A Key Agreement Protocol Using Band-Limited Random Signals and Feedback

Pao-Lo Liu

***Abstract*—Key distribution is an essential element in cryptography. In this paper, the framework of a classical key agreement protocol using band-limited random signals and feedback is presented. The secrecy is derived from masking information by privately held random signals. Critical parameters of the protocol are identified. Raw performance of the system is presented. The secrecy can be enhanced by taking advantages of measures, such as reconciliation and privacy amplification, developed for classical and quantum key agreement protocols.**

***Index Terms*—Communication system security, correlation, optical fiber communication, random noise.**

I. Introduction

COMMUNICATION SYSTEMS represent a critical infrastructure in the society. To ensure high security in the open environment, new ideas of cryptography are constantly being pursued and analyzed [1], [2]. Hardware devices, software algorithms, and coding protocols have been implemented in classical secure communication systems [1]–[9]. More recently, quantum cryptography and information processing have become the focus. Quantum key distribution can provide the ultimate security against eavesdropping [10]–[13]. Quantum information processing can crack classical algorithms in which security is granted by computational complexity [14], [15]. Since quantum systems require special devices, classical secure communication systems are used in most applications.

It has long been established that the one-time pad provides the ultimate security against eavesdropping [16]. However, techniques that can distribute the key securely at a rate comparable to the speed of modern communication systems are yet to establish. Therefore, most secure communication systems depend on keys with limited length for encryption and decryption. There are many algorithms and protocols involving keys, for example, secret key agreement protocols developed for wiretap or broadcast channels, the Diffie–Hellman key agreement method, and the RSA encryption technique [7]–[9], [17], [18].

In the Diffie–Hellman method, each party holds a secret. The channel is public but authenticated. Two parties share information publicly. They encode the public domain information with their private, secret numbers and communicate results to each other. Based on the information received, they can derive a shared key. The eavesdropper, however, is denied of secret numbers. She has to deal with the computationally intensive discrete logarithm.

Based on the same spirit of holding some information private and establishing the key jointly through discussions in public, a classical key agreement protocol using band-limited random signals and feedback is presented. In this paper, the framework of the protocol is described. The critical parameters and the raw performance of the system are presented.

Manuscript received February 07, 2009; revised August 08, 2009. First published September 01, 2009; current version published October 07, 2009.

The author is with the Department of Electrical Engineering, University at Buffalo, The State University of New York, Buffalo, NY 14260 USA (e-mail: paololiu@buffalo.edu).

Digital Object Identifier 10.1109/JLT.2009.2031421

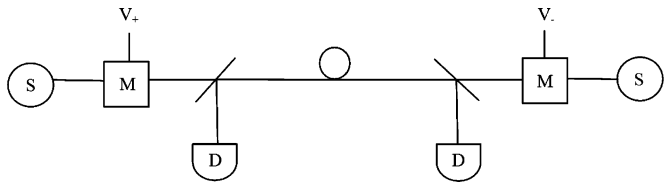

Fig. 1. Schematic diagram of a communication system for key exchange. S represents the carrier source. M is a modulator. It can be replaced by directly modulating the source. D represents the detector. Alice transmits V_+ and Bob transmits V_-. V_+ and V_- are baseband signals.

II. Key Agreement Protocol Using Feedback

Let us consider the following optical communication setup involving feedback. The schematic diagram of the system is shown in Fig. 1. V_+ is the baseband signal containing information. It is sent by Alice via amplitude modulation of the optical carrier and detected by Bob. Likewise, Bob transmits V_- to Alice. Alice holds a secret, analog, Gaussian random source $V_1(t)$, with a limited bandwidth of *W*. Similarly, Bob holds his own random source, $V_2(t)$. Alice adds a fraction, α, of the signal received from Bob as feedback to the local random signal. She transmits the combined signal as V_+. Bob does the same by using a feedback coefficient β. The signals can be represented by the following equations:

$$V_+(0,t) = V_1(t) + \alpha V_-(0,t) \tag{1}$$

$$V_-(L,t) = V_2(t) + \beta V_+(L,t). \tag{2}$$

Alice is located at $x = 0$; Bob at $x = L$. Signal originating from Alice is detected by Bob at a later time. In other words, $V_+(L,t) = V_+(0,t-\tau)$. Likewise, $V_-(0,t) = V_-(L,t-\tau)$, where τ is the signal transit time. In the system, V_+ and V_- are public, and V_1 and V_2 are private. Alice and Bob encode information by modulating α and β.

