to a subtree of T whose root belongs to L_t.
Procedure. The labelling proceeds in t steps. Given a leave x and a subtree T' of T which contains x, we denote by $\mathsf{Label}(x, T')$ the procedure which outputs all nodes of T' which have their parent node in P but are not in P themselves, where P denotes the path from the root of T' to x.

- In step 1, set $L_1 \leftarrow \mathsf{Label}(s_1, T)$.
- In step $i+1$, let T_{i+1} denote the smallest subtree of T which contains s_{i+1} and whose root belongs to L_i (T_{i+1} exists by construction), and let r_{i+1} denote its root. Set $L_{i+1} \leftarrow (L_i \setminus \{r_{i+1}\}) \cup \{\mathsf{Label}(s_{i+1}, T_{i+1})\}$.

After all steps are completed, output L_t.

Fig. 18. Labelling algorithm to compute the indices of a subset of keys in the GGM PRF construction which allows to reconstruct the output of the GGM PRF at all points except exactly t.

C Details for Maliciously Secure Constructions

C.1 GGM Instantiation of Punctured PRF with Malicious Keys

We use the GGM puncturable PRF with domain $[2N]$ and range $(\mathbb{F}_{p^r})^2 \times \{0,1\}^\lambda$. The underlying PRG of the first ℓ levels we denote by $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$. The PRG of the last level we denote by $G' : \{0,1\}^\lambda \to (\mathbb{F}_{p^r})^2 \times \{0,1\}^\lambda$. In the following by $\mathsf{PPRF}_{\mathsf{GGM}} = (\mathsf{PPRF}_{\mathsf{GGM}}.\mathsf{Puncture}, \mathsf{PPRF}_{\mathsf{GGM}}.\mathsf{Eval}, \mathsf{PPRF}_{\mathsf{GGM}}.\mathsf{PuncEval})$ we denote the standard GGM PPRF algorithms. By $\mathsf{PPRF}_{\mathsf{GGM}}.\mathsf{FullEval}(\mathsf{k}^*_{\mathsf{pprf}})$ we denote the algorithm that on input of a $\mathsf{k}^*_{\mathsf{pprf}}$ punctured at $\alpha \in [2N]$ evaluates the PRF on all values except α and returns the output values $\{s_j\}_{j \in [2N] \setminus \{\alpha\}}$.

In the following we explain how the GGM construction allows verification of malicious PPRF keys. We set the malicious key space to $\mathcal{K} = \{0,1\}^{2\lambda\ell} \times ((\mathbb{F}_{p^r})^2 \times \{0,1\}^\lambda)$. We restrict the puncturing algorithm $\mathsf{Puncture}^*$ to even inputs $\alpha \| 0 \in [2N]$, as these will later correspond to the actual output values. Note that the key $K_0^{\ell+1} \in \mathbb{F}_{p^r}^2$ takes a special role. Namely, with this key we capture a programmibility at the punctured point when it would be undefined otherwise: If $I = \{\alpha\}$ consists only of a single point, then the output value at this point α is set to be $K_0^{\ell+1}$ by Eval^* (if $|I| > 1$ this value is ignored).

Ver: On input $K = \{(K_0^i, K_1^i)_{i=1}^{\ell+1}\}$ and $I \subseteq [N]$, compute $\mathsf{k}^*_\alpha \leftarrow \mathsf{Puncture}^*(K, \alpha)$ for all $\alpha \in I$.
Return 1, if and only if for all $\alpha, \alpha' \in I, x \in [2N] \setminus \{\alpha \| 0, \alpha' \| 0\}$ it holds:

$$\mathsf{PPRF}_{\mathsf{GGM}}.\mathsf{PuncEval}(\mathsf{k}^*_\alpha, x) = \mathsf{PPRF}_{\mathsf{GGM}}.\mathsf{PuncEval}(\mathsf{k}^*_{\alpha'}, x).$$

$\mathsf{Puncture}^*$**:** On input $\{(K_0^i, K_1^i)_{i=1}^{\ell+1}\}$ and $\alpha \in [N]$, we set $\alpha_{\ell+1} = 0$ and proceed as follows: Let $\alpha_i^* = \alpha_1 \cdots \alpha_{i-1}\overline{\alpha_i}$ for all $i \in \{1, \ldots, \ell+1\}$.

1. Define $s^1_{\alpha_1^*} = K^1_{\overline{\alpha_1}}$.
2. For $i \in \{2, \ldots, \ell\}$:
   (a) Compute $(s^i_{2j}, s^i_{2j+1}) = G(s^{i-1}_j)$, for $j \in [0, \ldots, 2^{i-1}), j \neq \alpha_1 \cdots \alpha_{i-1}$ and $(s^{\ell+1}_{2j}, s^{\ell+1}_{2j+1}) = G'(s^\ell_j)$ for $j \in [N], j \neq \alpha$.
   (b) For $i \in \{1, \ldots, \ell+1\}$ compute:

$$s^i_{\alpha_i^\star} = K^i_{\overline{\alpha_i}} \oplus \bigoplus_{\substack{j \in [0,2^{i-1}),\\ j \neq \alpha_i^*}} s^i_{2j+\overline{\alpha_i}} \in \{0,1\}^\lambda.$$

3. Output the punctured key $\mathsf{k}^*_{\mathsf{pprf}} = \{s^i_{\alpha_i^\star}\}_{i=1}^{\ell+1}$.

For better readablity, we overload notation and denote by $\mathsf{Puncture}^*$ also the procedure taking only the required keys $\{K^i_{\overline{\alpha_i}}\}_{i=1}^{\ell+1}$ as input.

