entropy

MDPI

Article

An Efficient Advantage Distillation Scheme for Bidirectional Secret-Key Agreement

Yan Feng [1,†], Xue-Qin Jiang [1,*,†], Jia Hou [2,†], Hui-Ming Wang [3,†] and Yi Yang [1,†]

1 School of Information Science and technology, Donghua University, Shanghai 201620, China; 2151167@mail.dhu.edu.cn (Y.F.); yiyang@dhu.edu.cn (Y.Y.)
2 School of electronics and information, Soochow University, Soochow 215000, China; houjia@suda.edu.cn
3 School of electronic and Information Engineering, Xi'an Jiao Tong University, Xi'an 710000, China; xjbswhm@163.com
* Correspondence: xqjiang@dhu.edu.cn; Tel.: +86-181-4970-8519
† These authors contributed equally to this work.

Received: 30 July 2017; Accepted: 14 September 2017; Published: 18 September 2017

Abstract: The classical secret-key agreement (SKA) scheme includes three phases: (a) advantage distillation (AD), (b) reconciliation, and (c) privacy amplification. Define the transmission rate as the ratio between the number of raw key bits obtained by the AD phase and the number of transmitted bits in the AD. The unidirectional SKA, whose transmission rate is 0.5, can be realized by using the original two-way wiretap channel as the AD phase. In this paper, we establish an efficient bidirectional SKA whose transmission rate is nearly 1 by modifying the two-way wiretap channel and using the modified two-way wiretap channel as the AD phase. The bidirectional SKA can be extended to multiple rounds of SKA with the same performance and transmission rate. For multiple rounds of bidirectional SKA, we have provided the bit error rate performance of the main channel and eavesdropper's channel and the secret-key capacity. It is shown that the bit error rate (BER) of the main channel was lower than the eavesdropper's channel and we prove that the transmission rate was nearly 1 when the number of rounds was large. Moreover, the secret-key capacity C_s was from 0.04 to 0.1 as the error probability of channel was from 0.01 to 0.15 in binary symmetric channel (BSC). The secret-key capacity was close to 0.3 as the signal-to-noise ratio increased in the additive white Gaussian noise (AWGN) channel.

Keywords: two-way wiretap channel (TWWC); secret-key agreement (SKA); transmission rate; secret-key capacity

1. Introduction

The one-time pad was developed by Vernam [1], by which a group of users can communicate messages among themselves securely if they share a common secret key beforehand. However, the key rate should be at least the message rate [2], and so the problem of secure communication effectively turns into the problem of secret-key agreement (SKA). In the SKA problem, legitimate users Alice and Bob aim at agreeing on a sequence of bits (key) that must be kept secret from the passive eavesdropper Eve. As shown in Figure 1, the classical SKA scheme includes three phases: (a) advantage distillation (AD), (b) reconciliation, and (c) privacy amplification [3]. AD aims to provide the legitimate agents an advantage over the eavesdropper. Information reconciliation aims at generating an identical random sequence at both Alice and Bob. Privacy amplification is the step that extracts a secret key from the identical random sequence agreed upon by the legitimate agents [4].

Bounds for the secret-key capacity have been derived for a large variety of communication channels [5–9]. Unfortunately, most do not provide direct insight into the design of practical secret-key capacity-achieving schemes. SKA based on noisy channels was presented in [5,10] using an additional

insecure but authenticated public channel in which a third party can eavesdrop the communication but cannot forge it. This approach was recently extended in [11] to the model where the players share correlated Gaussian sources. In [12], opportunistic transmission was proposed for SKA over the quasi-static fading channel by sending signals only when the channel condition for the two legitimate players is better than the one for an adversary. The use of the reciprocity of wireless channels has been studied in [13–15] to study the key agreement. In [16], the SKA with public discussion was studied based on Gaussian and fading channels.

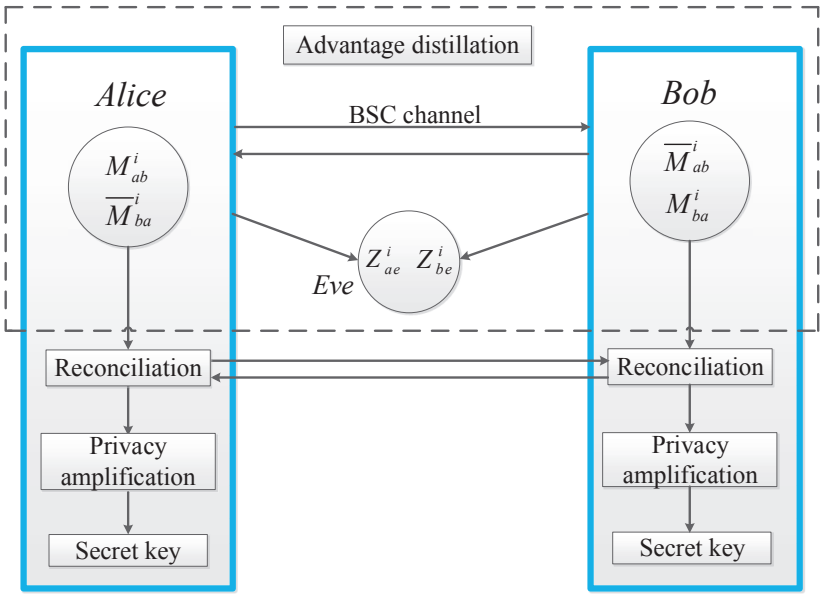

Figure 1. Block diagram of the secret key agreement (SKA) scheme.

It is well known that Wyner [17] introduced the wiretap channel, in which a sequence M is transmitted from Alice to Bob over the main channel, while Eve is wiretapping over the eavesdropper's channel. Wyner proved that Alice could send M to Bob in almost perfect secrecy if the main channel between Alice and Bob is better than Eve's eavesdropper channel. Nevertheless, the assumption that the main channel is better (lower error rate) than the eavesdropper's channel is generally impractical. This problem can be solved by using a two-way communication (TWC) as the main channel [18]. By using TWC, the message received by Eve over the eavesdropper's channel is noisier than the message received by Bob. Therefore, the TWC scheme can be used as an AD scheme. Obviously, if we combine this AD scheme with any reconciliation and privacy amplification steps, the result can be used as secret keys between Alice and Bob [19]. However, the SKA of [18] is unidirectional from Alice to Bob, and therefore the transmission rate of this SKA is slow.

