Entropy **2015**, *17*, 4940-4958; doi:10.3390/e17074940

OPEN ACCESS
entropy
ISSN 1099-4300
www.mdpi.com/journal/entropy

Article

Identity Authentication over Noisy Channels

Fanfan Zheng [1], Zhiqing Xiao [2], Shidong Zhou [2,4,5], Jing Wang [3,4,5] and Lianfen Huang [1,*]

[1] Department of Communication Engineering, Xiamen University, Xiamen 361005, China; E-Mail: zhengfanf@foxmail.com

[2] Department of Electronic Engineering, Tsinghua University, Beijing 100084, China; E-Mails: xzq.xiaozhiqing@gmail.com (Z.X.); zhousd@tsinghua.edu.cn (S.Z.)

[3] Research Institute of Information Technology, Tsinghua University, Beijing 100084, China; E-Mail: wangj@tsinghua.edu.cn

[4] State Key Laboratory on Microwave and Digital Communications, Tsinghua University, Beijing 100084, China

[5] Tsinghua National Laboratory for Information Science and Technology, Tsinghua University, Beijing 100084, China

* Author to whom correspondence should be addressed; E-Mail: lfhuang@xmu.edu.cn; Tel.: +86-592-2580142.

Academic Editors: James Park and Wanlei Zhou

Received: 7 April 2015 / Accepted: 9 July 2015 / Published: 14 July 2015

Abstract: Identity authentication is the process of verifying users' validity. Unlike classical key-based authentications, which are built on noiseless channels, this paper introduces a general analysis and design framework for identity authentication over noisy channels. Specifically, the authentication scenarios of single time and multiple times are investigated. For each scenario, the lower bound on the opponent's success probability is derived, and it is smaller than the classical identity authentication's. In addition, it can remain the same, even if the secret key is reused. Remarkably, the Cartesian authentication code proves to be helpful for hiding the secret key to maximize the secrecy performance. Finally, we show a potential application of this authentication technique.

Keywords: identification; authentication; information theoretic security; physical-layer security; wiretap channel

---

1. Introduction

Identity authentication (also known as identification or entity authentication) verifies users' identities to prevent potential losses caused by fraudsters [1,2]. The failure to properly authenticate users will result in serious damage, since the opponent can forge the valid identity to do anything [3].

The most common identity authentication is the challenge-response authentication [1]. As is illustrated in Figure 1, Alice and Bob share a secret key K for identity authentication. In case of potential frauds, Alice initiates a challenge X when an access request is received (even if with the identity declaration). Upon receiving the challenge X, the access requester shall make a response Y. The correctness of Y can be verified by the secret key K. If Y is correct, it demonstrates that the access requester matches the declared identity; otherwise, the access request will be rejected.

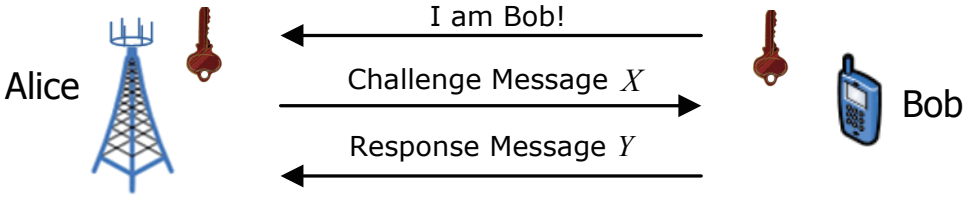

Figure 1. The challenge-response authentication model.

In conventional investigations (e.g., [4–6]), the channels are assumed to be noiseless, because the authentication model is designed on top of the channel coding, which converts the physical noisy channels into noiseless ones. Following this, as is depicted in Figure 2, an attacker, Eve, can completely eavesdrop on the authentication between the legitimate users Alice and Bob and then initiates an impersonation attack by forging a response message Y' before Bob replies. Eve's attack is successful if Alice accepts Y' as a correct response message (*i.e.*, $Y' = Y$). We use P to denote the success probability of this attack; then, we have $P \geq 2^{-I(K;X,Y)}$ (the rigorous proof will be given in Section 3.1). One can easily find out that this lower bound reduces to $P \geq 2^{-H(K)}$ when $H(K|X,Y) = 0$, since $I(K;X,Y) = H(K) - H(K|X,Y)$. In this case, all information of the secret key is used to protect Eve's attack one time. That is, the secret key K needs to be changed in every round of authentication, because Eve is aware of K after eavesdropping on X and Y.

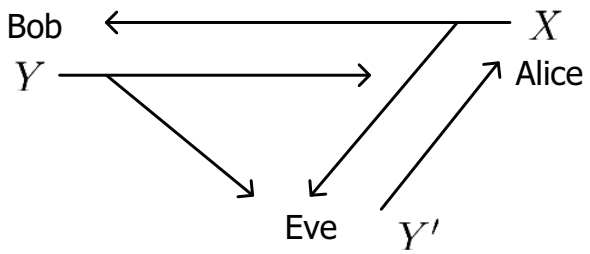

Figure 2. The challenge-response authentication over noiseless channels.

Unfortunately, the open-air nature of wireless communications makes it difficult to distribute, refresh and revoke the secret key K, especially in *ad hoc* networks [7]. Therefore, reusing the same secret key to authenticate several times is considered in practice. In this scenario, the success probability of Eve's attack in the i-th ($1 \leq i \leq n$, where n represents to use the same secret key n-times)

round of authentication is lower bounded by $P \geq 2^{-I(K;X^n,Y^n)/n}$ (the rigorous proof will be given in Section 4.1), where X^n and Y^n respectively denote the n-length sequences of X and Y. This lower bound suggests that after eavesdropping on several rounds of authentication, Eve can be aware of almost all of the information about the secret key K. Then, she can initiate an attack successfully with a high probability. That is, reusing the secret key will cause the secret key's information leakage. However, recent research [8,9] about the message authentication (also known as data-origin authentication, which validates a message's integrity and originator [1,2,10,11]) showed that channel noise can help prevent the secret key's information leakage based on Wyner's wiretap channel.

According to the results of Wyner's wiretap channel [12], perfectly secure transmission of a message is possible by using a codebook whose codeword rate is higher than the channel capacity between the source and the opponent. In this way, [8] introduced noisy channels into the classical Simmons's authentication model. By jointly designing the channel and authentication coding, Eve's success probability can reduce from $P \geq 2^{-H(K)/2}$ to $P = 2^{-H(K)}$, since the secret key can be hidden from her by channel noise. Furthermore, our previous work [9] introduced noisy channels into the systematic authentication code and proved that it is more robust and flexible than Simmons's authentication to protect against Eve's attacks.

There are two primary differences between message authentication and identity authentication [1,2]: (1) message authentication might not happen in real time, but identity authentication does; and (2) message authentication simply authenticates one message, and the process needs to be repeated for each new message. However, identity authentication authenticates the claimant for the entire duration of a session. Unlike the previous works [8,9], which focused on the message authentication over noisy channels, this paper develops the classical identity authentication over noisy channels and makes the following contributions.

(1) We present a general analysis and design framework of the challenge-response authentication, and investigate the authentication scenarios of single time and multiple times. For each scenario, we respectively derive an information-theoretic lower bound on the opponent's success probability in the classical model and our new one. This shows that after introducing channel noise into the classical authentication model, the opponent's success probability is significantly reduced.

