International Zurich Seminar on Communications (IZS), February 26 – 28, 2014

Unshared Secret Key Cryptography

(Invited Paper)

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*—Inspired by the *artificial noise* technique by Goel *et al.*, we propose an unshared secret key (USK) cryptosystem, where the artificial noise is redesigned as a one-time pad secret key aligned within the null space between transmitter and legitimate receiver. Unlike previously studied artificial noise techniques, rather than ensuring non-zero secrecy capacity, the USK cryptosystem guarantees Shannon's *perfect secrecy* without the need of secret key exchange.**

I. Introduction

Wireless communications provide flexibility and mobility for users, but equally the ease of access features undermines user privacy. Research on secure communication falls into two categories: network layer cryptography and physical layer security (PLS). The former assumes that the physical layer provides error-free data links, in which security depends on a shared secret key. In the latter, the strategy is to use wiretap codes to protect the secret data from eavesdropping, while security comes from specific channel limitations for the eavesdropper. Both categories are rooted in Shannon's *perfect secrecy* [1], defined as the mutual information $I(\mathbf{u};\,\mathbf{y}) = 0$; that is, the secret message $\mathbf{u}$ and the eavesdropper's received message $\mathbf{y}$ are mutually independent. Perfect secrecy requires one-time pad secret key [1].

The PLS scheme, known as *artificial noise* (AN) [2], is the basis for our unshared secret key (USK) cryptosystem. In the AN scheme, the transmitter (Alice) aligns a jamming signal, called artificial noise, within the null space between itself and the legitimate receiver (Bob), thus AN only degrades the eavesdropper's (Eve's) channel. The strategy is to use Gaussian distributed AN to guarantee non-zero secrecy capacity [3]. Given such secrecy capacity, infinite-length wiretap codes can be used to achieve strong secrecy [4]. More recently, we proposed a variant of AN using a finite *M*-QAM alphabet, called *practical secrecy* (PS) scheme, where instead of increasing the secrecy rate with AN, the eavesdropper's error probability is maximized [5].

In this work, we show that the PS scheme is *de facto* an USK, where AN serves as an unshared one-time pad secret key. The result is a development of our understanding of the benefits of AN, embracing both coding and cryptographic dimensions. We show that the USK provides Shannon's perfect secrecy, with no secret key exchange, under Goel *et al.*'s assumptions on the physical channels that enable the use of the AN scheme.

Our work differs from previous studies of AN [2], because it puts forward four new aspects that were not previously accounted for:

1) *Perfect secrecy*: we aim to achieving Shannon's perfect secrecy directly, rather than ensuring non-zero secrecy capacity.
2) *Finite alphabet*: we use a finite alphabet (*M*-QAM) rather than infinite-length wiretap codes.
3) *Artificial noise*: we have no requirement of the distribution of AN; that is, not necessarily Gaussian.
4) *Lattice precoding*: we introduce lattice precoding to MIMO wiretap channels, which avoids the diversity loss caused by conventional *singular value decomposition* (SVD) precoding of [2].

Notation: Matrices and column vectors are denoted by upper and lowercase boldface letters, and the Hermitian transpose, inverse, pseudoinverse of a matrix $\mathbf{B}$ by $\mathbf{B}^H$, $\mathbf{B}^{-1}$, and $\mathbf{B}^\dagger$, respectively. Let $\{X_n, X\}$ be 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. $\mathbf{I}_n$ denotes the identity matrix of size n. We write $\triangleq$ for equality in definition. A circularly symmetric complex Gaussian random variable x with variance σ^2 is denoted as $x \backsim \mathcal{N}_{\mathbb{C}}(0, \sigma^2)$. The real, complex, integer and complex integer numbers are denoted by $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}$ and $\mathbb{Z}[i]$, respectively. $H(X)$, $H(X|Y)$ and $I(X;Y)$ represent entropy, conditional entropy and mutual information, respectively. We use the standard asymptotic notation $f(x) = O(g(x))$ when $\limsup_{x\to\infty} |f(x)/g(x)| < \infty$. vol$(S)$ denotes the Euclidean volume of S.

II. System Model

We consider a MIMO wiretap system, including a transmitter (Alice), an intended receiver (Bob), and a passive eavesdropper (Eve), with $N_{\rm A}$, $N_{\rm B}$, and $N_{\rm E}$ antennas, respectively. The signals received by Bob and Eve are given, respectively, by

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

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

where the entries of $\mathbf{n}_{\rm B}$ and $\mathbf{n}_{\rm E}$ are i.i.d. complex random variables $\sim \mathcal{N}_{\mathbb{C}}(0, \sigma_{\rm B}^2)$ and $\mathcal{N}_{\mathbb{C}}(0, \sigma_{\rm E}^2)$, respectively. We assume that the matrices $\mathbf{H}$ and $\mathbf{G}$, representing the channels from

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

Alice to Bob and Alice to Eve, respectively, are mutually independent, i.e., Bob and Eve are not co-located. The entries of $\mathbf{H}$ and $\mathbf{G}$ are i.i.d. complex random variables $\sim \mathcal{N}_{\mathbb{C}}(0,\, 1)$.

