Conference Paper

Semantically Secure Lattice Codes for Compound MIMO Channels

Author(s):
Campello, Antonio; Ling, Cong; Belfiore, Jean-Claude

Publication Date:
2018-02

Permanent Link:
https://doi.org/10.3929/ethz-b-000245079

Rights / License:
In Copyright - Non-Commercial Use Permitted
Semantically Secure Lattice Codes for Compound MIMO Channels

Antonio Campello, Cong Ling
Department of Electrical and Electronic Engineering
Imperial College London, U.K.
Email: \{a.campello, c.ling\}@imperial.ac.uk

Jean-Claude Belfiore
Mathematical and Algorithmic Sciences Lab
France Research Center, Huawei Technologies
belfiore@telecom-paristech.fr

Abstract—We consider compound MIMO wiretap channels where minimal channel state information at the transmitter (CSIT) is assumed. Using the flatness factor for MIMO channels, we propose lattice codes universally achieving the secrecy capacity of compound MIMO wiretap channels up to a constant gap that is linear in the number of transmit antennas, independently on the number of eavesdropper antennas. The proposed approach improves upon existing works on secrecy coding for MIMO wiretap channels from an error probability perspective, and establishes information theoretical security (in fact semantic security). We also give an algebraic construction to reduce the code design complexity, as well as the decoding complexity of the legitimate receiver.

I. INTRODUCTION

Due to the open nature of the wireless medium, wireless communications are inherently vulnerable to eavesdropping attacks. Information theoretic security offers additional protection for wireless data, since it only relies on the physical properties of wireless channels, thus representing a competitive/complementary approach to security compared to traditional cryptography.

In the information theory community, a commonly used secrecy notion is strong secrecy: the mutual information \( I(M; Z^N) \) between the confidential message \( M \) and the channel output \( Z^N \) should vanish when the code length \( N \rightarrow \infty \). This assumption of uniformly distributed messages was dropped in [17], establishing semantic security: for any message distribution, the advantage obtained by an eavesdropper from its received signal vanishes for large block lengths. This notion is motivated by the fact that the plaintext can be fixed and arbitrary.

For the Gaussian wiretap channel, [15] introduced the secrecy gain of lattice codes while [11] proposed semantically secure lattice codes based on the lattice Gaussian distribution. To this aim, the flatness factor of a lattice was introduced in [11] as a fundamental criterion which implies that conditional outputs are indistinguishable for different input messages. Using a random coding argument, it was shown that there exist families of lattice codes which are good for secrecy, meaning that their flatness factor is vanishing, and achieve semantic security for rates up to \( 1/2 \) nat from the secrecy capacity.

Compared to the Gaussian wiretap channel, the cases of fading and multi-input multi-output (MIMO) wiretap channels are more technically challenging. The fundamental limits of fading wireless channels with secrecy constraints have been investigated in [1], [3], [4], [9], [7] where the achievable rates, secrecy capacity, and the secrecy outage probability were given. Although CSIT is sometimes available for the legitimate channel, it is hardly possible that it would be available for the eavesdropping channel. Schaefer and Loyka [18] studied the secrecy capacity of the compound MIMO wiretap channel, where a transmitter has no knowledge of the realization of the eavesdropping channel, except that it belongs to a given set (the compound set). The compound model represents a well-accepted, reasonable approach to information theoretic security, which assumes minimal CSIT of the eavesdropping channel [10], [8], and can also model multicast scenarios.

In this paper, we propose universal codes for compound Gaussian MIMO wiretap channels. Previously, [14] has established strong secrecy over ergodic stationary MIMO wiretap channels for secrecy rates that are within a constant gap to the secrecy capacity. Besides different channel models (compound vs. ergodic channels) considered, we obtain a smaller (and different in nature) gap by employing a different construction as in [14].

For a compound channel formed by the set of all matrices \( \mathbb{C}^a \times b \rightarrow \mathbb{C}^a \times b \), we have the secrecy capacity \( C_a - \max \{ a, 0 \} \geq C_e \), where \( C_a \) is the capacity of the legitimate channel, \( C_e \) is the capacity of the eavesdropper channel, and \( n_a \) is the number of transmit antennas and \( n_e \) is the number of transmit antennas and \( (x) = \max \{ x, 0 \} \). We also show how to extend the analysis in order to accommodate number-of-antennas mismatch, i.e., security is valid regardless of the number of antennas at the eavesdropper. This is a very appealing property, since the number of receive antennas of an eavesdropper may be unknown to the transmitter. Notice that previous works [2], [14] required \( n_e \geq n_a \).