Eval^***:** On input $K = \{(K_0^i, K_1^i)_{i=1}^{\ell+1}\}$,$I$ and $x \in [2N]$ proceed as follows:

1. If $\mathsf{Ver}(K, I) = 0$, return $\perp$.
2. If $\hat{I} = \{\alpha \| 0 : \alpha \in I\}$ consists of the single point x return $K_0^{\ell+1} \in \mathbb{F}_{p^r}^2$
3. Else, compute $\mathsf{k}^* \leftarrow \mathsf{Puncture}^*(K, \alpha)$ for some $\alpha\|0 \in \hat{I}\backslash\{x\}$ and return $(\omega, w) \leftarrow \mathsf{PPRF}_{\mathsf{GGM}}.\mathsf{PuncEval}(\mathsf{k}^*, x)$.

Again, we overload notation and for $\alpha \in [N]$ denote by $\mathsf{Eval}^*(K, I, \alpha)$ also the algorithm that calls $\mathsf{Eval}^*(K, I, x)$ for $x = \alpha\|0 \in [2N]$.

It is left to show that the algorithms indeed allow verification of malicious keys. Note that if $\mathsf{Ver}(K^*, I) = 1$, then for all $\alpha \in I, x \in [2N]\backslash\{\alpha\|0\}$ we have:

$$\mathsf{Eval}^*(K^*, I, x) = \mathsf{PPRF}_{\mathsf{GGM}}.\mathsf{PuncEval}(\mathsf{k}^*, x),$$

where $\mathsf{k}^* \leftarrow \mathsf{Puncture}^*(K^*, \alpha)$. By step (3) in the verification procedure, we have that this value is independent of the choice of α. This yields the required.

C.2 Malicious Setup for Single-Point PPRF

Formally, we define the PPRF PPRF_1 with domain $[N]$ and range $(\mathbb{F}_{p^r})^2$ as follows: Let $\mathsf{PPRF}_1 = (\mathsf{PPRF}_1.\mathsf{Puncture}, \mathsf{PPRF}_1.\mathsf{Eval})$, such that:

$\mathsf{PPRF}_1.\mathsf{Puncture}$**:** On input $\mathsf{k}_{\mathsf{pprf}} \in \{0,1\}^\lambda$, $\alpha \in [N]$, return $\mathsf{k}^*_{\mathsf{pprf}} \leftarrow \mathsf{PPRF}_{\mathsf{GGM}}.\mathsf{Puncture}(\mathsf{k}_{\mathsf{pprf}}, \alpha\|0)$.
$\mathsf{PPRF}_1.\mathsf{Eval}$**:** On input $\mathsf{k}_{\mathsf{pprf}} \in \{0,1\}^\lambda$ and $\alpha \in [N]$, return $(\omega, w) \leftarrow \mathsf{PPRF}_{\mathsf{GGM}}.\mathsf{Eval}(\mathsf{k}_{\mathsf{pprf}}, \alpha\|0)$.

We give the protocol for distributed setup of PPRF_1 with security against malicious adversaries in Figure 13.

Note that steps (1) to (6) correspond to the protocol in the semi-honest case with an additional level of PRG evaluation, where for the last level always the sum of the right leaves are given to the receiver. This will allow the receiver to check the hash value computed by the sender in step (7).

Theorem 15. *Assuming a black-box access to a PRG $G : \{0,1\}^\lambda \mapsto \{0,1\}^{2\lambda}$, a right-half injective PRG $G' : \{0,1\}^\lambda \mapsto (\mathbb{F}_{p^r})^2 \times \{0,1\}^\lambda$, and a collision resistant hash function $h\colon \{0,1\}^{\lambda N} \to \{0,1\}^\lambda$, there exists a 2-party protocol implementing $\mathcal{F}_{\mathsf{mal\text{-}PPRF}}$ (see Fig. 12) for the puncturable PRF PPRF_1, with malicious security in the parallel OT-hybrid model, and the following efficiency features. The interaction consists of ℓ* parallel *calls to $\mathcal{F}_{\mathsf{OT}}$, and uses additional communication of $r \log p + \lambda$. The computational complexity is dominated by $O(2^\ell)$ calls each to G and G'.*

Proof. When neither party is corrupted, the receiver R will indeed compute the correct punctured key $\mathsf{k}^*_{\mathsf{pprf}}$ and output value w in a protocol execution (the proof is similar to the semi-honest case and will be shown in more detail in the paragraph for security against malicious receiver.) Further, as the tree is punctured at an even value $\alpha\|0$, both parties hold the same values $\gamma_0, \ldots, \gamma_{N-1}$ for all odd leaves. Therefore, $\Gamma = \Gamma'$ in step (6d) of the protocol execution.