To establish the key, Alice transmits a sequence of random, binary symbols. To encode logic 1, Alice picks a positive feedback coefficient. To encode 0, she picks a negative coefficient. Bob does the same. Each symbol has duration *T*. $T >> \tau$. To ensure that V_1 and V_2 are sufficiently random during each symbol,

$WT > 1$. In other words, the average values of random signals, $\langle V_1(t)\rangle$ and $\langle V_2(t)\rangle$, are nearly zero. The angled brackets represent time averaging during each symbol.

In the limit of $\tau = 0$, (1) and (2) lead to

$$V_+(0,t) = \frac{V_1(t) + \alpha V_2(t)}{1-\alpha\beta} \tag{3}$$

$$V_-(L,t) = \frac{V_2(t) + \beta V_1(t)}{1-\alpha\beta} \tag{4}$$

$$\langle V_+^2(0,t)\rangle = \frac{\langle V_1^2(t)\rangle + \alpha^2\langle V_2^2(t)\rangle + 2\alpha\langle V_1(t)V_2(t)\rangle}{(1-\alpha\beta)^2} \tag{5}$$

$$\langle V_-^2(L,t)\rangle = \frac{\beta^2\langle V_1^2(t)\rangle + \langle V_2^2(t)\rangle + 2\beta\langle V_1(t)V_2(t)\rangle}{(1-\alpha\beta)^2} \tag{6}$$

$$\langle V_+(0,t)\cdot V_-(L,t)\rangle = \frac{\beta\langle V_1^2(t)\rangle + \alpha\langle V_2^2(t)\rangle + (1+\alpha\beta)\langle V_1(t)V_2(t)\rangle}{(1-\alpha\beta)^2}. \tag{7}$$

The quantities represented by (3)–(7) are all public, and hence available to Eve. The following measurements, however, are private, i.e., only available to Alice or Bob

$$\langle V_-(0,t)\cdot V_1(t)\rangle = \frac{\beta\langle V_1^2(t)\rangle + \langle V_1(t)V_2(t)\rangle}{1-\alpha\beta} \tag{8}$$

$$\langle V_+(L,t)\cdot V_2(t)\rangle = \frac{\alpha\langle V_2^2(t)\rangle + \langle V_1(t)V2(t)\rangle}{1-\alpha\beta}. \tag{9}$$

V_1 and V_2 are independent. In the approximation of $\langle \mathrm{V_1(t)V_2}(t)\rangle = 0$, (7)–(9) become

$$\langle V_+(0,t)\cdot V_-(L,t)\rangle = \frac{\beta\langle V_1^2(t)\rangle + \alpha\langle V_2^2(t)\rangle}{(1-\alpha\beta)^2} \tag{10}$$

$$\langle V_-(0,t)\cdot V_1(t)\rangle = \frac{\beta\langle V_1^2(t)\rangle}{1-\alpha\beta} \tag{11}$$

$$\langle V_+(L,t)\cdot V_2(t)\rangle = \frac{\alpha\langle V_2^2(t)\rangle}{1-\alpha\beta}. \tag{12}$$

The channel is assumed to be authenticated. Eve can monitor V_+ and V_-, but she cannot alter any signal in the channel without being detected. She is denied access to V_1 and V_2. She can evaluate any quantities derived from V_+ and V_-, but she cannot use V_1 and V_2.

The protocol calls for Alice and Bob to choose $V_1(t), V_2(t), \alpha$, and β such that $\langle V_+^2(0,t)\rangle = \langle V_-^2(L,t)\rangle$. The purpose is to limit the information that Eve can obtain on α and β. There are many possible combinations to accomplish this. One particular protocol, namely, $\langle V_1^2(t)\rangle \cong \langle V_2^2(t)\rangle$ and $|\alpha| = |\beta| < 1$, is discussed in this study. It may not look obvious, but the circuit consisting of two resistors and Johnson-noise-like sources represents another protocol [19]–[21]. It has inspired the development of this framework.