II. PROBLEM STATEMENT

We consider the following wiretap model. A transmitter sends information through a MIMO channel to a legitimate receiver (Bob) and is eavesdropped by an illegitimate user (Eve). The channel equations for Bob and Eve read:

\[
Y_b = H_b X + W_b \quad \text{and} \quad Y_e = H_e X + W_e ,
\]

where \( Y_b \) is the received output of Bob, \( Y_e \) is the received output of Eve, \( X \) is the transmitted signal, \( W_b \) and \( W_e \) are the noise vectors for Bob and Eve, respectively.

The channel equations for Bob and Eve are given by:

\[
Y_b = H_b X + W_b \quad \text{and} \quad Y_e = H_e X + W_e ,
\]

where \( Y_b \) and \( Y_e \) are the received signals at Bob and Eve, respectively. The noise vectors \( W_b \) and \( W_e \) are assumed to be independent and identically distributed (i.i.d.) Gaussian with zero mean and variance \( 1 \) and \( n_b \times T \) and \( n_e \times T \), respectively.

123
where $n_a$ is the number of transmit antennas, $n_b, n_e$ is the number of receive antennas for Bob and Eve, $T$ is the coherence time, and $W_b$ and $W_e$ have circularly symmetric complex Gaussian iid entries with variance $\sigma_b^2, \sigma_e^2$ per complex dimension. We denote the signal-to-noise ratios by

$$\rho_b \triangleq \frac{P}{\sigma_b^2} \quad \text{and} \quad \rho_e \triangleq \frac{P}{\sigma_e^2}.$$ 

We assume that the exact channel realizations $(H_b, H_e)$ are unknown to the transmitter but belong to a compound set $\mathcal{S} = \mathcal{S}_b \times \mathcal{S}_e \subset \mathbb{C}^{n_b \times n_a} \times \mathbb{C}^{n_e \times n_a}$. Suppose that $\mathcal{S}_b$ and $\mathcal{S}_e$ are the set of channels with same isotropic mutual information i.e.,

$$\mathcal{S}_b = \{ H_b \in \mathbb{C}^{n_b \times n_a} : \|I + \rho_b H_b^H H_b\| = e^{C_b}\} \quad \text{and} \quad \mathcal{S}_e = \{ H_e \in \mathbb{C}^{n_e \times n_a} : \|I + \rho_e H_e^H H_e\| = e^{C_e}\},$$

for fixed $C_b, C_e \geq 0$. In this case, it is known (e.g. [18]) that $C_e \geq (C_b - C_e)^+$. The worst case is achieved by taking a specific “isotropic” realization such that $H_b^H H_b$ and $H_e^H H_e$ are a multiple of the identity, from where we conclude that $C_e = C_b - C_e$. In what follows we construct lattice codes that approach the rate $C_e$ with semantic security. As a corollary, the semantic security capacity and the strong secrecy capacity for the compound set $\mathcal{S}_b \times \mathcal{S}_e$ coincide.

A. Notions of Security

A secrecy code (or, more precisely, an $(R, R', T)$ secrecy code) for the compound MIMO channel consists of:

(i) A set of messages $\mathcal{M}_T = \{1, \ldots, e^{TR}\}$

(ii) An auxiliary source $U$ taking values in $\mathcal{U}_T$ with entropy $R' = H(U)$.

(iii) An encoding function $f_T : \mathcal{M}_T \times \mathcal{U}_T \to \mathbb{C}^{n_a \times T}$ s.t.

$$\frac{1}{T} \mathbb{E}[\mathbb{E}[f_T(m, U)^\dagger f_T(m, U)]] \leq n_a P$$

(iv) A decoding function $g : \mathcal{S}_b \times \mathbb{R}^{n_b \times T} \to \mathcal{M}_T$.

