Secure Computation in a Bidirectional Relay

Navin Kashyap and Shashank V
Dept. of Electrical Communication Engineering
Indian Institute of Science, Bangalore, India
Email: {nkashyap,shashank}@ece.iisc.ernet.in

Andrew Thangaraj
Dept. of Electrical Engineering
Indian Institute of Technology, Madras, India
Email: andrew@ee.iitm.ac.in

***Abstract*—Bidirectional relaying, where a relay helps two user nodes to exchange equal length binary messages, has been an active area of recent research. A popular strategy involves a modified Gaussian MAC, where the relay decodes the XOR of the two messages using the naturally-occurring sum of symbols simultaneously transmitted by user nodes. In this work, we consider the Gaussian MAC in bidirectional relaying with an additional secrecy constraint for protection against a *honest but curious* relay. The constraint is that, while the relay should decode the XOR, it should be fully ignorant of the individual messages of the users. We exploit the symbol addition that occurs in a Gaussian MAC to design explicit strategies that achieve perfect independence between the received symbols and individual transmitted messages. Our results actually hold for a more general scenario where the messages at the two user nodes come from a finite Abelian group G, and the relay must decode the sum within G of the two messages. We provide a lattice coding strategy and study optimal rate versus average power trade-offs for asymptotically large dimensions.**

I. Introduction

A communication device or node, denoted R, is said to act as a relay between two other nodes, denoted A and B, if R facilitates communications from A to B by receiving messages from A and forwarding them to B. The relay R is said to be bidirectional if it additionally facilitates communications from B to A in the reverse direction. We will suppose that A, B and R are wireless communication nodes that are half-duplex (cannot transmit and receive simultaneously), and that A and B are not connected directly. Further, we will assume that all links between nodes are Gaussian channels. In such settings, bidirectional relaying typically happens in two phases: (1) (Gaussian) MAC phase, where A and B transmit to R, and (2) Broadcast phase, where R transmits to A and B. Two-phase bidirectional relaying has been extensively studied in the recent literature [1], [2], [3].

In the MAC phase, suppose that bits X and Y are modulated by A and B (independently at some common time) into real-valued transmitted symbols denoted by random variables U and V, respectively. Then, the relay will receive an instance of a random variable W, which can be modeled as

$$W = U + V + Z, \tag{1}$$

where we have assumed that the links A $\rightarrow$ R and B $\rightarrow$ R have unit gain (normalized), and Z denotes additive noise independent of U and V. An important departure from the standard Gaussian MAC is that the bidirectional relay R need not decode both the bits X and Y. Instead, it is sufficient to decode the eXclusive OR (XOR) $X \oplus Y$, and broadcast the XOR to A and B in the broadcast phase. This strategy, known as XOR coding, has been suggested and used by several authors, and has been generalized to the notion of physical layer network coding in [4], [5].

In this work, we consider the secure XOR-coded bidirectional relay scenario, where A and B intend that R decodes the XOR $X \oplus Y$ in the MAC phase, but remains completely ignorant of both the individual bits X and Y. In fact, we consider a more general scenario where X, Y take values in a finite Abelian group G, for example, a binary linear code. In the MAC phase, the relay R must be able to decode $X \oplus Y$, where $\oplus$ is now the group operation within G, while getting no information about the individual values of X and Y.

We design explicit randomized modulation strategies at the nodes A and B for achieving the objectives of perfect security of the individual messages X, Y, and correct decoding of their sum $X \oplus Y$ at the relay R in the Gaussian MAC phase. Interestingly, we achieve perfect security using the addition operation of U and V in (1), and this is an important novel contribution of our work. The tools used for achieving the objective of perfect security are characteristic functions and the Poisson summation formula from probability theory and Fourier analysis. For the noisy case, we provide a coding scheme based on nested lattice codes for perfectly secure and reliable group computation.

Security against an eavesdropping two-way or bidirectional relay was considered in [6] using friendly jammers that create a wiretap channel. Lattice codes have been proposed for Gaussian wiretap channels in [7]. Security for a network with several two-way realys arranged in a line with cooperative jamming was considered in [8], where a lattice-based scheme was proposed. In all of the above works, weak information-theoretic security (mutual information rate to eavesdropper tends to zero) has been used as a secrecy metric. In contrast, in this work, we achieve perfect secrecy i.e. the secret message is independent of the eavesdropper's received values.

Throughout this paper, $+$ denotes addition over the reals $\mathbb{R}$, and $\oplus$ denotes addition within a finite Abelian group G.

