Cryptography with Auxiliary Input and Trapdoor from Constant-Noise LPN

Yu Yu[1,2,3,4] and Jiang Zhang[2]

[1] Department of Computer Science and Engineering, Shanghai Jiao Tong University
[2] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China
[3] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[4] Westone Cryptologic Research Center, Beijing 100070, China
E-mail: {yuyuathk, jiangzhang09}@gmail.com

Abstract. Dodis, Kalai and Lovett (STOC 2009) initiated the study of the Learning Parity with Noise (LPN) problem with (static) exponentially hard-to-invert auxiliary input. In particular, they showed that under a new assumption (called Learning Subspace with Noise) the above is quasi-polynomially hard in the high (polynomially close to uniform) noise regime.

Inspired by the "sampling from subspace" technique by Yu (eprint 2009 / 467) and Goldwasser et al. (ITCS 2010), we show that standard LPN can work in a mode (reducible to itself) where the constant-noise LPN (by sampling its matrix from a random subspace) is robust against sub-exponentially hard-to-invert auxiliary input with comparable security to the underlying LPN. Plugging this into the framework of [DKL09], we obtain the same applications as considered in [DKL09] (i.e., CPA/CCA secure symmetric encryption schemes, average-case obfuscators, reusable and robust extractors) with resilience to a more general class of leakages, improved efficiency and better security under standard assumptions.

As a main contribution, under constant-noise LPN with certain sub-exponential hardness (i.e., $2^{\omega(n^{1/2})}$ for secret size n) we obtain a variant of the LPN with security on poly-logarithmic entropy sources, which in turn implies CPA/CCA secure public-key encryption (PKE) schemes and oblivious transfer (OT) protocols. Prior to this, basing PKE and OT on constant-noise LPN had been an open problem since Alekhnovich's work (FOCS 2003).

1 Introduction

Learning Parity with Noise. The computational version of learning parity with noise (LPN) assumption with parameters $n \in \mathbb{N}$ (length of secret) and $0 < \mu < 1/2$ (noise rate) postulates that for any $q = \mathsf{poly}(n)$ (number of queries) it is computationally infeasible for any probabilistic polynomial-time (PPT) algorithm to recover the random secret $\mathbf{x} \xleftarrow{\$} \{0,1\}^n$ given $(\mathbf{A},\ \mathbf{A}\cdot\mathbf{x}+\mathbf{e})$, where $\mathbf{a}$ is

a random $q \times n$ Boolean matrix, $\mathbf{e}$ follows $\mathcal{B}_\mu^q = (\mathcal{B}_\mu)^q$, $\mathcal{B}_\mu$ denotes the Bernoulli distribution with parameter μ (i.e., $\Pr[\mathcal{B}_\mu = 1] = \mu$ and $\Pr[\mathcal{B}_\mu = 0] = 1 - \mu$), '$\cdot$' denotes matrix vector multiplication over GF(2) and '+' denotes bitwise addition over GF(2). The decisional version of LPN simply assumes that $(\mathbf{A},\ \mathbf{A} \cdot \mathbf{x} + \mathbf{e})$ is pseudorandom. The two versions are polynomially equivalent [8,34,4].

Hardness of LPN. The computational LPN problem represents a well-known NP-complete problem "decoding random linear codes" [6] whose worst-case hardness is well-investigated. LPN was also extensively studied in learning theory, and it was shown in [21] that an efficient algorithm for LPN would allow to learn several important function classes such as 2-DNF formulas, juntas, and any function with a sparse Fourier spectrum. Under a constant noise rate, the best known LPN solvers [9,39] require time and query complexity both $2^{O(n/\log n)}$. The time complexity goes up to $2^{O(n/\log\log n)}$ when restricted to $q = \mathsf{poly}(n)$ queries [40], or even $2^{O(n)}$ given only $q = O(n)$ queries [42]. Under low noise rate $\mu = n^{-c}$ (for constant $0 < c < 1$), the best attacks [48,12,7,38,5] solve LPN with time complexity $2^{O(n^{1-c})}$ and query complexity $q = O(n)$ or more[5]. The low-noise LPN is mostly believed a stronger assumption than constant-noise LPN. In noise regime $\mu = O(1/\sqrt{n})$, LPN can be used to build public-key encryption (PKE) schemes and oblivious transfer (OT) protocols (more discussions below). Quantum algorithms are not known to have any advantages over classic ones in solving LPN, which makes LPN a promising candidate for "post-quantum cryptography". Furthermore, LPN enjoys simplicity and is more suited for weak-power devices (e.g., RFID tags) than other quantum-secure candidates such as LWE [46].

Cryptography in minicrypt. LPN was used as a basis for building lightweight authentication schemes against passive [29] and even active adversaries (e.g. [32,34], see [1] for a more complete literature). Kiltz et al. [37] and Dodis et al. [18] constructed randomized MACs from LPN, which implies a two-round authentication scheme with man-in-the-middle security. Lyubashevsky and Masny [41] gave an more efficient three-round authentication scheme from LPN (without going through the MAC transformation) and recently Cash, Kiltz, and Tessaro [13] reduced the round complexity to 2 rounds. Applebaum et al. [3] used LPN to construct efficient symmetric encryption schemes with certain key-dependent message (KDM) security. Jain et al. [30] constructed an efficient perfectly binding string commitment scheme from LPN. We refer to a recent survey [45] on the current state-of-the-art about LPN.

Cryptography beyond minicrypt. Alekhnovich [2] constructed the first (CPA secure) public-key encryption scheme from LPN with noise rate[6] $\mu = 1/\sqrt{n}$. By plugging the correlated products approach of [47] into Alekhnovich's CPA

[5] We are not aware of any non-trivial time-query tradeoff results to break low-noise LPN in time $2^{o(n^{1-c})}$ even with super-polynomial number of queries.

[6] More precisely, Alekhnovich's PKE is based on a variant called the Exact LPN whose noise vector is sampled from $\chi_{\mu q}^q$ for $\mu = \frac{1}{\sqrt{n}}$ (i.e., uniform random distribution over q-bit strings of Hamming weight μq), which is implied by LPN with noise rate μ.

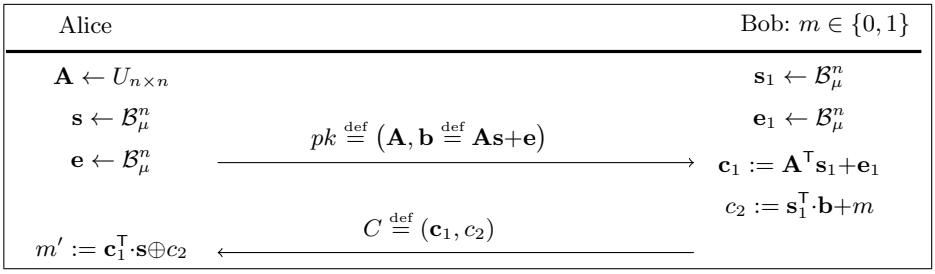

Fig. 1. A two-pass protocol by which Bob transmits a message bit m to Alice with passive security and noticeable correctness (for proper choice of μ), where Bob receives $m' = m+(\mathbf{s}_1^\mathsf{T}\cdot\mathbf{e})+(\mathbf{e}_1^\mathsf{T}\cdot\mathbf{s})$.

secure PKE scheme, Döttling et al. [20] constructed the first CCA secure PKE scheme from low-noise LPN. After observing that the complexity of the scheme in [20] was hundreds of times worse than Alekhnovich's original scheme, Kiltz et al. [36] proposed a neat and more efficient CCA secure construction by adapting the techniques from LWE-based encryption in [44] to the case of LPN. More recently, Döttling [19] constructed a PKE with KDM security. All the above schemes are based on LPN of noise rate $O(1/\sqrt{n})$. To see that noise rate $1/\sqrt{n}$ is inherently essential for PKE, we illustrate the (weakly correct) single-bit PKE protocol by Döttling et al. [20] in Figure 1, which is inspired by the counterparts based on LWE [46,23]. First, the decisional $\mathsf{LPN}_{\mu,n}$ assumption implies that $(\mathbf{A}, \mathbf{A}\mathbf{x}+\mathbf{e})$ is pseudorandom even when $\mathbf{x}$ is drawn from $X\sim\mathcal{B}_\mu^n$ (instead of $X\sim U_n$), which can be shown by a simple reduction [20]. Second, the passive security of the protocol is straightforward as $(pk, \mathbf{c}_1)$ is pseudorandom even when concatenated with the Goldreich-Levin[7] hardcore bit $\mathbf{s}_1^\mathsf{T}\cdot\mathbf{b}$ (replacing $\mathbf{b}$ with U_n by a hybrid argument). The final and most challenging part is correctness, i.e., m' needs to correlate with m at least noticeably. It is not hard to see for $n\mu^2 = O(1)$ and $\mathbf{e}, \mathbf{s} \leftarrow \mathcal{B}_\mu^n$ we have $\Pr[\langle\mathbf{e}, \mathbf{s}\rangle = 0] \geq 1/2 + \Omega(1)$, and thus noise rate $\mu = O(1/\sqrt{n})$ seems an inherent barrier[8] for the PKE to be correct. The scheme is "weak" in the sense that correctness is only $1/2 + \Omega(1)$ and it can be transformed into a standard CPA scheme (that encrypts multiple-bit messages with overwhelming correctness) using standard techniques (e.g., [20,15]). Notice a correct PKE scheme (with certain properties) yields also a (weak form of) 2-round oblivious transfer protocol against honest-but-curious receiver. Suppose that Alice has a choice $i \in \{0,1\}$, and she samples pk_i with trapdoor $\mathbf{s}$ (as described in the protocol) and a uniformly random pk_{1-i} without trapdoor.

[7] Typically (in the context of one-way functions), the Goldreich-Levin Theorem [25] assumes a uniformly random secret $\mathbf{s}$, which is however not necessary. A Markov argument suggests that $\mathbf{s}$ can follow any polynomial-time sampleable distribution, as long as f on $\mathbf{s}$ is hard to invert.

[8] In fact, $\mu = O(\sqrt{\log n/n})$ is sufficient to have a noticeable correctness, i.e., $1/2+1/\mathsf{poly}(n)$, but known PKE constructions avoid the strong noise by assuming noise rate $n^{-1/2}$ [36] or even lower rate $n^{-1/2-\epsilon}$ [2,20].

Upon receiving pk_0 and pk_1, Bob uses the scheme to encrypt two bits σ_0 and σ_1 under pk_0 and pk_1 respectively, and sends them to Alice. Alice can then recover σ_i and but knows nothing about σ_{1-i}. David et al. [16] constructed a universally composable OT under LPN with noise rate $1/\sqrt{n}$. Therefore, basing PKE (and OT) on LPN with noise rate $\mu = n^{-1/2+\epsilon}$ (and ideally a constant $0 < \mu < 1/2$) remains an open problem for the past decade.

LPN WITH AUXILIARY INPUT. Despite being only sub-exponentially secure, LPN is known to be robust against any constant-fraction of static linear leakages, i.e., for any constant $0 < \alpha < 1$ and any $f(\mathbf{x}; \mathbf{Z}) = (\mathbf{Z}, \mathbf{Zx})$ it holds that

$$\big(f(\mathbf{x}), \mathbf{A}, \mathbf{Ax} + \mathbf{e}\ \big) \overset{c}{\sim} \big(f(\mathbf{x}), \mathbf{A}, U_q\big)\ , \tag{1}$$

where $\mathbf{Z}$ is any $(1-\alpha)n \times n$ matrix (that can be sampled in polynomial time and independent of $\mathbf{A}$). The above can be seen by a change of basis so that the security is reducible from the LPN assumption with the same noise rate on a uniform secret of size αn. Motivated by this, Dodis, Kalai and Lovett [17] further conjectured that LPN is secure against any polynomial-time computable f such that 1) $\mathbf{x}$ given $f(\mathbf{x})$ has average min-entropy αn; or even 2) any f that is $2^{-\alpha n}$-hard-to-invert for PPT algorithms (see Definition 2 for a formal definition). Note the distinction between the two types of leakages: the former f is a lossy function and the latter can be even injective (the leakage $f(\mathbf{x})$ may already determine $\mathbf{x}$ in an information theoretical sense). However, they didn't manage to prove the above claim (i.e., LPN with auxiliary input) under standard LPN. Instead, they introduced a new assumption called Learning Subspace with Noise (LSN) as below, where the secret to be learned is the random subspace $\mathbf{V}$.

Assumption 1 (The LSN assumption [17]) *For any constant $\beta > 0$, there exists a polynomial $p = p_\beta(n)$ such that for any polynomial $q = \mathsf{poly}(n)$ the following two distributions are computationally indistinguishable:*

$$\big(\ (\mathbf{a}_1, \mathbf{V}\mathbf{a}_1 + U_n^{(1)} E_1), \cdots,\ (\mathbf{a}_q, \mathbf{V}\mathbf{a}_q + U_n^{(q)} E_q)\ \big) \overset{c}{\sim} \big(\ (\mathbf{a}_1, U_n^{(1)}), \cdots, (\mathbf{a}_q, U_n^{(q)})\ \big)\ ,$$

where $\mathbf{V} \sim U_{n \times \beta n}$ is a random $n \times \beta n$ matrix, $\mathbf{a}_1, \cdots, \mathbf{a}_q$ are vectors i.i.d. to $U_{\beta n}$, and $E_1, \cdots, E_q$ are Boolean variables (determining whether the respective noise is uniform randomness or nothing) i.i.d. to $\mathcal{B}_{1-\frac{1}{p}}$.

Then, the authors of [17] showed that LSN with parameters β and $p_\beta = p_\beta(n)$ implies the decisional LPN (as in (1)) under noise rate $\mu = (\frac{1}{2} - \frac{1}{4p_\beta})$ holds with $2^{-\alpha n}$-hard-to-invert auxiliary input (for any constant $\alpha > \beta$). Further, this yields many interesting applications such as CPA/CCA secure symmetric encryption schemes, average-case obfuscators for the class of point functions, reusable and robust extractors, all remain secure with exponentially hard-to-invert auxiliary input (see [17] for more details). We note that [17] mainly established the feasibility about cryptography with auxiliary input, and there remain issues to be addressed or improved. First, to counteract $2^{-\alpha n}$-hard-to-invert auxiliary input one needs to decide in advance the noise rate noise rate $1/2 - 1/4p_\beta$ (recall the

constraint $\beta < \alpha$). Second, Raz showed that for any constant β, $p_\beta = n^{\Omega(1)}$ is necessary (otherwise LSN can be broken in polynomial-time) and even with $p_\beta = n^{\Theta(1)}$ there exist quasi-polynomial attacks (see the full version of [17] for more discussions about Raz's attacks). Therefore, the security reduction in [17] is quite loose. As the main end result of [17], one needs a high-noise LPN for $\mu = 1/2 - 1/\mathsf{poly}(n)$ (and thus low efficiency due to the redundancy needed to make a correct scheme) only to achieve quasi-polynomial security (due to Raz's attacks) against $2^{-\alpha n}$-hard-to-invert leakage for some constant α (i.e., not any exponentially hard-to-invert leakage). Third, LSN is a new (and less well-studied) assumption and it was left as an open problem in [17] whether the aforementioned cryptographic applications can be based on the hardness of standard LPN, ideally admitting more general class of leakages, such as sub-exponentially or even quasi-polynomially hard-to-invert auxiliary input.

THE MAIN OBSERVATION. Yu [49] introduced the "sampling from subspace" technique to prove the above "LPN with auxiliary input" conjecture under standard LPN but the end result of [49] was invalid due to a flawed intermediate step. A similar idea was also used by Goldwasser et al. [26] in the setting of LWE, where the public matrix was drawn from a (noisy) random subspace. Informally, the observation (in our setting) is that, the decisional LPN with constant noise rate $0 < \mu < 1/2$ implies that for any constant $0 < \alpha < 1$, any 2^{-2n^α}-hard-to-invert f and any $q' = \mathsf{poly}(n)$ it holds that

$$(f(\mathbf{x}), \mathbf{A}', \mathbf{A}'\cdot\mathbf{x} + \mathbf{e}) \overset{c}{\sim} (\ f(\mathbf{x}), \mathbf{A}', U_{q'}\ ), \tag{2}$$

where $\mathbf{x} \sim U_n$[9], $\mathbf{e} \sim \mathcal{B}_\mu^{q'}$, and $\mathbf{A}'$ is a $q' \times n$ matrix with rows sampled from a random subspace of dimension $\lambda = n^\alpha$. Further, if the underlying LPN is $2^{\omega(n^{\frac{1}{1+\beta}})}$-hard[10] for any constant $\beta > 0$, then by setting $\lambda = \log^{1+\beta} n$, (2) holds for any $q' = \mathsf{poly}(n)$ and any $2^{-2\log^{1+\beta} n}$-hard-to-invert f. The rationale is that distribution $\mathbf{A}'$ can be considered as the multiplication of two random matrices $\mathbf{A} \overset{\$}{\leftarrow} \{0,1\}^{q'\times\lambda}$ and $\mathbf{V} \overset{\$}{\leftarrow} \{0,1\}^{\lambda\times n}$, i.e., $\mathbf{A}' \sim (\mathbf{A}\cdot\mathbf{V})$, where $\mathbf{V}$ constitutes the basis of the λ-dimensional random subspace and $\mathbf{A}$ is the random coin for sampling from $\mathbf{V}$. Unlike the LSN assumption whose subspace $\mathbf{V}$ is secret, the $\mathbf{V}$ and $\mathbf{A}$ in (2) are public coins (implied by $\mathbf{A}'$, see Remark 1). We have by the associative law $\mathbf{A}'\cdot\mathbf{x} = \mathbf{A}(\mathbf{V}\cdot\mathbf{x})$ and by the Goldreich-Levin theorem $\mathbf{V}\cdot\mathbf{x}$ is a pseudo-random secret (even conditioned on $\mathbf{V}$ and $f(\mathbf{x})$), and thus (2) is reducible from the standard decisional LPN on noise rate μ, secret size λ and query complexity q'. Concretely, assume that the LPN problem is $2^{\omega(n^{3/4})}$-hard then by setting $\lambda = n^{2/3}$ (resp., $\lambda = \log^{4/3} n$) we have that (2) is $2^{\Omega(n^{1/2})}$-secure (resp., $n^{\omega(1)}$-secure) with any auxiliary input that is $2^{-2n^{2/3}}$-hard (resp., $2^{-2\log^{4/3} n}$-hard) to

[9] We assume $\mathbf{x} \sim U_n$ to be in line with [17], but actually our results hold for any efficiently sampleable $\mathbf{x}$ as long as $\mathbf{x}$ given $f(\mathbf{x})$ is $2^{-2\lambda}$-hard-to-invert.

