Unshared Secret Key Cryptography: Achieving Shannon's Ideal Secrecy and Perfect Secrecy

Shuiyin Liu, Yi Hong, and Emanuele Viterbo
ECSE Department, Monash University
Melbourne, VIC 3800, Australia
Email: shuiyin.liu, yi.hong, emanuele.viterbo@monash.edu

***Abstract*—In cryptography, a shared secret key is normally mandatory to encrypt the confidential message. In this work, we propose the unshared secret key (USK) cryptosystem. Inspired by the *artificial noise* (AN) technique, we align a one-time pad (OTP) secret key within the null space of a multiple-output multiple-input (MIMO) channel between transmitter and legitimate receiver, so that the OTP is not needed by the legitimate receiver to decipher, while it is fully affecting the eavesdropper's ability to decipher the confidential message. We show that the USK cryptosystem guarantees Shannon's *ideal secrecy* and *perfect secrecy*, if an infinite lattice input alphabet is used.**

I. Introduction

Security is a critical issue in wireless communications. Nowadays secure wireless information exchange relies mainly on encryption, the process of encoding information in such a way that only the receiver with the secret key can decode it. It is widely accepted that a cryptosystem should be secure in terms of *information-theoretic security*, which stems from Shannon's *perfect secrecy* [1]. Perfect secrecy is achieved when the secret message $\mathbf{u}$ and the eavesdropper's (Eve) received message $\mathbf{y}$ are mutually independent, i.e., when $I(\mathbf{u};\mathbf{y})=0$. Perfect secrecy requires a one-time pad (OTP) secret key $\mathbf{v}$ [1]. A weaker version of perfect secrecy is *ideal secrecy* [1], that is, no matter how much of $\mathbf{y}$ is intercepted by Eve, there is no unique solution of $\mathbf{u}$ and $\mathbf{v}$ but many solutions of comparable probability. This kind of cryptosystem would have information theoretic security but not perfect secrecy [1].

One of the major weakness of traditional cryptosystems is the secret key exchanging. The problem is how to protect the key from unauthorized disclosure. To overcome this limitation, we propose the unshared secret key (USK) cryptosystem based on the *artificial noise* (AN) technique [2]. We redesign the AN as a OTP aligned within the null space of a MIMO channel between transmitter (Alice) and legitimate receiver (Bob). Consequently, the OTP is not needed by Bob to decipher, while it is fully affecting Eve's ability to decipher the confidential message. In [3, 4], we introduced the prototype of USK. In this work, we refine the analysis in [4] by considering an infinite lattice constellation input alphabet. We show that the proposed USK provide Shannon's ideal and perfect secrecy, under the same channel assumptions in [2] that enable the use of the AN scheme. The extension to practical systems using finite lattice input alphabets will be reported in the journal version.

This work is supported by ARC under Grant Discovery Project No. DP130100336.

Our work differs from previous studies of AN [2, 5], because it puts forward three new aspects:

1) *Shannon's secrecy*: we aim at achieving Shannon's ideal and perfect secrecy, rather than positive secrecy capacity.
2) *Artificial noise*: we have no special requirement of the distribution of AN; that is, not necessarily Gaussian.
3) *Secrecy outage*: we show that Shannon's ideal secrecy can be achieved with an arbitrarily small outage probability, when the number of antennas at each terminal is finite.

Section II presents the system model. Section III describes the USK cryptosystem with infinite lattice constellations. Section IV analyzes the security of the USK cryptosystem. Section V sets out the theoretical and practical conclusions. The Appendix contains the proofs of the theorems.

Notation: Matrices and column vectors are denoted by upper and lowercase boldface letters, and the Hermitian transpose, inverse, pseudo-inverse of a matrix $\mathbf{B}$ by $\mathbf{B}^H$, $\mathbf{B}^{-1}$, and $\mathbf{B}^\dagger$, respectively. Let $\{X_n, X\}$ be random variables defined on the same probability space. We write $X_n \overset{a.s.}{\to} X$, if X_n converges to X almost surely or with probability one. We use the standard asymptotic notation $f(x) = O(g(x))$ when $\limsup_{x\to\infty} |f(x)/g(x)| < \infty$. The real, complex, integer, and complex integer numbers are denoted by $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$, and $\mathbb{Z}[i]$, respectively. $H(\cdot)$, $H(\cdot|\cdot)$, and $I(\cdot;\cdot)$ represent entropy, conditional entropy, and mutual information, respectively.

II. System Model

The MIMO wiretap system model is given as follows. The number of antennas at the transmitter (Alice), the intended receiver (Bob), and the passive eavesdropper (Eve) are denoted by $N_{\rm A}$, $N_{\rm B}$, and $N_{\rm E}$, respectively. Alice transmits the information signal $\mathbf{x}$, and Bob and Eve receive $\mathbf{z}$ and $\mathbf{y}$, respectively,

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{n}_{\rm B}, \quad (1)$$

$$\mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{n}_{\rm E}, \quad (2)$$

where $\mathbf{H} \in \mathbb{C}^{N_{\rm B}\times N_{\rm A}}$ and $\mathbf{G} \in \mathbb{C}^{N_{\rm E}\times N_{\rm A}}$ are the channel matrices of Bob and Eve. We assume that all the channel matrix elements are i.i.d. $\mathcal{N}_{\mathbb{C}}(0,\,1)$ random variables (i.e., Bob and Eve are not co-located). We assume that the noise vectors

$\mathbf{n}_{\mathrm{B}}$ and $\mathbf{n}_{\mathrm{E}}$ have i.i.d. $\mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{B}}^2)$ and $\mathcal{N}_{\mathbb{C}}(0,\, \sigma_{\mathrm{E}}^2)$ components, respectively. Furthermore, we assume that

1) Alice knows the realization of $\mathbf{H}$ and the statistics of $\mathbf{G}$, which varies in each transmission.
2) Eve knows the realizations of $\mathbf{H}$ and $\mathbf{G}$.