(2) We find out that the Cartesian authentication code satisfies the optimal strategy to maximize the security performance. Then, with a slight improvement of the classical authentication, the security performance can be dramatically promoted.

(3) In the multiple-time authentication scenario, with the Cartesian authentication code, we show that the noise spreading over two separate channels can together hide the secret key from the opponent. In this way, the opponent's success probability can be effectively reduced.

(4) We show the potential applications of our work in wireless communications, such as cooperating with the secret key agreement from wireless channels [13,14] to prevent the information leakage of both the original and fresh secret key.

The rest of this paper is organized as follows. Section 2 provides various aspects of our authentication scheme in the given scenarios. Sections 3 and 4 compare the security performance between the classical challenge-response authentication and our proposed authentication in the authentication scenarios of

single time and multiple times, respectively. Section 5 introduces a potential application of our work. Section 6 concludes the paper.

Notation: Throughout this paper, the random variables are denoted by upper case letters (e.g., X), and the corresponding finite alphabets are denoted by calligraphic letters (e.g., $\mathcal{X}$). The n-length sequence of X is denoted by X^n (e.g., $X^n = X_1, X_2, ..., X_n$).

2. Proposed Authentication Scheme

2.1. Scenario

This paper considers the scenario depicted in Figure 3, where Alice, Bob and Eve share a wireless noisy medium. Alice is a critical node that has sensitive information. Suppose that Bob has the legitimate rights to access Alice, while Eve is a malicious attacker who covets Bob's authority. Additionally, Alice and Bob are assumed to be honest with each other. In this context, Bob and Alice agree on the challenge-response authentication scheme that allows Alice to verify whether the access requester is valid or not.

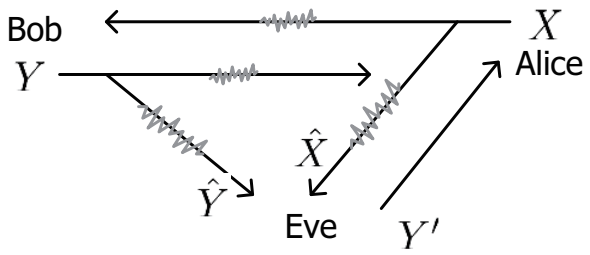

Figure 3. The challenge-response authentication over noisy channels.

2.2. Channel Model

Wyner's wiretap channel [12] is introduced in our scenario. The wiretap channel is defined by two discrete memoryless channels $\mathcal{X} \to (\mathcal{Y}, \mathcal{Z})$, where $\mathcal{X}$ is the input alphabet of the transmitter and $\mathcal{Y}$ and $\mathcal{Z}$ are the output alphabets at the legitimate receiver and the wiretapper, respectively. It is proven in [15] that the secrecy capacity is given by:

$$C_s = \max_{U \to X \to (YZ)} [I(U;Y) - I(U;Z)]^+ \tag{1}$$

where U is an auxiliary random variable [16] satisfying the Markov chain $U \to X \to (YZ)$.

According to the following Definition 1, if a wiretap channel is less noisy, there must exist a U satisfying $I(U;Y) \geq I(U;Z)$, then the secrecy capacity is positive. Actually, the selection $U = X$ is optimal for the entire rate-equivocation region [15,16], which results in:

$$C_s = \max[I(X;Y) - I(X;Z)]. \tag{2}$$

Definition 1 ([15,16]). *A wiretap channel $\mathcal{X} \to (\mathcal{Y}, \mathcal{Z})$ is less noisy if the main channel $\mathcal{X} \to \mathcal{Y}$ is less noisy than the wiretapper's channel $\mathcal{X} \to \mathcal{Z}$, i.e., for all possible $U \to X \to (Y, Z)$, $I(U;Y) \geq I(U;Z)$.*

In Figure 3, we assume that the channels between every two nodes among Alice, Bob and Eve are noisy, except that the one-way channel $Eve \rightarrow Alice$ is noiseless. This Eve's advantage does not incur any loss of generality, since a stronger opponent can lead to more general bounds. Then, it is able to construct two wiretap channels $Alice \rightarrow (Bob, Eve)$ and $Bob \rightarrow (Alice, Eve)$. Moreover, we firstly assume that they are both less noisy (the case that one of them is not less noisy is considered in Section 4.3), so the secrecy capacity of these two wiretap channels is positive. Then, there must exist a codebook (whose codeword rate is higher than the channel capacity between the source and the opponent) satisfying that Alice and Bob can obtain perfect transmitted messages, while Eve only receives completely equivocal observations [8,12,17].

Take the wiretap channel $Alice \rightarrow (Bob, Eve)$ in Figure 3 for example, $I(X;Y)$ and $I(X;\hat{X})$ respectively denote the codeword rate of channels $Alice \rightarrow Bob$ and $Alice \rightarrow Eve$. When this wiretap channel is less noisy, we have $I(X;Y) \geq I(X;\hat{X})$. Then, by a codebook whose codeword rate is $R \leq I(X;Y)$, Bob can perfectly receive Alice's message X, while Eve obtains an observation $\hat{X}$ with the equivocation $R_e = R - I(X;\hat{X})$. According to Equation (2), we have $C_s = \max R_e$. Additionally, there are several technologies (e.g., beamforming and artificial noise [18–20]) to ensure that a wiretap channel is less noisy (*i.e.*, $C_s > 0$). Thus, we can make the above assumption.

2.3. Authentication Model

Alice and Bob share a secret key K for authentication. The secret key K is only known to Alice and Bob, and it has been allocated beforehand. Let $\mathcal{X}$, $\mathcal{K}$ and $\mathcal{Y}$ respectively denote the finite alphabets of the challenge message, the secret key and the response message. The challenge message X and the secret key K are statistically independent, and they are uniformly distributed on $\mathcal{X}$ and $\mathcal{K}$, respectively.

Similar to the classical model (as is illustrated in Figure 1), in case of Eve's attack, when Alice receives an access request with an identity declaration (maybe true or false), she sends a challenge message X to the access requester. In this way, the access requester shall correctly make a response:

$$Y = f(X, K) \tag{3}$$

where $f(\cdot)$ encapsulates any prospective coding or modulation. Additionally, splitting code is not considered in this paper, *i.e.*, $H(Y|X,K) = 0$.

Upon receiving a response message $\tilde{Y}$, which may come from either Bob or Eve, Alice firstly generates the correct response message Y by the secret key K she owns, then compares it with $\tilde{Y}$. If $\tilde{Y} = Y$, this demonstrates that the access requester matches the declared identity; otherwise, the access request will be rejected.

Eve listens to the authentication between Alice and Bob. Since the wiretap channels are less noisy, by an appropriate codebook [21–24], Bob and Alice perfectly receive X and Y respectively, while Eve only obtains equivocal observations of X and Y, which are denoted by $\hat{X}$ and $\hat{Y}$.

Since Bob owns the secret key K, he is able to give response Y correctly whenever he wants to access Alice. That is, the authentication model can ensure the accessibility of a legitimate user. Eve, a potential attacker, also wants to access Alice. However, she is not aware of the secret key K *a priori*. Therefore, she listens to the authentications between Alice and Bob, observes $\hat{X}$ and $\hat{Y}$ and tries to

extract the information about the secret key K from the observations. Then, she requires access to Alice by disguising herself as Bob, which is known as the impersonation attack. Without loss of generality, we assume that Eve has infinite computation power and knows the authentication scheme.

This paper focuses on the success probability of the impersonation attack. Specifically, we hope to minimize Eve's success probability.