In this paper, emphasis is placed on the AD over the binary symmetric channel (BSC) and additive white Gaussian noise (AWGN) channel. We present a novel approach in building the two-way wiretap channel (TWWC) for bidirectional SKA. Different from all previous works, we will modify the original TWC scheme to be a bidirectional AD scheme to increase the transmission rate of the SKA and study the proposed AD over BSC and AWGN channel. We calculate the secret-key capacity of the proposed AD scheme to measure how many secret key bits can be shared between Alice and Bob. The advantages of the proposed bidirectional AD scheme are as follows.

- The proposed AD scheme provides an advantage of Alice and Bob over Eve when the channel between Alice and Bob is not less noisy than Eve's eavesdropper channel.
- The unidirectional SKA—whose transmission rate is 0.5—can be realized by using the original TWWC as the AD scheme. However, a bidirectional SKA whose transmission rate is 1 can be realized by using the proposed AD scheme.

The remainder of this paper is organized as follows. Section 2 presents a general two-way wiretap channel; A single round of the SKA with the proposed AD scheme is introduced in Section 3; The proposed AD scheme is extended to multiple rounds and is introduced in Section 4; Section 5 proposes a bidirectional secret-key agreement over AWGN channel; Section 6 shows performances of the proposed systems; Finally, conclusions are drawn in Section 7.

2. Original Two-Way Wiretap Channel

2.1. Transmission Scheme

A TWWC between Alice and Bob was described in [18], in which the channel from Alice to Bob was considered to be error-free due to the powerful Low Density Parity Check (LDPC) codes. In this paper, we consider an original TWWC model shown in Figure 2, in which both main channel and eavesdropper channel are not error free.

The notations used throughout this paper are given in Table 1. In the conventional TWWC, to initiate a secure communication, Bob first transmits a random sequence Q to Alice. For $i = 1, 2, \cdots, l$, the raw keys are M^i_{ab} and M^i_{ba}, the error vectors of the main channel and the eavesdropper's channel are E^i_{ab}, E^i_{ba}, E^i_{ae}, and E^i_{be}. E^0_{ba} denotes the error vector of the main channel and E^0_{be} denotes the error vector of the eavesdropper's channel. The superscript 0 represents the process where Bob sends a random sequence Q to Alice and i represents that a raw key M is transmitted in the i-th round. The subscripts ab, ba and ae, be denote sequences transmitted from Alice to Bob, from Bob to Alice and sequences wiretapped from Alice to Eve, and from Bob to Eve. We assume that the length of each sequence is n, so that the received sequences of Alice and Eve are

$$T_1 = E^0_{ba} \oplus Q, \tag{1}$$

$$TA_1 = E^0_{be} \oplus Q, \tag{2}$$

respectively, where the binary operator $\oplus$ denotes exclusive OR (XOR) operation [20]. Then, Alice uses the received sequence T_1 to calculate

$$U_1 = T_1 \oplus M^1_{ab}. \tag{3}$$

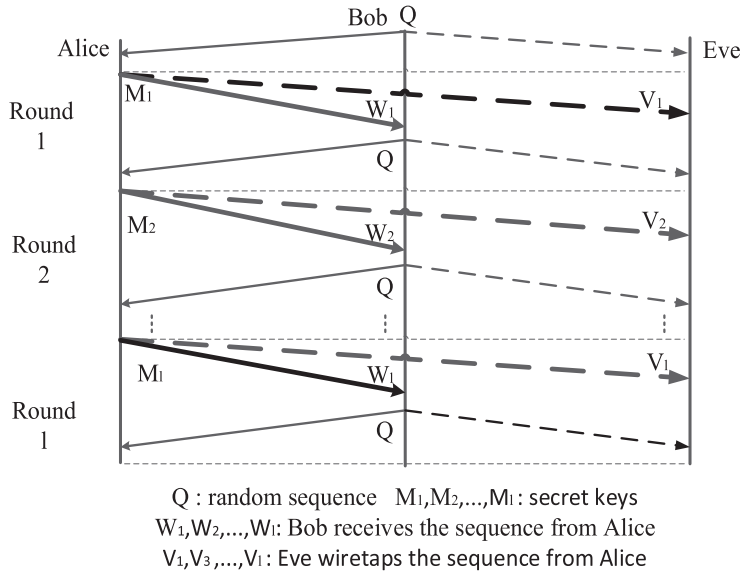

Figure 2. Advantage Distillation Scheme based on the original two-way wiretap channel.

Table 1. Symbols.

Symbols	Meaning
M_i	raw keys
Q	random sequence
E_{ba}^0	noise vector from Bob to Alice over BSC channel
E_{be}^0	noise vector from Bob to Eve over BSC channel
E_{ab}^i	noise vector from Alice to Bob over BSC channel
E_{ba}^i	noise vector from Bob to Alice over BSC channel
E_{ae}^i	noise vector from Alice to Eve over BSC channel
E_{be}^i	noise vector from Bob to Eve over BSC channel
T_1	noisy version of Q obtained by Alice
TA_1	noisy version of Q obtained by Eve
U_i	raw keys covered by T_i
V_i	noisy version of U_i obtained by Bob or Alice
T_i	equals to V_{i-1}
W_i	noisy version of U_i obtained by Eve
$\bar{M}_{ab}^1$	noisy version of raw keys obtained by Bob or Alice
Z_{ae}^1	noisy version of raw keys obtained by Eve
L_M	number of raw keys M
L_Q	number of random sequence Q
α	cross over probability between Alice and Bob
β	cross over probability between legitimate users and Eve
n_{ab}^i	noise vector from Alice to Bob over AWGN channel
n_{ba}^i	noise vector from Bob to Alice over AWGN channel
n_{ae}^i	noise vector from Alice to Eve over AWGN channel
n_{be}^i	noise vector from Bob to Eve over AWGN channel
C_m	capacity of the main channel
C_w	capacity of the eavesdropper's channel
C_s	secret-key capacity

Alice transmits U_1 to Bob through the main channel and Eve may wiretap this U_1 through the eavesdropper's channel. Bob and Eve can receive the noisy version of U_1, respectively, as

$$V_1 = U_1 \oplus E_{ab}^1, \tag{4}$$

$$W_1 = U_1 \oplus E_{ae}^1. \tag{5}$$

Since Bob knows the random sequence Q, he can XOR Q to U as

$$\bar{M}_{ab}^1 = V_1 \oplus Q = M_{ab}^1 \oplus E_{ba}^0 \oplus E_{ab}^1. \tag{6}$$