Our secure transmission strategy is based on the artificial noise scheme [2], which is summarized below.

A. Artificial Noise Scheme

In the AN scheme [2], N_{B} is assumed to be smaller than N_{A}, thus $\mathbf{H}$ has a non-trivial null space with an orthonormal basis given by columns of the matrix $\mathbf{Z} = \mathrm{null}(\mathbf{H}) \in \mathbb{C}^{N_{\mathrm{A}} \times (N_{\mathrm{A}} - N_{\mathrm{B}})}$. Let $\mathbf{u} \in \mathbb{C}^{N_{\mathrm{B}} \times 1}$ be the transmitted vector carrying the information, and let $\mathbf{v} \in \mathbb{C}^{(N_{\mathrm{A}} - N_{\mathrm{B}}) \times 1}$ represent the "artificial noise" generated by Alice, which is unknown to Bob and Eve.

Alice performs *SVD precoding* and transmits

$$\mathbf{x} = \mathbf{V} \begin{bmatrix} \mathbf{u} \\ \mathbf{v} \end{bmatrix} = \mathbf{V}_1 \mathbf{u} + \mathbf{Z}\mathbf{v}, \tag{3}$$

where the columns of $\mathbf{V} = [\mathbf{V}_1,\, \mathbf{Z}]$ are the right-singular vectors of $\mathbf{H}$ (i.e., $\mathbf{H} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^H$, where $\mathbf{U} \in \mathbb{C}^{N_{\mathrm{B}} \times N_{\mathrm{B}}}$, $\mathbf{\Lambda} \in \mathbb{C}^{N_{\mathrm{B}} \times N_{\mathrm{A}}}$, $\mathbf{V} \in \mathbb{C}^{N_{\mathrm{A}} \times N_{\mathrm{A}}}$, $\mathbf{U}^H\mathbf{U} = \mathbf{I}_{N_{\mathrm{B}}}$, $\mathbf{V}^H\mathbf{V} = \mathbf{I}_{N_{\mathrm{A}}}$).

Due to the orthogonality between $\mathbf{V}_1$ and $\mathbf{Z}$, the total transmission power $||\mathbf{x}||^2$ can be written as

$$||\mathbf{x}||^2 = ||\mathbf{u}||^2 + ||\mathbf{v}||^2. \tag{4}$$

Alice has an average transmit power constraint P, i.e.,

$$P \geq \mathrm{E}(||\mathbf{x}||^2) = \mathrm{E}(||\mathbf{u}||^2) + \mathrm{E}(||\mathbf{v}||^2). \tag{5}$$

The AN scheme in [2] is based on the assumptions below:

1) $\mathbf{u}$ and $\mathbf{v}$ are assumed to be Gaussian random vectors.
2) $N_{\mathrm{A}} > N_{\mathrm{B}}$, $N_{\mathrm{A}} > N_{\mathrm{E}}$ and $N_{\mathrm{E}} \geq N_{\mathrm{B}}$

The condition $N_{\mathrm{E}} \geq N_{\mathrm{B}}$ guarantees that Eve has at least the same number of degree of freedom as Bob.

Equations (1) and (2) can then be rewritten as

$$\mathbf{z} = \mathbf{H}\mathbf{V}_1\mathbf{u} + \mathbf{n}_{\mathrm{B}}, \tag{6}$$

$$\mathbf{y} = \mathbf{G}\mathbf{V}_1\mathbf{u} + \mathbf{G}\mathbf{Z}\mathbf{v} + \mathbf{n}_{\mathrm{E}}. \tag{7}$$

and show that $\mathbf{v}$ only degrades Eve's reception, but not Bob's.

The purpose of the AN scheme is to ensure a positive secrecy capacity [2]. To achieve such secrecy capacity, explicit wiretap codes are required.

B. Proposed AN Scheme

Different from the original AN scheme [2], we use the following assumptions in our proposed scheme.

1) We use infinite lattice constellations $\mathbf{u} \in \mathbb{Z}[i]^{N_{\mathrm{B}}}$, satisfying an average transmit power constraint.
2) We set a peak AN power constraint, $P_{\mathrm{v}} \geq ||\mathbf{v}||^2$.

We focus on information theoretic security, hence, our analysis will focus on Eve's equivocation $H(\mathbf{u}|\mathbf{y})$.

