Homomorphic Secret Sharing from Lattices Without FHE

Elette Boyle[1] *, Lisa Kohl[2] †, and Peter Scholl[3] ‡

[1] IDC Herzliya
Elette.Boyle@idc.ac.il

[2] Karlsruhe Institute of Technology
Lisa.Kohl@kit.edu

[3] Aarhus University
Peter.Scholl@cs.au.dk

Abstract. Homomorphic secret sharing (HSS) is an analog of somewhat- or fully homomorphic encryption (S/FHE) to the setting of secret sharing, with applications including succinct secure computation, private manipulation of remote databases, and more. While HSS can be viewed as a relaxation of S/FHE, the only constructions from lattice-based assumptions to date build *atop* specific forms of threshold or multi-key S/FHE.

In this work, we present new techniques directly yielding efficient 2-party HSS for polynomial-size branching programs from a range of lattice-based encryption schemes, *without S/FHE*. More concretely, we avoid the costly *key-switching* and *modulus-reduction* steps used in S/FHE ciphertext multiplication, replacing them with a new *distributed decryption* procedure for performing "restricted" multiplications of an input with a partial computation value. Doing so requires new methods for handling the blowup of "noise" in ciphertexts in a distributed setting, and leverages several properties of lattice-based encryption schemes together with new tricks in share conversion.

The resulting schemes support a superpolynomial-size plaintext space and negligible correctness error, with share sizes comparable to SHE ciphertexts, but cost of homomorphic multiplication roughly one order of magnitude faster. Over certain rings, our HSS can further support some level of packed SIMD homomorphic operations. We demonstrate the practical efficiency of our schemes within two application settings, where we compare favorably with current best approaches: 2-server private database pattern-match queries, and secure 2-party computation of low-degree polynomials.

1 Introduction

Homomorphic secret sharing (HSS) [9] is a form of secret sharing that supports a compact local evaluation on its shares. HSS can be viewed as the analog of fully (or somewhat-) homomorphic encryption (S/FHE) [42, 28] to the setting of secret sharing: a relaxation where homomorphic evaluation can be distributed among two parties who do not interact with each other. Over the past years, there has been a wave of HSS constructions for rich function classes (e.g., [9, 11, 27, 8, 23]) as well as an expanding range of corresponding applications. HSS suffices for many scenarios in which S/FHE can be applied (and even some for which it *cannot*), including low-communication secure computation [9, 12, 8], private manipulation of remote databases [31, 10, 21, 11, 43], methods of succinctly generating correlated randomness [8, 7], and more.

One of the appealing features of HSS compared to FHE is that allowing homomorphic evaluation to be distributed among two parties may constitute a simpler target to achieve. Indeed, forms of HSS for branching programs have been built from *discrete logarithm* type assumptions [9]; in contrast, obtaining encryption schemes from these structures that support comparable homomorphism on ciphertexts seems

*Supported in part by ISF grant 1861/16, AFOSR Award FA9550-17-1-0069, and ERC grant 742754 (project NTSC).

†Supported by ERC Project PREP-CRYPTO (724307), by DFG grant HO 4534/2-2 and by a DAAD scholarship. This work was done in part while visiting the FACT Center at IDC Herzliya, Israel.

‡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).

well beyond reach of current techniques. In regard to structures from which FHE does exist, the Learning With Errors (LWE) assumption [41] (and in turn its Ring LWE (RLWE) variant [40]) is known to imply strong versions of HSS [10, 24, 13].

However, in spite of its potential for comparative simplicity, all HSS constructions based on LWE or RLWE to date remain *at least* as complex as S/FHE. In particular, underlying each such HSS scheme is the common approach of beginning with and building atop some existing construction of FHE—relying on specific forms of threshold FHE, multi-key FHE, or even FHE-based "spooky encryption" [3, 10, 24, 13]. In this sense, current lattice-based HSS constructions serve predominantly as statements of feasibility, and have not been explored as a competitive alternative for use within applications.

Given the rapidly expanding set of HSS applications, together with the demonstrated power and success of leveraging lattices as a tool for advanced cryptography, a natural question is whether this situation can be improved. In particular, can we construct HSS from LWE and RLWE *without* (in some sense) S/FHE?

1.1 Our Results

In this work we consider precisely this question. We present and leverage new approaches for directly obtaining 2-party HSS schemes from LWE and RLWE, bypassing the intermediate step of fully (or even somewhat-) homomorphic encryption (S/FHE).

More concretely, our techniques avoid the costly *key-switching* and repeated *modulus-reduction* steps typically required for homomorphic multiplication of ciphertexts in existing (R)LWE-based FHE schemes [15, 29], and replace them instead with a new *distributed decryption* procedure for multiplying an encrypted value by a value in secret shared form, resulting in secret shares of the product. The cost of a homomorphic multiplication thus drops roughly to the cost of a decryption operation per party. This operation requires a new toolkit of methods for handling the blowup of "noise" from ciphertexts in a distributed setting, and leverages properties of lattice-based encryption schemes (such as key-dependent message security) in new ways.

Our construction takes inspiration from the HSS framework of [9], and yields a similar result: namely, HSS for the class of polynomial-size branching programs (capturing $\mathsf{NC1}$ and logspace computations). However, as discussed below, our construction offers several strong advantages over existing DDH-based schemes [9, 12, 8, 23], including *negligible* correctness error and *superpolynomial*-size plaintext space, as well as over S/FHE-based solutions for the same program class [3, 24], including cheaper multiplication, simpler setup, and *no noise growth*. We showcase these advantages via two sample applications: (1) Generating correlated randomness for secure 2-party computation in the prepocessing model, and (2) 2-server Private Information Retrieval for various private database queries such as conjunctive keyword search and pattern matching.

We now proceed to describe our main results.

HSS from Nearly Linear Decryption. Our core approach leverages the *"nearly linear"* structure of ciphertext decryption common to a range of lattice-based encryption schemes:

Definition 1 (Informal - *Nearly Linear Decryption*). *Let $R = \mathbb{Z}$ or $R = \mathbb{Z}[X]/(X^n + 1)$ for n a power of 2. Let $p, q \in \mathbb{N}$ be moduli with $p|q$ and $1 \ll p \ll q$. We say that an encryption scheme supports* nearly linear decryption *for messages $m \in R_p := R/pR$ if the secret key is $\mathbf{s} \in R_q^d$, and for any ciphertext $\mathbf{c} \in R_q^d$ encrypting m,*

$$\langle \mathbf{s}, \mathbf{c} \rangle = (q/p) \cdot m + e \mod q$$

for some "small" noise $e \in R$.

This captures, for example, the LWE-based schemes of Regev [41] and Applebaum *et al.* [2] (with $R = \mathbb{Z}, d = \lambda$), RLWE-based schemes of Lyubashevsky-Peikert-Regev [40] and Brakerski-Vaikutanathan [16] (with $R = \mathbb{Z}[X]/(X^n + 1), d = 2$), as well as various schemes based on Learning With Rounding [4] and Module-LWE [36]. For simplicity, we restrict ourselves to the decryption structure and polynomial rings R of the form specified above; however, our techniques extend to more general polynomial rings, as well as to encryption schemes which encode messages in low-order symbols (i.e., for which $\langle \mathbf{s}, \mathbf{c} \rangle = p \cdot e + m \mod q$).

We demonstrate how to exploit the near-linearity of decryption to support sequences of homomorphic *additions* over R, as well as homomorphic *"restricted" multiplications* over R of an evaluated value with an input. Ultimately, our scheme supports any sequence of these two homomorphic operations over R_r (for $r \in \mathbb{N}$ of choice) with negligible correctness error, subject to the requirement that the magnitude of computation values remain bounded by some chosen value B with $r \leq B \ll p$ (where the required size of p, and thus q, must grow with this bound). We remark that taking magnitude bound $B = 2$ suffices already to evaluate the class of polynomial-size branching programs with polynomial overhead [9]. Since efficiency is the primary focus of this work, however, we state our results as a function of these two operations directly, and applications can further exploit the ability to support large message spaces.

We achieve the stronger "public-key" variant of HSS [9], where the secret-sharing process can be split into a one-time setup phase (resulting in a public key pk and evaluation shares $(\mathsf{ek}_0, \mathsf{ek}_1)$) together with a separate "input encryption" phase, wherein any user can use pk to load his input x_i into secret-shared form (and where homomorphic evaluation can take place *across* parties' inputs). This variant of HSS facilitates applications of secure multi-party computation.

Theorem 1 (Informal - *Main HSS Construction*). *Given any encryption scheme with nearly linear decryption (as above) over ring R with parameters $p, q, d \in \mathbb{N}$, as well as magnitude bound $B \in \mathbb{N}$ for which $B \ll p \ll q/B$, and output modulus $r \leq B$, there exists 2-party public-key HSS for inputs in R_r with size:*

- *Public key $\mathsf{pk} = pk$ of the encryption scheme, Evaluation keys $\mathsf{ek}_b \in R_q^{d-1}$*
- *HSS shares of each input $x_i \in R_r$ consist of d ciphertexts.*

supporting any polynomial number of the following homomorphic operations over R_r (subject to the ℓ_∞ magnitude bound $\|y\|_\infty \leq B$ (in R) for all partial computation values y), with negligible correctness error, and the specified complexities:

- *Loading an input into memory ($y_i \leftarrow x_i$):* — *d decryptions*
- *Addition of memory values ($y_k \leftarrow y_i + y_j$):* — *1 addition over R_q^d*
- *Multiplication of input with memory value ($y_k \leftarrow x_i \cdot y_j$):* — *$d$ decryptions*
  "Terminal" multiplication (s.t. y_k appears in no future mult): — *1 decryption*

where "decryption" is essentially one inner product over R_q^d.

Plugging in the "LPR" RLWE-based scheme of [40] (where ciphertexts consist of $d = 2$ ring elements), our HSS shares consist of 4 R_q-elements per R_r-element plaintext, and homomorphic multiplication of an input and memory value in R_r is dominated by 4 R_q-multiplications (with correctness if the resulting product y over R maintains $\|y\|_\infty \leq B$). When incorporating the necessary choices of modulus q and dimension n, the resulting HSS shares will be of comparable size to the analogous SHE-based approach, but will offer significantly cheaper homomorphic multiplication operations—faster by approximately one order of magnitude. (See "Comparison to SHE-based solutions" discussion below.)

We further explore extensions and optimizations to the core construction, within the following settings:

1. *Secret-key HSS*: For applications where all secrets in the system originate from a single party; e.g., the client in 2-server Private Information Retrieval.
2. *Degree-2 computations*: For the special case of homomorphic evaluation of degree-2 polynomials (and extension to low-degree polynomials), with applications to secure computation.
3. *SIMD computations*: Direct support for homomorphic evaluation of "packed" single-instruction multiple data (SIMD) parallel computations on data items encoded as vectors. This has useful application to parallel computations, and to PIR-type applications, where one wishes to perform several identical evaluations on different database items.

Comparison to existing approaches. We briefly discuss our resulting HSS in reference to existing approaches for comparable function classes.

Comparison to Group-Based HSS. Our core construction framework resembles the HSS schemes of Boyle, Gilboa, and Ishai [9] and successors [12, 8, 23], which rely on various flavors of discrete logarithm type assumptions in cryptographically hard Abelian groups (e.g., Decisional Diffie Hellman (DDH) or circular security of ElGamal). We refer to this line as "group-based" HSS.

Despite many algorithmic and heuristic advances, all works in this line are subject to a common computation barrier: In addition to their upper bounds, Dinur, Keller, and Klein [23] showed that (barring a breakthrough in discrete logarithm techniques[4]) performing a homomorphic multiplication via this general approach with plaintext space size B and correctness error δ *requires* runtime $T = \Omega(\sqrt{B/\delta})$. Of particular note, this inherently restricts support to plaintext spaces of polynomial size B, as well as inverse-polynomial error δ.

- *Superpolynomial-size plaintext space.* In contrast, our HSS scheme can directly support operations within superpolynomial plaintext spaces over $\mathbb{Z}$ or $\mathbb{Z}[X]/(X^n + 1)$, with complexity growing roughly as the logarithm of the maximum magnitude B. This circumvents blowups associated with artificial emulation of larger input spaces by breaking input elements into small pieces (e.g., bits) and operating piecewise. Such blowups manifest even when operating over small inputs, as encodings of the *secret key* as a plaintext are necessary in order to support homomorphism.
- *Negligible error.* Our HSS also enjoys negligible correctness error. Beyond a theoretical distinction, this greatly affects efficiency. Even to obtain constant failure probability in group-based approaches, homomorphic evaluation of S multiplications requires computation scaling as $S^{3/2}$ [23], since the error of each individual multiplication must be pushed down to $\sim \delta/S$ to reach overall error δ. The presence (or non-presence) of error may further *leak* information about the secret inputs; this adds layers of complexity and overhead to HSS-based applications, wherein effects of error must be sanitized before homomorphically evaluated output shares can be exchanged [9, 12, 8].
- *Cheaper operations.* Overall, the resulting lattice-based schemes require cheaper operations than group-based alternatives, e.g. replacing cryptographic group exponentiations by simple polynomial ring multiplications (efficiently implementable using FFT). Most stark in contrast: the expensive "share-conversion" steps in group-based approaches—requiring large scales of repeated group multiplications and pattern matches, and dominating computation costs in homomorphic evaluation—are trivialized given our new techniques.

Comparison to SHE-based solutions. Two-server HSS can also be constructed from threshold variants of somewhat or fully homomorphic encryption, by replacing the (interactive) distributed decryption procedure with the non-interactive "rounding" technique from [24] to give additive shares of the output. Using FHE this can give HSS for circuits, although the computational overhead either grows with the depth of the circuit [15] or is independent of the circuit size but very large due to a costly bootstrapping step.[5]

SHE is reasonably practical for evaluating low-depth circuits, where the dominant cost is homomorphic multiplication. There are several different approaches to SHE multiplication, all of which have various complications due to the need for a "key-switching" procedure [15, 29] to avoid ciphertext expansion, as well as either modulus switching [15] or scale-invariant operations [14, 26] to reduce noise growth.[6]

Our approach avoids these complications, leading to a conceptually simpler and more efficient scheme with several advantages over SHE-based HSS.

- *Cheaper multiplication.* Our homomorphic multiplication procedure is much simpler and cheaper than in SHE, since we avoid costly ciphertext expansion or key/modulus-switching procedures which are inherent

[4] Namely, solving the Discrete Logarithm in a Interval problem with interval length R in time $o(\sqrt{R})$.

[5] Although the cost of bootstrapping has fallen dramatically in recent years [34, 25, 18, 19], the efficiency is still orders of magnitude worse than low-depth somewhat homomorphic encryption using SIMD operations.

[6] So-called "third generation" SHE schemes based on GSW [30] have simpler homomorphic multiplication, but much larger ciphertexts that grow with $\Omega(n \log^2 q)$ instead of $O(n \log q)$, for (R)LWE dimension n and modulus q.

in most SHE schemes. Concretely, our multiplication procedure has roughly the cost of *2 decryption operations* in SHE, which we estimate improves our performance by around an order of magnitude based on recent implementation results [32]. While our supported multiplications are of a "restricted" form, requiring one of the multiplicands to be an original input value, this has a mild effect within low-degree computations, which are anyway the competitive regime for SHE.

– *Simpler setup.* Since we do not need key-switching, we also avoid the cost of setting up the key-switching material in a distributed manner, which is a source of additional complexity in threshold FHE [3] as it requires generating several "quasi-encryptions" of s^2, where s is the secret-shared private key.
– *No noise growth.* Unlike FHE, ciphertexts in our homomorphic evaluation procedure do not incur noise growth, which increases ciphertext size and limits the number of homomorphic operations. Instead, we are only limited in that the parameters must be chosen based on an upper bound on the maximum size of any plaintext value (without modular reduction) during the computation.

Sample applications. To illustrate the potential of our techniques, we consider two example use-cases of HSS for branching programs. Firstly, we look at secure two-party computation of low-degree polynomials, and its application to generating various forms of correlated randomness. Many MPC protocols use preprocessed, correlated randomness such as Beaver multiplication triples, matrix multiplication triples or truth-table correlations to achieve a very fast "online" protocol. Protocols such as SPDZ [22] often use SHE to generate this randomness, whereas using HSS (considered in [8]) has potential to greatly improve computational costs, and reduce the round complexity to just a single round, while paying a slight overhead with larger ciphertexts. Secondly, we look at 2-server Private Information Retrieval (PIR), which allows a client to perform private queries to a public database. Our HSS for branching programs allows a much richer set of queries than previous, practical schemes based on one-way functions [43], and in this case we can reduce the share size compared with using SHE, as well as the computation.

1.2 Technical Overview

Recall our HSS is with respect to an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with *nearly linear decryption* over ring $R = \mathbb{Z}$ or $\mathbb{Z}[X]/(X^n+1)$ (as discussed above), with moduli $r \leq B \ll p \ll q/B$ and parameter d. Ciphertexts and the secret key of the encryption scheme are elements $\mathbf{c}, \mathbf{s} \in R_q^d$ with $\mathbf{s} = (1, \widehat{\mathbf{s}}) \in R_q \times R_q^{d-1}$, the plaintext space of encryption is R_p, and we will support homomorphic operations over R_r for computations for which all intermediate computation values y (as performed over R) remain bounded by $\|y\|_\infty \leq B$. (We will denote $y \in [R]_B$ to highlight that arithmetic is *not* performed modulo B.)

The core of our HSS resembles the DDH-based framework of [9], translated to the setting of lattice-based encryption. The HSS public key pk is precisely the public key of the encryption scheme.[7] The evaluation keys $(\mathsf{ek}_0, \mathsf{ek}_1) \in R_q^d \times R_q^d$ are additive secret shares of the key $\mathbf{s} \in R_q^d$ over R_q.[8] Homomorphic evaluation maintains the invariant that for every intermediate computation value $y \in [R]_B$, Party 0 and Party 1 will hold *additive shares* $(\mathbf{t}_0^y, \mathbf{t}_1^y) \in R_q^d \times R_q^d$ of the product $y \cdot \boldsymbol{s} \in R_q^d$ over R_q. This directly admits homomorphic addition, by locally adding the corresponding secret shares.

As usual, the challenge comes in addressing multiplication. We support homomorphic "restricted" multiplications, between any intermediate computation value y and input value x. To aid this operation, the HSS sharing of input $x \in [R]_B$ will be a (componentwise) encryption of $x \cdot \mathbf{s}$: i.e., d ciphertexts $\mathbf{C}^x = (\mathbf{c}^{x \cdot s_1}, \ldots, \mathbf{c}^{x \cdot s_d}) \in (R_q^d)^d$. Interestingly, these encryptions can be generated given just pk of the encryption, leveraging a weak form of key-dependent message (KDM) security implied by nearly linear decryption—see "KDM Security" discussion below. Combining the HSS encoding $\mathbf{C}^x$ of x with the secret shares $(\mathbf{t}_0^y, \mathbf{t}_1^y)$ for y, nearly linear decryption then gives us:

$$\text{for every } i \in [d]: \quad \langle \mathbf{t}_0^y, \mathbf{c}^{x \cdot s_i} \rangle + \langle \mathbf{t}_1^y, \mathbf{c}^{x \cdot s_i} \rangle = \langle y \cdot \mathbf{s}, \mathbf{c}^{x \cdot s_i} \rangle \approx (q/p) \cdot xy \cdot s_i \quad \text{over } R_q.$$

[7] Note that nearly linear decryption generically implies existence of a public-key encryption procedure.
[8] This can be decreased to $(d-1)$ R_q-elements communicated, as $s_1 = 1 \in R_q$.

Collectively, this *almost* yields the desired additive shares of $xy \cdot \mathbf{s} \in R_q^d$ to maintain the homomorphic evaluation invariant.

Rounding. Our first observation is that we can use the non-interactive rounding trick as in [24] to locally convert the approximate shares of $(q/p) \cdot xy \cdot s_i$ over R_q from above, to *exact* shares of $xy \cdot s_i$ over R_p. Concretely, each party simply scales his share by (p/q) and *locally* rounds to the nearest integer value. This operation heavily relies on the fact that there are 2 parties, and provides correct output shares over R_p with error probability pB/q, negligible for $p \ll q/B$.

However, this is not quite what we need: the resulting secret shares of $xy \cdot \mathbf{s}$ are over R_p, *not* R_q. This means we cannot use the shares again to "distributively decrypt" the original set of ciphertexts $\mathbf{C}^{x'}$ for any input x', a task whose operations must take place over R_q. (In fact, information about the $s_i \in R_q$ may even be *lost* when taken mod p.) Performing a second analogous multiplication would then necessitate a *second set* of ciphertexts, over a smaller modulus: namely with R_p playing the original role of R_q, and some $p_1 \ll p$ playing the previous role of p. In such fashion, one can devise a *leveled* HSS scheme operating via a sequence of decreasing moduli $q \gg p \gg p_1 \gg p_2 \gg \cdots p_{\text{deg}}$, where each step must drop by a superpolynomial factor to guarantee negligible correctness error. The size and complexity of such HSS scheme, however, would grow significantly with the desired depth of homomorphic computation.

Lifting. We avoid the above conundrum by (quite literally) doing *nothing*. Our observation is as follows. In general, converting secret shares up to a higher modulus constitutes a problem: e.g., even from $\mathbb{Z}_2$ to $\mathbb{Z}_3$ we have $1 + 1 \equiv 0 \in \mathbb{Z}_2$ turning to $1 + 1 \equiv 2 \in \mathbb{Z}_3$. However, if we can guarantee that the secret shared payload is *very small* compared to the modulus, this wraparound problem drops to a negligible fraction of possible secret shares. Concretely, given shares $t_0 + t_1 \equiv t \mod p$ for $t_0, t_1, t \in (-\lfloor p/2 \rceil, \ldots, \lfloor (p-1)/2 \rceil]$, then $t_0 + t_1 = t$ with equality (over $\mathbb{Z}$) unless $t - t_0$ falls $\leq -\lfloor p/2 \rceil$ or $> \lfloor (p-1)/2 \rceil$. If t_0 is randomly chosen and $t \ll p$, then these corner cases occur with only negligible probability. Conditioned on this, conversion to shares modulo q is immediate: it *already* holds that $t_0 + t_1 = t \mod q$.

Recall that we wish to perform share conversion on payload values of the form $y \cdot s_i \in R_q$. To use this trick, we must thus adjust the construction to guarantee any such value has low magnitude $\|y \cdot s_i\|_\infty \ll p$. This is done via two pieces. First, we leverage a result of Applebaum *et al.* [2], which allows us to replace a randomly sampled secret key $\mathbf{s} \in R_q^d$ of encryption with one sampled from the *low-magnitude* noise distribution, without loss of security. Second, we introduce an additional modulus level $B \ll p$, and address only computations which remain bounded in magnitude by $\|y\|_\infty \leq B$. Together, this will ensure each value $y \cdot s_i$ has small norm in comparison to p, and thus the shares of $y \cdot s_i$ over R_p can be *directly* interpreted as shares of $y \cdot s_i$ over R_q, successfully returning us to the desired homomorphic evaluation invariant. Finally, using the same low-magnitude-payload share conversion trick, in the final step of computation, the parties can convert their shares of $y \cdot \mathbf{s} = (y, y \cdot \widehat{\mathbf{s}})$ (recall $\mathbf{s} = (1, \widehat{\mathbf{s}})$) over R_q to shares of y over R_r for target output modulus r.