Alice uses $\langle V_-(0,t)V_1(t)\rangle$ to determine β and Bob uses $\langle V_+(L,t)V_2(t)\rangle$ to determine α, i.e., the information sent by the other party. They drop symbols with $\alpha = \beta$. They only keep the remaining ones with $\alpha = -\beta$ as preliminary key elements. In other words, only 50% of the symbols exchanged become key elements. To keep a subset of symbols as key elements also appears in a secret key agreement protocol involving correlated sources [22]. Eve can determine the binary information exchanged between Alice and Bob when $\alpha = \beta$ by using $\langle V_+(0,t)V_-(L,t)\rangle$. In other words, she can determine that both Alice and Bob transmit logic 1 or 0. However, she cannot determine which side holds a positive feedback coefficient when $\alpha = -\beta$. By keeping a series of symbols consisting of $\alpha = -\beta$, Alice and Bob can jointly establish the shared key in secret. They can use the key to encrypt and decrypt the plaintext. On the other hand, Eve is completely denied the key in the approximation of $\tau = 0$ and $\langle V_1(t)V_2(\mathrm{t})\rangle = 0$.

III. Secrecy Analysis in the Steady State

When $\tau \neq 0$, Eve can exploit the transit delay for eavesdropping. The transit delay poses as a security risk both during the initial turn-on of $V_1(t)$ and $V_2(t)$, and in the steady state. The security risk during the transient is addressed in the follow-up paper [23]. In this paper, the focus is in the steady state during which the bulk of signal exchange takes place. Alice and Bob depend on steady-state signals for determining the information sent by the other party.

When the delay is long, i.e., $W\tau >> 1$, $\langle V_1(t)\ V_1(t+\tau)\rangle, \langle V_2(t)V_2(t+\tau)\rangle$, and $\langle V_1(t)V_2(t+\tau)\rangle$ approach zero. Using (1) and (2), Eve can perform correlations, $\langle V_+(0,t)V_-(0,t)\rangle$ and $\langle V_-(\mathrm{L},t)V_+(L,t)\rangle$, to extract α and β. When τ is short, Eve can attempt to decipher using the difference between correlations, namely

$$\delta = \langle V_+(0,t)\cdot V_-(0,t)\rangle - \langle V_-(L,t)\cdot V_+(L,t)\rangle. \tag{13}$$

When $\delta > 0$, Eve concludes that a logic 1 is sent by Alice. When $\delta < 0$, she thinks that Bob sends logic 1. When τ is small, δ is often obscured by the randomness of $V_1(t)$ and $V_2(t)$, making it difficult for Eve to decipher.

Although V_1 and V_2 are independent, random sources, $\langle V_1(t)V_2(t)\rangle$ is not exactly zero because WT is finite. If $\langle V_1^2(t)\rangle$ exactly equals $\langle V_2^2(\mathrm{t})\rangle$ and $\alpha = -\beta$, (5)–(7) lead to

$$\langle V_+^2(0,t)\rangle - \langle V_-^2(L,t)\rangle = \frac{2(\alpha-\beta)\langle V_1(t)V_2(t)\rangle}{(1-\alpha\beta)^2} \tag{14}$$

$$\langle V_+(0,t)\cdot V_-(L,t)\rangle = \frac{(1+\alpha\beta)\langle V_1(t)V_2(t)\rangle}{(1-\alpha\beta)^2}. \tag{15}$$

From measurements of $V_+(0,t)$ and $V_-(L,t)$, Eve can determine the sign of $(\alpha-\beta)$ in (14) by using (15), and thus decipher the key. To prevent Eve from doing this, $\langle V_1^2(t)\rangle$ and $\langle V_2^2(t)\rangle$ must fluctuate. Such fluctuations occur naturally in deriving V_1 and V_2. The process starts with the generation of a long white Gaussian noise sequence. The noise is filtered by a low-pass filter with a flat frequency response from dc to 5 kHz, for example, and then normalized to mean-square fluctuation of 1. The long, band-limited random signal is truncated to 5 ms, for example, forming $V_1(t)$ and $V_2(t)$. The truncated sequence is not normalized, and $\langle V_1^2(t)\rangle$ and $\langle \mathrm{V_2^2}(t)\rangle$ fluctuate. Therefore, Eve has no advantage in using (14) and (15) than (13) to decipher.

