entropy

MDPI

Article

Unconditional Authentication Based on Physical Layer Offered Chain Key in Wireless Communication

Shaoyu Wang, Kaizhi Huang, Xiaoming Xu, Xiaoyan Hu, Jing Yang and Liang Jin *

Wireless Communication Technology Office, Information Engineering University, Zhengzhou 450002, China; shaoyuwang_ndsc@163.com (S.W.); huangkaizhi@tsinghua.org.cn (K.H.); ee_xiaomingxu@sina.com (X.X.); ndscpls@163.com (X.H.); wanzheng18@alumni.hust.edu.cn (J.Y.)
* Correspondence: liangjin@263.net

Abstract: Authentication is a critical issue in wireless communication due to the impersonation and substitution attacks from the vulnerable air interface launched by the malicious node. There are currently two kinds of authentication research in wireless communication. One is based on cryptography and relies on computational complexity, the other is based on physical layer fingerprint and can not protect data integrity well. Both of these approaches will become insecure when facing attackers with infinite computing power. In this paper, we develop a wireless unconditional authentication framework based on one-time keys generated from wireless channel. The proposed unconditional authentication framework provides a new perspective to resist infinite computing power attackers. We study the performance of the unconditional authentication framework in this paper. First, a physical layer offered chain key (PHYLOCK) structure is proposed, which can provide one-time keys for unconditional authentication. The physical layer offered chain keys are generated by XORing the physical layer updated keys extracted from the current channel state information (CSI) and the previous chain keys. The security of PHYLOCK is analyzed from the perspective of information theory. Then, the boundary of the deception probability is conducted. It is shown that unconditional authentication can achieve a probability of deception $2^{-\frac{1}{2}H(k)}$, where $H(k)$ is the entropy of the one-time key used for one message. Finally, the conditions for unconditional authentication are listed. Our analysis shows that the length of the key and the authentication code need to be twice the length of the message and the encoding rules of the authentication code need to satisfy the restrictions we listed.

Keywords: unconditional authentication; physical layer key generation; wireless communication

Citation: Wang, S.; Huang, K.; Xu, X.; Hu, X.; Yang, J.; Jin, L. Unconditional Authentication Based on Physical Layer Offered Chain Key in Wireless Communication. *Entropy* **2022**, *24*, 488. https://doi.org/10.3390/e24040488

Academic Editor: Song-Nam Hong

Received: 6 March 2022
Accepted: 29 March 2022
Published: 30 March 2022

1. Introduction

1.1. Physical Layer Authentication

Authentication is one of the two important aspects of information security, and the other is known to be confidentiality [1,2]. Especially in wireless communication, due to the broadcasting characteristics of wireless communication and the improvement of the malicious adversary's ability, wireless nodes are very vulnerable to impersonation and substitution attacks [3]. In an impersonation attack, the malicious adversary impersonates the transmitter and sends fraudulent information to the receiver when in reality nothing has been sent by the transmitter. While in a substitution attack, the malicious adversary intercepts legitimate message from the transmitter and successfully replaces the legitimate message with a fraudulent one [4,5]. With the rapid development of wireless communication and the increasing demand for communication security, authentication in wireless communication is becoming more and more indispensable [6]. Most of the existing wireless authentication approaches are based on computational complexity and become insecure when facing attackers with infinite computing power. In this paper, we propose an unconditional authentication framework to resist these attacks. Next, we will introduce the concepts and principles of authentication and the contributions of our paper.

Authentication needs to achieve two goals [7,8]. One goal is to ensure the integrity of the message. If the message received by the receiver is consistent with the message transmitted by the transmitter, the integrity of the message is achieved. However, merely achieving the integrity of the message is not sufficient, because the identity of the transmitter may be fake. For example, the receiver can confirm that the message is integral by the corresponding digest value, but cannot confirm who sent the message. Therefore, another goal is to confirm the identity of the transmitter. The receiver confirms that the message is from a legitimate transmitter by sharing the same secret key, which is the scope of our paper.