Ultimately, the HSS scheme uses three moduli levels: $B \ll p \ll q/B$. Correctness holds as long as the magnitude of computation values is bounded within $[R]_B$. Homomorphic evaluation maintains secret shares over R_q as its invariant. Each homomorphic multiplication drops down to R_p to remove effects of noise, then steps back up to shares over R_q to reinstate the invariant. An advantageous side effect of this structure is that, conditioned on remaining within magnitude bound B (e.g., Boolean computations), the size of our HSS shares is completely *independent* of the depth or size of the homomorphic computation.

To conclude, we highlight some of the additional ideas and techniques arising within our scheme and extensions.

KDM security. Our HSS reveals encryptions of the form $\mathsf{Enc}(x \cdot s_i)$, for input x and secret key $\mathbf{s}$ of the underlying encryption scheme. Key-dependent message (KDM) security of the encryption scheme with respect to this class of linear functions of $\mathbf{s}$ follows from its nearly linear decryption structure. As typical in KDM literature (following [2, 16]), this is shown by demonstrating as an intermediate step that such encryptions can be efficiently generated from knowledge only of the public key and rerandomized to "look like" fresh encryptions.

In our construction, we *leverage* this efficient generation procedure. This enables pk of the HSS to consist purely of the public key of the encryption scheme, while still allowing parties to encode their respective inputs

x as $\{\mathsf{Enc}(x \cdot s_i)\}_{i\in[d]}$. The corresponding encoding procedure is simpler and achieves better parameters than publishing $\{\mathsf{Enc}(s_i)\}_{i\in[d]}$ as part of pk (as was done in [9]), as this introduces extra ciphertexts as well as a second noise term that must be "drowned" by larger noise when scaling by x and rerandomizing.

Secret key as an input. For our RLWE-based HSS schemes with plaintext space $R_r = \mathbb{Z}_r[X]/(X^n+1)$, and when sampling the secret key $\mathbf{s} = (1, \widehat{s}) \in R_q^2$ from the low-magnitude noise distribution, it holds that $\widehat{s}$ *itself* lies within the supported input space R_r of the HSS. This is implicitly exploited in our attained HSS efficiency, e.g. where our encryptions of $x \cdot \boldsymbol{s} = (x, x\widehat{s}) \in R_q^2$ can consist of just *two* ciphertexts (instead of λ).

However, this also opens *qualitatively* new approaches toward optimization. For example, suppose the evaluation keys $\mathsf{ek}_0, \mathsf{ek}_1$ are augmented with shares of $(\widehat{s})^2$, as well as shares of $\widehat{s}$. We can then view the shares of $(\widehat{s}, (\widehat{s})^2) = \widehat{s}(1, \widehat{s})$ as HSS sharings of the computation value $\widehat{s}$, and thus use them to homomorphically multiply an input x by $\widehat{s}$. For degree 2, this allows us to save sending encryptions of $x \cdot \widehat{s}$ for inputs x, since we can now generate these "for free" using $\mathsf{ek}_0, \mathsf{ek}_1$ and the encryptions of x, reducing the share size by a factor of two.

SIMD operations. If the underlying encryption scheme is over a ring R of the right form, then our basic HSS supports homomorphic evaluation of "single instruction, multiple data" (SIMD) operations. Namely, suppose $R = \mathbb{Z}[X]/(X^n+1)$ where X^n+1 splits over R_r (for some prime $r \geq 2$) into pairwise different irreducible polynomials of degree $k \in \mathbb{N}$: that is, $R_r \cong \mathbb{F}_{r^k} \times \cdots \times \mathbb{F}_{r^k}$ for n/k copies of $\mathbb{F}_{r^k}$. In such case, our homomorphic additions and multiplications over R_r directly translate to corresponding SIMD operations within the individual computation "slots."

A caveat of this correspondence is that the magnitude bound requirement B over R_r (in *coefficient* embedding) does not translate directly to a per-slot magnitude bound of B (in CRT embedding). Thus current SIMD support can effectively handle low-degree computations, but suffers performance degradation as the degree increases, even if the magnitude of the SIMD computations is bounded. An interesting goal for future investigation will be to devise new ways of packing to mitigate this disadvantage.

2 Preliminaries

We begin this section by introducing some notation. For notation that we consider common knowledge we refer to Section A in the Appendix. We denote our security parameter by λ. Throughout this paper we consider all parameters to implicitly depend on λ, e.g. by $\ell \in \mathbb{N}$ we actually consider ℓ to be a function $\ell\colon \mathbb{N} \to \mathbb{N}$, but simply write ℓ in order to refer to $\ell(\lambda)$.

For a real number $x \in \mathbb{R}$, by $\lfloor x \rceil \in \mathbb{Z}$ we denote the element closest to $x \in \mathbb{R}$, where we round up when the first decimal place of x is 5 or higher.

In many cases, we will consider a ring which is either $R = \mathbb{Z}$ or $R = \mathbb{Z}[X]/(X^n+1)$, where $n \in \mathbb{N}$ with $n \leq \mathsf{poly}(\lambda)$ is a power of 2. We will denote the dimension of the corresponding ring over $\mathbb{Z}$ by N (i.e. $N = 1$ in the former case and $N = n$ in the latter). We denote this by saying R is of dimension N.

We employ the infinity norm on R. For $x \in R$ with coefficients $x_1, \ldots, x_N$, the infinity norm of x is defined as $\|x\|_\infty := \max_{i=1}^N |x_i|$.

For $p \in \mathbb{N}$, by R_p we denote R/pR. Note that we consider R_p as elements for which all coefficients are in the interval $(-\lfloor p/2 \rceil, \ldots, \lfloor (p-1)/2 \rceil]$. For $B \in \mathbb{N}$, we denote $[R]_B := \{x \in R \mid \|x\|_\infty \leq B\}$. More generally, for an interval $I \subseteq \mathbb{Z}$, we write $R|_I$ to denote all elements of R that have only coefficients in I.

We denote vectors by bold lower-case letters and matrices by bold upper-case letters. We interpret vectors as column-vectors. For a vector $\mathbf{x} \in R^\ell$, by x_i we refer to the i-th entry (for $i \in \{1, \ldots, \ell\}$).

We consider *public-key encryption schemes* that satisfy the security notion of *pseudorandomness of ciphertexts*. For a formal definition we refer to Definition 6 and 7 in the Appendix.

2.1 Homomorphic Secret Sharing

We consider homomorphic secret sharing (HSS) as introduced in [9]. By default, in this work, the term HSS refers to a public-key variant of HSS. Unlike [9], we do not need to consider non-negligible δ error failure probability.

Definition 2 (Homomorphic Secret Sharing). *A (2-party, public-key)* Homomorphic Secret Sharing (HSS) *scheme for a class of programs $\mathcal{P}$ over a ring R with input space $\mathcal{I} \subseteq R$ consists of PPT algorithms* $(\mathsf{HSS.Gen}, \mathsf{HSS.Enc}, \mathsf{HSS.Eval})$ *with the following syntax:*

- $\mathsf{HSS.Gen}(1^\lambda)$*: On input a security parameter 1^λ, the key generation algorithm outputs a public key* pk *and a pair of evaluation keys* $(\mathsf{ek}_0, \mathsf{ek}_1)$.
- $\mathsf{HSS.Enc}(\mathsf{pk}, x)$*: Given public key* pk *and secret input value $x \in \mathcal{I}$, the encryption algorithm outputs a ciphertext* ct.
- $\mathsf{HSS.Eval}(b, \mathsf{ek}_b, (\mathsf{ct}^{(1)}, \ldots, \mathsf{ct}^{(\rho)}), P, r)$*: On input party index $b \in \{0,1\}$, evaluation key ek_b, vector of ρ ciphertexts, a program $P \in \mathcal{P}$ with ρ input values and an integer $r \geq 2$, the homomorphic evaluation algorithm outputs $y_b \in R_r$, constituting party b's share of an output $y \in R_r$.*

The algorithms $(\mathsf{HSS.Gen}, \mathsf{HSS.Enc}, \mathsf{HSS.Eval})$ *should satisfy the following correctness and security requirements:*

- **Correctness:** *For all $\lambda \in \mathbb{N}$, for all $x^{(1)}, \ldots, x^{(\rho)} \in \mathcal{I}$, for all programs $P \in \mathcal{P}$ with size $|P| \leq \mathsf{poly}(\lambda)$ and $P(x^{(1)}, \ldots, x^{(\rho)}) \neq \perp$, for integer $r \geq 2$, for $(\mathsf{pk}, \mathsf{ek}_0, \mathsf{ek}_1) \leftarrow \mathsf{HSS.Gen}(1^\lambda)$ and for $\mathsf{ct}^{(i)} \leftarrow \mathsf{HSS.Enc}(1^\lambda, \mathsf{pk}, x^{(i)})$ we have*

$$\mathrm{Pr}^{\mathsf{cor}}_{\mathsf{HSS},(x^{(i)})_i,P,r}(\lambda) := \mathrm{Pr}\left[y_0 + y_1 = P(x^{(1)}, \ldots, x^{(\rho)}) \mod r\right] \geq 1 - \lambda^{-\omega(1)},$$

  where

$$y_b \leftarrow \mathsf{HSS.Eval}(b, \mathsf{ek}_b, (\mathsf{ct}^{(i)})_i, P, r)$$

  for $b \in \{0,1\}$ and where the probability is taken over the random coins of $\mathsf{HSS.Gen}$, $\mathsf{HSS.Enc}$ *and* $\mathsf{HSS.Eval}$.
- **Security:** *For all security parameters $\lambda \in \mathbb{N}$, for all PPT adversaries $\mathcal{A}$ that on input 1^λ output a bit $b \in \{0,1\}$ (specifying which encryption key to corrupt), and input values $x_0, x_1 \in \mathcal{I}$, we require the following advantage to be negligible in λ:*

$$\mathrm{Adv}^{\mathsf{sec}}_{\mathsf{HSS},\mathcal{A}}(\lambda) := \left| \mathrm{Pr}\left[\mathcal{A}(\mathsf{input}_b) = \beta \;\middle|\; \begin{array}{l} (b, x_0, x_1, \mathsf{state}) \leftarrow \mathcal{A}(1^\lambda), \\ \beta \leftarrow \{0,1\}, \\ (\mathsf{pk}, (\mathsf{ek}_0, \mathsf{ek}_1)) \leftarrow \mathsf{HSS.Gen}(1^\lambda), \\ \mathsf{ct} \leftarrow \mathsf{HSS.Enc}(\mathsf{pk}, x_\beta), \\ \mathsf{input}_b := (\mathsf{state}, \mathsf{pk}, \mathsf{ek}_b, \mathsf{ct}) \end{array} \right] - \frac{1}{2} \right|.$$

Remark 1. Within applications, we additionally consider a secret-key variant of HSS. For details we refer to Definition 8 in the Appendix.

2.2 Computational Models

Our main HSS scheme naturally applies to programs P in a computational model known as *Restricted Multiplication Straight-line (RMS)* programs [20, 9].

Definition 3 (RMS programs). *An RMS program consists of a magnitude bound B_{max} and an arbitrary sequence of the four following instructions, sorted according to a unique identifier $\mathsf{id} \in \mathcal{S}_{\mathsf{id}}$:*

- *Load an input into memory:* $(\mathsf{id}, \widehat{y}_j \leftarrow \widehat{x}_i)$.
- *Add values in memory:* $(\mathsf{id}, \widehat{y}_k \leftarrow \widehat{y}_i + \widehat{y}_j)$.
- *Add input values:* $(\mathsf{id}, \widehat{x}_k \leftarrow \widehat{x}_i + \widehat{x}_j)$.
- *Multiply memory value by input:* $(\mathsf{id}, \widehat{y}_k \leftarrow \widehat{x}_i \cdot \widehat{y}_j)$.
- *Output from memory, as R element:* $(\mathsf{id}, r, \widehat{O}_j \leftarrow \widehat{y}_i)$.

If at any step of execution the size of a memory value exceeds the bound B_{max} (i.e. $\|\widehat{y}_j\|_\infty > B_{\mathsf{max}}$), the output of the program on the corresponding input is defined to be $\perp$. Otherwise the output is the sequence of $\widehat{O}_j$ values, sorted by id. *We define the* size *(resp.,* multiplicative size*) of an RMS program P as the number of instructions (resp., multiplication and load input instructions). Note that we consider addition of input values merely for the purpose of efficiency. We denote the maximum number of additions on input values by $P_{\mathsf{inp}+}$.*

3 HSS from encryption with nearly linear decryption

As explained in the introduction, the core of our HSS construction is an encryption scheme with nearly linear decryption, where nearly linear means that for message $m \in R_p := R/pR$, secret key $\mathbf{s} \in R_q^d$, and ciphertext $\mathbf{c} \in R_q^d$ encrypting m, for some "small" noise $e \in R$ we have

$$\langle \mathbf{s}, \mathbf{c} \rangle = (q/p) \cdot m + e \mod q.$$

We begin in Section 3.1 by explaining our two main share conversion tricks, which allow two parties holding secret shares of $(q/p) \cdot m + e \mod q$ for small m to locally modify their values, such that in the end each party holds a secret share of the message m *modulo* q. In Section 3.2 we present our formal definition of nearly linear decryption, and prove two properties that it implies. Then, in Section 3.3 we give our HSS construction based on any such encryption scheme.

3.1 Computation on 2-party secret shared values

First, we present a local rounding trick as in [24] which allows to recover the shares of m (modulo p). The idea is that if q/p is large, the probability that the error term e leads to a rounding error is small. Note that it is crucial here that we are in the 2-party setting, where the secret shares of $(q/p) \cdot m + e \mod q$ have both approximately (that is, except for the error e) the same distance from some multiple of q/p. In fact, even for arbitrarily large gap between p and q, rounding for 3 or more parties fails with constant probability. For a proof of the rounding lemma we refer to Section B.1 in the Appendix.

Lemma 1 (Rounding of noisy shares). *Let $p, q \in \mathbb{N}$ be modulus values with $q/p \geq \lambda^{\omega(1)}$. Let $R \in \{\mathbb{Z}, \mathbb{Z}[X]/(X^n+1)\}$ be of dimension N. Let $t_0, t_1 \in R_q$ random subject to*

$$t_0 + t_1 = (q/p) \cdot m + e \mod q$$

for some $m \in R_p, e \in R$ with $q/(p \cdot \|e\|_\infty) \geq \lambda^{\omega(1)}$. Then there exists a deterministic polynomial time procedure Round *that takes an input $t_b \in R_q$ and outputs a value in R_p such that it holds*

$$\mathsf{Round}(t_0) + \mathsf{Round}(t_1) = m \mod p$$

with probability at least $1 - N \cdot (\|e\|_\infty + 1) \cdot p/q \geq 1 - \lambda^{-\omega(1)}$ over the choice of the shares t_0, t_1.

The following simple observation constitutes a crucial step of our HSS construction, as it will allow to have several levels of multiplication without requiring a sequence of decreasing moduli. While in general the conversion of secret shares from one modulus to another constitutes a problem, we observe that whenever the secret shared value is *small* in comparison to the modulus, and we use the centered representation of R_p with coefficients in $(-\lfloor p/2 \rceil, \ldots, \lfloor (p-1)/2 \rceil]$, then with high probability the secret sharing actually constitutes a secret sharing over R, so switching to an arbitrary modulus is trivial. Note that (as for rounding) this only holds true in the 2-party setting. For the proof we refer to Section B.1 in the Appendix.

Lemma 2 (Lifting the modulus of shares). *Let $p \in \mathbb{N}$ be a modulus with $p \geq \lambda^{\omega(1)}$. Let $R \in \{\mathbb{Z}, \mathbb{Z}[X]/(X^n+1)\}$ be of dimension N. Let $m \in R$ and $z_0, z_1 \in R_p$ be random, subject to*

$$z_0 + z_1 = m \mod p.$$

Then we have

$$z_0 + z_1 = m \text{ over } R$$

with probability at least $1 - (N \cdot (\|m\|_\infty + 1)/p) \geq 1 - \lambda^{-\omega(1)}$ over the choice of the shares z_0, z_1.

$\underline{\mathrm{Exp}^{\mathsf{kdm-ind}}_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda):}$
$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{PKE.Gen}(1^\lambda)$
$\beta \leftarrow \{0,1\}$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{KDM}}(\cdot,\cdot)}(1^\lambda, \mathsf{pk})$
if $\beta = \beta'$ **return** 1
else return 0

$\underline{\mathcal{O}_{\mathsf{KDM}}(x,j):}$
if $\beta = 0$
  return $\mathsf{PKE.OKDM}(\mathsf{pk}, x, j)$
else
  return $\mathsf{PKE.Enc}(\mathsf{pk}, 0)$

Fig. 1: Security challenge experiment for the KDM oracle.

3.2 Encryption with nearly linear decryption

We now formally introduce encryption with nearly linear decryption. Basically, we require the following properties: First, there is a way to encrypt certain key-dependent messages without knowledge of the secret key. Second, it is possible to "distributively decrypt" a ciphertext. More precisely, given an encryption of message m and secret shares of some multiple x of the secret key $\mathbf{s}$, there is a way to obtain secret shares of $x \cdot m$ *over the same modulus as the original secret shares.* These properties together enable us to perform several stages of distributed decryption. That is, given an encryption of $x \cdot \mathbf{s}$ (for some value x) and a secret share of $x' \cdot \mathbf{s}$ modulo q, distributed decryption results in a secret share of $x \cdot x' \cdot \mathbf{s}$ modulo q, which can serve as input to another distributed decryption. One way to achieve both properties at once is to require nearly linear decryption.

Definition 4 (Encryption scheme with nearly linear decryption). *Let* $\mathsf{PKE} := (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ *be a public-key encryption scheme with pseudorandom ciphertexts. We say that* PKE *is a public-key* encryption scheme with nearly linear decryption *if it further satisfies the following properties:*

- ***Parameters:*** *The scheme is parametrized by modulus values $p, q \in \mathbb{N}$, dimension $d \in \mathbb{N}$, and bounds $B_{\mathsf{sk}}, B_{\mathsf{ct}} \in \mathbb{N}$, where $p|q$, $p \geq \lambda^{\omega(1)}$, $q/p \geq \lambda^{\omega(1)}$ and $d, B_{\mathsf{sk}}, B_{\mathsf{ct}} \leq \mathsf{poly}(\lambda)$, as well as a ring R, which is either $\mathbb{Z}$ or the polynomial ring $\mathbb{Z}[X]/(X^n+1)$, where $n \leq \mathsf{poly}(\lambda)$ is a power of 2.*
- ***Message space and secret key:*** *The scheme has message space $\mathcal{M} := R_p := R/pR$ and ciphertext space $\mathcal{C} := R_q^d := (R/qR)^d$. The secret key $\mathbf{s}$ returned by $\mathsf{PKE.Gen}$ on input 1^λ is an element of R^d satisfying $\|\mathbf{s}\|_\infty \leq B_{\mathsf{sk}}$. Further, $\mathbf{s}$ is of the form $(1, \widehat{\mathbf{s}})$ for some $\widehat{\mathbf{s}} \in R_p^{d-1}$.*
- ***Nearly linear decryption:*** *For any $\lambda \in \mathbb{N}$, for any $(\mathsf{pk}, \mathbf{s})$ in the image of $\mathsf{Gen}(1^\lambda)$, for any message $m \in R_p$ and for any ciphertext $\mathbf{c} \in R_q^d$ in the image of $\mathsf{PKE.Enc}(\mathsf{pk}, m)$, for some $e \in R$ with $\|e\|_\infty \leq B_{\mathsf{ct}}$ it holds*

$$\langle \mathbf{s}, \mathbf{c} \rangle = (q/p) \cdot m + e \mod q.$$

Notation. *For $(\mathsf{pk}, \mathbf{s}) \leftarrow \mathsf{Gen}(1^\lambda)$ and $\mathbf{m} = (m_1, \ldots, m_d) \in R_p^d$, we denote by $\mathsf{PKE.Enc}(\mathsf{pk}, \mathbf{m})$ the componentwise encryption $\mathbf{C} \leftarrow (\mathsf{PKE.Enc}(\mathsf{pk}, m_1), \ldots, \mathsf{PKE.Enc}(\mathsf{pk}, m_d))$; we denote by $\mathbf{Dec}(\mathsf{sk}, \mathbf{C})$ the decryption $(\mathsf{PKE.Dec}(\mathsf{sk}, \mathbf{c}_1), \ldots, \mathsf{PKE.Dec}(\mathsf{sk}, \mathbf{c}_d)) \in R_p^d$ of the matrix of d ciphertexts $\mathbf{C} = (\mathbf{c}_1 | \ldots | \mathbf{c}_d) \in R_q^{d \times d}$.*

Remark 2. Encryption with nearly linear decryption can be instantiated based on LWE (e.g. with [41, 2], where $d = \lambda$) and based on RLWE (e.g. with [40, 16], where $d = 2$). Further, it can be instantiated with schemes based on assumptions like module-LWE [36] and LWR [4]. For more details on the instantiation from the RLWE-based encryption scheme of LPR [40], we refer to Section 4, and for the instantiation from the LWE-based encryption scheme of Regev [41] we refer to Section D in the Appendix.

We prove that our two desired properties are satisfied by any encryption scheme with nearly linear decryption. The first property allows anyone to compute an encryption of any linear function of the secret key without having access to the secret key itself, serving as a "KDM oracle." A similar notion, but for secret-key encryption schemes and with deterministic procedure, was introduced in [5]. For the proof of the following lemma we refer to Section B.2 in the Appendix.

Lemma 3 (KDM oracle). *Let* $\mathsf{PKE} := (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ *be a public-key encryption scheme with nearly linear decryption and parameters* $(p, q, d, B_{\mathsf{sk}}, B_{\mathsf{ct}}, R)$*. Then there exists a PPT procedure* $\mathsf{PKE.OKDM}$ *that takes as input a public key* pk*, a value* $x \in R$ *and an index* $j \in \{1, \ldots, d\}$ *and outputs a ciphertext* $\mathbf{c}_j$*, such that the following properties are satisfied.*

- ***Nearly linear decryption to the message*** $x \cdot s_j$***:*** *For any* $\lambda \in \mathbb{N}$*, for any* $(\mathsf{pk}, \mathbf{s})$ *in the image of* $\mathsf{Gen}(1^\lambda)$*, and for any ciphertext* $\mathbf{c}_j \in R_q^d$ *in the image of* $\mathsf{PKE.OKDM}(\mathsf{pk}, x, j)$*, it holds*

$$\langle \mathbf{s}, \mathbf{c}_j \rangle = (q/p) \cdot (x \cdot s_j) + e \mod q$$

  for some $e \in R$ *with* $\|e\|_\infty \leq B_{\mathsf{ct}}$*.*
- ***Security:*** *For any* $\lambda \in \mathbb{N}$ *and any PPT adversary* $\mathcal{A}$ *we have that*

$$\mathrm{Adv}^{\mathsf{kdm-ind}}_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda) := \left| \Pr\left[\mathrm{Exp}^{\mathsf{kdm-ind}}_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda) = 1 \right] - 1/2 \right|$$

  is negligible in λ*, where* $\mathrm{Exp}^{\mathsf{kdm-ind}}_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda)$ *is as defined in Figure 1*

By $\mathsf{PKE.}\mathbf{OKDM}(\mathsf{pk}, x)$ *we denote the KDM oracle that returns a componentwise encryption of* $x \cdot \mathbf{s}$*, i.e. that outputs the matrix* $(\mathsf{PKE.OKDM}(\mathsf{pk}, x, 1), \ldots, \mathsf{PKE.OKDM}(\mathsf{pk}, x, d)) \in R_q^{d \times d}$*.*

The following shows that any encryption with nearly linear decryption allows two parties to perform decryption *distributively*, employing their respective shares of the secret key to obtain a secret share of the corresponding message *modulo* q. Further, the scheme inherently supports homomorphic addition of ciphertexts, and the distributed decryption property holds accordingly for any sum of a bounded number of ciphertexts (generated from Enc or OKDM).