3. Single-Time Authentication

3.1. Noiseless Channels Model

The classical challenge-response authentication model assumes that channels are noiseless, because the authentication model is designed after the channel coding converts the noisy channels into noiseless ones. In this way, Eve can eavesdrop on the complete challenge message X to impersonate Bob's response. We denote the success probability of Eve's impersonation attack as P. In the single-time authentication (e.g., the initial authentication), it has been shown that:

$$P = \sum_{x \in \mathcal{X}} p(x) \max_{y \in \mathcal{Y}} p(y|x). \tag{4}$$

To simplify the analysis, we have the following lemma.

Lemma 1. *In the classical authentication model, Eve's success probability is lower bounded by:*

$$P \geq 2^{-I(K;X,Y)}, \tag{5}$$

with equality iff $p(y|x) \in \{c_+^1, 0\}$. *Note that* c_+^1 *means a constant* δ *that satisfies* $0 < \delta \leq 1$ *and the same hereinafter.*

Proof. This result is derived because:

$$\begin{aligned} -\log P =& -\log \sum_{x \in \mathcal{X}} p(x) \max_{y \in \mathcal{Y}} p(y|x) \\ \overset{(a)}{\leq}& -\sum_{x \in \mathcal{X}} p(x) \log \max_{y \in \mathcal{Y}} p(y|x) \\ =& -\sum_{x \in \mathcal{X}} p(x) \sum_{y \in \mathcal{Y}} p(y|x) \log \max_{y' \in \mathcal{Y}} p(y'|x) \\ \overset{(b)}{\leq}& -\sum_{x \in \mathcal{X}} p(x) \sum_{y \in \mathcal{Y}} p(y|x) \log p(y|x) \\ =& H(Y|X) \end{aligned} \tag{6}$$

and:

$$\begin{aligned} I(K;X,Y) =& H(X,Y) - H(X,Y|K) \\ =& H(X) + H(Y|X) - H(X|K) - H(Y|K,X) \\ \overset{(c)}{=}& H(Y|X). \end{aligned} \tag{7}$$

In Equation (6), inequality (a) comes from Jensen's inequality, and (a) with equality iff $\max_{y\in\mathcal{Y}} p(y|x)$ are equal for all $x \in \mathcal{X}$; (b) with equality iff there exists a subset of $\mathcal{Y}$ to satisfy $p(y|x) = \delta(x)$ $(0 < \delta(\cdot) \leq 1)$. Thus, Equation (5) with equality iff $p(y|x) \in \{\delta, 0\}$ $(0 < \delta \leq 1)$.

In Equation (7), equality (c) holds because the secret key K and the challenge message X are statistically independent (*i.e.*, $H(X) = H(X|K)$), and the splitting code is not considered (*i.e.*, $H(Y|K, X) = 0$). □

3.2. Noisy Channels Model

Consider the noisy channels. Since the wiretap channels are less noisy, Eve only obtains an equivocal observation of the challenge message, which is denoted by $\hat{X}$. We denote the success probability of Eve's impersonation attack as $\bar{P}$. Following the same steps as those used in Equation (6), $\bar{P}$ is lower bounded by:

$$\bar{P} \geq 2^{-H(Y|\hat{X})} \tag{8}$$

and $\bar{P}$ achieves its lower bound iff $p(y|\hat{x}) \in \{c_+^1, 0\}$.

To simplify the analysis, we draw the following lemma to show our scheme's advantage to protect against Eve's attack.

Lemma 2. *In our new authentication model, Eve's success probability is lower bounded by:*

$$\bar{P} \geq 2^{-I(K;X,Y)-H(X|\hat{X})+H(X|\hat{X},Y)}. \tag{9}$$

Proof. Please refer to Appendix A for technical details. □

According to Lemma 1 and Lemma 2, we have the following Theorem 1 and Example 1 to show the optimal strategy of our new scheme to protect against Eve's attack. We firstly declare the concepts of the Cartesian authentication code and the systematic Cartesian authentication code (the simplest Cartesian authentication code) and then present the theorem and the example.

Definition 2 ([25,26]). *If the authentication code satisfies that given any message y, there exists a unique source state x, such that $y = f(x, e)$ for every encoding rules e contained in y, i.e., the authentication code satisfies $H(X|Y) = 0$, then the code is called a Cartesian authentication code.*

Definition 3 ([27,28]). *If the Cartesian authentication code satisfies that the message y is formed by its source state x and an authenticator t (e.g., $y = (x, t) = (x, g(x, e))$ where e represents the encoding rule), then the code is called a systematic Cartesian authentication code.*

Theorem 1. *In our new authentication model, to promote the security performance maximally, the optimal strategy for $f(\cdot)$ is the Cartesian authentication code.*

Proof. The authentication's security performance is indicated by the achievable lower bound on Eve's success probability [4,5,8]. The lower the achievable bound is, the more secure the authentication is.

Thus, according to Equation (5) and Equation (9), we use $\underline{P}$ to represent the achievable lower bound of P (in Equation (5)) and denote the promoted performance as:

$$\begin{aligned}\Delta P &= (-\log \bar{P}) - (-\log \underline{P}) \\ &\overset{(d)}{\leq} H(X|\hat{X}) - H(X|\hat{X}, Y) \\ &\overset{(e)}{\leq} H(X) - H(X|Y) \\ &\overset{(f)}{\leq} H(X)\end{aligned} \tag{10}$$

where inequality (d) comes from Equation (9); inequality (e) holds since:

$$\begin{aligned}H(X|\hat{X}) - H(X|\hat{X}, Y) &= H(X|\hat{X}) - \Big(H(X, \hat{X}|Y) - H(\hat{X}|Y)\Big) \\ &= H(X|\hat{X}) - \Big(H(X|Y) + H(\hat{X}|X, Y) - H(\hat{X}|Y)\Big) \\ &= H(\hat{X}|Y) - H(X|Y)\end{aligned} \tag{11}$$

and $H(\hat{X}|Y)$ increases with the increase of $\hat{X}$'s equivocation; and inequality (f) follows from $H(X|Y) \geq 0$.

Obviously, in Equation (10), (f) with equality iff the Cartesian authentication code is used (*i.e.*, $H(X|Y) = 0$). Moreover, since $\hat{X}$'s maximum equivocation is $H(X)$, (e) with equality iff $H(X|\hat{X}) = H(X)$, *i.e.*, $p(x|\hat{x}) = 1/|\mathcal{X}|$ because x is uniformly chosen from $\mathcal{X}$. In addition, with the Cartesian authentication code, we have $p(y|x) \in \{1/|\mathcal{K}|, 0\}$ because k is uniformly chosen from $\mathcal{K}$. Thus, we have:

$$\begin{aligned}p(y|\hat{x}) &= \sum_{x \in \mathcal{X}} p(y|x)p(x|\hat{x}) \\ &\in \left\{\frac{1}{|\mathcal{K}|}\sum_{x \in \mathcal{X}} p(x|\hat{x}), 0\right\} \\ &= \left\{\frac{1}{|\mathcal{X}|}, 0\right\}.\end{aligned} \tag{12}$$

Then, according to the conditions for quality of Equation (5) (in Lemma 1) and Equation (9) (the same with Equation (8)'s), P and $\bar{P}$ can simultaneously achieve their lower bounds. Therefore, we have equality in (d).