A pair $(s_b, s_e) \in \mathcal{S}_b \times \mathcal{S}_e$ is referred to as a channel state (or channel realization). To ensure reliability for all channel states, we require a sequence of codes whose error probability for message $M$ vanishes:

$$P_{eM}(T) \triangleq \mathbb{P}(g(s_b, M) \neq M) \to 0, \forall s_b \in \mathcal{S}_b, \text{ as } T \to \infty.$$  \hspace{1cm} (4)

Let $p_M$ be a message distribution over $\mathcal{M}_T$. For channel coding, $p_M$ is usually assumed to be uniform, however this assumption is not sufficient for modern security protocols. Let $Y_e$ be the output of the channel to the eavesdropper, who is omniscient. In the limit of $T \to \infty$ the notion of semantic security coincides with the following [11],[17]:

$$\max_{m_t,m_e \in \mathcal{M}_T} \mathbb{V} (|p_{Y_e}|,|p_{Y_e}|) \to 0 \quad \forall s_e \in \mathcal{S}_e, \hspace{1cm} (5)$$

where $\mathbb{V}$ stands for the $l_1$ variational distance between distributions. In other words the eavesdropper cannot distinguish the output of the channel for different messages. This notion also requires a sequence of codes to be universally secure for all channel states. We say that a sequence of codes of rate approaching $R$ is semantically secure for compound MIMO if, for all $(s_b, s_e) \in \mathcal{S}$ it satisfies the reliability condition (4) and (5). In what follows we proceed to construct universally secure codes for the MIMO wiretap channel using lattice coset codes.

III. CORRELATED DISCRETE GAUSSIAN DISTRIBUTIONS

We exhibit in this subsection the important results and concepts for the definition and analysis of our lattice coding scheme.

A. Preliminary lattice definitions

A (complex) lattice $\Lambda$ with generator matrix $B_e$ is a discrete additive subgroup of $\mathbb{C}^{n_a}$ given by

$$\Lambda = L(B_e) = \{ B_e x : x \in \mathbb{Z}^{n_a} \}. \hspace{1cm} (6)$$

A complex lattice has an equivalent real lattice generated by the matrix $B_e$ obtained by stacking real and imaginary parts of matrix $B_e$.

A fundamental region $\mathcal{R}(\Lambda)$ for $\Lambda$, is any interior-disjoint region that tiles $\mathbb{C}^{n_a}$ through translates by vectors of $\Lambda$. For any $y, x \in \mathbb{C}^{n_a}$ we say that $y = x \ (\text{mod } \Lambda)$ iff $y - x \in \mathcal{R}(\Lambda)$. By convention, we fix a fundamental region and denote by $y \ (\text{mod } \Lambda)$ the unique representative $x \in \mathcal{R}(\Lambda)$ such that $y = x \ (\text{mod } \Lambda)$. The volume of $\Lambda$ is defined as the volume of a fundamental region for the equivalent real lattice, given by $V(\Lambda) = |B_e|$. Notice that if $B_e$ is full rank, then $V(\Lambda) > 0$.

B. The Flatness Factor

The discrete Gaussian distribution and the flatness factor will be used to measure bound the information leakage to an eavesdropper.

The pdf of a correlated Gaussian distribution with covariance matrix $\Sigma$ is

$$\mathcal{F}_{\gamma \Sigma}(x) = \frac{1}{\pi^{n_a}} \exp \{- \gamma(x - c)^T \Sigma^{-1} (x - c)\}.$$ 

where $\gamma = 0$ we omit the index. The flatness factor of a lattice quantifies the distance between $\mathcal{F}_{\gamma \Sigma}(x)$ and an uniform distribution over $\mathcal{R}(\Lambda)$.

Definition 1 (Flatness factor for correlated Gaussian distributions).

$$\epsilon_\Lambda(\sqrt{\Sigma}) \triangleq \max_{x \in \mathcal{R}(\Lambda)} |V(\Lambda) \mathcal{F}_{\gamma \Sigma}(x) - 1|$$

where $\mathcal{R}(\Lambda)$ is a fundamental region of $\Lambda$.

When $c = 0$ we ignore the index and write $\mathcal{F}_{\gamma \Sigma}(x) = \mathcal{F}_{\gamma \Sigma}(x)$. For a co-variance matrix $\Sigma$ we define the generalized-volume-to-noise ratio as $\gamma_\Lambda(\sqrt{\Sigma}) = V(\Lambda)^{1/n_a} / |\Sigma|^{1/n_a}$.