A. Artificial Noise Scheme

We first introduce the AN scheme [2]. Assuming $N_{\mathrm{B}} < N_{\mathrm{A}}$, $\mathbf{H}$ has a non-trivial null space $\mathbf{Z} = \mathrm{null}(\mathbf{H})$. Alice transmits

$$\mathbf{x} = \mathbf{P}\mathbf{u} + \mathbf{Z}\mathbf{v} \tag{3}$$

where $\mathbf{u}$ is the secret data vector and $\mathbf{P}$ is the precoding matrix. The AN $\mathbf{v}$ is generated by Alice and is unknown to Eve. In order to estimate the secrecy rate, both $\mathbf{u}$ and $\mathbf{v}$ are assumed to be Gaussian circularly symmetric random vectors.

The AN scheme is based on the channel assumptions below:

1) Alice only knows the realization of $\mathbf{H}$.
2) Eve knows the realizations of $\mathbf{H}$, $\mathbf{G}$, $\mathbf{Z}$ and $\mathbf{P}$.
3) $N_{\mathrm{A}} > N_{\mathrm{B}}$, $N_{\mathrm{A}} > N_{\mathrm{E}}$ and $N_{\mathrm{E}} \geq N_{\mathrm{B}}$.

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

$$\mathbf{z} = \mathbf{H}\mathbf{P}\mathbf{u} + \mathbf{n}_{\mathrm{B}}, \tag{4}$$

$$\mathbf{y} = \mathbf{G}\mathbf{P}\mathbf{u} + \mathbf{G}\mathbf{Z}\mathbf{v} + \mathbf{n}_{\mathrm{E}}. \tag{5}$$

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

In (3), the transmitted signal $\mathbf{x}$ depends on the precoding matrix $\mathbf{P}$. The AN scheme uses *SVD precoding*, given by

$$\mathbf{x}_{\mathrm{SVD}} = \mathbf{V}_1\mathbf{u} + \mathbf{Z}\mathbf{v}_{\mathrm{SVD}}, \tag{6}$$

where $\mathbf{P} = \mathbf{V}_1$ and the columns of $\mathbf{V} = [\mathbf{V}_1,\, \mathbf{Z}]$ are the right-singular vectors of $\mathbf{H}$, i.e., $\mathbf{H} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^H$.

For the AN scheme, given a positive secrecy rate, infinite-length wiretap codes can be used to achieve strong secrecy [4], i.e.,

$$\lim_{n\to\infty} I(\mathbf{u};\mathbf{y}) = 0, \tag{7}$$

where n represents the codeword length.

B. Practical Secrecy Scheme

Based on the AN scheme, we proposed the PS scheme, where the security measure in AN, secrecy capacity, is replaced by Eve's error probability [5]. Although the transmission model is the same as that given in (4) and (5), $\mathbf{u}$ and $\mathbf{v}$ are not required to be Gaussian distributed. The settings of the PS scheme are given below.

1) Uniform $M-$QAM signalling, i.e., $\Re(\mathbf{u})$ and $\Im(\mathbf{u}) \in \mathcal{C}^{N_{\mathrm{B}}}$, where $\mathcal{C} = \{-\sqrt{M}+1,\, -\sqrt{M}+3,\, ...,\, \sqrt{M}-1\}$, is used.
2) There is no requirement on the distribution of $\mathbf{v}$.

The PS scheme can use either SVD precoding or *lattice precoding* [6], in which

$$\mathbf{x}_{\mathrm{LP}} = \mathbf{H}^{\dagger}(\mathbf{u} - A\hat{\mathbf{w}}) + \mathbf{Z}\mathbf{v}_{\mathrm{LP}}, \tag{8}$$

where $A = 2\sqrt{M}$, $\mathbf{P} = \mathbf{H}^{\dagger}$ and

$$\hat{\mathbf{w}} = \arg \min_{\mathbf{w}\in\mathbb{Z}[i]^{N_{\mathrm{B}}}} \|\mathbf{H}^{\dagger}(\mathbf{u} - A\mathbf{w})\|^2. \tag{9}$$

Compared with the AN scheme, where the achievability of security is based on an infinite length code, the PS scheme is designed for practical communication systems, which make use of a finite alphabet. However, a security scheme based on error probability may be not safe in the sense of information-theoretic security.