[10] Informally, we say that a cryptographic scheme/problem Π is T-secure/hard if every probabilistic adversary of time (and query, if applicable) complexity T achieve advantage no more than $1/T$ in breaking/solving Π.

invert. Plugging (2) into the framework of [17] we obtain the same applications (CPA/CCA secure symmetric encryption schemes, average-case obfuscators for point functions, reusable and robust extractors) under standard (constant-noise) LPN with improved efficiency (as the noise is constant rather than polynomially close to uniform) and tighter security against sub-exponentially (or even quasi-polynomially) hard-to-invert auxiliary input.

PKE FROM CONSTANT-NOISE LPN. More surprisingly, we show a connection from "LPN with auxiliary input" to "basing PKE on (constant-noise) LPN". The feasibility can be understood by the single-bit weak PKE in Figure 1 with some modifications: assume that LPN is $2^{\omega(n^{\frac{1}{2}})}$-hard (i.e., $\beta = 1$), then for $\lambda = \log^2 n/4$ we have that (2) holds on any $\mathbf{x} \sim X$ with min-entropy $\mathbf{H}_\infty(X) \geq \log^2 n/2$. Therefore, by replacing the uniform matrix $\mathbf{A}$ with $\mathbf{A}' \sim (U_{n\times\lambda} \cdot U_{\lambda\times n})$, and sampling $\mathbf{s},\mathbf{s}_1 \leftarrow X$ and $\mathbf{e},\mathbf{e}_1 \leftarrow \mathcal{B}_\mu^n$ for constant μ and $X \sim \chi_{\log n}^n$ [11], we get that $\mathbf{s}_1^\mathsf{T}\mathbf{e}$ and $\mathbf{e}_1^\mathsf{T}\mathbf{s}$ are both $(1/2 + 1/\mathsf{poly}(n))$-biased to 0 independently, and thus the PKE scheme has noticeable correctness. We then transform the weak PKE into a full-fledged CPA secure scheme, where the extension is not trivial (more than a straightforward parallel repetition plus error-correction codes). In particular, neither $X \sim \chi_{\log n}^n$ or $X \sim \mathcal{B}_{\log n/n}^n$ can guarantee security and correctness simultaneously and thus additional ideas are needed (more details deferred to Section 4.3).

PKE WITH CCA SECURITY. Once we have a CPA scheme based on constant-noise LPN, we can easily extend it to a CCA one by using the techniques in [20], and thus suffer from the same performance slowdown as that in [20]. A natural question is whether we can construct a simpler and more efficient CCA scheme as that in [36]. Unfortunately, the techniques in [36] do not immediately apply to the case of constant-noise LPN. The reason is that in order to employ the ideas from the LWE-based encryption scheme [44], the scheme in [36] has to use a variant of LPN (called knapsack LPN), and the corresponding description key is exactly the secret of some knapsack LPN instances. Even though there is a polynomial time reduction [43] from the LPN problem to the knapsack LPN problem, such a reduction will map the noise distribution of the LPN problem into the secret distribution of the knapsack LPN problem. If we directly apply the techniques in [36], the resulting scheme will not have any guarantee of correctness because the corresponding decryption key follows the Bernoulli distribution with constant parameter μ. Recall that for the correctness of our CPA secure PKE scheme, the decryption key cannot simply be chosen from either $\chi_{\log n}^n$ or $\mathcal{B}_{\log n/n}^n$. Fortunately, based on several new observations and some new technical lemmas, we mange to adapt the idea of [44,36] to construct a simpler and efficient CCA secure PKE scheme from constant-noise LPN.

OT FROM CONSTANT-NOISE LPN. PKE and OT are incomparable in general [24]. But if the considered PKE scheme has some additional properties, then

[11] Recall that for $m \ll n$ we have by Stirling's approximation that $\binom{n}{m} \approx n^m/m!$ and thus $\chi_{\log n}^n$ (uniform distribution over n-bit strings of Hamming weight $\log n$) is of min-entropy roughly $\log^2 n - \log n \log\log n \geq \log^2 n/2$.

we can build OT protocol from it in a black-box way [24]. Gertner et al. [24] showed that if the public key of some CPA secure PKE scheme can be indistinguishably sampled (without knowing the corresponding secret key) from the public key distribution produced by honestly running the key generation algorithm, then we can use it to construct an OT protocol with honest parties (and thus can be transformed into a standard OT protocol by using zero-knowledge proof). It is easy to check that our CPA secure PKE scheme satisfies this property under the LPN assumption. Besides, none of the techniques used in transforming Alekhnovich's CPA secure PKE scheme into a universally composable OT protocol [16] prevent us from obtaining a universally composable OT protocol from our CPA secure PKE scheme. In summary, our results imply that there exists (universally composable) OT protocol under constant-noise LPN assumption. We omit the details, and refer to [24,16] for more information.

2 Preliminaries

NOTATIONS AND DEFINITIONS. We use capital letters (e.g., X, Y) for random variables and distributions, standard letters (e.g., x, y) for values, and calligraphic letters (e.g. $\mathcal{X}$, $\mathcal{E}$) for sets and events. Vectors are used in the column form and denoted by bold lower-case letters (e.g., $\mathbf{a}$). We treat matrices as the sets of its column vectors and denoted by bold capital letters (e.g., $\mathbf{A}$). The support of a random variable X, denoted by $\mathsf{Supp}(X)$, refers to the set of values on which X takes with non-zero probability, i.e., $\{x : \Pr[X = x] > 0\}$. For set $\S$ and binary string s, $|\S|$ denotes the cardinality of $\S$ and $|s|$ refers to the Hamming weight of s. We use $\mathcal{B}_\mu$ to denote the Bernoulli distribution with parameter μ, i.e., $\Pr[\mathcal{B}_\mu = 1] = \mu$, $\Pr[\mathcal{B}_\mu = 0] = 1 - \mu$, while $\mathcal{B}_\mu^q$ denotes the concatenation of q independent copies of $\mathcal{B}_\mu$. We use χ_i^n to denote a uniform distribution over $\{\mathbf{e} \in \{0,1\}^n : |\mathbf{e}| = i\}$. We denote by $\mathcal{D}_\lambda^{n_1 \times n} \stackrel{\text{def}}{=} (U_{n_1 \times \lambda} \cdot U_{\lambda \times n})$ to be a matrix distribution induced by multiplying two random matrices. For $n, q \in \mathbb{N}$, U_n (resp., $U_{q \times n}$) denotes the uniform distribution over $\{0,1\}^n$ (resp., $\{0,1\}^{q \times n}$) and independent of any other random variables in consideration, and $f(U_n)$ (resp., $f(U_{q \times n})$) denotes the distribution induced by applying function f to U_n (resp., $U_{q \times n}$). $X \sim D$ denotes that random variable X follows distribution D. We use $s \leftarrow S$ to denote sampling an element s according to distribution S, and let $s \xleftarrow{\$} \S$ denote sampling s uniformly from set $\S$.

ENTROPY NOTIONS. For $0 < \mu < 1/2$, the binary entropy function is defined as $\mathbf{H}(\mu) \stackrel{\text{def}}{=} \mu \log(1/\mu) + (1-\mu)\log(1/(1-\mu))$. We define the Shannon entropy and min-entropy of a random variable X respectively, i.e.,

$$\mathbf{H}_1(X) \stackrel{\text{def}}{=} \sum_{x \in \mathsf{Supp}(X)} \Pr[X = x] \log \frac{1}{\Pr[X = x]}, \quad \mathbf{H}_\infty(X) \stackrel{\text{def}}{=} \min_{x \in \mathsf{Supp}(X)} \log(1/\Pr[X = x]) \ .$$

Note that $\mathbf{H}_1(\mathcal{B}_\mu) = \mathbf{H}(\mu)$. The average min-entropy of a random variable X conditioned on another random variable Z is defined as

$$\mathbf{H}_\infty(X|Z) \stackrel{\text{def}}{=} -\log\left(\mathbb{E}_{z \leftarrow Z}\left[2^{-\mathbf{H}_\infty(X|Z=z)}\right]\right) \ .$$

INDISTINGUISHABILITY AND STATISTICAL DISTANCE. We define the (t,ε)- *computational distance* between random variables X and Y, denoted by $X \underset{(t,\varepsilon)}{\sim} Y$, if for every probabilistic distinguisher $\mathcal{D}$ of running time t it holds that

$$\mid \Pr[\mathcal{D}(X)=1] - \Pr[\mathcal{D}(Y)=1] \mid \leq \varepsilon \ .$$

The *statistical distance* between X and Y, denoted by $\mathsf{SD}(X,Y)$, is defined by

$$\mathsf{SD}(X,Y) \stackrel{\mathsf{def}}{=} \frac{1}{2}\sum_{x} |\Pr[X=x] - \Pr[Y=x]| \ .$$

Computational/statistical indistinguishability is defined with respect to distribution ensembles (indexed by a security parameter). For example, $X \stackrel{\mathsf{def}}{=} \{X_n\}_{n\in\mathbb{N}}$ and $Y \stackrel{\mathsf{def}}{=} \{Y_n\}_{n\in\mathbb{N}}$ are computationally indistinguishable, denoted by $X \stackrel{c}{\sim} Y$, if for every $t = \mathsf{poly}(n)$ there exists $\varepsilon = \mathsf{negl}(n)$ such that $X \underset{(t,\varepsilon)}{\sim} Y$. X and Y are statistically indistinguishable, denoted by $X \stackrel{s}{\sim} Y$, if $\mathsf{SD}(X,Y) = \mathsf{negl}(n)$.

SIMPLIFYING NOTATIONS. To simplify the presentation, we use the following simplified notations. Throughout, n is the security parameter and most other parameters are functions of n, and we often omit n when clear from the context. For example, $q = q(n) \in \mathbb{N}$, $t = t(n) > 0$, $\epsilon = \epsilon(n) \in (0,1)$, and $m = m(n) = \mathsf{poly}(n)$, where poly refers to some polynomial.

Definition 1 (Learning Parity with Noise). *The* ***decisional*** $\mathsf{LPN}_{\mu,n}$ *problem (with secret length n and noise rate $0 < \mu < 1/2$) is hard if for every $q = \mathsf{poly}(n)$ we have*

$$(\mathbf{A},\ \mathbf{A}\cdot\mathbf{x}+\mathbf{e}) \stackrel{c}{\sim} (\mathbf{A}, U_q) \ , \tag{3}$$

where $q\times n$ matrix $\mathbf{A} \sim U_{q\times n}$, $\mathbf{x} \sim U_n$ and $\mathbf{e} \sim \mathcal{B}_\mu^q$. The ***computational*** $\mathsf{LPN}_{\mu,n}$ *problem is hard if for every $q = \mathsf{poly}(n)$ and every PPT algorithm $\mathcal{D}$ we have*

$$\Pr[\ \mathcal{D}(\mathbf{A},\ \mathbf{A}\cdot\mathbf{x}+\mathbf{e}) = \mathbf{x}\ ] \ = \ \mathsf{negl}(n) \ , \tag{4}$$

where $\mathbf{A} \sim U_{q\times n}$, $\mathbf{x} \sim U_n$ and $\mathbf{e} \sim \mathcal{B}_\mu^q$.

LPN WITH SPECIFIC HARDNESS. *We say that the decisional (resp., computational) $\mathsf{LPN}_{\mu,n}$ is T-hard if for every $q \leq T$ and every probabilistic adversary of running time T the distinguishing (resp., inverting) advantage in (3) (resp., (4)) is upper bounded by $1/T$.*

Definition 2 (Hard-to-invert function). *Let n be the security parameter and let $\kappa = \omega(\log n)$. A polynomial-time computable function $f : \{0,1\}^n \to \{0,1\}^l$ is $2^{-\kappa}$-hard-to-invert if for every PPT adversary $\mathcal{A}$*

$$\Pr_{\mathbf{x}\sim U_n}[\ \mathcal{A}(f(\mathbf{x})) = \mathbf{x}\ ] \ \leq \ 2^{-\kappa} \ .$$

Lemma 1 (Union bound). *Let $\mathcal{E}_1, \cdots, \mathcal{E}_l$ be any (not necessarily independent) events such that $\Pr[\mathcal{E}_i] \geq (1-\epsilon_i)$ for every $1 \leq i \leq l$, then we have*

$$\Pr[\ \mathcal{E}_1 \wedge \cdots \wedge \mathcal{E}_l\ ] \ \geq\ 1 - (\epsilon_1 + \cdots + \epsilon_l)\ .$$

We will use the following (essentially the Hoeffding's) bound on the Hamming weight of a high-noise Bernoulli vector.

Lemma 2. *For any $0 < p < 1/2$ and $\delta \leq (\frac{1}{2} - p)$, we have*

$$\Pr[\ |\mathcal{B}_\delta^q| > (\frac{1}{2} - \frac{p}{2})q\ ] < \exp^{-\frac{p^2 q}{8}}\ .$$

3 Learning Parity with Noise with Auxiliary Input

3.1 Leaky Sources and (Pseudo)randomness Extraction

We define below two types of leaky sources and recall two technical lemmas for (pseudo)randomness extraction from the respective sources, where $\mathbf{x}$ for TYPE-II source is assumed to be uniform only for alignment with [17] (see Footnote 7).

Definition 3 (Leaky sources). *Let $\mathbf{x}$ be any random variable over $\{0,1\}^n$ and let $f : \{0,1\}^n \to \{0,1\}^l$ be any polynomial-time computable function. $(\mathbf{x}, f(\mathbf{x}))$ is called an (n,κ) TYPE-I (resp., TYPE-II) leaky source if it satisfies condition 1 (resp., condition 2) below:*

1. ***Min-entropy leaky sources.*** *$\mathbf{H}_\infty(\mathbf{x}|f(\mathbf{x})) \geq \kappa$ and $f(\mathbf{x})$ is polynomial-time sampleable.*
2. ***Hard-to-invert leaky sources.*** *$\mathbf{x} \sim U_n$ and f is $2^{-\kappa}$-hard-to-invert.*

Lemma 3 (Goldreich-Levin Theorem [25]). *Let n be a security parameter, let $\kappa = \omega(\log n)$ be polynomial-time computable from n, and let $f : \{0,1\}^n \to \{0,1\}^l$ be any polynomial-time computable function that is $2^{-\kappa}$-hard-to-invert. Then, for any constant $0 < \beta < 1$ and $\lambda = \lceil \beta\kappa \rceil$, it holds that*

$$(f(\mathbf{x}), \mathbf{V}, \mathbf{V}\cdot\mathbf{x}) \stackrel{c}{\sim} (f(\mathbf{x}), \mathbf{V}, U_\lambda)\ ,$$

where $\mathbf{x} \sim U_n$ and $\mathbf{V} \sim U_{\lambda \times n}$ is a random $\lambda \times n$ Boolean matrix.

Lemma 4 (Leftover hash lemma [28]). *Let $(X, Z) \in \mathcal{X} \times \mathcal{Z}$ be any joint random variable with $\mathbf{H}_\infty(X|Z) \geq k$, and let $\mathcal{H} = \{h_\mathbf{V} : \mathcal{X} \to \{0,1\}^l, \mathbf{V} \in \{0,1\}^s\}$ be a family of universal hash functions, i.e., for any $x_1 \neq x_2 \in \mathcal{X}$, $\Pr_{\mathbf{V} \stackrel{\$}{\leftarrow} \{0,1\}^s}[h_\mathbf{V}(x_1) = h_\mathbf{V}(x_2)] \leq 2^{-l}$. Then, it holds that*

$$\mathsf{SD}\left(\ (Z, \mathbf{V}, h_\mathbf{V}(X))\ ,\ (Z, \mathbf{V}, U_l\ )\right)\ \leq\ 2^{l-k}\ ,$$

where $\mathbf{V} \sim U_s$.

