Wiretap Polar Codes in Encryption Schemes Based on Learning with Errors Problem

Aswin Rajagopalan*, Andrew Thangaraj*, Shweta Agrawal†,
*Department of Electrical Engineering, Indian Institute of Technology, Madras
{ee15s053, andrew}@ee.iitm.ac.in
†Department of Computer Science and Engineering, Indian Institute of Technology, Madras
shweta@iitm.ac.in

***Abstract*—The Learning with Errors (LWE) problem has been extensively studied in cryptography due to its strong hardness guarantees, efficiency and expressiveness in constructing advanced cryptographic primitives. In this work, we show that using polar codes in conjunction with LWE-based encryption yields several advantages. To begin, we demonstrate the obvious improvements in the efficiency or rate of information transmission in the LWE-based scheme by leveraging polar coding (with no change in the cryptographic security guarantee). Next, we integrate wiretap polar coding with LWE-based encryption to ensure provable semantic security over a wiretap channel in addition to cryptographic security based on the hardness of LWE. To the best of our knowledge this is the first wiretap code to have cryptographic security guarantees as well. Finally, we study the security of the private key used in LWE-based encryption with wiretap polar coding, and propose a key refresh method using random bits used in wiretap coding. Under a known-plaintext attack, we show that non-vanishing information-theoretic secrecy can be achieved for the key. We believe our approach is at least as interesting as our final results: our work combines cryptography and coding theory in a novel "non blackbox-way" which may be relevant to other scenarios as well.**

I. Introduction

The study of the problem of secure communication, pioneered by Shannon, has received significant attention over the last several decades. Broadly speaking, the two main approaches to this problem are information-theoretic secrecy and cryptography. In the former, there are no assumptions made on the computational power of the adversary, but one must assume that the channel between the legitimate user and adversary suffers more noise than that between the two legitimate users [1]. In the latter, there are no assumptions made on the channel or number of links wiretapped by the adversary, but the adversary is assumed to be computationally bounded.

In this work, we study the possibility of achieving the best of both worlds. In particular, we propose a hybrid scheme which combines the benefits of wiretap polar codes [2] [3] with lattice based cryptography [4]. In more detail, our construction achieves information-theoretic security in wiretap channels with an advantage for the legitimate receiver over the wiretapper and computational security based on the learning with errors (LWE) problem when both the eavesdropper and the legitimate receiver have noiseless channels. The choice of LWE based encryption as the underlying cryptographic scheme is natural in hindsight, due to the structure of the LWE problem. The LWE assumption roughly states that noisy inner products over a finite field are indistinguishable from elements chosen uniformly at random to a computationally bounded adversary. Here, the noise is chosen from a Gaussian-like distribution which composes well with the noise of the wiretap channel. This enables us to analyze the codeword received by the adversary from both an information-theoretic and cryptographic point of view. For more details, we refer the reader to the main body of the paper.

The remainder of the paper is organized as follows. In Section II, we recap the existing wiretap polar coding scheme and encryption scheme using LWE. In Section III, we introduce LWE-based encryption with polar coding and demonstrate its advantages. In Section IV, we integrate wiretap polar coding with LWE-based encryption and provide a scheme that gives computational security over a noiseless channel and information theoretic guarantees over a wiretap channel. In Section V, we analyze the security of the key of our scheme under passive known-plaintext attacks in wiretap channels. We also provide a modified scheme which gives improved information-theoretic guarantees for the security of the key. Section VI includes possible extensions to our work.

II. Preliminaries

In this section we briefly introduce ideas in polar coding used for achieving secrecy capacity in wiretap channels and basic ideas of symmetric key cryptography using Learning With Errors problem. We follow standard notation to let F_q, where q is prime, denote the finite field with q elements, while X^n (and other similar notation) denote length-n vectors.

