Information Reconciliation Using Reliability in Secret Key Agreement Scheme with ESPAR Antenna

Takayuki Shimizu, Hisato Iwai, and Hideichi Sasaoka

Doshisha University, 1-3 Tatara, Miyakodani, Kyotanabe city, Kyoto, 610-0394 Japan
etj1101@mail4.doshisha.ac.jp, {iwai,hsasaoka}@mail.doshisha.ac.jp

Abstract. As a countermeasure for eavesdroppers in wireless communications, a secret key agreement scheme using a variable directional antenna called ESPAR antenna was developed. In this scheme, the process of information reconciliation is necessary to correct the discrepancies between the legitimate users' keys. In this paper, we propose a new information reconciliation protocol using the reliability of the raw keys. The proposed information reconciliation protocol is a modified version of the protocol used in quantum key distribution called Cascade. The results of simulations show that the proposed protocol can correct errors with less the number of disclosed bits and less the number of communications than those of Cascade.

Keywords: key agreement, ESPAR antenna, information reconciliation, Cascade.

1 Introduction

As wireless communications become increasingly pervasive, they are becoming targets for attacks. Unfortunately, it is easy for an adversary to eavesdrop wireless communications because of the broadcast nature of wireless communications. To establish secure communication links in wireless communications, two types of cryptographic techniques, public-key cryptography and symmetric-key cryptography, are generally used. In wireless LAN systems, the symmetric-key cryptography such as AES [1] is used because of its high processing speed. However, the symmetric-key cryptography has two operational issues: key distribution and key management. Moreover, since cryptographic techniques used currently are based on unproven assumptions regarding the hardness of computational problems, they would be broken if the assumptions were to be debunked.

Meanwhile, information-theoretic cryptography has been developing [2,3,4] as a cryptographic technique for which security is proven even against an adversary with unbounded computing power. There are several information-theoretically secure cryptographic techniques such as one-time pad [2] and secret communications over a noisy channel [3, 4]. To share one-time pad keys, an information-theoretically secure key agreement scheme from correlated source outputs was

A.U. Schmidt and S. Lian (Eds.): MobiSec 2009, LNICST 17, pp. 148–159, 2009.

proposed [5, 6]. Quantum key distribution [7] is also known as an information-theoretically secure key agreement scheme.

Recently, novel techniques utilizing radio propagation characteristics for secret key agreement have been developed [8,9,10,11] as information-theoretically secure key agreement. They exploit the reciprocity of radio propagation characteristics, which provides similar radio propagation characteristics for two communicating terminals, while it is difficult for an eavesdropper at a different location to obtain the similar characteristics because of the locality of the radio propagation characteristics. This is a good approach to solve the issues of key distribution and key management because they can provide a one-time key whenever it is needed. In particular, a secret key agreement scheme using an electronically steerable parasitic array radiator (ESPAR) antenna [12] is more effective for environments where the fluctuation of the radio propagation characteristics is slow such as indoor wireless LAN environments [9].

In the secret key agreement scheme using the ESPAR antenna, secret keys are generated based on received signal strength indicator (RSSI) profiles measured by two legitimate users. The generated raw keys, however, may contain some errors (the discrepancies between the legitimate users' keys), which are caused by the noise and other effects at the receivers. In this situation, the legitimate users need to eliminate or correct the errors by public discussion, while the amount of the information revealed in the public discussion to eliminate or correct errors is as little as possible. This process is called information reconciliation. So far, various information reconciliation protocols have been proposed [7, 9, 13, 14, 15]. Among them, Cascade [13] is representative one and is widely used in quantum key distribution because of its high performance being close to the theoretical limit on the number of exchanged bits.

In this paper, we propose a modified version of Cascade using the reliability of the keys in which RSSI information is used as the reliability to correct errors effectively. We carry out numerical simulations, and the results of the simulations show that our information reconciliation protocol is suitable for the secret key agreement scheme using the ESPAR antenna.