Security against malicious receiver. On input α, the simulator forwards α to the functionality. On output $\mathsf{k}^*_{\mathsf{pprf}} = \{k_i\}_{i=1}^{\ell+1}$ and w, the simulator proceeds as follows:

- For $i \in \{1, \ldots, \ell\}$ define $s^i_{\alpha_1,\ldots,\alpha_{i-1}\overline{\alpha_i}} = k_i$ and $s^{\ell+1}_{\alpha\|1} = k_{\ell+1}$. Set $K^1_{\overline{\alpha_1}} = s^1_{\overline{\alpha_1}}$.
- For $i \in \{2, \ldots, \ell\}$: Compute $(s^i_{2j}, s^i_{2j+1}) = G(s^{i-1}_j)$, for $j \in [0, \ldots, 2^{i-1}), j \neq \alpha_1, \ldots, \alpha_{i-1}$.
- Compute $(s^{\ell+1}_{2j}, s^{\ell+1}_{2j+1}) = G'(s^\ell_j)$, for $j \in [0, \ldots, 2^\ell), j \neq \alpha\|0$.
- For $i \in \{1 \ldots, \ell+1\}$: Compute

$$K^i_{\overline{\alpha_i}} = \bigoplus_{j \in [0,2^{i-1})} s^i_{2j+\overline{\alpha_i}},$$

  where we set $\alpha_{\ell+1} = 0$.
- Compute

$$c = w - \sum_{j \in [N]\setminus\{\alpha\}} s^{\ell+1}_{2j}.$$

- Set $\gamma_j = s^{\ell+1}_{2j+1}$ for $j \in [N]$, and compute $\Gamma = h(\gamma_0, \ldots, \gamma_{N-1})$.

Finally, the simulator forwards $\{K^i_{\overline{\alpha_i}}\}_{i=1}^{\ell}$ (where the i-th key corresponds to the i-th OT message), $K^{\ell+1}_1$, c and Γ to the receiver.

Note that the values $\{K^i_{\overline{\alpha_i}}\}_{i=1}^{\ell+1}$ and Γ correspond to the values computed by the sender in a real protocol execution. We have to show that the key $\mathsf{k}'^*_{\mathsf{pprf}} = \{s'_{\alpha^*_i}\}_{i=1}^{\ell+1} \leftarrow \mathsf{Puncture}^*(\{K^i\}_{i=1}^{\ell+1}, \alpha)$ computed by the receiver in a protocol execution corresponds to the key $\mathsf{k}^*_{\mathsf{pprf}} = \{k_i\}_{i=1}^{\ell+1}$ returned by the functionality. We have:

- $s'^1_{\alpha^\star_1} = K^1_{\overline{\alpha_1}} = k_1$.
- Assume that we have $s'^{i-1}_j = s^{i-1}_j$ for all $j \in [0, \ldots, 2^{i-1}), j \neq \alpha_1, \ldots, \alpha_{i-1}$ for some i. Then we have the same for level i, as this is true for all values off the path, and further because of

$$s'^i_{\alpha^*_i} = K^i_{\overline{\alpha_i}} \oplus \bigoplus_{\substack{j \in [0,2^{i-1}),\\ j \neq \alpha^*_i}} s^i_{2j+\overline{\alpha_i}} = s^i_{\alpha^*_i}.$$

  As $s^i_{\alpha^*_i} = k_i$ for all $i \in \{1, \ldots, \ell_1\}$, the keys agree as required.

  Further, it holds

$$\begin{aligned} c &= w - \sum_{j \in [N]\setminus\{\alpha\}} s^{\ell+1}_{2j} = -s^{\ell+1}_{\alpha\|0} + \beta - \sum_{j \in [N]\setminus\{\alpha\}} s^{\ell+1}_{2j} \\ &= \beta - \sum_{j \in [N]} s^{\ell+1}_{2j}, \end{aligned}$$

where $s^{\ell+1}_{\alpha\|0} \leftarrow \mathsf{PPRF}_{\mathsf{GGM}}.\mathsf{Eval}(\mathsf{k}_{\mathsf{pprf}}, \alpha\|0)$ (for the key $\mathsf{k}_{\mathsf{pprf}} \in \{0,1\}^\lambda$ corresponding to $\mathsf{k}^*_{\mathsf{pprf}}$).

Security against malicious sender. On input of the OT messages $K = \{(K^i_0, K^i_1)_{i=1}^{\ell}\}$, key $K^{\ell+1}_1$, correction value c and a hash value Γ, the simulator proceeds as follows: First, the simulator computes Γ_α for each $\alpha \in [N]$ as follows:

1. Compute $\mathsf{k}^*_{\mathsf{pprf}} \leftarrow \mathsf{Puncture}^*(\{K^i_{\overline{\alpha_i}}\}_{i=1}^{\ell+1}, \alpha)$.
2. Compute $\{s_j(\alpha)\}_{j \in [2N]\setminus\{\alpha\|0\}} \leftarrow \mathsf{PPRF.FullEval}(\mathsf{k}^*_{\mathsf{pprf}}, \alpha\|0)$.

3. Compute
$$w = c - \sum_{j \in [N] \setminus \{\alpha\}} s_{2j}(\alpha)$$
4. Set $\gamma_j(\alpha) = s_{2j+1}(\alpha)$ for $j \in [N]$, and compute $\Gamma'_\alpha = h(\gamma_0(\alpha), \ldots, \gamma_{N-1}(\alpha))$.

Note that this is exactly how an honest receiver, on input α, would proceed. If the sender behaved honestly, we should have $\Gamma_1 = \Gamma_2 \cdots = \Gamma_N = \Gamma$.