A. Wiretap channel and security metrics

The wiretap model, shown in Fig. 1, involves two channels $W_1 : X \to Y$ and $W_2 : X \to Z$ [1]. For the purpose of this

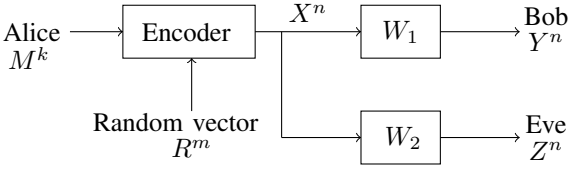

Fig. 1: Wiretap Channel Model

work, we assume that the input and output alphabet of W_1 and W_2 are F_q, i.e., $X, Y, Z \in F_q$. A message $M^k \in F_q^k$ is encoded by Alice to a codeword X^n, typically using a random vector $R^m \in F_q^m$. The legitimate receiver Bob receives Y^n through W_1 and decodes it to an estimate $\hat{M}^k$. Eve receives Z^n through W_2. The goal is to design a coding scheme that ensures probability of decoding error is negligibly small for Bob, i.e., $\Pr\{\hat{M}^k \neq M^k) \to 0$ (reliability), and negligibly small leak of information to Eve, i.e., $I(M^k; Z^n) \to 0$ (strong secrecy).

In [5], the idea of semantic secrecy was extended to the wiretap setting. Formally, semantic secrecy is measured in terms of the metric termed advantage, denoted $\text{Adv}(M^k; Z^n)$, which measures the improvement obtained in estimation of any function of M^k by the use of Z^n maximized over all distributions of M^k [5], [6]. As shown in [5], semantic secrecy and strong secrecy are related as follows:

$$\text{Adv}(M^k; Z^n) \leq \sqrt{2 \ln 2 \max_{P_{M^k}} I(M^k; Z^n)}. \tag{1}$$

From (1), it is clear that schemes that achieve strong secrecy will also achieve semantic secrecy. By s-bit semantic secrecy, we mean that $\text{Adv}(M^k; Z^n) \leq 2^{-s}$. So, the number of bits of semantic secrecy can be computed as

$$s \approx -\frac{1}{2} \log_2 \left(2 \ln 2 \max_{P_{M^k}} I(M^k; Z^n) \right). \tag{2}$$

B. Wiretap polar coding

For a channel $W(y|x)$ with q-ary input $x \in F_q$ and output $y \in \mathcal{Y}$, the Bhattacharya parameter is defined as [7]

$$Z(W) = \frac{1}{q(q-1)} \sum_{x, x' \in F_q, x \neq x'} \sum_{y \in \mathcal{Y}} \sqrt{W(y|x) W(y|x')}.$$

The channel W has capacity, denoted $C(W)$, close to $\log_2 q$ bits per channel use if $Z(W) \approx 0$, and capacity close to 0 if $Z(W) \approx 1$.

For the purposes of polar coding, we assume that W_1 and W_2 are q-ary symmetric channels. Let $n = 2^b$ be a power of 2. As shown in [8], [9], n instances of W_1 and W_2 can be transformed into n q-ary input channels $W_1^{(i)}$ and $W_2^{(i)}$, $1 \leq i \leq n$, which are polarized as either good or bad channels depending on their Bhattacharya parameters $Z(W_1^{(i)})$ and $Z(W_2^{(i)})$. For achieving strong secrecy on the wiretap channel [2], the following definitions of good and bad polarized channels are made using a security function denoted α_n and a parameter $\beta \in [0, 1/2]$:

$$\mathcal{I}(\alpha_n, W_2) = \{i : C(W_2^{(i)}) < \alpha_n\} \ (\alpha_n\text{-poor for Eve}) \tag{3}$$

$$\mathcal{G}(W_1) = \{i : Z(W_1^{(i)}) < 2^{-n^\beta}/n\} \text{ (good for Bob)} \tag{4}$$

$$\mathcal{B}(W_1) = \{i : Z(W_1^{(i)}) \geq 2^{-n^\beta}/n\} \text{ (bad for Bob)} \tag{5}$$

Let $\mathcal{I}_M = \mathcal{I}(\alpha_n, W_2) \cap \mathcal{G}(W_1)$ denote the symbol channels that are both α_n-poor for Eve and good for Bob. Let $\mathcal{I}_R = [n] \setminus \mathcal{I}(\alpha_n, W_2)$ denote the channel indices which are not poor for Eve. We assume that $k = |\mathcal{I}_M|$ and $m = |\mathcal{I}_R|$.