2 Secret Key Agreement Scheme Using ESPAR Antenna

In this section, we recall the secret key agreement scheme using the ESPAR antenna [9]. The assumed conditions are as follows. There are two legitimate users, an access point (AP) equipped with an ESPAR antenna and an user terminal (UT) equipped with an omni-directional antenna. There is also an eavesdropper equipped with an omni-directional antenna. AP and UT can communicate with an identical frequency by using a method such as time division duplex (TDD).

Figure 1 shows the procedure of the secret key agreement scheme. The procedure consists of three steps: (1) randomness sharing, (2) information reconciliation, (3) privacy amplification. In the randomness sharing, AP and UT

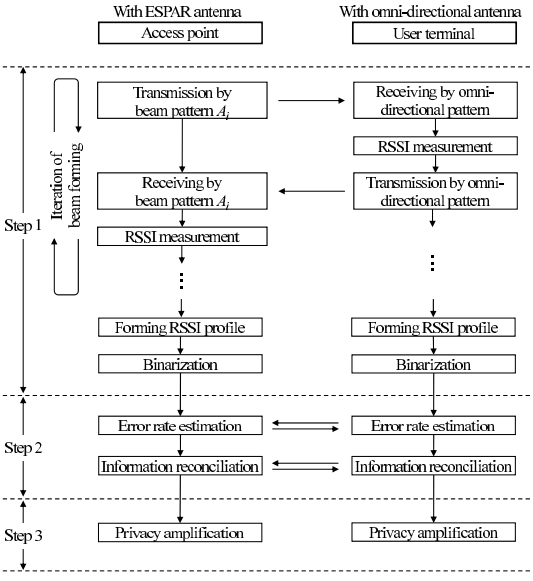


Fig. 1. Procedure of secret key agreement scheme using ESPAR antenna

generate key candidates from their RSSI profiles. Firstly, one terminal transmits one packet and the other measure RSSI alternately, where the beam pattern of the ESPAR antenna is fixed. Then, the beam pattern of the ESPAR antenna is switched randomly by changing the reactance values of the ESPAR antenna. This process is repeated until the sufficient length of RSSI profiles is obtained. After measuring the RSSI profiles, AP and UT binarize their RSSI profiles in order to generate key candidates, where the median of each RSSI profile is used as the threshold for binarization.

In the information reconciliation, AP and UT correct the discrepancies between their key candidates by public discussion. To eliminate the errors, AP and UT remove RSSIs around the threshold, where the positions to be removed are sent over a public channel because such the RSSIs are susceptible to the noise. Furthermore, the remaining errors are corrected based on the syndromes of the key candidates by applying error correcting techniques, where the syndrome of UT is sent over the public channel. To minimize the amount of the information leaked to the eavesdropper, AP and UT estimate the bit error rate of the key candidates by generating and disclosing dummy keys [16], and they set appropriate parameters of the information reconciliation protocol such as the length of elimination and an error correcting code.

In the privacy amplification, AP and UT generate a secure secret key from the identical key candidates by diminishing the partial information leaked to the eavesdropper. The privacy amplification can be realized by using universal hash functions [17]. Thus, AP and UT share an identical secure secret key.

3 Cascade Protocol

In this section, we recall Cascade protocol [13]. The conventional information reconciliation protocol using error correcting codes [9] may introduce additional errors if the number of errors is greater than the error correcting capability, and the reconciliation fails. In contrast, Cascade never introduces additional errors, and the number of errors decreases exponentially by iteratively applying Cascade.

Before describing the algorithm of Cascade, we explain BINARY, which plays the role in detecting and correcting the discrepancies of the legitimate users' keys in Cascade. An example of BINARY is shown in Fig. 2. When the legitimate users' keys have an odd number of errors, AP and UT perform an interactive binary search to find and correct an error in the following manner.