Let $I \subset [n]$ be the set of α's consistent with Γ, that is
$$I = \{\alpha \in [n] \mid \Gamma_\alpha = \Gamma\}$$

If $I = \emptyset$ then abort. We extract the sender's input β as follows:

- Pick an $\alpha \in I$.
- For all $j \in [2N] \backslash \alpha \| 0$, define $s_j = s_j(\alpha)$.
- If $|I| = 1$, set $s_{\alpha\|0} = 0$.
- Otherwise, pick $\alpha' \in I$ (with $\alpha' \neq \alpha$), define $s_{\alpha\|0} = s_{\alpha\|0}(\alpha')$.
- Set
$$\beta = -s_{\alpha\|0} + w.$$
- Input $\beta, K^* = \{K, (0, K_1^{\ell+1})\}\}, I$ to the functionality.

We have $\mathsf{Ver}(K, I) = 1$ because of the following.

Claim. Except with negligible probability, all choices of $\alpha, \alpha' \in I$ in the above procedure lead to the same vector $\boldsymbol{s} = (s_0, \ldots, s_{N-1})$.

Proof. The case $|I| = 1$ is trivial. For $|I| > 1$, it suffices to show that for all $\alpha, \alpha' \in I$ and $j \in [2N] \setminus \{\alpha\|0, \alpha\|0'\}$, $s_j(\alpha) = s_j(\alpha')$. Suppose for a contradiction that this does not hold, so there exist $j \in [2N], \alpha, \alpha' \in [N]$ such that $s_j(\alpha) \neq s_j(\alpha')$. From the fact that $\Gamma_\alpha = \Gamma_{\alpha'}$ and the collision-resistance of h, we have $\gamma_i(\alpha) = \gamma_i(\alpha')$ for all $i \in [N]$, except with negligible probability. Recall that for each $(s_{2i}(\alpha), s_{2i+1}(\alpha)), (s_{2i}(\alpha'), s_{2i+1}(\alpha'))$, where $i \notin \{\alpha, \alpha'\}$, we have $(s_{2i}(\alpha), s_{2i+1}(\alpha)) = G'(\rho)$ and $(s_{2i}(\alpha'), s_{2i+1}(\alpha')) = G'(\rho')$, for some ρ, ρ'. From the right-half injectivity of G', we have that, if $s_{2i+1}(\alpha) = \gamma_i = \gamma'_i = s_{2i+1}(\alpha')$ then it must hold that $\rho = \rho'$. Hence, we must have $s_j(\alpha) = s_j(\alpha')$ for all $j \in [2N] \setminus \{\alpha\|0, \alpha\|0'\}$, which completes the claim.

Note that the punctured key returned by the functionality equals the key computed in the real protocol execution. Next, we show that the correction value w corresponds to the one computed in the real protocol execution. For $|I| = 1$ this follows, as $\mathsf{Eval}^*(K^*, I, \alpha) = 0$. For $|I| > 1$, this follows as for all $\alpha \in I, x \in I \backslash \{\alpha\}$, $\mathsf{k}^*_{\mathsf{pprf}} \leftarrow \mathsf{Puncture}^*(K, x)$, it holds $\mathsf{PPRF.Eval}(\mathsf{k}^*_{\mathsf{pprf}}, \alpha\|0) = s_{\alpha\|0}$ and thus $-\mathsf{PPRF.Eval}(\mathsf{k}_{\mathsf{pprf}}, \alpha\|0) + \beta = -s_{\alpha\|0} + \beta = w$ as required.

In the real execution the receiver aborts, if $\Gamma' \neq \Gamma$. By previous considerations this is equivalent to $\alpha \in I$. It follows that the functionality aborts if and only if the real protocol execution would have aborted.

C.3 Malicious Setup of t PPRFs with Consistent Offset

Theorem 16. *There exists a 4-message 2-party protocol $\Pi_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$ which securely implements the functionality $\mathcal{F}_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}(1^\lambda, N, p, r)$ for the puncturable PRF PPRF in the $\mathcal{F}_{\mathsf{g\text{-}rev\text{-}VOLE}^-}$, parallel $\mathcal{F}_{\mathsf{mal}\text{-}\mathsf{PPRF}}$-hybrid model, with malicious security, using t parallel calls to $\mathcal{F}_{\mathsf{mal}\text{-}\mathsf{PPRF}}$, and only one call to $\mathcal{F}_{\mathsf{g\text{-}rev\text{-}VOLE}}$, and further communication of $(N + t + 2)r \log p$ bits. Furthermore, when $p = 2$, the functionality can be implemented in the parallel $\mathcal{F}_{\mathsf{mal}\text{-}\mathsf{PPRF}}$-hybrid model, using no call to $\mathcal{F}_{\mathsf{g\text{-}rev\text{-}VOLE}}$.*

Proof. If both parties are honest, after execution of the protocol, R and S hold values $\boldsymbol{v}_R^j = (v_{R,0}^j, v_{R,2}^j, \ldots, v_{R,2N-2}^j)$, $\boldsymbol{v}_R'^j = (v_{R,1}^j, v_{R,3}^j, \ldots, v_{R,2N-1}^j)$ and $\boldsymbol{v}_S^j = (v_{S,0}^j, v_{S,2}^j, \ldots, v_{S,2N-2}^j)$, $\boldsymbol{v}_S'^j = (v_{S,1}^j, v_{S,3}^j, \ldots, v_{S,2N-1}^j)$, such that

$$\boldsymbol{v}_R^j + \boldsymbol{v}_S^j = (\beta_j + \gamma_j)\boldsymbol{e}_{\alpha_j} = \chi \cdot y_j \cdot \boldsymbol{e}_{\alpha_j} \text{ and } \boldsymbol{v}_R'^j + \boldsymbol{v}_S'^j = x \cdot y_j \cdot \boldsymbol{e}_{\alpha_j},$$

and thus $(\boldsymbol{v}_R^j + \tau \cdot \boldsymbol{v}_R'^j) + (\boldsymbol{v}_S^j + \tau \cdot \boldsymbol{v}_S'^j) = X \cdot y_j \cdot \boldsymbol{e}_{\alpha_j}$, where $X = \chi + \tau \cdot x$. Computing the scalar product with $(\tau_0, \ldots, \tau_{N-1})$ on both sides of the equation yields the required.