Then, we can draw Theorem 1 because $H(X|Y) = 0$ is a sufficient and necessary condition to achieve $\Delta P = H(K)$. □

Remark 1. *Theorem 1 demonstrates that a slight improvement (e.g., Example 1) can significantly promote the security performance. Specifically, since the wiretap channel $Alice \to (Bob, Eve)$ is less noisy (i.e., the secrecy capacity is positive), Eve only obtains an equivocal challenge message $\hat{X}$. When using the Cartesian authentication code, the response message Y contains all of the information of the challenge message X. Then, the transmitting process of the challenge message X is equal to a secret key agreement, which generates $H(X|\hat{X})$ new secret key information.*

Example 1. *In practical classical authentication, the response message Y is a short data block, which comes from the challenge message X and the secret key K, i.e., $Y = f(X, K)$ where $f(\cdot)$ encapsulates*

a compressive function. However, in our new authentication model, if we improve the response message to $Y = (X, g(X, K))$ *(i.e., the systematic Cartesian authentication code, where* $g(\cdot)$ *is the compressive function in* $f(\cdot)$*), Eve's success probability will reduce to:*

$$\bar{P} \geq 2^{-I(K;X,Y)-H(X|\hat{X})} \tag{13}$$

according to Equation (9).

4. Multiple-Time Authentication

In practical networks, the secret key K is reused to authenticate Bob's identity for several rounds. In each round, Eve can choose to initiate an attack. She attacks in the i-th round authentication based on the information of the previous $i-1$ rounds of authentication. The attack is successful if her fake response message passes Alice's authentication.

4.1. Noiseless Channels Model

Compared with the single-time authentication, Eve obtains additional $i-1$ challenge messages and response messages. We use P_i to denote the success probability of Eve's attack in the i-th round of authentication. Following from the same steps as those used in the proof of Lemma 1, the lower bound on P_i is derived as:

$$P_i \geq 2^{-I(K;X_i,Y_i|X^{i-1},Y^{i-1})}, \tag{14}$$

with equality iff $p(y_i|x^i, y^{i-1}) \in \{c_+^1, 0\}$.

Since $(X^{i-1}, Y^{i-1}) \rightarrow K \rightarrow (X_i, Y_i)$ forms a Markov chain, we have $I(K; X_i, Y_i|X^{i-1}, Y^{i-1}) \leq I(K; X_i, Y_i)$. Obviously, reusing the secret key K results in the increase of Eve's success probability.

Moreover, Eve will choose the attack that maximizes her success probability, *i.e.*,

$$P = \max\{P_1, P_2, ..., P_n\}. \tag{15}$$

Consequently, we have the following lemma.

Lemma 3. *In the classical authentication model, Eve's success probability is lower bounded by:*

$$P \geq 2^{-I(K;X^n,Y^n)/n} \tag{16}$$

where n *represents that the secret key is used* n *times.*

Proof. This result is derived due to:

$$\begin{aligned} -\sum_{i=1}^{n} \log P_i &\leq \sum_{i=1}^{n} I(K; X_i, Y_i|X^{i-1}, Y^{i-1}) \\ &= I(K; X^n, Y^n), \end{aligned} \tag{17}$$

and the maximum must be greater than or equal to the average, *i.e.*,

$$\begin{aligned}\max\{\log P_1, \log P_2, ..., \log P_n\} \geq & \frac{1}{n}\sum_{i=1}^{n}\log P_i \\ \geq & -\frac{1}{n}I(K; X^n, Y^n).\end{aligned} \tag{18}$$

□

Remark 2. *This lower bound demonstrates that if Eve initiates an attack at any round i ($1 \leq i \leq n$), no authentication strategy can prevent her from being successful with probability at least $2^{-I(K;X^n,Y^n)/n}$. A secret key K is used optimally when all of these success probabilities are (roughly) equal* [5,6]. *Thus, in an optimal scheme, the secret key is split into n nearly equal parts, each of which is allocated to protect against an attack at the i-th round of authentication. Then, after eavesdropping on n rounds of authentication, Eve may be aware of almost all of the information about the secret key and able to attack successfully with a high probability.*

4.2. Noisy Channels Model

Consider the noisy channels. Since the wiretap channels are less noisy, Eve obtains $i-1$ rounds of equivocal challenge messages $\hat{X}^{i-1}$ and response messages $\hat{Y}^{i-1}$ and an equivocal challenge message $\hat{X}_i$ in the i-th round. We use $\bar{P}_i$ to denote the success probability of Eve's attack in the i-th round of authentication. Following the same steps as those used in Equation (6), the lower bounded on $\bar{P}_i$ is derived as:

$$\bar{P}_i \geq 2^{-H(Y_i|\hat{X}_i,\hat{X}^{i-1},\hat{Y}^{i-1})}, \tag{19}$$

with equality iff $p(y_i|\hat{x}^{i-1}, \hat{y}^{i-1}, x^i) \in \{c_+^1, 0\}$. Further, we have the following lemma.

Lemma 4. *In our new authentication model, Eve's success probability at the i-th round of authentication is lower bounded by:*

$$\begin{aligned}-\log \bar{P}_i \leq & I(K; X_i, Y_i|X^{i-1}, Y^{i-1}) - H(X_i|\hat{X}_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1}) \\ & + H(X_i|\hat{X}_i) + I(X^{i-1}, Y^{i-1}; X_i, Y_i|\hat{X}^{i-1}, \hat{Y}^{i-1}).\end{aligned} \tag{20}$$

Proof. Please refer to Appendix B for technical details. □

According to Equation (14) and Equation (20), in multiple-time authentication, we still can deduce that the Cartesian authentication code is optimal to promote the security performance (*i.e.*, Theorem 1). By the following Theorem 2, we demonstrate this inference in Remark 4.

Theorem 2. *If there are no information leaks to Eve in the wiretap channels (i.e., $I(X_i; \hat{X}_i) = 0$ and $I(Y_i; \hat{Y}_i) = 0$), Eve's success probability is lower bounded by:*

$$\bar{P} \geq 2^{-H(Y)}. \tag{21}$$

Proof. As is explained in Section 2.2, since the wiretap channels $Alice \rightarrow (Bob, Eve)$ and $Bob \rightarrow (Alice, Eve)$ are less noisy, there must exist a codebook, such that the transmitted messages can be

perfectly obtained by Alice and Bob, but completely hidden from Eve [8,12,17], *i.e.*, $I(X_i;\hat{X}_i)=0$ and $I(Y_i;\hat{Y}_i)=0$. Then, Equation (20) becomes:

$$\begin{aligned}-\log \bar{P}_i \leq & I(K;X_i,Y_i|X^{i-1},Y^{i-1})+H(X_i)+I(Y^{i-1};X_i,Y_i|X^{i-1})-H(X_i|Y_i)\\ =& I(K;X_i,Y_i|X^{i-1},Y^{i-1})+H(X_i)+H(X_i,Y_i)-H(X_i,Y_i|X^{i-1},Y^{i-1})\\ & -H(X_i|Y_i)\\ =& -H(X_i,Y_i|K,X^{i-1},Y^{i-1})+H(X_i)+H(X_i,Y_i)-H(X_i|Y_i)\\ =& -H(X_i,Y_i|K)+H(X_i)+H(X_i,Y_i)-H(X_i|Y_i)\\ =& H(X_i,Y_i)-H(X_i|Y_i)\\ =& H(Y_i).\end{aligned} \tag{22}$$