3.2 The Main Technical Lemma and Immediate Applications

Inspired by [49,26], we state a technical lemma below where the main difference is that we sample from a random subspace of sublinear-sized dimension (rather than linear-sized one [49] or from a noisy subspace in the LWE setting [26]).

Theorem 1 (LPN with hard-to-invert auxiliary input). *Let n be a security parameter and let $0 < \mu < 1/2$ be any constant. Assume that the decisional $\mathsf{LPN}_{\mu,n}$ problem is hard, then for every constant $0 < \alpha < 1$, $\lambda = n^{\alpha}$, $q' = \mathsf{poly}(n)$, and every $(n, 2\lambda)$ TYPE-I or TYPE-II leaky source $(\mathbf{x}, f(\mathbf{x}))$, we have*

$$(f(\mathbf{x}), \mathbf{A}', \mathbf{A}'\cdot\mathbf{x} + \mathbf{e}) \overset{c}{\sim} (\ f(\mathbf{x}), \mathbf{A}', U_{q'}\ ), \tag{5}$$

where $\mathbf{e} \sim \mathcal{B}_{\mu}^{q'}$, and $\mathbf{A}' \sim \mathcal{D}_{\lambda}^{q' \times n}$ is a $q' \times n$ matrix, i.e., $\mathbf{A}' \sim (\mathbf{A}\cdot\mathbf{V})$ for random matrices $\mathbf{A} \overset{\$}{\leftarrow} \{0,1\}^{q' \times \lambda}$ and $\mathbf{V} \overset{\$}{\leftarrow} \{0,1\}^{\lambda \times n}$.

Furthermore, if the $\mathsf{LPN}_{\mu,n}$ problem is $2^{\omega(n^{\frac{1}{1+\beta}})}$-hard for any constant $\beta > 0$ and any superconstant hidden by $\omega(\cdot)$ then the above holds for any $\lambda = \Theta(\log^{1+\beta} n)$, any $q' = \mathsf{poly}(n)$ and any $(n, 2\lambda)$ TYPE-I/TYPE-II leaky source.

Remark 1 (Closure under composition). The random subspace $\mathbf{V}$ and the random coin $\mathbf{A}$ can be public as well, which is seen from the proof below but omitted from (5) to avoid redundancy (since they are implied by $\mathbf{A}'$). That is, there exists a PPT Simu such that $(\mathbf{A}', \mathsf{Simu}(\mathbf{A}'))$ is $2^{-\Omega(n)}$-close to $(\mathbf{A}', (\mathbf{A},\mathbf{V}))$. Therefore, (5) can be written in an equivalent form that is closed under composition, i.e., for any $q' = \mathsf{poly}(n)$ and $l = \mathsf{poly}(n)$

$$\left(f(\mathbf{x}), \mathbf{V}, \left(\mathbf{A}_i, (\mathbf{A}_i\cdot\mathbf{V})\cdot\mathbf{x} + \mathbf{e}_i\right)_{i=1}^{l}\right) \overset{c}{\sim} \left(f(\mathbf{x}), \mathbf{V}, \left(\mathbf{A}_i, U_{q'}^{(i)}\right)_{i=1}^{l}\right) ,$$

where $\mathbf{A}_1, \cdots, \mathbf{A}_l \overset{\$}{\leftarrow} \{0,1\}^{q' \times \lambda}$, $\mathbf{e}_1, \cdots, \mathbf{e}_l \sim \mathcal{B}_{\mu}^{q'}$ and $\mathbf{V} \overset{\$}{\leftarrow} \{0,1\}^{\lambda \times n}$. This will be a useful property for constructing symmetric encryption schemes w.r.t. hard-to-invert auxiliary input (see more details in [17]).

Proof of Theorem 1. We have by the assumption of $(\mathbf{x}, f(\mathbf{x}))$ and Lemma 3 or Lemma 4 that

$$\begin{aligned} &(f(\mathbf{x}), \mathbf{V}, \mathbf{V}\cdot\mathbf{x}) \overset{c}{\sim} (f(\mathbf{x}), \mathbf{V}, \mathbf{y}) \\ \Rightarrow\ &(f(\mathbf{x}), (\mathbf{A}, \mathbf{V}), (\mathbf{A}\cdot\mathbf{V})\cdot\mathbf{x}+\mathbf{e}) \overset{c}{\sim} (f(\mathbf{x}), (\mathbf{A}, \mathbf{V}), \mathbf{A}\cdot\mathbf{y} + \mathbf{e}) \ . \end{aligned}$$

where $\mathbf{y} \sim U_{\lambda}$. Next, consider T-hard decisional $\mathsf{LPN}_{\mu,\lambda}$ problem on uniform secret $\mathbf{y}$ of length λ (instead of n), which postulates that for any $q' \leq T$

$$\begin{aligned} &(\mathbf{A}, \mathbf{A}\cdot\mathbf{y}+\mathbf{e}) \underset{T, 1/T}{\sim} (\mathbf{A}, U_{q'}) \\ \Rightarrow\ &(f(\mathbf{x}), (\mathbf{A}, \mathbf{V}), \mathbf{A}\cdot\mathbf{y}+\mathbf{e}) \underset{T-\mathsf{poly}(n),\ 1/T}{\sim} (f(\mathbf{x}), (\mathbf{A}, \mathbf{V}), U_{q'}) \ . \end{aligned}$$

Under the LPN assumption with standard asymptotic hardness (i.e., $T = \lambda^{\omega(1)}$) and by setting parameter $\lambda = n^{\alpha}$ we have $T = n^{\omega(1)}$, which suffices for our purpose since for any $q' = \mathsf{poly}(n)$, any PPT adversary wins the above distinguishing game with advantage no greater than $n^{-\omega(1)}$. In case that $\mathsf{LPN}_{\mu,\lambda}$ is $2^{\omega(n^{\frac{1}{1+\beta}})}$-hard, substitution of $\lambda = \Theta(\log^{1+\beta} n)$ into $T = 2^{\omega(\lambda^{\frac{1}{1+\beta}})}$ also yields $T = n^{\omega(1)}$. Therefore, in both cases the above two ensembles are computationally indistinguishable in security parameter n. The conclusion then follows by a triangle inequality. □

A COMPARISON WITH [17]. The work of [17] proved results similar to Theorem 1. In particular, [17] showed that the LSN assumption with parameters β and $p = \mathsf{poly}_{\beta}(n)$ implies LPN with $2^{-\alpha n}$-hard auxiliary input (for constant $\alpha > \beta$), noise rate $\mu = 1/2 - 1/4p$ and quasi-polynomial security (in essentially the same form as (5) except for a uniform matrix $\mathbf{A}'$). In comparison, by sampling $\mathbf{A}'$ from a random subspace of sublinear dimension $\lambda = n^{\alpha}$ (for $0 < \alpha < 1$), constant-noise LPN implies that (5) holds with $2^{-\Omega(n^{\alpha})}$-hard auxiliary input, constant noise and comparable security to the underlying LPN. Furthermore, assume constant-noise LPN with $2^{\omega(n^{\frac{1}{1+\beta}})}$-hardness (for constant $\beta > 0$), then (2) holds for $2^{-\Omega(\log^{1+\beta})}$-hard auxiliary input, constant noise and quasi-polynomial security.

IMMEDIATE APPLICATIONS. This yields the same applications as considered in [17], such as CPA/CCA secure symmetric encryption schemes, average-case obfuscators for point functions, reusable and robust extractors, all under standard (constant-noise) LPN with improved efficiency (by bringing down the noise rate) and tighter security against sub-exponentially (or even quasi-polynomially) hard-to-invert auxiliary input. The proofs simply follow the route of [17] and can be informally explained as: the technique (by sampling from random subspace) implicitly applies pseudorandomness extraction (i.e., $\mathbf{y} = \mathbf{V} \cdot \mathbf{x}$) so that the rest of the scheme is built upon the security of $(\mathbf{A}, \mathbf{A}\mathbf{y} + \mathbf{e})$ on secret $\mathbf{y}$ (which is pseudorandom even conditioned on the leakage), and thus the task is essentially to obtain the aforementioned applications from standard LPN (without auxiliary input). In other words, our technique allows to transform any applications based on constant-noise LPN into the counterparts with auxiliary input under the same assumption. Therefore, we only sketch some applications in the full version of this work and refer to [17] for the redundancy.

4 CPA Secure PKE from Constant-Noise LPN

We show a more interesting application, namely, to build public-key encryption schemes from constant-noise LPN, which has been an open problem since the work of [2]. We refer to Appendix A.2 for standard definitions of public-key encryption schemes, correctness and CPA/CCA security.

4.1 Technical Lemmas

We use the following technical tool to build PKE scheme from constant-noise LPN. It would have been an immediate corollary of Theorem 1 for sub-exponential hard LPN on squared-logarithmic min-entropy sources (i.e., $\beta = 1$), except for the fact that the leakage is also correlated with noise. Notice that we lose the "closure under composition" property by allowing leakage to be correlated with noise, and thus our PKE scheme will avoid this property.

Theorem 2 (LPN on squared-log entropy). *Let n be a security parameter and let $0 < \mu < 1/2$ be any constant. Assume that the computational $\mathsf{LPN}_{\mu,n}$ problem is $2^{\omega(n^{\frac{1}{2}})}$-hard (for any superconstant hidden by $\omega(\cdot)$), then for every $\lambda = \Theta(\log^2 n)$, $q' = \mathsf{poly}(n)$, and every polynomial-time sampleable $\mathbf{x} \in \{0,1\}^n$ with $\mathbf{H}_\infty(\mathbf{x}) \geq 2\lambda$ and every probabilistic polynomial-time computable function $f : \{0,1\}^{n+q'} \times \mathcal{Z} \to \{0,1\}^{O(\log n)}$ with public coin Z, we have*

$$\big(f(\mathbf{x},\mathbf{e};Z), Z, \mathbf{A}', \mathbf{A}'\cdot\mathbf{x}+\mathbf{e}\big) \overset{c}{\sim} \big(f(\mathbf{x},\mathbf{e};Z), Z, \mathbf{A}', U_{q'}\big),$$

where noise vector $\mathbf{e} \sim \mathcal{B}_\mu^{q'}$ and $q' \times n$ matrix $\mathbf{A}' \sim \mathcal{D}_\lambda^{q'\times n}$.

Proof sketch. It suffices to adapt the proof of Theorem 1 as follows. First, observe that (by the chain rule of min-entropy)

$$\mathbf{H}_\infty(\mathbf{x}|f(\mathbf{x},\mathbf{e};Z),Z,\mathbf{e}) \geq \mathbf{H}_\infty(\mathbf{x}|Z,\mathbf{e}) - O(\log n) = \mathbf{H}_\infty(\mathbf{x}) - O(\log n) \geq 2\lambda - O(\log n).$$

For our convenience, write $\mathbf{A}' \sim (\mathbf{A}\cdot\mathbf{V})$ for $\mathbf{A} \sim U_{q'\times\lambda}$, $\mathbf{V} \sim U_{\lambda\times n}$, and let $\mathbf{y}, \mathbf{r} \sim U_\lambda$. Then, we have by Lemma 4

$$\begin{aligned}
&(f(\mathbf{x},\mathbf{e};Z), Z, \mathbf{e}, \mathbf{V}, \mathbf{V}\cdot\mathbf{x}) \overset{s}{\sim} (f(\mathbf{x},\mathbf{e};Z), Z, \mathbf{e}, \mathbf{V}, \mathbf{y}) \\
\Rightarrow\ &(f(\mathbf{x},\mathbf{e};Z), Z, (\mathbf{A}\cdot\mathbf{V}), (\mathbf{A}\cdot\mathbf{V})\cdot\mathbf{x}+\mathbf{e}) \overset{s}{\sim} (\ f(\mathbf{x},\mathbf{e};Z), Z, (\mathbf{A}\cdot\mathbf{V}), \mathbf{A}\cdot\mathbf{y}+\mathbf{e}\ )\ .
\end{aligned}$$

Next, $2^{\omega(\lambda^{\frac{1}{2}})}$-hard computational $\mathsf{LPN}_{\mu,\lambda}$ problem with secret size λ postulates that for any $q' \leq 2^{\omega(\lambda^{\frac{1}{2}})} = n^{\omega(1)}$ (recall $\lambda = \Theta(\log^2 n)$) and any probabilistic $\mathcal{D}$, $\mathcal{D}'$ of running time $n^{\omega(1)}$

$$\begin{aligned}
&\Pr[\ \mathcal{D}'(\mathbf{A},\ \mathbf{A}\cdot\mathbf{y}+\mathbf{e}) = \mathbf{y}\ ] \ =\ n^{-\omega(1)} \\
\Rightarrow\ &\Pr[\ \mathcal{D}'(f(\mathbf{x},\mathbf{e};Z), Z, \mathbf{A}, \mathbf{A}\cdot\mathbf{y}+\mathbf{e}) = \mathbf{y}\ ] \ =\ n^{-\omega(1)} \\
\Rightarrow\ &(f(\mathbf{x},\mathbf{e};Z), Z, \mathbf{A}, \mathbf{A}\cdot\mathbf{y}+\mathbf{e}, \mathbf{r}, \mathbf{r}^\mathsf{T}\cdot\mathbf{y}) \overset{c}{\sim} (f(\mathbf{x},\mathbf{e};Z), Z, \mathbf{A}, \mathbf{A}\cdot\mathbf{y}+\mathbf{e}, \mathbf{r}, U_1) \\
\Rightarrow\ &(f(\mathbf{x},\mathbf{e};Z), Z, \mathbf{A}, \mathbf{A}\cdot\mathbf{y}+\mathbf{e}) \overset{c}{\sim} (f(\mathbf{x},\mathbf{e};Z), Z, \mathbf{A}, U_{q'}) \\
\Rightarrow\ &(f(\mathbf{x},\mathbf{e};Z), Z, (\mathbf{A}\cdot\mathbf{V}), \mathbf{A}\cdot\mathbf{y}+\mathbf{e}) \overset{c}{\sim} (f(\mathbf{x},\mathbf{e};Z), Z, (\mathbf{A}\cdot\mathbf{V}), U_{q'})\ \ ,
\end{aligned}$$

where the first implication is trivial since Z is independent of $(\mathbf{A},\mathbf{y},\mathbf{e})$ and any $O(\log n)$ bits of leakage affects unpredictability by a fact of $\mathsf{poly}(n)$, the second step is the Goldreich-Levin theorem [25] with $\mathbf{r} \sim U_\lambda$, and the third implication

uses the sample-preserving reduction from [4] and is reproduced as Lemma 18. The conclusion follows by a triangle inequality. □

We will use Lemma 5 to estimate the noise rate of an inner product between Bernoulli-like vectors .

Lemma 5. *For any* $0 < \mu \leq 1/8$ *and* $\ell \in \mathbb{N}$*, let* $E_1, \cdots, E_\ell$ *be Boolean random variables i.i.d. to* $\mathcal{B}_\mu$*, then* $\Pr[\ \bigoplus_{i=1}^{\ell} E_i = 0\ ] > \frac{1}{2} + 2^{-(4\mu\ell+1)}$.

Proof. We complete the proof by Fact 1 and Fact 2

$$\Pr[\ \bigoplus_{i=1}^{\ell} E_i = 1\ ] = \frac{1}{2}(1-(1-2\mu)^\ell) < \frac{1}{2}(1-2^{-4\mu\ell}) \ = \ \frac{1}{2} - 2^{-(4\mu\ell+1)} \ .$$

Fact 1 (Piling-up lemma) *For* $0 < \mu < 1/2$ *and random variables* E_1*,* E_2*,* $\cdots$*,* E_ℓ *that are i.i.d. to* $\mathcal{B}_\mu$ *we have* $\bigoplus_{i=1}^{\ell} E_i \ \sim \ \mathcal{B}_\sigma$ *with* $\sigma = \frac{1}{2}(1-(1-2\mu)^\ell)$.

Fact 2 (Mean value theorem) *For any* $0 < x \leq 1/4$ *we have* $1 - x > 2^{-2x}$.

We recall the following facts about the entropy of Bernoulli-like distributions. In general, there's no closed formula for binomial coefficient, but an asymptotic estimation like Fact 3 already suffices for our purpose, where the binary entropy function can be further bounded by Fact 4 (see also Footnote 11).

Fact 3 (Asymptotics for binomial coefficients (e.g. [27], p.492)) *For any* $0 < \mu < 1/2$*, and any* $n \in \mathbb{N}$ *we have* $\binom{n}{\mu n} \ = \ 2^{n\mathbf{H}(\mu) - \frac{\log n}{2} + O(1)}$.

Fact 4 *For any* $0 < \mu < 1/2$*, we have* $\mu \log(1/\mu) < \mathbf{H}(\mu) < \mu(\log(1/\mu) + \frac{3}{2})$.