Lemma 4 (Distributed decryption of sums of ciphertexts). *Let* $\mathsf{PKE} := (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ *be a public-key encryption scheme with nearly linear decryption and parameters* $(p, q, d, B_{\mathsf{sk}}, B_{\mathsf{ct}}, R)$*, where* R *has dimension* N*. Let* $\mathsf{PKE.OKDM}$ *be the KDM oracle from Lemma 3. Let* $B_{\mathsf{add}} \in \mathbb{N}$ *with* $B_{\mathsf{add}} \leq \mathsf{poly}(\lambda)$*. Then there exists a deterministic polynomial time decryption procedure* $\mathsf{PKE.DDec}$ *with the following syntax and properties:*

- $\mathsf{PKE.DDec}(b, t_b, \mathbf{c})$*: On input a bit* $b \in \{0, 1\}$*, "key" share* $\mathbf{t}_b \in R_q^d$ *and ciphertext* $\mathbf{c}$*, outputs a message in* R*.*
- *For all* $x \in R_p$ *with* $p/\|x\|_\infty \geq \lambda^{\omega(1)}$ *and* $q/(p \cdot \|x\|_\infty) \geq \lambda^{\omega(1)}$*, for all* $(\mathsf{pk}, \mathbf{s}) \leftarrow \mathsf{Gen}(1^\lambda)$*, for all messages* $m_1 \ldots, m_{B_{\mathsf{add}}} \in R_p$*, for all encryptions* $\mathbf{c}_i$ *of* m_i *that are either output of* $\mathsf{PKE.Enc}$ *or of* $\mathsf{PKE.OKDM}$ *(in that case we have* $m_i = x_i \cdot s_j$ *for some value* $x_i \in R_p$ *and some index* $j \in \{1, \ldots, d\}$*) and for shares* $\mathbf{t}_0, \mathbf{t}_1 \in R_q^d$ *random subject to*

$$\mathbf{t}_0 + \mathbf{t}_1 = x \cdot \mathbf{s} \mod q$$

  for $\mathbf{c} := \sum_{i=1}^{B_{\mathsf{add}}} \mathbf{c}_i$ *and* $m := \sum_{i=1}^{B_{\mathsf{add}}} m_i$ *it holds*

$$\mathsf{PKE.DDec}(0, \mathbf{t}_0, \mathbf{c}) + \mathsf{PKE.DDec}(1, \mathbf{t}_1, \mathbf{c}) = x \cdot m \mod q$$

  with probability over the random choice of the shares $\mathbf{t}_0, \mathbf{t}_1$ *of at least*

$$1 - N \cdot (N \cdot B_{\mathsf{add}} \cdot \|x\|_\infty \cdot B_{\mathsf{ct}} \cdot p/q + \|x \cdot m\|_\infty / p + p/q + 1/p) \geq 1 - \lambda^{-\omega(1)}.$$

For $\mathbf{C} = (\mathbf{c}_1 | \ldots | \mathbf{c}_d) \in R_p^{d \times d}$ *by* $\mathbf{m} \leftarrow \mathsf{PKE.}\mathbf{DDec}(b, \mathbf{t}_b, \mathbf{C})$ *we denote the componentwise decryption* $\mathbf{m} \leftarrow (\mathsf{PKE.DDec}(b, \mathbf{t}_b, \mathbf{c}_1), \ldots, \mathsf{PKE.DDec}(b, \mathbf{t}_b, \mathbf{c}_d)) \in R_p^d$*.*

Proof. Let Round be the procedure for rounding of noisy shares from Lemma 1. We define $\mathsf{PKE.DDec}$ to be the algorithm that on input $b \in \{0, 1\}, \mathbf{t}_b \in R^d, \mathbf{c} \in R_q^d$ outputs

$$\mathsf{Round}(\langle \mathbf{t}_b, \mathbf{c} \rangle \mod q) \in R_q.$$

We prove that $\mathsf{PKE.DDec}$ indeed satisfies the required in Section B.2 in the Appendix. The idea is that nearly linear decryption allows (almost) homomorphic addition of ciphertexts with linear growth in the error. As $q/(p \cdot \|x\|_\infty) \geq \lambda^{\omega(1)}$ and the vectors $\mathbf{t}_b$ are individually random, by Lemma 1 we can recover $x \cdot m \mod p$ with overwhelming probability. Finally, as $p \geq \lambda^{\omega(1)}$, by Lemma 2 we can *lift* the modulus q (as with overwhelming probability the shares constitute a correct sharing of $x \cdot m$ over R).

Remark 3. Note that our techniques also extend to encryption schemes which encrypt messages in low-order symbols, e.g. where $\langle \mathbf{s}, \mathbf{c} \rangle = m + p \cdot e \mod q$ for p and q coprime. For more details we refer to Remark 4 in the Appendix.

3.3 HSS from encryption with nearly linear decryption

We now present our construction of a public-key HSS from an encryption scheme with nearly linear decryption. For various extensions that allow to improve the efficiency in specific applications, we refer to Section 3.4. We give an overview of the key and encryption sizes, as well as the evaluation costs of all schemes in Tables 1 and 2 at the end of Section 3.4.

Theorem 2 (HSS from encryption with nearly linear decryption). *Let* $\mathsf{PKE} := (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ *be a secure public-key encryption scheme with nearly linear decryption and parameters* $(p, q, d, B_{\mathsf{sk}}, B_{\mathsf{ct}}, R)$.

- *Let* $B_{\mathsf{inp}} \in \mathbb{N}$ *with* $p/B_{\mathsf{inp}} \geq \lambda^{\omega(1)}$ *and* $q/(B_{\mathsf{inp}} \cdot p) \geq \lambda^{\omega(1)}$.
- *Let* $\mathsf{PKE.OKDM}$ *be the KDM oracle from Lemma 3.*
- *Let* $\mathsf{PKE.DDec}$ *be the distributed decryption from Lemma 4.*
- *Let* $\mathsf{PRF} \colon \mathcal{K} \times \mathcal{S}_{\mathsf{id}} \to R_q^d$ *be a pseudorandom function.*

Then the scheme $\mathsf{HSS} = (\mathsf{HSS.Gen}, \mathsf{HSS.Enc}, \mathsf{HSS.Eval})$ *given in Figure 2 is a 2-party public-key homomorphic secret sharing scheme with input space* $[R]_{B_{\mathsf{inp}}}$ *for the class of RMS programs with magnitude bound* B_{max}*, where* $p/B_{\mathsf{max}} \geq \lambda^{\omega(1)}$ *and* $q/(B_{\mathsf{max}} \cdot p) \geq \lambda^{\omega(1)}$*. More precisely,* HSS *satisfies the following.*

- ***Correctness:*** *For any* $\lambda \in \mathbb{N}$*, for any* $x^{(1)}, \ldots, x^{(\rho)} \in [R]_{B_{\mathsf{inp}}}$*, for any polynomial-sized RMS program* P *with* $P(x^{(1)}, \ldots, x^{(\rho)}) \neq \perp$ *and magnitude bound* B_{max} *with* $p/B_{\mathsf{max}} \geq \lambda^{\omega(1)}$ *and* $q/(B_{\mathsf{max}} \cdot p) \geq \lambda^{\omega(1)}$*, and for any integer* $r \geq 2$*, there exist a PPT adversary* $\mathcal{B}$ *on the pseudorandomness of* PRF *such that*

$$\Pr^{\mathsf{cor}}_{\mathsf{HSS},(x^{(i)})_i,P,r}(\lambda) \geq 1 - \left(\mathrm{Adv}^{\mathsf{prf}}_{\mathsf{PRF},\mathcal{B}}(\lambda) + \lambda^{-\omega(1)}\right).$$

- ***Security:*** *For every PPT adversary* $\mathcal{A}$ *on the security of* HSS*, there exists an PPT adversary* $\mathcal{B}$ *on the security of* $\mathsf{PKE.OKDM}$ *such that*

$$\mathrm{Adv}^{\mathsf{sec}}_{\mathsf{HSS},\mathcal{A}}(\lambda) \leq \mathrm{Adv}^{\mathsf{kdm-ind}}_{\mathsf{PKE.OKDM},\mathcal{B}}(\lambda).$$

Proof. We present the construction of the HSS in Figure 2. For the proof of correctness we refer to Lemma 5.

For the proof of security we employ a hybrid argument. We define the corresponding games in Figure 3. Game $\mathbf{G}^0_{\mathsf{HSS},\mathcal{A}}(\lambda)$ corresponds to the HSS security game, therefore we have

$$\mathrm{Adv}^{\mathsf{sec}}_{\mathcal{A},\mathsf{HSS}}(\lambda) = \left|\Pr\left[\mathbf{G}^0_{\mathsf{HSS},\mathcal{A}}(\lambda) = 1\right] - 1/2\right|.$$

From a PPT adversary $\mathcal{A}$ distinguishing between $\mathbf{G}^0_{\mathsf{HSS},\mathcal{A}}(\lambda)$ and $\mathbf{G}^1_{\mathsf{HSS},\mathcal{A}}(\lambda)$ we can construct a PPT adversary $\mathcal{B}$ on the security of $\mathsf{PKE.OKDM}$ as follows. On input $(b, x_0, x_1, \mathsf{state})$ by $\mathcal{A}$ and input of the public key pk by the security challenge experiment of the KDM oracle, $\mathcal{B}$ chooses $\beta \in \{0, 1\}$, $\mathbf{s}_0 \xleftarrow{\$} R_q^d$, sets $\mathbf{s}_1 := \mathbf{s} - \mathbf{s}_0 \mod q$ and queries $\mathbf{c}_j \leftarrow \mathcal{O}_{\mathsf{KDM}}(x_\beta, j)$ for all $j \in \{1, \ldots, d\}$. Finally, $\mathcal{B}$ sends pk, $\mathsf{ek}_b := (K, \mathbf{s}_b)$ and $\mathbf{C}$ to $\mathcal{A}$, where $\mathbf{C} := (\mathbf{c}_1 | \ldots | \mathbf{c}_d) \in R_q^{d \times d}$. If the security challenge experiment of the KDM oracle returns real

$\underline{\mathsf{HSS.Gen}(1^\lambda):}$

- Generate a key pair $(\mathsf{pk}, \mathbf{s}) \leftarrow \mathsf{PKE.Gen}(1^\lambda)$ for encryption and draw a PRF key $K \xleftarrow{\$} \mathcal{K}$. //Recall $\mathbf{s} = (1, \widehat{\mathbf{s}}) \in R_q \times R_q^{d-1}$.
- **Secret share the secret key.** Choose $\mathbf{s}_0 \xleftarrow{\$} R_q^d$ at random. Define

$$\mathbf{s}_1 := \mathbf{s} - \mathbf{s}_0 \mod q.$$

- Output pk and $\mathsf{ek}_b \leftarrow (K, \mathbf{s}_b)$.

$\underline{\mathsf{HSS.Enc}(1^\lambda, \mathsf{pk}, x):}$

- **Encrypt the input.** Compute and output $\mathbf{C}^x \leftarrow \mathsf{PKE.}\mathbf{OKDM}(\mathsf{pk}, x)$.
  //This corresponds to $\mathbf{C}^x = \mathsf{PKE.}\mathbf{Enc}(\mathsf{pk}, x \cdot \mathbf{s}) \in R_q^{d \times d}$.

$\underline{\mathsf{HSS.Eval}(b, \mathsf{ek}_b, (\mathbf{C}^{x^{(1)}}, \ldots, \mathbf{C}^{x^{(\rho)}}), P, r):}$

Parse $(K, \mathbf{s}_b) =: \mathsf{ek}_b$, parse P as a sequence of RMS operations and proceed as follows.

- **Load an input into memory:** On instruction $(\mathsf{id}, \mathbf{C}^x)$ compute

$$\mathbf{t}_b^x := \mathsf{PKE.}\mathbf{DDec}(b, \mathbf{s}_b, \mathbf{C}^x) + (1-2b) \cdot \mathsf{PRF}(K, \mathsf{id}) \mod q.$$

- **Add values in memory:** On instruction $(\mathsf{id}, \mathbf{t}_b^x, \mathbf{t}_b^{x'})$ compute

$$\mathbf{t}_b^{x+x'} \leftarrow \mathbf{t}_b^x + \mathbf{t}_b^{x'} + (1-2b) \cdot \mathsf{PRF}(K, \mathsf{id}) \mod q.$$

- **Add input values:** On instruction $(\mathsf{id}, \mathbf{C}^x, \mathbf{C}^{x'})$ compute

$$\mathbf{C}^{x+x'} \leftarrow \mathbf{C}^x + \mathbf{C}^{x'} \mod q.$$

- **Multiply memory value by input:** On instruction $(\mathsf{id}, \mathbf{t}_b^x, \mathbf{C}^{x'})$ compute

$$\mathbf{t}_b^{x \cdot x'} := \mathsf{PKE.}\mathbf{DDec}(b, \mathbf{t}_b^x, \mathbf{C}^{x'}) + (1-2b) \cdot \mathsf{PRF}(K, \mathsf{id}) \mod q.$$

- **Output from memory, as element in R_r:** On instruction $(\mathsf{id}, \mathbf{t}_b^x)$ parse $\mathbf{t}_b^x =: (x_b, \widehat{\mathbf{t}_b^x})$ for some $x_b \in R_q$, $\widehat{\mathbf{t}_b^x} \in R_q^{d-1}$ and output

$$x_b \mod r.$$

Fig. 2: 2-party public-key homomorphic secret sharing scheme HSS for the class of RMS programs from encryption with nearly linear decryption. Here, $x \in R$ with $\|x\|_\infty \leq B_{\mathsf{inp}}$ is an input value. Throughout, *input values* $x \in R$ are represented by encryptions $\mathbf{C}^x$ of $x \cdot \mathbf{s}$ and *memory values* $x \in R$ are represented by shares $(\mathbf{t}_0^x, \mathbf{t}_1^x) \in R_q^d \times R_q^d$ with $\mathbf{t}_0^x + \mathbf{t}_1^x = x \cdot \mathbf{s} \mod q$.

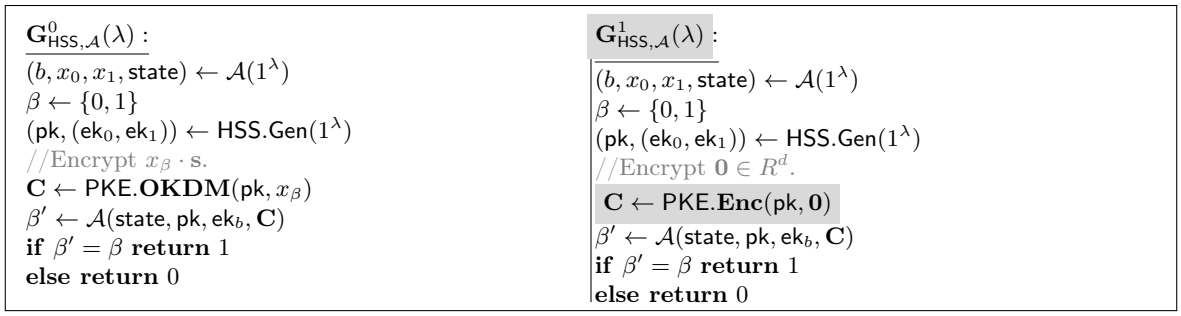

Fig. 3: Games $\mathbf{G}^0_{\mathsf{HSS},\mathcal{A}}(\lambda)$ and $\mathbf{G}^1_{\mathsf{HSS},\mathcal{A}}(\lambda)$ in the proof of Theorem 2 (Sec. of HSS).

encryptions of $x \cdot s_j$, the distribution of ek_b equals the distribution of game $\mathbf{G}^0_{\mathsf{HSS},\mathcal{A}}(\lambda)$. On the other hand, if the experiment returns encryptions of 0, the distribution of ek_b equals the distribution of game $\mathbf{G}^1_{\mathsf{HSS},\mathcal{A}}(\lambda)$. We have thus

$$\left|\Pr\left[\mathbf{G}^0_{\mathsf{HSS},\mathcal{A}}(\lambda) = 1\right] - \Pr\left[\mathbf{G}^1_{\mathsf{HSS},\mathcal{A}}(\lambda) = 1\right]\right| \leq \mathrm{Adv}^{\mathsf{kdm-ind}}_{\mathsf{PKE.OKDM},\mathcal{B}}(\lambda).$$

As in game $\mathbf{G}^1_{\mathsf{HSS},\mathcal{A}}(\lambda)$ the view of $\mathcal{A}$ is independent of β, it holds

$$\Pr\left[\mathbf{G}^1_{\mathsf{HSS},\mathcal{A}}(\lambda) = 1\right] = 1/2.$$

Lemma 5 (Correctness of the HSS). *Let* HSS *be the HSS from Figure 2. Let $N = 1$ if $R = \mathbb{Z}$, let $N = n$ if $R = \mathbb{Z}[X]/(X^n + 1)$. Then, for all $\lambda \in \mathbb{N}$, for all inputs $x^{(1)}, \ldots, x^{(\rho)} \in [R]_{B_{\mathsf{inp}}}$, for all RMS programs P, s.t.*

- *P is of size $|P| \leq \mathsf{poly}(\lambda)$*
- *P has magnitude bound B_{max} with $p/B_{\mathsf{max}} \geq \lambda^{\omega(1)}$ and $q/(B_{\mathsf{max}} \cdot p) \geq \lambda^{\omega(1)}$,*
- *P has maximum number of input addition instructions $P_{\mathsf{inp}+}$*

for $(\mathsf{pk}, \mathsf{ek}_0, \mathsf{ek}_1) \leftarrow \mathsf{HSS.Gen}(1^\lambda)$, for $\mathbf{C}^{x^{(i)}} \leftarrow \mathsf{HSS.Enc}(1^\lambda, \mathsf{pk}, x^{(i)})$, there exists an PPT adversary $\mathcal{B}$ on the pseudorandom function PRF *with such that correctness holds with probability at least*

$$\begin{aligned}\Pr^{\mathsf{cor}}_{\mathsf{HSS},(x^{(i)})_i,P}(\lambda) \geq 1 &- \mathrm{Adv}^{\mathsf{prf}}_{\mathsf{PRF},\mathcal{B}}(\lambda) - N \cdot (B_{\mathsf{max}} + 1)/q \\ &- |P| \cdot d \cdot N^2 \cdot P_{\mathsf{inp}+} \cdot B_{\mathsf{max}} \cdot (B_{\mathsf{ct}} \cdot p/q + B_{\mathsf{sk}}/p)\,. \\ &- |P| \cdot d \cdot N \cdot (p/q + 1/p).\end{aligned}$$

Proof. We prove correctness via a hybrid argument. Let $\varepsilon_0 := \Pr^{\mathsf{cor}}_{\mathsf{HSS},(x^{(i)})_i,P,r}(\lambda)$. Recall that by ε^0 we denote the probability that homomorphic evaluation of a program P on input $(x^{(1)}, \ldots, x^{(\rho)}) \in [R]^\rho_{B_{\mathsf{inp}}}$ employing our HSS presented in Figure 2 is successful (over the random choices of $\mathsf{HSS.Gen}, \mathsf{HSS.Enc}$). Our goal is to prove that for all $x^{(1)}, \ldots, x^{(\rho)} \in [R]_{B_{\mathsf{inp}}}$ and for all bounded RMS programs P the probability ε_0 is negligible in λ.

To this end, let $\varepsilon_1 := \Pr^1_{\mathsf{HSS},(x^{(i)})_i,P,r}(\lambda)$ denote the probability that evaluation yields the correct output, where we replace every evaluation of the PRF by inserting a value $\mathbf{r} \xleftarrow{\$} R^d_q$ chosen at random. We show that if the probabilities ε_0 and ε_1 differ significantly, then there exists an adversary $\mathcal{B}$ attacking the underlying PRF PRF. Namely, $\mathcal{B}$ homomorphically evaluates the program P on input $(x^{(1)}, \ldots, x^{(\rho)})$, but instead of evaluating $\mathsf{PRF}(K, \mathsf{id})$ the adversary $\mathcal{B}$ queries its PRF oracle. Finally, $\mathcal{B}$ returns *real* if homomorphic evaluation does not yield the correct result, and *random* otherwise. This yields

$$|\varepsilon_0 - \varepsilon_1| \leq \mathrm{Adv}^{\mathsf{prf}}_{\mathsf{PRF},\mathcal{B}}(\lambda).$$

It is left to give a lower bound for the probability ε_1. To that end, we prove that with overwhelming probability over the choice of $\mathbf{r} \leftarrow R_q^d$ (in place of the PRF evaluation) all shares $(\mathbf{t}_0^x, \mathbf{t}_1^x)$ computed during homomorphic evaluation of P satisfy

$$\mathbf{t}_0^x + \mathbf{t}_1^x = x \cdot \mathbf{s} = (x, x \cdot \widehat{\mathbf{s}}) \mod q \tag{1}$$

if the function evaluation of P at point $(\mathbf{t}_0^x, \mathbf{t}_1^x)$ corresponds to $x \in R$, where $\mathbf{s} = (1, \widehat{\mathbf{s}}) \in R \times R^{d-1}$ is the secret key returned by $\mathsf{PKE.Gen}$ on input 1^λ. Further, we have that $(\mathbf{t}_0^x, \mathbf{t}_1^x)$ are distributed uniformly at random conditioned on Equation 1.

Assuming Equation 1 is true, by Lemma 2 we have $x_0 + x_1 = x$ over R (and thus over R_r) with probability at least $1 - N \cdot (B_{\mathsf{max}} + 1)/q$.

It is left to prove that indeed Equation 1 holds true during homomorphic evaluation of P except with negligible probability. Recall that $\mathsf{PKE.DDec}$ is the procedure for distributed decryption from Lemma 4. First, assume that distributed decryption is always successful. In this case we prove that any instruction preserves correctness. Note that we do not need to consider the addition of input values and the output of a memory value, as those do not affect the shares.