Eve only knows TA_1, which is the noisy version of Q, and she can only XOR TA_1 to W_1 as

$$Z_{ae}^1 = W_1 \oplus TA_1 = M_{ab}^1 \oplus E_{ba}^0 \oplus E_{be}^0 \oplus E_{ae}^1. \tag{7}$$

As shown in Figure 3, the raw key M is transmitted unidirectionally from Alice to Bob in the original TWWC. By comparing $\bar{M}_{ab}^1$ and Z_{ae}^1, Eve has one more noisy term than Bob. Therefore, as long as the main channel is not worse than the passive eavesdropper's channel (the weight of E_{ba}^0 is not higher than that of E_{be}^0 and E_{ae}^1), it is guaranteed that Eve is unable to arrive at the same sequence as

Alice and Bob. Alice and Bob can use any reconciliation scheme and privacy amplification function to transform the raw key $\bar{M}_{ab}^{1}$ and Z_{ae}^{1} into a much shorter secret key. Because of her errors, Eve is unable to predict Alice's or Bob's output of the privacy amplification. Finally, the secret key would be used as a one-time pad to ensure information-theoretic security between Alice and Bob. Furthermore, it is easy to see that this SKA is unidirectional from Alice to Bob. If Bob wants to send raw keys to Alice, they need another secure transmission with their roles exchanged.

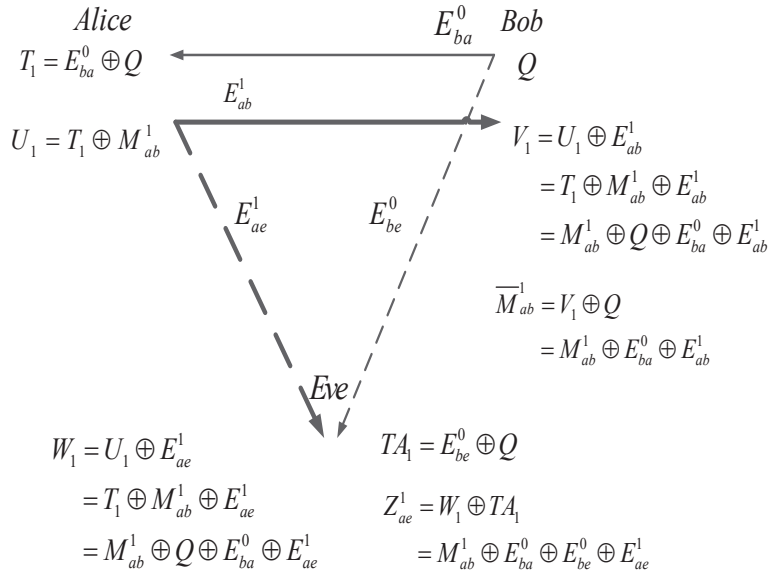

Figure 3. Original two-way wiretap channel.

2.2. Transmission Rate

Following the literature [3], we denote η as the transmission rate of the AD scheme. Let L_M be the number of raw keys, and L_Q be the number of random sequences. Then, the transmission rate is calculated as

$$\eta = \frac{L_M}{L_M + L_Q}. \tag{8}$$

Following the definition, the transmission rate η_{uni} of the original unidirectional TWC scheme is

$$\eta_{uni} = \frac{n}{n+n} = \frac{1}{2}. \tag{9}$$

3. Bidirectional Secret-Key Agreement

If we use the above TWWC for AD in SKA, the raw keys are unidirectionally transmitted from Alice to Bob and the transmission rate η_{uni} is just $\frac{1}{2}$. In order to increase the transmission rate of the SKA, we modify the original unidirectional TWWC to a bidirectional TWWC for the AD step of the SKA between Alice and Bob .

3.1. Proposed Advantage Distillation scheme

Assuming that there are l rounds of SKA between Alice and Bob, the first round of the proposed bidirectional AD scheme is as follows.

3.1.1. Preprocessing

Bob sends a random sequence Q, $Q = (q_0, q_1, \cdots, q_{n-1})$ to Alice. The received sequences by Alice and Eve, respectively, are

$$T_1 = Q \oplus E_{ba}^0, \tag{10}$$

$$TA_1 = Q \oplus E_{be}^0, \tag{11}$$

where $T_1 = (t_0^1, t_1^1, \cdots, t_{n-1}^1), t_k^1 = q_k \oplus e_{ba_k}^0$ and $TA_1 = (ta_0^1, ta_1^1, \cdots, ta_{n-1}^1), ta_k^1 = q_k \oplus e_{be_k}^0$, $0 \leq k \leq n-1$.

3.1.2. SKA from Alice to Bob

(A1. 1) Alice uses the received sequence T_1 to calculate

$$U_1 = T_1 \oplus M_{ab}^1, \tag{12}$$

where $U_1 = (u_0^1, u_1^1, \cdots, u_{n-1}^1), u_k^1 = t_k^1 \oplus m_{ab_k}^1$. Alice sends U_1 over the main channel and Eve wiretaps U_1 through the eavesdropper's channel.

(A1. 2) Bob and Eve receive the noisy version of U_1 as V_1 and W_1, respectively, as

$$V_1 = U_1 \oplus E_{ab}^1 = M_{ab}^1 \oplus Q \oplus E_{ba}^0 \oplus E_{ab}^1, \tag{13}$$

$$W_1 = U_1 \oplus E_{ae}^1 = M_{ab}^1 \oplus Q \oplus E_{ba}^0 \oplus E_{ae}^1. \tag{14}$$

(A1. 3) Bob knows Q, so he can XOR Q to V_1 as

$$\bar{M}_{ab}^1 = V_1 \oplus Q = M_{ab}^1 \oplus E_{ba}^0 \oplus E_{ab}^1, \tag{15}$$

where $\bar{M}_{ab}^1 = (\bar{m}_{ab_0}^1, \bar{m}_{ab_1}^1, \cdots, \bar{m}_{ab_{n-1}}^1)$ is the received raw key. Eve only knows the noisy version of Q, which is TA_1. Therefore, she can only XOR TA_1 to W_1 as

$$Z_{ae}^1 = W_1 \oplus TA_1 = M_{ab}^1 \oplus E_{ba}^0 \oplus E_{be}^0 \oplus E_{ae}^1, \tag{16}$$

where $Z_{ae}^1 = (z_{ae_0}^1, z_{ae_1}^1, \cdots, z_{ae_{n-1}}^1)$ in the eavesdropped raw key.

3.1.3. SKA from Bob to Alice

(B1. 1) Before Bob sends the raw key M_{ba}^1 to Alice, he has to make

$$T_2 = V_1. \tag{17}$$

Then, we can calculate

$$U_2 = T_2 \oplus M_{ba}^1 \tag{18}$$

and send U_2 to Alice through the main channel when Eve wiretaps it via the eavesdropper's channel.