The wiretap polar encoder creates a vector $V^n = [V_1, V_2, \ldots, V_n]$ as follows: (1) message symbols are assigned to indices in $\mathcal{I}_M$, i.e., $V_{\mathcal{I}_M} = M^k$, (2) random symbols are assigned to indices in $\mathcal{I}_R$, i.e., $V_{\mathcal{I}_R} = R^m$, (3) zeros or any other frozen symbols are assigned to the remaining indices in V^n. The codeword is generated $X^n = V^n G_n$, where G_n denotes the polar code generator matrix [8], [9]. The entire wiretap polar encoding process described above is denoted $X^n = WP_n(M^k \| R^m)$.

1) Security: From [2], we have $I(M^k; Z^n) \leq |\mathcal{I}(\alpha_n, W_2)| \alpha_n$. By choosing the security function α_n, we bound the mutual information leaked to Eve for any input distribution of messages, and compute semantic secrecy through (2).

2) Reliability and chaining: Since $\mathcal{B}(W_1) \cap \mathcal{I}_R \neq \phi$ in general, a chaining construction [3] over multiple blocks is needed to ensure reliability. Pick a subset of message indices $\mathcal{I}_E \subset \mathcal{I}_M$ such that $|\mathcal{I}_E| = |\mathcal{B}(W_1) \cap \mathcal{I}_R|$. Random symbols placed in $\mathcal{I}_E$ in the j-th block are used in $\mathcal{B}(W_1) \cap \mathcal{I}_R$ in the $(j+1)$-th block for $j = 1, 2, \ldots$. In the first block, random secret symbols known to both Alice and Bob are used in $\mathcal{B}(W_1) \cap \mathcal{I}_R$.

C. Symmetric key encryption scheme based on LWE

Let q be a prime number, and l, n be such that $q = \text{poly}(l)$ and $n > l \log q$. Let $D_{q,\alpha}$ denote the discrete Gaussian[1] distribution on the integers from $-(q/2-1)$ to $q/2-1$ with standard deviation αq, i.e. $E \sim D_{q,\alpha}$ has PMF $\Pr(E = i) \propto e^{-i^2/2\alpha q}$ for integer i, $-(q-1)/2 \leq i \leq (q-1)/2$. The parameter α is chosen as $1/\text{poly}(l)$ and satisfies $\alpha q > 2\sqrt{l}$.

The LWE problem is to find $S^l \in F_q^l$ given $U^n = (S^l A + E^n) \mod q$, where $A \in F_q^{(l \times n)}$ is uniformly random and $E^n \in F_q^n$ chosen *i.i.d* according to $D_{q,\alpha}$. With parameters chosen as above, it has been shown [10] that solving LWE is at least as hard as solving a shortest vector problem (GAPSVP) in $O(n/\alpha)$ in the worst case. We will use the decisional version of the LWE problem [10], [11] which states that distinguishing an LWE sample from an uniformly random vector is as hard as the search version for a computationally bounded adversary.

Below, we recap a symmetric key encryption scheme based on LWE [4]. Here, S^l plays the role of the shared secret key.
Encryption: n message bits $M^n \in \{0,1\}^n$ are encrypted as

$$Y^n = \frac{(q+1)}{2} M^n + S^l A + E \mod q. \tag{6}$$

Send (A, Y).
Decryption: Using S^l, A and Y^n, compute

$$Y^n - S^l A = \frac{(q+1)}{2} M^n + E \mod q. \tag{7}$$

If $-q/4 \leq (Y_i - S^l A) \leq q/4$, decrypt as $\hat{M}_i = 0$, else $\hat{M}_i = 1$, $1 \leq i \leq n$.

[1] A Gaussian distribution discretized over a lattice, so that non-lattice points have weight zero, and lattice points have weight proportional to a Gaussian. Please see [10] for a formal definition.

Since the distribution of S^lA+E is close to uniform, distribution of Y is also close to uniform. This is the basis for the security of M^n in encryptions based on LWE. The probability of decoding error is upper bounded by the probability that $E \geq q/4$ or $E \leq -q/4$, which can be calculated using the distribution of E.

III. Polar coded LWE

In this section, we will introduce polar coded secret key encryption using LWE. This has similarities to other encryption schemes in [4], [12].

