On the Robustness of Learning Parity with Noise

Nan Yao[1], Yu Yu[1,3(✉)], Xiangxue Li[2,3,4(✉)], and Dawu Gu[1]

[1] Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai, China
yyuu@sjtu.edu.cn

[2] Department of Computer Science and Technology,
East China Normal University, Shanghai, China
xxli@cs.ecnu.edu.cn

[3] Westone Cryptologic Research Center, Beijing, China

[4] National Engineering Laboratory for Wireless Security, XUPT, Xi'an, China

Abstract. The Learning Parity with Noise (LPN) problem is well understood in learning theory and cryptography and has been found quite useful in constructing various lightweight cryptographic primitives. There exists non-trivial evidence that the problem is robust on high-entropy secrets (and even given hard-to-invert leakages), and the justified results by Dodis, Kalai and Lovett (STOC 2009) were established under non-standard hard learning assumptions. The recent progress by Suttichaya and Bhattarakosol (Information Processing Letters, Volume 113, Issues 14–16) claimed that LPN remains provably secure (reducible from the LPN assumption itself) as long as the secret is sampled from any linear min-entropy source, and thereby resolves the long-standing open problem. In the paper, we point out that their proof is flawed and their understanding about LPN is erroneous. We further offer a remedy with some slight adaption to the setting of Suttichaya and Bhattarakosol.

Keywords: Learning Parity with Noise · High-entropy secrets · Provable security · Leftover Hash Lemma

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), $q \in \mathbb{N}$ (number of queries) and $0 < \mu < 1/2$ (noise rate) postulates that it is computationally infeasible to recover the n-bit secret $s \in \mathbb{Z}_2^n$ given $(a{\cdot}s{\oplus}e,\ a)$, where a is a random $q{\times}n$ matrix, e follows Ber_μ^q, Ber_μ denotes the Bernoulli distribution with parameter μ (i.e., $\Pr[\mathsf{Ber}_\mu = 1] = \mu$ and $\Pr[\mathsf{Ber}_\mu = 0] = 1-\mu$), '$\cdot$' denotes matrix vector multiplication over GF(2) and '$\oplus$' denotes bitwise XOR. The decisional version of LPN simply assumes that $a \cdot s \oplus e$ is pseudorandom (i.e., computationally indistinguishable from uniform randomness) given a. While seemingly stronger, the decisional version is known to be polynomially equivalent to its computational counterpart [4,8,21].

K.-Y. Lam et al. (Eds.): ICICS 2016, LNCS 9977, pp. 99–106, 2016.
DOI: 10.1007/978-3-319-50011-9_8

Hardness of LPN. The computational LPN problem represents a well-known NP-complete problem "decoding random linear codes" [6] and thus its worst-case hardness is well understood. LPN was also extensively studied in learning theory, and it was shown in [15] 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 (i.e., $\mu = \Theta(1)$), the best known LPN solvers [9,25] 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 [26], or even $2^{O(n)}$ given only $q = O(n)$ queries [28]. Under low noise rate $\mu = n^{-c}$ $(0 < c < 1)$, the security of LPN is less well understood: on the one hand, for $q = n + O(1)$ we can already do an efficient distinguishing attack with advantage $2^{-O(n^{1-c})}$ that matches the statistical indistinguishability (from uniform randomness) of the LPN samples ; on the other hand, for (even super-)polynomial q the best known attacks [5,7,10,24,31] are not asymptotically better, i.e., still at the order of $2^{\Theta(n^{1-c})}$. We mention that LPN does not succumb to known quantum algorithms, which makes it a promising candidate for "post-quantum cryptography". Furthermore, LPN also enjoys simplicity and is more suited for weak-power devices (e.g., RFID tags) than other quantum-secure candidates such as LWE [30].

LPN-based Cryptographic Applications. LPN was used as a basis for building lightweight authentication schemes against passive [18] and even active adversaries [20,21] (see [1] for a more complete literature). Recently, Kiltz et al. [23] and Dodis et al. [13] constructed randomized MACs based on the hardness of LPN, which implies a two-round authentication scheme with man-in-the-middle security. Lyubashevsky and Masny [27] gave an efficient three-round authentication scheme whose security can be based on LPN or weak pseudorandom functions (PRFs). Applebaum et al. [3] showed how to constructed a linear-stretch pseudorandom generator (PRG) from LPN. We mention other not-so-relevant applications such as public-key encryption schemes [2,14,22], oblivious transfer [11], commitment schemes and zero-knowledge proofs [19], and refer to a recent survey [29] on the current state-of-the-art about LPN.