- **Load an input into memory:** Consider intruction $(\mathsf{id}, \mathbf{C}^x)$ for $b \in \{0, 1\}$.
  Assuming correctness of distributed decryption it holds

$$\begin{aligned}\mathbf{t}_0^x + \mathbf{t}_1^x =& \mathsf{PKE.}\mathbf{DDec}(0, \mathbf{s}_0, \mathbf{C}^x) + \mathbf{r} + \mathsf{PKE.}\mathbf{DDec}(1, \mathbf{s}_1, \mathbf{C}^x) - \mathbf{r} \mod q \\ =& 1 \cdot (x \cdot \mathbf{s}) \mod q = x \cdot \mathbf{s} \mod q.\end{aligned}$$

- **Add values in memory:** Assuming correctness holds for shares $(\mathbf{t}_0^x, \mathbf{t}_1^x)$ and $(\mathbf{t}_0^{x'}, \mathbf{t}_1^{x'})$ we have, as required,

$$\begin{aligned}\mathbf{t}_0^{x+x'} + \mathbf{t}_1^{x+x'} &= \mathbf{t}_0^x + \mathbf{t}_0^{x'} + \mathbf{r} + \mathbf{t}_1^x + \mathbf{t}_1^{x'} - \mathbf{r} \mod q \\ &= x \cdot \mathbf{s} + x' \cdot \mathbf{s} \mod q = (x + x') \cdot \mathbf{s} \mod q.\end{aligned}$$

- **Multiply memory value by input:** Assuming correctness holds for the share $(\mathbf{t}_0^x, \mathbf{t}_1^x)$ and assuming correctness of distributed decryption it holds

$$\begin{aligned}\mathbf{t}_0^{x \cdot x'} + \mathbf{t}_1^{x \cdot x'} =& \mathsf{PKE.}\mathbf{DDec}(0, \mathbf{t}_0^x, \mathbf{C}^{x'}) + \mathsf{PKE.}\mathbf{DDec}(1, \mathbf{t}_1^x, \mathbf{C}^{x'}) \mod q \\ =& x \cdot (x' \cdot \mathbf{s}) \mod q = (x \cdot x') \cdot \mathbf{s} \mod q.\end{aligned}$$

  As $\mathbf{r}$ is chosen at random, the distribution of $(\mathbf{t}_0^y, \mathbf{t}_1^y) \in R_q^d$ for $y \in \{x, x + x', x \cdot x'\}$ is random conditioned on Equation 1.

It is left to bound the probability that distributed decryption fails. As for all x computed throughout the evaluation of program P the distribution of $(\mathbf{t}_0^x, \mathbf{t}_1^x) \in R_q^d$ is random conditioned on Equation 1, by Lemma 4 for all messages $m_1 \ldots, m_{P_{\mathsf{inp}+}} \in R_p$ and for all encryptions $\mathbf{c}_i$ of m_i that are output of $\mathsf{PKE.OKDM}$ distributed decryption of $\sum_{i=1}^{P_{\mathsf{inp}+}} \mathbf{c}_i$ fails with probability at most

$$N^2 \cdot P_{\mathsf{inp}+} \cdot \|x\|_\infty \cdot B_{\mathsf{ct}} \cdot p/q + N \cdot \|x \cdot m\|_\infty / p + N \cdot (p/q + 1/p),$$

where $m := \sum_{i=1}^{P_{\mathsf{inp}+}} m_i$. Throughout the evaluation of P we are guaranteed $\|x\|_\infty \leq B_{\mathsf{max}}$ for all intermediary values $x \in R$. Further, for the messages $m_i = x_i \cdot s_{j_i}$ corresponding to outputs of $\mathsf{PKE.OKDM}$ we have

$$\|x \cdot \sum_{i=1}^{P_{\mathsf{inp}+}} x_i \cdot s_{j_i}\|_\infty \leq \sum_{i=1}^{P_{\mathsf{inp}+}} \|x \cdot x_i \cdot s_{j_i}\|_\infty \leq P_{\mathsf{inp}+} \cdot N \cdot B_{\mathsf{max}} \cdot B_{\mathsf{sk}}.$$

Finally, applying a union bound over all $|P| \cdot d$ decryptions yields

$$\begin{aligned}\varepsilon_1 \geq 1 &- N \cdot (B_{\mathsf{max}} + 1)/q - |P| \cdot d \cdot N^2 \cdot P_{\mathsf{inp}+} \cdot B_{\mathsf{max}} \cdot (B_{\mathsf{ct}} \cdot p/q + B_{\mathsf{sk}}/p) \\ &- |P| \cdot d \cdot N \cdot (p/q + 1/p).\end{aligned}$$

3.4 Extensions

In the following we briefly describe some extensions which are tailored to special applications and improve the HSS construction introduced in the previous section in terms of efficiency. For a complete treatment, we refer the reader to Section C in the Appendix.

Secret-key HSS. For certain applications, where all secret inputs originate from a single party, it is sufficient to consider a *secret-key* HSS. This allows a more efficient instantiation for two reasons. First, the underlying encryption scheme is not required to support ciphertexts from a KDM oracle (but has to be KDM secure), which slightly saves in noise parameters. Further, we can save in terms of computations (at the cost of a larger share size), by replacing the DDec steps for loading an input x into memory, by instead sending the secret shares of $x \cdot \mathbf{s}$ as an additional part of the HSS share.

HSS for degree-2 polynomials. For the restricted class of degree-2 polynomials, we can achieve improved efficiency in both the secret-key and public-key setting, by leveraging the fact that our HSS need only support terminal multiplications.

For the secret-key case, as we do not need to load inputs, we actually only need one level of distributed decryption. This has two advantages: First, it suffices to encrypt $x \in R_p$ instead of $x \cdot \mathbf{s} \in R_p^d$, as the output is not required to allow another distributed encryption. Second, for the same reason, we do not need to lift the modulus of the output of the distributed decryption back to q. Thus, we can take $p \leq \mathsf{poly}(\lambda)$ and $q \geq \lambda^{\omega(1)}$ (as we no longer must apply Lemma 2).

The idea of our public-key HSS is to change the way inputs are loaded into memory. The idea is to obtain the shares of $x \cdot \mathbf{s} = (x, x \cdot s_2, \ldots, x \cdot s_d) \in R^d$ by decrypting $\mathsf{PKE.Enc}(\mathsf{pk}, x)$ with $\mathbf{s}$ *and* with $s_2 \cdot \mathbf{s}, \ldots, s_d \cdot \mathbf{s}$. This strategy requires a quadratic number of secret shares (namely shares of $\mathbf{s} \cdot \mathbf{s}^\top$), but reduces the number of required encryption from d to 1 (as only encryptions of x are required). An additional advantage of this approach is that we only have to require the underlying encryption scheme to be IND-CPA secure (instead of satisfying pseudorandomness of ciphertexts).

HSS supporting SIMD operations. We show that our basic HSS supports "single instruction, multiple input" (SIMD), if the underlying ring R is of the right form. Namely, we show that if $R = \mathbb{Z}[X]/(X^n + 1)$ for $n \in \mathbb{N}$, $n \leq \mathsf{poly}(\lambda)$ a power of 2, such that $X^n + 1$ splits over R_r (for some prime $r \geq 2$) into pairwise different irreducible polynomials of degree $k \in \mathbb{N}$ (i.e. $R_r \cong (\mathbb{F}_{r^k})^{n/k}$), one can evaluate a program P simultaneously on n/k inputs in $\mathbb{F}_{r^k}$. However, there are some caveats regarding magnitude growth with respect to the SIMD versus coefficient representations (see Section C.4).

Complexity. For an overview of key sizes and sizes of ciphertext/shares of our schemes $\mathsf{HSS}, \mathsf{skHSS}, \mathsf{HSS}^2$ and skHSS^2, we refer to Table 1. For an overview of the evaluation costs, we refer to Table 2. Recall that d is the size of a ciphertext of $\mathsf{PKE}/\mathsf{SKE}$. Further, recall that for skHSS^2 we can allow $p \leq \mathsf{poly}(\lambda)$ and therefore also smaller (but still super-polynomial) modulus q.

4 Instantiations and Efficiency Analysis

Our HSS schemes can be instantiated in a number of ways, using LWE or RLWE-based encryption schemes satisfying the nearly-linear decryption property from Definition 4. In this section we focus on a particularly efficient RLWE-based instantiation using the "LPR" encryption scheme [39]. In Section D of the Appendix we also show how to use standard Regev encryption based on LWE [41], but this is less efficient in terms of share size.

4.1 Instantiation from Ring-LWE

Definition 5 (Decisional Ring Learning With Errors). *Let n be a power of 2, $q \geq 2$ be an integer, $R = \mathbb{Z}[X]/(X^n + 1)$ and $R_q = R/(qR)$. Let $\mathcal{D}_{\mathsf{err}}$ be an error distribution over R and $\mathcal{D}_{\mathsf{sk}}$ be a secret key distribution over R. Let $s \leftarrow \mathcal{D}_{\mathsf{sk}}$. The $\mathsf{RLWE}_{n,q,\mathcal{D}_{\mathsf{err}},\mathcal{D}_{\mathsf{sk}}}$ problem is to distinguish the following two distributions over R_q^2:*

	HSS (Fig. 2)	skHSS (Fig. 8)	HSS^2 (Fig. 10)	skHSS^2 (Fig. 11)
pk/sk:	$\lvert\mathsf{pk}\rvert$	d	$\lvert\mathsf{pk}\rvert$	d
ek_b:	$d + \lvert K\rvert$	$d + \lvert K\rvert$	$d^2 + \lvert K\rvert$	$d + \lvert K\rvert$
$\mathsf{ct}/\mathsf{sh}_b$:	d^2	$d^2 + d$	d	$2d$

Table 1: Overview of sizes of keys and of ciphertexts/shares. Here, $\lvert\mathsf{pk}\rvert$ denotes public key size of the underlying encryption scheme, $\lvert K\rvert$ denotes PRF key size. Values are expressed in units of R_q elements.

	HSS (Fig. 2)	skHSS (Fig. 8)	HSS^2 (Fig. 10)	skHSS^2 (Fig. 11)
Load	$d^2 \cdot \mathsf{mult}_q$	0	$d^2 \cdot \mathsf{mult}_q$	0
Add (mem,nt)	$d \cdot \mathsf{add}_q$	$d \cdot \mathsf{add}_q$	$d \cdot \mathsf{add}_q$	$d \cdot \mathsf{add}_q$
Add (mem,t)	$1 \cdot \mathsf{add}_r$	$1 \cdot \mathsf{add}_r$	$1 \cdot \mathsf{add}_r$	$1 \cdot \mathsf{add}_p$
Add (input)	$d^2 \cdot \mathsf{add}_q$	$d^2 \cdot \mathsf{add}_q$	$d \cdot \mathsf{add}_q$	$d \cdot \mathsf{add}_q$
Multiply (nt)	$d^2 \cdot \mathsf{mult}_q$	$d^2 \cdot \mathsf{mult}_q$	–	–
Multiply (t)	$d \cdot \mathsf{mult}_q$	$d \cdot \mathsf{mult}_q$	$d \cdot \mathsf{mult}_q$	$d \cdot \mathsf{mult}_q$

Table 2: Overview of evaluation costs, where we restrict to the dominant cost and omit the cost for evaluating the PRF. For $\mathsf{mod} \in \{r, p, q\}$ by $\mathsf{add}_{\mathsf{mod}}$ and $\mathsf{mult}_{\mathsf{mod}}$ we denote the number of additions and multiplications over R_{mod} required, respectively. By "nt" and "t" we denote *non-terminal* and *terminal* operations (i.e. not followed by another multiplication).

$\underline{\mathsf{LPR.Gen}(1^\lambda):}$

1. Sample $a \leftarrow R_q, \widehat{s} \leftarrow \mathcal{D}_{\mathsf{sk}}, e \leftarrow \mathcal{D}_{\mathsf{err}}$ and compute $b = a \cdot \widehat{s} + e$ in R_q.
2. Let $\mathbf{s} = (1, \widehat{s})$ and output $\mathsf{pk} = (a, b), \mathsf{sk} = \mathbf{s}$.

$\underline{\mathsf{LPR.Enc}(\mathsf{pk}, m):}$

1. To encrypt $m \in R_p$, first sample $v \leftarrow \mathcal{D}_{\mathsf{sk}}, e_0, e_1 \leftarrow \mathcal{D}_{\mathsf{err}}$.
2. Output the ciphertext $(c_0, c_1) \in R_q^2$, where $c_1 = -av + e_0$ and $c_0 = bv + e_1 + (q/p) \cdot m$.

$\underline{\mathsf{LPR.OKDM}(\mathsf{pk}, m):}$

1. Compute $\mathbf{c}^0 = \mathsf{LPR.Enc}(0)$ and $\mathbf{c}^m = \mathsf{LPR.Enc}(m)$.
2. Output the tuple $(\mathbf{c}^m, \mathbf{c}^0 + (0, (q/p) \cdot m))$ as encryptions of $m \cdot \mathbf{s}$.

$\underline{\mathsf{LPR.DDec}(b, \mathbf{t}_b, \mathbf{c}^x):}$

1. Given $b \in \{0, 1\}$, a ciphertext $\mathbf{c}^x$ and a share $\mathbf{t}_b$ of $m \cdot \mathbf{s}$, first parse $\mathbf{c}^x = (c_0, c_1)$ and $\mathbf{t}_b = (t_{b,0}, t_{b,1})$.
2. Output $(d_0, d_1) := (\lfloor (p/q) \cdot (c_0 \cdot t_{b,0} + c_1 \cdot t_{b,1}) \rceil \mod p) \mod q$

Fig. 4: Ring-LWE based instantiation of PKE with approximately linear decryption, with procedures for HSS from Section 3

– $\mathcal{O}_{\mathcal{D}_{\mathsf{err}}, s}$: *Output* (a, b) *where* $a \leftarrow R_q, e \leftarrow \mathcal{D}_{\mathsf{err}}$ *and* $b = a \cdot s + e$
– U: *Output* $(a, u) \leftarrow R_q^2$

Formally, for a PPT adversary $\mathcal{A}$ *we define the advantage* $\mathrm{Adv}^{\mathsf{rlwe}}_{n,q,\mathcal{D}_{\mathsf{err}},\mathcal{D}_{\mathsf{sk}}}(\lambda) = |\Pr_{s \leftarrow \mathcal{D}_{\mathsf{sk}}}[\mathcal{A}^{\mathcal{O}_{\mathcal{D}_{\mathsf{err}}, s}}(\lambda) = 1] - \Pr_{s \leftarrow \mathcal{D}_{\mathsf{sk}}}[\mathcal{A}^{U}(\lambda) = 1]|$.

In Figure 4 we present the core algorithms for our RLWE-based instantation using the LPR [39] public-key encryption scheme $\mathsf{LPR} = (\mathsf{LPR.Gen}, \mathsf{LPR.Enc})$, as well as the auxiliary algorithms LPR.OKDM and LPR.DDec

used by our HSS constructions. We use an error distribution $\mathcal{D}_{\mathsf{err}}$ where each coefficient is a rounded Gaussian with parameter σ, which gives $B_{\mathsf{err}} = 8\sigma$ as a high-probability bound on the ℓ_∞ norm of samples from $\mathcal{D}_{\mathsf{sk}}$, with failure probability $\mathtt{erf}(8/\sqrt{2}) \approx 2^{-49}$. We choose the secret-key distribution such that each coefficient of s is uniform in $\{0, \pm 1\}$, subject to the constraint that only h_{sk} coefficients are non-zero.[9]

The following lemma (proven in Section 4 of the Appendix) shows that LPR satisfies the nearly-linear decryption property for our HSS scheme. Furthermore, notice that ciphertexts output by LPR.Enc are pseudorandom under the decisional ring-LWE assumption, by a standard hybrid argument [40]. Therefore, the correctness and security properties of the LPR.OKDM and LPR.DDec procedures follow from Lemmas 3 and 4.

Lemma 6. *Assuming hardness of* $\mathsf{RLWE}_{n,q,\mathcal{D}_{\mathsf{err}},\mathcal{D}_{\mathsf{sk}}}$*, the scheme* LPR *(Figure 4) is a public-key encryption scheme with nearly-linear decryption over* $R = \mathbb{Z}[X]/(X^n + 1)$*, with ciphertext dimension* $d = 2$ *and bounds* B_{sk} *and* $B_{\mathsf{ct}} = B_{\mathsf{err}} \cdot (2h_{\mathsf{sk}} + 1)$*.*

4.2 Parameters and Efficiency Analysis

We now analyse the efficiency of our RLWE-based instantiation and compare it with using HSS constructed from somewhat homomorphic encryption, for various different settings of parameters.

For comparison with HSS based on DDH [9], we remark that for non-SIMD computations, DDH-based HSS shares can be smaller than both our approach and SHE. However, we estimate that homomorphic evaluation is around an order or magnitude faster than the times reported in [8] due to the expensive share conversion procedure, and when using SIMD both this and the share size can be dramatically improved.

Parameter estimation. We derived parameters for our HSS based on LPR using the bounds for correctness from Lemma 5, chosen to ensure that each RMS multiplication of a ring-element during evaluation is correct with probability $1 - 2^{-\kappa}$, where we chose $\kappa = 40$. To compare with constructing HSS from SHE, we estimated parameters for the "BFV" scheme based on RLWE [14, 26], currently one of the leading candidate SHE schemes. To modify this to achieve HSS with additive output sharing, we need to increase the size of q by around 2^κ bits. With both schemes we chose parameters estimated to have at least 80 bits of computational security, see Section D in the Appendix for more details.

Share size. Tables 3–4 show BFV ciphertext parameters for different multiplicative depths of circuit, and plaintext modulus 2 or $\approx 2^{128}$, respectively, to illustrate different kinds of Boolean and arithmetic computations. Table 5 gives our HSS parameters for various choices of B_{max}, the maximum value any plaintext coefficient can hold during the computation. Note that in contrast to SHE, our parameters depend only on this bound and not the multiplicative depth, although we are more restricted in that we can only perform homomorphic multiplications where one value is an input.

This means that comparing parameters of the two schemes is very application-dependent. For instance, for Boolean computations where we can have $B_{\mathsf{max}} = 2$, our scheme has smaller parameters than SHE for all computations of depth > 3, so this can give a significant advantage for very high degree functions that can be expressed as an RMS program. However, if SIMD computations are required then B_{max} must be chosen to account for the worst-case coefficient growth, which is not directly related to the plaintexts, so our scheme would likely have larger ciphertexts than SHE in most cases. For operations on large integers, the parameters in both schemes quickly get very large, though our parameters grow slightly quicker due to the increase in B_{max}.

Computational efficiency. The relative computational efficiency of the schemes is much clearer, and is the main advantage of our scheme over SHE. The cost of a homomorphic RMS multiplication with RLWE is roughly twice the cost of a decryption in any RLWE-based scheme (including BFV) with the same parameters. Recently, Halevi et al. [32] described an optimized implementation of BFV using CRT arithmetic, where according to their single-threaded runtimes, decryption costs between 20–30x less than multiplication

[9] Choosing a sparse secret like this does incur a small loss in security, and only gives us a small gain in parameters for the HSS. The main reason we choose s like this is to allow a fair comparison with SHE schemes, which typically have to use sparse secrets to obtain reasonable parameters.

(including key-switching) for the ranges of parameters we consider (cf. [32, Table 3]). This indicates a *10–15x improvement in performance* for homomorphic evaluation with our scheme compared with SHE, assuming similar parameters and numbers of multiplications. We remark that this comparison deserves some caution, since other SHE schemes such as BGV [15] may have different characteristics; we have not run experiments with BGV, but due to the complications in key-switching and modulus-switching we expect the improvement to still be around an order of magnitude.

Depth	N	$\log q$	Security
1	4096	102	145.1
2	4096	118	122.6
3	4096	134	106.2
4	4096	150	93.73
5	4096	164	85.53
6	8192	186	157.5
7	8192	202	142.9
8	8192	220	129.8
9	8192	236	120.1
10	8192	252	111.9

Table 3: BFV parameters with plaintext modulus 2

Depth	N	$\log q$	Security
1	16384	456	124.3
2	16384	602	92.44
3	32768	750	154.2

Table 4: BFV parameters with plaintext modulus $\approx 2^{128}$

B_{max}	N	$\log q$	Security
2	4096	137	103.3
2^{16}	4096	167	83.74
2^{32}	8192	203	142.0
2^{64}	8192	267	104.9
2^{128}	16384	399	143.9
2^{256}	16384	655	84.60

Table 5: RLWE based HSS parameters for RMS programs with maximum plaintext size B_{max}

5 Applications

In this section we highlight some applications of HSS for which our scheme seems well-suited. There are four primary approaches to compare: approaches not relying on HSS, using DDH-based or one-way function-based HSS, using HSS based on SHE, or using our new HSS. We remark that the concrete practicality of SHE-based HSS approaches has also not been considered before this work.

5.1 Secure 2-PC for low-degree polynomials

Perhaps the most natural application of HSS is to achieve a very succinct form of multi-party computation. After a setup phase to create the key material $\mathsf{pk}, (\mathsf{ek}_0, \mathsf{ek}_1)$, each party publishes HSS-shares of its input, which can then be directly used to compute additive shares of the output. Even the simplest case of evaluating degree-2 polynomials has many interesting applications, and also allows us to use our optimized HSS scheme from Section 3.4, where shares consist of *a single* RLWE ciphertext, instead of two. The main motivating example we look at is to MPC protocols in the *preprocessing model*, where correlated randomness is pre-generated ahead of time to help increase efficiency when the actual computation takes place. This correlated randomness can take many forms, but the most common are Beaver triples, namely additive shares of (a, b, c) where $c = a \cdot b$ and a, b are random elements of a (typically) large prime field. These can easily be generated using degree-2 HSS, where each party inputs two field elements, and are also highly amenable to SIMD processing.

Looking at Tables 4–5, for an example of degree 2 functions over a 128-bit message space, BFV with depth 1 requires a dimension $N = 16384$ and modulus $\log q = 456$, whereas our scheme would need to use $B_{\mathsf{max}} \approx 2^{256}$, giving the same dimension and a slightly larger modulus of around 655 bits. Therefore, our communication cost will be slightly larger than using SHE-based HSS, but we expect to gain from the lower computational costs that come with our multiplication.

Using DDH-type HSS [8], an m-bit triple can be created with $3712(5m/4 + 160)$ bits of communication, giving 148kB for $m = 128$, meaning our communication is 20x higher for producing a single triple (at

2682kB), but orders of magnitude smaller (∼900x) when amortized using SIMD (over $n = 16834$ triples). Computation requirements will greatly favor our approach.

We can also compare this with other approaches to Beaver triple generation. The SPDZ protocol [22] uses SHE (without HSS) to create triples; as well as the more complex homomorphic multiplication, this incurs extra costs in an interactive distributed decryption protocol, which adds a round of interaction that we can avoid using HSS with local rounding. The latest version of SPDZ [35] uses linearly-homomorphic encryption instead of SHE, and reports ciphertexts with $\log q$ as small as 327 bits, around half the size of ours. This would likely beat HSS in terms of communication and computation, but still has the undesirable feature of 2 rounds of interaction, whereas with HSS (and a small one-time setup), the triples are obtained after just one message from each party.

The recent work of Boyle et al. [8] considered an interesting alternative approach to triple generation using so-called "cryptographic capsules", where HSS evaluation of a local PRG is used to expand a small, initial amount of correlated randomness into many more triples. This allows communication complexity *sublinear in the number triples*. They showed that this can be done with $O(\beta^2)$ Boolean RMS multiplications, where β is a parameter related to the locality of the PRG. With a DDH-like scheme, their protocol involves significant complications to ensure correct triples in the presence of a non-negligible failure probability for multiplication, making it quite impractical. However, using our HSS or SHE-based HSS with negligible error considerably simplifies this approach; it is not immediately clear of the best way to instantiate the parameters, but since it is a Boolean computation with relatively small degree it seems well-suited to our HSS scheme. We leave this exploration, as well as extending to other distributions, as an interesting direction of future research.