Security against malicious receiver: Receive from $\mathcal{A}$ input $y = (y_1, \ldots, y_t) \in \mathbb{F}_p$ to $\mathcal{F}_{\mathsf{rev\text{-}VOLE}}$ and (not necessarily distinct) inputs $\alpha_1, \ldots, \alpha_t \in [N]$ to $\mathcal{F}_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$. For $j \in [t]$ we define $\boldsymbol{e}_{\alpha_j}$ to be the α_j-th unit vector, and $\boldsymbol{u} = \sum_{i=1}^t y_j \boldsymbol{e}_j$. The simulator forwards $\alpha_1, \ldots, \alpha_t$ and $y_1, \ldots, y_t$ to $\mathcal{F}_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$, and for each $j \in \{1, \ldots, t\}$ forwards k_j^* and z_j to $\mathcal{A}$ for each $j \in \{1, \ldots, t\}$. On inputs $\tau, \tau_0, \ldots, \tau_{N-1}$ of $\mathcal{A}$, the simulator draws $X \xleftarrow{\$} \mathbb{F}_{p^r}$, computes for $i \in [N], j \in \{1, \ldots, t\}$:

$$(v_{R,2i}^j, v_{R,2i+1}^j) \leftarrow \mathsf{PPRF.Eval}'(\mathsf{k}_j^*, i)$$

and sends X and $V_{S,j} = X \cdot \tau_{\alpha_j} \cdot y_j - \sum_{i=0}^{N-1} \tau_i \cdot (v_{R,2i}^j + \tau \cdot v_{R,2i+1}^j)$ to $\mathcal{A}$. It is left to show that this is indistinguishable from a real protocol execution. Let x be the input of the sender to the functionality. We set $\chi = X - \tau \cdot x$. For $j \in \{1, \ldots, t\}$ we have $\gamma_j + \beta_j = \chi \cdot y_j$, $c_j + b_j = x \cdot y_j$, and $(\omega_j, w_j) = -\mathsf{PPRF.Eval}(\mathsf{k}_j, \alpha_j) + (\beta_j, b_j)$ (since S is honest). Thus, we have

$$(\omega_j, w_j) + (\gamma_j, c_j) = -\mathsf{PPRF.Eval}(\mathsf{k}_j, \alpha_j) + (x \cdot y_j, \chi \cdot y_j).$$

For $\mathsf{PPRF.Eval}'$ (as defined in Figure 16) for all $i \in [N]$ this yields

$$\mathsf{PPRF.Eval}'(\mathsf{k}_j^*, i) = -\mathsf{PPRF.Eval}(\mathsf{k}_j, i) + (x \cdot y_j, \chi \cdot y_j) \cdot \Delta_{i,\alpha_j},$$

where $\Delta_{i,\alpha_j} = 1$ iff $i = \alpha_j$. Let $(v_{S,2i}^j, v_{S,2i+1}^j) \leftarrow \mathsf{PPRF.Eval}(\mathsf{k}_j, i)$ for $j \in \{1, \ldots, t\}, i \in [N]$. Then, for $i \in [N], j \in \{1, \ldots, t\}$ we have $(v_{R,2i}^j, v_{R,2i+1}^j) = -(v_{S,2i}^j, v_{S,2i+1}^j) + (x \cdot y_j, \chi \cdot y_j) \cdot \Delta_{i,\alpha_j}$. This yields the required, as for each $j \in \{1, \ldots, t\}$ we have $\sum_{i=0}^{N-1} \tau_i \cdot y_j \cdot \Delta_{i,\alpha_j} = \tau_{\alpha_j} \cdot y_j$.

Security against malicious sender: On input $((\boldsymbol{\beta}, \chi), (\boldsymbol{b}, x))$ to the functionality $\mathcal{F}_{\mathsf{g\text{-}rev\text{-}VOLE}}$ and $(\hat{\beta}_j, \hat{b}_j), I_j, K_j^*$ to $\mathcal{F}_{\mathsf{mal\text{-}PPRF}}$ by $\mathcal{A}$, the simulator draws challenges $\tau, \tau_0, \ldots, \tau_{N-1} \leftarrow \mathbb{F}_{p^r}$ uniformly at random, and forwards all to $\mathcal{A}$. On input X and $V_{S,1}, \ldots, V_{S,t}$ by $\mathcal{A}$, the simulator proceeds as follows:

1. Set $\delta_j = \hat{\beta}_j - \beta_j$, $d_j = \hat{b}_j - b$ for $j \in \{1, \ldots, t\}$. If there exists a $j \in \{1, \ldots, t\}$ with $d_j \neq 0$, but $\delta_j - \tau \cdot d_j = 0$, abort.
2. For $i \in [N], j \in \{1, \ldots, t\}$: Compute

   $$(v_{S,2i}^j, v_{S,2i+1}^j) \leftarrow \mathsf{Eval}^*(K_i^*, I, i)$$

   and $\hat{V}_{S,j} = \sum_{i=0}^{N-1} \tau_i \cdot (v_{S,2i}^j + \tau \cdot v_{S,2i+1}^j)$. For each $j \in \{1, \ldots, t\}$ with $d_j \neq 0$ find α_j^*, such that

   $$\hat{V}_{S,j} - V_{S,j} = \tau_{\alpha_j^*} \cdot (\delta_j - \tau \cdot d_j), \tag{2}$$

   where $\tau_{\alpha_j^*}$ corresponds to the α_j^*-th coefficient chosen by the simulator. If such an α_j^* does not exist or is not unique, abort.
3. For $j \in \{1, \ldots, t\}$ set

   $$\hat{I}_j = \begin{cases} I_j \cap \{\alpha_j^*\} & \text{if } d_j \neq 0, \\ I_j & \text{else} \end{cases}.$$

4. Parse $K_j^* = \{(K_{j,0}, K_{j,1})_{i=1}^{\ell+1}\}$. Set

$$\hat{K}_{j,0}^{\ell+1} = \begin{cases} K_{j,0}^{\ell+1} - (\delta_j, d_j) & \text{if } d_j \neq 0, \\ K_{j,0}^{\ell+1} & \text{else} \end{cases}.$$

   Define $\hat{K}_j^\star = \{(K_{j,0}^i, K_{j,1}^i)_{i=1}^{\ell}\} \cup \{(\hat{K}_{j,0}^{\ell+1}, K_{j,1}^{\ell+1})\}$.
5. Input x, $\hat{I}_1, \ldots, \hat{I}_t$ and $\hat{K}_1^*, \ldots, \hat{K}_t^*$ to the functionality $\mathcal{F}_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$. If the functionality does not reply *success*, abort.

We have to show that the probability of the simulation aborting is negligibly close to the probability that the receiver would have aborted in a real execution.

As τ is chosen at random from $\mathbb{F}_{p^r}$ by the simulator, by a union bound over $j \in \{1, \ldots, t\}$, the probability that there exists a $j \in \{1, \ldots, t\}$ with $\delta_j \neq 0$ and $\delta_j - \tau \cdot d_j = 0$ is upper bounded by t/p^r.

Next, we show that passing the verification check, corresponds to guessing the input α_j of the receiver for all j with $d_j \neq 0$.

For $j \in \{1, \ldots, t\}$ it holds $(\omega_j, w_j) = -\mathsf{PPRF.Eval}^*(K_j^*, I_j, \alpha_j) + (\beta_j, b_j) + (\delta_j, d_j)$. Therefore, for the value $v_R^j \in [2N]$ computed by an honest receiver during the real protocol execution, we have

$$(v_{R,2i}^j, v_{R,2i+1}^j) = -\mathsf{PPRF.Eval}(\mathsf{k}_j, i) + ((x, \chi) \cdot y_j + (\delta_j, d_j)) \cdot \Delta_{i,\alpha_j},$$

for all $i \in [N], j \in \{1, \ldots, t\}$. As we have $\sum_{i=1}^N \tau_j(\delta_j + \tau \cdot d_j)\Delta_{i,\alpha_j} = \tau_{\alpha_j}\delta_j + \tau \cdot d_j$, we see that the sender passes the check in the real execution of the protocol, if and only if he provides $V_{S_1}, \ldots, V_{S_t}$, such that $V_{S,j} = \hat{V}_{S,j} - \tau_{\alpha_j} \cdot (\delta_j - \tau \cdot d_j)$ for all $j \in \{1, \ldots, t\}$ with $d_j \neq 0$. Thus, if the sender guessed α_j^* such that $\alpha_j = \alpha_j^*$ for all such j, then the real execution check would have passed. On the other hand, if Equation 2 does not have a solution, the sender would have failed the real world check independent of the choices $\alpha_1, \ldots, \alpha_t$ of the receiver. The coefficients $\tau_0, \ldots, \tau_{N-1}$ provided by the simulator are distinct except with probability at most N/p^r, therefore Equation 2 has a unique solution for each j with $d_j \neq 0$ except with negligible probability.

Finally, by the definition of Eval^*, we have $-\mathsf{PPRF.Eval}^*(K_j^*, I_j, \alpha_j) + (\beta_j, b_j) + (\delta_j, d_j) = -\mathsf{PPRF.Eval}^*(\hat{K}_j^*, I_j, \alpha_j) + (\beta_j, b_j)$, therefore the output to R corresponds to the output in the real protocol execution.

Note that for $p = 2$, we extract x by finding $j \in \{1, \ldots, t\}$ such that $\chi_j + c \cdot x_j = X$ and set $d_j = x_j - x$.

C.4 Proof of PCG Protocol for VOLE

Definition 22 (Dual-LPN assumption with static leakage). *Let $H \in \mathbb{F}_p^{N \times n}$, and consider the following game $G_b(\lambda)$ with a p.p.t. adversary $\mathcal{A}$, parameterized by a bit b and the security parameter λ:*

- *Sample $\boldsymbol{e} \xleftarrow{\$} \mathcal{D}_{t,N}$. Let $S = \{\alpha_1, \ldots, \alpha_t\} \in [N]^t$ be the sorted indices of non-zero entries in $\boldsymbol{e}$.*
- *$\mathcal{A}$ sends t sets $I_1, \ldots, I_t \subseteq [n]$.*
- *If $\alpha_j \in I_j$ for all $j \in \{1, \ldots, t\}$ then send success to $\mathcal{A}$, otherwise abort.*
- *If $b = 1$, let $\boldsymbol{y} = \boldsymbol{e} \cdot H$, otherwise sample $\boldsymbol{y} \xleftarrow{\$} \mathbb{F}_p^n$*
- *Send $\boldsymbol{y}$ to $\mathcal{A}$, who then outputs a bit b' (in case of abort, define the output of $\mathcal{A}$ to be $\perp$)*

The assumption states that $\Pr[\mathcal{A}^{G_0(\lambda)} = 1] - \Pr[\mathcal{A}^{G_1(\lambda)} = 1]$ is negligible in λ.