The Error in [32] and Our Contributions. In the standard LPN, the secret vector is assumed to be generated uniformly at random and kept confidential. However, for the version where the secret vector is sampled from some arbitrary distribution with sufficient amount of min-entropy, its hardness is still unclear. In the paper [32], the authors claimed a positive answer on the open question. More specifically, they show that if the l-bit secret is of min-entropy $k = \Omega(l)$, then the LPN problem (on such a weak secret) is hard as long as the standard one is (on uniform secrets). Unfortunately, we find that the claim in [32] is flawed. Loosely speaking, the main idea of [32, Theorem 4] is the following: denote by $\mathcal{D}$ a distribution over $\mathbb{Z}_2^l$ with min-entropy $k = \Omega(l)$ and let $n = k - 2\log(1/\epsilon)$ for some ϵ negligible in the security parameter[1], sample $B \xleftarrow{\$} \mathbb{Z}_2^{m\times n}$, $C \xleftarrow{\$} \mathbb{Z}_2^{n\times l}$,

[1] The security argument in [32] is quite informal: it defines a number of parameters without specifying which one is the main security parameter. We assume WLOG that the security parameter is l (the length of the secret).

$E \leftarrow \mathsf{Ber}_{\alpha}^{m\times n}$, $F \xleftarrow{\$} \mathbb{Z}_2^{n\times l}$ and $e \leftarrow \mathsf{Ber}_{\beta}^{m}$, and let $A = BC \oplus EF$. The authors of [32] argue that $As \oplus e$ is computationally indistinguishable from uniform even conditioned on A and that A is statistically close to uniform. Quantitatively, the standard $\mathrm{LPN}_{n,\frac{1}{2}-\frac{(1-\alpha)^n}{2}}$ assumption implies $\mathrm{LPN}^{\mathcal{D}}_{\frac{1}{2}-(\frac{1}{2}-\beta)(1-\alpha)^n}$. We stress that the proofs are incorrect for at least the following reasons:

1. For a reasonable assumption, the noise rate should be bounded away from uniform at least polynomially, i.e., $(1-\alpha)^n/2 \geq 1/\mathsf{poly}(l)$. Otherwise, the hardness assumption is trivial and useless as it does not imply any efficient (polynomial-time computable) cryptographic applications.
2. $A = BC \oplus EF$ is not statistically close to uniform. BC is sampled from a random subspace of dimension $n < k \leq l$ and thus far from being uniform over $\mathbb{Z}_2^{m\times l}$ (recall that $m \gg l$). Every entry of matrix EF is distributed to $\mathsf{Ber}_{1/2-(1-\alpha)^n/2}$ for $(1-\alpha)^n/2 \geq 1/\mathsf{poly}(l)$ (see item 1 above). Therefore, the XOR sum of BC and EF never amplifies to statistically uniform randomness.
3. There are a few flawed intermediate statements. For example, the authors prove that every entry of EF is distributed according to $\mathsf{Ber}_{1/2-(1-\alpha)^n/2}$ and then conclude that EF follows $\mathsf{Ber}^{m\times l}_{1/2-(1-\alpha)^n/2}$, which is not true since there's no guarantee that the entries of EF are all independent.

We fix the flaw using the "sampling from random subspace" technique [16,33].

2 Preliminaries

Notations and Definitions. We use $[n]$ to denote set $\{1, \ldots, n\}$. 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. 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 $\mathcal{S}$ and binary string s, $|\mathcal{S}|$ denotes the cardinality of $\mathcal{S}$ and $|s|$ refers to the Hamming weight of s. We use Ber_{μ} to denote the Bernoulli distribution with parameter μ, i.e., $\Pr[\mathsf{Ber}_{\mu} = 1] = \mu$, $\Pr[\mathsf{Ber}_{\mu} = 0] = 1-\mu$, while Ber_{μ}^{q} denotes the concatenation of q independent copies of Ber_{μ}. For $n \in \mathbb{N}$, U_n denotes the uniform distribution over $\mathbb{Z}_2^n$ and independent of any other random variables in consideration, and $f(U_n)$ denotes the distribution induced by applying function f to U_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 $s \xleftarrow{\$} \mathcal{S}$ denote sampling s uniformly from set $\mathcal{S}$.