5.2 2-server PIR

An attractive application of HSS is to obtain highly succinct Private Information Retrieval (PIR) protocols for $m \geq 2$ servers. Here, m servers hold a public database DB and allow clients to submit private queries to DB, such that both the query and response remain hidden to up to $m - 1$ colluding servers.[10] When using HSS, we can obtain a very simple, 1-round protocol where the client first sends an encryption of its query to both servers, who respond with an additive share of the result. Note that we only need the more efficient, secret-key version of HSS, such as our scheme from Section 3.4 with $m = 2$ servers.

Recent works on 2-server PIR have used HSS for point functions[11] to support basic queries including equality conditions, range queries and disjoint OR clauses, based on simple schemes using only one-way functions [11, 43]. However these techniques degrade dramatically for more complex queries, due to the relatively weak homomorphic ability of the underlying HSS. With HSS for branching programs we can significantly increase the expressiveness of queries, at the cost of some overhead in ciphertext size and running time.

In a bit more detail, suppose that a client issues a simple $COUNT$ query,[12] which applies some predicate Q to each row $x_i \in \mathsf{DB}$, and returns $\sum_i Q(x_i)$, that is, the number of rows in DB that match Q. The general idea is that the client splits Q into HSS shares s^1, s^2, and sends s^j to server j. For each row $x_i \in \mathsf{DB}$, the servers then use homomorphic evaluation with the function $f_{x_i}(Q) := Q(x_i)$ on the shares, to obtain a shared 0/1 value indicating whether a match occurred. Given additive shares modulo r of the results $q_1, \ldots, q_D$ (where $D = |\mathsf{DB}|$), the servers can sum up the shares and send the result to the client, who reconstructs the result $q = \sum q_i$ (this assumes that $r < n$, so wraparound does not occur).

Below we analyse some useful classes of predicates that are much more expressive than function classes that can be handled using one-way function based approaches, and seem well-suited for our scheme supporting RMS programs.

[10] Using S/FHE alone instead of HSS allows for the stronger setting of single-server PIR. However, a major advantage of HSS with additive reconstruction is that shares across many rows can easily be combined, allowing more expressive queries with simpler computation.

[11] Actually, these works use *function secret-sharing* [10] for point functions, which in this case is equivalent to HSS for the same class of functions.

[12] Other queries such as returning the record identifier, or min/max and range queries can easily be supported with similar techniques, as previously shown in [43, 8].

Conjunctive keyword search. Suppose that each entry in DB is a document x with a list of keywords $W_x = \{w_1^x, \ldots, w_m^x\}$, and the query is a *COUNT* query consisting of an arbitrary conjunction of keywords, each in $\{0,1\}^\ell$. That is, for a query $W = \{w_1, \ldots, w_k\}$ containing keywords shared bit-by-bit using the HSS, the servers will compute a sharing of

$$\#\{(x, W_x) \in \mathsf{DB} : W \subseteq W_x\}$$

To evaluate the query on a single entry of DB as an RMS program, we maintain the result f as a secret-shared memory value, which is initially set to 1. We then iterate over each query keyword $w_i \in W$, letting w_{ij} denote the j-th bit of w_i, and update f as

$$f := \sum_{w^x \in W_x} f \cdot \prod_{j=1}^{m} (1 \oplus w_j^x \oplus w_{ij})$$

Note that the i-th product evaluates to 1 iff $x^x = w_i$, and since all w^x are distinct, at most one of these will be 1. Multiplication by f applies a conjunction with the previous keyword, and must be performed inside the summation as f is a memory value. All other product terms are linear functions (over $\mathbb{Z}$) in the inputs w_i (via $a \oplus b = a + b - 2ab$), so each product can be evaluated left-to-right as an RMS program, for a total of $m \cdot \ell \cdot k$ RMS multiplications after iterating over all k query keywords.

Comparison to SHE-based HSS. When using SHE, the number of homomorphic multiplications is roughly the same as our case, and the multiplicative depth is $\log(m\ell k)$. For a concrete example, suppose that each document has $m = 10$ keywords of length $\ell = 128$ bits, and a client's query has $k = 4$ keywords. Using either our HSS scheme or HSS from SHE would need around 5120 multiplications per document, with a multiplicative depth of 13. This needs SHE parameters of $\log q \approx 300$ and dimension $n = 8192$ for the BFV scheme as above, whereas with our scheme we can use the best case of $B_{\mathsf{max}} = 2$, giving $\log q \approx 137$ and $n = 4096$. Using our secret-key HSS (Figure 8) and LPR instantiation, the share size is $3n \log q$ bits ≈ 210kB, around $1/3$ of the SHE ciphertext size using BFV. The communication cost for the whole query would be 107MB for our HSS, and 314MB with BFV, whilst we estimate the computational costs of homomorphic evaluation per document are around 2.5s and 300s, respectively, so even with the relatively high communication cost, for matching several documents using our HSS would certainly give a significant performance improvement.

However, one drawback of our approach is that handling SIMD computations is more challenging, since the B_{max} bound must be chosen much larger to account for the coefficient growth of the plaintext polynomials, which may continue to grow even when the packed plaintext messsages themselves are only bits. If the number of documents in the database is large enough to warrant SIMD processing then it seems likely that SHE will be preferable, since $n = 8192$ documents could be searched at once without increasing the parameters.

Pattern-matching queries. Suppose here that the client wants to search for the occurrence of a pattern $p = (p_1, \ldots, p_m) \in \{0,1\}^m$ in each row $x = (x_1, \ldots, x_n) \in \{0,1\}^n$. An RMS program for computing the pattern-matching predicate, with public input x and private input p, can be done with $m \cdot n$ multiplications using a similar method to the previous example, modified slightly to compute the OR of matching p with every position in x.

Comparison to SHE-based HSS. When using SHE, this computation has depth $\log(nm)$, also requiring around $n \cdot m$ homomorphic multiplications. The comparison with our scheme is then similar to the keyword search example, depending on the parameters chosen. For another example, if we have a fairly large string of length $n = 10000$, and a pattern of size $m = 100$, then the SHE-based HSS must support depth 20, giving parameters $(n, \log q) = (16384, 434)$. Again, we can use our HSS with parameters for $B_{\mathsf{max}} = 2$, which lead to ciphertexts around 8.5x smaller than with SHE.

References

[1] Martin R. Albrecht, Rachel Player, and Sam Scott. "On the concrete hardness of Learning with Errors". In: *J. Mathematical Cryptology* 9.3 (2015), pp. 169–203. DOI: http://dx.doi.org/10.1007/s10623-015-0048-8. URL: http://www.degruyter.com/view/j/jmc.2015.9.issue-3/jmc-2015-0016/jmc-2015-0016.xml.

[2] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. "Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems". In: *CRYPTO 2009*. LNCS. Springer, Heidelberg, Aug. 2009.

[3] Gilad Asharov, Abhishek Jain, Adriana López-Alt, Eran Tromer, Vinod Vaikuntanathan, and Daniel Wichs. "Multiparty Computation with Low Communication, Computation and Interaction via Threshold FHE". In: *EUROCRYPT 2012*. LNCS. Springer, Heidelberg, Apr. 2012.

[4] Abhishek Banerjee, Chris Peikert, and Alon Rosen. "Pseudorandom Functions and Lattices". In: *EUROCRYPT 2012*. LNCS. Springer, Heidelberg, Apr. 2012.

[5] Florian Böhl, Gareth T. Davies, and Dennis Hofheinz. "Encryption Schemes Secure under Related-Key and Key-Dependent Message Attacks". In: *PKC 2014*. LNCS. Springer, Heidelberg, Mar. 2014.

[6] Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky. "Circular-Secure Encryption from Decision Diffie-Hellman". In: *CRYPTO 2008*. LNCS. Springer, Heidelberg, Aug. 2008.

[7] Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai. "Compressing Vector OLE". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018*. 2018.

[8] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, and Michele Orrù. "Homomorphic Secret Sharing: Optimizations and Applications". In: *ACM CCS 17*. ACM Press, 2017.

[9] Elette Boyle, Niv Gilboa, and Yuval Ishai. "Breaking the Circuit Size Barrier for Secure Computation Under DDH". In: *CRYPTO 2016, Part I*. LNCS. Springer, Heidelberg, Aug. 2016.

[10] Elette Boyle, Niv Gilboa, and Yuval Ishai. "Function Secret Sharing". In: *EUROCRYPT 2015, Part II*. LNCS. Springer, Heidelberg, Apr. 2015.

[11] Elette Boyle, Niv Gilboa, and Yuval Ishai. "Function Secret Sharing: Improvements and Extensions". In: *ACM CCS 16*. ACM Press, Oct. 2016.

[12] Elette Boyle, Niv Gilboa, and Yuval Ishai. "Group-Based Secure Computation: Optimizing Rounds, Communication, and Computation". In: *EUROCRYPT 2017, Part II*. LNCS. Springer, Heidelberg, 2017.

[13] Elette Boyle, Niv Gilboa, Yuval Ishai, Huijia Lin, and Stefano Tessaro. "Foundations of Homomorphic Secret Sharing". In: *ITCS 2018*. LIPIcs, Jan. 2018.

[14] Zvika Brakerski. "Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP". In: *CRYPTO 2012*. LNCS. Springer, Heidelberg, Aug. 2012.

[15] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. "(Leveled) fully homomorphic encryption without bootstrapping". In: *ITCS 2012*. ACM, Jan. 2012.

[16] Zvika Brakerski and Vinod Vaikuntanathan. "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages". In: *CRYPTO 2011*. LNCS. Springer, Heidelberg, Aug. 2011.

[17] Hao Chen, Kim Laine, and Rachel Player. "Simple Encrypted Arithmetic Library - SEAL v2.1". In: *FC 2017 Workshops*. LNCS. Springer, Heidelberg, Apr. 2017.

[18] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. "Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds". In: *ASIACRYPT 2016, Part I*. LNCS. Springer, Heidelberg, Dec. 2016.

[19] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. "Faster Packed Homomorphic Operations and Efficient Circuit Bootstrapping for TFHE". In: *ASIACRYPT 2017, Part I*. LNCS. Springer, Heidelberg, Dec. 2017.

[20] Richard Cleve. "Towards Optimal Simulations of Formulas by Bounded-Width Programs". In: *Computational Complexity* 1 (1991), pp. 91–105. DOI: 10.1007/BF01200059. URL: https://doi.org/10.1007/BF01200059.

[21] Henry Corrigan-Gibbs, Dan Boneh, and David Mazières. "Riposte: An Anonymous Messaging System Handling Millions of Users". In: *2015 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 2015.

[22] Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias. "Multiparty Computation from Somewhat Homomorphic Encryption". In: *CRYPTO 2012*. LNCS. Springer, Heidelberg, Aug. 2012.

[23] Itai Dinur, Nathan Keller, and Ohad Klein. "An Optimal Distributed Discrete Log Protocol with Applications to Homomorphic Secret Sharing". In: *CRYPTO 2018, Part III*. LNCS. Springer, Heidelberg, Aug. 2018.

[24] Yevgeniy Dodis, Shai Halevi, Ron D. Rothblum, and Daniel Wichs. "Spooky Encryption and Its Applications". In: *CRYPTO 2016, Part III*. LNCS. Springer, Heidelberg, Aug. 2016.

[25] Léo Ducas and Daniele Micciancio. "FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second". In: *EUROCRYPT 2015, Part I*. LNCS. Springer, Heidelberg, Apr. 2015.
[26] Junfeng Fan and Frederik Vercauteren. *Somewhat Practical Fully Homomorphic Encryption*. Cryptology ePrint Archive, Report 2012/144. `http://eprint.iacr.org/2012/144`. 2012.
[27] Nelly Fazio, Rosario Gennaro, Tahereh Jafarikhah, and William E. Skeith III. "Homomorphic Secret Sharing from Paillier Encryption". In: *Provable Security - 11th International Conference, ProvSec 2017, Proceedings*. 2017, pp. 381–399.
[28] Craig Gentry. "Fully homomorphic encryption using ideal lattices". In: *41st ACM STOC*. ACM Press, 2009.
[29] Craig Gentry, Shai Halevi, and Nigel P. Smart. "Homomorphic Evaluation of the AES Circuit". In: *CRYPTO 2012*. LNCS. Springer, Heidelberg, Aug. 2012.
[30] Craig Gentry, Amit Sahai, and Brent Waters. "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based". In: *CRYPTO 2013, Part I*. LNCS. Springer, Heidelberg, Aug. 2013.
[31] Niv Gilboa and Yuval Ishai. "Distributed Point Functions and Their Applications". In: *EUROCRYPT 2014*. LNCS. Springer, Heidelberg, May 2014.
[32] Shai Halevi, Yuriy Polyakov, and Victor Shoup. *An Improved RNS Variant of the BFV Homomorphic Encryption Scheme*. Cryptology ePrint Archive, Report 2018/117. `https://eprint.iacr.org/2018/117`. 2018.
[33] Shai Halevi and Victor Shoup. "Algorithms in HElib". In: *CRYPTO 2014, Part I*. LNCS. Springer, Heidelberg, Aug. 2014.
[34] Shai Halevi and Victor Shoup. "Bootstrapping for HElib". In: *EUROCRYPT 2015, Part I*. LNCS. Springer, Heidelberg, Apr. 2015.
[35] Marcel Keller, Valerio Pastro, and Dragos Rotaru. "Overdrive: Making SPDZ Great Again". In: *EUROCRYPT 2018, Part III*. LNCS. Springer, Heidelberg, 2018.
[36] Adeline Langlois and Damien Stehlé. "Worst-case to average-case reductions for module lattices". In: *Des. Codes Cryptography* 75.3 (2015), pp. 565–599.
[37] Hendrik W Lenstra Jr. "Finding isomorphisms between finite fields". In: *Mathematics of Computation* (1991), pp. 329–347.
[38] Tancrède Lepoint and Michael Naehrig. "A Comparison of the Homomorphic Encryption Schemes FV and YASHE". In: *AFRICACRYPT 14*. LNCS. Springer, Heidelberg, May 2014.
[39] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. "A Toolkit for Ring-LWE Cryptography". In: *EUROCRYPT 2013*. LNCS. Springer, Heidelberg, May 2013.
[40] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *EUROCRYPT 2010*. LNCS. Springer, Heidelberg, 2010.
[41] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *37th ACM STOC*. ACM Press, May 2005.
[42] Ronald L. Rivest, Len Adleman, and Michael L. Dertouzos. "On data banks and privacy homomorphisms". In: *Foundations of secure computation (Workshop, Georgia Inst. Tech., 1977)*. Academic, New York, 1978, pp. 169–179.
[43] Frank Wang, Catherine Yun, Shafi Goldwasser, Vinod Vaikuntanathan, and Matei Zaharia. "Splinter: Practical Private Queries on Public Data". In: *14th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2017*. 2017, pp. 299–313.

A Preliminaries

We say that ℓ is *negligible in* λ if its inverse vanishes asymptotically faster than any polynomial in λ, also denoted by $\ell \leq \lambda^{-\omega(1)}$. We say $\ell \leq \mathsf{poly}(\lambda)$, if there exists a polynomial $p[X] \in \mathbb{N}[X]$ and a $\lambda_0 \in \mathbb{N}$ such that for all $\lambda \geq \lambda_0$ we have $\ell(\lambda) \leq \mathsf{poly}(\lambda)$. If no such polynomial exist, we write $\ell \geq \lambda^{\omega(1)}$.

We say that $\mathcal{A}$ is *probabilistic polynomial time* (PPT), if $\mathcal{A}$ is a probabilistic algorithm with running time polynomial in λ. We use $y \leftarrow \mathcal{A}(x)$ to denote that y is assigned the output of $\mathcal{A}$ running on input x.

For $\ell \in \mathbb{N}$ a prime power, by $\mathbb{F}_\ell$ we denote a finite field consisting of ℓ elements.

For an arbitrary set $\mathcal{S}$, by $x \xleftarrow{\$} \mathcal{S}$ we denote the process of sampling an element x from $\mathcal{S}$ uniformly at random.

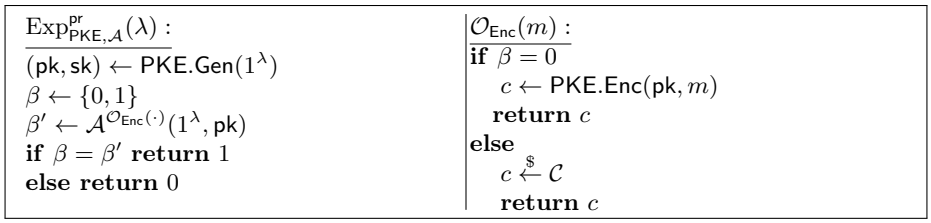

Fig. 5: Security challenge experiment for pseudorandomness of ciphertexts.

Definition 6 (Public-key encryption scheme). *We say a tuple of PPT algorithms* $\mathsf{PKE} := (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ *is a* public-key encryption scheme *with message space* $\mathcal{M}$ *and ciphertext space* $\mathcal{C}$*, if it is of the following syntax.*

- $\mathsf{PKE.Gen}(1^\lambda)$*: On input* 1^λ *the key generation algorithm* $\mathsf{PKE.Gen}$ *returns a key pair* $(\mathsf{pk}, \mathsf{sk})$*.*
- $\mathsf{PKE.Enc}(\mathsf{pk}, m)$*: On input of the public key* pk *and a message* $m \in \mathcal{M}$*, the encryption algorithm returns a ciphertext* $c \in \mathcal{C}$*.*
- $\mathsf{PKE.Dec}(\mathsf{sk}, c)$*: On input of the secret key* sk *and a ciphertext* $c \in \mathcal{C}$*, the deterministic decryption algorithm returns a message* $m \in \mathcal{C}$ *or* $\perp$*.*

Further, we require PKE *to satisfy* correctness*, that is for every* $\lambda \in \mathbb{N}$*, for every* $(\mathsf{pk}, \mathsf{sk})$ *in the image of* $\mathsf{PKE.Gen}$*, for every message* $m \in \mathcal{M}$ *and for every ciphertext* c *in the image of* $\mathsf{PKE.Enc}(\mathsf{pk}, m)$ *we require*

$$\mathsf{PKE.Dec}(\mathsf{sk}, c) = m.$$

Throughout this paper we only consider public-key encryption schemes that are secure *in the sense of Definition 7.*

Definition 7 (Pseudorandomness of ciphertexts). *We say a public-key encryption scheme* $\mathsf{PKE} := (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ *with ciphertext space* $\mathcal{C}$ *satisfies* pseudorandomness of ciphertexts *or simply* PKE *is* secure*, if for every PPT adversary* $\mathcal{A}$ *the advantage*

$$\mathrm{Adv}^{\mathsf{pr}}_{\mathsf{PKE},\mathcal{A}}(\lambda) := \left| \Pr\left[\mathrm{Exp}^{\mathsf{pr}}_{\mathsf{PKE},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2} \right|$$

is negligible in λ*, where* $\mathrm{Exp}^{\mathsf{pr}}_{\mathsf{PKE},\mathcal{A}}(\lambda)$ *is as defined in Figure 5.*

B HSS from encryption with nearly linear decryption

B.1 Computation on 2-party secret shared values

Lemma 1 (Rounding of noisy shares). *Let* $p, q \in \mathbb{N}$ *be modulus values with* $q/p \geq \lambda^{\omega(1)}$*. Let* $R \in \{\mathbb{Z}, \mathbb{Z}[X]/(X^n+1)\}$ *be of dimension* N*. Let* $t_0, t_1 \in R_q$ *random subject to*

$$t_0 + t_1 = (q/p) \cdot m + e \mod q$$

for some $m \in R_p, e \in R$ *with* $q/(p \cdot \|e\|_\infty) \geq \lambda^{\omega(1)}$*. Then there exists a deterministic polynomial time procedure* Round *that takes an input* $t_b \in R_q$ *and outputs a value in* R_p *such that it holds*

$$\mathsf{Round}(t_0) + \mathsf{Round}(t_1) = m \mod p$$

with probability at least $1 - N \cdot (\|e\|_\infty + 1) \cdot p/q \geq 1 - \lambda^{-\omega(1)}$ *over the choice of the shares* t_0, t_1*.*

Proof. We define Round to be the algorithm that on input $t_b \in R_q$ outputs

$$\lfloor (p/q) \cdot t_b \rceil \mod p \in R_p.$$

In order to prove correctness of Round we consider the values of t_0 and t_1 as elements in R. We express t_0 in the basis of (q/p), i.e. let $I := [-q/(2p), q/(2p))$, let $z_0 \in R_p$, $r_0 \in R|_I$ such that $t_0 = (q/p) \cdot z_0 + r_0$. Let $l \in R$ such that $t_1 = (q/p) \cdot (m - z_0) + e - r_0 + q \cdot l$ in R. Then we have

$$\begin{aligned}
\mathsf{Round}(t_0) &= \lfloor (p/q) \cdot ((q/p) \cdot z_0 + r_0) \rceil \mod p \\
&= \lfloor z_0 + \underbrace{(p/q) \cdot r_0}_{\in R|_{[-1/2,1/2)}} \rceil \mod p \\
&= z_0 \mod p
\end{aligned}$$

and

$$\begin{aligned}
\mathsf{Round}(t_1) &= \lfloor (p/q) \cdot ((q/p) \cdot (m - z_0) + e - r_0 + q \cdot l) \rceil \mod p \\
&= \lfloor m - z_0 + p \cdot l + (p/q) \cdot (e - r_0) \rceil \mod p.
\end{aligned}$$

Now, assume $e - r_0 \in R|_{[-q/(2p),q/(2p))}$. In this case it holds

$$\begin{aligned}
\mathsf{Round}(t_1) &= \lfloor m - z_0 + p \cdot l + \underbrace{(p/q) \cdot (e - r_0)}_{\in R|_{[-1/2,1/2)}} \rceil \mod p \\
&= m - z_0 \mod p.
\end{aligned}$$

It is left to compute the probability of $e - r_0 \in R|_I$. This is the case, whenever all coefficients of r_0 are not "too close" to the boundaries of the interval I (constituting the *good area*). As t_0 is chosen uniformly at random, we have that the distribution of z_0 is the uniform distribution over R_p and the distribution of r_0 is the uniform distribution over $R|_I$. For every $j \in \{1, \ldots, N\}$, for the j-th component of r_0 the probability that it is outside the interval

$$I_j := (-q/(2p) + e_j, q/(2p) + e_j]$$

is at most

$$(\|e\|_\infty + 1) \cdot p/q.$$

A union bound over all components of r_0 yields thus correct rounding with probability at least

$$1 - N \cdot (\|e\|_\infty + 1) \cdot p/q.$$

Lemma 2 (Lifting the modulus of shares). *Let $p \in \mathbb{N}$ be a modulus with $p \geq \lambda^{\omega(1)}$. Let $R \in \{\mathbb{Z}, \mathbb{Z}[X]/(X^n + 1)\}$ be of dimension N. Let $m \in R$ and $z_0, z_1 \in R_p$ be random, subject to*

$$z_0 + z_1 = m \mod p.$$

Then we have

$$z_0 + z_1 = m \text{ over } R$$

with probability at least $1 - (N \cdot (\|m\|_\infty + 1)/p) \geq 1 - \lambda^{-\omega(1)}$ over the choice of the shares z_0, z_1.