A. LWE channel

The channel induced during the LWE encryption/decryption (see (7)), which we will call the LWE channel, can be described as

$$Y = (X + E) \mod q, \tag{8}$$

where $X \in \{0, 1, \ldots, q-1\}$ is the transmitted symbol, $E \sim D_{q,\alpha}$ is discrete Gaussian and Y is the output symbol. We will denote the LWE channel as W_1 and its transition matrix as $W_1(y|x)$. Since the channel is $\mod q$ addition, it is clear that the rows of $W_1(y|x)$ are permutations of the PMF of E. Therefore, W_1 is symmetric.

Any error-correcting code that is effective over W_1 can be combined with LWE encryption to improve the overall transmission rate. We consider polar codes here because they have been shown to achieve capacity over symmetric channels and have proved to be effective over wiretap channels as well.

B. Polarization of LWE channel

We will consider n instances of the LWE channel W_1, where $n = 2^b$ is a power of 2. After the polarization transform, we obtain n symbol channels $W_1^{(i)}$. A symbol channel is classified as good, if its Bhattacharya parameter $Z(W_1^{(i)})$ satisfies $Z(W_1^{(i)}) \leq 2^{-n^\beta}/n$ (for a parameter β), and classified as bad otherwise. From [7, Theorem 4, Prop 4], we have

$$Z(W^{(2i)}) = Z(W^{(i)})^2, \tag{9}$$

$$Z(W^{(2i-1)}) \leq \min\{q\, Z(W^{(i)}), \\ 2Z(W^{(i)}) + (q-1)Z(W^{(i)})^2\}. \tag{10}$$

Using these relations recursively, we can evaluate upper bounds on $Z(W_1^{(i)})$ for each i. Using these upper bounds, the symbol channels are classified as good. Though working with upper bounds reduces rate, this appears to be the best-known procedure currently for q-ary channels.

We denote the good and bad channels as $\mathcal{G}(W_1)$ and $\mathcal{B}(W_1)$, respectively. Further, let $k = |\mathcal{G}(W_1)|$ be the number of good channels.

C. Polar-coded encryption and decryption

Generate parameters and matrices as per LWE encryption in Section II-C. Let G_n denote the generator matrix for the polar code [8].

Encryption: To encrypt a message $M^k \in F_q^k$, we generate a vector U^n by mapping the message M^k to the good channel indices $\mathcal{G}(W_1)$ and setting the bad channel indices $\mathcal{B}(W_1)$ to frozen symbols known to both Alice and Bob. Compute

$$Y^n = U^nG_n + S^lA + E^n \mod q.$$

Send (A, Y^n).

Decryption: Using S^l, A and Y^n, compute

$$Y^n - S^lA = U^nG_n + E^n \mod q.$$

Run the successive cancellation decoding algorithm of the polar code [8] to decode M^k.

Security: Assume there exists an algorithm which can distinguish $U^nG_n + S^lA + E^n \mod q$ from an uniformly random vector from F_q^n. Then, from [10, Lemma 4.2], there exists an efficient algorithm to find M^k and S^l by solving the search LWE problem in a lattice, which is the union of lattices defined by the rows of matrices A and G_n. So, breaking polar-coded LWE is at least as hard as solving an LWE problem.

Reliablity: Probability of block error of the q-ary polar code is upper bounded by 2^{-n^β} [7], which is small for suitably large values of n.

D. Transmission rate vs decoding error probability

A gain in transmission rate or decoding error probability is to be expected when any error-correction code is introduced. We will compare uncoded LWE and polar-coded LWE for varying values of $q\alpha$, the standard deviation of the error E.

Uncoded: The rate of transmission of LWE (Section II-C) without any coding is seen to be 1 bit per channel use for all values of $q\alpha$. The decoding error probability varies with $q\alpha$, and is upper bounded as $n\Pr(E \notin [-q/4, q/4])$.

Polar-coded: For polar-coded LWE, the rate is $\frac{|\mathcal{G}(W_1)|}{n} \log_2 q$ bits per channel use and the the decoding error probability is upper bounded by 2^{-n^β}. Hence, multiple rates and decoding error probabilities are possible by varying the parameter β at the same value of $q\alpha$.

Fig. 2 shows a plot of the upper bound on decoding error probability versus rate of transmission for $n = 8192$ and $q = 127$ with different values of $q\alpha$. We observe that variation of β provides useful tradeoffs between decoding error probability and rate of transmission. At $q\alpha = 4$, more than two times the rate of uncoded transmission is possible at the same decoding error probability.