Entropy Definitions. For a random variable X and any $x \in \mathsf{Supp}(X)$, the sample-entropy of x with respect to X is defined as

$$\mathbf{H}_X(x) \stackrel{\mathsf{def}}{=} \log(1/\Pr[X = x])$$

from which we define the Shannon entropy and min-entropy of X respectively, i.e.,

$$\mathbf{H}_1(X) \stackrel{\mathsf{def}}{=} \mathbb{E}_{x\leftarrow X}[\ \mathbf{H}_X(x)\ ],\ \mathbf{H}_{\infty}(X) \stackrel{\mathsf{def}}{=} \min_{x\in\mathsf{Supp}(X)} \mathbf{H}_X(x).$$

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 D of running time t it holds that

$$|\ \Pr[\mathsf{D}(X)=1] - \Pr[\mathsf{D}(Y)=1]\ | \le \varepsilon.$$

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 $X \underset{(t,\varepsilon)}{\sim} Y$, and they 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.

We will use the decisional version of the LPN assumption which is known to be polynomially equivalent to the computational counterpart.

Definition 1 (LPN). *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*

$$(A,\ A{\cdot}X{\oplus}E) \stackrel{c}{\sim} (A, U_q) \tag{1}$$

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

$$\Pr[\ \mathsf{D}(A,\ A{\cdot}X{\oplus}E) = X\ ]\ =\ \mathsf{negl}(n),$$

where $A \sim U_{qn}$, $X \sim U_n$ and $E \sim \mathsf{Ber}_\mu^q$.

Lemma 1 (Leftover Hash Lemma [17]). *Let $(X,Z) \in \mathcal{X} \times \mathcal{Z}$ be any joint random variable with $\mathbf{H}_\infty(X|Z) \ge k$, and let $\mathcal{H} = \{h_b : \mathcal{X} \to \mathbb{Z}_2^l, b \in \mathbb{Z}_2^s\}$ be a family of universal hash functions, i.e., for any $x_1 \ne x_2 \in \mathcal{X}$, $\Pr_{b \xleftarrow{\$} \mathbb{Z}_2^s}[h_b(x_1) = h_b(x_2)] \le 2^{-l}$. Then, it holds that*

$$\mathsf{SD}\ \Big((Z,B,h_B(X))\ ,\ (Z,B,U_l)\Big)\ \le\ 2^{l-k},$$

where $B \sim U_s$.

3 Correcting the Errors

3.1 The Main Contribution of [32]

In the standard LPN, the secret is assumed to be generated uniformly at random and kept confidential. However, it remains open whether or not the hardness of the LPN can still hold when secret is not uniform but sampled from any distribution of linear entropy (in the secret length). The recent work [32] claims a positive answer on the open question. More specifically, the authors show that the standard $\mathrm{LPN}_{n,\frac{1}{2}-\frac{(1-\alpha)^n}{2}}$ assumption implies $\mathrm{LPN}^{\mathcal{D}}_{\frac{1}{2}-(\frac{1}{2}-\beta)(1-\alpha)^n}$ for any $\mathcal{D}$ of min-entropy $k = \Omega(l)$ and $n = k - 2\log(1/\epsilon)$.

3.2 How the Proof Goes Astray

The statement in [32, Theorem 4] does not hold. We recall that the setting of [32]: let $\mathcal{D}$ be any distribution over $\mathbb{Z}_2^l$ with min-entropy $k = \Omega(l)$ and let $n = k - 2\log(1/\epsilon)$ for some negligible ϵ, sample $B \xleftarrow{\$} \mathbb{Z}_2^{m\times n}$, $C \xleftarrow{\$} \mathbb{Z}_2^{n\times l}$, $E \leftarrow \mathsf{Ber}_\alpha^{m\times n}$, $F \xleftarrow{\$} \mathbb{Z}_2^{n\times l}$ and $e \leftarrow \mathsf{Ber}_\beta^m$, and let $A = BC \oplus EF$. As we pointed out in Sect. 1, there are a few flaws in their proof. First, the noise rate $1/2-(1-\alpha)^n/2$ is too strong to make any meaningful statements. Second, the matrix A is far from statistically uniform and there's not even any evidence that it could be pseudorandom. Third, the claim that EF follows $\mathsf{Ber}^{m\times l}_{1/2-(1-\alpha)^n/2}$ is not justified since they only show that each entry of EF follows $\mathsf{Ber}_{1/2-(1-\alpha)^n/2}$. It remains to show that entries of EF are all independent, which is less likely to be proven. Notice that here machinery such as two-source extraction does not help as the extracted bits are biased.

