On Measures of Information Theoretic Security

(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*—While information-theoretic security is stronger than computational security, it has long been considered impractical. In this work, we provide new insights into the design of practical information-theoretic cryptosystems. Firstly, from a theoretical point of view, we give a brief introduction into the existing information theoretic security criteria, such as the notions of Shannon's perfect/ideal secrecy in cryptography, and the concept of strong secrecy in coding theory. Secondly, from a practical point of view, we propose the concept of *ideal secrecy outage* and define a outage probability. Finally, we show how such probability can be made arbitrarily small in a practical cryptosystem.**

I. Information Theoretic Security Criteria

The security definition in information-theoretic security is formalized by use of some information-theoretic measure (e.g. entropy or statistical distance). Thus, it does not depend on a specific computational model and can provide security even when the adversary has unlimited computing power. Up to date, the principle of information-theoretic security is widely accepted as the strictest notion of security. Various security measures have been reported and developed since Shannon's work [1]. In what follows, we introduce the classical criteria of information theoretic security.

A. Shannon's Secrecy

We first introduce Shannon's shared key-based model. 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

$$\begin{aligned}\lim_{K\to\infty} H(\{\mathbf{m}_i\}_1^K \,|\, \{\mathbf{y}_i\}_1^K) &\neq 0,\\ \lim_{K\to\infty} H(\{k_i\}_1^K \,|\, \{\mathbf{y}_i\}_1^K) &\neq 0.\end{aligned} \tag{1}$$

Definition 2: A secrecy system is *perfect* when

$$H(\{\mathbf{m}_i\}_1^K \,|\, \{\mathbf{y}_i\}_1^K) = H(\{\mathbf{m}_i\}_1^K). \tag{2}$$

In the special case that $\{\mathbf{m}_i\}_1^K$ and $\{k_i\}_1^K$ are i.i.d. and mutually independent (which also means that $\{\mathbf{y}_i\}_1^K$ are i.i.d.), using the entropy chain rule, we have

$$H(\{\mathbf{m}_i\}_1^K) = \sum_{i=1}^K H(\mathbf{m}_i), \tag{3}$$

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

$$H(\{\mathbf{m}_i\}_1^K \,|\, \{\mathbf{y}_i\}_1^K) = \sum_{i=1}^K H(\mathbf{m}_i|\mathbf{y}_i), \tag{4}$$

$$H(\{k_i\}_1^K \,|\, \{\mathbf{y}_i\}_1^K) = \sum_{i=1}^K H(k_i|\mathbf{y}_i). \tag{5}$$

From (4) and (5), 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 one i. The above definition of ideal secrecy does not guarantee that all the messages are equally secured. To protect all the messages, in this work, we use a slightly stronger condition as our design criterion for ideal secrecy, given by

Definition 3: If $\{\mathbf{m}_i\}_1^K$ and $\{k_i\}_1^K$ are i.i.d. and mutually independent, a secrecy system is *ideal* when

$$H(\mathbf{m}_i|\mathbf{y}_i) \neq 0 \text{ and } H(k_i|\mathbf{y}_i) \neq 0, \text{ for all } i. \tag{6}$$

From (3) and (4), perfect secrecy is achieved when

$$H(\mathbf{m}_i|\mathbf{y}_i) = H(\mathbf{m}_i), \text{ for all } i. \tag{7}$$

B. Secrecy Capacity and Strong Secrecy

Wyner [2] and later Csiszár and Körner [3] proposed a keyless model, called the *wiretap channel*. Wyner has shown that if the eavesdropper (Eve) intercepts a degraded version of the intended receiver's (Bob's) signal, a prescribed degree of data confidentiality could simultaneously be attained by channel coding without any secret key. The associated notion of *secrecy capacity* was introduced to characterize the maximum transmission rate from the transmitter (Alice) to Bob, below which Eve is unable to obtain any information. Khisti and Wornell studied the ergodic secrecy capacity for multiple-input, single-output, multiple eavesdropper (MISOME) system in [4]. For quasi-static fading channels, the outage probability of secrecy capacity is derived in [5]. We recall from [6] the definition of instantaneous secrecy capacity for demonstration:

$$C_{\mathrm{S}} \triangleq \max_{p(\mathbf{u})} \{I(\mathbf{u};\mathbf{z}) - I(\mathbf{u};\mathbf{y})\}. \tag{8}$$

where $\mathbf{u}$ is the information vector, $\mathbf{z}$ and $\mathbf{y}$ are the received vector at Bob and Eve, respectively. The maximum is taken over all possible input distributions $p(\mathbf{u})$.

If $C_{\mathrm{S}} > 0$, Alice can limit the information leakage to Eve by means of channel coding. Csiszár [7] proposed the *strong secrecy* criterion for the wiretap code design.

Definition 4: A *strong secrecy rate* R is achievable if there exist a sequence of wiretap codes $\{\mathcal{C}_n\}$ of increasing length

n and rate R, such that both Bob's error probability and the amount of information obtained by Eve approach zero when $n \to \infty$ [7,8], i.e.,

$$\lim_{n\to\infty} \Pr\{\hat{\mathbf{u}} \neq \mathbf{u}\} = 0, \qquad \text{(reliability)}$$

$$\lim_{n\to\infty} I(\mathbf{u};\mathbf{y}) = 0, \qquad \text{(strong secrecy)}$$

where $\hat{\mathbf{u}}$ represents Bob's estimation of $\mathbf{u}$.