II. The Noiseless Setting

The general set-up is as follows: nodes A and B possess messages X, Y, which are independent random variables (rvs), uniformly distributed over a finite Abelian group G. The messages X and Y are randomly modulated, independently at

some common time, into $\mathbb{R}^d$-valued rvs U and V, respectively, which are transmitted to the relay R; here, d is some positive integer. To explain the randomized modulation scheme for achieving perfect secrecy, we first consider the setting where $Z = 0$ in (1), so that the relay receives $W = U + V$. In this setting, the requirements of the modulation scheme can be summarized as follows ($\perp\!\!\!\perp$ denotes statistical independence):

(Z1) $(U, X) \perp\!\!\!\perp (V, Y)$;
(Z2) $U + V \perp\!\!\!\perp X$ and $U + V \perp\!\!\!\perp Y$; and
(Z3) $U + V$ almost surely determines $X \oplus Y$.

We will show that it is, in fact, possible to construct such rvs U, V. This is somewhat surprising since it can be easily shown that we cannot have non-degenerate real-valued rvs U and V such that $U + V \perp\!\!\!\perp U$ and $U + V \perp\!\!\!\perp V$. To explain without clutter the ideas behind our construction, we consider first the simplest case of $G = \mathbb{Z}_2$, i.e., the integers modulo 2.

A. Secure Computation of XOR at the Relay

In this section, X and Y are independent and identically distributed (iid) uniform binary rvs, and $X \oplus Y$ denotes their modulo-2 sum (XOR). We describe a construction of integer-valued rvs U and V satisfying (Z1)–(Z3).

1) Conditions on PMFs and characteristic functions: We first derive conditions under which integer-valued rvs U and V can satisfy properties (Z1)–(Z3). We introduce some notation: for $k \in \mathbb{Z}$, let $p_U(k) = \Pr[U = k]$, $p_V(k) = \Pr[V = k]$, and for $a \in \{0, 1\}$, let $p_{U|a}(k) = \Pr[U = k \mid X = a]$, $p_{V|a}(k) = \Pr[V = k \mid Y = a]$. Thus, $p_U = (1/2)(p_{U|0}+p_{U|1})$ and $p_V = (1/2)(p_{V|0} + p_{V|1})$.

Property (Z1) is equivalent to requiring that the joint probability mass function (pmf) of (U, V, X, Y) be expressible as

$$p_{UVXY}(k, l, a, b) = (1/2)(1/2)p_{U|a}(k)p_{V|b}(l) \qquad (2)$$

for $k, l \in \mathbb{Z}$ and $a, b \in \{0, 1\}$. Property (Z3) is satisfied by any U, V such that

$$\begin{aligned} p_{U|0}(k) = p_{V|0}(k) = 0 \quad &\text{for all odd } k \in \mathbb{Z}, \\ p_{U|1}(k) = p_{V|1}(k) = 0 \quad &\text{for all even } k \in \mathbb{Z}. \end{aligned} \qquad (3)$$

Finally, we turn our attention to (Z2). Let us define, for $k \in \mathbb{Z}$, $p_{U+V}(k) = \Pr[U + V = k]$, and for $a \in \{0, 1\}$, $p_{U+V|X=a}(k) = \Pr[U+V = k \mid X = a]$ and $p_{U+V|Y=a}(k) = \Pr[U+V = k \mid Y = a]$. Assuming $(U, X) \perp\!\!\!\perp (V, Y)$, we have $p_{U+V} = p_U * p_V$, $p_{U+V|X=a} = p_{U|a} * p_V$, and $p_{U+V|Y=a} = p_U * p_{V|a}$, where $*$ denotes the convolution operation. Thus, when $(U, X) \perp\!\!\!\perp (V, Y)$, (Z2) holds iff

$$p_U * p_V = p_{U|a} * p_V = p_U * p_{V|a} \quad \text{for } a \in \{0, 1\}. \qquad (4)$$

It helps to view this in the Fourier domain. Let φ_U, φ_V, $\varphi_{U|a}$ etc. denote the respective characteristic functions of the pmfs p_U, p_V, $p_{U|a}$ etc. — for example, $\varphi_{U|a}(t) = \sum_{k\in\mathbb{Z}} p_{U|a}(k)e^{ikt}$. Then, (4) is equivalent to

$$\varphi_U\varphi_V = \varphi_{U|a}\varphi_V = \varphi_U\varphi_{V|a} \quad \text{for } a \in \{0, 1\}. \qquad (5)$$

Note that $\varphi_U = (1/2)(\varphi_{U|0} + \varphi_{U|1})$ and $\varphi_V = (1/2)(\varphi_{V|0} + \varphi_{V|1})$. Hence, (5) should be viewed as a requirement on the conditional pmfs $p_{U|a}$ and $p_{V|a}$, $a \in \{0, 1\}$.