Since X and K are respectively uniformly distributed on $\mathcal{X}$ and $\mathcal{K}$, we have $H(Y_i)=H(Y)$. Then, similar to the proof of Lemma 3, we have:

$$-\log \bar{P} \leq -\frac{1}{i}\sum_{n=1}^{i}\log \bar{P}_i \leq H(Y). \tag{23}$$

□

Remark 3. *In the classical authentication model, after Eve eavesdrops on several rounds of authentication, the knowledge of the challenge messages and response messages enable the information of the secret key to be determined (i.e., Lemma 3). In contrast, in our new authentication model, Eve's success probability can remain the same even if she continues eavesdropping (i.e., Theorem 2).*

Remark 4. *$H(X,Y)$ is constant, since X and K are uniformly distributed, and:*

$$\begin{aligned}H(X,Y) &= H(Y)+H(X|Y)\\ &\geq H(Y).\end{aligned} \tag{24}$$

Then, with the Cartesian authentication code, $\bar{P}$'s lower bound reduces to:

$$\bar{P} \geq 2^{-H(X,Y)}. \tag{25}$$

4.3. Single-Wiretap Channel and Double-Wiretap Channels

As is depicted in Figure 3, the channels $Bob \rightarrow Alice$ and $Alice \rightarrow Bob$ are approximately the same if the response message is replied to in the coherence time, but the channels $Bob \rightarrow Eve$ and $Alice \rightarrow Eve$ are not equivalent. Therefore, it is possible that only one wiretap channel in Figure 3 satisfies the less noisy wiretap channel (*i.e.*, $C_s > 0$). If a wiretap channel is not less noisy, it cannot ensure that Equation (1) remains positive under the optimal selection $U = X$ for less noisy wiretap channels [16]. Without loss of generality, if a wiretap channel in Figure 3 is not less noisy, we assume that Eve can obtain what legitimate users receive.

As is shown in Table 1, to show the distinctions, we use $\bar{P}_i(\hat{X}^i,\hat{Y}^{i-1})$ instead of $\bar{P}_i$ to denote the success probability of Eve's attack when the wiretap channels $Bob \rightarrow (Alice, Eve)$ and $Alice \rightarrow$

(Bob, Eve) are both less noisy. Furthermore, similar to the analysis in the proof of Theorem 1, we introduce $\Delta\bar{P}_i(\hat{X}^i, \hat{Y}^{i-1})$ to denote the promoted performance in the corresponding wiretap channels, *i.e.*,

$$\Delta\bar{P}_i(\hat{X}^i, \hat{Y}^{i-1}) = \left(-\log \underline{\bar{P}_i}(\hat{X}^i, \hat{Y}^{i-1})\right) - \left(-\log \underline{P_i}(X^i, Y^{i-1})\right) \tag{26}$$

where $\underline{\bar{P}_i}(\hat{X}^i, \hat{Y}^{i-1})$ and $\underline{P_i}(X^i, Y^{i-1})$ respectively represent the achievable lower bounds on $\bar{P}_i(\hat{X}^i, \hat{Y}^{i-1})$ and $P_i(X^i, Y^{i-1})$.

Table 1. Terminologies of Eve's success probability and the promoted performance.

$Alice \to (Bob, Eve)$	$Bob \to (Alice, Eve)$	Eve's success probability	The promoted performance
$C_s > 0$	$C_s > 0$	$\bar{P}_i(\hat{X}^i, \hat{Y}^{i-1})$	$\Delta\bar{P}_i(\hat{X}^i, \hat{Y}^{i-1})$
$C_s > 0$	$C_s = 0$	$\bar{P}_i(\hat{X}^i, Y^{i-1})$	$\Delta\bar{P}_i(\hat{X}^i, Y^{i-1})$
$C_s = 0$	$C_s > 0$	$\bar{P}_i(X^i, \hat{Y}^{i-1})$	$\Delta\bar{P}_i(X^i, \hat{Y}^{i-1})$

In the same way, we respectively use $\bar{P}_i(\hat{X}^i, Y^{i-1})$ and $\bar{P}_i(X^i, \hat{Y}^{i-1})$ to represent Eve's success probability when only the $Alice \to (Bob, Eve)$ channel is less noisy and only the $Bob \to (Alice, Eve)$ channel is less noisy. In addition, we introduce $\Delta\bar{P}_i(\hat{X}^i, Y^{i-1})$ and $\Delta\bar{P}_i(X^i, \hat{Y}^{i-1})$ to respectively denote the promoted performance in the corresponding wiretap channels (note that $\Delta\bar{P}_i(\hat{X}^i, Y^{i-1})$ and $\Delta\bar{P}_i(X^i, \hat{Y}^{i-1})$ are two special cases of $\Delta\bar{P}_i(\hat{X}^i, \hat{Y}^{i-1})$), *i.e.*,

$$\begin{aligned}
\Delta\bar{P}_i(\hat{X}^i, Y^{i-1}) &= \left(-\log \underline{\bar{P}_i}(\hat{X}^i, Y^{i-1})\right) - \left(-\log \underline{P_i}(X^i, Y^{i-1})\right), \\
\Delta\bar{P}_i(X^i, \hat{Y}^{i-1}) &= \left(-\log \underline{\bar{P}_i}(X^i, \hat{Y}^{i-1})\right) - \left(-\log \underline{P_i}(X^i, Y^{i-1})\right)
\end{aligned} \tag{27}$$

where $\underline{\bar{P}_i}(\hat{X}^i, Y^{i-1})$ and $\underline{\bar{P}_i}(X^i, \hat{Y}^{i-1})$ respectively represent the achievable lower bounds on $\bar{P}_i(\hat{X}^i, Y^{i-1})$ and $\bar{P}_i(X^i, \hat{Y}^{i-1})$.

Then, according to Equation (20), we respectively have:

$$\Delta\bar{P}_i(\hat{X}^i, \hat{Y}^{i-1}) = H(X_i|\hat{X}_i) + I(X^{i-1}, Y^{i-1}; X_i, Y_i|\hat{X}^{i-1}, \hat{Y}^{i-1}) - H(X_i|\hat{X}^i, Y_i, \hat{Y}^{i-1}), \tag{28a}$$

$$\Delta\bar{P}_i(\hat{X}^i, Y^{i-1}) = H(X_i|\hat{X}_i) - H(X_i|\hat{X}^i, Y^{i-1}), \tag{28b}$$

$$\Delta\bar{P}_i(X^i, \hat{Y}^{i-1}) = I(Y^{i-1}; X_i, Y_i|X^{i-1}, \hat{Y}^{i-1}). \tag{28c}$$

Furthermore, with the Cartesian authentication code, we respectively have:

$$\Delta\bar{P}_i(\hat{X}^i, \hat{Y}^{i-1}) = H(X_i|\hat{X}_i) + I(X^{i-1}, Y^{i-1}; X_i, Y_i|\hat{X}^{i-1}, \hat{Y}^{i-1}), \tag{29a}$$

$$\Delta\bar{P}_i(\hat{X}^i, Y^{i-1}) = H(X_i|\hat{X}_i), \tag{29b}$$

$$\Delta\bar{P}_i(X^i, \hat{Y}^{i-1}) = I(Y^{i-1}; X_i, Y_i|X^{i-1}, \hat{Y}^{i-1}). \tag{29c}$$

To simplify the analysis, we draw the following Theorem 3 to show our scheme's advantage to protect against Eve's attack.