C. Discussion

In terms of the cost, Shannon's perfect secrecy can be achieved only when the secret key is at least of the size of the plaintext, while Csiszár's strong secrecy requires infinite length wiretap codes. Obviously, neither of them is achievable in practice. In fact, it is common for a cryptosystem to leak some information (i.e., $H(\mathbf{m}_i|\mathbf{y}_i) < H(\mathbf{m}_i)$) but nevertheless maintain its security properties even against an adversary that has unlimited computational resources (see http://en.wikipedia.org/wiki/Information-theoretic_security). Therefore, it is meaningful to study the application of Shannon's ideal secrecy in practical cryptosystem design.

II. Ideal Secrecy Outage

We consider physical layer cryptograph in a wireless system. We use our slightly stronger definition of ideal secrecy in (6) and drop the subscript i for simplicity. In general, $H(\mathbf{m}|\mathbf{y})$ and $H(k|\mathbf{y})$ are functions of Eve's channel matrix. It is reasonable to assume that Alice only knows the statistics of Eve's channel. Although Alice cannot know the exact values in $H(\mathbf{m}|\mathbf{y})$ and $H(k|\mathbf{y})$, she may be able to evaluate their cumulative distribution functions (cdf), given by

$$\Pr\{H(\mathbf{m}|\mathbf{y}) < x_1\} \text{ and } \Pr\{H(k|\mathbf{y}) < x_2\}, \tag{9}$$

where $0 < x_1 < H(\mathbf{m})$ and $0 < x_2 < H(k)$.

We refer to the event

$$\{H(\mathbf{m}|\mathbf{y}) < x_1\} \cup \{H(k|\mathbf{y}) < x_2\}, \tag{10}$$

as the *ideal secrecy outage*. We refer to

$$P_{\text{out}}(x_1, x_2) \triangleq \max\{\Pr\{H(\mathbf{m}|\mathbf{y}) < x_1\}, \Pr\{H(k|\mathbf{y}) < x_2\}\}, \tag{11}$$

as the *ideal secrecy outage probability*. If $P_{\text{out}} \to 0$, then $H(\mathbf{m}|\mathbf{y}) \geq x_1$ and $H(k|\mathbf{y}) \geq x_2$ almost surely.

Remark 1: The proposed concept of ideal secrecy outage serves as a new measure of information theoretic security, which is tailored for practical secure communications. In what follows, we provide an example to show how P_{out} can be made arbitrarily small in a practical cryptosystem.

Example 1: In [9–12], we proposed the *Unshared Secret Key Cryptography* (USK) to comply with two security goals: *(i)* the secret key is not needed by Bob to decipher, *(ii)* the secret key is fully affecting Eve's ability to decipher the ciphertext. Although those two goals seem to contradict each other, this can be reconciled by aligning a one-time pad (OTP) secret key within the null space of a MIMO channel between Alice and Bob. In this way, the OTP nulls out at Bob, but adds a certain degree of uncertainty to the received signal at Eve. The USK secrecy properties are discussed below.

Suppose that $\mathbf{m}$ contains n mutually independent information bits. In the USK scheme, Alice maps the n bits to N_{B} (corresponding to Bob's antenna number) elements of $\mathbf{u}$ for B channel uses. Each element of $\mathbf{u}$ is uniformly selected from a M-QAM constellation $\tilde{\mathcal{Q}}$, where $\Re(\tilde{\mathcal{Q}}) = \Im(\tilde{\mathcal{Q}}) = \{0, 1, ..., \sqrt{M}-1\}$. We ignore the shifting and scaling operations at Alice to minimize the transmit power. To secure the total B transmitted vectors $\{\mathbf{u}_j\}_1^B$, Alice enciphers $\{\mathbf{u}_j\}_1^B$ into the cryptograms $\{\mathbf{y}_j\}_1^B$ using a sequence of i.i.d. *unshared* keys $\{k_j\}_1^B$. The USK scheme has the following property of

$$H(\mathbf{m}|\{\mathbf{y}_j\}_1^B) = H(\{k_j\}_1^B|\{\mathbf{y}_j\}_1^B) = H(\{\mathbf{u}_j\}_1^B|\{\mathbf{y}_j\}_1^B), \tag{12}$$

and guarantees that for any given $0 < x < H(\mathbf{m})$,

$$P_{\text{out}}(x, x) < O(\varepsilon^B), \tag{13}$$

where $\varepsilon > 0$ can be made arbitrarily small by increasing M and the transmission power. The rigorous proofs for these properties are provided in [12].

III. Conclusions

In this paper, we surveyed the existing measures of information theoretic security. Moreover, we proposed a tailor-made measure for practical information-theoretic cryptosystems, called ideal secrecy outage. An example has been provided to show that the outage probability can be made arbitrarily small in a practical cryptosystem. Going forward, a variety of fascinating research problems remain open, such as generalizing the concept of ideal secrecy outage to relaying networks.

References

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

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] 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.

[5] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

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

[8] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," Oct. 2012. [Online]. Available: http://arxiv.org/abs/1210.6673

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

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

[11] ——, "Unshared secret key cryptography: Achieving Shannon's ideal secrecy and perfect secrecy," in *Proc. IEEE Information Theory Workshop (ITW'14)*, Tasmania, Australia, Oct. 2014.

[12] ——, "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.