3.3 The Remedy

Now we give an easy remedy using the techniques from [16,33]. Let $\mathcal{D} \in \mathbb{Z}_2^l$ be any distribution with min-entropy $k = \Omega(l)$, $n = k - \omega(\log l)$, let $B \xleftarrow{\$} \mathbb{Z}_2^{m\times n}$, $C \xleftarrow{\$} \mathbb{Z}_2^{n\times l}$, $A = BC$ and $e \leftarrow \mathsf{Ber}_\alpha^m$, According to Leftover Hash Lemma, we have

$$(C, C\cdot s) \overset{s}{\sim} (C, U_n),$$

which in turn implies

$$(BC, (BC)\cdot s \oplus e) \overset{s}{\sim} (BC, B\cdot U_n \oplus e).$$

Note that the standard $\mathrm{LPN}_{n,\alpha}$ implies

$$(B, B\cdot U_n \oplus e) \overset{c}{\sim} (B, U_m).$$

It follows that

$$(BC, (BC)\cdot s \oplus e) \overset{c}{\sim} (BC, U_m)$$

and therefore completes the proof. This also simplifies the proof in [32] by eliminating the need for matrices E and F. Notice that we require that A is sampled from a random subspace of dimension n, instead of a uniform distribution.

4 Remarks on the Applications

In [32], the authors apply their result to the probabilistic CPA symmetric-key encryption scheme in [12], where the secret key is sampled from an arbitrary distribution with sufficient min-entropy. However, the noise rate $\frac{1}{2} - \frac{(1-\alpha)^n}{2}$ is either statistically close to uniform (and thus infeasible to build any efficient applications), or it does not yield the desired conclusion due to flawed proofs.

Acknowledgments. The work was supported by the National Natural Science Foundation of China Grant (Nos. 61472249, 61572192, 61572149, 61571191), and International Science & Technology Cooperation & Exchange Projects of Shaanxi Province (2016KW-038).

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, October 2003
3. Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 595–618. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03356-8_35
4. Applebaum, B., Ishai, Y., Kushilevitz, E.: Cryptography with constant input locality. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 92–110. Springer, Heidelberg (2007). doi:10.1007/978-3-540-74143-5_6. Full version: 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: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 520–536. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29011-4_31
6. Berlekamp, E., McEliece, R.J., van Tilborg, H.: On the inherent intractability of certain coding problems. IEEE Trans. Inf. Theory **24**(3), 384–386 (1978)
7. Bernstein, D.J., Lange, T., Peters, C.: Smaller decoding exponents: Ball-Collision decoding. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 743–760. Springer, Heidelberg (2011). doi:10.1007/978-3-642-22792-9_42
8. Blum, A., Furst, M., Kearns, M., Lipton, R.J.: Cryptographic primitives based on hard learning problems. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 278–291. Springer, Heidelberg (1994). doi:10.1007/3-540-48329-2_24
9. Blum, A., Kalai, A., Wasserman, H.: Noise-tolerant learning, the parity problem, and the statistical query model. J. ACM **50**(4), 506–519 (2003)
10. 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 Trans. Inf. Theory **44**(1), 367–378 (1998)
11. David, B., Dowsley, R., Nascimento, A.C.A.: Universally composable oblivious transfer based on a variant of LPN. In: Gritzalis, D., Kiayias, A., Askoxylakis, I. (eds.) CANS 2014. LNCS, vol. 8813, pp. 143–158. Springer, Heidelberg (2014). doi:10.1007/978-3-319-12280-9_10