1.2. Related Works

There are two approaches for achieving authentication in wireless communication. One approach is to use "physical fingerprints", which can be roughly divided into two categories: channel-based and radio frequency (RF) fingerprint-based schemes. The channel-based schemes [9–13] use CSI as a special kind of fingerprint that represents and discriminates different user identities. Another way of channel-based authentication is by generating an authentication vector according to both the CSI and the shared secret key. Paper [14] proposes an authentication scheme based on channel coding, where the shared key and CSI between two legitimate devices are combined against the adversary's attack. A hybrid authentication protocol is proposed to integrate the CSI into the higher-layer security protocol without assuming a reliable reference channel estimation [15]. In [16,17], a key-based physical layer challenge-response authentication mechanism (PHY-CRAM) is studied, which doesn't require any channel estimation or training. However, such schemes don't provide integrity protection and cannot detect if the message has been manipulated or not. The RF fingerprint-based scheme [18–20] identifies a device according to the unique features of the waveform. RF fingerprint is caused by imperfections inherent in the hardware components. RF fingerprint-based authentication is more suitable for identity verification, while it is impractical to authenticate every symbol through this scheme. The other approach is called "authentication codes approach" [21–24]. This approach relies on modern cryptography and is a kind of computational security. Generally speaking, "authentication codes approach" belongs to coding theory and improves the chance of detecting deception by intentionally introducing redundant information in the transmitted message. "Authentication codes approach" reduces communication efficiency since extra authentication codes are transmitted. "Authentication codes approach", such as the well-known message authentication codes (MAC) in cryptography, are the most popular solution to provide security services of data integrity and authentication in network communications. We take hash-based message authentication codes (HMAC) as an example to illustrate the principle of message authentication codes. The security of HMAC is based on the same shared root key and hash functions. Hash functions map from larger domains to smaller ranges and verify the integrity of the message while the shared root key verifies the identity of the transmitter. The security of MAC depends on the computational complexity and can be cracked if the malicious adversary with efficient computing resources. Especially in wireless communication, the transmitter and receiver share an unchanged root key due to the difficulty of key agreement and distribution. Wireless communication is more vulnerable to the malicious adversary.

1.3. Our Contributions

The focus of this paper is unconditional authentication in wireless communication, which is to study the performance of the authentication system if the malicious adversary with infinite computing resources. The security of the authentication methods discussed above are all based on computational complexity and is not an unconditional authentication from the perspective of information theory. It is difficult to achieve unconditional authentication like the well-known one-time pad for encryption. Fortunately, the unique and random characteristics of wireless channels can provide a source for generating true random keys, which is called physical layer key generation technology in most literature.

Physical layer key generation has the potential to solve the key distribution problem, and thus makes unconditional authentication possible.

In this paper, we aim to propose an unconditional authentication framework based on one-time keys generated from the wireless channels. The framework can provide theoretical guidance for the authentication in wireless communication. Specifically, the contributions of this paper are summarized as follows:

- We derive the lower bound of unconditional authentication based on an unchanged key. We assume the adversary Mallory with unlimited computing resources and analyze the impersonation and substitution attacks. The probability of deception $\geq 2^{-\frac{1}{2}H(k)}$ is strictly derived from the perspective of information theory, where $H(k)$ is the entropy of the shared key. However, the lower bound $2^{-\frac{1}{2}H(k)}$ holds only for sending one authenticated message. The same key can not be used twice.
- Physical layer offered chain key (PHYLOCK) structure [25] is introduced to provide one-time keys for unconditional authentication so that we can achieve the lower bound $2^{-\frac{1}{2}H(k)}$. PHYLOCK can provide the root of trust for key generation and authentication. We conduct a security analysis of PHYLOCK and prove that PHYLOCK is more secure than the traditional physical layer key generation.
- Some conditions of unconditional authentication are listed. To realize the lower bound of unconditional authentication, encoding rules need to comply with some conditions. The conditions show that the length of the key and the authentication code are twice the length of the message.

The rest of this paper is organized as follows. Section 2 introduces the system and authentication model. Section 3 derives the lower bound of unconditional authentication based on an unchanged key. Section 4 points out that the pseudo-random key is not able to achieve unconditional authentication. Section 5 presents the structure and procedure of PHYLOCK and conducts security analysis of PHYLOCK. Following that Section 5 gives the definition and conditions of unconditional authentication. Section 6 concludes the paper and points out the significance, limitations, and future research of our paper.