In this work, we analyze and enhance the security of the PS scheme under the same channel assumptions as AN. To simplify our analysis, we unify the notation of $\mathbf{u}$ by defining

$$\tilde{\mathbf{u}} \triangleq \begin{cases} \mathbf{u} - A\hat{\mathbf{w}} & \text{lattice precoding} \\ \mathbf{u} & \text{SVD precoding} \end{cases} \tag{10}$$

We define the noise-plus-interference term at Eve as

$$\tilde{\mathbf{n}}_{\mathrm{v}} \triangleq \mathbf{G}\mathbf{Z}\mathbf{v} + \mathbf{n}_{\mathrm{E}}. \tag{11}$$

III. Unshared Secret Key Cryptosystem

In this section, we first interpret the PS scheme from a cryptographic perspective, and then prove its security in terms of perfect secrecy.

A. Encryption

The AN $\mathbf{v}$ used in the PS scheme can be treated as a one-time pad secret key. Alice randomly (without any predefined distribution) chooses $\mathbf{v}$ from the set S defined by

$$S \triangleq \left\{\mathbf{v} \in \mathbb{R}^{N_{\mathrm{A}}-N_{\mathrm{B}}}\colon \|\mathbf{v}\|^2 \leq P\right\}, \tag{12}$$

where P represents the transmission power constraint on $\mathbf{v}$.

The message $\tilde{\mathbf{u}}$ is received by Eve as a lattice point in: $\Lambda_{\mathbb{C}} = \{\mathbf{G}\mathbf{P}\tilde{\mathbf{u}},\, \tilde{\mathbf{u}} \in \mathbb{Z}[i]^{N_{\mathrm{B}}}\}$ (see Fig. 1). The set S can be further partitioned into D subsets S_1, ..., S_D, i.e.,

$$S = \bigcup_{k=1}^{D} S_k, \tag{13}$$

where

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

Later, we will show that the value of D can be uniquely characterized by P.

Assuming $\mathbf{v} \in S_k$, $1 \leq k \leq D$, the PS scheme thus can be viewed as a cryptosystem that encrypts $\tilde{\mathbf{u}}$ to $\mathbf{y}$ using a secret key $\mathbf{v}$, such that $\mathbf{G}\mathbf{P}\tilde{\mathbf{u}}$ is the k^{th} closest lattice point to $\mathbf{y}$ (see Fig. 1).

From Eve's perspective, we assume that she knows P and the above encryption process. Since Eve cannot know the secret key $\mathbf{v}$, she cannot know the distribution of k either. It means that Eve only knows that $\mathbf{G}\mathbf{P}\tilde{\mathbf{u}}$ is hidden inside the D closest lattice points to $\mathbf{y}$, but cannot locate it. Moreover, Eve cannot distinguish which lattice point has the highest probability of being $\mathbf{G}\mathbf{P}\tilde{\mathbf{u}}$, thus the probability that Eve obtains $\mathbf{G}\mathbf{P}\tilde{\mathbf{u}}$ is uniform over all D lattice points. By taking the codebook size of $\mathbf{u}$ into account, for a given $\mathbf{G}\mathbf{P}$, we have

$$\Pr\{\mathbf{G}\mathbf{P}\tilde{\mathbf{u}}|\mathbf{y}\} = \Pr\{\mathbf{u}|\mathbf{y}\} = \frac{1}{\min\left\{D,\, M^{N_{\mathrm{B}}}\right\}}, \tag{14}$$

or equivalently

$$H(\mathbf{u}|\mathbf{y}) = \log \min\left\{D,\, M^{N_{\mathrm{B}}}\right\}. \tag{15}$$

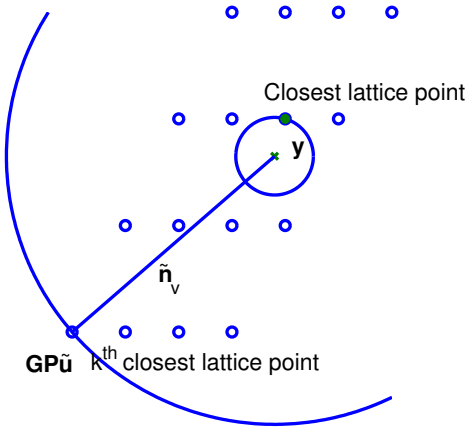

Fig. 1. Achieving perfect secrecy.