(B1. 2) In this step, when Bob transmits the sequence U_2 to Alice, the noise of the two channels are E_{ba}^1 and E_{be}^1, respectively. Both Alice and Eve receive a noisy version of U_2 as V_2 and W_2:

$$V_2 = U_2 \oplus E_{ba}^1 = M_{ba}^1 \oplus U_1 \oplus E_{ab}^1 \oplus E_{ba}^1, \tag{19}$$

$$W_2 = U_2 \oplus E_{be}^1 = M_{ba}^1 \oplus U_1 \oplus E_{ab}^1 \oplus E_{be}^1. \tag{20}$$

(B1. 3) Alice has the knowledge of U_1 and Eve has the knowledge of W_2, therefore Alice can obtain the intended raw key by

$$\bar{M}_{ba}^{1} = V_2 \oplus U_1 = M_{ba}^{1} \oplus E_{ab}^{1} \oplus E_{ba}^{1} \tag{21}$$

and Eve can obtain the intended sequence by

$$Z_{be}^{1} = W_2 \oplus W_1 = M_{ba}^{1} \oplus E_{ab}^{1} \oplus E_{ae}^{1} \oplus E_{be}^{1}. \tag{22}$$

Step A1 and Step B1 correspond to the first round of our proposed bidirectional AD scheme for SKA, which is shown in Figure 4. Note that Steps A1.1–A1.3 provide raw keys M_{ab}^{1} and $\bar{M}_{ab}^{1}$; we can do the reconciliation to correct errors between M_{ab}^{1} and $\bar{M}_{ab}^{1}$ and do the privacy amplification to get the secret keys shared between Alice and Bob. Similarly, Steps B1.1–B1.3 provide raw keys M_{ba}^{1} and $\bar{M}_{ba}^{1}$, based on which we can also do the reconciliation and privacy amplification steps and obtain secret keys between Alice and Bob.

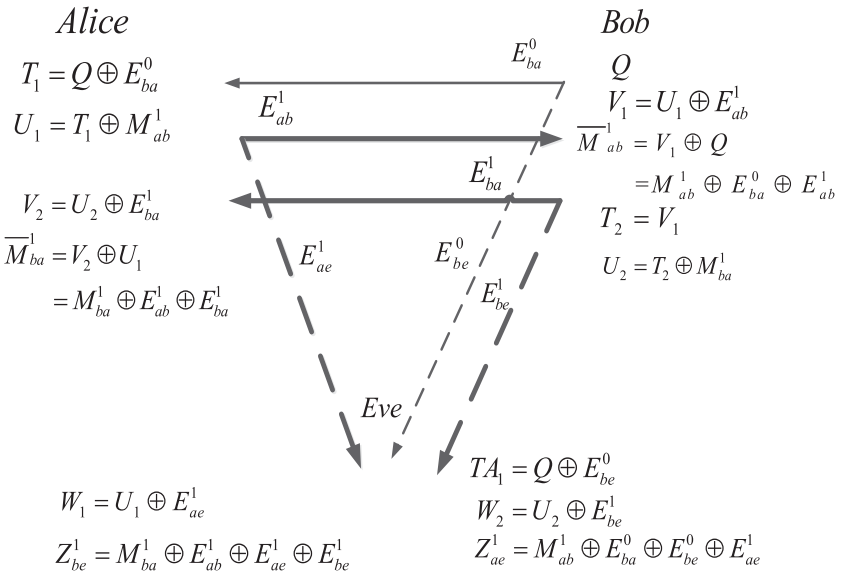

Figure 4. First round of bidirectional secret-key agreement.

Let us define L_M^i as the number of the raw keys, L_Q as the number of the random sequence Q. Then, the transmission rate η_{bi}^{i} of the proposed bidirectional AD over i round is

$$\eta_{bi}^{i} = \frac{L_M^i}{L_M^i + L_Q}. \tag{23}$$

For example, for $i = 1, 2$, η_{bi}^{1} and η_{bi}^{2} equals to $\frac{2}{3}$ and $\frac{4}{5}$, respectively. However, for a large number of rounds, such as $l = 100$, η_{bi}^{100} almost equals to 1. Now, let us analyze the error probability of the main and eavesdropper's channels in the following theorem.

Theorem 1. *Let the error probability of E_{ba}^{i} and E_{ab}^{i} be denoted as $\Pr(e_{ba_k}^{i} = 1) = \Pr(e_{ab_k}^{i} = 1) = \alpha$ and the error probability of E_{be}^{i} and E_{ae}^{i} be denoted as $\Pr(e_{be_k}^{i} = 1) = \Pr(e_{ae_k}^{i} = 1) = \beta$. After a round of the bidirectional TWC, the bit error probability of the main channel is $2\alpha(1-\alpha)$, and the bit error probability of the eavesdropper's channel is $\alpha(1-\beta)^2 + 2(1-\alpha)(1-\beta)\beta + \alpha\beta^2$.*

Proof. Since Bob receives $\bar{M}^1_{ab} = M^1_{ab} \oplus E^0_{ba} \oplus E^1_{ab}$ and the raw key is M^1_{ab}, the bit error probability of raw key M^1_{ab} is

$$\begin{aligned} \Pr(\bar{m}^1_{ab_k} \neq m^1_{ab_k}) &= \Pr(e^0_{ba_k} = 1)\Pr(e^1_{ab_k} = 0) + \Pr(e_{ba_k} = 0)\Pr(e^1_{ab_k} = 1) \\ &= \alpha(1-\alpha) + (1-\alpha)\alpha \\ &= 2\alpha(1-\alpha). \end{aligned} \tag{24}$$

Since Eve only has $Z^1_{ae} = M^1_{ab} \oplus E^0_{ba} \oplus E^0_{be} \oplus E^1_{ae}$, her bit error probability is

$$\begin{aligned} \Pr(z^1_{ae_k} \neq m^1_{ab_k}) &= \Pr(e^0_{ba_k} = 1)\Pr(e^0_{be_k} = 0)\Pr(e^1_{ae_k} = 0) + \Pr(e^0_{ba_k} = 0)\Pr(e^0_{be_k} = 1)\Pr(e^1_{ae_k} = 0) \\ &\quad + \Pr(e^0_{ba_k} = 0)\Pr(e^0_{be_k} = 0)\Pr(e^1_{ae_k} = 1) + \Pr(e^0_{ba_k} = 1)\Pr(e^0_{be_k} = 1)\Pr(e^1_{ae_k} = 1) \\ &= \alpha(1-\beta)(1-\beta) + (1-\alpha)\beta(1-\beta) + (1-\alpha)(1-\beta)\beta + \alpha\beta\beta \\ &= \alpha(1-\beta)^2 + 2(1-\alpha)(1-\beta)\beta + \alpha\beta^2. \end{aligned} \tag{25}$$