Functionality $\mathcal{F}_{\mathsf{sVOLE}}$:

PARAMETERS: $n, p, r \in \mathbb{N}$.

FUNCTIONALITY:

- Sample $\boldsymbol{u} \xleftarrow{\$} \mathbb{F}_p^n, \boldsymbol{v} \xleftarrow{\$} \mathbb{F}_{p^r}^n$, $x \xleftarrow{\$} \mathbb{F}_{p^r}$, and let $\boldsymbol{w} = \boldsymbol{u}x + \boldsymbol{v}$
  - If S is corrupt: receive $x, \boldsymbol{w}$ from $\mathcal{A}$ and recompute $\boldsymbol{v} = \boldsymbol{w} - \boldsymbol{u}x$
  - If R is corrupt: receive $\boldsymbol{u}, \boldsymbol{v}$ from $\mathcal{A}$ and recompute $\boldsymbol{w} = \boldsymbol{u}x + \boldsymbol{v}$
- Output $(x, \boldsymbol{w})$ to S and $(\boldsymbol{u}, \boldsymbol{v})$ to R

Fig. 19. Functionality for corruptible subfield-VOLE correlated randomness

Protocol Π_{sVOLE}:

PARAMETERS: $1^\lambda, N = 2^\ell, n, p, r, t \in \mathbb{N}$. PPRF is a puncturable PRF with domain $[N] = \{0,1\}^\ell$, key space $\{0,1\}^\lambda$, and range $\mathbb{F}_{p^r}$, supporting verification of malicious keys.
$H \in \mathbb{F}_p^{N \times n}$ is a matrix for which dual-LPN is hard.

PROTOCOL:

1. R samples a weight-t vector $\boldsymbol{e} \xleftarrow{\$} \mathcal{D}_{t,N}$. Let $S = \{\alpha_1, \ldots, \alpha_t\} \in [N]^t$ be the sorted indices of non-zero entries in $\boldsymbol{e}$, and $y_i = e_{\alpha_i} \in \mathbb{F}_p^*$.
2. S samples $x \xleftarrow{\$} \mathbb{F}_{p^r}$ and $\mathsf{k}_{\mathsf{pprf}} \xleftarrow{\$} \{0,1\}^\lambda$.
3. S and R call $\mathcal{F}_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$ (with the roles of sender and receiver reversed) on inputs $(\boldsymbol{y}, \alpha_1, \ldots, \alpha_t)$ and $(\mathsf{k}_{\mathsf{pprf}}, x)$.
4. R receives a punctured key k_j^* and value $z_j \in \mathbb{F}_{p^r}$, for $j \in \{1, \ldots, t\}$.
5. S receives the master keys $\mathsf{k}_1, \ldots, \mathsf{k}_t$.
6. R outputs $(\boldsymbol{u}, \boldsymbol{v}) \leftarrow G_{\mathsf{sVOLE}}.\mathsf{Expand}(0, \{\mathsf{k}_j^*, z_j\}_{j=1}^t, \boldsymbol{e})$
7. S outputs $(x, \boldsymbol{w}) \leftarrow G_{\mathsf{sVOLE}}.\mathsf{Expand}(1, \{\mathsf{k}_1, \ldots, \mathsf{k}_t\}, x)$

Fig. 20. Protocol for realizing random subfield VOLE of length n with malicious security

Definition 23 (Dual-LPN assumption with adaptive leakage). *Let $H \in \mathbb{F}_p^{N \times n}$, and consider the following game $G_b^{\mathsf{a}}(\lambda)$ with a p.p.t. adversary $\mathcal{A}$, parameterized by a bit b and the security parameter λ:*

- *Sample $\boldsymbol{e} \xleftarrow{\$} \mathcal{D}_{t,N}$. Let $S = \{\alpha_1, \ldots, \alpha_t\} \in [N]^t$ be the sorted indices of non-zero entries in $\boldsymbol{e}$.*
- *If $b = 1$, let $\boldsymbol{y} = \boldsymbol{e} \cdot H$, otherwise sample $\boldsymbol{y} \xleftarrow{\$} \mathbb{F}_p^n$*
- *Send $\boldsymbol{y}$ to $\mathcal{A}$*
- *$\mathcal{A}$ responds with t sets $I_1, \ldots, I_t \subseteq [n]$*
- *If $\alpha_j \in I_j$ for all $j \in \{1, \ldots, t\}$ then send success to $\mathcal{A}$, otherwise send $fail$*
- *$\mathcal{A}$ outputs a bit b'*

The assumption states that $\Pr[\mathcal{A}^{G_0^{\mathsf{a}}(\lambda)} = 1] - \Pr[\mathcal{A}^{G_1^{\mathsf{a}}(\lambda)} = 1]$ is negligible in λ.