In summary, we have the following lemma.

Lemma 1. *Suppose that the conditional pmfs $p_{U|a}$ and $p_{V|a}$, $a \in \{0, 1\}$, satisfy (3) and (5). Then, the rvs U, V, X, Y with joint pmf given by (2) have properties (Z1)–(Z3).*

The idea now is to construct pmfs that satisfy the hypotheses of Lemma 1. To do this, we rely upon methods and results from Fourier analysis. The key tool we need is the Poisson summation formula, which we briefly recall here. Our description is based largely on Section XIX.5 in [9].

2) Poisson summation formula: Let ψ be the characteristic function of a real-valued random variable X, such that $\int_{-\infty}^{\infty} |\psi(t)|dt < \infty$. In particular, ψ is continuous and $\psi(0) = 1$. Since ψ is absolutely integrable, the random variable X has a continuous density f. The Poisson summation formula [9, Chapter XIX, equation (5.9)] states that for any $T > 0$ and $s \in \mathbb{R}$, we have for all $\zeta \in \mathbb{R}$,

$$\sum_{n=-\infty}^{\infty} \psi(\zeta+2n\pi/T)\, e^{-is(2n\pi/T)} = T \sum_{k=-\infty}^{\infty} f(kT+s)\, e^{i(kT+s)\zeta}, \qquad (6)$$

provided that the series on the left converges to a continuous function $\Psi(\zeta)$. Note that $\Psi(0) = T\sum_{k=-\infty}^{\infty} f(kT+s)$, which is a non-negative quantity. If $\Psi(0) \neq 0$, then dividing both sides of (6) by $\Psi(0)$ yields the important fact that $\Psi(\zeta)/\Psi(0)$ is the characteristic function of a discrete random variable supported within the set $\{kT+s : k \in \mathbb{Z}\}$, the probability mass at the point $kT+s$ being equal to $f(kT+s)/\sum_{k=-\infty}^{\infty} f(kT+s)$.

A special case of interest is when ψ is compactly supported. Let $T > 0$ be such that $\psi(t) = 0$ whenever $|t| \geq \pi/T$. It is straightforward to see that the series on the left-hand-side of (6) converges to a continuous function Ψ, and that $\Psi(0) = \psi(0) = 1$. From this, we infer that Ψ is the characteristic function of a discrete rv, as explained above. For future reference, we record this in the form of a proposition.

Proposition 2. *Let ψ be a characteristic function such that $\psi(t) = 0$ whenever $|t| \geq \pi/T$ for some $T > 0$, and let f be the corresponding probability density function. Then, for any $s \in \mathbb{R}$, the function $\Psi : \mathbb{R} \to \mathbb{C}$ defined by*

$$\Psi(\zeta) = \sum_{n=-\infty}^{\infty} \psi(\zeta + 2n\pi/T)\, e^{-is(2n\pi/T)}$$

is the characteristic function of a discrete rv supported within the set $\{kT + s : k \in \mathbb{Z}\}$. The probability mass at the point $kT + s$ is equal to $Tf(kT + s)$.

It should be noted that compactly supported characteristic functions do indeed exist — see e.g., [9, Section XV.2, Table 1], [10], [11]. We also give an explicit construction after the proof of Theorem 3 in the next subsection.

3) General construction: Let ψ be a characteristic function (of a continuous random variable X) with the properties that

(C1) $\psi(t) = 0$ for $|t| \geq \pi/2$, and

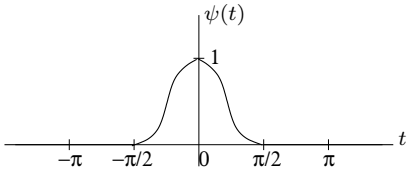

Fig. 1. A generic characteristic function supported on $[-\pi/2, \pi/2]$.

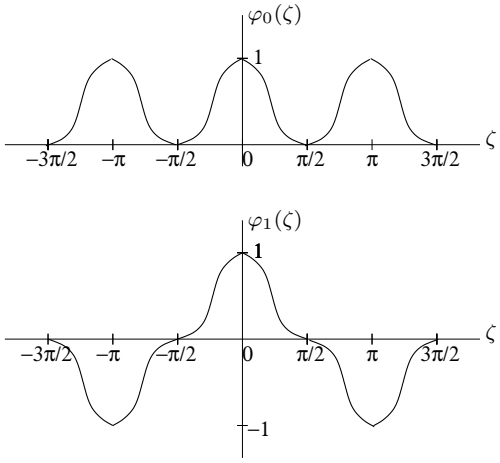

Fig. 2. The periodic functions φ_0 and φ_1 derived from ψ.