In our applications, the matrix $\Sigma$ will be determined by the channel realization (1), and we will deal with lattices of dimension $n_a T$, where $T$ is the coherence time. Figure 1 shows the effect of fading on the lattice Gaussian function. A function which is flat over the Gaussian channel (corresponding to $\Sigma = I$) (a) need not be flat for a channel in deep fading.
(corresponding to a ill-conditioned $\Sigma$) (b), in which case an eavesdropper could clearly distinguish one dimension of the signal.

$$\Sigma = \begin{pmatrix} 0.25 \\ 0.25 \text{diag}(6,1/6) \end{pmatrix}$$

Fig. 1: Illustration of the Gaussian periodic function for the lattice $\mathbb{Z}^2$ and different co-variance matrices with same determinant.

C. The discrete Gaussian Distribution

In order to define our coding scheme, we need a last element, which is the distribution of the sent signals. To this purpose, we define the discrete Gaussian distribution $D_{\Lambda + \epsilon, \sqrt{\Sigma}}$ as the distribution assuming values on $\Lambda + \epsilon$, such that the probability of each point $\lambda + \epsilon$ is given by

$$D_{\Lambda + \epsilon, \sqrt{\Sigma}}(\lambda + \epsilon) = \frac{f_{\sqrt{\Sigma}}(\lambda + \epsilon)}{f_{\sqrt{\Sigma}}(\epsilon)}.$$ 

Its relation to the continuous Gaussian distribution can be done via the smoothing parameter or the flatness factor. For instance, a vanishing flatness factor guarantees that the power per-dimension of $D_{\Lambda + \epsilon, \sigma I}$ is approximately $\sigma^2$.

The next proposition ([14, Appendix I-A]) says that the sum of a continuous Gaussian and a discrete Gaussian is approximately a continuous Gaussian, provided that the flatness factor is small.

**Lemma 1.** Given $x_1$ sampled from discrete Gaussian distribution $D_{\Lambda + \epsilon, \sqrt{\Sigma}}$, and $x_2$ sampled from continuous Gaussian distribution $f_{\sqrt{\Sigma}}$. Let $\Sigma_0 = \Sigma_1 + \Sigma_2$ and let $\Sigma_1 = \Sigma_1^1 + \Sigma_2^1$. If $\sqrt{\Sigma_1^1} \geq \eta_e(\Lambda)$ for $\varepsilon \leq \frac{1}{2}$, then the distribution $g$ of $x = x_1 + x_2$ is close to $f_{\sqrt{\Sigma}}$:

$$g(x) \in f_{\sqrt{\Sigma}}(x) [1 - 4\varepsilon, 1 + 4\varepsilon].$$

1) Construction A: A general “flexible” construction can be defined via “generalized reductions”. For let $\phi_p: \Lambda_{\text{base}} \to \mathbb{Z}[i]^T_p$ be a surjective homomorphism from a base lattice $\Lambda_{\text{base}}$ of complex dimension $N$ to the vector space $\mathbb{Z}[i]^T$ (also referred to as a reduction). Define the lattice $\Lambda(\mathcal{C})$ as the pre-image of a linear code $\mathcal{C}$,

$$\Lambda(\mathcal{C}) = \phi^{-1}(\mathcal{C}).$$

If $\mathcal{C}$ has length $T$ and dimension $k$, the volume of $\Lambda(\mathcal{C})$ equals $p^{T-k}V(\Lambda_{\text{base}})$. For instance if $T = 2N$, $\Lambda_{\text{base}} = \mathbb{Z}[i]^T$ mapping $\phi$ is the reduction modulo $p$:

$$\phi(a_1 + b_1 i, a_2 + b_2 i, \ldots, a_N + b_N i) = (a_1 \mod p, b_1 \mod p, a_2 \mod p, b_2 \mod p, \ldots, a_N \mod p, b_N \mod p).$$

we recover an analogue to Loeliger’s (mod-p) Construction A [12]. In this case we obtain a nested lattice between $\mathbb{Z}[i]^T$ and $pZ[i]^T$. More refined “direct” constructions can be obtained by using number theory and prime ideals of $\mathbb{Z}[i]$. Notice that, for this construction, if $C_1 \subset C_2$, we obtain two nested lattices $\Lambda(C_1) \subset \Lambda(C_2)$, from where we can perform coset codes. We choose the “reliability lattice” $\Lambda_0 = \Lambda(C_2)$, the “secrecy lattice” $\Lambda_\varepsilon = \Lambda(C_1)$. The parameters of the code are chosen according to the achievable rates, and will be describe more carefully later on.