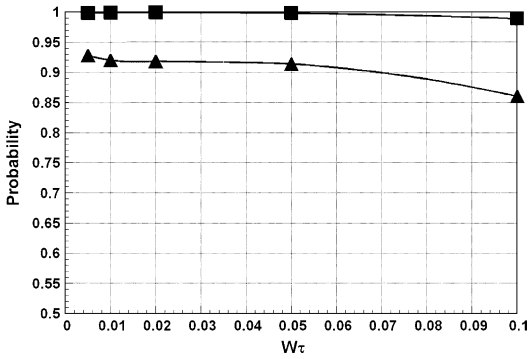

Fig. 2. Probability for Alice or Bob to correctly decipher the information as a function of $W\tau$. *WT* is assumed to be 25. The top set of square data points are obtained with $|\alpha| = |\beta| = 0.4$. The bottom set of triangular data points are obtained with $|\alpha| = |\beta| = 0.2$. Data points are connected by curve segments for the convenience of viewing.

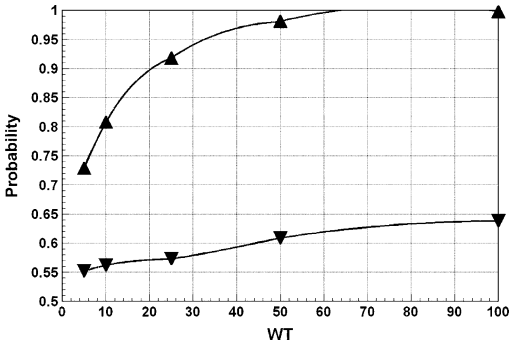

Fig. 3. Probability of Alice, Bob, and Eve to correctly decipher the information as a function of *WT*. $W\tau$ is assumed to be 0.02 and $|\alpha| = |\beta| = 0.2$. Data for Alice or Bob are represented by upward triangles. Data for Eve are represented by downward triangles. Data points are connected by curve segments for the convenience of viewing.

When Eve uses (13) to decipher, the secrecy of the system depends on numerical values of the following critical parameters: *WT*, magnitude of α, β, and $W\tau$. Their values should be chosen to differentiate Alice and Bob from Eve in their abilities to correctly decipher symbols. Since random signals are used, the performance of the system is best evaluated by using statistical analysis. The following results are obtained by performing simulations in MATLAB.

Alice uses (11) and Bob uses (12) to determine β and α, i.e., the information sent by the other party. The distribution of all measurements on α and β consists of two peaks: one positive and the other negative. When logic 1 is sent by Alice, but Bob detects a negative α, it constitutes an error. The error probability or error rate depends on values of critical parameters. With a fixed *WT* of 25, the probability for Alice or Bob to decipher correctly is shown in Fig. 2 as a function of $W\tau$. Two sets of data are shown. The top set corresponds to $|\alpha|, |\beta| = 0.4$. The bottom set corresponds to $|\alpha|, |\beta| = 0.2$. With a fixed $W\tau$ of 0.02 and $|\alpha|, |\beta| = 0.2$, the probability for Alice or Bob to decipher correctly is presented by upward triangles in Fig. 3 as a function of *WT*.

Eve uses (10) to decide whether $\alpha = \beta$ or $\alpha = -\beta$. The distribution of all measurements on (10) consists of three peaks: one positive, one centered at zero, and the third negative. The peak centered at zero corresponds to incidences of $\alpha = -\beta$. If a measured result is sufficiently far from zero, i.e., halfway beyond the distance between the positive or negative peak and zero, Eve concludes that $\alpha = \beta$; otherwise, $\alpha = -\beta$. With strategically chosen values of $WT = 25, W\tau = 0.02$, and $|\alpha|, |\beta| = 0.2$, Eve has a success rate of 91.6%. For comparison, Alice and Bob have a success rate of 91.8%. Eve is as accurate as Alice and Bob in deciding whether $\alpha = \beta$ or $\alpha = -\beta$. The critical issue is how inaccurate Eve becomes when she attempts to decipher when $\alpha = -\beta$.

