Abstract—In this paper, we use the hardness of quantization over general lattices as the basis of developing a physical layer secrecy system. Assuming that the channel state observed by the legitimate receiver and the eavesdropper are distinct, this asymmetry is used to develop a cryptosystem that resembles the McEliece cryptosystem, designed to be implemented at the physical layer. We ensure that the legitimate receiver observes a specific lattice over which decoding is known to be possible in polynomial-time, while the eavesdropper observes a lattice over which decoding will prove to have the complexity of lattice quantization over a general lattice.

I. INTRODUCTION

Security is and will remain one of the primary design requirements in any communication system. Depending on the nature of security desired, there are multiple means by which secure communication is enabled [5], [6]. An increasingly important means of securing communication is by exploiting asymmetries (between the legitimate pair and the wiretapper) at the physical layer. There are many schemes already in existence designed to enable physical layer security [2], [5]. In general, there are two settings in which physical layer security is conventionally studied: information-theoretic and computational.

From the information-theoretic perspective, the Wyner wiretap model is the arguably one of the best studied secure-communication models [2]. In this setting, the legitimate transmitter (Alice) wishes to communicate a message \( W \) to a legitimate receiver (Bob) through a noisy channel. An eavesdropper (Eve) is present that can overhear the communication through another noisy medium. This wiretap model is depicted in Figure 1. The notion of secrecy employed here is that of perfect secrecy, i.e., the eavesdropper is not assumed to be computationally bounded and we desire that there is absolutely no leakage of information. However, the results obtained using the Wyner wiretap model can be fairly pessimistic - if the wiretapper has a “better” channel than the legitimate receiver, the capacity of this model is zero.

Given the stringent nature of the information-theoretic perfect secrecy, the notion of computational secrecy (which forms the basis of many cryptosystems) has received significant attention [6]. Computational secrecy aims to create a computational asymmetry in the system, enabling the legitimate receiver to determine the message at low complexity while ensuring that it is exponentially complex for the eavesdropper to do so. Indeed, a large number of secure systems deployed today use a cryptosystem based on computational asymmetry. However, a majority of these cryptosystems operate at layers higher than the physical layer. Although mechanisms for exploiting the physical layer for computational secrecy have been studied ([7] and references therein), a not-so-uncommon mindset is to use cryptosystems at higher layers and to assume that perfect-secrecy is only relevant the physical layer.

In this paper, we utilize channel-asymmetry in enabling computational secrecy at the physical layer using lattices. Our approach is similar to that of a McEliece cryptosystem. A McEliece cryptosystem is based on the difficulty of syndrome decoding for a general linear codes, which is known to be NP hard [4]. However, decoding of particular classes of codes (such as BCH or Goppa) is known to be possible with low complexity. Thus, a McEliece cryptosystem is designed so that the legitimate receiver observes a very specific code while the eavesdropper is faced with a general linear code. The McEliece cryptosystem, however, does not use channel asymmetry as its basis, and requires key exchanges making it is a higher (network or application)-layer cryptosystem. This paper, we build a cryptosystem that does not require key exchanges and is designed to operate at the physical layer. We use lattices and the fact that lattice decoding of a general lattice is NP-hard [8] to build this physical-layer cryptosystem. Indeed, the shortest vector problem (SVP) in lattices has already been used to develop cryptosystems [9]. However, these cryptosystems typically operate at higher layers, and it is our goal to bring this to the physical layer. In short, the main idea is to encode Alice’s transmission such that Bob observes a lattice that is easy to decode while Eve observes a general lattice over which lattice quantization is exponentially hard.

Lattices for communication over additive Gaussian noise (AGN) channels have already been studied in detail [10]. Elements from the ensemble of Construction-A lattices [11] have been shown to be optimal for the AGN channel [13], [14]. However, general Construction-A lattices do not lend themselves to low complexity encoding and decoding algorithms. Thus, specific lattice structures are now being studied to enable lattice-based communication. One such effort is the design of low density lattice codes (LDLCs) [15], while another is a specific structured design of block-triangular Construction-A

1This work was supported in part by a Brazilian national fellowship.
lattices \[ [12]. \] In this paper, we use one of these specific lattices as the communication lattice to the legitimate receiver (Bob), and “scrambling” it so a general lattice is observed at the eavesdropper.