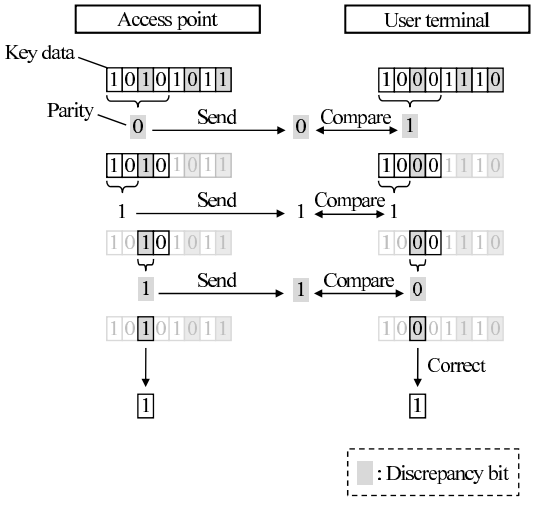


Fig. 2. Example of BINARY

BINARY:

1. AP and UT calculate the parity of the first half of their key candidates.
2. AP sends UT the calculated parity.
3. UT determines whether an odd number of errors occurred in the first half or in the last half by comparing the parity of UT to that of AP.
4. The steps 1∼3 are repeatedly applied to the half block determined in the step 3 until one error is found. Finally, the found error is corrected.

Let us now describe the algorithm of Cascade. Cascade proceeds in several passes. The number of passes is determined by the legitimate users before execution. AP and UT perform Cascade in the following manner.

Cascade:

1. AP and UT permute their key candidates in random order.
2. In the pass i, AP and UT divide the permuted key candidates into blocks of k_i bits and calculate the parities of all the blocks.
3. AP sends the parities of all AP's blocks to UT.
4. By using BINARY, UT corrects an error in each block whose parity differs from that of AP's corresponding block. At this point, the blocks of AP and UT in the pass i have an even number of errors.
5. In the pass i (> 1), let l be the position of the bit corrected at the step 4. AP and UT find that the blocks including l in the passes $1 \sim i-1$ have an odd number of errors. Let $\mathcal{A}$ be the set of the blocks including l.
6. AP and UT choose the smallest block in $\mathcal{A}$ and use BINARY to find and correct another error.
7. Let l' be the position of the bit corrected at the step 6 and $\mathcal{B}$ be the set of the blocks including l' in the passes $1 \sim i$. AP and UT find that the blocks of the set $(\mathcal{B} \cup \mathcal{A}) \backslash (\mathcal{B} \cap \mathcal{A})$ have an odd number of errors.
8. AP and UT update the set $\mathcal{A}$ according to $\mathcal{A} \leftarrow (\mathcal{B} \cup \mathcal{A}) \backslash (\mathcal{B} \cap \mathcal{A})$.
9. The steps 6∼8 are repeatedly applied until $\mathcal{A} = \emptyset$, at which the pass i ends. At the end of the pass i, each block in the passes $1 \sim i$ has an even number of errors (perhaps zero).

In Cascade, almost all errors are corrected until the end of the pass 2 when the appropriate block length is set in each pass [18]. The block lengths k_1 of the pass 1 and k_2 of the pass 2 minimizing the number of disclosed bits are as follows:

$$k_1 = \left\lfloor \frac{4 \ln 2}{3 p_{\mathrm{e}}} \right\rfloor \tag{1}$$

$$k_2 = \left\lfloor \frac{4 \ln 2}{p_{\mathrm{e}}} \right\rfloor, \tag{2}$$

where p_{e} denotes the bit error rate of the keys. In the case of k_i ($i \geq 3$), the block lengths have not been optimized. The original Cascade [13] sets k_i ($i \geq 3$) as follows:

$$k_i = 2k_{i-1} \quad (i \geq 3). \tag{3}$$

In practice, we estimate the bit error rate p_{e} by using dummy keys and set the block lengths according to Eqs. (1) ∼ (3).

4 Cascade Using Reliability

In this section, we propose a modified version of Cascade using the reliability of the keys, which is suitable for the secret key agreement scheme using the ESPAR antenna. When we apply the conventional Cascade to the secret key agreement using the ESPAR antenna, BINARY is not the best method to search and correct errors because BINARY searches errors with binary search using only binary

key data and does not utilize RSSI information. Let K_x and K_y be the random variables of AP's key and UT's key, respectively. In this case, the conventional Cascade is considered hard-decision information reconciliation, and therefore AP and UT need to exchange at least

$$n_{\min}^{\text{hard}} = nH(K_x|K_y) = nH(K_y|K_x) \tag{4}$$

of information on average for their reconciliation by the Slepian-Wolf theorem [19], where n and $H(A|B)$ denote the key length and the conditional entropy of A given B, respectively.