Proof. We have to show that for $z_0 \xleftarrow{\$} R_p$ random, with overwhelming probability it holds $m - z_0 \in R_p$ (without computing modulo p). Recall that we consider R_p as elements whose coefficients are all in $I := (-\lfloor p/2 \rceil, \ldots, \lfloor (p-1)/2 \rceil]$. Thus, $m - z_0 \in R_p$, whenever for all $j = \{1, \ldots, N\}$, the j-th coefficient of z_0 is in $I_j := [-\lfloor (p-1)/2 \rceil + m_j, \ldots, \lfloor p/2 \rceil + m_j)$. For every j we have $|I \cap I_j| \geq p - m_j - 1$. A union bound over all coefficients yields that $m - z_0 \in R_p$ (and thus $z_0 + z_1 = m$ over R) except with probability at most

$$N \cdot (\|m\|_\infty + 1)/p.$$

B.2 Encryption with nearly linear decryption

Lemma 3 (KDM oracle). *Let* $\mathsf{PKE} := (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ *be a public-key encryption scheme with nearly linear decryption and parameters* $(p, q, d, B_{\mathsf{sk}}, B_{\mathsf{ct}}, R)$*. Then there exists a PPT procedure* $\mathsf{PKE.OKDM}$ *that takes as input a public key* pk*, a value* $x \in R$ *and an index* $j \in \{1, \ldots, d\}$ *and outputs a ciphertext* $\mathbf{c}_j$*, such that the following properties are satisfied.*

- ***Nearly linear decryption to the message*** $x \cdot s_j$***:*** *For any* $\lambda \in \mathbb{N}$*, for any* $(\mathsf{pk}, \mathbf{s})$ *in the image of* $\mathsf{Gen}(1^\lambda)$*, and for any ciphertext* $\mathbf{c}_j \in R_q^d$ *in the image of* $\mathsf{PKE.OKDM}(\mathsf{pk}, x, j)$*, it holds*

$$\langle \mathbf{s}, \mathbf{c}_j \rangle = (q/p) \cdot (x \cdot s_j) + e \mod q$$

  for some $e \in R$ *with* $\|e\|_\infty \leq B_{\mathsf{ct}}$*.*
- ***Security:*** *For any* $\lambda \in \mathbb{N}$ *and any PPT adversary* $\mathcal{A}$ *we have that*

$$\mathrm{Adv}^{\mathsf{kdm-ind}}_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda) := \left| \Pr\left[\mathrm{Exp}^{\mathsf{kdm-ind}}_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda) = 1 \right] - 1/2 \right|$$

  is negligible in λ*, where* $\mathrm{Exp}^{\mathsf{kdm-ind}}_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda)$ *is as defined in Figure 1*

By $\mathsf{PKE.}\mathbf{OKDM}(\mathsf{pk}, x)$ *we denote the KDM oracle that returns a componentwise encryption of* $x \cdot \mathbf{s}$*, i.e. that outputs the matrix* $(\mathsf{PKE.OKDM}(\mathsf{pk}, x, 1), \ldots, \mathsf{PKE.OKDM}(\mathsf{pk}, x, d)) \in R_q^{d \times d}$*.*

Proof. We define $\mathsf{PKE.OKDM}$ to be the algorithm that on input of a public key pk, a value $x \in R$ and an index $j \in \{1, \ldots, d\}$ computes an encryption

$$\mathbf{c} \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, 0)$$

and outputs

$$\mathbf{c}_j := (q/p) \cdot x \cdot \mathbf{e}_j + \mathbf{c} \mod q,$$

where $\mathbf{e}_j \in R_q^d$ is the j-th unit vector.

It is left to prove that $\mathsf{PKE.OKDM}$ meets the required properties. As PKE is a encryption scheme with nearly linear decryption, we have

$$\mathbf{c} = (q/p) \cdot 0 + e = e \mod q$$

for some $e \in R$ with $\|e\|_\infty \leq B_{\mathsf{ct}}$. We thus have

$$\langle \mathbf{s}, \mathbf{c}_j \rangle = (q/p) \cdot x \cdot \langle \mathbf{s}, \mathbf{e}_j \rangle + \langle \mathbf{s}, \mathbf{c} \rangle = (q/p) \cdot (x \cdot s_j) + e \mod q,$$

as required for nearly linear decryption.

In order to prove security of $\mathsf{PKE.OKDM}$, we proceed via a series of games depicted in Figure 6. We have

$$\mathrm{Adv}^{\mathsf{kdm-ind}}_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda) := \left| \Pr\left[\mathbf{G}^0_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda) = 1 \right] - \frac{1}{2} \right|.$$

From an adversary distinguishing between $\mathbf{G}^0_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda)$ and $\mathbf{G}^1_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda)$, we can construct an adversary $\mathcal{B}$ on the pseudorandomness of ciphertexts with

$$\left| \Pr\left[\mathbf{G}^0_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda) = 1 \right] - \Pr\left[\mathbf{G}^1_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda) = 1 \right] \right| \leq \mathrm{Adv}^{\mathsf{pr}}_{\mathsf{PKE},\mathcal{B}}(\lambda).$$

In game $\mathbf{G}^1_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda)$ the view of $\mathcal{A}$ is independent of β, as the vectors $\mathbf{c}_j$ and $\mathbf{c}$ are both distributed uniformly at random over R_p^d. We have thus

$$\Pr\left[\mathbf{G}^1_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda) = 1 \right] = \frac{1}{2}.$$

As PKE satisfies indistinguishability of ciphertexts by prerequisites, we have thus that

$$\mathrm{Adv}^{\mathsf{kdm-ind}}_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda) \leq \mathrm{Adv}^{\mathsf{pr}}_{\mathsf{PKE},\mathcal{B}}(\lambda)$$

is negligible in λ as required.

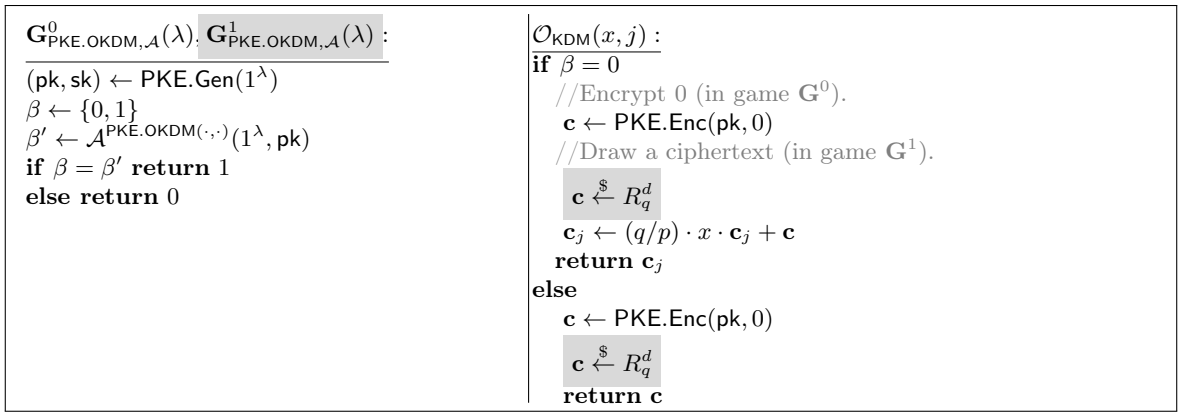

Fig. 6: Games $\mathbf{G}^0_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda)$ and $\mathbf{G}^1_{\mathsf{PKE.OKDM},\mathcal{A}}(\lambda)$ in the proof of Lemma 3 (Security of OKDM).

Lemma 4 (Distributed decryption of sums of ciphertexts). *Let* $\mathsf{PKE} := (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ *be a public-key encryption scheme with nearly linear decryption and parameters* $(p, q, d, B_{\mathsf{sk}}, B_{\mathsf{ct}}, R)$*, where* R *has dimension* N*. Let* $\mathsf{PKE.OKDM}$ *be the KDM oracle from Lemma 3. Let* $B_{\mathsf{add}} \in \mathbb{N}$ *with* $B_{\mathsf{add}} \leq \mathsf{poly}(\lambda)$*. Then there exists a deterministic polynomial time decryption procedure* $\mathsf{PKE.DDec}$ *with the following syntax and properties:*

- $\mathsf{PKE.DDec}(b, t_b, \mathbf{c})$*: On input a bit* $b \in \{0,1\}$*, "key" share* $\mathbf{t}_b \in R_q^d$ *and ciphertext* $\mathbf{c}$*, outputs a message in* R*.*
- *For all* $x \in R_p$ *with* $p/\|x\|_\infty \geq \lambda^{\omega(1)}$ *and* $q/(p \cdot \|x\|_\infty) \geq \lambda^{\omega(1)}$*, for all* $(\mathsf{pk}, \mathbf{s}) \leftarrow \mathsf{Gen}(1^\lambda)$*, for all messages* $m_1 \ldots, m_{B_{\mathsf{add}}} \in R_p$*, for all encryptions* $\mathbf{c}_i$ *of* m_i *that are either output of* $\mathsf{PKE.Enc}$ *or of* $\mathsf{PKE.OKDM}$ *(in that case we have* $m_i = x_i \cdot s_j$ *for some value* $x_i \in R_p$ *and some index* $j \in \{1, \ldots, d\}$*) and for shares* $\mathbf{t}_0, \mathbf{t}_1 \in R_q^d$ *random subject to*

$$\mathbf{t}_0 + \mathbf{t}_1 = x \cdot \mathbf{s} \mod q$$

for $\mathbf{c} := \sum_{i=1}^{B_{\mathsf{add}}} \mathbf{c}_i$ *and* $m := \sum_{i=1}^{B_{\mathsf{add}}} m_i$ *it holds*

$$\mathsf{PKE.DDec}(0, \mathbf{t}_0, \mathbf{c}) + \mathsf{PKE.DDec}(1, \mathbf{t}_1, \mathbf{c}) = x \cdot m \mod q$$

with probability over the random choice of the shares $\mathbf{t}_0, \mathbf{t}_1$ *of at least*

$$1 - N \cdot (N \cdot B_{\mathsf{add}} \cdot \|x\|_\infty \cdot B_{\mathsf{ct}} \cdot p/q + \|x \cdot m\|_\infty/p + p/q + 1/p) \geq 1 - \lambda^{-\omega(1)}.$$

For $\mathbf{C} = (\mathbf{c}_1 | \ldots | \mathbf{c}_d) \in R_p^{d \times d}$ *by* $\mathbf{m} \leftarrow \mathsf{PKE.DDec}(b, \mathbf{t}_b, \mathbf{C})$ *we denote the componentwise decryption* $\mathbf{m} \leftarrow (\mathsf{PKE.DDec}(b, \mathbf{t}_b, \mathbf{c}_1), \ldots, \mathsf{PKE.DDec}(b, \mathbf{t}_b, \mathbf{c}_d)) \in R_p^d$*.*

Proof. Let Round be the procedure for rounding of noisy shares from Lemma 1. Recall that we defined $\mathsf{PKE.DDec}$ to be the algorithm that on input $b \in \{0,1\}, \mathbf{t}_b \in R^d, \mathbf{c} \in R_q^d$ outputs

$$(\mathsf{Round}(\langle \mathbf{t}_b, \mathbf{c} \rangle \mod q)) \mod q.$$

We start by proving that nearly linear decryption holds true also for the sum of a bounded number of ciphertexts, but with an increased error term. To that end, let $m := \sum_{i=1}^{B_{\mathsf{add}}} m_i$. Because PKE is an encryption scheme with nearly linear decryption and by Lemma 3, for all $i \in \{1, \ldots, B_{\mathsf{add}}\}$ we have

$$\langle \mathbf{s}, \mathbf{c}_i \rangle = (q/p) \cdot m_i + e_i \mod q, \tag{2}$$

where $\|e_i\|_\infty \leq B_{\mathsf{ct}}$. This yields

$$\langle \mathbf{s}, \sum_{i=1}^{B_{\mathsf{add}}} \mathbf{c}_i \rangle = \sum_{i=1}^{B_{\mathsf{add}}} \langle \mathbf{s}, \mathbf{c}_i \rangle = \sum_{i=1}^{B_{\mathsf{add}}} ((q/p) \cdot m_i + e_i) = (q/p) \cdot m + \sum_{i=1}^{B_{\mathsf{add}}} e_i \mod q,$$

where $\| \sum_{i=1}^{B_{\mathsf{add}}} e_i \|_\infty \leq \sum_{i=1}^{B_{\mathsf{add}}} \|e_i\|_\infty \leq B_{\mathsf{add}} \cdot B_{\mathsf{ct}}$.

It thus holds

$$\langle \mathbf{t}_0, \mathbf{c} \rangle + \langle \mathbf{t}_1, \mathbf{c} \rangle = x \cdot \langle \mathbf{s}, \mathbf{c} \rangle = (q/p) \cdot (x \cdot m) + (x \cdot e) \mod q$$

for some $e \in R$ with $\|e\|_\infty \leq B_{\mathsf{add}} \cdot B_{\mathsf{ct}}$.

By Lemma 1 we have

$$\mathsf{Round}(\langle \mathbf{t}_0, \mathbf{c} \rangle \mod q) + \mathsf{Round}(\langle \mathbf{t}_1, \mathbf{c} \rangle \mod q) = x \cdot m \mod p$$

except with probability at most

$$N \cdot (\|x \cdot e\|_\infty + 1) \cdot p/q \quad \leq \quad N \cdot (N \cdot B_{\mathsf{add}} \cdot \|x\|_\infty \cdot B_{\mathsf{ct}} + 1) \cdot p/q.$$

Whenever Round is successful, by Lemma 2 we have

$$(\mathsf{Round}(\langle \mathbf{t}_0, \mathbf{c} \rangle \mod q)) + (\mathsf{Round}(\langle \mathbf{t}_1, \mathbf{c} \rangle \mod q)) = x \cdot m \mod q$$

except with probability at most $N \cdot (\|x \cdot m\|_\infty + 1)/p$.

Remark 4 (Distributed decryption for low-order symbol encryption schemes). As mentioned in the main part, our techniques carry over to encryption schemes which encrypt messages in low-order symbols, i.e. where p and q are coprime and for which for message $m \in R_p := R/pR$, secret key $\mathbf{s} \in R_q^d$, and ciphertext $\mathbf{c} \in R_q^d$ encrypting m, we have

$$\langle \mathbf{s}, \mathbf{c} \rangle = m + p \cdot e \mod q$$

for some "small" noise $e \in R$.

For this class of encryption schemes, we define $\mathsf{PKE.OKDM}$ as the algorithm that on input of a public key pk, a value $x \in R$ with $\|x\|_\infty \leq B_{\mathsf{inp}}$ and an index $j \in \{1, \ldots, d\}$ computes an encryption $\mathbf{c} \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, 0)$ and outputs $\mathbf{c}_j := x \cdot \mathbf{e}_j + \mathbf{c} \mod q$, where $\mathbf{e}_j \in R_q^d$ is the j-th unit vector.

Further, we define $\mathsf{PKE.DDec}$ to be the algorithm that on input $b \in \{0,1\}, \mathbf{t}_b \in R^d, \mathbf{c} \in R_q^d$ outputs

$$((\langle \mathbf{t}_b, \mathbf{c} \rangle \mod q) \mod p) \mod q.$$

C HSS extensions

C.1 Secret-key HSS

Definition 8 (Secret-key HSS). Secret-key HSS *is a weaker notion of HSS, where the role of the public key* pk *is replaced by a* secret *key* sk *and where* $\mathsf{HSS.Enc}$ *is replaced by the following algorithm.*

- $\mathsf{HSS.Share}(\mathsf{sk}, x)$*: Given secret key* sk *and secret input value* $x \in \mathcal{I}$*, the encryption algorithm outputs a pair of shares* $(\mathsf{sh}_0, \mathsf{sh}_1)$.

The correctness and security requirements are as above, but where $\mathsf{HSS.Enc}$ *is replaced by* $\mathsf{HSS.Share}$ *and* $\mathsf{ct}^{(i)}$, ct *are replaced by* $\mathsf{sh}_b^{(i)}$, sh_b*, respectively.*

Definition 9 (Secret-key encryption scheme with nearly linear decryption). *We say a tuple of PPT algorithms* $\mathsf{SKE} := (\mathsf{SKE.Gen}, \mathsf{SKE.Enc}, \mathsf{SKE.Dec})$ *is a* secret-key encryption scheme *with message space* $\mathcal{M}$ *and ciphertext space* $\mathcal{C}$*, if it has the properties and the syntax of a public-key encryption scheme, but where* $\mathsf{pk} = \mathsf{sk}$.

We say SKE *is* key dependent message (KDM) secure *(see e.g.[6], also known as* circular secure*) with respect to the family of functions* $\mathcal{Y}$ *from the secret key space of* SKE *to the message space of* SKE*, if for every PPT adversary* $\mathcal{A}$ *that only queries* $f \in \mathcal{Y}$ *the probability*

$$\mathrm{Adv}^{\mathsf{kdm}}_{\mathsf{SKE},\mathcal{Y},\mathcal{A}}(\lambda) := \left| \Pr\left[\mathrm{Exp}^{\mathsf{kdm}}_{\mathsf{SKE},\mathcal{Y},\mathcal{A}}(\lambda) = 1 \right] - \frac{1}{2} \right|$$

is negligible in λ*, where* $\mathrm{Exp}^{\mathsf{kdm}}_{\mathsf{SKE},\mathcal{Y},\mathcal{A}}(\lambda)$ *is as defined in Figure 7.*

If a secure secret-key encryption scheme SKE *complies with the properties of Definition 4 (where* $\mathsf{pk} = \mathsf{sk} = \mathbf{s}$*), we say* SKE *is a* secret-key encryption scheme with nearly linear decryption.

$\underline{\mathrm{Exp}^{\mathsf{kdm}}_{\mathsf{SKE},\Upsilon,\mathcal{A}}(\lambda):}$
$\mathsf{sk} \leftarrow \mathsf{PKE.Gen}(1^\lambda)$
$\beta \leftarrow \{0,1\}$
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{Enc}}(\cdot)}(1^\lambda)$
if $\beta = \beta'$ **return** 1
else return 0

$\underline{\mathcal{O}_{\mathsf{Enc}}(f):}$
if $\beta = 0$
  $c \leftarrow \mathsf{PKE.Enc}(\mathsf{sk}, f(\mathsf{sk}))$
  return c
else
  $c \leftarrow \mathsf{PKE.Enc}(\mathsf{sk}, 0)$
  return c

Fig. 7: Security challenge experiment for KDM security with respect to the family of functions Υ.

$\underline{\mathsf{skHSS.Gen}(1^\lambda):}$

- Generate a secret key $\mathbf{s} \leftarrow \mathsf{SKE.Gen}(1^\lambda)$ for encryption and draw a PRF key $K \xleftarrow{\$} \mathcal{K}$.
- **Secret share the secret key.** Choose $\mathbf{s}_0 \xleftarrow{\$} R_q^d$ at random. Define

$$\mathbf{s}_1 := \mathbf{s} - \mathbf{s}_0 \mod q.$$

- Output $\mathbf{s}$ and $\mathsf{ek}_b \leftarrow (K, \mathbf{s}_b)$.

$\underline{\mathsf{skHSS.Share}(1^\lambda, \mathbf{s}, x):}$

- **Encrypt the input.** Compute $\mathbf{C}^x \leftarrow \mathsf{SKE.Enc}(\mathbf{s}, x \cdot \mathbf{s})$.
- **Secret share the input.** Choose $\mathbf{t}_0^x \xleftarrow{\$} R_q^d$ at random. Define

$$\mathbf{t}_1^x := x \cdot \mathbf{s} - \mathbf{t}_0^x \mod q$$

  and output $((\mathbf{C}^x, \mathbf{t}_0^x), (\mathbf{C}^x, \mathbf{t}_1^x))$.

$\underline{\mathsf{skHSS.Eval}(b, \mathsf{ek}_b, ((\mathbf{C}^{x^{(1)}}, \mathbf{t}_b^{x^{(1)}}), \ldots, (\mathbf{C}^{x^{(\rho)}}, \mathbf{t}_b^{x^{(\rho)}})), P, r):}$

- **Load an input into memory:** On instruction $(\mathsf{id}, (\mathbf{C}^x, \mathbf{t}_b^x))$ return $\mathbf{t}_b^x$.
- **Add/multiply/output:** As $\mathsf{HSS.Eval}(b, \mathsf{ek}_b, (\mathbf{C}^{x^{(i)}})_i, P, r)$ (Fig. 2).

Fig. 8: 2-party secret-key homomorphic secret sharing scheme skHSS for the class of RMS programs from encryption with nearly linear decryption. Here, $x \in R$ with $\|x\|_\infty \leq B_{\mathsf{inp}}$ is an input value. Throughout, *input values* $x \in R$ are represented by encryptions $\mathbf{C}^x$ of $x \cdot \mathbf{s}$ and *memory values* $x \in R$ are represented by shares $(\mathbf{t}_0^x, \mathbf{t}_1^x) \in R_q^d \times R_q^d$ with $\mathbf{t}_0^x + \mathbf{t}_1^x = x \cdot \mathbf{s} \mod q$.

Remark 5. Lemma 4 on distributed decryption carries over to secret-key encryption schemes with nearly linear decryption (where we only consider outputs of SKE.Enc to be decrypted).

Theorem 3 (Secret-key HSS from encryption with nearly linear decryption). *Let* $\mathsf{SKE} := (\mathsf{SKE.Gen}, \mathsf{SKE.Enc}, \mathsf{SKE.Dec})$ *be a secret-key encryption scheme with nearly linear decryption and parameters* $(p, q, d, B_{\mathsf{sk}}, B_{\mathsf{ct}}, R)$.