□

Let C_m and C_w, $p_m = 2\alpha(1-\alpha)$, and $p_w = \alpha(1-\beta)^2 + 2(1-\alpha)(1-\beta)\beta + \alpha\beta^2$ denote the capacity of the main channel and eavesdropper's channel, bit error probability of main channel and eavesdropper's channel, respectively. Assuming $\alpha = \beta$, the BER of the main channel and the eavesdropper's channel are summarized in Table 2. We can also receive the secret-key capacity C_s,

$$C_s = C_m - C_w = (1 - H_b(p_m)) - (1 - H_b(p_w)), \tag{26}$$

where $H_b(p)$ is the binary entropy function. Assuming $\alpha = \beta$, $p(m^1_{ab_k} = 1) = p(m^1_{ab_k} = 0) = \frac{1}{2}$. Then, we can obtain

$$\begin{aligned} C_s &= (1 - p_m \log_2 \frac{1}{p_m} + (1-p_m)\log_2 \frac{1}{1-p_m}) - (1 - p_w \log_2 \frac{1}{p_w} + (1-p_w)\log_2 \frac{1}{1-p_w}) \\ &= (2\alpha - 2\alpha^2)\log_2(2\alpha - 2\alpha^2) + \frac{1}{2}\log_2(1 - 2\alpha + 2\alpha^2) \\ &\quad - (3\alpha - 6\alpha^2 + 4\alpha^3)\log_2(3\alpha - 6\alpha^2 + 4\alpha^3) - \frac{1}{2}\log_2(1 - 3\alpha + 6\alpha^2 - 4\alpha^3). \end{aligned} \tag{27}$$

Table 2. Bit error rate (BER) of main channel and the eavesdropper's channel.

$\alpha = \beta$	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**
Main channel	0.093	0.165	0.216	0.247	0.258
Eavesdropper's channel	0.244	0.392	0.468	0.496	0.499

For the varying α and β, the corresponding C_m, C_w and C_s are summarized in Table 3.

Table 3. Channel capacity and secret-key capacity.

$\alpha = \beta$	**0.01**	**0.02**	**0.03**	**0.04**	**0.05**
C_m	0.87	0.79	0.72	0.66	0.61
C_w	0.83	0.72	0.63	0.56	0.50
C_s	0.04	0.07	0.09	0.10	0.11

4. Multiple Rounds of Secret-Key Agreement

Assume that there are l rounds of SKA. Then, the ith round of bidirectional AD (shown in Figure 5) is as follows.

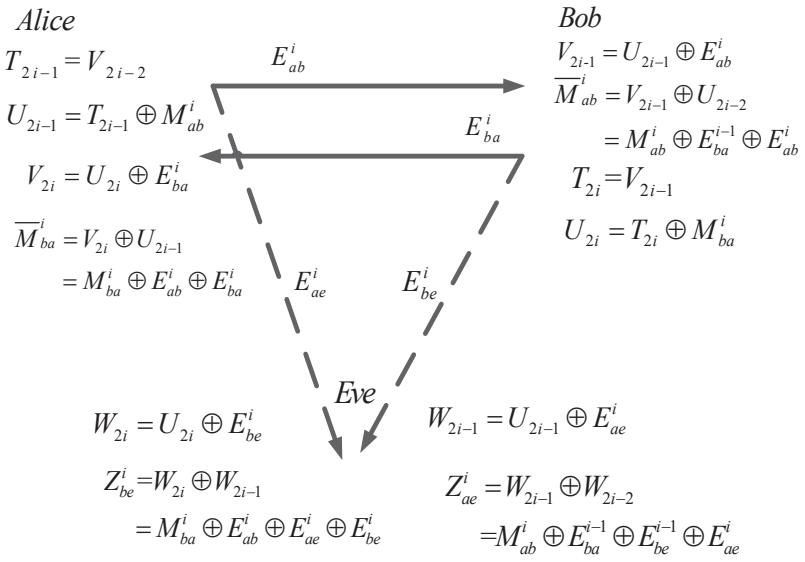

Figure 5. The i-th round of bidirectional secret-key agreement.

4.1. SKA from Alice to Bob

(A2. 1) Let

$$T_{2i-1} = V_{2i-2}. \tag{28}$$

Then, Alice sends the raw key M^i_{ab} to Bob by

$$U_{2i-1} = T_{2i-1} \oplus M^i_{ab}. \tag{29}$$

(A2. 2) Bob and Eve can receive the noisy version of U_{2i-1} as

$$V_{2i-1} = U_{2i-1} \oplus E^i_{ab} = M^i_{ab} \oplus U_{2i-2} \oplus E^{i-1}_{ba} \oplus E^i_{ab}, \tag{30}$$

$$W_{2i-1} = U_{2i-1} \oplus E^i_{ae} = M^i_{ab} \oplus U_{2i-2} \oplus E^{i-1}_{ba} \oplus E^i_{ae}. \tag{31}$$

(A2. 3) Bob and Eve have the knowledge of U_{2i-2} and W_{2i-2}. Therefore, they can obtain the noisy version of M^i_{ab} by XOR U_{2i-2} and W_{2i-2} to V_{2i-1} and W_{2i-1}, respectively. The result is calculated as

$$\bar{M}^i_{ab} = V_{2i-1} \oplus U_{2i-2} = M^i_{ab} \oplus E^{i-1}_{ba} \oplus E^i_{ab} \tag{32}$$

and

$$Z^i_{ae} = W_{2i-1} \oplus W_{2i-2} = M^i_{ab} \oplus E^{i-1}_{ba} \oplus E^{i-1}_{be} \oplus E^i_{ae}. \tag{33}$$

4.2. SKA from Bob to Alice

(B2. 1) In the i-th round, Bob has to make

$$T_{2i} = V_{2i-1}. \tag{34}$$

Then, he sends the raw key M_{ba}^{i} in the noisy form, which is

$$U_{2i} = T_{2i} \oplus M_{ba}^{i}, \tag{35}$$

over the main channel. Meanwhile, Eve may wiretap it by the eavesdropper's channel.