In the proposed protocol, BINARY is replaced with error correction using the reliability of the keys in which we utilize RSSI information as the reliability measure to search errors effectively. Let R_x and R_y be the random variables of AP's RSSI and UT's RSSI, respectively. In this case, the proposed protocol is considered soft-decision information reconciliation, and therefore AP and UT need to exchange at least

$$\begin{aligned} n_{\min}^{\text{soft}} &= nH(K_x|K_y, R_y) \\ &= nH(K_x|R_y) \quad (\because H(K_y|R_y) = 0) \\ &= nH(K_y|R_x) \\ &\leq n_{\min}^{\text{hard}} \end{aligned} \tag{5}$$

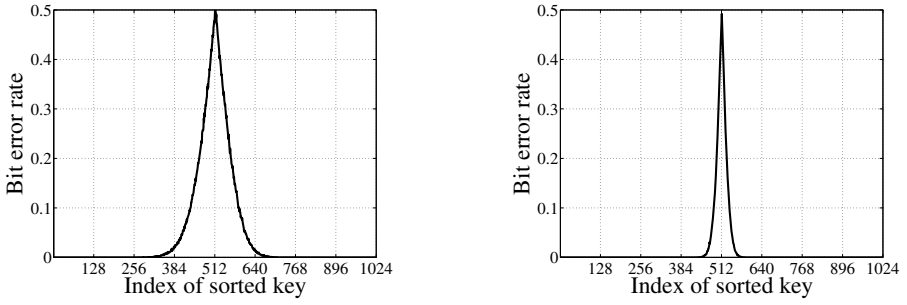
of information on average for their reconciliation. Equation (5) shows that we can correct errors with less the number of disclosed bits by utilizing RSSI information than that of the conventional Cascade.

Before describing the algorithm of the error correction using the reliability, we define the reliability of the keys by taking into account a feature of key candidate generated from RSSI profile. Figure 3 shows examples of the bit error rate with regard to each bit of key candidates of 1024 bit sorted in ascending order of RSSI when SNR (Signal to Noise Ratio) is 20 dB and 30 dB. It can be seen from this figure that the bit error rate of key bits near the threshold of binarization, i.e. the median, is higher because key bits near the threshold are more susceptible to the noise. This figure allows us to conclude that key bits near the threshold of binarization have lower reliability. By taking into account the fact, we define the reliability α_i of the i th key bit as

$$\alpha_i = |r_i - r_{\text{th}}|, \tag{6}$$

where r_i and r_{th} denote the i th measured RSSI and the threshold of binarization, respectively.

Having defined the reliability, we will now explain the algorithm of the error correction using the reliability. An example of the error correction using the reliability is shown in Fig. 4. When the legitimate users' keys have an odd number of errors, AP and UT perform an interactive reliability-based search to find and correct an error in the following manner.



(a) SNR=20 dB (b) SNR=30 dB

Fig. 3. Examples of bit error rate with regard to each bit of key candidates sorted in ascending order of RSSI

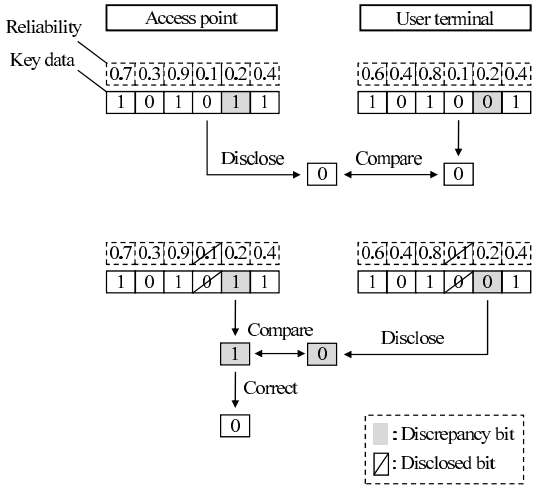


Fig. 4. Example of error correction using reliability in proposed protocol

Error correction using reliability:

1. AP sends the least reliable bit among the undisclosed bits to UT.
2. UT compares the bit sent by AP to the corresponding bit of UT. If the compared bits are different, UT corrects the error. If the compared bits are equal, UT sends the least reliable bit among the undisclosed bits to AP.
3. AP compares the bit sent by UT to the corresponding bit of AP. If the compared bits are different, AP corrects the error. If the compared bits are equal, AP sends the least reliable bit among the undisclosed bits to UT.
4. The steps 2∼3 are repeatedly applied until one error is corrected.

5 Simulation Setting

5.1 System Model

We developed test equipment using ZigBee^{TM} [20], which conforms to IEEE802.15.4, of the secret key agreement scheme using the ESPAR antenna [9]. Therefore, we carry out numerical simulations assuming a model of IEEE802.15.4 to evaluate the performance of the proposed protocol. There are AP equipped with an ESPAR antenna and UT equipped with an omni-directional antenna. We assume that the eavesdropper is a passive attacker, i.e. she only listens to communications between AP and UT and does not interfere into them.

5.2 Simulation Model

Figure 5 shows the environment of the simulation. There are AP and UT in the same room enclosed by concrete walls on four sides in which there are no reflecting and scattering objects. The size of the room is 10 m × 8 m. Throughout the simulation, the position of AP is fixed to the center of the room, (0.0 m, 0.0 m), and the position of UT is fixed to (3.0 m, 2.0 m).

The parameters of the simulation are specified in Table 1. AP uses a 7-elements ESPAR antenna. The reactance vector of the ESPAR antenna is set randomly at every RSSI measurement. The carrier frequency is set to 2.480 GHz. The ray-tracing technique [21] is used to generate the propagation channel characteristics considering the effect of difference in receive levels and phases between the terminals. To simplify the calculation, we assume a 2-dimentional model of indoor environment neglecting the effect of the floor and the ceiling. We take into account up to 6 times reflections by the walls. The key length is set to 1024 bit. We perform information reconciliation only by using Cascade or the proposed protocol without other information reconciliation protocols such as the

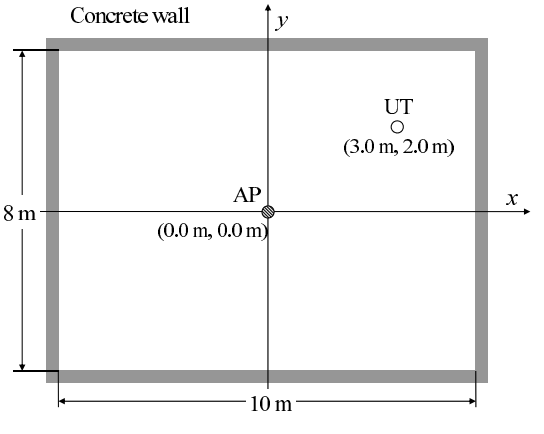


Fig. 5. Simulation environment

Table 1. Parameters of the simulations

Room size	8 m × 10 m
Positions	AP: (0.0 m, 0.0 m) UT: (3.0 m, 2.0 m)
Antennas	AP: 7-elements ESPAR antenna UT: omni-directional antenna
Carrier frequency	2.480 GHz
Channel model	2D Ray-tracing Reflection: up to 6 times Vertical polarization
Wall material	Concrete ($\varepsilon_r = 6.76$, $\sigma = 0.0023\,\mathrm{S/m}$, $\mu_r = 1$)
Reactance vector	Random
Key length	1024 bit
Information reconciliation	Cascade or proposed protocol

reconciliation protocol using error correcting codes. In Cascade and the proposed protocol, we assume the bit error rate of keys are known, and hence the block length of each pass is optimized according to Eqs. (1) $\sim$ (3).

6 Simulation Results

In this section, we show the comparisons of performance between the proposed protocol and Cascade when SNR varies.