- *Let* SKE *satisfy KDM security with respect to the function family*

$$\Upsilon := \left\{ f_{x,j} \colon R^d \to R, \mathbf{s} \mapsto x \cdot s_j \colon x \in R \text{ s.t. } \|x\|_\infty \leq B_{\mathsf{inp}} \wedge 1 \leq j \leq d \right\},$$

  where $B_{\mathsf{inp}} \in \mathbb{N}$ *with* $p/B_{\mathsf{inp}} \geq \lambda^{\omega(1)}$ *and* $q/(B_{\mathsf{inp}} \cdot p) \geq \lambda^{\omega(1)}$,
- *Let* SKE.DDec *be the distributed decryption procedure from Lemma 4.*
- *Let* $\mathsf{PRF} \colon \mathcal{K} \times \mathcal{S}_{\mathsf{id}} \to R_q^d$ *be a pseudorandom function.*

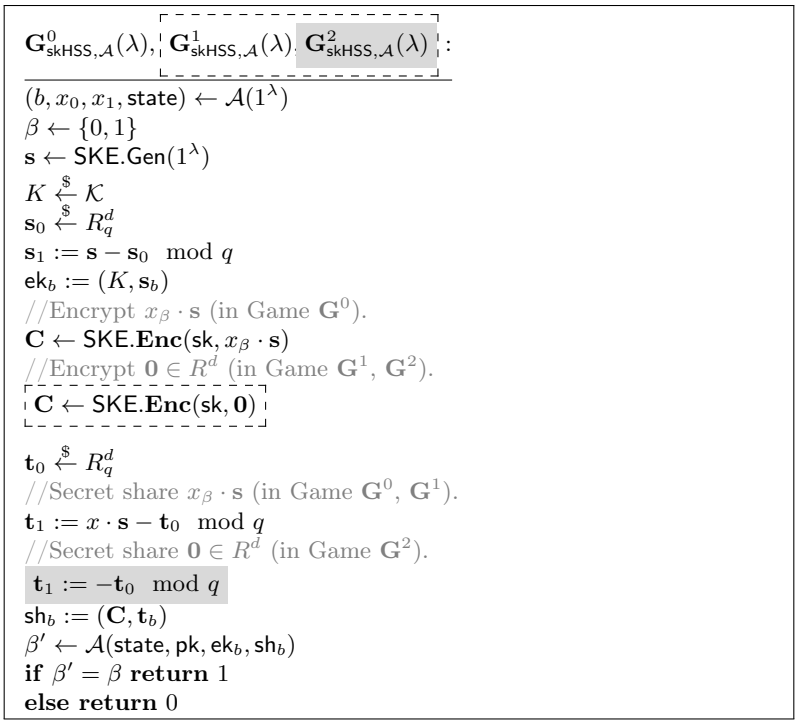

Fig. 9: Games $\mathbf{G}^0_{\mathsf{skHSS},\mathcal{A}}(\lambda)$ and $\mathbf{G}^1_{\mathsf{skHSS},\mathcal{A}}(\lambda)$ in the proof of Theorem 3 (Security of skHSS).

Then there exists a 2-party secret-key homomorphic secret sharing scheme $\mathsf{skHSS} = (\mathsf{skHSS.Gen}, \mathsf{skHSS.Enc}, \mathsf{skHSS.Eval})$ *with input space* $[R]_{B_{\mathsf{inp}}} = \{x \in R \mid \|x\|_\infty \leq B_{\mathsf{inp}}\}$ *for the class of RMS programs, as given in Figure 8, that satisfies the following.*

- ***Correctness:*** *For any security parameter* $\lambda \in \mathbb{N}$*, for any inputs* $x^{(1)}, \ldots, x^{(\rho)} \in [R]_{B_{\mathsf{inp}}}$*, for any polynomially bounded RMS programs* P *with* $P(x^{(1)}, \ldots, x^{(\rho)}) \neq \perp$ *and for any integer* $r \geq 2$*, there exist a PPT adversary* $\mathcal{B}$ *on the pseudorandomness of* PRF *such that*

$$\Pr^{\mathsf{cor}}_{\mathsf{skHSS},(x^{(i)})_i,P,r}(\lambda) \geq 1 - \left(\mathrm{Adv}^{\mathsf{prf}}_{\mathsf{PRF},\mathcal{B}}(\lambda) + \lambda^{-\omega(1)}\right).$$

- ***Security:*** *For every PPT adversary* $\mathcal{A}$ *on the security of* skHSS*, there exists an PPT adversary* $\mathcal{B}$ *on the KDM security of* SKE *such that*

$$\mathrm{Adv}^{\mathsf{sec}}_{\mathsf{skHSS},\mathcal{A}}(\lambda) \leq \mathrm{Adv}^{\mathsf{kdm}}_{\mathsf{SKE},\Upsilon,\mathcal{B}}(\lambda).$$

Proof. We give the secret-key HSS construction in Figure 8. The proof of correctness carries over from the proof of correctness of the public-key HSS (Lemma 5).

We prove security via a hybrid argument. For an overview of the games see Figure 9. Game $\mathbf{G}^0_{\mathsf{skHSS},\mathcal{A}}(\lambda)$ corresponds to the HSS security game, therefore we have

$$\mathrm{Adv}^{\mathsf{sec}}_{\mathcal{A},\mathsf{skHSS}}(\lambda) = \left|\Pr\left[\mathbf{G}^0_{\mathsf{skHSS},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2}\right|.$$

Note that from an adversary $\mathcal{A}$ distinguishing between $\mathbf{G}^0_{\mathsf{HSS},\mathcal{A}}(\lambda)$ and $\mathbf{G}^1_{\mathsf{HSS},\mathcal{A}}(\lambda)$ we can construct a PPT adversary $\mathcal{B}$ on the KDM security of SKE as follows.

$\underline{\mathsf{HSS}^2.\mathsf{Gen}(1^\lambda):}$

- Generate a key pair $(\mathsf{pk}, \mathbf{s}) \leftarrow \mathsf{PKE.Gen}(1^\lambda)$ for encryption and draw a PRF key $K \xleftarrow{\$} \mathcal{K}$.
- **Secret share the tensor product of a secret key.** Choose $\mathbf{S}_0 \xleftarrow{\$} R_q^{d\times d}$ at random. Define

$$\mathbf{S}_1 := \mathbf{s} \cdot \mathbf{s}^\top - \mathbf{S}_0 \mod q.$$

- Output pk and $\mathsf{ek}_b \leftarrow (K, \mathbf{S}_b)$.

$\underline{\mathsf{HSS}^2.\mathsf{Enc}(1^\lambda, \mathsf{pk}, x):}$

- **Encrypt the input.** Compute and output $\mathbf{c}^x \leftarrow \mathsf{PKE.Enc}(\mathsf{pk}, x)$.

$\underline{\mathsf{HSS}^2.\mathsf{Eval}(b, \mathsf{ek}_b, (\mathbf{c}^{x^{(1)}}, \ldots, \mathbf{c}^{x^{(\rho)}}), P, r):}$

Parse $(K, \mathbf{S}_b) =: \mathsf{ek}_b$, and let $\mathbf{S}_{b,i}$ denote the i-th column of $\mathbf{S}_b$. Parse P (restricted to the class of degree 2 polynomials) as a sequence of RMS operations and proceed as follows.

- **Load an input into memory:** On instruction $(\mathsf{id}, \mathbf{c}^x)$ compute

$$\forall i \le d\colon t_{b,i}^x := \mathsf{PKE.DDec}(b, \mathbf{S}_{b,i}, \mathbf{c}^x) + (1-2b)\cdot \mathsf{PRF}(K, \mathsf{id}) \mod q$$

  and return the share

$$\mathbf{t}_b^x := (t_{b,1}^x, \ldots, t_{b,d}^x) \in R_q^d.$$

- **Add/multiply/output:** Proceed as $\mathsf{HSS.Eval}'(b, \mathsf{ek}_b, (\mathbf{c}^{x^{(i)}})_i, P, r)$ (Fig. 2), where $\mathsf{HSS.Eval}'$ is as $\mathsf{HSS.Eval}$, but operates on single encryptions instead of d-tuples of encryptions.

Fig. 10: 2-party public-key homomorphic secret sharing scheme HSS^2 for the class of degree-2 polynomials from encryption with nearly linear decryption. Here, $x \in R$ with $\|x\|_\infty \le B_{\mathsf{inp}}$ is an input value. Throughout, *input values* $x \in R$ are represented by encryptions $\mathbf{c}^x$ of x and *memory values* are $x \in R$ are represented by shares $(\mathbf{t}_0^x, \mathbf{t}_1^x) \in R_q^d \times R_q^d$ with $\mathbf{t}_0^x + \mathbf{t}_1^x = x \cdot \mathbf{s} \mod q$.

On input $(b, x_0, x_1, \mathsf{state})$ of $\mathcal{A}$, $\mathcal{B}$ chooses $\beta \in \{0,1\}$, $\mathbf{s}_0, \mathbf{t}_0 \xleftarrow{\$} R_q^d$, sets $\mathbf{s}_1 := \mathbf{s} - \mathbf{s}_0 \mod q$, $\mathbf{t}_1 := x \cdot \mathbf{s} - \mathbf{t}_0 \mod q$ and for all $j \in \{1, \ldots, d\}$ queries $\mathbf{c}_j \leftarrow \mathcal{O}_{\mathsf{Enc}}(x_\beta, j)$. Finally, $\mathcal{B}$ sends $\mathsf{ek}_b := (K, \mathbf{s}_b)$ and $\mathsf{sh}_b := (\mathbf{C}, \mathbf{t}_b)$ to $\mathcal{A}$, where $\mathbf{C} := (\mathbf{c}_1 | \ldots | \mathbf{c}_d) \in R_q^{d\times d}$. If the KDM security experiment returns real encryptions of $x \cdot s_j$, the distribution of ek_b equals the distribution of game $\mathbf{G}^0_{\mathsf{HSS},\mathcal{A}}(\lambda)$. On the other hand, if the KDM security experiment returns encryptions of 0, the distribution of ek_b equals the distribution of game $\mathbf{G}^1_{\mathsf{HSS},\mathcal{A}}(\lambda)$. We have thus

$$\left|\Pr\left[\mathbf{G}^0_{\mathsf{HSS},\mathcal{A}}(\lambda) = 1\right] - \Pr\left[\mathbf{G}^1_{\mathsf{HSS},\mathcal{A}}(\lambda) = 1\right]\right| \le \mathrm{Adv}^{\mathsf{kdm-ind}}_{\mathsf{PKE.OKDM},\mathcal{B}}(\lambda).$$

As the distribution of $(\mathbf{t}_0, \mathbf{t}_1)$ in game $\mathbf{G}^1$ is random over $R^d \times R^d$ conditioned on $\mathbf{t}_0 + \mathbf{t}_1 = x \cdot \mathbf{s} \mod q$, each value on its own $\mathbf{t}_1$ is indistinguishable from being distributed uniformly at random over R^d. We have thus

$$\Pr\left[\mathbf{G}^1_{\mathsf{HSS},\mathcal{A}}(\lambda) = 1\right] = \Pr\left[\mathbf{G}^2_{\mathsf{HSS},\mathcal{A}}(\lambda) = 1\right].$$

Finally, as in game $\mathbf{G}^2_{\mathsf{HSS},\mathcal{A}}(\lambda)$, the view of $\mathcal{A}$ is independent of β, it holds

$$\Pr\left[\mathbf{G}^2_{\mathsf{HSS},\mathcal{A}}(\lambda) = 1\right] = \frac{1}{2}.$$

C.2 HSS for degree-2 polynomials

Theorem 4 (HSS for degree-2 polynomials). *Let* $\mathsf{PKE} := (\mathsf{PKE.Gen}, \mathsf{PKE.Enc}, \mathsf{PKE.Dec})$ *be a public-key encryption scheme with nearly linear decryption and parameters* $(p, q, d, B_{\mathsf{sk}}, B_{\mathsf{ct}}, R)$.

- *Let* $B_{\mathsf{inp}} \in \mathbb{N}$ *with* $p/B_{\mathsf{inp}} \geq \lambda^{\omega(1)}$ *and* $q/(B_{\mathsf{inp}} \cdot p) \geq \lambda^{\omega(1)}$.
- *Let* $\mathsf{PKE.DDec}$ *be the distributed decryption procedure as defined in Lemma 4.*
- *Let* $\mathsf{PRF}\colon \mathcal{K} \times \mathcal{S}_{\mathsf{id}} \to R_q^d$ *be a pseudorandom function.*

Then there exists a 2-party public-key homomorphic secret sharing scheme $\mathsf{HSS}^2 = (\mathsf{HSS}^2.\mathsf{Gen}, \mathsf{HSS}^2.\mathsf{Enc}, \mathsf{HSS}^2.\mathsf{Eval})$ *with input space* $[R]_{B_{\mathsf{inp}}}$ *for the class of degree-2 polynomials, as given in Figure 10, that satisfies the following.*

- ***Correctness:*** *For any security paramter* $\lambda \in \mathbb{N}$*, for any inputs* $x^{(1)}, \ldots, x^{(\rho)} \in [R]_{B_{\mathsf{inp}}}$*, for any degree-2 polynomial* P *of polynomially bounded size and with* $P(x^{(1)}, \ldots, x^{(\rho)}) \neq \perp$ *and for any integer* $r \geq 2$*, there exist a PPT adversary* $\mathcal{B}$ *on the pseudorandomness of* PRF *such that*

$$\Pr^{\mathsf{cor}}_{\mathsf{HSS}^2,(x^{(i)})_i,P,r}(\lambda) \geq 1 - \left(\mathrm{Adv}^{\mathsf{prf}}_{\mathsf{PRF},\mathcal{B}}(\lambda) + \lambda^{-\omega(1)}\right).$$

- ***Security:*** *For every PPT adversary* $\mathcal{A}$ *on the security of* HSS*, there exists an PPT adversary* $\mathcal{B}$ *on the security of* PKE *such that*

$$\mathrm{Adv}^{\mathsf{sec}}_{\mathsf{HSS}^2,\mathcal{A}}(\lambda) \leq \mathrm{Adv}^{\mathsf{pr}}_{\mathsf{PKE},\mathcal{B}}(\lambda).$$

Proof. Let P we a program with

- P is of size $|P| \leq \mathsf{poly}(\lambda)$
- P has magnitude bound B_{max} with $p/B_{\mathsf{max}} \geq \lambda^{\omega(1)}$ and $q/(B_{\mathsf{max}} \cdot p) \geq \lambda^{\omega(1)}$,
- P has maximum number of input addition instructions $P_{\mathsf{inp}+}$.

The construction of HSS^2 is given in Figure 10. For the proof of correctness we built on the proof of correctness of our basic public-key HSS (Lemma 5).

It is left to show that loading an input into the memory actually yields $\mathbf{t}_0^x + \mathbf{t}_1^x = x \cdot \mathbf{s} \in R_q^d$ as required. Note that for $\mathbf{s} = (s_1, \ldots, s_d)$ and $\mathbf{S} := \mathbf{s} \cdot \mathbf{s}^\top$, for the i-th colum $\mathbf{S}_i$ of $\mathbf{S}$ we have $\mathbf{S}_i = s_i \cdot \mathbf{s}$. As PKE satsifies nearly linear decryption, for $i \leq d$ it thus holds

$$x_b = \mathsf{PKE.DDec}(b, \mathbf{S}_{b,i}, \mathbf{c}^x) + (1-2b) \cdot \mathsf{PRF}(K, \mathsf{id}) \mod q$$

by Lemma 4 we have $x_0 + x_1 = s_i \cdot x \mod q$ except with probability

$$N^2 \cdot P_{\mathsf{inp}+} \cdot \|s_i\|_\infty \cdot B_{\mathsf{ct}} \cdot p/q + N \cdot \|s_i \cdot x\|_\infty / p + N \cdot (p/q + 1/p).$$

Thus, as in the proof of the basic public-key HSS we have correctness of a single load input with probability at least

$$1 - d \cdot N^2 \cdot P_{\mathsf{inp}+} \cdot B_{\mathsf{sk}} \cdot B_{\mathsf{ct}} \cdot p/q - d \cdot N^2 \cdot B_{\mathsf{inp}}/p - d \cdot N \cdot (p/q + 1/p).$$

Therefore, using the observations of the proof of Lemma 5 together with the fact that messages encrypted do not contain the secret key, we obtain that correctness holds at least with probability

$$\begin{aligned}\Pr^{\mathsf{cor}}_{\mathsf{HSS}^2,(x^{(i)})_i,P}(\lambda) \geq 1 &- \mathrm{Adv}^{\mathsf{prf}}_{\mathsf{PRF},\mathcal{B}}(\lambda) - N \cdot (B_{\mathsf{max}} + 1)/q \\ &- |P| \cdot d \cdot N^2 \cdot P_{\mathsf{inp}+} \cdot \max(B_{\mathsf{max}}, B_{\mathsf{sk}}) \cdot B_{\mathsf{ct}} \cdot p/q \\ &- |P| \cdot d \cdot N \cdot \max(B_{\mathsf{max}}, N \cdot B_{\mathsf{inp}})/p \\ &- |P| \cdot d \cdot N \cdot (p/q + 1/p).\end{aligned}$$

For the proof of security, the proof of security of our basic public-key HSS (Theorem 2) carries over directly. Note that we would actually only require IND-CPA security, as we do not require a KDM oracle. This is due to the fact that for the evaluation of degree-2 polynomials it suffices to encrypt the input x (instead of $x \cdot \mathbf{s}$).

$\underline{\mathsf{skHSS}^2.\mathsf{Gen}(1^\lambda):}$

– $(\mathbf{s}, (\mathsf{ek}_0, \mathsf{ek}_1)) \leftarrow \mathsf{skHSS.Gen}(1^\lambda)$ (see Fig. 8)

$\underline{\mathsf{skHSS}^2.\mathsf{Share}(1^\lambda, \mathbf{s}, x):}$

– **Encrypt the input.** Compute $\mathbf{c}^x \leftarrow \mathsf{SKE.Enc}(\mathbf{s}, x)$.
– **Secret share the input.** Choose $\mathbf{t}_0^x \xleftarrow{\$} R_q^d$ at random. Define

$$\mathbf{t}_1^x := x \cdot \mathbf{s} - \mathbf{t}_0^x \mod q$$

and output $((\mathbf{c}^x, \mathbf{t}_0^x), (\mathbf{c}^x, \mathbf{t}_1^x))$.

$\underline{\mathsf{skHSS}^2.\mathsf{Eval}(b, \mathsf{ek}_b, (\mathsf{sh}^{(1)}, \ldots, \mathsf{sh}^{(\rho)}), P, p):}$

Parse $(K, \mathbf{s}_b) =: \mathsf{ek}_b$ and for $i \in \{1, \ldots, \rho\}$ parse $\mathsf{sh}^{(i)} =: (\mathbf{c}^{x^{(i)}}, \mathbf{t}_0^{x^{(i)}})$. Parse P (restricted to the class of degree-2 polynomials) as a sequence of RMS operations and proceed as follows.

– **Load an input into memory:** On instruction $(\mathsf{id}, (\mathbf{c}^x, \mathbf{t}_b^x))$ return $\mathbf{t}_b^x$.
– **Add values in memory:** On instruction (id, x_b, x_b') compute

$$y_b \leftarrow x_b + x_b' \mod p.$$

On instruction $(\mathsf{id}, \mathbf{t}_b^x, \mathbf{t}_b^{x'})$ compute

$$\mathbf{t}_b^{x+x'} \leftarrow \mathbf{t}_b^x + \mathbf{t}_b^{x'} + (1-2b) \cdot \mathsf{PRF}(K, \mathsf{id}) \mod q.$$

– **Add input values:** On instruction $(\mathsf{id}, \mathbf{c}^x, \mathbf{c}^{x'})$ compute

$$\mathbf{c}^{x+x'} \leftarrow \mathbf{c}^x + \mathbf{c}^{x'} \mod q.$$

– **Multiply memory value by input:** On instruction $(\mathsf{id}, \mathbf{t}_b^x, \mathbf{c}^{x'})$ compute

$$t_b := \langle \mathbf{t}_b^x, \mathbf{c}^{x'} \rangle \mod q$$

and return $y_b := \mathsf{Round}(t_b)$. //Recall that for $t_0 + t_1 = (q/p) \cdot x \cdot x' + e \mod q$ we have $\mathsf{Round}(t_0) + \mathsf{Round}(t_1) = x \cdot x' \mod p$.
– **Output from memory, as element in R_p:** On (id, x_b) output x_b.
On instruction $(\mathsf{id}, \mathbf{t}_b^x)$ parse $\mathbf{t}_b^x =: (x_b, \widehat{\mathbf{t}}_b^x)$ for some $x_b \in R_q$, $\widehat{\mathbf{t}}_b^x \in R_q^{d-1}$ and output

$$x_b \mod p.$$

Fig. 11: 2-party secret-key homomorphic secret sharing scheme skHSS^2 for the class of degree-2 polynomials from encryption with nearly linear decryption. Here, $x \in R$ with $\|x\|_\infty \leq B_{\mathsf{inp}}$ is an input value. We consider encryptions $\mathbf{c}^x$ of x to represent *input values* and shares $(\mathbf{t}_0^x, \mathbf{t}_1^x) \in R_q^d \times R_q^d$ with $\mathbf{t}_0^x + \mathbf{t}_1^x = x \cdot \mathbf{s} \mod q$ to represent *(non-terminal) memory values* (this is represented by the trivial load instruction). Further, we have *terminal memory values* represented as shares $(x_0, x_1) \in R_p^d \times R_p^d$. Only non-terminal memory values can be part of multiplications.

C.3 Secret-key HSS for degree-2 polynomials

Theorem 5 (Secret-key HSS for degree-2 polynomials). *Let* $\mathsf{SKE} := (\mathsf{SKE.Gen}, \mathsf{SKE.Enc}, \mathsf{SKE.Dec})$ *be a* relaxed version *of secret-key encryption scheme with nearly linear decryption and parameters* $(p, q, d, B_{\mathsf{sk}}, B_{\mathsf{ct}}, R)$*, where we do not require* $p \geq \lambda^{\omega(1)}$ *(i.e. we can choose* $p \leq \mathsf{poly}(\lambda)$*).*

- *Let* SKE *satisfy KDM security with respect to the function family of constant functions*

$$\Upsilon_{\mathsf{const}} := \left\{ f_x \colon R^d \to R, \mathbf{s} \mapsto x \colon x \in [R]_{B_{\mathsf{inp}}} \right\},$$

  where $B_{\mathsf{inp}} \in \mathbb{N}$ *with* $p/B_{\mathsf{inp}} \geq \lambda^{\omega(1)}$ *and* $q/(B_{\mathsf{inp}} \cdot p) \geq \lambda^{\omega(1)}$*. .*
- *Let* Round *be the procedure for the rounding of noisy shares as defined in Lemma 1. (Recall that this procedure corresponds to distributed decryption without lifting the modulus to* q*.)*
- *Let* $\mathsf{PRF} \colon \mathcal{K} \times \mathcal{S}_{\mathsf{id}} \to R_q^d$ *be a pseudorandom function.*

Then there exists a 2*-party secret-key homomorphic secret sharing scheme* $\mathsf{skHSS}^2 = (\mathsf{skHSS}^2.\mathsf{Gen}, \mathsf{skHSS}^2.\mathsf{Enc}, \mathsf{skHSS}^2.\mathsf{Eval})$ *with input space* $[R]_{B_{\mathsf{inp}}}$ *for the class of degree-*2 *polynomials with output space* R_p*, as given in Figure 11, that satisfies the following.*

- ***Correctness:*** *For any security parameter* $\lambda \in \mathbb{N}$*, for any inputs* $x^{(1)}, \ldots, x^{(\rho)} \in [R]_{B_{\mathsf{inp}}}$ *and for any degree-*2 *polynomial* P *of size* $|P| \leq \mathsf{poly}(\lambda)$ *with* $P(x^{(1)}, \ldots, x^{(\rho)}) \neq \perp$*, there exist a PPT adversary* $\mathcal{B}$ *on the pseudorandomness of* PRF *such that*

$$\Pr^{\mathsf{cor}}_{\mathsf{skHSS}^2, (x^{(i)})_i, P, p}(\lambda) \geq 1 - \left(\mathrm{Adv}^{\mathsf{prf}}_{\mathsf{PRF}, \mathcal{B}}(\lambda) + \lambda^{-\omega(1)} \right),$$

  where $N = 1$ *if* $R = \mathbb{Z}$*, let* $N = n$ *if* $R = \mathbb{Z}[X]/(X^n + 1)$*.*
- ***Security:*** *For every PPT adversary* $\mathcal{A}$ *on the security of* skHSS*, there exists an PPT adversary* $\mathcal{B}$ *on the security of* SKE *such that*

$$\mathrm{Adv}^{\mathsf{sec}}_{\mathsf{skHSS}^2, \mathcal{A}}(\lambda) \leq \mathrm{Adv}^{\mathsf{kdm}}_{\mathsf{SKE}, \Upsilon_{\mathsf{const}}, \mathcal{B}}(\lambda).$$

Proof. Let P we a program with

- P is of size $|P| \leq \mathsf{poly}(\lambda)$
- P P has magnitude bound B_{max} with $p/B_{\mathsf{max}} \geq \lambda^{\omega(1)}$ and $q/(B_{\mathsf{max}} \cdot p) \geq \lambda^{\omega(1)}$,
- P has maximum number of input addition instructions $P_{\mathsf{inp}+}$.