2. System and Authentication Model

We consider a peer-to-peer wireless system depicted in Figure 1, where a legitimate transmitter (Alice) wants to send messages to the receiver (Bob). To overcome channel fading, accurate acquisition of CSI is essential to achieve spectrum and energy efficiency in wireless systems [26,27]. Alice and Bob obtain reciprocal CSI via various channel estimation methods. CSI is location-specific and time-varying due to path loss and channel fading [14,28]. It is difficult for an adversary to obtain information about the legitimate CSI as long as the distance between the malicious adversary and legitimate nodes is larger than half of the wavelength. CSI provides a source of common randomness that the malicious adversary has not or only partially, which can be used to generate secret keys shared only by Alice and Bob.

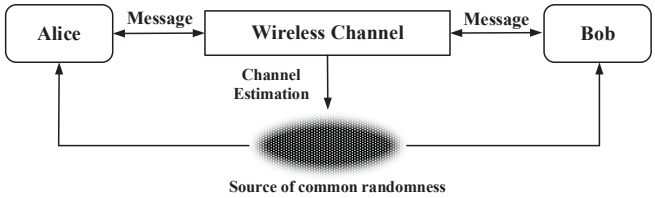

Figure 1. System model.

Due to the broadcasting characteristics of wireless communication, wireless communication is vulnerable to various attacks. In this paper, we focus on the authentication problem that the legitimate receiver should be able to ensure the identity and the integrity of received messages, which is a major requirement of secure communications. In many sce-

narios, authentication is considered even more important than confidentiality since many messages might not be "secret", but should be "authentic". The authentication system is illustrated in Figure 2, where the message from Alice is authenticated by Bob and the reverse is the same. The authentication encoder outputs the authentication code c, which is a function of the secret key k and the message m. Then, the authentication code c together with the message m are sent to the receiver Bob. Bob uses the same encoder algorithm with the received message $\tilde{m}$ and the shared key k as input to generate the authentication code $\tilde{c}$. If $c = \tilde{c}$, Bob considers the received message as verified (i.e., the integrity test is successful). Otherwise, Bob judges that the message is not integral or from other illegal parties. We consider an active malicious adversary named Mallory that aims to deceive Bob to accept the fraudulent message. Attacks from Mallory can be divided into two types. One is the impersonation attack (successfully creating a fraudulent message) and the other is the substitution attack (successfully replacing a valid message with a fraudulent one). We consider a scenario in which Mallory has unlimited computing resources, which is different from the case of cryptography-based authentication, but indeed a major requirement for unconditional authentication. Furthermore, we assume Mallory knows everything about the system, except for the shared secret key. This is a well-known assumption in cryptography, known as Kerckhoff's principle. It is equally reasonable to adopt Kerckhoff's principle for authentication.

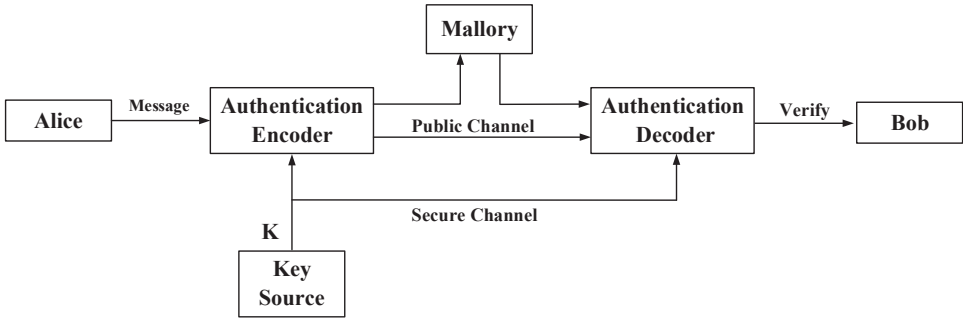

Figure 2. Authentication model.

3. Lower Bound of Unconditional Authentication Based on an Unchanged Key

In this section, we analyze the lower bound of unconditional authentication based on an unchanged key, which is a basic analysis of Sections 4 and 5.