Different from Shannon's one-time pad cryptosystem, the one-time pad secret key $\mathbf{v}$ is not shared between Alice and Bob. In particular, it is independently generated by Alice, but not needed by Bob to decipher, while it is fully affecting Eve's ability to decipher the original message. We name this kind cryptosystem as Unshared Secret Key (USK) cryptosystem.

B. Decryption

From (4), Bob can simply run maximum likelihood decoding to estimate $\mathbf{u}$. We then show how to increase Eve's uncertainty of $\mathbf{u}$, i.e., $H(\mathbf{u}|\mathbf{y})$.

Based on (15), increasing $H(\mathbf{u}|\mathbf{y})$ is equivalent to increasing D. The value of D depends on the channel matrices $\mathbf{G}$ and $\mathbf{H}$. In this work, we assume $\mathbf{G}$ and $\mathbf{H}$ are not fixed, but are Gaussian random matrices. In this sense, for a given $\mathbf{v}$ and a positive integer c, $\Pr\{D > c|\mathbf{G},\mathbf{H}\}$ is also a random variable depending on $\mathbf{G}$ and $\mathbf{H}$, and $\tilde{\mathbf{n}}_v$ is a Gaussian random vector with i.i.d. entries $\mathcal{N}_{\mathbb{C}}(0, \tilde{\sigma}_v^2)$ where

$$\tilde{\sigma}_v^2 = ||\mathbf{v}||^2 + \sigma_E^2. \tag{16}$$

We recall that the realizations of G of $\mathbf{G}$ and H of $\mathbf{H}$ are known at Eve. Note that if we can ensure $\Pr\{D > c|\mathbf{G},\mathbf{H}\} \overset{a.s.}{\to} 1$, then $D > c$ for almost any realizations G and H (see [7, Def. 1.3]).

In fact, the idea behind the original PS scheme was to ensure $\Pr\{D > 1|\mathbf{G},\mathbf{H}\} \overset{a.s.}{\to} 1$, which is a special case of the USK with $c = 1$.

C. Achieving Perfect Secrecy

We now show how large P should be to guarantee perfect secrecy, i.e.,

$$I(\mathbf{u};\mathbf{y}) = 0. \tag{17}$$

From [1, Th.6], the necessary and sufficient condition to achieve perfect secrecy is

$$\Pr\{\mathbf{u}\} = \Pr\{\mathbf{u}|\mathbf{y}\}. \tag{18}$$

Since $\Pr\{\mathbf{u}\} = 1/M^{N_B}$, based on (14), a sufficient condition to achieve perfect secrecy is $D \geq M^{N_B}$.

In what follows, we evaluate the value of D by choosing $||\mathbf{v}||^2 = P$, i.e., on the surface of S in (12).

Lemma 1: Let $\mathrm{vol}(\Lambda_{\mathbb{C}})$ be the volume of the *Voronoi* cell of $\Lambda_{\mathbb{C}}$.

$$\Pr\left\{D \leq M^{N_B}|\mathbf{G},\mathbf{H}\right\} \leq \frac{M^{N_B}\mathrm{vol}(\Lambda_{\mathbb{C}})}{\pi^{N_E}P^{N_E}} \triangleq \Delta. \tag{19}$$

Proof: See Appendix A. ■

Note that Δ is a random variable depending on $\Lambda_{\mathbb{C}}$ defined by the random matrices $\mathbf{G}$ and $\mathbf{H}$. From Lemma 1, by sending Δ to zero, $\Pr\{D \leq M^{N_B}|\mathbf{G},\mathbf{H}\}$ is forced to zero as well, i.e., achieving perfect secrecy. In the following theorem, we show how to ensure $\Delta \overset{a.s.}{\to} 0$.

Lemma 2: Let

$$\kappa \triangleq M^{N_B/(2N_E)}/\sqrt{\pi}. \tag{20}$$

If $P = \rho^2/\Phi^{2N_B/N_E}$ and $\rho > \kappa$, then $\Delta \overset{a.s.}{\to} 0$ as $N_B \to \infty$, or equivalently,

$$\Pr\left\{\Delta > \left(\frac{\rho}{\kappa}\right)^{-N_B}\right\} < O\left(\left(\frac{\rho}{\kappa}\right)^{-N_B}\right) \tag{21}$$

where Φ depends on the precoder, i.e.,

$$\Phi_{\mathrm{LP}} = \left[\frac{(N_E - N_B)!}{(N_A - N_B)!}\cdot\frac{N_A!}{N_E!}\right]^{\frac{1}{2N_B}} \quad \text{for lattice precoding} \tag{22}$$

$$\Phi_{\mathrm{SVD}} = \left[\frac{(N_E - N_B)!}{N_E!}\right]^{\frac{1}{2N_B}} \quad \text{for SVD precoding} \tag{23}$$

Proof: Available in the journal version. ■

Lemmas 1 and 2 allow us to deduce our main theorem.