4.2 Weakly Correct 1-bit PKE from Constant-Noise LPN

As stated in Theorem 2, for any constant $0 < \mu < 1/2$, $2^{\omega(n^{\frac{1}{2}})}$-hard $\mathsf{LPN}_{\mu,n}$ implies that $(\mathbf{A}' \cdot \mathbf{x} + \mathbf{e})$ is pseudorandom conditioned on $\mathbf{A}'$ for $\mathbf{x} \sim X$ with squared-log entropy, where the leakage due to f can be omitted for now as it is only needed for CCA security. If there exists X satisfying the following three conditions at the same time then the 1-bit PKE as in Figure 1 instantiated with the square matrix $\mathbf{A}' \leftarrow \mathcal{D}_\lambda^{n \times n}$, $\mathbf{s}, \mathbf{s}_1 \leftarrow X$ and $\mathbf{e}, \mathbf{e}_1 \leftarrow \mathcal{B}_\mu^n$ will be secure and noticeably correct (since $\mathbf{s}_1^\mathsf{T}\mathbf{e}$ and $\mathbf{e}_1^\mathsf{T}\mathbf{s}$ are both $(1/2 + 1/\mathsf{poly}(n))$-biased to 0 independently).

1. **(Efficiency)** $X \in \{0,1\}^n$ can be sampled in polynomial time.
2. **(Security)** $\mathbf{H}_\infty(X) = \Omega(\log^2 n)$ as required by Theorem 2.
3. **(Correctness)** $|X| = O(\log n)$ such that $\Pr[\langle X, \mathcal{B}_\mu^n \rangle = 0] \geq 1/2 + 1/\mathsf{poly}(n)$.

Note that any distribution $X \in \{0,1\}^n$ satisfying $|X| = O(\log n)$ implies that $\mathbf{H}_\infty(X) = O(\log^2 n)$ (as the set $\{\mathbf{x} \in \{0,1\}^n : |\mathbf{x}| = O(\log n)\}$ is of size $2^{O(\log^2 n)}$), so the job is to maximize the entropy of X under constraint $|X| = O(\log n)$. The first candidate seems $X \sim \mathcal{B}_{\mu'}^n$ for $\mu' = \Theta(\frac{\log n}{n})$, but it does not

meet the security condition because the noise rate μ' is so small that a Chernoff bound only ensures (see Lemma 19) that $\mathcal{B}^n_{\mu'}$ is $(2^{-O(\mu' n)} = 1/\mathsf{poly}(n))$-close to having min-entropy $\Theta(n\mathbf{H}(\mu')) = \Theta(\log^2 n)$. In fact, we can avoid the lower-tail issue by letting $X \sim \chi^n_{\log n}$, namely, a uniform distribution of Hamming weight exact $\log n$, which is of min-entropy $\Theta(\log^2 n)$ by Fact 3. Thus, $X \sim \chi^n_{\log n}$ is a valid option to obtain a single-bit PKE with noticeable correctness.

4.3 CPA Secure PKE from Constant-Noise LPN

Unlike [20] where the extension from the weak single-bit PKE to a fully correct scheme is almost immediate (by a parallel repetition and using error correcting codes), it is not trivial to amplify the noticeable correctness of the single-bit scheme to an overwhelming probability, in particular, the scheme instantiated with distribution $X \sim \chi^n_{\log n}$ would no longer work. To see the difficulty, we define below our CPA secure scheme $\Pi_X = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ that resembles the counterpart for low-noise LPN (e.g., [20,15]), where distribution X is left undefined (apart from the entropy constraint).

Distribution X: X is a polynomial-time sampleable distribution satisfying $\mathbf{H}_\infty(X) = \Omega(\log^2 n)$ and we set $\lambda = \Theta(\log^2 n)$ such that $2\lambda \le \mathbf{H}_\infty(X)$.

$\mathsf{KeyGen}(1^n)$**:** Given a security parameter 1^n, it samples matrix $\mathbf{A} \sim \mathcal{D}^{n\times n}_\lambda$, column vectors $\mathbf{s} \sim X$, $\mathbf{e} \sim \mathcal{B}^n_\mu$, computes $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$ and sets $(pk, sk) := ((\mathbf{A}, \mathbf{b}), \mathbf{s})$.

$\mathsf{Enc}_{pk}(\mathbf{m})$**:** Given the public key $pk = (\mathbf{A}, \mathbf{b})$ and a plaintext $\mathbf{m} \in \{0,1\}^n$, Enc_{pk} chooses

$$\mathbf{S}_1 \sim (X^{(1)}, \cdots, X^{(q)}) \in \{0,1\}^{n\times q}, \mathbf{E}_1 \sim \mathcal{B}^{n\times q}_\mu$$

where $X^{(1)}, \cdots, X^{(q)}$ are i.i.d. to X. Then, it outputs $C = (\mathbf{C}_1, \mathbf{c}_2)$ as ciphertext, where

$$\begin{aligned} \mathbf{C}_1 &:= \mathbf{A}^\mathsf{T}\mathbf{S}_1 + \mathbf{E}_1 \ \in \{0,1\}^{n\times q}, \\ \mathbf{c}_2 &:= \mathbf{S}_1^\mathsf{T}\mathbf{b} + \mathbf{G}\cdot\mathbf{m} \in \{0,1\}^q, \end{aligned}$$

and $\mathbf{G} \in \{0,1\}^{q\times n}$ is a generator matrix for an efficiently decodable code (with error correction capacity to be defined and analyzed in Section 4.4).

$\mathsf{Dec}_{sk}(\mathbf{C}_1, \mathbf{c}_2)$**:** On secret key $sk = \mathbf{s}$, ciphertext $(\mathbf{C}_1, \mathbf{c}_2)$, it computes

$$\tilde{\mathbf{c}}_0 := \mathbf{c}_2 - \mathbf{C}_1^\mathsf{T}\mathbf{s} \ = \ \mathbf{G}\cdot\mathbf{m} + \mathbf{S}_1^\mathsf{T}\mathbf{e} - \mathbf{E}_1^\mathsf{T}\mathbf{s}$$

and reconstructs $\mathbf{m}$ from the error $\mathbf{S}_1^\mathsf{T}\mathbf{e} - \mathbf{E}_1^\mathsf{T}\mathbf{s}$ using the error correction property of $\mathbf{G}$.

We can see that the CPA security of Π_X, for any X with $\mathbf{H}_\infty(X) = \Omega(\log^2 n)$, follows from applying Theorem 2 twice (once for replacing the pubic key $\mathbf{b}$ with uniform randomness, and again together with the Goldreich Levin Theorem for encrypting a single bit) and a hybrid argument (to encrypt many bits).

Theorem 3 (CPA Security). *Assume that the decisional* $\mathsf{LPN}_{\mu,n}$ *problem is* $2^{\omega(n^{\frac{1}{2}})}$*-hard for any constant* $0 < \mu < 1/2$*, then* Π_X *is* IND-CPA *secure.*

4.4 Which X Makes a Correct Scheme?

$X \sim \chi^n_{\log n}$ MAY NOT WORK. To make a correct scheme, we need to upper bound $|\mathbf{S}_1^\mathsf{T}\mathbf{e} - \mathbf{E}_1^\mathsf{T}\mathbf{s}|$ by $q(1/2 - 1/\mathsf{poly}(n))$, but in fact we do not have any useful bound even for $|\mathbf{S}_1^\mathsf{T}\mathbf{e}|$. Recall that $\mathbf{S}_1^\mathsf{T}$ is now a $q\times n$ matrix and parse $\mathbf{S}_1^\mathsf{T}\mathbf{e}$ as Boolean random variables $W_1, \cdots, W_q$. First, although every W_i satisfies $\Pr[W_i = 0] \geq 1/2 + 1/\mathsf{poly}(n)$, they are not independent (correlated through $\mathbf{e}$). Second, if we fix any $|\mathbf{e}| = \Theta(n)$, all $W_1, \cdots, W_q$ are now independent conditioned on $\mathbf{e}$, but then we could no longer guarantee that $\Pr[W_i = 0|\mathbf{e}] \geq 1/2 + \mathsf{poly}(n)$ as $\mathbf{S}_1$ follows $(\chi^n_{\log n})^q$ rather than $(\mathcal{B}^n_{\log n/n})^q$. Otherwise said, condition #3 (as in Section 4.2) is not sufficient for overwhelming correctness. We introduced a tailored version of Bernoulli distribution (with upper/lower tails chopped off).

Definition 4 (Distribution $\widetilde{\mathcal{B}}^n_{\mu_1}$). *Define $\widetilde{\mathcal{B}}^n_{\mu_1}$ to be distributed to $\mathcal{B}^n_{\mu_1}$ conditioned on $(1 - \frac{\sqrt{6}}{3})\mu_1 n \leq |\mathcal{B}^n_{\mu_1}| \leq 2\mu_1 n$. Further, we define an $n\times q$ matrix distribution, denoted by $(\widetilde{\mathcal{B}}^n_{\mu_1})^q$, where every column is i.i.d. to $\widetilde{\mathcal{B}}^n_{\mu_1}$.*

$\widetilde{\mathcal{B}}^n_{\mu_1}$ IS EFFICIENTLY SAMPLEABLE. $\widetilde{\mathcal{B}}^n_{\mu_1}$ can be sampled in polynomial-time with exponentially small error, e.g., simply sample $\mathbf{e} \leftarrow \mathcal{B}^n_{\mu_1}$ and outputs $\mathbf{e}$ if $(1 - \frac{\sqrt{6}}{3})\mu_1 n \leq |\mathbf{e}| \leq 2\mu_1 n$. Otherwise, repeat the above until such $\mathbf{e}$ within the Hamming weight range is obtained or the experiment failed (then output $\perp$ in this case) for a predefined number of times (e.g., n).

$\widetilde{\mathcal{B}}^n_{\mu_1}$ IS OF MIN-ENTROPY $\Omega(\log^2 n)$. For $\mu_1 = \Omega(\log n/n)$, it is not hard to see that $\widetilde{\mathcal{B}}^n_{\mu_1}$ is a convex combination of $\chi^n_{(1-\frac{\sqrt{6}}{3})\mu_1 n}$, $\cdots$, $\chi^n_{2\mu_1 n}$, and thus of min-entropy $\Omega(\log^2 n)$ by Fact 3.

Therefore, Π_X when instantiated with $X \sim \widetilde{\mathcal{B}}^n_{\mu_1}$ is CPA secure by Theorem 4, and we proceed to the correctness of the scheme.

Lemma 6. *For constants $\alpha > 0$, $0 < \mu \leq 1/10$ and $\mu_1 = \alpha \log n/n$, let $\mathbf{S}_1 \sim (\widetilde{\mathcal{B}}^n_{\mu_1})^q$, $\mathbf{e} \sim \mathcal{B}^n_\mu$, $\mathbf{E}_1 \sim \mathcal{B}^{n\times q}_\mu$ and $\mathbf{s} \sim \widetilde{\mathcal{B}}^n_{\mu_1}$, we have*

$$\Pr\left[\ \left|\mathbf{S}_1^\mathsf{T}\mathbf{e} - \mathbf{E}_1^\mathsf{T}\mathbf{s}\right| \leq \left(\frac{1}{2} - \frac{1}{2n^{3\alpha/2}}\right)q\ \right] \ \geq\ 1 - 2^{-\Omega(n^{-3\alpha}q)}\ .$$

Proof. It is more convenient to consider $\left|\mathbf{S}_1^\mathsf{T}\mathbf{e} - \mathbf{E}_1^\mathsf{T}\mathbf{s}\right|$ conditioned on $|\mathbf{e}| \leq 1.01\mu n$ (except for a $2^{-\Omega(n)}$-fraction) and $|\mathbf{s}| \leq 2\mu n$. We have by Lemma 7 and Lemma 8 that $\mathbf{S}_1^\mathsf{T}\mathbf{e}$ and $\mathbf{E}_1^\mathsf{T}\mathbf{s}$ are identical distributed to $\mathcal{B}^q_{\delta_1}$ and $\mathcal{B}^q_{\delta_2}$ respectively, where $\delta_1 \leq 1/2 - n^{-\alpha/2}$ and $\delta_2 \leq 1/2 - n^{-\alpha}/2$. Thus, $(\mathbf{S}_1^\mathsf{T}\mathbf{e} - \mathbf{E}_1^\mathsf{T}\mathbf{s})$ follows $\mathcal{B}^q_\delta$ for $\delta \leq 1/2 - n^{-3\alpha/2}$ by the Piling-up lemma, and then we complete the proof with Lemma 2.

CONCRETE PARAMETERS. Enc_{pk} simply uses a generator matrix $\mathbf{G} : \{0,1\}^{q\times n}$ that efficiently corrects up to a $(1/2 - n^{-3\alpha/2}/2)$-fraction of bit flipping errors, which exists for $q = O(n^{3\alpha+1})$ (e.g., [22]). We can now conclude the correctness of the scheme since every encryption will be correctly decrypted with overwhelming probability and thus so is the event that polynomially many of them occur simultaneously (even when they are not independent, see Lemma 1).

Theorem 4 (Correctness). *Let $0 < \mu \leq 1/10$ and $\alpha > 0$ be any constants, let $q = \Theta(n^{3\alpha+1})$ and $\mu_1 = \alpha \log n/n$, and let $X \sim \widetilde{\mathcal{B}}^n_{\mu_1}$. Assume that the decisional $\mathsf{LPN}_{\mu,n}$ problem is $2^{\omega(n^{\frac{1}{2}})}$-hard, then Π_X is a correct scheme.*

Lemma 7. *For any $0 < \mu \leq 1/10$, $\mu_1 = O(\log n/n) \leq 1/8$ and any $\mathbf{e} \in \{0,1\}^n$ with $|\mathbf{e}| \leq 1.01\mu n$,*

$$\Pr[\langle \widetilde{\mathcal{B}}^n_{\mu_1}, \mathbf{e}\rangle = 0] \geq 1/2 + 2^{-\frac{\mu_1 n}{2}} \ .$$

Proof. Denote by $\mathcal{E}$ the event $(1 - \frac{\sqrt{6}}{3})\mu_1 n \leq |\mathcal{B}^n_{\mu_1}| \leq 2\mu_1 n$ and thus $\Pr[\mathcal{E}] \geq (1 - 2\exp^{-\mu_1 n/3})$ by the Chernoff bound. We have by Lemma 5

$$\begin{aligned}\frac{1}{2} + 2^{-(4.04\mu\mu_1 n+1)} &\leq \Pr[\langle \mathcal{B}^n_{\mu_1}, \mathbf{e}\rangle = 0] \\ &\leq \Pr[\mathcal{E}] \cdot \Pr[\langle \widetilde{\mathcal{B}}^n_{\mu_1}, \mathbf{e}\rangle = 0] \ + \ \Pr[\neg\mathcal{E}] \cdot \Pr[\langle \mathcal{B}^n_{\mu_1}, \mathbf{e}\rangle = 0 | \neg\mathcal{E}] \\ &\leq \Pr[\langle \widetilde{\mathcal{B}}^n_{\mu_1}, \mathbf{e}\rangle = 0] \ + \ \Pr[\neg\mathcal{E}] \ .\end{aligned}$$

For $0 < \mu \leq 1/10$, $\Pr[\langle \widetilde{\mathcal{B}}^n_{\mu_1}, \mathbf{e}\rangle = 0] \geq 1/2 + 2^{-(4.04\mu\mu_1 n+1)} - 2\exp^{-\mu_1 n/3} > 1/2 + 2^{-\mu_1 n/2}$.

Lemma 8. *For any $0 < \mu \leq 1/8$, $\mu_1 = O(\log n/n)$, and any $\mathbf{s} \in \{0,1\}^n$ with $|\mathbf{s}| \leq 2\mu_1 n$, we have by Lemma 5*

$$\Pr[\langle \mathcal{B}^n_{\mu}, \mathbf{s}\rangle = 0] \ \geq \ 1/2 + 2^{-(8\mu\mu_1 n+1)} \ \geq \ 1/2 + 2^{-(\mu_1 n+1)} \ .$$

5 CCA-Secure PKE from Constant-Noise LPN

In this section, we show how to construct CCA-secure PKE from constant-noise LPN. Our starting point is the construction of a tag-based PKE against selective tag and chosen ciphertext attacks from LPN, which can be transformed into a standard CCA-secure PKE by using known techniques [11,35]. We begin by first recalling the definitions of tag-based PKE.

5.1 Tag-Based Encryption

A tag-based encryption (TBE) scheme with tag-space $\mathcal{T}$ and message-space $\mathcal{M}$ consists of three PPT algorithms $\mathcal{TBE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$. The randomized key generation algorithm KeyGen takes the security parameter n as input, outputs a public key pk and a secret key sk, denoted as $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$. The randomized encryption algorithm Enc takes pk, a tag $\mathbf{t} \in \mathcal{T}$, and a plaintext $\mathbf{m} \in \mathcal{M}$ as inputs, outputs a ciphertext C, denoted as $C \leftarrow \mathsf{Enc}(pk, \mathbf{t}, \mathbf{m})$. The deterministic algorithm Dec takes sk and C as inputs, outputs a plaintext $\mathbf{m}$, or a special symbol $\perp$, which is denoted as $\mathbf{m} \leftarrow \mathsf{Dec}(sk, \mathbf{t}, C)$. For correctness, we require that for all $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$, any tag $\mathbf{t}$, any plaintext $\mathbf{m}$ and any $C \leftarrow \mathsf{Enc}(pk, \mathbf{t}, \mathbf{m})$, the equation $\mathsf{Dec}(sk, \mathbf{t}, C) = \mathbf{m}$ holds with overwhelming probability.