Throughout the paper, we consider the *worst-case* scenario (for Alice) that Eve's channel is noiseless, i.e.,

$$\mathbf{y} = \mathbf{G}\mathbf{V}_1\mathbf{u} + \mathbf{G}\mathbf{Z}\mathbf{v}. \tag{8}$$

Using *Data Processing Inequality*, it is simple to show that Eve's channel noise can only increase her equivocation:

$$H(\mathbf{u}|\mathbf{G}\mathbf{V}_1\mathbf{u} + \mathbf{G}\mathbf{Z}\mathbf{v}) \leq H(\mathbf{u}|\mathbf{G}\mathbf{V}_1\mathbf{u} + \mathbf{G}\mathbf{Z}\mathbf{v} + \mathbf{n}_{\mathrm{E}}).$$

C. Shannon's Secrecy

We consider a cryptosystem where a sequence of K messages $\{\mathbf{m}_i\}_1^K$ are enciphered into the cryptograms $\{\mathbf{y}_i\}_1^K$ using a sequence of secret keys $\{k_i\}_1^K$. We recall from [1] the definition of Shannon's ideal secrecy and perfect secrecy.

Definition 1: A secrecy system is *ideal* when

$$\begin{aligned} \lim_{K\to\infty} H(\{\mathbf{m}_i\}_1^K \,|\, \{\mathbf{y}_i\}_1^K) &\neq 0, \\ \lim_{K\to\infty} H(\{k_i\}_1^K \,|\, \{\mathbf{y}_i\}_1^K) &\neq 0. \end{aligned} \tag{9}$$

Definition 2: A secrecy system is *perfect* when

$$H(\{\mathbf{m}_i\}_1^K \,|\, \{\mathbf{y}_i\}_1^K) = H(\{\mathbf{m}_i\}_1^K). \tag{10}$$

In the special case that $\{\mathbf{m}_i\}_1^K$ and $\{k_i\}_1^K$ are mutually independent, using the entropy chain rule, ideal secrecy is achieved if $H(\mathbf{m}_i|\mathbf{y}_i) \neq 0$ and $H(k_i|\mathbf{y}_i) \neq 0$ for at least some i. To protect all the messages, we can use a stronger condition:

$$H(\mathbf{m}_i|\mathbf{y}_i) \neq 0 \text{ and } H(k_i|\mathbf{y}_i) \neq 0, \text{ for all } i, \tag{11}$$

as our design criterion for ideal secrecy.

In this case, perfect secrecy is achieved when

$$H(\mathbf{m}_i|\mathbf{y}_i) = H(\mathbf{m}_i), \text{ for all } i. \tag{12}$$

D. Lattice Preliminaries

To describe our scheme, it is convenient to introduce some lattice preliminaries. An n-dimensional *complex lattice* $\Lambda_{\mathbb{C}}$ in a complex space $\mathbb{C}^m$ $(n \leq m)$ is the discrete set defined by:

$$\Lambda_{\mathbb{C}} = \left\{\mathbf{B}\mathbf{u}\colon \mathbf{u} \in \mathbb{Z}[i]^n\right\},$$

where the *basis* matrix $\mathbf{B} = [\mathbf{b}_1 \cdots \mathbf{b}_n]$ has linearly independent columns.

$\Lambda_{\mathbb{C}}$ can also be easily represented as $2n$-dimensional *real* lattice $\Lambda_{\mathbb{R}}$ [6]. In what follows, we introduce some lattice parameters of $\Lambda_{\mathbb{C}}$, which have a corresponding value for $\Lambda_{\mathbb{R}}$.

The *Voronoi region* of $\Lambda_{\mathbb{C}}$, defined by

$$\mathcal{V}_i(\Lambda_{\mathbb{C}}) = \left\{\mathbf{y} \in \mathbb{C}^m\colon \|\mathbf{y} - \mathbf{x}_i\| \leq \|\mathbf{y} - \mathbf{x}_j\|, \forall\, \mathbf{x}_i \neq \mathbf{x}_j\right\},$$

gives the nearest neighbor decoding region of lattice point $\mathbf{x}_i$.

The volume of any $\mathcal{V}_i(\Lambda_{\mathbb{C}})$, defined as $\mathrm{vol}(\Lambda_{\mathbb{C}}) \triangleq |\det(\mathbf{B}^H\mathbf{B})|$, is equivalent to the volume of the corresponding real lattice.

III. Unshared Secret Key Cryptosystem

In this section, we consider the system model with an infinite lattice constellation, satisfying the average transmit power constraint. This provides the theoretical basis for unshared secret key cryptosystems.

A. Encryption

We consider a sequence of K mutually independent messages $\{\mathbf{m}_i\}_1^K$, where each $\mathbf{m}$ is mapped to a transmitted vector $\mathbf{u} \in \mathbb{Z}[i]^{N_\mathrm{B}}$. The probability distribution of $\mathbf{u}$ can be arbitrary, but has finite $\mathrm{E}(||\mathbf{u}||^2)$. To secure the K transmitted vectors $\{\mathbf{u}_i\}_1^K$, Alice enciphers $\{\mathbf{u}_i\}_1^K$ into the cryptograms $\{\mathbf{y}_i\}_1^K$ using a sequence of mutually independent secret keys $\{\mathbf{v}_i\}_1^K$. We assume that $\{\mathbf{v}_i\}_1^K$ and $\{\mathbf{u}_i\}_1^K$ are mutually independent, and $\{\mathbf{G}_i\}_1^K$ are mutually independent Gaussian random matrices. No assumption is needed about the statistics of $\{\mathbf{H}_i\}_1^K$ across the K channel uses, since its realization is known to both Alice and Eve.