(C2) $\psi(t)$ is real and non-negative for all $t \in \mathbb{R}$.[1]

Note that since ψ is real-valued, it must be an even function: $\psi(-t) = \psi(t)$ for all $t \in \mathbb{R}$. Since ψ is integrable over $\mathbb{R}$, by the Fourier inversion formula, the random variable X has a continuous density f. Note that Proposition 2 holds for $T \leq 2$.

Let φ be the periodic function with period 2π that agrees with ψ on $[-\pi, \pi]$. Note that $\varphi(\zeta) = \sum_{n=-\infty}^{\infty} \psi(\zeta + 2\pi n)$. Thus, applying Proposition 2 with $T = 1$ and $s = 0$, we find that φ is the characteristic function of an integer-valued random variable, with pmf given by

$$p(k) = f(k) \text{ for all } k \in \mathbb{Z}. \tag{7}$$

Next, for $s = 0, 1$, define φ_s as follows: for $\zeta \in \mathbb{R}$,

$$\varphi_s(\zeta) = \sum_{n=-\infty}^{\infty} \psi(\zeta + n\pi) e^{-isn\pi}.$$

It is easily seen that φ_0 is the periodic extension of ψ with period π, i.e., φ_0 is the periodic function with period π that agrees with ψ on $[-\pi/2, \pi/2]$, as depicted at the top of Figure 2 for a generic ψ shown in Figure 1. On the other hand, φ_1 is periodic with period 2π: its graph is obtained from that of φ_0 by reflecting about the ζ-axis every second copy of ψ, as depicted at the bottom of Figure 2.

Applying Proposition 2 with $T = 2$ and $s \in \{0, 1\}$, we get that φ_0 and φ_1 are characteristic functions of rvs supported within the even and odd integers, respectively. The pmf corresponding to φ_0 is given by

$$p_0(k) = \begin{cases} 2f(k) & \text{if } k \text{ is an even integer} \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

and that corresponding to φ_1 is

$$p_1(k) = \begin{cases} 2f(k) & \text{if } k \text{ is an odd integer} \\ 0 & \text{otherwise.} \end{cases} \tag{9}$$

From (7)–(9), we have $p(k) = \frac{1}{2}(p_0(k) + p_1(k))$ for all $k \in \mathbb{Z}$.

Finally, note that since $\varphi_0(t)$ and $\varphi_1(t)$ differ from $\varphi(t)$ only when $\varphi(t) = 0$, we have

$$\varphi^2 = \varphi\varphi_0 = \varphi\varphi_1. \tag{10}$$

We can now prove the following theorem.

Theorem 3. *Let X, Y be iid Bernoulli$(1/2)$ rvs. Suppose that we are given a probability density function $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$ with a non-negative real characteristic function ψ such that $\psi(t) = 0$ for $|t| \geq \pi/2$. Set $p_{U|0} = p_{V|0} = p_0$ and $p_{U|1} = p_{V|1} = p_1$, where p_0 and p_1 are as in (8) and 9). Then, the resulting $\mathbb{Z}$-valued rvs U and V satisfy properties (Z1)–(Z3). Additionally, the rvs U and V have finite variance iff ψ is twice differentiable, in which case the variance equals $-\psi''(0)$.*

Based on this theorem, secure computation of XOR at the relay works as follows: the nodes A and B modulate their bits independently to an integer k, with probability $p_0(k)$ (from (8)) if the bit is 0, or with probability $p_1(k)$ (from (9)) if the bit is 1. The probability distributions can be chosen such that the modulated symbols have finite average power. The sum of the integers from A and B received at the relay R is independent of the individual bits of A and B. However, the XOR of the two bits can be recovered at R with probability 1.

Proof of Theorem 3. With $p_{U|0} = p_{V|0} = p_0$ and $p_{U|1} = p_{V|1} = p_1$, we have $p_U = p_V = p$, where p is as in (7).

Clearly, (3) holds. To verify (5), note that, by virtue of (10), we have for $a \in \{0, 1\}$, $\varphi_U\varphi_V = \varphi^2 = \varphi\varphi_a$. But, by construction, $\varphi_U\varphi_{V|a} = \varphi_V\varphi_{U|a} = \varphi\varphi_a$. Therefore, by Lemma 1, the rvs (U, V, X, Y) with joint pmf given by (2) have the properties (Z1)–(Z3).