IV. Wiretap-coded LWE-based encryption

In this section, we consider the use of LWE-based encryption over the wiretap channel model as shown in Fig. 1. The main channel W_1 is the LWE channel from Section III. The wiretapper's channel W_2 is assumed to be weaker with respect to W_1 (for instance, W_2 could be degraded with

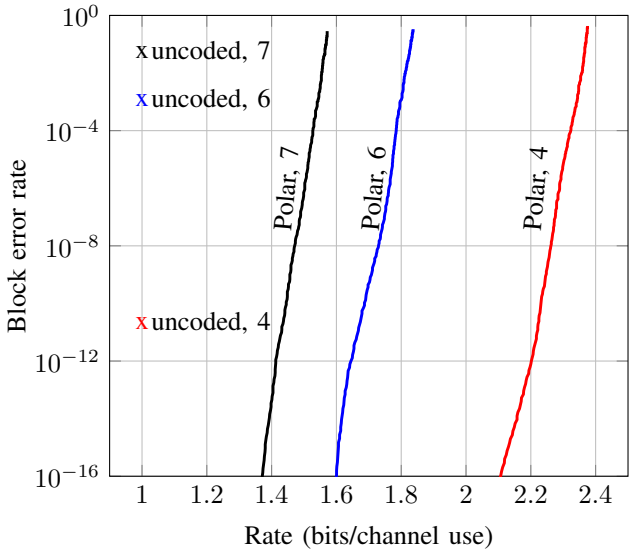

Fig. 2: Decoding error vs rate, $n = 8192$, $q = 127$, β varied from 0.2 to 0.49. The value of $q\alpha$ is shown next to plot.

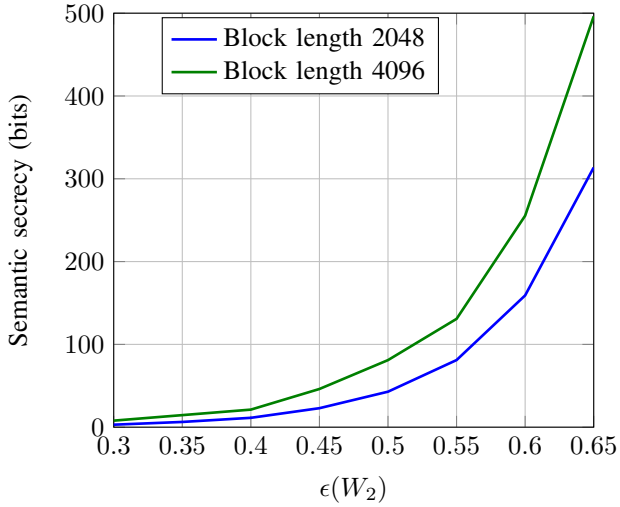

Fig. 3: Semantic secrecy for wiretap polar code.

respect to W_1), so that a wiretap polar code (see Section II-B) can be constructed with positive rate. Our goal is to design a coding/encryption scheme with quantifiable semantic secrecy when W_2 is a weaker wiretapper's channel, while retaining LWE-based cryptographic security always.

Encryption: Construct the wiretap polar code as in Section II-B. Select parameters, vectors and matrices as per LWE encryption in Section II-C. Compute

$$Y^n = WP_n(M^k \| R^m) + S^l A + E^n \mod q. \tag{11}$$

Send (A, Y^n). Use suitable block chaining for polar wiretap coding as described in Section II-B.

Decryption: Decode M^k from $Y^n - S^l A$ using the wiretap polar code.

The LWE-based security is clear from the construction. However, it is interesting to consider the security of M^k over a wiretap channel.

A. Semantic secrecy over wiretap channel

In this subsection, we will assume that W_2 has a q-ary output alphabet, is symmetric and degraded with respect to W_1. Based on this assumption, we quantify the semantic secrecy for a fixed value of security function α_n. An important remark here is that, for secrecy over wiretap channel, we do not require the secret key S^l and will assume that it is known to the eavesdropper.