Since $\{\mathbf{v}_i\}_1^K$ and $\{\mathbf{u}_i\}_1^K$ are mutually independent, from (11) and (12), we only need to demonstrate the encryption process for one transmitted vector $\mathbf{u}_i$. For simplicity, we drop the subscript i.

For each $\mathbf{u}$, Alice randomly and independently (without any predefined distribution) chooses a one-time pad secret key $\mathbf{v}$, from a ball of radius $\sqrt{P_\mathrm{v}}$:

$$S \triangleq \left\{\mathbf{v} \in \mathbb{C}^{N_\mathrm{A}-N_\mathrm{B}}\colon ||\mathbf{v}||^2 \le P_\mathrm{v}\right\}, \tag{13}$$

and transmits

$$\mathbf{x} = \mathbf{V}_1\mathbf{u} + \mathbf{Z}\mathbf{v}. \tag{14}$$

In the worst-case scenario, when $\mathbf{n}_\mathrm{E} = \mathbf{0}$, Eve will receive

$$\mathbf{y} = \mathbf{G}\mathbf{V}_1\mathbf{u} + \tilde{\mathbf{n}}_\mathrm{v}, \tag{15}$$

where $\tilde{\mathbf{n}}_\mathrm{v} = \mathbf{G}\mathbf{Z}\mathbf{v}$.

The message $\mathbf{u}$ is received by Eve as a lattice point (see Fig. 1) in:

$$\Lambda_\mathbb{C} = \{\mathbf{G}\mathbf{V}_1\mathbf{u}, \mathbf{u} \in \mathbb{Z}[i]^{N_\mathrm{B}}\}. \tag{16}$$

This enables us to partition the set S into D disjoint subsets S_1, ..., S_D, such that

$$S = \bigcup_{k=1}^{D} S_k, \tag{17}$$

where

$$S_k \triangleq \left\{\mathbf{v}\colon \mathbf{G}\mathbf{V}_1\mathbf{u} \in \Lambda_\mathbb{C} \text{ is the } k^{\text{th}} \text{ closest lattice point to } \mathbf{y}\right\}. \tag{18}$$

As shown in Fig. 1, the value of D is determined by

$$D = |S_{R_{\max}} \cap \Lambda_\mathbb{C}|, \tag{19}$$

where $S_{R_{\max}}$ is a sphere centered at $\mathbf{y}$ with radius

$$R_{\max}(P_\mathrm{v}) \triangleq \max_{||\mathbf{v}||^2 \le P_\mathrm{v}} \|\mathbf{G}\mathbf{Z}\mathbf{v}\| = \sqrt{\lambda_{\max} P_\mathrm{v}}, \tag{20}$$

where $\lambda_{\max}$ is the largest eigenvalue of $(\mathbf{G}\mathbf{Z})^H(\mathbf{G}\mathbf{Z})$.

Assuming $\mathbf{v} \in S_k$, $1 \le k \le D$, the signal model in (15) can be viewed as an encryption algorithm that encrypts $\mathbf{u}$ to $\mathbf{y}$ using a one time pad secret key $\mathbf{v}$, such that $\mathbf{G}\mathbf{V}_1\mathbf{u}$ is the k^{th} closest lattice point to $\mathbf{y}$.

The security problem lies in how much Eve knows about k. The value of k is uniquely determined by the vector $\tilde{\mathbf{n}}_\mathrm{v}$. Since we assume that the realizations of $\mathbf{G}$ and $\mathbf{Z}$ are known to Eve, k is a function of $\mathbf{v}$. Since $\mathbf{v}$ is randomly and independently selected by Alice and is never disclosed to anyone, Eve can neither know its realization nor its distribution. Thus, given $\mathbf{y}$, Eve is not able to estimate the distribution of the index k, or more specifically, she only knows that $\mathbf{G}\mathbf{V}_1\mathbf{u} \in S_{R_{\max}} \cap \Lambda_\mathbb{C}$.

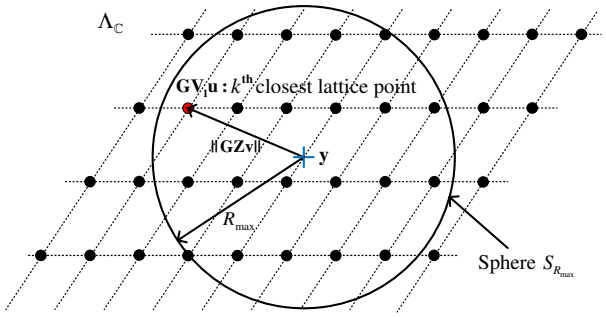

Fig. 1. The USK cryptosystem with infinite constellations.

Remark 1: The index k can be interpreted as the *effective* one-time pad secret key, whose randomness comes from the artificial noise. The effective key space size is D.

Remark 2: Different from Shannon's one-time pad cryptosystem, the effective one-time pad secret key k is not pre-shared between Alice and Bob. This motivates the name of this cryptosystem as *Unshared Secret Key* (USK) cryptosystem.