Theorem 3. *With the Cartesian authentication code, we have:*

$$\Delta\bar{P}_i(\hat{X}^i, \hat{Y}^{i-1}) \geq \Delta\bar{P}_i(\hat{X}^i, Y^{i-1}) + \Delta\bar{P}_i(X^i, \hat{Y}^{i-1}). \tag{30}$$

Proof. Specifically, when $i = 1$, X^{i-1}, $\hat{X}^{i-1}$, Y^{i-1} and $\hat{Y}^{i-1}$ do not exist. At this time, Equation (29a) is same with Equation (29b), and Equation (29c) is equal to zero. Hence, Equation (30) is satisfied.

When $i \geq 2$, we have:

$$\begin{aligned}
&\Delta\bar{P}_i(\hat{X}^i, \hat{Y}^{i-1}) - \Delta\bar{P}_i(\hat{X}^i, Y^{i-1}) - \Delta\bar{P}_i(X^i, \hat{Y}^{i-1}) \\
=&H(X_i|\hat{X}_i) + I(X^{i-1}, Y^{i-1}; X_i, Y_i|\hat{X}^{i-1}, \hat{Y}^{i-1}) \\
&- H(X_i|\hat{X}_i) - I(Y^{i-1}; X_i, Y_i|X^{i-1}, \hat{Y}^{i-1}) \\
=&H(X^{i-1}, Y^{i-1}|\hat{X}^{i-1}, \hat{Y}^{i-1}) - H(X^{i-1}, Y^{i-1}|X_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1}) \\
&- I(Y^{i-1}; X_i, Y_i|X^{i-1}, \hat{Y}^{i-1}) \\
=&H(X^{i-1}|\hat{X}^{i-1}, \hat{Y}^{i-1}) + H(Y^{i-1}|X^{i-1}, \hat{X}^{i-1}, \hat{Y}^{i-1}) \\
&- H(X^{i-1}|X_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1}) - H(Y^{i-1}|X_i, Y_i, X^{i-1}, \hat{X}^{i-1}, \hat{Y}^{i-1}) \\
&- I(Y^{i-1}; X_i, Y_i|X^{i-1}, \hat{Y}^{i-1}) \\
=&H(X^{i-1}|\hat{X}^{i-1}, \hat{Y}^{i-1}) + H(Y^{i-1}|X^{i-1}, \hat{Y}^{i-1}) - H(X^{i-1}|X_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1}) \\
&- H(Y^{i-1}|X_i, Y_i, X^{i-1}, \hat{Y}^{i-1}) - I(Y^{i-1}; X_i, Y_i|X^{i-1}, \hat{Y}^{i-1}) \\
=&H(X^{i-1}|\hat{X}^{i-1}, \hat{Y}^{i-1}) - H(X^{i-1}|X_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1}) \\
\geq&0.
\end{aligned} \tag{31}$$

Then, Equation (30) is proven. □

Additionally, without the Cartesian authentication code, Equation (30) does not certainly hold. Because according to Equation (28) and Equation (31), we have:

$$\begin{aligned}
&\Delta\bar{P}_i(\hat{X}^i, \hat{Y}^{i-1}) - \Delta\bar{P}_i(\hat{X}^i, Y^{i-1}) - \Delta\bar{P}_i(X^i, \hat{Y}^{i-1}) \\
=&\Big(H(X^{i-1}|\hat{X}^{i-1}, \hat{Y}^{i-1}) - H(X^{i-1}|X_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1})\Big) \\
&- \Big(H(X_i|\hat{X}^i, Y_i, \hat{Y}^{i-1}) - H(X_i|\hat{X}^i, Y^{i-1})\Big)
\end{aligned} \tag{32}$$

where $H(X^{i-1}|\hat{X}^{i-1}, \hat{Y}^{i-1}) - H(X^{i-1}|X_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1}) \geq 0$ and $H(X_i|\hat{X}^i, Y_i, \hat{Y}^{i-1}) - H(X_i|\hat{X}^i, Y^{i-1}) \geq 0$.

Remark 5. *Theorem 3 demonstrates that with the Cartesian authentication code, the noise of two separate wiretap channels can together hide the secret key information from Eve. Therefore, though the secret key information is all contained in the response message Y, by securely transmitting the challenge message X, we can further reduce Eve's success probability from $P \geq 2^{-H(Y)}$ to $P \geq 2^{-H(X,Y)}$ (i.e., Remark 4).*

5. Application

Since the physical channels are noisy and the challenge-response authentication is widely applied in existing communication systems, our authentication scheme has significant potential foreground. By our work, the existing systems can be smoothly upgraded with great promotion of the security performance. In the sequel, we present an application of protecting the secret key agreement in wireless communications by an improved authentication scheme (*i.e.*, Example 1).

Since wireless channels are reciprocal in space and varied in time [7], extracting secret keys through channel characteristics is considered as one of the most developed solutions for the secret key renewal [13,14]. As is depicted in Figure 4a, Alice wants to negotiate secret keys with her legitimate user Bob. If Alice and Bob exchange a sequence of known pilots in the coherence time Δt, they can have almost the same channel characteristic to generate the same secret key [13,14]. Unfortunately, this secret key agreement may incur the following risks, which can be prevented by our new authentication model.

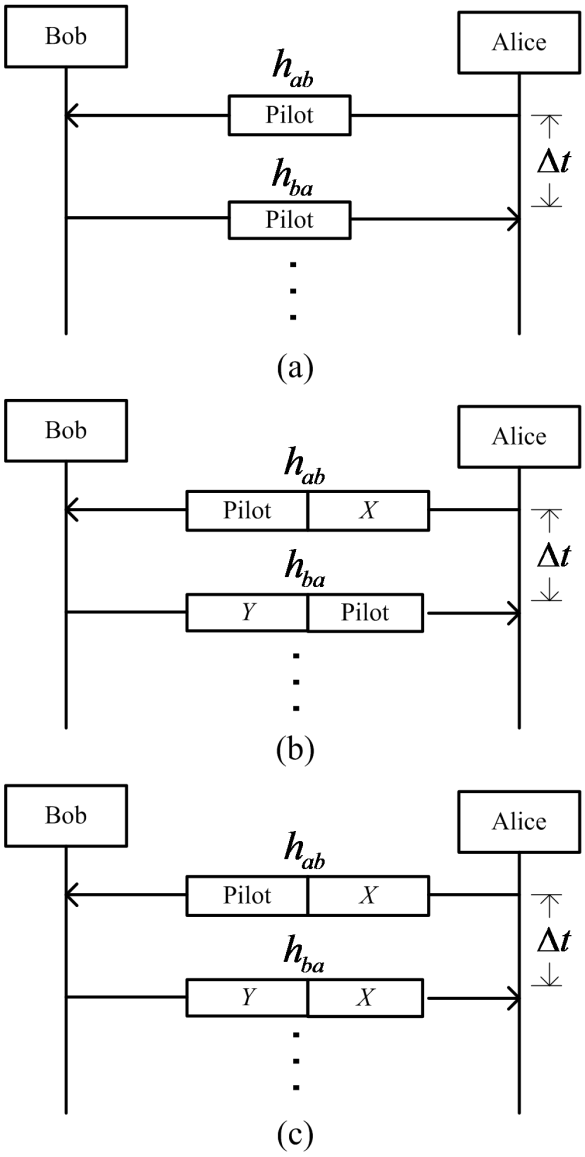

Figure 4. (**a**) Example of the secret key agreement from wireless channels. (**b**) The secret key agreement is protected by the challenge-response authentication. (**c**) The secret key agreement is improved by our proposed authentication model.