Fig. 1. The channel model: \( X \) is the legitimate source while \( Y_B \) is the signal observed by the legitimate receiver. \( Y_E \) is observed by the eavesdropper.

The rest of this paper is structured as follows: the next section presents the system model. Section II-B summarizes some lattice preliminaries. In Section III, we present two mechanisms for lattice-based computational secrecy - the first based on simple channel inversion and the second on channel diagonalization and inverse water-filling. Section IV describes a particular lattice construction based on a block-lower-triangular scheme as presented in \[ [12], \] while Section V concludes the paper.

II. SYSTEM MODEL

A quick note on notation. For a matrix \( H \), \( H^{-1} \) denotes its inverse and \( H^T \) its transpose. \( X^n \) denotes an \( n \times 1 \) vector. Oftentimes, the vector \( X^n \) is abbreviated as \( X \).

As mentioned in the introduction, the Wyner wiretap model is considered in this paper. There is one transmitter, Alice, that wishes to communicate with Bob. Eve is a wiretapper that must be denied access to the information being transmitted. The channel is an intersymbol interference (ISI) channel that can be written in matrix form as

\[
Y_B = HX + N_B
\]

where \( G \) is an \( n \times n \) matrix that is independently generated and thus distinct from \( H \). To make this notion of independence precise, a special case would be the case where the entries of both \( H \) and \( G \) are drawn i.i.d. over a suitable distribution.

A. Assumptions

The main assumption is that the transmitter and legitimate receiver know the channel transformation \( H \). The fact that \( H \) and \( G \) are two different matrices is the main asymmetry being used in this design. \( H \) can be estimated in a wireless time division duplex (TDD) setting by both the sender and receiver. In a frequency division duplex (FDD) setting, a feedback mechanism is needed to ensure that the channel estimate is available to the transmitter. A couple of points:

1) \( G \) is not assumed to be known to either Alice or Bob. Even the presence of an eavesdropper need not be known to the legitimate pair. It suffices that \( G \) and \( H \) be “sufficiently” different.

2) The channel state of the legitimate pair \( H \) can be known to the eavesdropper, and even then the secrecy results obtained are meaningful.

B. Lattice Preliminaries

A lattice \( \Lambda \) is a collection of vectors in \( \mathbb{R}^n \), of the form:

\[
\Lambda = \{ \lambda = Gx, x \in \mathbb{Z}^n \}
\]

where \( \mathbb{Z}^n \) is the integer lattice, a collection of all integers vectors of length \( n \) and \( G \) is an \( n \times n \) real-valued matrix. Let \( \Omega \) denotes the fundamental Voronoi region of the lattice \( \Lambda \) and \( \mathbb{V} \) denotes the volume of \( \Omega \). There are two figures of merits for lattice: The volume to noise ratio (VNR) and the normalized second moment (NSM), whose definitions can be found in \[ [10]. \] The VNR measures a lattices suitability for communication over AGN channels, while the NSM the same for compression of Gaussian sources with a squared distortion measure. Overall, “good” lattices with respect to both VNR and NSM are known to exist. These “good” lattices, are also known to achieve the capacity of an additive Gaussian noise (AGN) channel are known to exist \[ [14]. \]

Next, we proceed to describing the physical-layer lattice based cryptosystem envisioned in this paper. The lattices used for communication may or may not be “good” for source or channel coding. They will, however, be structured to ensure efficient decoding and the legitimate receiver while making decoding at the eavesdropper difficult.

III. LATTICE-BASED CRYPTOGRAPHY

The design of a lattice based cryptosystem can be attained in a fairly straightforward manner, along the same lines as the McEliece cryptosystem.