B. Analyzing Eve's Equivocation

Suppose that Eve knows P_v, $R_{\max}(P_\mathrm{v})$, D and the encryption process (15). The posterior probability that Eve obtains $\mathbf{u}$, or equivalently, finds k, from the cryptogram $\mathbf{y}$, is

$$\Pr\{\mathbf{u}|\mathbf{y}\} = \Pr\{k|\mathbf{y}\} = \Pr\{\mathbf{u}|\mathbf{u} \in \mathcal{U}\}, \tag{21}$$

where

$$\mathcal{U} \triangleq \left\{\mathbf{u}'\colon \mathbf{G}\mathbf{V}_1\mathbf{u}' \in S_{R_{\max}} \cap \Lambda_\mathbb{C}\right\}. \tag{22}$$

For any $\mathbf{u}' \in \mathcal{U}$, using Bayes' theorem, we have

$$\Pr\{\mathbf{u} = \mathbf{u}'|\mathbf{u} \in \mathcal{U}\} = \frac{\Pr\{\mathbf{u} = \mathbf{u}'\}}{\Pr\{\mathbf{u} \in \mathcal{U}\}}. \tag{23}$$

Using (21) and (23), Eve's equivocation is given by

$$H(\mathbf{u}|\mathbf{y}) = H(k|\mathbf{y}) = \sum_{\mathbf{u}' \in \mathcal{U}} \frac{\Pr\{\mathbf{u} = \mathbf{u}'\}}{\Pr\{\mathbf{u} \in \mathcal{U}\}} \log \frac{\Pr\{\mathbf{u} \in \mathcal{U}\}}{\Pr\{\mathbf{u} = \mathbf{u}'\}}. \tag{24}$$

Since $\Pr\{\mathbf{u} \in \mathcal{U}\} = \sum_{\mathbf{u}' \in \mathcal{U}} \Pr\{\mathbf{u} = \mathbf{u}'\}$ and $|\mathcal{U}| = D$,

1) if $D \ge 2$, then $\Pr\{\mathbf{u} \in \mathcal{U}\} > \Pr\{\mathbf{u} = \mathbf{u}'\}$, so that

$$H(k|\mathbf{y}) = H(\mathbf{u}|\mathbf{y}) > 0. \qquad \text{(ideal secrecy)}$$

2) if $D \to \infty$, then $\Pr\{\mathbf{u} \in \mathcal{U}\} \to 1$, so that

$$H(k|\mathbf{y}) = H(\mathbf{u}|\mathbf{y}) = H(\mathbf{u}). \qquad \text{(perfect secrecy)}$$

As shown above, Eve's equivocation depends on the value of D, which is known to Eve but not to Alice. We then estimate the value of D from Alice's perspective. According to (17) and (18), D is a function of $\mathbf{G}$. Although Alice cannot know the exact value of D, she is able to estimate its cumulative distribution function (cdf), denoted by

$$F_D(d,\, P_\mathrm{v}) \triangleq \Pr\{D < d\}, \tag{25}$$

where d is a positive integer.

In the next section, we will show that Alice can ensure $F_D(d,\, P_\mathrm{v}) \to 0$ by increasing P_v, i.e., she can guarantee that $D \ge d$, for any given d.

IV. The Security of USK

To prove the main theorems, we first introduce some lemmas. We first define

$$\kappa(d) \triangleq d^{1/(2N_{\rm E})}/\sqrt{\pi} \text{ and } \Delta(d) \triangleq \frac{\kappa(d)^{2N_{\rm E}}\text{vol}(\Lambda_{\mathbb{C}})}{P_{\rm v}^{N_{\rm E}}}, \quad (26)$$

where d is a positive integer and

$$\text{vol}(\Lambda_{\mathbb{C}}) = |\det((\mathbf{G}\mathbf{V}_1)^H(\mathbf{G}\mathbf{V}_1))|. \quad (27)$$

Here, $\mathbf{G}$ is a complex Gaussian random matrix, while $\mathbf{V}_1$ is deterministic. Thus, $\Delta(d)$ is a random variable from Alice perspective. The following two lemmas are used to evaluate $F_D(d,\, P_{\rm v})$ in (25).

Lemma 1: If $P_{\rm v} = \rho^2/\Phi^{2N_{\rm B}/N_{\rm E}}$ and $\rho > \kappa(d)$, then $\Delta(d) \overset{a.s.}{\to} 0$ as $N_{\rm B} \to \infty$, or equivalently,

$$\Pr\left\{\Delta(d) > \left(\frac{\rho}{\kappa(d)}\right)^{-N_{\rm B}}\right\} < O\left(\left(\frac{\rho}{\kappa(d)}\right)^{-N_{\rm B}}\right) \quad (28)$$

where

$$\Phi = \left[\frac{(N_{\rm E}-N_{\rm B})!}{N_{\rm E}!}\right]^{\frac{1}{2N_{\rm B}}}. \quad (29)$$

Proof: See Appendix A. ∎

We next provide a more accurate expression of the tail distribution of $\Delta(d)$ for finite $N_{\rm B}$.