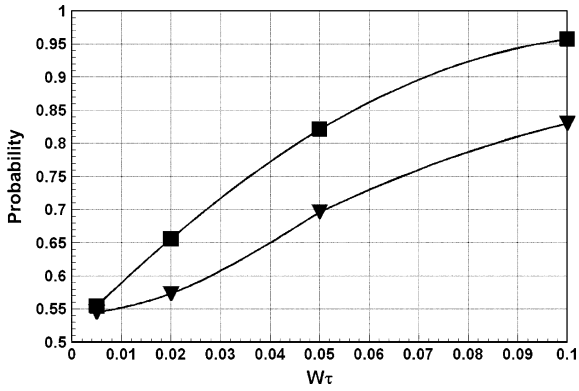

Fig. 4. Probability for Eve to decipher as a function of $W\tau$. *WT* is assumed to be 25. The top set of square data points are obtained with $|\alpha| = |\beta| = 0.4$. The bottom set of triangular data points are obtained with $|\alpha| = |\beta| = 0.2$. Data points are connected by curve segments for the convenience of viewing.

When $\alpha = -\beta$, Eve relies on (13) to decipher. With fixed Wτ of 0.02 and $|\alpha|, |\beta| = 0.2$, the probability for Eve to decipher correctly as a function of *WT* is shown in Fig. 3. Eve's data are labeled as downward triangles in the bottom curve. With strategically chosen values of $WT = 25, W\tau = 0.02$, and $|\alpha|, |\beta| = 0.2$, Eve has only a success rate of 57.3%. It is substantially lower than what Alice and Bob have at 91.8%. This difference provides an opportunity for secret key agreement. For the purpose of completeness, Fig. 4 shows the probability for Eve to decipher correctly as a function of $W\tau$. *WT* is assumed to be 25. Data shown in Fig. 4 for Eve can be compared directly with data shown in Fig. 2 for Alice and Bob. Obviously, one cannot simply choose a large value for α and β to increase the success rate of Alice and Bob. By doing so, Eve also has a high success rate. One must choose α, β, *WT*, and $W\tau$ strategically to differentiate Alice and Bob from Eve.

IV. Discussion

Ideally, Alice and Bob should be correct 100% of the time. For Eve, it is 50% corresponding to totally random choices between logics 1 and 0. In the range of critical parameters studied, the protocol does provide different degrees of differentiation between Alice, Bob, and Eve. However, the system is far from being ideal. Statistically, Eve still has a chance to intercept the key. Alice and Bob do make few mistakes. Their keys may not be identical initially. The situation is similar to what happens in nonideal quantum cryptography. The mechanisms, however, are completely different. If errors are eliminated by using a large feedback coefficient, Eve will enjoy a high success rate in correctly deciphering the key too [19]–[21]. Alice and Bob have to tolerate some error and accept finite information leak to Eve. To

handle the error, they can take advantages of the reconciliation technique developed for secret key agreement and quantum encryption [24]. With strategically identified parameters, namely, $WT = 25, W\tau = 0.02$, and $|\alpha| = |\beta| = 0.2$, the error rate for Alice and Bob is 8.2%. This falls comfortably within the range of error rate that can be dealt with efficiently by using existing reconciliation techniques. Only a limited number of bits in the stream will be used up for error detection and correction.

Although the key is generated jointly by Alice and Bob through communications and distillation, this protocol is different from other secret key agreement protocols and quantum cryptography. In secret key agreement protocols using public channels, the signal detected by Eve is different from that of Bob [5]–[9]. In this protocol, Eve detects identical signals as Alice and Bob. The feedback in [7] represents additional information exchange. In this protocol, feedback represents the partial reflection of the incoming baseband signal. In chaotic communications, the sender encodes the information in chaotic signals. The legitimate receiver must have the means to recreate and synchronize the chaotic signals. In this protocol, the secrecy is derived by using two privately held random signals: one at the sender and the other at the receiver. These two random signals are independent and hidden from each other. Different from quantum cryptography, the classical key exchange protocol cannot detect the presence of the eavesdropper. Alice and Bob must assume that Eve is constantly monitoring the signals. On the other hand, the classical signaling enables Alice and Bob to know exactly what Eve gets. This opens up opportunities for countermeasure. Alice and Bob can implement a privacy amplification measure to discriminate against Eve [25], [26]. For example, Alice can inform Bob in public to drop the first *N* bits that are correctly identified by Eve. Alice does not announce where these bits are. Since Bob has the same key sequence after reconciliation, both of them can drop bits synchronously. Eve only knows that a percentage of her key elements are correct. She does not know the exact locations of the correct key elements. By dropping a wrong element, the key becomes scrambled. Such a countermeasure can enhance the security of the system by reducing the success rate of Eve toward 50%, i.e., random guessing.