A. Channel Inversion

The simplest construction is when the matrix \( H \) is invertible. In this construction, if \( \Lambda \) is a lattice that enables low complexity encoding and decoding at the legitimate pair. Then, the following policy is used:

\[
Y_E = GX + N_E
\]

\(^2\)This paper utilizes the time-varying/ISI nature of the medium, and the arguments do not hold if it is a constant channel.
Encoding: map message \( m \) to a lattice point \( \lambda \in \Lambda \). This is possible due to the low-complexity nature of encoding associated with \( \Lambda \).

Transmission: Alice communicates

\[
X = CH^{-1}\lambda
\]

where \( C \) is a suitable normalization constant so that the power constraint at the transmitter is met.

Decoding: Bob observes \( Y^n_B = C\lambda + N^n_B \). Given the structure of \( \Lambda \), decoding this to recover \( \lambda \) and thus the message \( m \) is possible with polynomial complexity.

Eavesdropper: The eavesdropper observes:

\[
Y^n_E = CGH^{-1}\lambda + N^n_E
\]

If \( G \) and \( H \) are independently generated with i.i.d. entries over a continuous valued distribution, it is easy to verify that the probability that \( GH^{-1} \) is a unitary matrix goes to zero as \( n \to \infty \). This implies that the new lattice \( GH^{-1}\lambda \) no longer has the desired low-complexity structure and thus cannot be decoded using polynomial-time algorithms. Note that, if \( H \) is unknown to the eavesdropper, decoding is particularly difficult. Even if \( H \) is known to the eavesdropper and \( G \) is invertible, the eavesdropper can construct:

\[
HG^{-1}Y^n_E = C\lambda + HG^{-1}N^n_E
\]

Given that \( HG^{-1} \) is not unitary, such a transformation would result in correlated noise at the eavesdropper with covariance \( G^{-1}H^HHG^{-1} \), which is not a scaled version of an identity matrix. As the lattice \( \Lambda \)'s Voronoi region is designed to be decodable in the presence of white noise, decoding will fail at the eavesdropper.

B. SVD and Inverse Water-filling

In general, however, \( H \) may not be an invertible matrix. Moreover, channel inversion at the transmission is not a good strategy in a communication system as it lowers the rates that can be supported by the medium. A strategy that is somewhat less naïve is presented next:

Assuming the singular value decomposition (SVD) of the channel matrix is given by:

\[
H = UDV
\]

where \( U \) and \( V \) are \( n \times n \) unitary matrices and \( D \) is a diagonal matrix comprised of its singular values. We assume the diagonal values in \( D \) are arranged in decreasing order. Given this, we can rewrite the received signal at Bob as:

\[
Y^n_B = UDVX^n + N^n_E
\]

through suitable unitary transformations, we can obtain:

\[
\tilde{Y}^n_B = U'Y^n_B = D\tilde{X}^n + N^n_E
\]

where \( \tilde{X}^n = VX^n \). This process effectively diagonalizing the legitimate channel. If we define a minimum threshold for the channel gain \( t \) below which communication is feasible, then \( D \) can be subdivided into the following form:

\[
D = \begin{bmatrix} D_1 & 0 \\ 0 & \hat{D} \end{bmatrix}
\]

where \( \hat{D} \) comprises of channel gains that are less than or equal to \( t \). If \( \hat{D} \) is a \( k \times k \) matrix, then it is desirable that only \( k \) dimensions be used for communication. A traditional wireless/multiple antenna communication system would treat these \( k \) dimensions as independent parallel channels and waterfill across them [16]. This approach is known to be optimal, but the lattice-based secrecy benefits of such a scheme are unclear. Instead, using the \( k \) parallel dimensions to communicate a lattice vector makes them dependent. This dependence need not always result in a lower rate, but it can lead to the physical-layer lattice cryptosystem studied in this paper.

Encoding: A \( k \)-dimensional lattice point encoded using a lattice which permits low-complexity encoding and decoding is now used to communicate over the legitimate channel. This \( k \) dimensional lattice can be obtained by truncating an existing \( n \) dimensional lattice construction. This lattice point is then enhanced to \( n \) dimensions by zero padding. This zero padded lattice point is denoted by \( \hat{\lambda} \).