2) Main result: The lattice $\Lambda_\varepsilon$ controls the eavesdropper confusion, and has to be chosen in such a way that the flatness factor vanishes universally for any eavesdropper realization (universally good for secrecy), so that it does not leak any information. Our main result is the following theorem, stating the existence of schemes with vanishing probability of error and information leakage for universally any pair realizations in the compound set $S_\lambda \times S_\varepsilon$.

**Theorem 1.** There exists a sequence of pairs of nested lattices $(\Lambda_0, \Lambda_\varepsilon)_{T \to \infty}$, $\Lambda_0 \subset \Lambda_\varepsilon \subset \mathbb{C}^{nT}$, such that, as $T \to \infty$, the lattice coding scheme universally achieves any secrecy rates

$$R < (C_b - C_e - n_\varepsilon)^{+},$$
where \( m \) is the number of transmit antennas.

B. The Legitimate Channel: Reliability

It was shown in [6] that if \( X \sim D_{\Lambda_0,\sigma_0} \), then the maximum-a-posteriori (MAP) decoder for the signal \( Y_b \) is equivalent to lattice decoding of \( F_b Y_b \), where \( F_b \) is the MMSE-GDFE matrix to be defined in the sequel. We cannot claim directly that \( X \sim D_{\Lambda_0,\sigma_0} \), since the message distribution in \( M \) need not be uniform. Nevertheless, we show that reliability is still possible for all individual messages.

The full decoding process is depicted in Figure 2b. Bob first applies a filtering matrix \( F_b \) so that

\[
\widetilde{Y}_b = F_b Y_b = R_b X + W_{b,\text{eff}},
\]

where \( R_b^T R_b = H_b^T H_b + \rho_b^{-1} I \) and \( F_b^T R_b = \rho_b^{-1} H_b \). The effective noise is then

\[
W_{b,\text{eff}} = (F_b Y_b - R_b X) + F_b W_b.
\]

The next step is to decode \( \widetilde{Y}_b \) in \( R_b \Lambda_b \) in order to obtain \( Q_{R_b \Lambda_b}(\widetilde{Y}_b) \), which is then regneued into the element of the coset \( R_b \Lambda_b / R_b \Lambda_b \) through the operation mod \( R_b \Lambda_b \). We can then invert the linear transformation associated to \( R_b \) (notice that \( R_b \) is full rank) in order to obtain the coset in \( \Lambda_0 / \Lambda_b \), and re-map it to the message space \( M \) through \( f^{-1} \). Using the fact that the effective noise is sub-Gaussian [14] with parameter \( \sigma_{\text{eff}}^2 \). Therefore, as long as \( \epsilon' \approx 0 \) the probability of error tends to zero if we choose \( \Lambda_b \) to be AWGN good.

C. The Eavesdropper Channel: Semantic Security

For a fixed realization \( \mathbf{H}_e \), the key element for bounding the information leakage is the following lemma [11, Lemma 2]:

**Lemma 2.** Suppose that there exists a random variable with density \( q \) taking values in \( \mathbb{C}^{n_e \times T} \) such that \( \forall (p_{Y_e|m}, q_{Y_e}) \leq \varepsilon_T \) for all \( m \in M \). Then, for all message distributions

\[
\mathbb{E}[(M; Y_e)] \leq 2T \varepsilon_T R - 2 \varepsilon_T \log 2 \varepsilon_T.
\]

We show that if the distribution is sufficiently flat, then \( Y_e|m \) is statistically close to a multivariate Gaussian. Let \( \mathbf{H}_e \) be a completion of \( \mathbf{H}_e \) (for any completion) and therefore will also be secure.

\[
\mathbf{H}_e \sim \mathcal{N}(0, \sqrt{\Sigma_0}), \quad \text{where} \quad \varepsilon_T = \varepsilon_{\mathcal{H}_e,\Lambda_e}(\sqrt{\Sigma_0})\text{ and } \Sigma_0 = \mathbf{H}_e \mathbf{H}_e^H \sigma_e^2 I + \Sigma_3^{-1} = \mathbf{H}_e \mathbf{H}_e^H \sigma_e^2 + \sigma_e^2 I.
\]