The construction of skHSS^2 is given in Figure 11. For the proof of correctness, we first switch the PRF to random as in the proof of correctness of our public-key HSS (Lemma 5). Again, from a difference in the probability of correct evaluation, we can construct an adversary $\mathcal{B}$ on the security of PRF.

Note that for all encryptions $\mathbf{c}^x$ of some input value x we have

$$\langle \mathbf{s}, \mathbf{c}^x \rangle = (q/p) \cdot m + e$$

for some $e \in \mathbb{R}_q$ with $\|e\|_\infty \leq B_{\mathsf{ct}}$ as PKE satisfies nearly linear decryption. Assuming the programm P has a maximum number of input addition instructions $P_{\mathsf{inp}+} \leq \mathsf{poly}(\lambda)$, we thus have for all encryption $\mathbf{c}^x$ computed during the evaluation of P that

$$\langle \mathbf{s}, \mathbf{c}^x \rangle = (q/p) \cdot m + e$$

for some $e \in \mathbb{R}_q$ with $\|e\|_\infty \leq P_{\mathsf{inp}+} \cdot B_{\mathsf{ct}}$. For all $(\mathbf{t}_0^x, \mathbf{t}_1^x) \in R_q \times R_q$, we have $\mathbf{t}_0^x + \mathbf{t}_1^x = x \cdot \mathbf{s}$, as this holds true for input values and is preserved by addition.

We now consider multiplication of a memory value by an input value. By previous considerations we have

$$\begin{aligned} t_0 + t_1 &= \langle \mathbf{t}_0^x + \mathbf{t}_1^x, \mathbf{c}^{x'} \rangle \\ &= x \cdot \langle \mathbf{s}, \mathbf{c}^{x'} \rangle = (q/p) \cdot x \cdot x' + x \cdot e, \end{aligned}$$

for some $e \in R_q$ with $\|e\|_\infty \leq P_{\mathsf{inp}+} \cdot B_{\mathsf{ct}}$.

Further, $t_0, t_1 \in R_q$ are distributed uniformly at random conditioned on this equation, as we switched the PRF output to random values.

Thus, by Lemma 1 we have

$$\mathsf{Round}(t_0) + \mathsf{Round}(t_1) = m \mod p$$

except with probability at most

$$N \cdot (\|e \cdot x\|_\infty + 1) \cdot p/q \leq N^2 \cdot P_{\mathsf{inp}+} \cdot B_{\mathsf{ct}} \cdot B_{\mathsf{max}} \cdot p/q + N \cdot p/q$$

over the choice of the shares t_0, t_1. A union bound yields thus correctness of multiplication with probability at least $1 - |P| \cdot N^2 \cdot P_{\mathsf{inp}+} \cdot B_{\mathsf{ct}} \cdot B_{\mathsf{max}} \cdot p/q - N \cdot p/q$.

This yields correctness of the output of terminal memory values. For the output of non-terminal values we obtain correctness of outputs except with probability B_{add}/q.

Altogether, we obtain that the HSS evaluation is correct with probability at least

$$\begin{aligned}\Pr^{\mathsf{cor}}_{\mathsf{skHSS}^2,(x^{(i)})_i,P,p}(\lambda) \geq & 1 - \mathrm{Adv}^{\mathsf{prf}}_{\mathsf{PRF},\mathcal{B}}(\lambda) - B_{\mathsf{add}}/q \\ & - |P| \cdot N^2 \cdot P_{\mathsf{inp}+} \cdot B_{\mathsf{ct}} \cdot B_{\mathsf{max}} \cdot p/q - N \cdot p/q.\end{aligned}$$

For the proof of security, we proceed as in the proof of security of our secret-key HSS (Theorem 3), except that now we only require KDM security with respect to the family of constant function $\Upsilon_{\mathsf{const}}$, because the encryptions are independent of the secret key itself.

C.4 HSS supporting SIMD

Theorem 6 (HSS supporting SIMD operations). *$R = \mathbb{Z}[X]/(X^n + 1)$ for $n \in \mathbb{N}$, $n \leq \mathsf{poly}(\lambda)$ a power of 2, such that $X^n + 1$ splits over R_r into pairwise different irreducible polynomials of degree $k \in \mathbb{N}$ for some prime $r \geq 2$ with $r \leq \mathsf{poly}(\lambda)$.*

- *Let $\mathbb{F}_r$ be a finite field of degree r.*
- *Let $B_{\mathsf{inp}} \in \mathbb{N}$ such that $p/B_{\mathsf{inp}} \geq \lambda^{\omega(1)}$, $q/(B_{\mathsf{inp}} \cdot p) \geq \lambda^{\omega(1)}$ and $B_{\mathsf{inp}} \geq r/2$ (i.e. such that for all $x \in R_r$ we have $\|x\|_\infty \leq B_{\mathsf{inp}}$).*
- *Let HSS be the HSS from Definiton 2 for the class of RMS programs with input space $[R]_{B_{\mathsf{inp}}}$ constructed from an encryption scheme with parameters $(p, q, d, B_{\mathsf{sk}}, B_{\mathsf{ct}}, R)$.*

Then there exists an HSS $\mathsf{HSS}^{\mathsf{simd}}$, with input space $\mathcal{I}^{\mathsf{simd}} := \mathbb{F}_{r^k}$, that supports evaluation of a single instruction on n/k inputs simultaneously, such that the following hold.

- ***Correctness:*** *For any security parameter $\lambda \in \mathbb{N}$, for any input vectors $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(\rho)} \in (\mathcal{I}^{\mathsf{simd}})^{n/k}$ and for any polynomially bounded RMS programs P with $P(x_j^{(1)}, \ldots, x_j^{(\rho)}) \neq \perp$ (for all $j \in \{1, \ldots, n/k\}$), there exists inputs $y^{(1)}, \ldots, y^{(\rho)} \in [R]_{B_{\mathsf{inp}}}$ and a PPT adversary $\mathcal{B}$ on the correctness of HSS such that*

$$\Pr^{\mathsf{cor}}_{\mathsf{HSS}^{\mathsf{simd}},(\mathbf{x}^{(i)})_i,P,r}(\lambda) \geq \Pr^{\mathsf{cor}}_{\mathsf{HSS},(y_i)_i,P,r}(\lambda).$$

- ***Security:*** *For every PPT adversary $\mathcal{A}$ on the security of the scheme $\mathsf{HSS}^{\mathsf{simd}}$, there exists an PPT adversary $\mathcal{B}$ on the security of HSS such that*

$$\mathrm{Adv}^{\mathsf{sec}}_{\mathsf{HSS}^{\mathsf{simd}},\mathcal{A}}(\lambda) \leq \mathrm{Adv}^{\mathsf{sec}}_{\mathsf{HSS},\mathcal{A}}(\lambda).$$

Proof. Let $\Psi\colon (\mathbb{F}_{r^k})^{n/k} \to R_r$ be an isomorphism and Ψ^{-1} its inverse. By the generalized Chinese remainder theorem and [37] both exist and are efficiently computable. For $i \in \{1, \ldots, n/k\}$ let $\Psi_i\colon R_r \to \mathbb{F}_{r^k}$ denote the i-th component of Ψ.

We define $\mathsf{HSS}^{\mathsf{simd}}$ as the homomorphic secret sharing scheme that for a program P and input $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(\rho)}$, sets up

– $(\mathsf{pk}, \mathsf{ek}_0, \mathsf{ek}_1) \leftarrow \mathsf{HSS.Gen}(1^\lambda)$,
– $\mathsf{ct}^{(i)} \leftarrow \mathsf{HSS.Enc}(1^\lambda, \mathsf{pk}, \Psi(\mathbf{x}^{(i)}))$,
– $y_b \leftarrow \mathsf{HSS.Eval}(b, \mathsf{ek}_b, (\mathbf{C}^{\Psi(\mathbf{x}^{(1)})}, \ldots, \mathbf{C}^{\Psi(\mathbf{x}^{(\rho)})}), P, r)$ and
– outputs $\Psi^{-1}(y_b)$.

Note that whenever correctness of HSS holds, we have $y_0 + y_1 = P(\Psi(\mathbf{x}^{(1)}), \ldots, \Psi(\mathbf{x}^{(\rho)})) \mod r$. For the following we consider all elements in R as elements of R_r. As Ψ is an isomorphism, we have

$$P\left(\Psi(\mathbf{x}^{(1)}), \ldots, \Psi(\mathbf{x}^{(\rho)})\right) = \Psi\left(P(x_1^{(1)}, \ldots, x_1^{(\rho)}), \ldots, P(x_{n/k}^{(1)}, \ldots, x_{n/k}^{(\rho)})\right)$$

over R_r. This yields

$$\begin{aligned}\Psi^{-1}(y_0) + \Psi^{-1}(y_1) = \Psi^{-1}(y_0 + y_1) &= \Psi^{-1}\left(P(\Psi(\mathbf{x}^{(1)}), \ldots, \Psi(\mathbf{x}^{(\rho)}))\right) \\ &= \left(P(x_1^{(1)}, \ldots, x_1^{(\rho)}), \ldots, P(x_{n/k}^{(1)}, \ldots, x_{n/k}^{(\rho)})\right)\end{aligned}$$

and thus

$$\mathrm{Pr}^{\mathsf{cor}}_{\mathsf{HSS}^{\mathsf{simd}}, (\mathbf{x}^{(i)})_i, P, r}(\lambda) \geq \mathrm{Pr}^{\mathsf{cor}}_{\mathsf{HSS}, (y_i)_i, P, r}(\lambda)$$

as required.

For security, note that from a PPT adversary $\mathcal{A}$ of the security of $\mathsf{HSS}^{\mathsf{simd}}$ we can construct an adversary $\mathcal{B}$ on the security of HSS as follows. On input $(b, \mathbf{x}_0, \mathbf{x}_1, \mathsf{state})$ of $\mathcal{A}$, the adversary $\mathcal{B}$ sends $(b, \Psi(\mathbf{x}_0), \Psi(\mathbf{x}_1), \mathsf{state})$ to its own security experiment. On receiving a tuple $(\mathsf{pk}, \mathsf{ek}_b, \mathsf{ct})$ back, $\mathcal{B}$ forwards $(\mathsf{pk}, \mathsf{ek}_b, \mathsf{ct})$ to $\mathcal{A}$. Finally, $\mathcal{B}$ forwards the bit β' sent by $\mathcal{A}$ to its own experiment. As $\mathsf{HSS}^{\mathsf{simd}}.\mathsf{Enc}(1^\lambda, \mathsf{pk}, \mathbf{x}_\beta)$ (the encryption that $\mathcal{A}$ expects to receive) corresponds to $\mathsf{HSS.Enc}(1^\lambda, \mathsf{pk}, \Psi(\mathbf{x}_\beta))$ (the encryption that $\mathcal{B}$ receives from its own security experiment), we have indeed

$$\mathrm{Adv}^{\mathsf{sec}}_{\mathsf{HSS}^{\mathsf{simd}}, \mathcal{A}}(\lambda) \leq \mathrm{Adv}^{\mathsf{sec}}_{\mathsf{HSS}, \mathcal{A}}(\lambda).$$

Remark 6. Note that a disadvantage of this approach is that in order to guarantee correctness, we need to have a worst-case bound on the execution size of the program P with respect to arbitrary values $y^{(1)}, \ldots, y^{(\rho)} \in R_r$, even if the input values $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(\rho)} \in (\mathbb{F}_{r_k})^{n/k}$ are bounded. This is due to the fact that Ψ does not preserve "smallness" of values.

D Further Instantiations and Details on Parameters

D.1 Proof of Lemma 6

Lemma 7 (Lemma 6, restated). *The scheme* LPR *(Figure 4) is a public-key encryption scheme with nearly-linear decryption over* $R = \mathbb{Z}[X]/(X^n + 1)$*, with ciphertext dimension* $d = 2$ *and bounds* B_{sk} *and* $B_{\mathsf{ct}} = B_{\mathsf{err}} \cdot (2h_{\mathsf{sk}} + 1)$.

Proof. Notice that for a ciphertext $\mathbf{c} = (c_0, c_1) = \mathsf{LPR.Enc}(m)$, we have

$$\langle \mathbf{c}, \mathbf{s} \rangle = c_0 + c_1 \cdot \widehat{s} = bv + e_1 + (q/p) \cdot m - avs + e_0 \widehat{s} = ev + e_1 + e_0 s + (q/p) \cdot m$$

This means that LPR satisfies property 3 of Definition 4, with noise bound B_{ct} given by the maximum of $\|ev + e_1 + e_0 s\|_\infty$. Since $\|e\|_\infty \leq B_{\mathsf{err}}$ and v has only h_{sk} non-zero coefficients of ± 1, it follows that the product ev has coefficients bounded by $B_{\mathsf{err}} \cdot h_{\mathsf{sk}}$. Summing up, the total noise bound in a fresh ciphertext is therefore $B_{\mathsf{ct}} = B_{\mathsf{err}} \cdot (2h_{\mathsf{sk}} + 1)$.

We conclude that LPR is a PKE with approximately linear decryption (Definition 4) and parameters $(p, q, d = 2, B_{\mathsf{sk}} = 1, B_{\mathsf{ct}}, R)$.

$\underline{\mathsf{Regev.Gen}(1^\lambda):}$

1. Sample $\mathbf{A} \leftarrow \mathbb{Z}_q^{M\times n}, \widehat{\mathbf{s}} \leftarrow \chi_{\mathsf{sk}}^n$ and $\mathbf{e} \leftarrow \chi^M$
2. Compute $\mathbf{b} = \mathbf{A}\cdot\widehat{\mathbf{s}} + \mathbf{e} \mod q$.
3. Let $\mathbf{s} = (1, \widehat{\mathbf{s}})$ and output $\mathsf{pk} = \mathbf{P} := (\mathbf{b} \| -\mathbf{A}) \in \mathbb{Z}_q^{M\times(n+1)}$ and $\mathsf{sk} = \mathbf{s}$.

$\underline{\mathsf{Regev.Enc}(\mathsf{pk}, m):}$

1. To encrypt $m \in \mathbb{Z}_p$, first let $\mathbf{m} = (m, 0, \ldots, 0) \in \mathbb{Z}_p^{n+1}$
2. Sample $\mathbf{r} \leftarrow \{0,1\}^M$
3. Output the ciphertext $\mathbf{c} = \mathbf{P}^T \cdot \mathbf{r} + (q/p)\cdot\mathbf{m} \mod q$

$\underline{\mathsf{Regev.OKDM}(\mathsf{pk}, m):}$

1. Compute $\mathbf{c}_i^0 = \mathsf{LPR.Enc}(0)$, for $i = 1, \ldots, n$ and $\mathbf{c}^m = \mathsf{LPR.Enc}(m)$.
2. Let $\mathbf{m} = (0, \ldots, 0, (q/p)\cdot m, \ldots, 0) \in \mathbb{Z}_q^{n+1}$ (where only the i-th component is non-zero)
3. Output the tuple $(\mathbf{c}^m, \mathbf{c}_1^0 + \mathbf{m}_1, \ldots, \mathbf{c}_n^0 + \mathbf{m}_n)$ as encryptions of $m\cdot\mathbf{s}$.

$\underline{\mathsf{Regev.DDec}(b, \mathbf{c}^x, \mathbf{t}_b):}$

1. Given a bit b, a ciphertext $\mathbf{c}^x$ and a share $\mathbf{t}_b$ of $m\cdot\mathbf{s}$, output the share

$$(\lfloor (p/q)\cdot\langle \mathbf{c}^x, \mathbf{t}_b\rangle \rceil \mod p) \mod q$$

where the reduction modulo p is into the range $(-p/2, \ldots, p/2]$.

Fig. 12: LWE-based instantiation of PKE with approximately linear decryption, with procedures for HSS from Section 3

D.2 Other Instantiations

As well as the efficient, RLWE-based construction from Section 4, our HSS can be instantiated based on a number of different lattice-based encryption schemes, including standard Regev encryption [41] and also the "lower-order symbol" variants of (R)LWE schemes, as described in Section 3.

Definition 10 (Decisional Learning With Errors). *Let $n \geq 1$ and $q \geq 2$ be integers. Let χ be an error distribution over $\mathbb{Z}$ and χ_{sk} be a secret key distribution over $\mathbb{Z}^n$. For $\mathbf{s} \leftarrow \chi_{\mathsf{sk}}$, define $\mathsf{LWE}_{\chi,\mathbf{s}}$ to be the distribution obtained by sampling $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ uniformly at random, $e \leftarrow \chi$ and outputting $(\mathbf{a}, b = \langle \mathbf{a}, \mathbf{s}\rangle + e) \in \mathbb{Z}_q^{n+1}$.*

The decisional-$\mathsf{LWE}_{n,q,\chi,\chi_{\mathsf{sk}}}$ problem is to distinguish polynomially many samples $(\mathbf{a}_i, b_i) \leftarrow \mathsf{LWE}_{\chi,\mathbf{s}}$ from the same number of samples taken from the uniform distribution on $(\mathbb{Z}_q^n, \mathbb{Z}_p)$, where the secret $\mathbf{s} \leftarrow \chi_{\mathsf{sk}}$.

Figure 12 shows the instantiation from standard Regev encryption based on LWE. The pseudorandomness of ciphertexts of Regev follows from a standard argument based on the leftover hash lemma and the decisional-LWE problem [41]. Likewise, correctness of the distributed decryption procedure can be analysed in the same way as the proof of Lemma 6, and correctness of the OKDM procedure follows from Lemma 3.

D.3 Parameter estimation

In this section we expand on our parameter estimation methodology for both our HSS, and the HSS derived from the BFV SHE scheme.

Parameter estimation for our HSS from ring-LWE. To estimate parameters for our scheme, we start with a choice of B_{max}, an upper bound on the ℓ_∞ norm of plaintexts throughout the computation, a

parameter $\sigma = 8$ for the RLWE noise distribution, a statistical security parameter $\kappa = 40$, and the number of non-zero entries in the secret key, $h_{\mathsf{sk}} = 64$. We choose the parameters so that each RMS multiplication has a failure probability no more than $2^{-\kappa}$, by adapting the formula from Lemma 5.

Plugging in $d = 2$, $P_{\mathsf{inp}+} = 1$ (assuming for simplicity there are not too many homomorphic additions of inputs), $B_{\mathsf{sk}} = 1$, and ignoring lower-order terms, this means we require[13]

$$2 \cdot N \cdot B_{\mathsf{max}} \cdot (2 \cdot N \cdot B_{\mathsf{ct}} \cdot p/q + h_{\mathsf{sk}}/p) \leq 2^{-\kappa} \tag{3}$$

To ensure this holds, we set $p = N \cdot B_{\mathsf{max}} \cdot h_{\mathsf{sk}} \cdot 2^{\kappa+2}$, and $q \geq 2^{\kappa+3} \cdot p \cdot N^2 \cdot B_{\mathsf{max}} \cdot B_{\mathsf{ct}}$, which, combined with the value of B_{ct} from the LPR scheme, give a bound on q as

$$q \geq 2^{2\kappa+5} \cdot N^3 \cdot B_{\mathsf{max}}^2 \cdot B_{\mathsf{err}} \cdot h_{\mathsf{sk}} \cdot (2h_{\mathsf{sk}} + 1) \tag{4}$$

To obtain a secure set of parameters, we fix an initial value of N, which defines the smallest possible q satisfying the above, and then iterate this process with increasing N until the parameters are predicted to have at least 80 bits of security according to the LWE estimator tool[14] by Albrecht et al. [1].

Parameter estimation for HSS from homomorphic encryption. We compare our HSS scheme with HSS constructed from the BFV somewhat homomorphic encryption scheme from ring-LWE, which is based on Brakerski's scale-invariant scheme [14], ported to the ring-LWE setting by Fan and Vercauteren [26]. To support HSS evaluation, we increase the modulus q of BFV ciphertexts so that after homomorphic evaluation, we can run our distributed decryption procedure to recover additive shares (modulo p) of the output with probability at least $1 - 2^{-\kappa}$.

In more detail, our parameter selection process is as follows. Given a multiplicative depth parameter L, we fix the noise standard deviation $\sigma = 8$, secret key weight $h_{\mathsf{sk}} = 64$ and relinearization parameter $w = 2^{32}$ (these are common choices from the literature, and consistent with our HSS), choose an initial dimension N, then find the smallest modulus q allowing evaluation of depth-L circuits followed by correct distributed decryption into additive shares. We remark that this results in a modulus q around 2^{κ} times larger than a standard FHE ciphertext, to allow for distributed decryption. We then use the LWE estimator tool to estimate the cost of various attacks; this process is iterated with increasing N until we obtain parameters with at least 80 bits of estimated security[15].

To find the size of q, we used the criterion $2 \cdot N \cdot \nu \cdot p/q \leq 2^{-\kappa}$ to ensure correct decryption into shares of all N coefficients of a ciphertext with noise magnitude ν and plaintext modulus $p|q$, with failure probability $2^{-\kappa}$ (cf. Lemma 1). For a binary secret key, the noise after evaluating a depth-L circuit can be bounded by $\nu \leq C_1^L \cdot V + L \cdot C_1^{L-1} \cdot C_2$ from [38], where

$$C_1 = (1 + 4/\delta) \cdot \delta^2 \cdot p, \quad C_2 = \delta^2 \cdot (1 + p^2) + \delta \cdot \log_w q \cdot w \cdot B_{\mathsf{err}}$$

Here, δ is a ring expansion factor measuring the amount by which the ℓ_∞ norm of ring elements can grow after multiplication. When $R = \mathbb{Z}[X]/(X^n + 1)$ we have a worst-case value of $\delta = N$, however, in practice the noise growth from homomorphic operations is much smaller than this, since the polynomials involved are all zero-centered and with small coefficients. So instead, we follow a heuristic approach taken in [32] and let $\delta = 2\sqrt{N}$. This is similar to parameter selection methods used in software libraries such as HElib [33] and SEAL [17], and can be analysed more formally using the canonical embedding norms of random variables.

[13] Here we have applied a small optimization to the original equation, replacing one N term by h_{sk}, which accounts for our choice of a sparse secret key and can be seen from the proof of Lemma 5.

[14] Available at `https://bitbucket.org/malb/lwe-estimator/`

[15] If 128-bit security is desired and not achieved, in all our examples it suffices to double the dimension and increase the modulus by a few bits.