Theorem 17. *Let PPRF be a t-puncturable PRF, and suppose that $(\mathcal{HW}_t, \mathbf{C}, \mathbb{F}_p)$-$\mathsf{dual}$-$\mathsf{LPN}(N, n)$ with static leakage holds. The protocol in Fig. 20 securely realizes the functionality $\mathcal{F}_{\mathsf{sVOLE}}$ (Fig. 19).*

Proof. The case where both parties are corrupted is straightforward. When neither party is corrupted, by inspection, the outputs of the honest parties satisfy $\boldsymbol{w} = \boldsymbol{u}x + \boldsymbol{v}$, so we just need to show that these values are uniform subject to this constraint. The VOLE sender's $\boldsymbol{u}$ output is pseudorandom under the dual-LPN assumption, since we have $\boldsymbol{u} = \boldsymbol{e} \cdot H$, and the receiver's x is uniformly random. Finally the sender's $\boldsymbol{v} = \boldsymbol{v}_1 \cdot H$ value is pseudorandom, since $\boldsymbol{v}_1$ consists of pseudorandom PPRF outputs, and the matrix H has full rank.

R *is corrupted.* The simulator Sim_S proceeds as follows.

1. Sim_S receives the malicious R's inputs to $\mathcal{F}_{\mathsf{mal}\text{-}t\text{-}\mathsf{PPRF}}$, $\boldsymbol{y}, S = (\alpha_1, \ldots, \alpha_t)$, and defines the weight $\leq t$ error vector $\boldsymbol{e}$.
2. Sim_S samples a PPRF key $\mathsf{k}_{\mathsf{pprf}} \xleftarrow{\$} \{0,1\}^\lambda$ and computes the key $\mathsf{k}^*_{\mathsf{pprf}} = \mathsf{PPRF.Puncture}(\mathsf{k}_{\mathsf{pprf}}, S)$ punctured at S.
3. It sends $\mathsf{k}^*_{\mathsf{pprf}}$ to R, along with random $z_j \xleftarrow{\$} \mathbb{F}_{p^r}$, for $j \in \{1, \ldots, t\}$.
4. Sim_S computes $\boldsymbol{u}, \boldsymbol{w} = G_{\mathsf{sVOLE}}.\mathsf{Expand}(0, \mathsf{k}^*_{\mathsf{pprf}}, \{z_j\}_{j=1}^t, \boldsymbol{e})$ and then sends $\boldsymbol{u}, \boldsymbol{w}$ to $\mathcal{F}_{\mathsf{sVOLE}}$.

Notice that the only difference between the simulation and the real execution is the way the z_j values are computed. In the protocol, z_j masks the sender's inputs with PPRF evaluations at the punctured points, whereas in the simulation z_j is random. These two views are indistinguishable, by the security of PPRF; any adversary that distinguishes the two executions can be used to win the PPRF selective security game, $\mathsf{Exp\text{-}s\text{-}pPRF}$, with exactly the same advantage.

S *is corrupted.*

1. Sim_R receives from S $x \in \mathbb{F}_{p^r}$, the subsets $I_1, \ldots, I_t$ and keys $K^*_1, \ldots, K^*_t \in \mathcal{K}$
2. Sample $\alpha_1, \ldots, \alpha_t \xleftarrow{\$} [N]$, and for each $j \in \{1, \ldots, t\}$, check that (i) $\alpha_j \in I_j$, and (ii) $\mathsf{Ver}(K^*_j, I_j) = 1$. If any check fails, abort.
3. Sim_R computes the PPRF outputs $\boldsymbol{v}_1$ using $\mathsf{Eval}^*(K^*_j, I_j, x)$, for all x, j, and uses these to compute $\boldsymbol{w} = \boldsymbol{v}_1 \cdot H$ that is sent to $\mathcal{F}_{\mathsf{sVOLE}}$, along with x.

Notice that the probability of abort is identical in both executions, since Sim_R samples a noise vector just as in the real protocol. Also, the outputs of the corrupt VOLE receiver, computed by Sim_R, are identically distributed to those in the protocol. The only difference between the two executions is the way the honest sender's outputs $(\boldsymbol{u}, \boldsymbol{v})$ are computed; here, we rely on the leaky variant of dual-LPN to argue that $\boldsymbol{u}$ is pseudorandom.

In particular, we show that any distinguisher $\mathcal{D}$, who distinguishes the real and ideal executions, can be used against the dual-LPN assumption with static leakage. We construct an adversary for game G as follows: Invoke $\mathcal{D}$ with an execution of Π_{sVOLE}, and, running Sim_R, receive the adversary's guesses $I_1, \ldots, I_t$. Instead of sampling α_j as Sim_R does, forward the guesses to game G. If G aborts, send *abort* to $\mathcal{D}$, otherwise, continue running Sim_R. At the end of the execution (if it did not abort) send to $\mathcal{D}$ the honest sender's output $(\boldsymbol{u}, \boldsymbol{v})$, where $\boldsymbol{u}$ is set to the $\boldsymbol{y}$ vector received from G, and $\boldsymbol{v} = \boldsymbol{w} - \boldsymbol{u}x$. Output whatever $\mathcal{D}$ outputs.

When $b = 1$, the view of $\mathcal{D}$ is as in the real protocol, whereas when $b = 0$ it is exactly as in the simulation, hence, our advantage against the game G is exactly the same as the advantage of $\mathcal{D}$ against the protocol.