Lemma 2: If $P_{\rm v} = \rho^2/\Phi^{2N_{\rm B}/N_{\rm E}}$ and $\rho > \kappa(d)$, then

$$\Pr\left\{\Delta(d) > \left(\frac{\rho}{\kappa(d)}\right)^{-N_{\rm B}}\right\} < \Upsilon\left(\frac{\rho}{\kappa(d)}\right), \quad (30)$$

where $\kappa(d)$ is given in (26), Φ is given (29), and

$$\Upsilon(x) = \sum_{i=1}^{N_{\rm B}} \left(xe^{1-x}\right)^{N_{\rm E}-i+1}. \quad (31)$$

Proof: See Appendix B. ∎

Lemmas 1 and 2 enable us to prove the following lemma.

Lemma 3: If $P_{\rm v} = \rho^2/\Phi^{2N_{\rm B}/N_{\rm E}}$ and $\rho > \kappa(d)$, $F_D(d, P_{\rm v}) \to 0$ as $N_{\rm B} \to \infty$, or equivalently,

$$F_D(d, P_{\rm v}) < O\left(\left(\frac{\rho}{\kappa(d)}\right)^{-N_{\rm B}}\right), \quad (32)$$

and for finite $N_{\rm B}$, we have

$$F_D(d, P_{\rm v}) < \left(\frac{\rho}{\kappa(d)}\right)^{-N_{\rm B}} + \Upsilon\left(\frac{\rho}{\kappa(d)}\right), \quad (33)$$

where $\kappa(d)$ is given in (26), Φ is given in (29), and $\Upsilon(x)$ is given in (31).

Proof: See Appendix C. ∎

A. Achieving Ideal Secrecy and Secrecy Outage

From (11) and the discussion following (24), ideal secrecy is achieved when $D \geq 2$.

Theorem 1: If $P_{\rm v} > \kappa(d)^2/\Phi^{2N_{\rm B}/N_{\rm E}}$ and $d \geq 2$, as $N_{\rm B} \to \infty$,

$$D \overset{a.s.}{\geq} d, \quad (34)$$

where $\kappa(d)$ is given in (26) and Φ is given in (29).

Proof: Using Lemma 3, the proof is straightforward. ∎

Theorem 1 shows that for the USK, Eve cannot find a unique solution $\mathbf{u}$, since D is almost surely greater than 2.

We next estimate the *secrecy outage probability* when $N_{\rm B}$ is finite, defined by

$$P_{\text{out}}(d) \triangleq \Pr\{D < d\} = F_D(d,\, P_{\rm v}), \quad (35)$$

for any $d \geq 2$.

Theorem 2: Let $N_{\min} = \min\{N_{\rm E} - N_{\rm B} + 1,\, N_{\rm B}\}$. If

$$P_{\rm v} = \varepsilon^{-2/N_{\min}}\kappa(d)^2/\Phi^{2N_{\rm B}/N_{\rm E}} \quad (36)$$

and $d \geq 2$, then

$$P_{\text{out}}(d) < O(\varepsilon), \quad (37)$$

for any arbitrarily small $\varepsilon > 0$, i.e., ideal secrecy is achieved with probability $1 - O(\varepsilon)$, where $\kappa(d)$ is given in (26) and Φ is given in (29).

Proof: Using Lemma 3, the proof is straightforward. ∎

Theorem 2 shows that for finite $N_{\rm B}$, the outage of ideal secrecy can be made arbitrarily small by increasing $P_{\rm v}$.

B. Achieving Perfect Secrecy

From (12), perfect secrecy requires

$$H(\mathbf{u}|\mathbf{y}) = H(\mathbf{u}). \quad (38)$$

According to (24), the problem then reduces to ensuring $D \to \infty$. From Theorems 1 and 2, perfect secrecy requires infinite AN peak power $P_{\rm v}$, which is of theoretical interest only.

C. Discussions

We remark that the USK cryptosystem with $D \geq 2$ is already cryptanalytically unbreakable, since Eve simply does not have enough information to identify $\mathbf{u}$ (see Fig. 1).

Most recently, we have shown that the constraint $N_{\rm E} < N_{\rm A}$ can be removed by combining the USK scheme with cooperative jamming technique in [7].

V. Conclusions

We proposed an unshared secret key (USK) cryptosystem based on the artificial noise technique. For large $N_{\rm B}$, the proposed scheme provides Shannon's ideal secrecy and perfect secrecy, by simply increasing the power allocated to the artificial noise component. For finite $N_{\rm B}$, we have shown that ideal secrecy can be obtained with an arbitrarily small outage.

Appendix

A. Proof of Lemma 1

Recalling that

$$\Delta(d) = \frac{\kappa(d)^{2N_{\rm E}}|\det((\mathbf{G}\mathbf{V}_1)^H(\mathbf{G}\mathbf{V}_1))|}{P_{\rm v}^{N_{\rm E}}}. \quad (39)$$

From Alice's perspective, $\mathbf{G}$ is a complex Gaussian random matrix. The matrix $\mathbf{V}_1$ with orthonormal columns is known. According to [8], $\mathbf{G}\mathbf{V}_1$ a Gaussian random matrix with i.i.d. elements. Moreover, $|\det((\mathbf{G}\mathbf{V}_1)^H(\mathbf{G}\mathbf{V}_1))|$ can be expressed as the product of independent Chi-squared variables [9]:

$$|\det((\mathbf{G}\mathbf{V}_1)^H(\mathbf{G}\mathbf{V}_1))| = \prod_{i=1}^{N_{\rm B}} \frac{1}{2}\mathcal{X}^2\left(2(N_{\rm E}-i+1)\right). \quad (40)$$