Theorem 1: If $P > \kappa^2/\Phi^{2N_B/N_E}$, perfect secrecy is achieved almost surely as $N_B \to \infty$, where κ is given in (20) and Φ is given in (22) or (23).

IV. Conclusions

We have revisited the role that artificial noise plays in cryptography, showing that it can be used as unshared one-time pad secret keys. The proposed unshared secret key cryptosystem provides Shannon's perfect secrecy, and enjoys exemption from secret key exchange. Our work has highlighted that USK is valid for a finite alphabet such as M-QAM and a arbitrarily distributed artificial noise. Both lattice and SVD precoding are applicable to USK, significantly enhancing the utility of the cryptosystem. The basis is now established for future advances on generalizing USK to other channel.

Appendix

A. Proof of Lemma 1

Let $\mathcal{S}_p$ be a sphere of radius R centered at $\mathbf{y}$, where $\mathrm{vol}(\mathcal{S}_p) = M^{N_B}\mathrm{vol}(\Lambda_{\mathbb{C}})$. Let K be the number of the points in $\mathcal{S}_p \cap \Lambda_{\mathbb{C}}$. We have

$$K \approx \frac{\mathrm{vol}(\mathcal{S}_p)}{\mathrm{vol}(\Lambda_{\mathbb{C}})} = M^{N_B}. \tag{24}$$

We recall that $\mathbf{GP\tilde{u}}$ is the k^{th} closest lattice point to $\mathbf{y}$ and $D \geq k$. Thus, if $\mathbf{GP\tilde{u}} \notin \mathcal{S}_p$, we have $D > M^{N_B}$.

Let $\mathcal{S}'_{\rm p}$ be a sphere with the same radius R centered at $\mathbf{GP\tilde{u}}$. If $\mathbf{GP\tilde{u}} \notin \mathcal{S}_{\rm p}$, then $\mathbf{y} \notin \mathcal{S}'_{\rm p}$, and vice versa. Therefore, we have

$$\begin{aligned} & \Pr\left\{D \leq M^{N_{\rm B}} | \mathbf{G}, \mathbf{H}\right\} \\ = \; & \Pr\left\{\mathbf{GP\tilde{u}} \in \mathcal{S}_{\rm p}\right\} \\ = \; & \Pr\left\{\mathbf{y} \in \mathcal{S}'_{\rm p}\right\} \\ = \; & \int_{\mathcal{S}'_{\rm p}} f(\tilde{\mathbf{n}}_{\rm v}) d\tilde{\mathbf{n}}_{\rm v} \\ \leq \; & \frac{M^{N_{\rm B}} {\rm vol}(\Lambda_{\mathbb{C}})}{\pi^{N_{\rm E}} \tilde{\sigma}_{\rm v}^{2N_{\rm E}}} \\ \leq \; & \frac{M^{N_{\rm B}} {\rm vol}(\Lambda_{\mathbb{C}})}{\pi^{N_{\rm E}} P^{N_{\rm E}}}, \end{aligned} \tag{25}$$

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

$$\begin{aligned} f(\tilde{\mathbf{n}}_{\rm v}) \; = \; & \frac{1}{\pi^{N_{\rm E}} \tilde{\sigma}_{\rm v}^{2N_{\rm E}}} \exp\left(-\frac{||\tilde{\mathbf{n}}_{\rm v}||^2}{\tilde{\sigma}_{\rm v}^2}\right) \\ \leq \; & \frac{1}{\pi^{N_{\rm E}} \tilde{\sigma}_{\rm v}^{2N_{\rm E}}} \\ = \; & \frac{1}{\pi^{N_{\rm E}} \left(P + \sigma_{\rm E}^2\right)^{N_{\rm E}}} \\ \leq \; & \frac{1}{\pi^{N_{\rm E}} P^{N_{\rm E}}}. \end{aligned} \tag{26}$$

■

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. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[4] I. Csiszár, "Almost independence and secrecy capacity," *Problems of Information Transmission*, vol. 32, pp. 40–47, 1996.

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

[6] B. M. Hochwald, C. B. Peel, and A. L. Swindlehurst, "A vector perturbation technique for near-capacity multiantenna multiuser communications-Part II: Perturbation," *IEEE Trans. Commun.*, vol. 53, pp. 537–544, Mar. 2005.

[7] A. DasGupta, "Asymptotic theory of statistics and probability," in *Springer Texts in Statistics*. Springer-Verlag, 2008.