The assertion about the variance of U and V follows from Lemma 2 in [9, Section XV.4]. We omit the details. □

For completeness, we give an explicit construction of a compactly supported, twice-differentiable characteristic function ψ. Consider the density (from [9, Section XV.2, Table 1])

$$h(x) = \begin{cases} \frac{1}{2\pi} & \text{if } x = 0 \\ \frac{1-\cos x}{\pi x^2} & \text{if } x \neq 0 \end{cases} \tag{11}$$

which has characteristic function $\hat{h}(t) = \max\{0, 1 - |t|\}$. The function $g = \hat{h} * \hat{h}$, where $*$ denotes convolution, can be explicitly computed to be

$$g(t) = (\hat{h} * \hat{h})(t) = \begin{cases} \frac{1}{2}|t|^3 - t^2 + \frac{2}{3} & \text{if } |t| \leq 1 \\ \frac{1}{6}(2 - |t|)^3 & \text{if } 1 \leq |t| \leq 2 \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

[1]There is no loss of generality in imposing this requirement. Suppose that a random variable X has characteristic function ψ, which is complex-valued in general. Let X_1, X_2 be iid rvs with the same distribution as X. Then, $X_1 - X_2$ has characteristic function $\psi\overline{\psi} = |\psi|^2$.

Proposition 4. *The function $f(x) = (3\pi^2/4)\,[h(\pi x/4)]^2$, with h as in (11), is a density function whose characteristic function is given by*

$$\psi(t) = \tfrac{3}{2}\, g(\tfrac{4t}{\pi}),$$

where g is as in (12). The function ψ is non-negative with $\psi(t) = 0$ for $|t| \geq \pi/2$. Furthermore, ψ is twice differentiable, with $\psi''(0) = -48/\pi^2$.

We omit the simple proof of the proposition.

B. Extension to Finite Abelian Groups

A close look at the modulations in the previous section reveals the following structure: points from the lattice $2\mathbb{Z}$ and its coset (in $\mathbb{Z}$) $1 + 2\mathbb{Z}$ are chosen for sending bit 0 and 1, respectively, according to a carefully chosen probability distribution given by Theorem 3. In essence, we have a fine lattice $\Lambda = \mathbb{Z}$ and a coarse lattice $\Lambda_0 = 2\mathbb{Z}$ with the quotient group Λ/Λ_0 consisting of the two cosets $2\mathbb{Z}$ and $1 + 2\mathbb{Z}$ making up the probabilistically-chosen modulation alphabet. Note that the quotient group in this case is isomorphic to $\mathbb{Z}_2$, and this enables recovery of the XOR of the bits (addition in $\mathbb{Z}_2$) from integer addition of transmitted symbols modulo the coarse lattice. Also, the choice of the probability distribution (from Theorem 3) ensures that the choice of coset at each transmitter is independent of the integer sum at the relay.

Now, any finite Abelian group G can be expressed as the quotient group Λ/Λ_0 for some pair of nested lattices $\Lambda_0 \subseteq \Lambda$. Indeed, any such G is isomorphic to a direct sum of cyclic groups: $G \cong \mathbb{Z}_{N_1} \oplus \mathbb{Z}_{N_2} \oplus \cdots \oplus \mathbb{Z}_{N_k}$ for some positive integers $N_1, N_2, \ldots, N_k$ [12, Theorem 2.14.1]. Here, $\mathbb{Z}_{N_j}$ denotes the group of integers modulo-N_j. Taking $\Lambda = \mathbb{Z}^k$ and $\Lambda_0 = A\,\mathbb{Z}^k$, where A is the diagonal matrix $\mathrm{diag}(N_1, N_2, \ldots, N_k)$, we have $G \cong \Lambda/\Lambda_0$. So, the finite Abelian group case is equivalent to considering the quotient group, i.e., the group of cosets, of a coarse lattice Λ_0 within a fine lattice Λ. These lattices may be taken to be full-rank lattices in $\mathbb{R}^d$.

For a full-rank lattice Λ in $\mathbb{R}^d$, let

$$\mathcal{V}(\Lambda) = \{\mathbf{x} \in \mathbb{R}^d : \|\mathbf{x}\| < \|\mathbf{x} - \mathbf{z}\| \text{ for all } \mathbf{z} \in \Lambda,\ \mathbf{z} \neq \mathbf{0}\}, \tag{13}$$

where $\|\cdot\|$ denotes the Euclidean (L^2) norm, be the interior of the Voronoi region of Λ around the point $\mathbf{0}$. In words, $\mathcal{V}(\Lambda)$ is the set of points of $\mathbb{R}^d$ for which $\mathbf{0}$ is the unique closest point of the lattice Λ. The *dual lattice* is defined as $\Lambda^* = \{\mathbf{y} \in \mathbb{R}^d : \mathbf{x}^T\mathbf{y} \in \mathbb{Z}\}$, and the *Fourier dual* is $\hat{\Lambda} = 2\pi\Lambda^*$. The *determinant* of Λ, denoted by $\det\Lambda$, is equal to $|\det A|$ for any (square) matrix A such that $\Lambda = A\mathbb{Z}^d$.