Using the properties of the Chi-squared distribution and the central limit theorem, it is simple to show that as $N_{\rm B} \to \infty$, if $P_{\rm v} = \rho^2/\Phi^{2N_{\rm B}/N_{\rm E}}$, where Φ is given in (29),

$$\begin{aligned}\Pr\left\{\Delta(d) > (\rho/\kappa(d))^{-N_{\rm B}}\right\} &< 1/2\exp\left(-\frac{N_{\rm B}^2\log^2(\rho/\kappa(d))}{2\log 2N_{\rm B}}\right)\\ &= O\left((\rho/\kappa(d))^{-N_{\rm B}}\right), \end{aligned} \quad (41)$$

i.e., if $\rho > \kappa(d)$, $\Delta(d) \overset{a.s.}{\to} 0$ as $N_{\rm B} \to \infty$. A more detailed proof will be reported in the journal version. ■

B. Proof of Lemma 2

We recall (39) and (40) and consider the random variable

$$\Psi \triangleq \prod_{i=1}^{N_{\rm B}} \frac{\mathcal{X}^2\left(2(N_{\rm E}-i+1)\right)}{2(N_{\rm E}-i+1)}. \quad (42)$$

Recalling that $N_{\rm E} \geq N_{\rm B}$. By substituting Ψ, $P_{\rm v} = \rho^2/\Phi^{2N_{\rm B}/N_{\rm E}}$ and $\rho > \kappa(d)$ to the right side of (39), we have

$$\Delta(d) = (\rho/\kappa(d))^{-2N_{\rm E}}\,\Psi \leq (\rho/\kappa(d))^{-2N_{\rm B}}\,\Psi.$$

Consequently, we obtain

$$\begin{aligned}&\Pr\left\{\Delta(d) > (\rho/\kappa(d))^{-N_{\rm B}}\right\}\\ &\leq \Pr\left\{\Psi > (\rho/\kappa(d))^{N_{\rm B}}\right\}\\ &\overset{a}{\leq} \Pr\left\{\sum_{i=1}^{N_{\rm B}} \frac{\mathcal{X}^2\left(2(N_{\rm E}-i+1)\right)}{2(N_{\rm E}-i+1)} > N_{\rm B}\rho/\kappa(d)\right\}\\ &< \sum_{i=1}^{N_{\rm B}} \Pr\left\{\mathcal{X}^2\left(2(N_{\rm E}-i+1)\right) \geq 2(N_{\rm E}-i+1)\rho/\kappa(d)\right\}\\ &\leq \sum_{i=1}^{N_{\rm B}} \left(e^{1-\rho/\kappa(d)}\rho/\kappa(d)\right)^{N_{\rm E}-i+1} \triangleq \Upsilon(\rho/\kappa(d)),\end{aligned}$$

where (a) holds due to the inequality of arithmetic and geometric means. ■

C. Proof of Lemma 3

We pick an element $\mathbf{v}_0$ from $\mathcal{S}$ with $||\mathbf{v}_0||^2 = P_{\rm v}$. Suppose that $\mathbf{v}_0 \in S_{k_0}$, where k_0 is the corresponding effective secret key. Since $D \geq k_0$, we have

$$F_D(d, P_{\rm v}) = \Pr\{D < d\} < \Pr\{k_0 \leq d\}. \quad (43)$$

The problem then reduces to evaluating $\Pr\{k_0 \leq d\}$.

Let $\mathcal{S}_R$ be a sphere of radius $R \leq R_{\max}(P_{\rm v})$ centered at $\mathbf{y}$, where $\mathrm{vol}(\mathcal{S}_R) = d{\cdot}\mathrm{vol}(\Lambda_{\mathbb{C}})$ (see Fig. 1). Let K be the number of the points in $\mathcal{S}_R \cap \Lambda_{\mathbb{C}}$. We have

$$K \approx \frac{\mathrm{vol}(\mathcal{S}_R)}{\mathrm{vol}(\Lambda_{\mathbb{C}})} = d. \quad (44)$$

If $\mathbf{GV}_1\mathbf{u} \in \mathcal{S}_R$, we have $k_0 \leq d$, and vice versa. Thus, the two events are equivalent, i.e.,

$$\Pr\{k_0 \leq d\} = \Pr\{\mathbf{GV}_1\mathbf{u} \in \mathcal{S}_R\}. \quad (45)$$

Let $\mathcal{S}'_R$ be a sphere with the same radius R centered at $\mathbf{GV}_1\mathbf{u}$. If $\mathbf{GV}_1\mathbf{u} \in \mathcal{S}_R$, then $\mathbf{y} \in \mathcal{S}'_R$, and vice versa. Thus, the two events are equivalent, i.e.,

$$\Pr\{\mathbf{GV}_1\mathbf{u} \in \mathcal{S}_R\} = \Pr\{\mathbf{y} \in \mathcal{S}'_R\}. \quad (46)$$

From (43), (45) and (46), we have

$$\begin{aligned}&F_D(d, P_{\rm v})\\ <\ &\Pr\{\mathbf{y} \in \mathcal{S}'_R\}\\ =\ &\Pr\{\mathbf{y} \in \mathcal{S}'_R|\mathrm{vol}(\mathcal{S}'_R) \leq C\}\cdot\Pr\{\mathrm{vol}(\mathcal{S}'_R) \leq C\} +\\ &\Pr\{\mathbf{y} \in \mathcal{S}'_R|\mathrm{vol}(\mathcal{S}'_R) > C\}\cdot\Pr\{\mathrm{vol}(\mathcal{S}'_R) > C\}\\ <\ &\Pr\{\mathbf{y} \in \mathcal{S}'_R|\mathrm{vol}(\mathcal{S}'_R) \leq C\} + \Pr\{\mathrm{vol}(\mathcal{S}'_R) > C\}, \end{aligned} \quad (47)$$

where C is a positive number.