The computation of semantic secrecy is simple if W_2 is degraded with respect to a q-ary erasure channel with erasure probability ϵ, denoted W_ϵ, which has the transition matrix $\Pr(y = u|x = u) = 1 - \epsilon$, $\Pr(y = e|x = u) = \epsilon$ for $u \in \{0, 1, \ldots, q-1\}$. The following lemma is easy to establish and we skip the short proof.

Lemma 1. *A symmetric q-ary channel W is degraded with respect to the q-ary erasure channel $W_{\epsilon(W)}$ with erasure probability $\epsilon(W) = qw_{\min}$, where $w_{\min}$ is the minimum element in any row of the transition matrix $W(y|x)$.*

Using Lemma 1, we have

$$|\mathcal{I}(W_2, \alpha_n)| \leq |\mathcal{I}(W_{\epsilon(W_2)}, \alpha_n)|. \tag{12}$$

The RHS above can be computed using the following relationships that apply to the symbol channels of a q-ary erasure channel, denoted $W_\epsilon^{(i)}$, when q is prime [8], [9].

$$Z(W_\epsilon^{(2j-1)}) = 2Z(W_\epsilon^{(j)}) - Z(W_\epsilon^{(j)})^2, \tag{13}$$

$$Z(W_\epsilon^{(2j)}) = Z(W_\epsilon^{(j)})^2, \tag{14}$$

$$C(W_\epsilon^{(i)}) = 1 - Z(W_\epsilon^{(i)}), \tag{15}$$

where $C(W_\epsilon^{(i)})$ is the capacity of the i-th symbol channel. It is shown in [2, Propostion 16] that the information leaked to the eavesdropper is upper bounded by the sum of the bit channel capacities of the α_n poor channels of Eve. Using this result and (12), we can compute the following bound:

$$I(M^k; Z^n) \leq \alpha_n |\mathcal{I}(W_{\epsilon(W_2)}, \alpha_n)|. \tag{16}$$

Now, we can use (1) and (2) to calculate the number of bits of semantic secrecy. Fig. 3 shows the computed semantic secrecy versus $\epsilon(W_2)$ for $n = 4096$ and $n = 2048$ with $q = 113$. For each ϵ, the value of α_n was chosen so that there are 500 good symbol channels for $n = 4096$ and 300 good symbol channels for $n = 2048$.

B. Worst-case $\epsilon(W_2)$ for a fixed W_1 and secrecy capacity

Since $\epsilon(W_2)$ quantifies the information leaked to the eavesdropper, it is interesting to characterize the least $\epsilon(W_2)$ (leaks the most information) over all W_2 that are degraded with respect to W_1 (denoted $W_2 \preceq W_1$) and achieve a secrecy capacity of $C_s = C(W_1) - C(W_2)$. The worst-case $\epsilon(W_2)$ is

actually a function of W_1 alone and can be written down as follows:

$$\epsilon^*(W_1) = \min_{\substack{W_2 \preceq W_1 \\ C(W_2)=C(W_1)-C_s}} \epsilon(W_2)$$

The distribution of the error E determines W_1. While the choice of discrete Gaussian is justified in certain cryptographic reductions, the choice remains unclear in the wiretap scenario. One possible method to choose W_1 and the distribution of E is to maximize the worst-case $\epsilon(W_2)$. In other words, choose W_1 as $W_1 = \arg\max \epsilon^*(W_1)$.

As of now, this problem remains as future work.

V. Security of key and key refresh

In this section, we consider a passive, known-plaintext attack, where the attacker knows M^k and is interested in learning the secret private key S^l. Note that the attacker receives the exact ciphertext with no noise (i.e., there is no wiretap channel). By learning S^l, an attacker breaks all subsequent encryptions. So, a known-plaintext attack on the key is important to study. In [13], information-theoretic security of the secret key in a class of randomized encryption schemes was shown to reduce with the number of transmissions.

One of the advantages of wiretap polar coding is that it allows for refresh of key with information-theoretic guarantees on the security of the key. The encryption step in wiretap-coded LWE with key refresh is as follows. Assume the length of the secret $l = m < |\mathcal{I}_M|+|\mathcal{I}_R|$, and the length of the message $k = |\mathcal{I}_M|+|\mathcal{I}_R|-l$.