We consider the following game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ given in [35].

Init. The adversary $\mathcal{A}$ takes the security parameter n as inputs, and outputs a target tag $\mathbf{t}^*$ to the challenger $\mathcal{C}$.

KeyGen. The challenger $\mathcal{C}$ computes $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$, gives the public key pk to the adversary $\mathcal{A}$, and keeps the secret key sk to itself.

Phase 1. The adversary $\mathcal{A}$ can make decryption queries for any pair $(\mathbf{t}, C)$ for any polynomial time, with a restriction that $\mathbf{t} \neq \mathbf{t}^*$, and the challenger $\mathcal{C}$ returns $\mathbf{m} \leftarrow \mathsf{Dec}(sk, \mathbf{t}, C)$ to $\mathcal{A}$ accordingly.

Challenge. The adversary $\mathcal{A}$ outputs two equal length plaintexts $\mathbf{m}_0, \mathbf{m}_1 \in \mathcal{M}$. The challenger $\mathcal{C}$ randomly chooses a bit $b^* \xleftarrow{\$} \{0,1\}$, and returns the challenge ciphertext $C^* \leftarrow \mathsf{Enc}(pk, \mathbf{t}^*, \mathbf{m}_{b^*})$ to the adversary $\mathcal{A}$.

Phase 2. The adversary can make more decryption queries as in Phase 1.

Guess. Finally, $\mathcal{A}$ outputs a guess $b \in \{0,1\}$. If $b = b^*$, the challenger $\mathcal{C}$ outputs 1, else outputs 0.

Advantage. $\mathcal{A}$'s advantage is defined as $\mathrm{Adv}^{\text{ind-stag-cca}}_{\mathcal{TBE},\mathcal{A}}(1^n) \stackrel{\text{def}}{=} |\Pr[b = b^*] - \frac{1}{2}|$.

Definition 5 (IND-sTag-CCA). *We say that a TBE scheme $\mathcal{TBE}$ is* IND-sTag-CCA *secure if for any PPT adversary $\mathcal{A}$, its advantage* $\mathrm{Adv}^{\text{ind-stag-cca}}_{\mathcal{TBE},\mathcal{A}}(1^n)$ *is negligible in n.*

For our convenience, we will use the following corollary, which is essentially a q-fold[12] (transposed) version of Theorem 2 with $q' = n$ and 2 bits of linear leakage (rather than $O(\log n)$ bits of arbitrary leakage) per copy. Following [36], the leakage is crucial for the CCA security proof.

Corollary 1. *Let n be a security parameter and let $0 < \mu < 1/2$ be any constant. Assume that the computational $\mathsf{LPN}_{\mu,n}$ problem is $2^{\omega(n^{\frac{1}{2}})}$-hard (for any super-constant hidden by $\omega(\cdot)$). Then, for every $\mu_1 = \Omega(\log n/n)$ and $\lambda = \Theta(\log^2 n)$ such that $2\lambda \leq \mathbf{H}_\infty(\widetilde{\mathcal{B}}^n_{\mu_1})$, and every $q = \mathsf{poly}(n)$, we have*

$$\left((\mathbf{S}_0^\mathsf{T}\mathbf{e}, \mathbf{E}_0^\mathsf{T}\mathbf{s}), \mathbf{e}, \mathbf{s}, \mathbf{A}, \mathbf{S}_0^\mathsf{T}\mathbf{A} + \mathbf{E}_0^\mathsf{T} \right) \stackrel{c}{\sim} \left((\mathbf{S}_0^\mathsf{T}\mathbf{e}, \mathbf{E}_0^\mathsf{T}\mathbf{s}), \mathbf{e}, \mathbf{s}, \mathbf{A}, U_{q\times n} \right),$$

where the probability is taken over $\mathbf{S}_0 \sim (\widetilde{\mathcal{B}}^n_{\mu_1})^q$, $\mathbf{E}_0 \sim \mathcal{B}^{n\times q}_\mu$, $\mathbf{A} \sim \mathcal{D}^{n\times n}_\lambda$, $U_{q\times n}$, $\mathbf{s} \leftarrow \widetilde{\mathcal{B}}^n_{\mu_1}$, $\mathbf{e} \leftarrow \mathcal{B}^n_\mu$ and internal random coins of the distinguisher.

5.2 Our Construction

Our construction is built upon previous works in [44,36]. A couple of modifications are made to adapt the ideas of [44,36], which seems necessary due to the absence of a meaningful knapsack version for our LPN (with poly-log entropy and non-uniform matrix). Let n be the security parameter, let $\alpha > 0$, $0 < \mu \leq 1/10$ be any constants, let $\mu_1 = \alpha \log n/n$, $\beta = (\frac{1}{2} - \frac{1}{n^{3\alpha}})$, $\gamma = (\frac{1}{2} - \frac{1}{2n^{3\alpha/2}})$ and choose

[12] Please do not confuse q' with q, where q' is the number of samples in LPN (see Theorem 2) and is set to n (for a square matrix), and q is the number of parallel repetitions of LPN on independent secrets and noise vectors.

$\lambda = \Theta(\log^2 n)$ such that $2\lambda \leq \mathbf{H}_\infty(\widetilde{\mathcal{B}}^n_{\mu_1})$. Let the plaintext-space $\mathcal{M} = \{0,1\}^n$, and let $\mathbf{G} \in \{0,1\}^{q\times n}$ and $\mathbf{G}_2 \in \{0,1\}^{\ell\times n}$ be the generator matrices that can correct at least βq and $2\mu\ell$ bit flipping errors in the codeword respectively, where $q = O(n^{6\alpha+1})$, $\ell = O(n)$ and we refer to [22] and [33] for explicit constructions of the two codes respectively. Let the tag-space $\mathcal{T} = \mathbb{F}_{2^n}$. We use a matrix representation $\mathbf{H_t} \in \{0,1\}^{n\times n}$ for finite field elements $\mathbf{t} \in \mathbb{F}_{2^n}$ [14,10,36] such that $\mathbf{H_0} = \mathbf{0}$, $\mathbf{H_t}$ is invertible for any $\mathbf{t} \neq \mathbf{0}$, and $\mathbf{H_{t_1}} + \mathbf{H_{t_2}} = \mathbf{H_{t_1+t_2}}$. Our TBE scheme $\mathcal{TBE}$ is defined as follows:

$\mathsf{KeyGen}(1^n)$**:** Given a security parameter n, first uniformly choose matrices $\mathbf{A} \xleftarrow{\$} \mathcal{D}^{n\times n}_\lambda, \mathbf{C} \xleftarrow{\$} \mathcal{D}^{\ell\times n}_\lambda$, $\mathbf{S}_0, \mathbf{S}_1 \xleftarrow{\$} (\widetilde{\mathcal{B}}^n_{\mu_1})^q$ and $\mathbf{E}_0, \mathbf{E}_1 \xleftarrow{\$} \mathcal{B}^{n\times q}_\mu$. Then, compute $\mathbf{B}_0 = \mathbf{S}_0^\mathsf{T}\mathbf{A} + \mathbf{E}_0^\mathsf{T}, \mathbf{B}_1 = \mathbf{S}_1^\mathsf{T}\mathbf{A} + \mathbf{E}_1^\mathsf{T} \in \{0,1\}^{q\times n}$, and set $(pk, sk) = (\ (\mathbf{A}, \mathbf{B}_0, \mathbf{B}_1, \mathbf{C}), (\mathbf{S}_0, \mathbf{S}_1))$.

$\mathsf{Enc}(pk, \mathbf{t}, \mathbf{m})$**:** Given the public key $pk = (\mathbf{A}, \mathbf{B}_0, \mathbf{B}_1, \mathbf{C})$, a tag $\mathbf{t} \in \mathbb{F}_{2^n}$, and a plaintext $\mathbf{m} \in \{0,1\}^n$, randomly choose

$$\mathbf{s} \xleftarrow{\$} \widetilde{\mathcal{B}}^n_{\mu_1}, \mathbf{e}_1 \xleftarrow{\$} \mathcal{B}^n_\mu, \mathbf{e}_2 \xleftarrow{\$} \mathcal{B}^\ell_\mu, \mathbf{S}'_0, \mathbf{S}'_1 \xleftarrow{\$} (\widetilde{\mathcal{B}}^n_{\mu_1})^q, \mathbf{E}'_0, \mathbf{E}'_1 \xleftarrow{\$} \mathcal{B}^{n\times q}_\mu$$

and define

$$\begin{aligned}
\mathbf{c} &:= \mathbf{A}\mathbf{s} + \mathbf{e}_1 && \in \{0,1\}^n\\
\mathbf{c}_0 &:= (\mathbf{G}\mathbf{H_t} + \mathbf{B}_0)\mathbf{s} + (\mathbf{S}'_0)^\mathsf{T}\mathbf{e}_1 - (\mathbf{E}'_0)^\mathsf{T}\mathbf{s} && \in \{0,1\}^q\\
\mathbf{c}_1 &:= (\mathbf{G}\mathbf{H_t} + \mathbf{B}_1)\mathbf{s} + (\mathbf{S}'_1)^\mathsf{T}\mathbf{e}_1 - (\mathbf{E}'_1)^\mathsf{T}\mathbf{s} && \in \{0,1\}^q\\
\mathbf{c}_2 &:= \mathbf{C}\mathbf{s} + \mathbf{e}_2 + \mathbf{G}_2\mathbf{m} && \in \{0,1\}^\ell.
\end{aligned}$$

Finally, return the ciphertext $C = (\mathbf{c}, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2)$.

$\mathsf{Dec}(sk, \mathbf{t}, C)$**:** Given the secret key $sk = (\mathbf{S}_0, \mathbf{S}_1)$, tag $\mathbf{t} \in \mathbb{F}_{2^n}$ and ciphertext $C = (\mathbf{c}, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2)$, first compute

$$\tilde{\mathbf{c}}_0 := \mathbf{c}_0 - \mathbf{S}_0^\mathsf{T}\mathbf{c} = \mathbf{G}\mathbf{H_t}\mathbf{s} + (\mathbf{S}'_0 - \mathbf{S}_0)^\mathsf{T}\mathbf{e}_1 + (\mathbf{E}_0 - \mathbf{E}'_0)^\mathsf{T}\mathbf{s}.$$

Then, reconstruct $\mathbf{b} = \mathbf{H_t}\mathbf{s}$ from the error $(\mathbf{S}'_0 - \mathbf{S}_0)^\mathsf{T}\mathbf{e}_1 + (\mathbf{E}_0 - \mathbf{E}'_0)^\mathsf{T}\mathbf{s}$ by using the error correction property of $\mathbf{G}$, and compute $\mathbf{s} = \mathbf{H_t}^{-1}\mathbf{b}$. If it holds that

$$|\underbrace{\mathbf{c} - \mathbf{A}\mathbf{s}}_{=\mathbf{e}_1}| \leq 2\mu n \wedge |\underbrace{\mathbf{c}_0 - (\mathbf{G}\mathbf{H_t} + \mathbf{B}_0)\mathbf{s}}_{=(\mathbf{S}'_0)^\mathsf{T}\mathbf{e}_1 - (\mathbf{E}'_0)^\mathsf{T}\mathbf{s}}| \leq \gamma q \wedge |\underbrace{\mathbf{c}_1 - (\mathbf{G}\mathbf{H}_t + \mathbf{B}_1)\mathbf{s}}_{=(\mathbf{S}'_1)^\mathsf{T}\mathbf{e}_1 - (\mathbf{E}'_1)^\mathsf{T}\mathbf{s}}| \leq \gamma q$$

then reconstruct $\mathbf{m}$ from $\mathbf{c}_2 - \mathbf{C}\mathbf{s} = \mathbf{G}_2\mathbf{m} + \mathbf{e}_2$ by using the error correction property of $\mathbf{G}_2$, else let $\mathbf{m} = \perp$. Finally, return the decrypted result $\mathbf{m}$.

Remark 2. As one can see, the matrix $\mathbf{S}_1$ in the secret key $sk = (\mathbf{S}_0, \mathbf{S}_1)$ can also be used to decrypt the ciphertext, i.e., compute $\tilde{\mathbf{c}}_1 := \mathbf{c}_1 - \mathbf{S}_1^\mathsf{T}\mathbf{c} = \mathbf{G}\mathbf{H_t}\mathbf{s} + (\mathbf{S}'_1 - \mathbf{S}_1)^\mathsf{T}\mathbf{e}_1 + (\mathbf{E}_1 - \mathbf{E}'_1)^\mathsf{T}\mathbf{s}$ and recover $\mathbf{s}$ from $\tilde{\mathbf{c}}_1$ by using the error correction property of $\mathbf{G}$. Moreover, the check condition

$$|\mathbf{c} - \mathbf{A}\mathbf{s}| \leq 2\mu n \wedge |\mathbf{c}_0 - (\mathbf{G}\mathbf{H_t} + \mathbf{B}_0)\mathbf{s}| \leq \gamma q \wedge |\mathbf{c}_1 - (\mathbf{G}\mathbf{H}_t + \mathbf{B}_1)\mathbf{s}| \leq \gamma q$$

guarantees that the decryption results are the same when we use either $\mathbf{S}_0$ or $\mathbf{S}_1$ in the decryption. This fact seems not necessary for the correctness, but it is very important for the security proof. Looking ahead, it allows us to switch the "exact decryption key" between $\mathbf{S}_0$ and $\mathbf{S}_1$.

Correctness and Equivalence of the Secret Keys $\mathbf{S_0}, \mathbf{S_1}$. In the following, we show that for appropriate choice of parameters, the above scheme $\mathcal{TBE}$ is correct, and has the property that both $\mathbf{S}_0$ and $\mathbf{S}_1$ are equivalent in terms of decryption.

- The correctness of the scheme requires the following:
  1. $|(\mathbf{S}'_0 - \mathbf{S}_0)^\mathsf{T}\mathbf{e}_1 + (\mathbf{E}_0 - \mathbf{E}'_0)^\mathsf{T}\mathbf{s}| \leq \beta q$ (to let $\mathbf{G}$ reconstruct $\mathbf{s}$ from $\tilde{\mathbf{c}}_0$).
  2. $|\mathbf{c} - \mathbf{A}\mathbf{s}| \leq 2\mu n \wedge |\mathbf{c}_0 - (\mathbf{G}\mathbf{H_t} + \mathbf{B}_0)\mathbf{s}| \leq \gamma q \wedge |\mathbf{c}_1 - (\mathbf{G}\mathbf{H_t} + \mathbf{B}_1)\mathbf{s}| \leq \gamma q$.
  3. $|\mathbf{e}_2| \leq 2\mu\ell$ (such that $\mathbf{G}_2$ can reconstruct $\mathbf{m}$ from $\mathbf{c}_2 - \mathbf{C}\mathbf{s} = \mathbf{G}_2\mathbf{m} + \mathbf{e}_2$).
- For obtaining CCA security, we also need to show that $\mathbf{S}_0$ and $\mathbf{S}_1$ have the same decryption ability except with negligible probability, namely,
  1. If $|\mathbf{c} - \mathbf{A}\mathbf{s}| \leq 2\mu n \wedge |\mathbf{c}_0 - (\mathbf{G}\mathbf{H_t} + \mathbf{B}_0)\mathbf{s}| \leq \gamma q$, then $\mathbf{G}$ can reconstruct $\mathbf{s}$ from a code within bounded error $|(\mathbf{S}'_0 - \mathbf{S}_0)\mathbf{e}_1 + (\mathbf{E}_0 - \mathbf{E}'_0)\mathbf{s}| \leq \beta q$.
  2. If $|\mathbf{c} - \mathbf{A}\mathbf{s}| \leq 2\mu n \wedge |\mathbf{c}_1 - (\mathbf{G}\mathbf{H_t} + \mathbf{B}_1)\mathbf{s}| \leq \gamma q$, then $\mathbf{G}$ can reconstruct $\mathbf{s}$ from a code within bounded error $|(\mathbf{S}'_1 - \mathbf{S}_1)\mathbf{e}_1 + (\mathbf{E}_1 - \mathbf{E}'_1)\mathbf{s}| \leq \beta q$.

It suffices to show that each Hamming weight constraint above holds (with overwhelming probability) individually and thus polynomially many of them hold simultaneously (with overwhelming probability as well) by Lemma 1. First, Chernoff bound guarantees that $\Pr[|\mathbf{e}_1| \leq 2\mu n] = 1 - 2^{-\Omega(n)}$ and $\Pr[|\mathbf{e}_2| \leq 2\mu\ell] = 1 - 2^{-\Omega(\ell)}$. Second, for $i \in \{0, 1\}$ the bound $|(\mathbf{S}'_i)^\mathsf{T}\mathbf{e}_1 - (\mathbf{E}'_i)^\mathsf{T}\mathbf{s}| \leq \gamma q$ is ensured by Lemma 6 and we further bound $|(\mathbf{S}'_i - \mathbf{S}_i)\mathbf{e}_1 + (\mathbf{E}_i - \mathbf{E}'_i)\mathbf{s}| \leq \beta q$ with Lemma 9 below (proof similar to Lemma 6 and thus deferred to Appendix B).