In the earlier discussions, V_1 and V_2 are random signals. Alice and Bob transmit signals synchronously in real time. Neither the loss of the fiber nor the noise of the transmission system is an issue. The loss can be compensated by using a fiber amplifier at the receiving end. The mistakes that Alice and Bob make are due, almost entirely, to the randomness of V_1 and V_2, and not the noise or the bit error rate of the fiber transmission system. The main concern is the transit time. The nominal values of critical parameters discussed before imply $T/\tau = 1250$. Except for an extremely short link span, the rate for key exchange is severely limited. For example, with a transit delay of 10 μs or 2 km of fiber, the duration of a symbol is 12.5 ms. The raw key exchange rate is only 40 b/s, which is very low. The opportunity for implementing the protocol is in digital communication systems. In digital systems, $V_+(0,t)$ and $V_-(L,t)$ are digitized. In addition, transmissions between Alice and Bob take place not in real time, but as responses to each other. Alice sends one digitized value of $V_+(0,t)$. So does Bob. After receiving the information, Bob calculates V_- and sends it back to Alice. So does Alice. In this case, τ represents the sampling time, i.e., time between digitization; again, $T >> \tau$. The transit time of the communication channel is no longer a critical parameter in the protocol. For the aforementioned critical parameters and 10-bit digitization, there are 1.25×10^4 bits in each symbol. For an optical link with a data rate of 10 Gb/s, the effective rate for raw key exchange can be 400 kb/s. Of course, the duration of real time needed to generate a key still depends on the transit time of the communication channel. After all, it takes T/τ or 1250 correspondences to establish a key element. However, Alice and Bob can establish multiple key elements simultaneously by using time-division multiplexing to realize the full effective rate.

In analyzing the security of the protocol, no restriction is imposed on the capability of the eavesdropper. Eve can detect the signal with arbitrarily high resolution both in time and sensitivity. In a normal man-in-the middle attack, Mallory intercepts the information sent by Alice and retransmits it to Bob. In the proposed protocol, information is embedded in the sign of the reflection coefficient. It can only be determined after many, e.g., 1250, rounds of signal exchange. Before knowing the information, i.e., the sign of reflection coefficient, Mallory can only relay signals between Alice and Bob. This gives Mallory no more advantage than performing passive eavesdropping. Mallory can pretend to be Bob by using his own random source to establish the shared secret key with Alice; likewise, with Bob. However, the key generated between him and Alice will not match the key generated between him and Bob. In addition, the signal in the channel is jointly generated by two parties in communication. When Mallory is in the middle, the signal received by Bob will be different from the signal sent by Alice and *vice versa*. Alice and Bob can use an authenticated channel to compare signals sent and received in each and every exchange. Any difference beyond certain limit determined by the transit delay immediately exposes Mallory. The proposed protocol is only vulnerable to the man-in-the-middle attack if Mallory can completely prevent Alice and Bob from communicating to each other. Any system, including quantum cryptography, is subject to the same vulnerability without authentication.

The optical carrier is not a concern in the proposed protocol. The feedback in the protocol involves no carrier reflection, only the feedback of the baseband modulation signal. Since $\langle V_+^2 \rangle \cong \langle V_-^2 \rangle$ nominally, there is no net energy flow from the node with positive reflection coefficient to the node with negative reflection coefficient. The power flow is balanced.

The security of the proposed protocol is derived from using secret keys. The key represents an integral part of the whole information. The eavesdropper and the legitimate user detect same signals, but Eve cannot decipher the information without the secret key.

The purpose of this paper is to demonstrate the principle of operation. Numerical results provide sufficient data to prove that the proposed protocol works. Future, analytical studies are expected to find bounds, e.g., maximum key generation rate, conditions needed to realize a prescribed limit on information leak, etc.

As shown in the follow-up study, the transit time poses as a serious security risk during the transient turn-on [23]. How-

ever, by ramping up the reflection coefficient and digitizing the signal with adequate sampling time and quantization accuracy, the security risk can be mitigated. Eve cannot decipher the information by using any transient signals.