(B2. 2) Alice can receive V_{2i}, consisting of the noisy vector E_{ba}^{i} and U_{2i}, and Eve can receive W_{2i}, which consists of the noisy vector E_{be}^{i} and U_{2i},

$$V_{2i} = U_{2i} \oplus E_{ba}^{i} = M_{ba}^{i} \oplus U_{2i-1} \oplus E_{ab}^{i} \oplus E_{ba}^{i}, \tag{36}$$

$$W_{2i} = U_{2i} \oplus E_{be}^{i} = M_{ba}^{i} \oplus U_{2i-1} \oplus E_{ab}^{i} \oplus E_{be}^{i}. \tag{37}$$

(B2. 3) Alice and Eve have the knowledge of U_{2i-1} and W_{2i-1}, respectively. Therefore, they can obtain the noisy version of M_{ba}^{i} by XOR U_{2i-1} and W_{2i-1} to (36) and (37). The $\bar{M}_{ba}^{i}$ and Z_{be}^{i} can be received by

$$\bar{M}_{ba}^{i} = V_{2i} \oplus U_{2i-1} = M_{ba}^{i} \oplus E_{ab}^{i} \oplus E_{ba}^{i}, \tag{38}$$

and

$$Z_{be}^{i} = W_{2i} \oplus W_{2i-1} = M_{ba}^{i} \oplus E_{ab}^{i} \oplus E_{ae}^{i} \oplus E_{be}^{i}. \tag{39}$$

As shown in Figure 6, the secret sequence M is transmitted bidirectionally between Alice and Bob in our proposed scheme. The BER of the main channel and eavesdropper's channel in the i-th round is the same as that of the first round. Transmission rate after l rounds of the proposed AD is

$$\eta_{bi}^{l} = \frac{2l-1}{2l},$$

which is close to 1 when l is large enough.

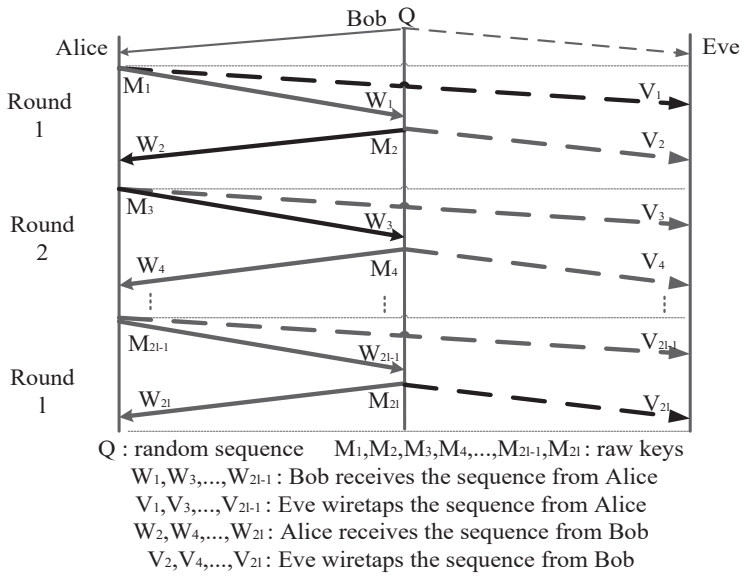

Figure 6. Proposed bidirectional advantage distillation scheme.

5. Bidirectional Secret-Key Agreement over AWGN Channel

Now, let us demonstrate the proposed AD scheme over the AWGN channel. Assume that there are l rounds of SKA over AWGN channel as well. Then, the i-th round shown in Figure 7 is as follows.

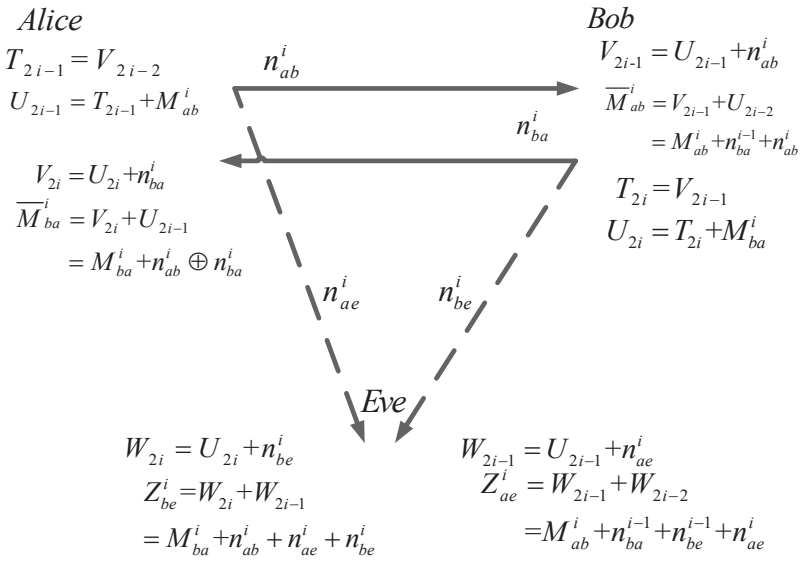

Figure 7. The i-th round of bidirectional secret-key agreement over AWGN channel.

5.1. SKA from Alice to Bob

(A3. 1) Let

$$T_{2i-1} = V_{2i-2}. \tag{40}$$

Then, Alice sends the raw key M^i_{ab} to Bob by

$$U_{2i-1} = T_{2i-1} + M^i_{ab}, \tag{41}$$

where $(U_1, U_2, \cdots, U_{2l}) \in (+1, -1)$

(A3. 2) Bob and Eve can receive the noisy version of U_{2i-1} as

$$V_{2i-1} = U_{2i-1} + n^i_{ab} = M^i_{ab} + U_{2i-2} + n^{i-1}_{ba} + n^i_{ab}, \tag{42}$$

$$W_{2i-1} = U_{2i-1} + n^i_{ae} = M^i_{ab} + U_{2i-2} + n^{i-1}_{ba} + n^i_{ae}, \tag{43}$$

where the variance of AWGN over the main channel and the eavesdropper's channel are σ^2_m and σ^2_w, respectively.

(A3. 3) Bob and Eve can obtain the noisy version of M^i_{ab} by minusing U_{2i-2} and W_{2i-2} to V_{2i-1} and W_{2i-1}, respectively. The result will be

$$\bar{M}^i_{ab} = V_{2i-1} + U_{2i-2} = M^i_{ab} + n^{i-1}_{ba} + n^i_{ab} \tag{44}$$

and

$$Z^i_{ae} = W_{2i-1} + W_{2i-2} = M^i_{ab} + n^{i-1}_{ba} + n^{i-1}_{be} + n^i_{ae}, \tag{45}$$

where the variance of AWGN n_{be} or n_{ae} is σ^2_w.