12. Dodis, Y., Kalai, Y.T., Lovett, S.: On cryptography with auxiliary input. In: ACM Symposium on Theory of Computing, pp. 621–630 (2009)
13. Dodis, Y., Kiltz, E., Pietrzak, K., Wichs, D.: Message authentication, revisited. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 355–374. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29011-4_22
14. Döttling, N., Müller-Quade, J., Nascimento, A.C.A.: IND-CCA secure cryptography based on a variant of the LPN problem. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 485–503. Springer, Heidelberg (2012). doi:10.1007/978-3-642-34961-4_30
15. 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, 21–24 October 2006
16. Goldwasser, S., Kalai, Y., Peikert, C., Vaikuntanathan, V.: Robustness of the learning with errors assumption. In: Innovations in Theoretical Computer Science, ITCS 2010, pp. 230–240. Tsinghua University Press (2010)
17. Håstad, J., Impagliazzo, R., Levin, L., Luby, M.: Construction of pseudorandom generator from any one-way function. SIAM J. Comput. **28**(4), 1364–1396 (1999)
18. Hopper, N.J., Blum, M.: Secure human identification protocols. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 52–66. Springer, Heidelberg (2001). doi:10.1007/3-540-45682-1_4
19. Jain, A., Krenn, S., Pietrzak, K., Tentes, A.: Commitments and efficient zero-knowledge proofs from learning parity with noise. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 663–680. Springer, Heidelberg (2012). doi:10.1007/978-3-642-34961-4_40
20. Juels, A., Weis, S.A.: Authenticating pervasive devices with human protocols. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 293–308. Springer, Heidelberg (2005). doi:10.1007/11535218_18
21. Katz, J., Shin, J.S.: Parallel and concurrent security of the HB and HB^+ protocols. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 73–87. Springer, Heidelberg (2006). doi:10.1007/11761679_6
22. Kiltz, E., Masny, D., Pietrzak, K.: Simple chosen-ciphertext security from low-noise LPN. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 1–18. Springer, Heidelberg (2014). doi:10.1007/978-3-642-54631-0_1
23. Kiltz, E., Pietrzak, K., Cash, D., Jain, A., Venturi, D.: Efficient authentication from hard learning problems. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 7–26. Springer, Heidelberg (2011). doi:10.1007/978-3-642-20465-4_3
24. Kirchner, P.: Improved generalized birthday attack. Cryptology ePrint Archive, report 2011/377 (2011). http://eprint.iacr.org/2011/377
25. Levieil, É., Fouque, P.-A.: An improved LPN algorithm. In: Prisco, R., Yung, M. (eds.) SCN 2006. LNCS, vol. 4116, pp. 348–359. Springer, Heidelberg (2006). doi:10.1007/11832072_24
26. Lyubashevsky, V.: The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem. In: Chekuri, C., Jansen, K., Rolim, J.D.P., Trevisan, L. (eds.) APPROX/RANDOM -2005. LNCS, vol. 3624, pp. 378–389. Springer, Heidelberg (2005). doi:10.1007/11538462_32
27. Lyubashevsky, V., Masny, D.: Man-in-the-middle secure authentication schemes from LPN and weak PRFs. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8043, pp. 308–325. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40084-1_18

28. May, A., Meurer, A., Thomae, E.: Decoding random linear codes in $\tilde{\mathcal{O}}(2^{0.054n})$. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 107–124. Springer, Heidelberg (2011). doi:10.1007/978-3-642-25385-0_6
29. Pietrzak, K.: Cryptography from learning parity with noise. In: Bieliková, M., Friedrich, G., Gottlob, G., Katzenbeisser, S., Turán, G. (eds.) SOFSEM 2012. LNCS, vol. 7147, pp. 99–114. Springer, Heidelberg (2012). doi:10.1007/978-3-642-27660-6_9
30. 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)
31. Stern, J.: A method for finding codewords of small weight. In: Cohen, G., Wolfmann, J. (eds.) Coding Theory 1988. LNCS, vol. 388, pp. 106–113. Springer, Heidelberg (1989). doi:10.1007/BFb0019850
32. Suttichaya, V., Bhattarakosol, P.: Solving the learning parity with noises open question. Inf. Process. Lett. **113**(14–16), 562–566 (2013)
33. Yu, Y., Zhang, J.: Cryptography with auxiliary input and trapdoor from constant-noise LPN. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 214–243. Springer, Heidelberg (2016). doi:10.1007/978-3-662-53018-4_9