Firstly, when there exists potential opponents (e.g., Eve proactively responds to the pilot sequence before Bob sends anything), the secret key agreement should be protected by the identity authentication (e.g., as is depicted in Figure 4b, the secret key agreement is protected by the challenge-response authentication).

Secondly, the amount of new secret key information generated once is too little to replace the original one. Thus, by the classical challenge-response authentication, several times of secret key agreement will cause the information leakage of the original secret key. Under this circumstance, Eve's success probability will increase before the renewal of the original secret key. However, in our new authentication model, Eve's success probability is significantly reduced and can remain the same even if the secret key is reused (*i.e.*, Equation (21)). Then, the original secret key's renewal can be ensured to be completed with high security performance.

Thirdly, without loss of generality, the pilot sequence is public. Then, Eve can respectively have the channel characteristics of $Alice \to Eve$ and $Bob \to Eve$. Moreover, if she is aware of the distribution of the scatters in the environment, she can estimate the channel characteristics of $Alice \leftrightarrow Bob$ with high probability [29–31]. Then, she can filch the new secret keys. However, as is depicted in Figure 4c, if we use the challenge message X to replace the public pilot sequence for Alice's channel estimation, the information leakage of the new secret key can be effectively reduced.

Actually, the improved secret key agreement (*i.e.*, Figure 4c) is similar to Example 1. Then, according to Equations (5) and (13), Eve's success probability of obtaining the new secret key will reduce to $2^{-H(X|\hat{X})}$ times of its original when the wiretap channel $Alice \to (Bob, Eve)$ is less noisy.

6. Conclusion

In this paper, we have built the challenge-response authentication model over noisy channels. Towards this end, we have respectively derived the information-theoretic lower bounds on the opponent's success probability in the authentication scenarios of single time and multiple times. In comparison with the classical authentication model, analysis results have shown that our new authentication model is more secure. Remarkably, it has been proven that the Cartesian authentication code can maximize the security performance. In addition, with the Cartesian authentication code, it has been proven that the noise spreading over two separate wiretap channels can together hide the secret key. Finally, we have proposed an improved challenge-response authentication and applied it to the secret key agreement from wireless channels. Thus, we have established the utility of channel noise in identity authentication applications.

Acknowledgments

The authors would like to thank Xianglin Yan for her language revision on this paper.

This work was supported in part by the National High Technology Research and Development Program (ss2015AA011306), the National Basic Research Program of China (2013CB329002), the National Natural Science Foundation of China (61440002), the National Science and Technology Major Project (2014ZX03004003-006), the Keygrant Project of Chinese Ministry of Education (313005), the International Science and Technology Cooperation Program (2012DFG12010), the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2012D02), the Natural Science Foundation of Fujian Province of China (2014J01250) and the Tsinghua-Qualcomm Joint Research Program.

Author Contributions

Fanfan Zheng conceived of this work, derived all involved conclusions and wrote this paper. Zhiqing Xiao participated in the derivation of some conclusions and contributed valuable suggestions to develop the composition. Shidong Zhou, Jing Wang and Lianfen Huang conducted the theoretical analyses of this work and contributed valuable suggestions to consummate this paper. All authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

Appendix

A. Proof of Lemma 2

We have the facts that:

$$\begin{aligned} I(K;\hat{X},Y) =& H(\hat{X},Y) - H(\hat{X},Y|K) \\ =& H(\hat{X}) + H(Y|\hat{X}) - H(\hat{X}|K) - H(Y|K,\hat{X}) \\ \overset{(g)}{=}& H(Y|\hat{X}) - H(Y|K,\hat{X}) \\ \overset{(h)}{=}& H(Y|\hat{X}) - H(X|\hat{X}) + H(X|K,\hat{X},Y) \end{aligned} \tag{33}$$

and:

$$\begin{aligned} I(K;\hat{X},Y) =& H(K) - H(K|\hat{X},Y) \\ \overset{(i)}{=}& H(K) - H(K|X,Y) - H(X|\hat{X},Y) + H(X|K,\hat{X},Y) \\ \overset{(j)}{=}& I(K;X,Y) - H(X|\hat{X},Y) + H(X|K,\hat{X},Y). \end{aligned} \tag{34}$$

Hence, according to the equality (h) in Equation (33) and the equality (j) in Equation (34), we have:

$$\bar{P} \geq 2^{-H(Y|\hat{X})} = 2^{-I(K;X,Y)-H(X|\hat{X})+H(X|\hat{X},Y)}. \tag{35}$$

The derivation reasons of Equation (33) and Equation (34) are listed in the following.

In Equation (33), equality (g) holds due to the fact that K and $\hat{X}$ are statistically independent. Equality (h) comes from:

$$\begin{aligned} H(Y,X|K,\hat{X}) =& H(Y|K,\hat{X}) + H(X|\hat{X},Y,K) \\ =& H(X|K,\hat{X}) + H(Y|X,\hat{X},K) \overset{(k)}{=} H(X|\hat{X}) \end{aligned} \tag{36}$$

where equality (k) follows from the Markov chain $K \to \hat{X} \to X$ and $H(Y|X,K) = 0$.

In Equation (34), equality (i) comes from:

$$\begin{aligned} H(K,X|\hat{X},Y) =& H(K|\hat{X},Y) + H(X|\hat{X},Y,K) \\ =& H(X|\hat{X},Y) + H(K|X,Y) \end{aligned} \tag{37}$$

and equality (j) follows from $I(K;X,Y) = H(K) - H(K|X,Y)$.

B. Proof of Lemma 4

Firstly, following the same steps as those used in the proof of Lemma 2, we have:

$$\begin{aligned}-\log \bar{P}_i \leq & H(Y_i|\hat{X}_i, \hat{X}^{i-1}, \hat{Y}^{i-1}) \\ = & I(K; X_i, Y_i|\hat{X}^{i-1}, \hat{Y}^{i-1}) + H(X_i|\hat{X}_i) \\ & - H(X_i|\hat{X}_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1}).\end{aligned} \tag{38}$$

Furthermore, we have:

$$\begin{aligned}I(K; X_i, Y_i|\hat{X}^{i-1}, \hat{Y}^{i-1}) = & H(K|\hat{X}^{i-1}, \hat{Y}^{i-1}) - H(K|X_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1}) \\ \overset{(l)}{=} & H(K|X^{i-1}, Y^{i-1}) + H(X^{i-1}, Y^{i-1}|\hat{X}^{i-1}, \hat{Y}^{i-1}) \\ & - H(X^{i-1}, Y^{i-1}|\hat{X}^{i-1}, \hat{Y}^{i-1}, K) \\ & - H(K|X_i, Y_i, X^{i-1}, Y^{i-1}) \\ & - H(X^{i-1}, Y^{i-1}|X_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1}) \\ & + H(X^{i-1}, Y^{i-1}|\hat{X}^{i-1}, \hat{Y}^{i-1}, K) \\ = & I(K; X_i, Y_i|X^{i-1}, Y^{i-1}) + I(X^{i-1}, Y^{i-1}; X_i, Y_i|\hat{X}^{i-1}, \hat{Y}^{i-1})\end{aligned} \tag{39}$$

where equality (l) comes from:

$$\begin{aligned}H(K|\hat{X}^{i-1}, \hat{Y}^{i-1}) = & H(K, X^{i-1}, Y^{i-1}|\hat{X}^{i-1}, \hat{Y}^{i-1}) - H(X^{i-1}, Y^{i-1}|K, \hat{X}^{i-1}, \hat{Y}^{i-1}) \\ = & H(K|X^{i-1}, Y^{i-1}) + H(X^{i-1}, Y^{i-1}|\hat{X}^{i-1}, \hat{Y}^{i-1}) \\ & - H(X^{i-1}, Y^{i-1}|K, \hat{X}^{i-1}, \hat{Y}^{i-1})\end{aligned} \tag{40}$$

and:

$$\begin{aligned}H(K|X_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1}) = & H(K, X^{i-1}, Y^{i-1}|X_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1}) - H(X^{i-1}, Y^{i-1}|K, \hat{X}^{i-1}, \hat{Y}^{i-1}) \\ = & H(X^{i-1}, Y^{i-1}|X_i, Y_i, \hat{X}^{i-1}, \hat{Y}^{i-1}) + H(K|X^{i-1}, Y^{i-1}, X_i, Y_i) \\ & - H(X^{i-1}, Y^{i-1}|K, \hat{X}^{i-1}, \hat{Y}^{i-1}).\end{aligned} \tag{41}$$