5.2. SKA from Bob to Alice

(B3. 1) In the ith round, Bob has to make

$$T_{2i} = V_{2i-1}. \tag{46}$$

Then, he sends the raw key M_{ba}^i in the noisy form, which is

$$U_{2i} = T_{2i} + M_{ba}^i \tag{47}$$

over the main channel.

(B3. 2) Alice can receive V_{2i}, consisting of the noisy vector E_{ba}^i and U_{2i}, and Eve can receive W_{2i}, which consists of the noisy vector E_{be}^i and U_{2i},

$$V_{2i} = U_{2i} + n_{ba}^i = M_{ba}^i + U_{2i-1} + n_{ab}^i + n_{ba}^i, \tag{48}$$

$$W_{2i} = U_{2i} + n_{be}^i = M_{ba}^i + U_{2i-1} + n_{ab}^i + n_{be}^i. \tag{49}$$

(B3. 3) Alice and Eve can obtain the noisy version of M_{ba}^i by minusing U_{2i-1} and W_{2i-1} to (48) and (49). $\bar{M}_{ba}^i$ and Z_{be}^i can be received by

$$\bar{M}_{ba}^i = V_{2i} + U_{2i-1} = M_{ba}^i + n_{ab}^i + n_{ba}^i, \tag{50}$$

and

$$Z_{be}^i = W_{2i} + W_{2i-1} = M_{ba}^i + n_{ab}^i + n_{ae}^i + n_{be}^i. \tag{51}$$

Now, let us calculate the capacity of the main channel and the eavesdropper's channel by C_m and C_w. Because the variance of the main channel and the eavesdropper's channel are σ_m and σ_w, we can calculate

$$C_m = \frac{1}{2}\log_2(1 + \frac{P}{\sigma_m^2 + \sigma_m^2}) = \frac{1}{2}\log_2(1 + \frac{P}{2\sigma_m^2}), \tag{52}$$

and

$$C_w = \frac{1}{2}\log_2(1 + \frac{P}{\sigma_m^2 + \sigma_w^2 + \sigma_w^2}) = \frac{1}{2}\log_2(1 + \frac{P}{2\sigma_m^2 + \sigma_w^2}). \tag{53}$$

We can also receive the secret-key capacity C_s over it.

$$C_s = C_m - C_w = \frac{1}{2}[\log_2(1 + \frac{P}{2\sigma_m^2}) - \log_2(1 + \frac{P}{2\sigma_m^2 + \sigma_w^2})]. \tag{54}$$

6. Performance Analysis

In this section, we evaluate performance of the proposed AD scheme over BSC channel in terms of BER and C_s and performance of the proposed AD scheme over AWGN channel C_s. The length n of raw key M^i is 10,000. BER simulation results are shown in Figure 8. With the increasing crossover probability p, the BER increases as well. This indicates that performance of the main channel between Alice and Bob is superior to that of the eavesdropper's channel under the same number l of rounds and length n of the secret sequence.

We also show the capacity of main channel, eavesdropper's channel, and the difference between them that is secret-key capacity over BSC channel in Figure 9 and over AWGN channel in Figure 10. Assuming that $\alpha = \beta \leq 0.09$, the secret-key capacity increases as α and β increase. However, when $\alpha = \beta \geq 0.1$, the secret-key capacity decreases with the increase of α and β. In the AWGN channel, the C_s is close to 0.3 when the signal-to-noise ratio (SNR) is from 0 to 50.

Comparing to the AD schemes using the original two-way wiretap channel, the advantage of our scheme is that we need fewer rounds of communication between Alice and Bob to obtain the same amount of keys. Furthermore, since we need fewer rounds of communication, we also need less XOR operations to obtain the same amount of keys. In each round of the unidirectional AD scheme, using the original two-way wiretap channel, Alice and Bob need 1 XOR operation, respectively, in (3) and (6). In each round of the proposed bidirectional AD scheme, Alice needs 2 operations in (12) and (21), and Bob needs 2 operations in (15) and (18). Therefore, in each round of the proposed bidirectional AD scheme, the number of XOR operations is two times higher than that in the unidirectional AD scheme. However, our bidirectional scheme also has a transmission rate of secret keys which is two times greater than that of the unidirectional AD scheme. Therefore, our scheme needs the same number of XOR operations to obtain the same amount of secret keys as the unidirectional AD scheme. We have listed the transmission rate, XOR operations of the unidirectional AD scheme and the proposed bidirectional AD in Table 4.

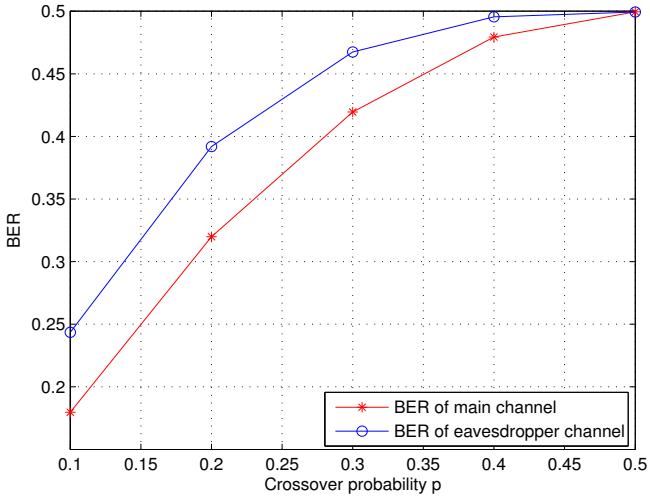

Figure 8. The BER performance of the main channel and eavesdropper's channel over binary symmetric channel (BSC).

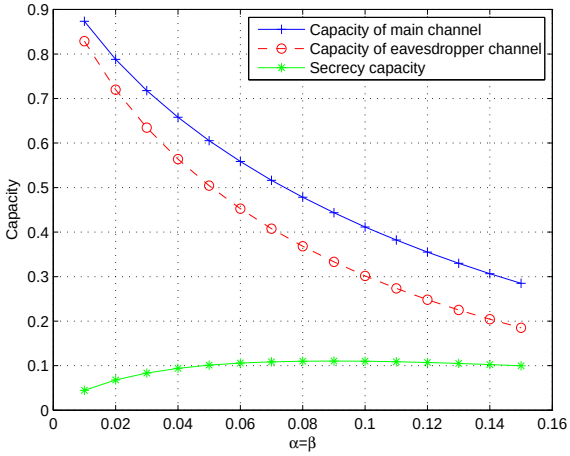

Figure 9. The secret-key capacity and capacities of the main channel and eavesdropper's channel over BSC channel.