Transmission: Alice transmits

\[
X = CV^t\hat{D}^{-1}\hat{\lambda}.
\]

Here, \( \hat{D}^{-1} \) equals

\[
\hat{D}^{-1} = \begin{bmatrix} D_1^{-1} & 0 \\ 0 & 0 \end{bmatrix}
\]

and \( C \) is the power normalization constant. Note that this is, in essence, truncated inverse water-filling. Such a scheme is definitely not optimal from the perspective of maximizing rate for the legitimate channel. However, it ensures that the structural properties of the lattice are maintained as it is communicated across the legitimate channel.

Reception: Bob first constructs \( \tilde{Y}^n_B \) from \( Y^n_B \) by multiplying \( U^t \), and then uses the first \( k \) positions to determine the \( k \)-dimensional lattice point being communicated. As the lattice admits a low complexity decoding algorithm and is structured to handle i.i.d. Gaussian noise, this decoding is successful with high probability.

Eavesdropper: The eavesdropper, as before, observes a general lattice given by:

\[
Y^n_E = CGV^t\hat{D}^{-1}\hat{\lambda} + N^n_E
\]

with no particular relationship between \( H \) and \( G \), this lattice is a general one. Even the knowledge of the encoding strategy and \( H \) does not help, as any linear processing will result in colored noise at the receiver.

Note that both the schemes presented here relied on the assumption that neither \( H \) nor \( G \) are a multiple of identity, i.e. constant channels. In essence, channel variation and inter-symbol interference are being used to instill an asymmetry between the legitimate receiver and eavesdropper, which is essential to the analysis. Moreover, this analysis lends itself naturally to multiple antenna channels as well. In the multiple antenna context, both static and varying channels are of interest, and this scheme is applicable to either of these settings.
IV. CONSTRUCTION OF LATTICES THAT PERMIT EFFICIENT ENCODING AND DECODING

As mentioned earlier, the family of low density lattice codes (LDLCs) in [15] is one example of lattices that can be used for this lattice-based cryptosystem. Here, we summarize an alternate scheme developed in [12]. Note that this serves as a summary of the unpublished work in [12] only, and is not an original contribution by the authors of this paper.

This construction of the class of lattices in [12] is based on the Construction-A framework [11]. The ensemble of Construction-A lattices is known to contain lattices that are good for source and channel coding [10]. Hence, this class of lattices is of particular interest to us. Unfortunately, a randomly chosen Construction-A lattice does not afford either low-complexity encoding or decoding. Thus, a specific construction is required to enable low complexity processing.

In general, Construction-A lattices are of the form:

\[ \Lambda = p^{-1} G \mathbb{Z}_p^k + \mathbb{Z}^n \]

where \( G \) is an \( n \times k \) “generator” matrix, \( \mathbb{Z}_p^k \) is the set of all \( k \)-length vectors modulo \( p \) and the multiplication between \( G \) and \( \mathbb{Z}_p^k \) is defined modulo \( p \). All other operations are over the real field.

This construction is based on the understanding that a short block length is sufficient for realizing shaping gain, while longer block lengths are required to achieve coding gain. Thus, the Construction-A parity check matrix for this lattice is structured as follows:

\[ F = \begin{bmatrix} K & 0 & \ldots & 0 \\ A_{21} & K & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ A_{11} & A_{12} & \ldots & K \end{bmatrix} \]

In short, the parity-check matrix is chosen to be block lower triangular. Here \( K \) is a suitable “small” parity check matrix that provides shaping gain. For example, it could be the parity check matrix corresponding to the Leech lattice, or one corresponding to a low-density generator matrix (LDGM) code. Its sole purpose is to enable, within a dimension of a few tens, for much of the shaping gain to be captured. \( A_{ij} \) are, on the other hand, chosen to be matrices such that the overall parity check matrix \( F \) is “good” from the perspective of coding gain.