Let Λ_0 be a sublattice of Λ of index N (i.e., the number of cosets of Λ_0 in Λ is N). List the cosets of Λ_0 in Λ as $\Lambda_0, \Lambda_1, \ldots, \Lambda_{N-1}$, which constitute the quotient group $G = \Lambda/\Lambda_0$. As before, $\oplus$ denotes addition within G.

Consider rvs X, Y uniformly distributed over G. We wish to construct rvs U, V taking values in Λ, having the properties (Z1)–(Z3). The following theorem shows that this is possible.

Theorem 5. *Suppose that $\psi : \mathbb{R}^d \to \mathbb{R}_{\geq 0}$ is the characteristic function of a probability density function $f : \mathbb{R}^d \to \mathbb{R}_{\geq 0}$, such that $\psi(\mathbf{t}) = 0$ for $\mathbf{t} \notin \mathcal{V}(\hat{\Lambda}_0)$, where $\hat{\Lambda}_0$ is the Fourier dual of Λ_0. For $j = 0, 1, \ldots, N-1$, define the pmf p_j as follows: $p_j(\mathbf{k}) = (\det\Lambda_0) f(\mathbf{k})$ if $\mathbf{k} \in \Lambda_j$; otherwise, $p_j(\mathbf{k}) = 0$. Finally, define a random variable U (resp. V) jointly distributed with X (resp. Y) as follows: if $X = \Lambda_j$ (resp. $Y = \Lambda_j$), U (resp. V) is a random point from Λ_j picked according to the distribution p_j. Then, the resulting Λ-valued rvs U, V satisfy properties (Z1)–(Z3). Additionally, if ψ is twice differentiable, then $E\|U\|^2 = E\|V\|^2 = -\nabla^2\psi(\mathbf{0})$, where $\nabla^2 = \sum_{j=1}^d \partial_j^2$ is the Laplacian operator.*

As with Theorem 3 and XOR, the above theorem allows for secure computation at the relay of the group operation $X \oplus Y$. The theorem is proved in a manner completely analogous to Theorem 3, the main difference being that the multi-dimensional Poisson summation formula is used in place of (6). We skip the proof for lack of space.

While any characteristic function ψ supported within $\mathcal{V}(\hat{\Lambda}_0)$ suffices for the construction of Theorem 5, it is of interest to use a ψ for which $-\nabla^2\psi(\mathbf{0})$ is the least among such ψ's. This would yield random variables U and V of least second moment, having the desired properties. It turns out that the second moment cannot be made arbitrarily small. Indeed, the following result, adapted from [10], gives a precise and complete answer to the question of how small $-\nabla^2\psi(\mathbf{0})$ can be for a characteristic function ψ supported within a ball of radius R in $\mathbb{R}^d$.

Theorem 6 ([10], Theorem 5.1)**.** *If ψ is a characteristic function such that $\psi(\mathbf{t}) = 0$ for $\|\mathbf{t}\| \geq \rho$, then*

$$-\nabla^2\psi(\mathbf{0}) \geq \frac{4}{\rho^2}\, j_{\frac{d-2}{2}}^2, \tag{14}$$

where j_k denotes the first positive zero of the Bessel function J_k. Furthermore, equality holds iff $\psi(\mathbf{t}) = \widetilde{\psi}(\mathbf{t}/\rho)$ for a certain non-negative characteristic function $\widetilde{\psi}$ supported within the unit ball.

A precise expression for $\widetilde{\psi}$ and the corresponding density function can be found in [10].

III. The Gaussian Noise Setting

The modulation scheme of Section II-B extends in a very natural way to a lattice coding scheme that can be used for secure and *reliable* computation over a Gaussian MAC channel as in (1), where Z is now iid Gaussian noise. We describe the coding scheme below.

Code: A $(\Lambda^{(d)}, \Lambda_0^{(d)})$ code consists of a pair of full-rank nested lattices $\Lambda_0^{(d)} \subseteq \Lambda^{(d)}$ in $\mathbb{R}^d$. The computation is performed in the group $G^{(d)} = \Lambda^{(d)}/\Lambda_0^{(d)}$, whose $N^{(d)} \triangleq |\Lambda^{(d)}/\Lambda_0^{(d)}|$ elements are listed as $\Lambda_0, \Lambda_1, \ldots, \Lambda_{N^{(d)}-1}$.