Table 4. Transmission rate number of XOR operations of different schemes with l rounds, l is large enough. TWWC: two-way wiretap channel.

Scheme	Transmission Rate	Number of XOR Operations
Unidirectional TWWC scheme	0.5	$2l$
Bidirectional TWWC scheme	1	$4l$

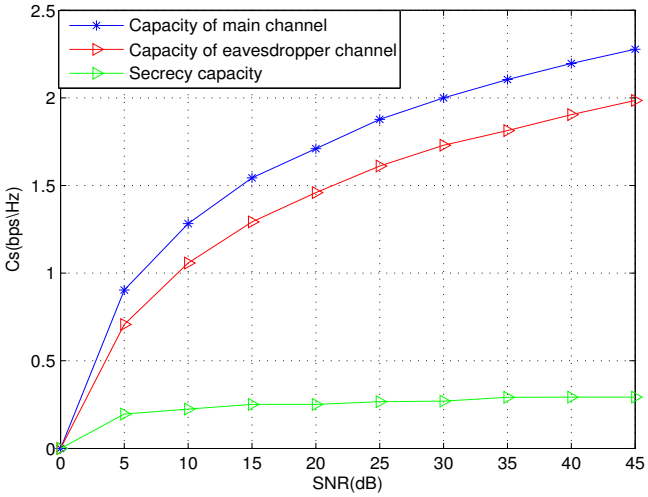

Figure 10. The secret-key capacity and capacities over additive white Gaussian noise (AWGN) channel.

7. Conclusions

In this paper, we modified the original unidirectional TWWC to a bidirectional TWWC for the AD step of the SKA between Alice and Bob over BSC channel and AWGN channel. The proposed bidirectional secret-key agreement can be used to distribute keys between Alice and Bob and its transmission rate is better than the secret-key agreement of unidirectional TWWC. The BER and capacity were calculated first, and then we evaluated the performance of the proposed AD scheme in terms of BER over BSC channel and secret-key capacity over both channels. The BER of the main channel is lower than the eavesdropper's channel, and analysis of the transmission rate is nearly 1 when the number of rounds is large. Moreover, The secret-key capacity C_s is from 0.04 to 0.1 as the error probability of channel is from 0.01 to 0.15 in the BSC channel. In the AWGN channel, the secret-key capacity is close to 0.3 as the SNR increases.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (61671143,61571315,61631004), Shanghai Rising-Star Program (15QA1400100), Key Accident Prevention Technology Project for State Administration of Work Safety (zhishu-0016-2017AQ) and Langfang Research and Development Program about Science & Technology (2016011034).

Author Contributions: Xue-Qin Jiang proposed the new AD scheme; Hui-Ming Wang analyzed the secret-key capacity; Jia hou designed all the simulations; Yi Yang performed the simulations; Yan Feng wrote the paper. All authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Vernam, G.S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Trans. Am. Inst. Electr. Eng.* **1926**, *45*, 295–301.
2. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715.
3. Tomasin, S. Secret key agreement by LLR thresholding and syndrome feedback over awgn channel. *IEEE Commun. Lett.* **2014**, *18*, 26–29.

4. Cao, Y.; Jiang, X.Q.; Wang, H.M.; Bai, E.; Li, J. Advantage distillation over MIMO wiretap channels based on generalized extended orthogonal space-time block codes. In Proceedings of the 2016 International Conference on Computer, Information and Telecommunication Systems (CITS), Kunming, China, 6–8 July 2016; pp. 1–5.
5. Maurer, U. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742.
6. Csiszar, I.; Narayan, P. Common randomness and secret key generation with a helper. *IEEE Trans. Inf. Theory* **2000**, *46*, 344–366.
7. Csiszar, I.; Narayan, P. Secrecy capacities for multiterminal channel Models. *IEEE Trans. Inf. Theory* **2008**, *54*, 2437–2452.
8. Watanabe, S.; Oohama, Y. Secret key agreement from vector Gaussian sources by rate limited public communication. *Proc. IEEE Int. Symp. Inf. Theory* **2010**, 93, 2597–2601.
9. Nitinawarat, S.; Narayan, P. Secret key generation for correlated Gaussian sources. *IEEE Trans. Inf. Theory* **2012**, *58*, 3373–3391.
10. Ahlswede, R.; Csiszar, I. Common randomness in information theory and cryptography-Part I: Secret sharing. *IEEE Trans. Inf. Theory* **1993**, *39*, 1121–1132.
11. Naito, M.; Watanabe, S.; Matsumoto, R.; Uyematsu, T. Secret key agreement by soft-decision of signals in Gaussian Maurer's model. *IEICE Trans. Fundam.* **2009**, *92*, 525–534.
12. Bloch, M.; Barros, J.; Rodriguez, M.R.D.; McLaughlin, S.W. Wireless information-theoretic security. *IEEE Trans. Inf. Theory* **2008**, *54*, 2515–2534.
13. Kobara, K.; Morozov, K.; Imai, H. On the possibility of key agreement using variable directional antenna. In Proceedings of the 1st Joint Workshop on Information Security, Seoul, Korea, 20–21 September 2006; pp. 1432–1436.
14. 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 Propag.* **2005**, *53*, 3776–3784,.
15. Ye, C.; Mathur, S.; Reznik, A.; Shah, Y.; Trappe, W.; Mandayam, N.B. Information-theoretically secret key generation for fading wireless channels. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 240–254.
16. Isaka, M.; Kawata, S. Signal sets for secret key agreement with public discussion based on Gaussian and fading channels. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 523–531.
17. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387.
18. Wen, H.; Gong, G.; Ho, P.H. Build-in wiretap channel I with feedback and LDPC codes. *J. Commun. Netw.* **2009**, *11*, 538–643.
19. Bloch, M.; Barros, J. *Physical-Layer Security: From Information Theory to Security Engineering*; Cambridge University Press: Cambridge, UK, 2011.
20. Pacher, C.; Grabenweger, P.; Martinez-Mateo, J.; Martin, V. An information reconciliation protocol for secret-key agreement with small leakage. In Proceedings of the 2015 IEEE International Symposium on Information Theory (ISIT), Hong Kong, China, 14–19 June 2015; pp. 730–734.