Encoding for this lattice proceeds as follows: a vector \( X \) is determined that solves the equation

\[ FX = \begin{bmatrix} 0 \\ m \end{bmatrix} \]

where \( m \) is the message to be communicated. Note that this encoding procedure can result in multiple solutions for \( X \) in \( \mathbb{R}^n \). Thus, our interest is in determining that solution which is closest to the origin. In general, solving for a vector closest to the origin in a lattice is an NP-hard problem. However, given the structure of the lattice, this can be solved recursively. By breaking \( X \) into \( l \) parts:

\[ X^t = [X_1^t \ X_2^t \ \ldots \ X_l^t] \]

and solving consecutive equations of the form:

\[ KX_i = \begin{bmatrix} 0 \\ m_i \end{bmatrix} \]

where the closest vector problem is now reduced to one over a much smaller scale than the original problem.

Decoding proceeds using conventional mechanisms in nonbinary low density parity check (LDPC) codes. If \( A_{ij} \) are chosen in a manner to render the code a good LDPC, a belief propagation algorithm can be used for decoding.

This concludes the summary of this particular construction. Multiple other constructions exist and are being actively researched to enable lattice-based communication, and such constructions can be used in this cryptosystem as well as non-trivial linearly transformed versions of these lattices result in general lattices over which decoding is hard.

V. CONCLUSION

This paper builds a physical-layer based cryptosystem using the hardness of lattice quantization of generalized lattices. This scheme uses no key, either public or private. It uses the channel channel asymmetry between the legitimate pair and the eavesdropper in developing the scheme. Although analytically simple in design, this scheme is a natural application of lattices to both communication and secrecy.

VI. ACKNOWLEDGMENT

We thank Ankit Ghiya, Sang Hyun Lee, Krishna Narayanan and Henry Pfister for their work on constructing block lower-triangular Construction-A lattices.

REFERENCES

[1] T. Cover and J. Thomas, “Elements of Information Theory”. Springer, 1991.
[2] A. D. Wyner, “The wiretap channel”. Bell System Technical Journal, 1975.
[3] A. Shamir, “Identity-based cryptosystems and signature schemes”. Advances in Cryptology, Lecture notes in Computer Science, 1985.
[4] R. J. McEliece, “A public-key cryptosystem based on algebraic coding theory”, DSN Progress Report, 1978.
[5] Y. Liang, H. V. Poor and S. Shamai, “Information theoretic security”, Foundations and Trends in Communications, NOW Publishers, 2009.
[6] M. Y. Rhee, “Cryptography and secure communications”, McGraw Hill, New York, 1993.
[7] M. Debbah, H. El Gamal, H. V. Poor and S. Shamai (Shitz), “Wireless physical layer security”, EURASIP Journal on Wireless Communications and Networking, 2009.
[8] D. Micciancio and S. Goldwasser, “Complexity of lattice problems”, Springer, 2002.
[9] Chris Peikert, “Public-key cryptosystems from the worst-case shortest vector problem”, in Proceedings of the 41st annual ACM symposium on Theory of computing, 2009.
[10] R. Zamir, “Lattices are everywhere”, Proc. ITA workshop, 2009.
[11] J. H. Conway and N. J. A. Sloane, “Sphere packings, lattices and groups”, Springer, 1988.
[12] A. Ghiya, S. Lee, K. Narayanan, H. Pfister and S. Vishwanath, “Low density Construction-A lattices”, preprint.
[13] R. Urbanke, B. Rimoldi, “Lattice codes can achieve capacity on the AWGN channel”, IEEE Transactions on Information Theory, 1995.
[14] U. Erez and R. Zamir, “Achieving 0.5 log(1 + SNR) over the additive white Gaussian noise channel with lattice encoding and decoding”, IEEE Transactions on Information Theory, 2004.
[15] N. Sommer and M. Feder and O. Shalvi, “Low density lattice codes”, Proceedings of the IEEE International Symposium on Information Theory 2006.
[16] A. Goldsmith, “Wireless Communications”, Cambridge University Press, 2005.