6.1 The Number of Disclosed Bits

Figure 6 shows the number of disclosed bits in information reconciliation until the discrepancies of the legitimate users' keys are completely corrected. In this figure, we also indicate the theoretical limit calculated from Eqs. (4) and (5). From this figure, we observe that by using the proposed protocol, we can decrease the number of disclosed bits at all values of SNR and can achieve performance being close to the theoretical limit of soft-decision information reconciliation.

6.2 The Number of Communications

We consider the number of communications in information reconciliation. We defined the number of communications as the number of times a protocol discloses parities or key bits until the discrepancies of the legitimate users' keys are completely corrected. Figure 7 shows the number of communications in information reconciliation. It can be seen from the figure that when SNR is more than 10 dB, the proposed protocol can correct the discrepancies with less the number of communications than that of Cascade. The reason why the number of communications around SNR of 0 dB is fewer is because the block length around SNR of 0 dB is so short (probably 2 bits) that the discrepancies of the keys can be corrected with a few number of communications.

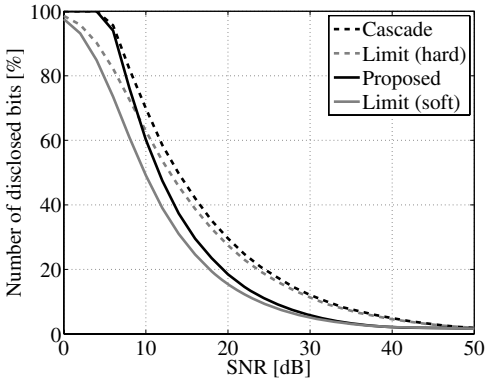


Fig. 6. Number of disclosed bits in information reconciliation

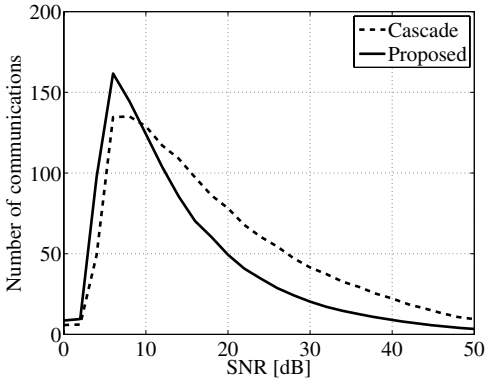


Fig. 7. Number of communications in information reconciliation

6.3 The Efficiency of Protocol

We consider the efficiency of a protocol [15] which indicate how close the protocol is to the theoretical limit. The efficiency of Cascade is defined as follows:

$$\zeta^{\mathrm{hard}} = \frac{H(K_x) - n^{-1}C^{\mathrm{hard}}}{H(K_x) - H(K_x|K_y)} \leq 1, \tag{7}$$

where C^{hard} denotes the number of disclosed bits in Cascade. On the other hand, the efficiency of the proposed protocol is defined as follows:

$$\zeta^{\mathrm{soft}} = \frac{H(K_x) - n^{-1}C^{\mathrm{soft}}}{H(K_x) - H(K_x|R_y)} \leq 1, \tag{8}$$

where C^{soft} denotes the number of disclosed bits in the proposed protocol. Note that the denominators of Eqs. (7) and (8) are different because Cascade is

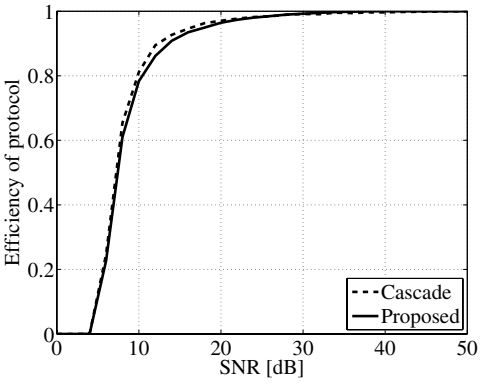


Fig. 8. Efficiency of protocol

hard-decision reconciliation protocol, while the proposed protocol is soft-decision reconciliation protocol.