Lemma 9. *For constants $\alpha > 0$, $0 < \mu \leq 1/10$ and $\mu_1 = \alpha \log n/n$, let $\mathbf{S}$ and $\mathbf{S}'$ be i.i.d. to $(\widetilde{\mathcal{B}}^n_{\mu_1})^q$, $\mathbf{E}$ and $\mathbf{E}'$ be i.i.d. to $\mathcal{B}^{n\times q}_\mu$, $\mathbf{s} \sim \widetilde{\mathcal{B}}^n_{\mu_1}$ and $\mathbf{e} \sim \mathcal{B}^n_\mu$. Then,*

$$\Pr\left[\ \left|(\mathbf{S}' - \mathbf{S})^\mathsf{T}\mathbf{e} + (\mathbf{E} - \mathbf{E}')^\mathsf{T}\mathbf{s}\right| \leq (\frac{1}{2} - \frac{1}{n^{3\alpha}})q\ \right] \ \geq\ 1 - 2^{-\Omega(n^{-6\alpha}q)}\ .$$

Security of the TBE Scheme. We now show that under the LPN assumption, the above scheme $\mathcal{TBE}$ is IND-sTag-CCA secure in the standard model.

Theorem 5. *Assume that the decisional $\mathsf{LPN}_{\mu,n}$ problem is $2^{\omega(n^{\frac{1}{2}})}$-hard for any constant $0 < \mu \leq 1/10$, then our TBE scheme $\mathcal{TBE}$ is* IND-sTag-CCA *secure.*

Proof. Let $\mathcal{A}$ be any PPT adversary that can attack our TBE scheme $\mathcal{TBE}$ with advantage ϵ. We show that ϵ must be negligible in n. We continue the proof by using a sequence of games, where the first game is the real IND-sTag-CCA security game, while the last is a random game in which the challenge ciphertext is independent from the choices of the challenge plaintexts. Since any PPT adversary $\mathcal{A}$'s advantage in a random game is exactly 0, the security of $\mathcal{TBE}$ can be established by showing that $\mathcal{A}$'s advantage in any two consecutive games are negligibly close.

Game 0. The challenger $\mathcal{C}$ honestly runs the adversary $\mathcal{A}$ with the security parameter n, and obtains a target tag $\mathbf{t}^*$ from $\mathcal{A}$. Then, it simulates the IND-sTag-CCA security game for $\mathcal{A}$ as follows:

KeyGen. First uniformly choose matrices $\mathbf{A} \xleftarrow{\$} \mathcal{D}_\lambda^{n\times n}, \mathbf{C} \xleftarrow{\$} \mathcal{D}_\lambda^{\ell\times n}$, $\mathbf{S}_0, \mathbf{S}_1 \xleftarrow{\$} (\widetilde{\mathcal{B}}_{\mu_1}^n)^q$ and $\mathbf{E}_0, \mathbf{E}_1 \xleftarrow{\$} \mathcal{B}_\mu^{n\times q}$. Then, compute $\mathbf{B}_0 = \mathbf{S}_0^\mathsf{T}\mathbf{A} + \mathbf{E}_0^\mathsf{T}, \mathbf{B}_1 = \mathbf{S}_1^\mathsf{T}\mathbf{A} + \mathbf{E}_1^\mathsf{T} \in \{0,1\}^{q\times n}$. Finally, $\mathcal{C}$ sends $pk = (\mathbf{A}, \mathbf{B}_0, \mathbf{B}_1, \mathbf{C})$ to the adversary $\mathcal{A}$, and keeps $sk = (\mathbf{S}_0, \mathbf{S}_1)$ to itself.

Phase 1. After receiving a decryption query $(\mathbf{t}, (\mathbf{c}, \mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2))$ from the adversary $\mathcal{A}$, the challenger $\mathcal{C}$ directly returns $\perp$ to $\mathcal{A}$ if $\mathbf{t} = \mathbf{t}^*$. Otherwise, it first computes

$$\tilde{\mathbf{c}}_0 := \mathbf{c}_0 - \mathbf{S}_0^\mathsf{T}\mathbf{c} = \mathbf{G}\mathbf{H}_\mathbf{t}\mathbf{s} + (\mathbf{S}_0' - \mathbf{S}_0)^\mathsf{T}\mathbf{e}_1 + (\mathbf{E}_0 - \mathbf{E}_0')^\mathsf{T}\mathbf{s}.$$

Then, it reconstruct $\mathbf{b} = \mathbf{H}_\mathbf{t}\mathbf{s}$ from the error $(\mathbf{S}_0' - \mathbf{S}_0)^\mathsf{T}\mathbf{e}_1 + (\mathbf{E}_0 - \mathbf{E}_0')^\mathsf{T}\mathbf{s}$ by using the error correction property of $\mathbf{G}$, and compute $\mathbf{s} = \mathbf{H}_\mathbf{t}^{-1}\mathbf{b}$. If

$$|\mathbf{c} - \mathbf{A}\mathbf{s}| \le 2\mu n \wedge |\mathbf{c}_0 - (\mathbf{G}\mathbf{H}_\mathbf{t} + \mathbf{B}_0)\mathbf{s}| \le \gamma q \wedge |\mathbf{c}_1 - (\mathbf{G}\mathbf{H}_\mathbf{t} + \mathbf{B}_1)\mathbf{s}| \le \gamma q$$

is true, reconstruct M from $\mathbf{c}_2 - \mathbf{C}\mathbf{s} = \mathbf{G}_2\mathbf{m} + \mathbf{e}_2$ by using the error correction property of $\mathbf{G}_2$, else let $\mathbf{m} = \perp$. Finally, return the decrypted result $\mathbf{m}$ to the adversary $\mathcal{A}$.

Challenge. After receiving two equal length plaintexts $\mathbf{m}_0, \mathbf{m}_1 \in \mathcal{M}$ from the adversary $\mathcal{A}$, the challenger $\mathcal{C}$ first randomly chooses a bit $b^* \xleftarrow{\$} \{0,1\}$, and

$$\mathbf{s} \xleftarrow{\$} \widetilde{\mathcal{B}}_{\mu_1}^n, \mathbf{e}_1 \xleftarrow{\$} \mathcal{B}_\mu^n, \mathbf{e}_2 \xleftarrow{\$} \mathcal{B}_\mu^\ell, \mathbf{S}_0', \mathbf{S}_1' \xleftarrow{\$} (\widetilde{\mathcal{B}}_{\mu_1}^n)^q, \mathbf{E}_0', \mathbf{E}_1' \xleftarrow{\$} \mathcal{B}_\mu^{n\times q}$$

Then, it defines

$$\begin{aligned}
\mathbf{c}^* &:= \mathbf{A}\mathbf{s} + \mathbf{e}_1 && \in \{0,1\}^n \\
\mathbf{c}_0^* &:= (\mathbf{G}\mathbf{H}_{\mathbf{t}^*} + \mathbf{B}_0)\mathbf{s} + (\mathbf{S}_0')^\mathsf{T}\mathbf{e}_1 - (\mathbf{E}_0')^\mathsf{T}\mathbf{s} && \in \{0,1\}^q \\
\mathbf{c}_1^* &:= (\mathbf{G}\mathbf{H}_{\mathbf{t}^*} + \mathbf{B}_1)\mathbf{s} + (\mathbf{S}_1')^\mathsf{T}\mathbf{e}_1 - (\mathbf{E}_1')^\mathsf{T}\mathbf{s} && \in \{0,1\}^q \\
\mathbf{c}_2^* &:= \mathbf{C}\mathbf{s} + \mathbf{e}_2 + \mathbf{G}_2\mathbf{m}_{b^*} && \in \{0,1\}^\ell,
\end{aligned}$$

and returns the challenge ciphertext $(\mathbf{c}^*, \mathbf{c}_0^*, \mathbf{c}_1^*, \mathbf{c}_2^*)$ to the adversary $\mathcal{A}$.

Phase 2. The adversary can adaptively make more decryption queries, and the challenger $\mathcal{C}$ responds as in Phase 1.

Guess. Finally, $\mathcal{A}$ outputs a guess $b \in \{0,1\}$. If $b = b^*$, the challenger $\mathcal{C}$ outputs 1, else outputs 0.

EVENT. Let F_i be the event that $\mathcal{C}$ outputs 1 in Game i for $i \in \{0, 1, \ldots, 6\}$.

Lemma 10. $|\Pr[F_0] - \frac{1}{2}| = \epsilon$.

Proof. This lemma immediately follows the fact that $\mathcal{C}$ honestly simulates the attack environment for $\mathcal{A}$, and only outputs 1 if and only if $b = b^*$.

Game 1. This game is identical to Game 0 except that the challenger $\mathcal{C}$ changes the key generation phase as follows:

KeyGen. First uniformly choose matrices $\mathbf{A} \xleftarrow{\$} \mathcal{D}_\lambda^{n\times n}, \mathbf{C} \xleftarrow{\$} \mathcal{D}_\lambda^{\ell\times n}$, $\mathbf{S}_0, \mathbf{S}_1 \xleftarrow{\$} (\widetilde{\mathcal{B}}_{\mu_1}^n)^q$, $\mathbf{E}_0, \mathbf{E}_1 \xleftarrow{\$} \mathcal{B}_\mu^{n\times q}$, and $\mathbf{B}'_1 \xleftarrow{\$} \{0,1\}^{q\times n}$. Then, compute $\mathbf{B}_0 = \mathbf{S}_0^\mathsf{T}\mathbf{A} + \mathbf{E}_0^\mathsf{T}, \mathbf{B}_1 = \mathbf{S}_1^\mathsf{T}\mathbf{A} + \mathbf{E}_1^\mathsf{T} \in \{0,1\}^{q\times n}$. Finally, $\mathcal{C}$ sends $pk = (\mathbf{A}, \mathbf{B}_0, \mathbf{B}'_1, \mathbf{C})$ to the adversary $\mathcal{A}$, and keeps $sk = (\mathbf{S}_0, \mathbf{S}_1)$ to itself.

Lemma 11. *If the decisional* $\mathsf{LPN}_{\mu,n}$ *problem is* $2^{\omega(n^{\frac{1}{2}})}$*-hard, then we have* $|\Pr[F_1] - \Pr[F_0]| \leq \mathsf{negl}(n)$.

Proof. Since the only difference between Game 0 and Game 1 is that $\mathcal{C}$ replaces $\mathbf{B}_1 = \mathbf{S}_1^\mathsf{T}\mathbf{A} + \mathbf{E}_1^\mathsf{T} \in \{0,1\}^{q\times n}$ in Game 0 with a randomly chosen $\mathbf{B}'_1 \xleftarrow{\$} \{0,1\}^{q\times n}$ in Game 1. we have that Game 0 and Game 1 are computationally indistinguishable for any PPT adversary $\mathcal{A}$ by our assumption and Corollary 1. This means that $|\Pr[F_1] - \Pr[F_0]| \leq \mathsf{negl}(n)$ holds.

Game 2. This game is identical to Game 1 except that the challenger $\mathcal{C}$ changes the key generation phase as follows:

KeyGen. First uniformly choose matrices $\mathbf{A} \xleftarrow{\$} \mathcal{D}_\lambda^{n\times n}, \mathbf{C} \xleftarrow{\$} \mathcal{D}_\lambda^{\ell\times n}$, $\mathbf{S}_0, \mathbf{S}_1 \xleftarrow{\$} (\widetilde{\mathcal{B}}_{\mu_1}^n)^q$, $\mathbf{E}_0, \mathbf{E}_1 \xleftarrow{\$} \mathcal{B}_\mu^{n\times q}$, and $\mathbf{B}''_1 \xleftarrow{\$} \{0,1\}^{q\times n}$. Then, compute $\mathbf{B}_0 = \mathbf{S}_0^\mathsf{T}\mathbf{A} + \mathbf{E}_0^\mathsf{T}, \mathbf{B}_1 = \mathbf{S}_1^\mathsf{T}\mathbf{A} + \mathbf{E}_1^\mathsf{T} \in \{0,1\}^{q\times n}$ and $\mathbf{B}'_1 = \mathbf{B}''_1 - \mathbf{G}\mathbf{H}_{\mathbf{t}^*}$. Finally, $\mathcal{C}$ sends $pk = (\mathbf{A}, \mathbf{B}_0, \mathbf{B}'_1, \mathbf{C})$ to the adversary $\mathcal{A}$, and keeps $sk = (\mathbf{S}_0, \mathbf{S}_1)$ to itself.

Challenge. After receiving two equal length plaintexts $\mathbf{m}_0, \mathbf{m}_1 \in \mathcal{M}$ from the adversary $\mathcal{A}$, the challenger $\mathcal{C}$ first randomly chooses a bit $b^* \xleftarrow{\$} \{0,1\}$, and

$$\mathbf{s} \xleftarrow{\$} \widetilde{\mathcal{B}}_{\mu_1}^n, \mathbf{e}_1 \xleftarrow{\$} \mathcal{B}_\mu^n, \mathbf{e}_2 \xleftarrow{\$} \mathcal{B}_\mu^\ell, \mathbf{S}'_0, \mathbf{S}'_1 \xleftarrow{\$} (\widetilde{\mathcal{B}}_{\mu_1}^n)^q, \mathbf{E}'_0, \mathbf{E}'_1 \xleftarrow{\$} \mathcal{B}_\mu^{n\times q}$$

Then, it defines

$$\begin{aligned}
\mathbf{c}^* &:= \mathbf{A}\mathbf{s} + \mathbf{e}_1 && \in \{0,1\}^n \\
\mathbf{c}_0^* &:= (\mathbf{G}\mathbf{H}_{\mathbf{t}^*} + \mathbf{B}_0)\mathbf{s} + (\mathbf{S}'_0)^\mathsf{T}\mathbf{e}_1 - (\mathbf{E}'_0)^\mathsf{T}\mathbf{s} && \in \{0,1\}^q \\
\mathbf{c}_1^* &:= (\mathbf{G}\mathbf{H}_{\mathbf{t}^*} + \mathbf{B}_1)\mathbf{s} + (\mathbf{S}_1)^\mathsf{T}\mathbf{e}_1 - (\mathbf{E}_1)^\mathsf{T}\mathbf{s} && \in \{0,1\}^q \\
\mathbf{c}_2^* &:= \mathbf{C}\mathbf{s} + \mathbf{e}_2 + \mathbf{G}_2\mathbf{m}_{b^*} && \in \{0,1\}^\ell,
\end{aligned}$$

and returns the challenge ciphertext $(\mathbf{c}^*, \mathbf{c}_0^*, \mathbf{c}_1^*, \mathbf{c}_2^*)$ to the adversary $\mathcal{A}$.

Lemma 12. $\Pr[F_2] = \Pr[F_1]$.

Proof. Because of $\mathbf{B}''_1 \xleftarrow{\$} \{0,1\}^{q\times n}$, we have that $\mathbf{B}'_1 = \mathbf{B}''_1 - \mathbf{G}\mathbf{H}_{\mathbf{t}^*}$ is also uniformly distributed over $\{0,1\}^{q\times n}$. This means that the public key in Game 2 has the same distribution as that in Game 1. In addition, since $\mathbf{S}_1 \xleftarrow{\$} (\widetilde{\mathcal{B}}_{\mu_1}^n)^q$ and $\mathbf{E}_1 \xleftarrow{\$} \mathcal{B}_\mu^{n\times q}$ are chosen from the same distribution as $\mathbf{S}'_1$ and $\mathbf{E}'_1$ respectively. By the fact that $\mathbf{B}_1 = \mathbf{S}_1^\mathsf{T}\mathbf{A} + \mathbf{E}_1^\mathsf{T} \in \{0,1\}^{q\times n}$ is not included in the public key $pk = (\mathbf{A}, \mathbf{B}_0, \mathbf{B}'_1, \mathbf{C})$ (and thus $\mathcal{A}$ has no information about $\mathbf{S}_1$ and $\mathbf{E}_1$ before the challenge phase), we have that the challenge ciphertext in Game 2 also has the same distribution as that in Game 1. In all, Game 2 is identical to Game 1 in the adversary's view. Thus, we have $\Pr[F_2] = \Pr[F_1]$.