Encryption: Pick $\mathcal{I}'_M \subseteq \mathcal{I}_M$ such that $|\mathcal{I}'_M| = k$. The message M^k is assigned to symbol channel indices in $\mathcal{I}'_M$. Pick $\mathcal{I}'_R = (\mathcal{I}_M \setminus \mathcal{I}'_M) \cup \mathcal{I}_R$. The random vector R^m is assigned to symbol channel indices in $\mathcal{I}'_R$. Zeros or frozen symbols are assigned to remaining symbol channel indices. Compute

$$Y^n = WP_n(M^k \| R^m) + S^l A + E^n \mod q. \tag{17}$$

Send (Y^n, A). Set $S^l = R^m$ for the next block.

The decryption process is obvious here, except for requirement of the chaining construction to decode random bits in bad indices for Bob, which has been skipped to keep the description simple.

In the theorem which follows, we present a non-vanishing lower bound on the equivocation of the key to a known-plaintext attacker. Let S_i^l denote the LWE secret key in the i-th round, and let $S_{1:\mu}^l = S_1^l, S_2^l, \ldots, S_\mu^l$ be the collection of secret keys over μ rounds. Let $M_{1:\mu}^k$, $R_{1:\mu}^m$, $A_{1:\mu}$, $E_{1:\mu}^n$ and $Y_{1:\mu}^n$ be similar collections of message bits, random vectors, matrices, error vectors and received symbols over μ rounds.

Theorem 1.

$$H(S_i^l \mid M_{1:\mu}^k, A_{1:\mu}, Y_{1:\mu}^n) = c > 0,$$

where

$$c = H(R_1^m \mid M_{1:2}^k, A_{1:2}, Y_{1:2}^n) + H(E_1^n \mid M_1^k, R_1^m, A_1, Y_1^n) - \lim_{\eta \to 0+} \left(H(\eta) + \eta \log(q^{m\mu+l} - 1) \right).$$

Proof. The proof uses ideas from [13] along with the use of the properties of wiretap polar coding. We skip the details of the proof for want of space. □

Theorem 1 is to be contrasted with the results in [13], where the security of the key is shown to go to zero for a class of randomized encryption schemes. In this case, the nonzero equivocation is because of the refresh of the key.

VI. Conclusion

In this paper, we combined polar codes with LWE-based encryption methods to design encryption schemes that offer both semantic secrecy in wiretap channel and computational security in noiseless channel. We have also calculated the semantic secrecy metric of the designed wiretap-LWE encryption scheme assuming degradation with respect to a suitable erasure channel. Then, we derived information-theoretic guarantees of the key under passive known plaintext attacks and suggested a key refresh method using random bits of wiretap polar encoding to give nonvanishing information-theoretic guarantees for the key.

References

[1] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, Oct 2011.

[3] E. Şaşoğlu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*. IEEE, 2013, pp. 1117–1121.

[4] O. Regev, "The learning with errors problem (invited survey)," in *2010 IEEE 25th Annual Conference on Computational Complexity*, June 2010, pp. 191–204.

[5] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO)*. Springer, 2012, pp. 294–311.

[6] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct 2015.

[7] E. Şaşoğlu, E. Telatar, and E. Arikan, "Polarization for arbitrary discrete memoryless channels," in *Information Theory Workshop, 2009. ITW 2009. IEEE*. IEEE, 2009, pp. 144–148.

[8] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[9] E. Şaşoğlu, "Polarization and polar codes," *Foundations and Trends in Communications and Information Theory*, vol. 8, no. 4, pp. 259–381, 2012. [Online]. Available: http://dx.doi.org/10.1561/0100000041

[10] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, pp. 34:1–34:40, Sep. 2009. [Online]. Available: http://doi.acm.org/10.1145/1568318.1568324

[11] D. Micciancio and C. Peikert, "Trapdoors for lattices: Simpler, tighter, faster, smaller," Cryptology ePrint Archive, Report 2011/501, 2011, https://eprint.iacr.org/2011/501.

[12] H. Gilbert, M. J. B. Robshaw, and Y. Seurin, *How to Encrypt with the LPN Problem*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 679–690. [Online]. Available: https://doi.org/10.1007/978-3-540-70583-3_55

[13] F. Oggier and M. J. Mihaljevic, "An information-theoretic security evaluation of a class of randomized encryption schemes," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 158–168, 2014.