Figure 8 shows the efficiency of Cascade and the proposed protocol calculated by Eqs. (7) and (8). The efficiency of the proposed protocol is almost identical with that of Cascade. In SNRs above 20 dB, the both achieve efficiency over 0.95. From this result, we can say that the proposed protocol successfully utilizes RSSI information.

7 Conclusion

In this paper, we propose a new information reconciliation protocol using the reliability of the keys for the secret key agreement scheme using the ESPAR antenna. The proposed information reconciliation protocol is a modified version of Cascade protocol utilizing RSSI as the reliability, which is suitable for the secret key agreement scheme using the ESPAR antenna. As the results of the simulations, we can conclude that the proposed protocol can correct errors with less the number of disclosed bits and less the number of communications than those of Cascade.

References

1. Daemen, V.R.J.: The Design of Rijndael: AES–The Advanced Encryption Standard. Springer, Heidelberg (2002)
2. Shannon, C.E.: Communication theory of secrecy systems. Bell syst. Tech. J. 28, 656–715 (1949)
3. Wyner, A.D.: The wire-tap channel. Bell syst. Tech. J. 54(8), 1355–1387 (1975)
4. Csiszár, I., Körner, J.: Broadcast channels with confidential messages. IEEE Trans. Inform. Theory 24(3), 339–348 (1978)
5. Maurer, U.M.: Secret key agreement by public discussion from common information. IEEE Trans. Inform. Theory 39(3), 733–742 (1993)

6. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography–Part I: Secret sharing. IEEE Trans. Inform. Theory 39(4), 1121–1132 (1993)
7. Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental quantum cryptography. J. Cryptology 5(1), 3–28 (1992)
8. Hershey, J.E., Hassan, A.A., Yarlagadda, R.: Unconventional cryptographic keying variable management. IEEE Trans. Commun. 43(1), 3–6 (1995)
9. Aono, T., Higuchi, K., Ohira, T., Komiyama, B., Sasaoka, H.: Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. IEEE Trans. Antennas and Propagation 53(11), 3776–3784 (2005)
10. Wilson, R., Tse, D., Scholtz, R.: Channel identification: secret sharing using reciprocity in UWB channels. IEEE Trans. Inform. Forensics and Security 2(3), 364–375 (2007)
11. Bloch, M., Barros, J., Rodrigues, M., McLaughlin, S.: Wireless information-theoretic security. IEEE Trans. Inform. Forensics and Security 54(6), 2515–2534 (2008)
12. Kawakami, H., Ohira, T.: Electrically steerable passive array radiator (ESPAR) antennas. IEEE Antennas and Propagation Magazine 47(2), 43–50 (2005)
13. Brassard, G., Salvail, L.: Secret key reconciliation by public discussion. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 410–423. Springer, Heidelberg (1994)
14. Buttler, W.T., Lamoreaux, S.K., Torgerson, J.R., Nickel, G.H., Donahue, C.H., Peterson, C.G.: Fast, efficient error reconciliation for quantum cryptography. Phys. Rev. A. 67(5), 052303 (2003)
15. Bloch, M., Thangaraj, A., McLaughlin, S., Merolla, J.: LDPC-based gaussian key reconciliation. In: 2006 IEEE Inform. Theory Workshop (ITW 2006), Punta del Este, Uruguay, pp. 116–120 (2006)
16. Imai, H., Kobara, K., Morozov, K.: On the possibility of key agreement using variable directional antenna. In: 1st Joint Workshop on Inform. Security (JWIS 2006), Seoul, Korea, pp. 153–167 (2006)
17. Bennett, C., Brassard, G., Crépeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. Inform. Theory 41(6), 1915–1923 (1995)
18. Sugimoto, T., Yamazaki, K.: A study on secret key reconciliation protocol "Cascade". IEICE Trans. Fundamentals E83-A(10), 1987–1991 (2000)
19. Slepian, D., Wolf, J.: Noiseless coding of correlated information sources. IEEE Trans. Inform. Theory 19(4), 471–480 (1973)
20. ZigBee Alliance, `http://www.zigbee.org/`
21. Goldsmith, A.: Wireless communications. Cambridge University Press, Cambridge (2005)