Game 3. This game is identical to Game 2 except that the challenger $\mathcal{C}$ changes the key generation phase as follows:

KeyGen. First uniformly choose matrices $\mathbf{A} \xleftarrow{\$} \mathcal{D}_\lambda^{n\times n}, \mathbf{C} \xleftarrow{\$} \mathcal{D}_\lambda^{\ell\times n}$, $\mathbf{S}_0, \mathbf{S}_1 \xleftarrow{\$} (\widetilde{\mathcal{B}}_{\mu_1}^n)^q$, and $\mathbf{E}_0, \mathbf{E}_1 \xleftarrow{\$} \mathcal{B}_\mu^{n\times q}$. Then, compute $\mathbf{B}_0 = \mathbf{S}_0^\intercal \mathbf{A} + \mathbf{E}_0^\intercal, \mathbf{B}_1 = \mathbf{S}_1^\intercal \mathbf{A} + \mathbf{E}_1^\intercal \in \{0,1\}^{q\times n}$ and $\mathbf{B}'_1 = \mathbf{B}_1 - \mathbf{G}\mathbf{H}_{\mathbf{t}^*}$. Finally, $\mathcal{C}$ sends $pk = (\mathbf{A}, \mathbf{B}_0, \mathbf{B}'_1, \mathbf{C})$ to the adversary $\mathcal{A}$, and keeps $sk = (\mathbf{S}_0, \mathbf{S}_1)$ to itself.

Lemma 13. *If the decisional* $\mathsf{LPN}_{\mu,n}$ *problem is* $2^{\omega(n^{\frac{1}{2}})}$*-hard, then* $|\Pr[F_3] - \Pr[F_2]| \leq \mathsf{negl}(n)$.

Proof. Since the only difference between Game 2 and Game 3 is that $\mathcal{C}$ replaces the randomly chosen $\mathbf{B}''_1 \xleftarrow{\$} \{0,1\}^{q\times n}$ in Game 2 with $\mathbf{B}_1 = \mathbf{S}_1^\intercal \mathbf{A} + \mathbf{E}_1^\intercal \in \{0,1\}^{q\times n}$ in Game 3, by our assumption and Corollary 1 we have that Game 2 and Game 3 are computationally indistinguishable for any PPT adversary $\mathcal{A}$ seeing $(\mathbf{S}_1^\intercal \mathbf{e}_1, \mathbf{E}_1^\intercal \mathbf{s})$ in the challenge ciphertext. This means that $|\Pr[F_3] - \Pr[F_2]| \leq \mathsf{negl}(n)$ holds.

Remark 3. Note that for the challenge ciphertext $(\mathbf{c}, \mathbf{c}_0^*, \mathbf{c}_1^*, \mathbf{c}_2^*)$ in Game 3, we have that $\mathbf{c}_1^* := (\mathbf{G}\mathbf{H}_{\mathbf{t}_1^*} + \mathbf{B}'_1)\mathbf{s} + \mathbf{S}_1^\intercal \mathbf{e}_1 - \mathbf{E}_1^\intercal \mathbf{s} = \mathbf{S}_1^\intercal \mathbf{c}$.

Game 4. This game is identical to Game 3 except that the challenger $\mathcal{C}$ answers the decryption queries by using $\mathbf{S}_1$ instead of $\mathbf{S}_0$.

Lemma 14. $|\Pr[F_4] - \Pr[F_3]| \leq \mathsf{negl}(n)$.

Proof. This lemma directly follows from the fact that both $\mathbf{S}_0$ and $\mathbf{S}_1$ have equivalent decryption ability except with negligible probability.

Game 5. This game is identical to Game 4 except that the challenger $\mathcal{C}$ changes the key generation phase and the challenge phase as follows:

KeyGen. First uniformly choose matrices $\mathbf{A} \xleftarrow{\$} \mathcal{D}_\lambda^{n\times n}, \mathbf{C} \xleftarrow{\$} \mathcal{D}_\lambda^{\ell\times n}$, $\mathbf{S}_0, \mathbf{S}_1 \xleftarrow{\$} (\widetilde{\mathcal{B}}_{\mu_1}^n)^q$, and $\mathbf{E}_0, \mathbf{E}_1 \xleftarrow{\$} \mathcal{B}_\mu^{n\times q}$. Then, compute $\mathbf{B}_0 = \mathbf{S}_0^\intercal \mathbf{A} + \mathbf{E}_0^\intercal, \mathbf{B}_1 = \mathbf{S}_1^\intercal \mathbf{A} + \mathbf{E}_1^\intercal \in \{0,1\}^{q\times n}$, $\mathbf{B}'_0 = \mathbf{B}_0 - \mathbf{G}\mathbf{H}_{\mathbf{t}^*}$ and $\mathbf{B}'_1 = \mathbf{B}_1 - \mathbf{G}\mathbf{H}_{\mathbf{t}^*}$. Finally, $\mathcal{C}$ sends $pk = (\mathbf{A}, \mathbf{B}'_0, \mathbf{B}'_1, \mathbf{C})$ to the adversary $\mathcal{A}$, and keeps $sk = (\mathbf{S}_0, \mathbf{S}_1)$ to itself.

Challenge. After receiving two equal length plaintexts $\mathbf{m}_0, \mathbf{m}_1 \in \mathcal{M}$ from the adversary $\mathcal{A}$, the challenger $\mathcal{C}$ first randomly chooses a bit $b^* \xleftarrow{\$} \{0,1\}$, and $\mathbf{s} \xleftarrow{\$} \widetilde{\mathcal{B}}_{\mu_1}^n, \mathbf{e}_1 \xleftarrow{\$} \mathcal{B}_\mu^n$ and $\mathbf{e}_2 \xleftarrow{\$} \mathcal{B}_\mu^\ell$. Then, it defines

$$\begin{aligned}
\mathbf{c}^* &:= \mathbf{A}\mathbf{s} + \mathbf{e}_1 && \in \{0,1\}^n \\
\mathbf{c}_0^* &:= (\mathbf{G}\mathbf{H}_{\mathbf{t}^*} + \mathbf{B}'_0)\mathbf{s} + \mathbf{S}_0^\intercal \mathbf{e}_1 - \mathbf{E}_0^\intercal \mathbf{s} = \mathbf{S}_0^\intercal \mathbf{c}^* && \in \{0,1\}^q \\
\mathbf{c}_1^* &:= (\mathbf{G}\mathbf{H}_{\mathbf{t}^*} + \mathbf{B}'_1)\mathbf{s} + \mathbf{S}_1^\intercal \mathbf{e}_1 - \mathbf{E}_1^\intercal \mathbf{s} = \mathbf{S}_1^\intercal \mathbf{c}^* && \in \{0,1\}^q \\
\mathbf{c}_2^* &:= \mathbf{C}\mathbf{s} + \mathbf{e}_2 + \mathbf{G}_2 \mathbf{m}_{b^*} && \in \{0,1\}^\ell,
\end{aligned}$$

and returns the challenge ciphertext $(\mathbf{c}, \mathbf{c}_0^*, \mathbf{c}_1^*, \mathbf{c}_2^*)$ to the adversary $\mathcal{A}$.

Lemma 15. *If the decisional* $\mathsf{LPN}_{\mu,n}$ *problem is* $2^{\omega(n^{\frac{1}{2}})}$*-hard, then we have that* $|\Pr[F_5] - \Pr[F_4]| \leq \mathsf{negl}(n)$.

Proof. One can easily show this lemma holds by using similar proofs from Lemma 10 to Lemma 14. We omit the details.

Game 6. This game is identical to Game 5 except that the challenger $\mathcal{C}$ changes the challenge phase as follows:

Challenge. After receiving two equal length plaintexts $\mathbf{m}_0, \mathbf{m}_1 \in \mathcal{M}$ from the adversary $\mathcal{A}$, the challenger $\mathcal{C}$ first randomly chooses $b^* \xleftarrow{\$} \{0,1\}, \mathbf{u} \xleftarrow{\$} \{0,1\}^n$ and $\mathbf{v} \xleftarrow{\$} \{0,1\}^\ell$. Then, it defines

$$\begin{array}{ll} \mathbf{c}^* := \mathbf{u} & \in \{0,1\}^n \\ \mathbf{c}_0^* := \mathbf{S}_0\mathbf{c}^* & \in \{0,1\}^q \\ \mathbf{c}_1^* := \mathbf{S}_1\mathbf{c}^* & \in \{0,1\}^q \\ \mathbf{c}_2^* := \mathbf{v} + \mathbf{G}_2\mathbf{m}_{b^*} & \in \{0,1\}^\ell, \end{array}$$

and returns the challenge ciphertext $(\mathbf{c}, \mathbf{c}_0^*, \mathbf{c}_1^*, \mathbf{c}_2^*)$ to the adversary $\mathcal{A}$.

Lemma 16. *If the decisional* $\mathsf{LPN}_{\mu,n}$ *problem is* $2^{\omega(n^{\frac{1}{2}})}$*-hard, then we have that* $|\Pr[F_6] - \Pr[F_5]| \leq \mathsf{negl}(n)$.

Proof. Since the only difference between Game 5 and Game 6 is that $\mathcal{C}$ replaces $\mathbf{c}^* = \mathbf{A}\mathbf{s} + \mathbf{e}_1$ and $\mathbf{c}_2^* = \mathbf{C}\mathbf{s} + \mathbf{e}_2 + \mathbf{G}_2\mathbf{m}_{b^*}$ in Game 5 with $\mathbf{c}^* := \mathbf{u}$ and $\mathbf{c}_2^* := \mathbf{v} + \mathbf{G}_2\mathbf{m}_{b^*}$ in Game 6, where $\mathbf{u} \xleftarrow{\$} \{0,1\}^n$ and $\mathbf{v} \xleftarrow{\$} \{0,1\}^\ell$, by our assumption and Corollary 1 we have that Game 5 and Game 6 are computationally indistinguishable for any PPT adversary $\mathcal{A}$. Obviously, we have that $|\Pr[F_6] - \Pr[F_5]| \leq \mathsf{negl}(n)$ holds.

Lemma 17. $\Pr[F_6] = \frac{1}{2}$.

Proof. This claim follows from the fact that the challenge ciphertext $(\mathbf{c}, \mathbf{c}_0^*, \mathbf{c}_1^*, \mathbf{c}_2^*)$ in Game 6 perfectly hides the information of $\mathbf{m}_{b^*}$.

In all, by Lemma 10 $\sim$ Lemma 17, we have that $\epsilon = |\Pr[F_0] = \frac{1}{2}| \leq \mathsf{negl}(n)$. This completes the proof of Theorem 5.

Acknowledgments

Yu Yu was supported by the National Basic Research Program of China Grant No. 2013CB338004, the National Natural Science Foundation of China Grant (Nos. 61472249, 61572192, 61572149 and U1536103), Shanghai excellent academic leader funds (No. 16XD1400200) and International Science & Technology Cooperation & Exchange Projects of Shaanxi Province (2016KW-038). Jiang Zhang is supported by the National Basic Research Program of China under Grant No. 2013CB338003 and the National Natural Science Foundation of China under Grant Nos. U1536205, 61472250 and 61402286.

References

1. Related work on LPN-based authentication schemes, http://www.ecrypt.eu.org/lightweight/index.php/HB
2. Alekhnovich, M.: More on average case vs approximation complexity. In: 44th Annual Symposium on Foundations of Computer Science. pp. 298–307. IEEE, Cambridge, Massachusetts (Oct 2003)
3. Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Advances in Cryptology - CRYPTO 2009. pp. 595–618 (2009)
4. Applebaum, B., Ishai, Y., Kushilevitz, E.: Cryptography with constant input locality. In: Advances in Cryptology - CRYPTO 2007. pp. 92–110 (2007), full version available at http://www.eng.tau.ac.il/~bennyap/pubs/input-locality-full-revised-1.pdf
5. Becker, A., Joux, A., May, A., Meurer, A.: Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In: Advances in Cryptology - EUROCRYPT 2012. pp. 520–536 (2012)
6. Berlekamp, E., McEliece, R.J., van Tilborg, H.: On the inherent intractability of certain coding problems. IEEE Transactions on Information Theory 24(3), 384–386 (1978)
7. Bernstein, D.J., Lange, T., Peters, C.: Smaller decoding exponents: Ball-collision decoding. In: Advances in Cryptology - CRYPTO 2011. pp. 743–760 (2011)
8. Blum, A., Furst, M.L., Kearns, M.J., Lipton, R.J.: Cryptographic primitives based on hard learning problems. In: Stinson, D.R. (ed.) Advances in Cryptology—CRYPTO '93. LNCS, vol. 773, pp. 278–291. Springer-Verlag (22–26 Aug 1993)
9. Blum, A., Kalai, A., Wasserman, H.: Noise-tolerant learning, the parity problem, and the statistical query model. Journal of the ACM 50(4), 506–519 (2003)
10. Boneh, D., Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. SIAM J. Comput. 36(5), 1301–1328 (Dec 2006), http://dx.doi.org/10.1137/S009753970544713X
11. Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. In: Cachin, C., Camenisch, J. (eds.) Advances in Cryptology – EUROCRYPT 2004, Lecture Notes in Computer Science, vol. 3027, pp. 207–222. Springer Berlin / Heidelberg (2004)
12. Canteaut, A., Chabaud, F.: A new algorithm for finding minimum-weight words in a linear code: Application to mceliece's cryptosystem and to narrow-sense BCH codes of length 511. IEEE Transactions on Information Theory 44(1), 367–378 (1998)
13. Cash, D., Kiltz, E., Tessaro, S.: Two-round man-in-the-middle security from LPN. In: Proceedings of the 13th Theory of Cryptography (TCC 2016-A). pp. 225–248 (2016)
14. Cramer, R., Damgård, I.: On the amortized complexity of zero-knowledge protocols. In: Halevi, S. (ed.) Advances in Cryptology – CRYPTO 2009, Lecture Notes in Computer Science, vol. 5677, pp. 177–191. Springer Berlin Heidelberg (2009), http://dx.doi.org/10.1007/978-3-642-03356-8_11
15. Damgård, I., Park, S.: How practical is public-key encryption based on lpn and ring-lpn? Cryptology ePrint Archive, Report 2012/699 (2012), http://eprint.iacr.org/2012/699
16. David, B., Dowsley, R., Nascimento, A.C.A.: Universally composable oblivious transfer based on a variant of LPN. In: Proceedings of the 13th International Conference on Cryptology and Network Security (CANS 2014). pp. 143–158 (2014)

17. Dodis, Y., Kalai, Y.T., Lovett, S.: On cryptography with auxiliary input. In: Mitzenmacher, M. (ed.) STOC. pp. 621–630. ACM (2009)
18. Dodis, Y., Kiltz, E., Pietrzak, K., Wichs, D.: Message authentication, revisited. In: Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2012). pp. 355–374 (2012)
19. Döttling, N.: Low noise lpn: Kdm secure public key encryption and sample amplification. In: Public-Key Cryptography–PKC 2015. pp. 604–626. Springer (2015)
20. Döttling, N., Müller-Quade, J., Nascimento, A.C.A.: IND-CCA secure cryptography based on a variant of the LPN problem. In: Advances in Cryptology – ASIACRYPT 2012. pp. 485–503 (2012)
21. Feldman, V., Gopalan, P., Khot, S., Ponnuswami, A.K.: New results for learning noisy parities and halfspaces. In: 47th Symposium on Foundations of Computer Science. pp. 563–574. IEEE, Berkeley, CA, USA (Oct 21–24 2006)
22. Forney, D.: Concatenated Codes. MIT Press (1966)
23. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Ladner, R.E., Dwork, C. (eds.) Proceedings of the 40th Annual ACM Symposium on Theory of Computing. pp. 197–206. ACM, Victoria, BC, Canada (17–20 May 2008)
24. Gertner, Y., Kannan, S., Malkin, T., Reingold, O., Viswanathan, M.: The relationship between public key encryption and oblivious transfer. In: Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on. pp. 325–335 (2000)
25. Goldreich, O., Levin, L.A.: A hard-core predicate for all one-way functions. In: Johnson [31], pp. 25–32
26. Goldwasser, S., Kalai, Y., Peikert, C., Vaikuntanathan, V.: Robustness of the learning with errors assumption. In: Innovations in Theoretical Computer Science, ITCS'10. pp. 230–240. Tsinghua University Press (2010)
27. Graham, R.L., Knuth, D.E., Patashnik, O.: Concrete Mathematics: A Foundation for Computer Science. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2nd edn. (1994)
28. Håstad, J., Impagliazzo, R., Levin, L., Luby, M.: Construction of pseudorandom generator from any one-way function. SIAM Journal on Computing 28(4), 1364–1396 (1999)
29. Hopper, N.J., Blum, M.: Secure human identification protocols. In: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2001). pp. 52–66 (2001)
30. Jain, A., Krenn, S., Pietrzak, K., Tentes, A.: Commitments and efficient zero-knowledge proofs from learning parity with noise. In: Advances in Cryptology – ASIACRYPT 2012. pp. 663–680 (2012)
31. Johnson, D.S. (ed.): Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing. Seattle, Washington (15–17 May 1989)
32. Juels, A., Weis, S.A.: Authenticating pervasive devices with human protocols. In: Shoup, V. (ed.) Advances in Cryptology—CRYPTO 2005. LNCS, vol. 3621, pp. 293–308. Springer-Verlag (14–18 Aug 2005)
33. Justesen, J.: A class of constructive asymptotically good algebraic codes. IEEE Trans. Info. Theory 18(5), 652–656 (1972)
34. Katz, J., Shin, J.S.: Parallel and concurrent security of the hb and hb^+ protocols. In: Vaudenay, S. (ed.) Advances in Cryptology—EUROCRYPT 2006. LNCS, vol. 4004, pp. 73–87. Springer-Verlag (2006)