We have thus the following bound for the information leakage (Equation (8) with \( \varepsilon_T \) replaced by \( 4 \varepsilon_T \)).

\[
I(M; Y_e) \leq 8T \varepsilon_T R - 8 \varepsilon_T \log 8 \varepsilon_T.
\]

Therefore, if the flatness factor \( \varepsilon_T = \varepsilon_{\mathcal{H}_e,\Lambda_e}(\sqrt{\Sigma_0}) = O(1/T) \), the leakage vanishes as \( T \) increases for the specific realization \( \mathcal{H}_e \). To achieve strong secrecy universally, we must, however, ensure the existence of a lattice with vanishing flatness factor for all possible \( \Sigma_3 \). The universality discussion is omitted due to space constraints (full details are available in [5]), but can be obtained similar to reliability in [6], with channel quantization. The secrecy condition, implies, in turn, that semantic security is possible for any VNR

\[
\gamma_{\mathcal{H}_e,\Lambda_e} (\sqrt{\Sigma_0}) = \frac{|\mathbf{H}_e^H H_b |^{1/n_e} T V(\Lambda_e) / n_e T |}{|\Sigma_0|^{1/n_e}} < \pi \quad \text{or} \quad (11)
\]

\[
V(\Lambda_e)^{1/n_e} T < |I + \rho_e \mathbf{H}_e^H \mathbf{H}_e|^{-1/n_e} \pi \sigma_e^2 = (\pi \sigma_e^2) e^{C_e/n_e}.
\]

Number-of-Antenna Mismatch. The last section assumed that the number of eavesdropper receive antennas is equal. However, due to universality, the arguments can be extended to any number of eavesdropper antennas. We provide a sketch of the case \( n_e < n_a \).

Let \( \mathbf{H}_e \in \mathbb{C}^{(n_a-n_e) \times n_a} \) be a completion of \( \mathbf{H}_e \) in (1) and consider the following surrogate (augmented) MIMO channel

\[
\begin{pmatrix}
Y_e \\
Y_e
\end{pmatrix} =
\begin{pmatrix}
H_e \\
\beta \Lambda_e
\end{pmatrix} X +
\begin{pmatrix}
W_e \\
W_e
\end{pmatrix},
\]

where \( \beta \mathbf{H}_e \) is scaled so that the capacity of the new channel is arbitrarily close to the original one. Indeed for any full rank completion \( \mathbf{H}_e \), from the matrix determinant lemma, we have \( |I + \rho_e \mathbf{H}_e^H \mathbf{H}_e| \geq e^{C_e} \). Therefore, by making \( \beta \rightarrow 0 \), the left-hand side tends to \( e^{C_e} \). For any signal \( X \), the information leakage of the surrogate channel is strictly greater than the original one (the the eavesdropper’s original channel is stochastically degraded with respect to the augmented one). A universally secure code for the \( n_a \times n_e \) MIMO compound channel will have vanishing information leakage for the surrogate \( n_a \times n_e \) channel (for any completion) and therefore will also be secure for the original \( n_e \times n_a \) channel.

D. Proof of Theorem 1: Achievable Secrecy Rates

From the previous subsections, semantic security can be achievable if \( \Lambda_0 \) and \( \Lambda_e \) satisfy

1) Reliability (4): \( \gamma_{R_b \Lambda_0}(\sigma_0) > \pi \epsilon \)
2) Secrecy (11): \( \gamma_{\mathcal{H}_e,\Lambda_e}(\sqrt{\Sigma_0}) < \pi \)
3) Sub-gaussianity of equivalent noise and power constraint: \( \varepsilon_{\mathcal{H}_e,\Lambda_e}(\sigma_0) \rightarrow 0 \)

The first two conditions can be satisfied for rates up to

\[
\log |I + \rho_e \mathbf{H}_e^H \mathbf{H}_e| - \log |I + \rho_e \mathbf{H}_e^H \mathbf{H}_e| - n_a
\]

nats per channel use, but the last conditions may, a priori, limit these rates to certain signal-to-noise ratio (SNR) regimes. However if condition 2) is satisfied, we automatically satisfy the condition for \( \varepsilon_{\mathcal{H}_e,\Lambda_e}(\sigma_0) \rightarrow 0 \), since

\[
V(\Lambda_e)^{1/n_e} T < V(\Lambda_e)^{1/n_e} T < \pi.
\]

Therefore if \( (\Lambda_e^T, \Lambda_e^T) \) is a sequence of nested universally-good/universally-secure pairs lattices, then we can achieve rates up to \( R \leq (C_b - C_e - n_a)^+ \).