We then evaluate the two terms in (47) separately. We use the same settings as Lemmas 1 and 2, i.e., $P_{\rm v} = \rho^2/\Phi^{2N_{\rm B}/N_{\rm E}}$, $\rho > \kappa(d)$. We set

$$C = \pi^{N_{\rm E}} P_{\rm v}^{N_{\rm E}} (\rho/\kappa(d))^{-N_{\rm B}}. \quad (48)$$

1) $\Pr\{\mathbf{y} \in \mathcal{S}'_R|\mathrm{vol}(\mathcal{S}'_R) \leq C\}$*:* Let $\mathcal{S}_{\rm C}$ be a sphere centered at $\mathbf{GV}_1\mathbf{u}$, where $\mathrm{vol}(\mathcal{S}_{\rm C}) = C$. Let $\mathcal{S}_{\rm C0}$ be a sphere centered at the origin, where $\mathrm{vol}(\mathcal{S}_{\rm C0}) = C$. Recalling that Alice knows $\mathbf{Z}$ and $\mathbf{v}_0$. From Alice perspective, $\tilde{\mathbf{n}}_{\rm v} = \mathbf{GZ}\mathbf{v}_0$ has i.i.d. $\mathcal{N}_{\mathbb{C}}(0, P_{\rm v})$ components [8]. Therefore, we have

$$\begin{aligned}&\Pr\{\mathbf{y} \in \mathcal{S}'_R|\mathrm{vol}(\mathcal{S}'_R) \leq C\} \leq \Pr\{\mathbf{y} \in \mathcal{S}_{\rm C}\}\\ &= \int_{\mathcal{S}_{\rm C0}} f(\tilde{\mathbf{n}}_{\rm v})d\tilde{\mathbf{n}}_{\rm v} \leq \frac{C}{\pi^{N_{\rm E}}P_{\rm v}^{N_{\rm E}}} = (\rho/\kappa(d))^{-N_{\rm B}}, \end{aligned} \quad (49)$$

where $f(\tilde{\mathbf{n}}_{\rm v})$ is the probability density function (pdf) of $\tilde{\mathbf{n}}_{\rm v}$. The last inequality holds since

$$f(\tilde{\mathbf{n}}_{\rm v}) = \frac{1}{\pi^{N_{\rm E}}P_{\rm v}^{N_{\rm E}}}\exp\left(-\frac{||\tilde{\mathbf{n}}_{\rm v}||^2}{P_{\rm v}}\right) \leq \frac{1}{\pi^{N_{\rm E}}P_{\rm v}^{N_{\rm E}}}. \quad (50)$$

2) $\Pr\{\mathrm{vol}(\mathcal{S}'_R) > C\}$*:* Since $\mathrm{vol}(\mathcal{S}'_R) = d{\cdot}\mathrm{vol}(\Lambda_{\mathbb{C}})$, we have

$$\Pr\{\mathrm{vol}(\mathcal{S}'_R) > C\} = \Pr\left\{\Delta(d) > (\rho/\kappa(d))^{-N_{\rm B}}\right\}. \quad (51)$$

From (47), (49), (51) and (28), as $N_{\rm B} \to \infty$,

$$F_D(d, P_{\rm v}) < O\left(\left(\frac{\rho}{\kappa(d)}\right)^{-N_{\rm B}}\right). \quad (52)$$

From (47), (49), (51) and (30), when $N_{\rm B}$ is finite,

$$F_D(d, P_{\rm v}) < \left(\frac{\rho}{\kappa(d)}\right)^{-N_{\rm B}} + \Upsilon\left(\frac{\rho}{\kappa(d)}\right). \quad (53)$$

■

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Confidential report*, 1946.

[2] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, Jun. 2008.

[3] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Communications Letters*, vol. 17, no. 7, pp. 1483–1486, 2013.

[4] ——, "Unshared secret key cryptography," in *International Zurich Seminar*, Zurich, Switzerland, 2014.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[6] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*, 2nd ed. New York: Springer-Verlag, 1993.

[7] S. Liu, Y. Hong, and E. Viterbo, "Unshared secret key cryptography: finite constellation inputs and ideal secrecy outage," in *Proc. IEEE GLOBECOM Workshop on Trusted Communications with Physical Layer Security'14*, submitted for publication.

[8] E. Lukacs and E. P. King, "A property of the normal distribution," *Ann. Math. Statist.*, vol. 25, no. 2, pp. 389–394, 1954.

[9] A. M. Tulino and S. Verdú, *Random Matrix Theory and Wireless Communications*. North America: Now Publishers Inc., 2004.