Encoding: We have messages X, Y at nodes $\mathtt{A}, \mathtt{B}$ that are independent rvs, uniformly distributed over $G^{(d)}$. We first pick a characteristic function ψ supported within $\mathcal{V}(\hat{\Lambda}_0^{(d)})$, as needed in Theorem 5. In fact, we impose the restriction

that ψ be supported within a ball centred at $\mathbf{0}$ with radius equal to the *packing radius*, $r_{\text{pack}}(\hat{\Lambda}_0^{(d)})$, of the dual lattice $\hat{\Lambda}_0^{(d)}$. Now, the packing radius is, by definition, the largest radius of a ball centred at $\mathbf{0}$ that is contained within $\mathcal{V}(\hat{\Lambda}_0^{(d)})$. So, if $\psi(\mathbf{t}) = 0$ for $\|\mathbf{t}\| \geq r_{\text{pack}}(\hat{\Lambda}_0)$, then $\psi(\mathbf{t})$ is certainly supported within $\mathcal{V}(\hat{\Lambda}_0)$. If $X = \Lambda_j$, node A transmits a random vector $\mathbf{u} \in \Lambda_j$ picked according to the distribution p_j of Theorem 5. Similarly, if $Y = \Lambda_k$, node B transmits a random vector $\mathbf{v} \in \Lambda_k$ picked according to the distribution p_k. The rate of transmission from A or B is $R^{(d)} = \frac{1}{d}\log_2 N^{(d)}$. The average transmit power per dimension at each node is $P^{(d)} = \frac{-\nabla^2\psi(\mathbf{0})}{d}$, as in Theorem 5. Thus, from Theorem 6, we see that an average transmit power per dimension as low as

$$P^{(d)} = \frac{4j_{\frac{d-2}{2}}^2}{\rho^2 d}, \tag{15}$$

with $\rho = r_{\text{pack}}(\hat{\Lambda}_0^{(d)})$, is achievable by a suitable choice of ψ. It was shown in [14] (see also [13]) that the first positive zero of the Bessel function J_k can be written as $j_k = k + ak^{1/3} + \mathcal{O}(k^{-1/3})$, where a is a constant independent of k. Therefore, in the large d regime,

$$P^{(d)} = \frac{d}{{r_{\text{pack}}}^2(\hat{\Lambda}_0^{(d)})}(1 + o(d)), \tag{16}$$

where $o(d) \to 0$ as $d \to \infty$, is achievable by a suitable choice of ψ using Theorem 6.

Decoding: The relay R receives $\mathbf{w} = \mathbf{u} + \mathbf{v} + \mathbf{z}$, where $\mathbf{z}$ is a Gaussian noise vector with d independent $N(0, \sigma^2)$ components, which are all independent of $\mathbf{u}$ and $\mathbf{v}$. The relay estimates $\Lambda_j \oplus \Lambda_k$ to be the coset represented by the closest vector to $\mathbf{w}$ in the lattice Λ, which we denote by $Q_\Lambda(\mathbf{w})$.

Security: Since the noise $\mathbf{z}$ is independent of everything else, Theorem 5 shows that $\mathbf{w}$ is independent of the individual messages X, Y. Hence, even in the noisy setting, perfect security continues to be guaranteed at the relay for any choice of the nested lattice code.

Reliability and achievable rate: Let $\mathrm{P}_{\text{err}}^{(d)}$ denote the probability that $Q_\Lambda(\mathbf{w})$ is different from the coset to which $\mathbf{u}+\mathbf{v}$ belongs. A rate $\mathcal{R}$ is said to be achievable with perfect secrecy if, for any $\epsilon > 0$, there exists a sequence of $(\Lambda^{(d)}, \Lambda_0^{(d)})$ codes such that $\mathrm{P}_{\text{err}}^{(d)} < \epsilon$ and $R^{(d)} > \mathcal{R} - \epsilon$ for sufficiently large d. The rate is said to be achieved with perfect secrecy at a transmit power per dimension $\mathcal{P}$ if we have in addition that $P^{(d)} < \mathcal{P} + \epsilon$ for sufficiently large d.

The *covering radius* of a lattice Λ, denoted by $r_{\text{cov}}(\Lambda)$, is the radius of the smallest ball centred at $\mathbf{0}$ that contains $\mathcal{V}(\Lambda)$. The proposition below characterizes achievable rates in terms of the covering radius of the coarse lattice $\Lambda_0^{(d)}$. We skip the proof, which follows easily from the results in [15] and [4].