We conjecture that this gap can be reduced with better bounds on the variational distance with respect to the flatness
factor. Theorem 1 is also a slight improvement on the main result of [11, Thm. 5] in the sense that one of the conditions on the SNR of Bob ($\text{SNR}_b > \epsilon$) is no longer needed.

V. ALGEBRAIC CONSTRUCTIONS

We close this paper with an alternative method for achieving semantic secrecy, assuming that the lattice admit an "algebraic reduction" and can absorb part of the channel state. In this method, inspired by previous works [7], [13] there is no increase in blocklength due to channel quantization and, in fact, any code which is good for the wiretap Gaussian channel can be coupled with this technique, as long as it also possesses an additional algebraic structure.

A. Algebraic Approach

Following [16], we define a lattice $\Lambda^T$ admitting algebraic reduction. In the sequel we denote the Frobenius norm of a matrix by $\|M\|_F \triangleq \sqrt{\text{tr}(M^TM)}$. 

**Definition 2.** We say that $\Lambda$ admits algebraic reduction if for any unit determinant matrix $M \in \mathbb{C}^{n_a \times n_b}$ there exists a matrix decomposition of the form $M = EU$, where $E$ and $U$ are unit-determinant satisfying the following properties:

1. $U\Lambda = \Lambda$ and
2. $\|E^{-1}\|_F \leq \alpha$ for some absolute constant $\alpha$ that does not depend on $M$.

The Golden Code is one example of lattice that admits algebraic reduction [13]. Any lattice built from the generalized Construction A admits a similar reduction. Furthermore, if we can relax the requirement (1) to include equivalence instead of equality, it is possible to exhibit constructions that admit algebraic reduction for any number of antennas [6].The proof of the following lemma shows that lattices admitting algebraic reduction has bounded flatness factor. The proof is omitted due to space constraints.

**Lemma 3.** Suppose that $\Lambda \subset \mathbb{C}^{n_a \times n_b}$ is such that its dual, $\Lambda^*$, admits algebraic reduction. Then

$$\varepsilon_{\Lambda}(\sqrt{\Sigma}) \leq \varepsilon_{\Lambda} \left( \sqrt{\alpha^{-1}(\det \Sigma)^{1/n_a}} \right).$$

Therefore, for any channel realization, a sufficient condition for the flatness factor in (11), $\varepsilon_{\Lambda}(\sqrt{\Sigma})$, to vanish is that the upper bound in Lemma 3 vanishes.

This can be achieved provided that

$$V(\Lambda) = \sqrt{n_a} < \pi e^{-C_e/n_a \alpha^{-1}} \sigma^2.$$

Notice that this last expression depends only on the determinant of $\Sigma$ or on the capacity of the eavesdropper channel, not on any individual realization. For this condition to hold, we only need a sequence of secrecy-good lattices for an eavesdropping AWGN channel with smaller noise variance (by factor $\alpha^{-1}$). Therefore, the following result holds.

**Theorem 2.** Let $(\Lambda^T, \Lambda^T)$ be a sequence of nested lattices where: (i) $\Lambda^T$ is universally good for the compound MIMO channel and (ii) $\Lambda^T$ satisfies Definition 2 and is secrecy good for the AWGN channel (Condition (12)). Then nested lattice Gaussian coding achieves any secrecy rates up to

$$R \leq \left( C_b - C_e - n_a - \alpha \log(\alpha) \right)^+. $$

Notice the extra gap with respect to Theorem 1. Although we have conjectured that the gap in Theorem 1 can be essentially removed, this is not the case for $\log \alpha$ in Theorem 2. Indeed, since $\alpha$ cannot be smaller than $\sqrt{n_a}$, this gap is always larger than $n_a \log n_a$. However the code construction can be reduced to the problem of finding good lattices for the Gaussian wiretap channel (with some additional algebraic structure), making the design potentially more practical.

REFERENCES


[14] Y. Liang, H. V. Poor, and S. Shamai. Secrecy capacity region of fading broad...