To prevent impersonation and substitution attacks from Mallory, Alice encodes the message m using a key k to produce the authentication code c.

$$c = f(m, k, v) \tag{1}$$

where v represents the initialization vector, which is usually a pseudo-random number. The initialization vector v guarantees that when Alice transmits the same message twice, the corresponding authentication codes are different. This makes it difficult for Mallory to perform a replay attack or obtain useful information about the authentication system. According to Kerckhoff's principle [29], we assume Mallory knows everything about the authentication system, includes the encoding rules $f(\cdot, \cdot)$, the message m, the initialization vector v, and the corresponding authentication code c, but does not know the shared key k. Since the initial vector v is known, in the following, we will simplify (1) as

$$c = f(m, k) \tag{2}$$

Equation (2) simplifies the problem without losing generality. In some authentication schemes, the encrypted message $\bar{m}$ instead of the message m is used to generate the authentication code c. However, it does not affect the universality of Equation (2) because we assume Mallory already knows the message m and there is a one-to-one mapping

between the encrypted messages $\bar{m}$ and the corresponding messages m. Then, Alice transmits the message and the corresponding authentication code together to Bob.

$$y = (m; c) \tag{3}$$

Bob will use c to test the received message m for authenticity.

Mallory attempts to use a false message m' to launch impersonation or substitution attacks. Bob will calculate $c' = f(m', k)$, if $c \neq c'$, Bob will discover Mallory's deception. Mallory's probability of escaping detection will be called p_0, which is the probability value when Mallory obtains the optimal strategy. In this paper, p_0 is the smallest probability of deception even though Mallory has unlimited computing resources, so we call p_0 the lower bound of unconditional authentication. Mallory can use the blind guessing scheme if Mallory does not have any prior information. For example, Mallory can successfully deceive Bob with probability $p_0 \geq |K|^{-1}$ just by guessing a key at random with all $|K|$ keys equally likely. Another scheme is to guess the corresponding authentication code c' at random with all $|C|$ codes equally likely and $p_0 \geq |C|^{-1}$. In fact, Mallory can always intercept the message between Alice and Bob and he can use the knowledge of m and c to restrict his guess, and thus improves the probability of deception.

We first discuss the probability of deception informally when the key k keeps unchanged and Mallory obtains only one piece of the message m and the corresponding authentication code c. Mallory can use Equation (2) to learn the key k. Since Mallory has infinite computing power and Mallory can search the entire keyspace K to find the keys that satisfy Equation (2). In order to reduce the probability of being deceived, Bob must reasonably construct encoding rules $f(\cdot, \cdot)$ so that Equation (2) has as many solutions as possible. The mapping among the message m, key k, and code c has a diagram like Figure 3, which depicts messages m as points in the left column and codes c as points in the right column. The lines directed from left to right are labeled by the key names $1, \ldots, K$ to show how these keys encode each m into a code c. Suppose there are n solutions and the probability that Mallory will pick the correct key is $\frac{1}{n}$. As one might expect, Bob must use a large number of possible keys to provide many solutions to Equation (2). However, Mallory need not guess the correct key. Mallory still succeeds if

$$f(m', k_0) = f(m', k) \tag{4}$$

where m' is the false message that Mallory wants to send to Bob, k is the correct key, k_0 is one of the n solutions satisfying $c' = f(m', k)$. Then, the probability of obtaining the correct c' is $\frac{n}{|K|}$. Therefore, the number of solutions n for every message can neither be too large nor too small. From the definition of p_0, we have

$$p_0 = \min\left\{\max\left\{\frac{1}{n}, \frac{n}{|K|}\right\}\right\} \tag{5}$$

$\max\left\{\frac{1}{n}, \frac{n}{|K|}\right\}$ means take the larger of the two probabilities. When $\frac{1}{n} = \frac{n}{|K|}$, p_0 takes the minimum value, that is $p_0 = |K|^{\frac{1}{2}}$.

Next, we will rigorously prove the lower bound of unconditional authentication from the perspective of information theory. Before the proof, we will list some natural restrictions on the behavior of Alice, Bob, and Mallory [30].