Thus, Equation (20) is derived by putting Equation (39) into Equation (38).
This completes our proof.

References

1. Menezes, A.J.; Vanstone, S.A.; Oorschot, P.C.V. *Handbook of Applied Cryptography*; CRC Press: Boca Raton, FL, USA, 1997.
2. Yang, L. Course Notes: Biometrics and Cryptography. Available online: http://web2.utc.edu/~Li-Yang/cpsc4600/08_Entity-Authentication14.ppt (accessed on 10 July 2015).
3. Yu, P.; Baras, J.; Sadler, B. *An Implementation of Physical Layer Authentication Using Software Radio*; Technical report, DTIC Document, ARL-TR-4888; Army Research Laboratory: Adelphi, MD, USA, July 2009.
4. Simmons, G.J. Authentication theory/coding theory. In *Advances in Cryptology*; Blakley, G.R., Chaum, D., Eds.; Springer: Berlin/Heidelberg, Germany, 1985; pp. 411–431.

5. Maurer, U.M. Authentication theory and hypothesis testing. *IEEE Trans. Inf. Theory* **2000**, *46*, 1350–1356.
6. Rosenbaum, U. A lower bound on authentication after having observed a sequence of messages. *J. Cryptol.* **1993**, *6*, 135–156.
7. Zeng, K.; Govindan, K.; Mohapatra, P. Non-cryptographic authentication and identification in wireless networks. *IEEE Trans. Wirel. Commun.* **2010**, *17*, 56–62.
8. Lai, L.; El Gamal, H.; Poor, H.V. Authentication over noisy channels. *IEEE Trans. Inf. Theory* **2009**, *55*, 906–916.
9. Zheng, F.; Xiao, Z.; Zhou, S.; Wang, J.; Huang, L. Message authentication over noisy channels. *Entropy* **2015**, *17*, 368–383.
10. Bellare, M. Course Notes: Modern Cryptography. Available online: http://cseweb.ucsd.edu/~mihir/cse207/w-mac.pdf (accessed on 10 July 2015).
11. Koç, Ç.K. Course Notes: Explorations in Cryptography. Available online: http://cs.ucsb.edu/~koc/ccs130h/notes/mac2.pdf (accessed on 10 July 2015).
12. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387.
13. Ren, K.; Su, H.; Wang, Q. Secret key generation exploiting channel characteristics in wireless communications. *IEEE Trans. Wirel. Commun.* **2011**, *18*, 6–12.
14. Chen, C.; Jensen, M.A. Improved channel quantization for secret key establishment in wireless systems. In Proceedings of 2010 IEEE International Conference on Wireless Information Technology and Systems (ICWITS), Honolulu, HI, USA, 28 August–3 September 2010; pp. 1–4.
15. Csiszár, I.; Korner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348.
16. Ozel, O.; Ulukus, S. Wiretap channels: Roles of rate splitting and channel prefixing. In Proceedings of 2011 IEEE International Symposium on Information Theory Proceedings (ISIT), St. Petersburg, Russia, 31 July–5 August 2011; pp. 628–632.
17. Bloch, M.; Barros, J. *Physical-Layer Security*; Cambridge University Press: Cambridge, UK, 2011.
18. Qin, H.; Chen, X.; Sun, Y.; Zhao, M.; Wang, J. Optimal power allocation for joint beamforming and artificial noise design in secure wireless communications. In Proceedings of 2011 IEEE International Conference on Communications Workshops (ICC), Kyoto, Japan, 5–9 June 2011; pp. 1–5.
19. Liao, W.C.; Chang, T.H.; Ma, W.K.; Chi, C.Y. Joint transmit beamforming and artificial noise design for QoS discrimination inwireless downlink. In Proceedings of 2010 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), Dallas, TX, USA, 14–19 March 2010; pp. 2562–2565.
20. Goel, S.; Negi, R. Guaranteeing secrecy using artificial noise. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2180–2189.
21. Thangaraj, A.; Dihidar, S.; Calderbank, A.R.; McLaughlin, S.W.; Merolla, J.M. Applications of LDPC codes to the wiretap channel. *IEEE Trans. Inf. Theory* **2007**, *53*, 2933–2945.
22. Klinc, D.; Ha, J.; McLaughlin, S.W.; Barros, J.A.; Kwak, B.J. LDPC codes for the Gaussian wiretap channel. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 532–540.

23. Richardson, T.J.; Shokrollahi, M.A.; Urbanke, R.L. Design of capacity-approaching irregular low-density parity-check codes. *IEEE Trans. Inf. Theory* **2001**, *47*, 619–637.
24. Subramanian, A.; Thangaraj, A.; Bloch, M.; McLaughlin, S.W. Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 585–594.
25. Ding, C.; Helleseth, T.; Klove, T.; Wang, X. A generic construction of Cartesian authentication codes. *IEEE Trans. Inf. Theory* **2007**, *53*, 2229–2235.
26. Li, Z.; Gao, S.; Wang, Z.; Thuraisingham, B.M.; Wu, W. A construction of Cartesian authentication code from orthogonal spaces over a finite field of odd characteristic. *Discrete Math., Alg. Appl.* **2009**, *1*, 105–114.
27. Sze, T.; Chanson, S.; Ding, C.; Helleseth, T.; Parker, M. Logarithm cartesian authentication codes. *Inf. Compu.* **2003**, *184*, 93–108.
28. Chanson, S.; Ding, C.; Salomaa, A. Cartesian authentication codes from functions with optimal nonlinearity. *Theor. Comput. Sci.* **2003**, *290*, 1737–1752.
29. Chen, G.; Zhang, Y.; Luan, F.; Xiao, L. Optimization of AP placement in indoor fingerprint positioning. In Proceedings of 2013 International Conference on ICT Convergence (ICTC), Jeju, South Korea, 14–16 October 2013; pp. 98–100.
30. Luan, F.; Zhang, Y.; Xiao, L.; Zhou, C.; Zhou, S. Fading characteristics of wireless channel on high-speed railway in hilly terrain scenario. *Int. J. Antennas Propag.* **2013**, *12*, 188–192.
31. Zhang, Y.; Li, Z.; Luan, F.; Xiao, L.; Zhou, S.; Wang, J. Measurement-based analysis of transmit antenna selection for in-cabin distributed MIMO system. *Int. J. Antennas Propag.* **2012**, *16*, 104–107.