V. Conclusion

The framework of a classical key agreement protocol using band-limited random signals with feedback is presented. The secret information possessed by Alice and Bob enables them to determine what is sent by the other party. Together they establish a shared key. Being denied access to the secret information, Eve has a much lower probability in correctly determining the key. The limited information that Eve gets is masked by the randomness of signals. Since many bytes of information exchange are needed to establish each element of the key, the system is communication intensive. This is different from key distribution systems that are computationally complex.

By performing statistical analysis, the performance of a specific protocol is studied. The difference in probabilities to successfully decipher is presented as a function of crucial parameters. Since it is a classical system, Alice and Bob know exactly what signals Eve detect. They can adopt additional countermeasures to enhance the security.

The protocol can be readily implemented in digital optical communications systems.

References

[1] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1996.

[2] H. Delfs and H. Knebl, *Introduction to Cryptography*, 2nd ed. Berlin, Germany: Springer-Verlag, 2007.

[3] L. E. Larson, J.-M. Liu, and L. S. Tsimring, *Digital Communications Using Chaos*. New York: Springer-Verlag, 2006.

[4] S. Donati and C. Mirasso, Eds., "Feature issue on "Optical chaos and applications to cryptography," *IEEE J. Quantum Electron.*, vol. 38, no. 9, pp. 1138–1140, Sep. 2002.

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

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

[7] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[8] U. M. Maurer, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, Mar. 1999.

[9] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5059–5067, Nov. 2008.

[10] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bangalore, India, 1984, pp. 175–179 [Online]. Available: http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf

[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Jan. 2002.

[12] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, "Long-distance quantum key distribution in optical fibre," *New J. Phys.* vol. 8, no. 9, p. 193, Sep. 2006 [Online]. Available: http://arxiv.org/ftp/quant-ph/papers/0607/0607177.pdf

[13] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nature Phys.* vol. 3, pp. 481–486, Jun. 2007 [Online]. Available: http://lanl.arxiv.org/ftp/quant-ph/papers/0607/0607182.pdf

[14] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Santa Fe, NM, Nov. 20–22, 1994, pp. 124–134 [Online]. Available: http://www-math.mit.edu/~shor/papers/algsfqc-dlf.pdf

[15] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[16] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

[17] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[18] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method of obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[19] L. B. Kish, "Totally secure classical communication utilizing Johnson-like noise and Kirchhoff's law," *Phys. Lett. A*, vol. 352, no. 3, pp. 178–182, Mar. 2006.

[20] R. Mingesz, Z. Gingl, and L. B. Kish, "Johnson(-like)-noise-Kirchhoff-loop based secure classical communicator demonstrated for ranges of two kilometers to two thousand kilometers," *Phys. Lett. A*, vol. 372, no. 7, pp. 978–984, Feb. 2008.

[21] P.-L. Liu, "A new look at the classical key exchange system based on amplified Johnson noise," *Phys. Lett. A* vol. 373, no. 10, pp. 901–904, Mar. 2009 [Online]. Available: http://dx.doi.org/10.1016/j.physleta.2009.01.022

[22] J. Muramatsu, K. Yoshimura, K. Arai, and P. Davis, "Some results on secret key agreement using correlated sources," *NTT Tech. Rev.* vol. 6, no. 2, 2008 [Online]. Available: https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200802rp1.pdf&mode=show_pdf

[23] P.-L. Liu, "Security risk during the transient in a key exchange protocol using random signals and feedback," *Phys. Lett. A* vol. 373, no. 36, pp. 3207–3211, Aug. 2009 [Online]. Available: http://dx.doi.org/10.1016/j.physleta.2009.07.030

[24] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, 1992.

[25] G. Brassard and L. Salvail, "Secret key reconciliation by public discussion," *Lecture Notes Comput. Sci.*, vol. 765, pp. 410–423, 1994.

[26] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

Pao-Lo Liu received the Ph.D. degree in applied physics from Harvard University, Cambridge, MA, in 1979.

During 1979 and 1984, he was with Bell Telephone Laboratories and Bell Communications Research. Since 1984, he has been with the Department of Electrical Engineering, University at Buffalo, The State University of New York, Buffalo. His current research interests include secure communication systems and distance learning.