(a) Alice and Bob use the $|K|$ keys at random, equally likely and independent of the message m. Therefore, we have $|K| = 2^{H(k)}$. Mallory is not subject to this restriction. He can use the keys in any way to help increase p_0.
(b) All $|C|$ coded messages are equally likely. In other words, every message is equally important. Alice and Bob do not have to protect some messages exclusively.
(c) Mallory picks m' at random from the $|C| - 1$ coded messages different from m', all equally likely.

(d) Any different messages m_1, m_2 cannot be encoded into the same c, i.e., $f(m_1, k_1) \neq f(m_2, k_2)$, hold for all k_1, k_2, if $m_1 \neq m_2$. This restriction only strengthens the lower bound of deception probability because there may be better strategies for Mallory if $f(m_1, k_1) = f(m_2, k_2)$.

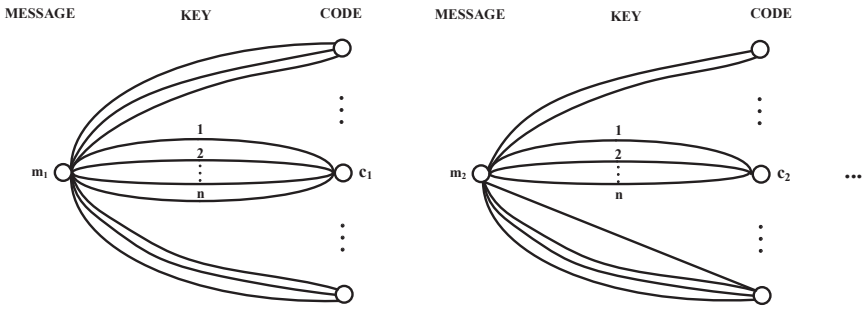

Figure 3. Diagram of message, key and code.

Knowing how the message m, m' and key k are distributed, we can compute the joint probability $P(m, c, m')$. Define $p_0(m, c, m')$ to be the deception probability when Mallory substitutes a given m' for a given m, knowing c. The probability $p_0(m, c, m')$ depends on how Mallory uses m, c, m' to determine a false code c'. Mallory knows the function $f(\cdot, \cdot)$ and the key distribution. Then, Mallory can compute the conditional probability distribution $P(c'|m, c, m')$ of the correct code $c' = f(m', k)$. Mallory maximizes his chance of success by selecting a c', which maximizes $P(c'|m, c, m')$. Then, Mallory achieves $p_0(m, c, m')$ by

$$p_0(m, c, m') = \underset{c'}{Max}\, P(c'|m, c, m')) \tag{6}$$

Then, p_0 is the weighted average deception probability of all $p_0(m, c, m')$ with weight $P(m, c, m')$.

$$p_0 = \sum_{m,c,m'} P(m, c, m')\, p_0(m, c, m') \tag{7}$$

Therefore, p_0 is optimal for Mallory when he adopts the best strategy. We now relate p_0 to the average uncertainty U, which Mallory has about the correct code c'. By the definition of conditional entropy, we can calculate U

$$\begin{aligned} U &= H(c'|m, c, m') \\ &= -\sum_{m,c,m',c'} P(m, c, m', c') \log P(c'|m, c, m') \end{aligned} \tag{8}$$

Next, we give **Lemma 1** to reveal the relationship between p_0 and U.

Lemma 1. *if Mallory chooses optimal c' to make (6) holds, then*

$$p_0 \geq 2^{-U} \tag{9}$$

The equality relationship in (9) holds if and only if all the possible c' for m' are equally likely and $P(m, c, m') \neq 0$. The equality in (9) means that there are exactly 2^U such c' for every given (m, c, m').

Proof. Since $(-\log x)'' = \frac{1}{x^2} > 0$, for all $x > 0$, the function $-\log x$ is concave. Then, we have Jenson's inequality expressed as

$$-\log\left(\sum_{i=1}^{n} \lambda_i x_i\right) \leq -\sum_{i=1}^{n} \lambda_i \log x_i \tag{10}$$

where $x_i > 0$, $\sum_i \lambda_i = 1$, $\lambda_i > 0$, $i = 1, 2, \ldots, n$. According to (6) and the concavity of the function $-\log x$, we have

$$\begin{aligned} U &= -\sum_{c'} \sum_{m,c,m'} P(m,c,m',c') \log P(c'|m,c,m') \\ &\overset{(a)}{=} -\sum_{m,c,m'} P(m,c,m') \log P(c'|m,c,m') \\ &\overset{(b)}{\geq} -\sum_{m,c,m'} P(m,c,m') \log p_0(m,c,m') \\ &\overset{(c)}{\geq} -\log \sum_{m,c,m'} P(m,c,m') p_0(m,c,m') \end{aligned} \tag{11}$$

where step (a) is to sum on c', step (b) is because $p_0(m,c,m') \geq P(c'|m,c,m')$, step (c) is based on the concavity of the function $-\log x$ and Jensen's inequality. Now, we can get **Lemma 1** from (7) and (11). □