35. Kiltz, E.: Chosen-ciphertext security from tag-based encryption. In: Halevi, S., Rabin, T. (eds.) Theory of Cryptography, Lecture Notes in Computer Science, vol. 3876, pp. 581–600. Springer Berlin Heidelberg (2006), http://dx.doi.org/10.1007/11681878_30
36. Kiltz, E., Masny, D., Pietrzak, K.: Simple chosen-ciphertext security from low-noise lpn. In: Krawczyk, H. (ed.) Public-Key Cryptography PKC 2014, Lecture Notes in Computer Science, vol. 8383, pp. 1–18. Springer Berlin Heidelberg (2014), http://dx.doi.org/10.1007/978-3-642-54631-0_1
37. Kiltz, E., Pietrzak, K., Cash, D., Jain, A., Venturi, D.: Efficient authentication from hard learning problems. In: Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2011). pp. 7–26 (2011)
38. Kirchner, P.: Improved generalized birthday attack. Cryptology ePrint Archive, Report 2011/377 (2011), http://eprint.iacr.org/2011/377
39. Levieil, E., Fouque, P.A.: An improved lpn algorithm. In: Proceedings of the 5th Conference on Security and Cryptography for Networks (SCN 2006). pp. 348–359 (2006)
40. Lyubashevsky, V.: The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem. In: Proceedings of the 9th International Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM 2005). pp. 378–389 (2005)
41. Lyubashevsky, V., Masny, D.: Man-in-the-middle secure authentication schemes from lpn and weak prfs. In: Advances in Cryptology - CRYPTO 2013. pp. 308–325 (2013)
42. May, A., Meurer, A., Thomae, E.: Decoding random linear codes in $\tilde{O}(2^{0.054n})$. In: Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2011). pp. 107–124 (2011)
43. Micciancio, D., Mol, P.: Pseudorandom knapsacks and the sample complexity of lwe search-to-decision reductions. In: Rogaway, P. (ed.) Advances in Cryptology – CRYPTO 2011, Lecture Notes in Computer Science, vol. 6841, pp. 465–484. Springer Berlin Heidelberg (2011)
44. Micciancio, D., Peikert, C.: Trapdoors for lattices: Simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology – EUROCRYPT 2012, Lecture Notes in Computer Science, vol. 7237, pp. 700–718. Springer Berlin Heidelberg (2012)
45. Pietrzak, K.: Cryptography from learning parity with noise. In: Proceedings of the Theory and Practice of Computer Science (SOFTSEM 2012). pp. 99–114 (2012)
46. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) STOC. pp. 84–93. ACM (2005)
47. Rosen, A., Segev, G.: Chosen-ciphertext security via correlated products. In: Reingold, O. (ed.) Theory of Cryptography, Lecture Notes in Computer Science, vol. 5444, pp. 419–436. Springer Berlin / Heidelberg (2009)
48. Stern, J.: A method for finding codewords of small weight. In: Coding Theory and Applications, 3rd International Colloquium. pp. 106–113 (1988)
49. Yu, Y.: The LPN problem with auxiliary input. (withdrawn) see historical versions at http://eprint.iacr.org/2009/467

A Definitions and Security Notions

A.1 Symmetric-Key Encryption Schemes with Auxiliary Input

Definition 6 (Symmetric-key encryption schemes). *A symmetric-key encryption scheme Π is a tuple (KeyGen,Enc,Dec) with message space $\mathcal{M}$, such that*

- $\mathsf{KeyGen}(1^n)$ *is a PPT algorithm that takes a security-parameter 1^n and outputs a symmetric key k.*
- $\mathsf{Enc}_k(m)$ *is a PPT algorithm that encrypts a message $m \in \mathcal{M}$ under key k and outputs a ciphertext c.*
- $\mathsf{Dec}_k(c)$ *is a deterministic polynomial-time algorithm that decrypts a ciphertext c using key k and outputs a plaintext m.*

Definition 7 (Correctness). *We say that a symmetric-key encryption scheme Π = (KeyGen, Enc, Dec) is correct, if it holds for every plaintext $m \in \mathcal{M}$ that*

$$\Pr_{k \leftarrow \mathsf{KeyGen}(1^n)}[\ \mathsf{Dec}_k(\mathsf{Enc}_k(m)) \neq m\ ] = \mathsf{negl}(n)\ .$$

Definition 8 (IND-CPA/IND-CCA SKE w.r.t. auxiliary input). *For $X \in \{CPA,CCA\}$, a symmetric-key encryption scheme Π = (KeyGen,Enc,Dec) is IND-X secure w.r.t. sub-exponentially hard-to-invert auxiliary input if there exists a constant $0 < \alpha < 1$ such that for any PPT adversary $\mathcal{A}$, any $2^{-\Omega(n^\alpha)}$-hard-to-invert function f*

$$\Pr[\ \mathsf{SKE}^{X}_{\Pi,f,\mathcal{A}}(1^n,\alpha) = 1\ ]\ \leq\ \frac{1}{2} + \mathsf{negl}(n)\ ,$$

where $\mathsf{SKE}^{cpa}_{\Pi,f,\mathcal{A}}(1^n,\alpha)$ is the IND-CPA indistinguishability experiment defined as below:

1. *On $k \leftarrow \mathsf{KeyGen}(1^n)$, the adversary takes as input 1^n, $f(k)$, and is given oracle access to Enc_k. Then, he outputs a pair of messages m_0 and m_1 of the same length.*
2. *A random bit $b \xleftarrow{\$} \{0,1\}$ is sampled, and then a challenge ciphertext $c \leftarrow \mathsf{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$.*
3. *$\mathcal{A}$ continues to have oracle access to Enc_k and finally outputs $b' \in \{0,1\}$.*
4. *The experiment outputs 1 if $b' = b$, and 0 otherwise.*

and $\mathsf{SKE}^{cca}_{\Pi,f,\mathcal{A}}(1^n,\alpha)$ is the IND-CCA indistinguishability experiment defined as below:

1. *On $k \leftarrow \mathsf{KeyGen}(1^n)$, the adversary takes as input 1^n, $f(k)$, and is given oracle access to Enc_k and Dec_k. Then, he outputs a pair of messages m_0 and m_1 of the same length.*
2. *A random bit $b \xleftarrow{\$} \{0,1\}$ is sampled, and then a challenge ciphertext $c \leftarrow \mathsf{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$.*
3. *$\mathcal{A}$ continues to have oracle access to Enc_k and Dec_k (with the exception that decryption for challenge ciphertext is not allowed) and finally outputs $b' \in \{0,1\}$.*
4. *The experiment outputs 1 if $b' = b$, and 0 otherwise.*

A.2 Public-Key Encryption Schemes

Definition 9 (Public-key encryption schemes). *A public key encryption scheme Π is a tuple (*KeyGen,Enc,Dec*) with message space $\mathcal{M}$, such that*

- $\mathsf{KeyGen}(1^n)$ *is a PPT algorithm that takes a security-parameter 1^n and outputs a pair of public and private keys (pk,sk).*
- $\mathsf{Enc}_{pk}(m)$ *is a PPT algorithm that encrypts message $m \in \mathcal{M}$ under public key pk and outputs a ciphertext c.*
- $\mathsf{Dec}_{sk}(c)$ *is a deterministic polynomial-time algorithm that decrypts a ciphertext c using secret key sk and outputs a plaintext m (or $\perp$).*

Definition 10 (Correctness). *We say that a public-key encryption scheme Π = (*KeyGen,Enc,Dec*) is correct, if it holds for every plaintext $m \in \mathcal{M}$ that*

$$\Pr_{(pk,sk)\leftarrow\mathsf{KeyGen}(1^n)}[\ \mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) \neq m\ ] = \mathsf{negl}(n)\ .$$

Definition 11 (IND-CPA/IND-CCA PKE). *For $X \in \{CPA, CCA\}$, a public-key encryption scheme Π = (*KeyGen,Enc,Dec*) is IND-X secure if for any PPT adversary $\mathcal{A}$*

$$\Pr[\ \mathsf{PKE}^{X}_{\Pi,\mathcal{A}}(1^n) = 1\ ]\ \leq\ \frac{1}{2} + \mathsf{negl}(n)\ ,$$

where $\mathsf{PKE}^{cpa}_{\Pi,\mathcal{A}}(1^n)$ is the IND-CPA indistinguishability experiment defined as below:

1. *On $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$, the adversary takes as input 1^n and pk. Then, he outputs a pair of messages m_0 and m_1 of the same length.*
2. *A random bit $b \xleftarrow{\$} \{0,1\}$ is sampled, and then a challenge ciphertext $c \leftarrow \mathsf{Enc}_{pk}(m_b)$ is computed and given to $\mathcal{A}$.*
3. *$\mathcal{A}$ continues his computation and finally outputs $b' \in \{0,1\}$.*
4. *The experiment outputs 1 if $b' = b$, and 0 otherwise.*

and $\mathsf{PKE}^{cca}_{\Pi\mathcal{A}}(1^n)$ is the IND-CCA indistinguishability experiment defined as below:

1. *On $(pk, sk) \leftarrow \mathsf{KeyGen}(1^n)$, the adversary takes as input 1^n and pk, and is given oracle access to Dec_{sk}. Then, he outputs a pair of messages m_0 and m_1 of the same length.*
2. *A random bit $b \xleftarrow{\$} \{0,1\}$ is sampled, and then a challenge ciphertext $c \leftarrow \mathsf{Enc}_{pk}(m_b)$ is computed and given to $\mathcal{A}$.*
3. *$\mathcal{A}$ continues to have oracle access to Dec_{sk} (with the exception that decryption for challenge ciphertext is not allowed) and finally outputs $b' \in \{0,1\}$.*
4. *The experiment outputs 1 if $b' = b$, and 0 otherwise.*

B Facts, Lemmas, Inequalities and Proofs Omitted

Lemma 18 (Sample-preserving reduction). *For the same assumptions and notations as in the proof of Theorem 2, we have*

$$\begin{aligned}&(f(\mathbf{x},\mathbf{e};Z),Z,\mathbf{A},\ \mathbf{A}\cdot\mathbf{y}+\mathbf{e},\mathbf{r}^{\mathsf{T}},\mathbf{r}^{\mathsf{T}}\cdot\mathbf{y}) \overset{c}{\sim} (f(\mathbf{x},\mathbf{e};Z),Z,\mathbf{A},\ \mathbf{A}\cdot\mathbf{y}+\mathbf{e},\mathbf{r}^{\mathsf{T}},U_1)\\ \Rightarrow\ &(f(\mathbf{x},\mathbf{e};Z),Z,\mathbf{A},\ \mathbf{A}\cdot\mathbf{y}+\mathbf{e}) \overset{c}{\sim} (f(\mathbf{x},\mathbf{e};Z),Z,\mathbf{A},U_{q'})\ .\end{aligned}$$

Proof. Assume for contradiction that there exists a polynomial $p(\cdot)$ and a PPT distinguisher $\mathcal{D}$ such that

$$\Pr[\,\mathcal{D}(f(\mathbf{x},\mathbf{e};Z),Z,\mathbf{A},\ \mathbf{A}\cdot\mathbf{y}+\mathbf{e})=0]-\Pr[\,\mathcal{D}(f(\mathbf{x},\mathbf{e};Z),Z,\mathbf{A},U_{q'})=0]\geq 1/p(n)$$

for infinitely many n's and we recall that $\mathbf{y},\mathbf{r}\sim U_\lambda$. Given input $(z_1,z,\mathbf{A},\mathbf{A}\cdot\mathbf{y}+\mathbf{e},\mathbf{r}^{\mathsf{T}})$, we use an efficient $\mathcal{D}'$ (which invokes $\mathcal{D}$) to predict the Goldreich-Levin hardcore bit $\mathbf{r}^{\mathsf{T}}\cdot\mathbf{y}$ with non-negligible probability (and thus a contradiction to the assumption). $\mathcal{D}'$ chooses a random $\mathbf{u}\xleftarrow{\$}\{0,1\}^{q'}$,computes a new $q'\times n$ Boolean matrix $\tilde{\mathbf{A}}=\mathbf{A}-\mathbf{u}\cdot\mathbf{r}^{\mathsf{T}}$, applies $\mathcal{D}$ on $(z_1,z,\tilde{\mathbf{A}},\mathbf{A}\mathbf{y}+\mathbf{e})$ and outputs his answer. Note that $\tilde{\mathbf{A}}\sim U_{q'\times n}$ and $\mathbf{A}\mathbf{y}+\mathbf{e}=\tilde{\mathbf{A}}\mathbf{y}+\mathbf{e}+\mathbf{u}\cdot\mathbf{r}^{\mathsf{T}}\mathbf{y}$. Therefore, when $\mathbf{r}^{\mathsf{T}}\mathbf{y}=0$ we have $(z_1,z,\tilde{\mathbf{A}},\mathbf{A}\mathbf{y}+\mathbf{e})$ follows $(f(\mathbf{x},\mathbf{e};Z),Z,\tilde{\mathbf{A}},\tilde{\mathbf{A}}\cdot\mathbf{y}+\mathbf{e})$ and for $\mathbf{r}^{\mathsf{T}}\mathbf{y}=1$ it is distributed according to $(f(\mathbf{x},\mathbf{e};Z),Z,\tilde{\mathbf{A}},U_{q'})$.

$$\begin{aligned}&\Pr[\mathcal{D}'(f(\mathbf{x},\mathbf{e};Z),Z,\tilde{\mathbf{A}},\tilde{\mathbf{A}}\mathbf{y}+\mathbf{e},\mathbf{r}^{\mathsf{T}})=\mathbf{r}^{\mathsf{T}}\cdot\mathbf{y}]\\ =\ &\Pr[\mathbf{r}^{\mathsf{T}}\cdot\mathbf{y}=0]\cdot\Pr[\mathcal{D}'(f(\mathbf{x},\mathbf{e};Z),Z,\tilde{\mathbf{A}},\tilde{\mathbf{A}}\mathbf{y}+\mathbf{e},\mathbf{r}^{\mathsf{T}})=0\mid\mathbf{r}^{\mathsf{T}}\cdot\mathbf{y}=0]\\ &\quad+\ \Pr[\mathbf{r}^{\mathsf{T}}\cdot\mathbf{y}=1]\cdot\Pr[\mathcal{D}'(f(\mathbf{x},\mathbf{e};Z),Z,\tilde{\mathbf{A}},\tilde{\mathbf{A}}\mathbf{y}+\mathbf{e},\mathbf{r}^{\mathsf{T}})=1\mid\mathbf{r}^{\mathsf{T}}\cdot\mathbf{y}=1]\\ =\ &\frac{1}{2}\big(\Pr[\,\mathcal{D}(f(\mathbf{x},\mathbf{e};Z),Z,\mathbf{A},\ \mathbf{A}\cdot\mathbf{y}+\mathbf{e})=0]\\ &\qquad+1-\Pr[\,\mathcal{D}(f(\mathbf{x},\mathbf{e};Z),Z,\mathbf{A},\ U_{q'})=0]\big)\\ \geq\ &\frac{1}{2}+\frac{1}{2p(n)}\ ,\end{aligned}$$

which completes the proof.

Proof of Lemma 9. Consider $|(\mathbf{S}_0'-\mathbf{S}_0)^{\mathsf{T}}\mathbf{e}+(\mathbf{E}_0-\mathbf{E}_0')^{\mathsf{T}}\mathbf{s}|$ conditioned on any $|\mathbf{e}|\leq 1.01\mu n$ (except for a $2^{-\Omega(n)}$-fraction) and $|\mathbf{s}|\leq 2\mu n$. We have by Lemma 7 and Lemma 8 that $\mathbf{S}_0^{\mathsf{T}}\mathbf{e}$, ${\mathbf{S}_0'}^{\mathsf{T}}\mathbf{e}$ are i.i.d. to $\mathcal{B}^q_{\delta_1}$, and ${\mathbf{E}_0}^{\mathsf{T}}\mathbf{s}$, ${\mathbf{E}_0'}^{\mathsf{T}}\mathbf{s}$ are i.i.d. to $\mathcal{B}^q_{\delta_2}$, where $\delta_1\leq 1/2-n^{-\alpha/2}$ and $\delta_2\leq 1/2-n^{-\alpha}/2$. Thus, $\big((\mathbf{S}_0'-\mathbf{S}_0)^{\mathsf{T}}\mathbf{e}+(\mathbf{E}_0-\mathbf{E}_0')^{\mathsf{T}}\mathbf{s}\big)$ follows $\mathcal{B}^q_\delta$ for $\delta\leq 1/2-2n^{-3\alpha}$ by the Piling-up lemma, and then we complete the proof with Lemma 2. □

Lemma 19 (Flattening Shannon entropy). *For any $n\in\mathbb{N}$, $0<\mu<1/2$ and any constant $0<\Delta<1$, there exists some random variable $W\in\{0,1\}^n$ such that $\mathbf{H}_\infty(W)\geq(1-\Delta)n\mathbf{H}(\mu)$ and $\mathsf{SD}(\mathcal{B}^n_\mu,W)\leq 2^{-\Omega(\mu n)}$.*