Proposition 7. *Let $\mathsf{M} > 0$ be a constant. A rate $\mathcal{R} = \frac{1}{2}\log_2\left(\frac{\mathsf{M}}{\sigma^2}\right)$ is achievable with perfect secrecy by a sequence of nested lattice pairs $(\Lambda^{(d)}, \Lambda_0^{(d)})$ satisfying $r_{cov}(\Lambda_0^{(d)}) = \sqrt{d\mathsf{M}}$ for each d.*

It now remains to characterize the average transmit power per dimension at which the rates guaranteed by Proposition 7 are achieved. From (16), it is clear that we need to relate $r_{\text{pack}}(\hat{\Lambda}_0)$ to $r_{\text{cov}}(\Lambda_0)$. Extending the arguments in [15], we can show that there exists a sequence of nested lattices $(\Lambda^{(d)}, \Lambda_0^{(d)})$ as guaranteed by Proposition 7 for which

$$\lim_{d\to\infty} \frac{1}{d}\, r_{\text{pack}}(\hat{\Lambda}_0^{(d)}) r_{\text{cov}}(\Lambda_0^{(d)}) = \frac{1}{2e}. \tag{17}$$

also holds (a proof will be given in a forthcoming full version of this paper). Using this result, we have the following theorem.

Theorem 8. *A rate $\mathcal{R} = \frac{1}{2}\log_2(\mathcal{P}/(4e^2\sigma^2))$ is achievable with perfect secrecy at a transmit power of $\mathcal{P}$.*

Proof: Take the constant M in Proposition 7 to be $(\frac{1}{2e})^2\mathcal{P}$ for some $\mathcal{P} > 0$, so that $r_{\text{cov}}(\Lambda_0^{(d)}) = \frac{1}{2e}\sqrt{d\mathcal{P}}$. We then find, via (16) and (17), that $\lim_{d\to\infty} P^{(d)} = \mathcal{P}$. ∎

At present, we do not have any outer bounds to suggest that the rates achieved in Theorem 8 are good. In particular, the factor $4e^2$ does not appear in any standard Gaussian-MAC capacity regions without the secrecy constraint.

REFERENCES

[1] I.-J. Baik and S.-Y. Chung, "Network coding for two-way relay channels using lattices," in *Proc. 2008 IEEE Int. Conf. Commun. (ICC'08)*, pp. 3898–3902.

[2] P. Popovski and H. Yomo, "Physical network coding in two-way wireless relay channels," in *Proc. 2007 IEEE Int. Conf. Commun. (ICC'07)*, pp. 707–712.

[3] M. Wilson, K. Narayanan, H. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bidirectional relaying," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5641–5654, Nov. 2010.

[4] B. Nazer and M. Gastpar, "Compute-and-Forward: Harnessing Interference through Structured Codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, October 2011.

[5] B. Nazer and M. Gastpar, "Reliable physical layer network coding," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 438–460, March 2011.

[6] R. Zhang, L. Song, Z. Han, B. Jiao, M. Debbah, "Physical layer security for two way relay communications with friendly jammers," *Proc. 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010)*, pp. 1-6, 6-10 Dec. 2010.

[7] F. Oggier, P. Solé, J.-C. Belfiore, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis," submitted to the *IEEE Trans. on Information Theory*, available arXiv:1103.4086v1 [cs.IT].

[8] X. He and A. Yener, "Providing secrecy with lattice codes," *Proc. 46th Annual Allerton Conference on Communication, Control, and Computing 2008*, pp. 1199-1206, 23-26 Sept. 2008.

[9] W. Feller, *An Introduction to Probability Theory and its Applications, Vol. 2*, 2nd ed., Wiley, 1971.

[10] W. Ehm, T. Gneiting, and D. Richards, "Convolution Roots of Radial Positive Definite Functions with Compact Support," *Trans. AMS*, vol. 356, no. 11, pp. 4655–4685, May 2004.

[11] H. Rubin and T.M. Sellke, "Zeroes of infinitely differentiable characteristic functions," in *A Festschrift for Herman Rubin*, Anirban DasGupta, ed., Institute of Mathematical Statistics Lecture Notes – Monograph Series, vol. 45, pp. 164–170, 2004.

[12] I.N. Herstein, *Topics in Algebra*, 2nd ed., Wiley, 1975.

[13] A. Elbert and A. Laforgia, "An asymptotic relation for the zeros of Bessel functions", *Journal of Math. Analysis and Applications*, vol. 98, no. 2, pp. 502–510, 1984.

[14] F.G. Tricomi, "Sulle funzioni di Bessel di ordine e argomento pressoché uguali," *Atti Accad. Sci. Torino Cl. Sci. Fis. Mat. Natur.*, vol. 83, pp. 3–20, 1949.

[15] U. Erez and R. Zamir, "Achieving 1/2log(1+SNR) on the AWGN channel with Lattice Encoding and Decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, October 2004.