The proof uses two inequalities in step (b) and step (c). Both must become equalities if equality holds in (9). The first inequality $p_0(m,c,m') \geq P(c'|m,c,m')$ requires all possible c' to be equally likely for given m, c, m'. In the discussion of Jensen's inequality, equality requires all $\log p_0(m,c,m')$ terms to be equal to U.

We next bound p_0 in terms of the conditional entropy $H(k)$, which indicates the uncertainty of the key.

Theorem 1. *Suppose* (6) *and restrictions (a), (b), (c), (d) all hold. Then,*

$$p_0 \geq 2^{-\frac{1}{2}H(k)} \tag{12}$$

Proof. First note that c' is only determined by $c' = f(m',k)$ if m', k are given. Then, c' contains less information than (m',k).

$$U = H(c'|m,c,m') \leq H(m',k|m,c,m') = H(k|m,c,m') \tag{13}$$

However, the conditional probability for k given m, c, m' depends only on m, c, so (13) becomes

$$U \leq H(k|m,c) \tag{14}$$

Since the message and the key are independent and c is only determined by $c = f(m,k)$, we have

$$H(k) = H(k|m) = H(k,c|m) \tag{15}$$

Due to the strong additivity of entropy, (15) becomes

$$H(k) = H(k,c|m) = H(c|m) + H(k|m,c) \tag{16}$$

(14) and (16) provides

$$U \leq H(k) - H(c|m) \tag{17}$$

and

$$U = H(c'|m,c,m') \leq H(c'|m') \tag{18}$$

Due to restriction (c), m' is equally likely to be any one of the $|C|$ coded messages. Then, by restriction (b), m and m' have the same distribution, and finally

$$U \leq H(c|m) \tag{19}$$

Now, compare (17) and (19). If $H(c|m) \geq \frac{1}{2}H(k)$, $U \leq \frac{1}{2}H(k)$ follows from (17). If $H(c|m) \leq \frac{1}{2}H(k)$, $U \leq \frac{1}{2}H(k)$ follows from (19). **Theorem 1** holds for both cases. □

Theorem 1 indicates Mallory can find $2^{\frac{1}{2}H(k)}$ solutions $k \in S(m_i, c_i) = \{k | f(m_i, k) = c_i\}$ and Mallory's uncertainty about the key is $\frac{1}{2}H(k)$ with one message and code. When Mallory intercepts a second $m_j, c_j, j \neq i$, Mallory's uncertainty about the key will drop rapidly because the real key fits both $k \in S(m_i, c_i)$ and $k \in S(m_j, c_j), i \neq j$. As Mallory intercepts more messages, the unchanged key will eventually be disclosed. Therefore, the key needs to be changed with each message sent.

4. Security Analysis under Pseudo-Random Key

Cryptography-based stream ciphers [31,32] are regarded as one of the technologies that generate constantly changing keys in wireless communication. However, it is impossible to achieve unconditional authentication using stream ciphers when Mallory has infinite computing power. In the following, we list two main reasons for this conclusion. The first reason is that more and more attack methods against stream ciphers appear, such as the algebraic attack [33], resynchronization attack [34], etc. The stream cipher is a computing security scheme and will become insecure when facing Mallory with infinite computing power. The second reason is that the stream cipher keys are generated by the initial key, and the entropy of the initial key is constant. From the perspective of information theory, as Mallory intercepts more and more messages and codes (m_i, c_i), the entropy of the initial key will gradually decrease and finally be cracked by Mallory. Therefore, only true random keys can achieve unconditional authentication.

5. Unconditional Authentication Based on PHYLOCK

In this section, we first introduce the structure and procedure of the physical layer offered chain key (PHYLOCK), which acts as a key generator and provides one-time keys for unconditional authentication. Then, we analyze the security of PHYLOCK and prove that PHYLOCK is a reliable secure key generator. Finally, we define unconditional authentication and list the conditions for achieving unconditional authentication under the framework of this paper.

5.1. The Structure and Procedure of PHYLOCK

The structure of PHYLOCK is shown in Figure 4, which includes three kinds of keys. The initial key K^0 is the start of PHYLOCK and provides the root of trust for Alice and Bob. K^0 is pre-stored by Alice and Bob through a secure channel and keeps unchanged in subsequent procedures. The physical layer updated key X^i is generated from the wireless channel between Alice and Bob, which provides a source of common randomness, just as shown in Figure 5. It is almost impossible for Mallory who is located at a different place from Alice and Bob to obtain the same source of randomness for key generation. This is called the spatial decorrelation assumption in most key generation research exploiting channel randomness [35,36]. Figure 5 is the block diagram of the physical layer updated key generation. The procedure for extracting secret bits is generally divided into five phases. The first phase is channel probing. The purpose is to extract the same CSI between Alice and Bob, which is usually achieved by sending pilot symbols to each other. The second phase is filtering to obtain as consistent CSI as possible on the Alice and Bob sides. In the third phase, Alice and Bob input the CSI into the equal probability quantizer, respectively, and perform 1-bit quantization. In the information reconciliation phase, Alice and Bob should reconcile to a common key through public discussion while leaking as little information as possible. Finally, the privacy amplification phase applies universal hash functions to the reconciled information to ensure the shared secret key completely unknown to Mallory.

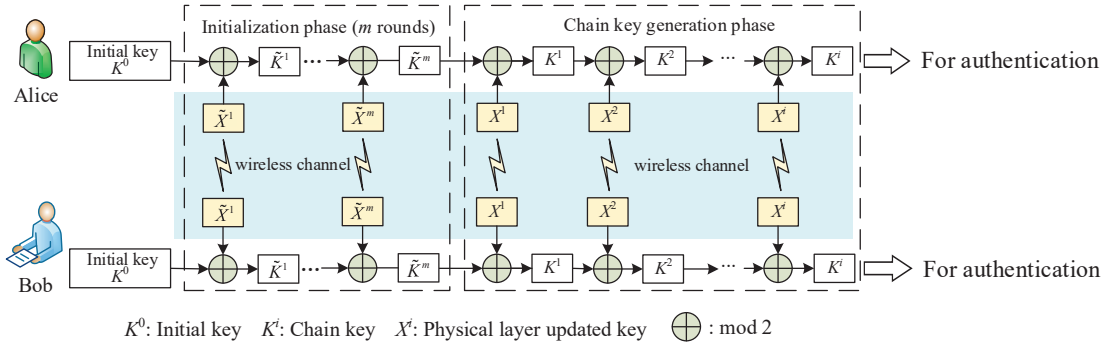

Figure 4. Structure of PHYLOCK.

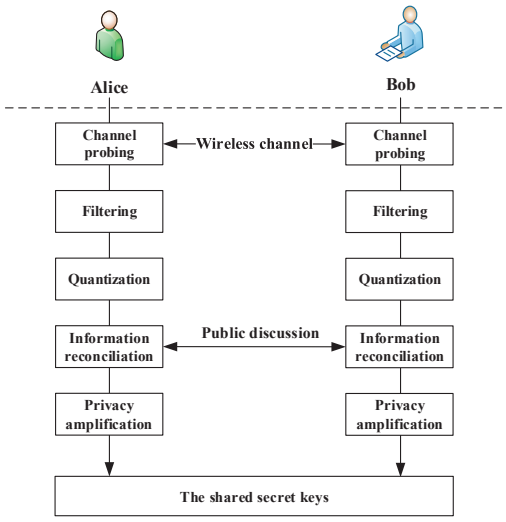

Figure 5. A block diagram of physical layer updated key generation.

Chain key $K^i, i > 0$ is the one-time key used for unconditional authentication. Different from the traditional physical layer key generation [37,38], we perform XOR operation on the previous chain key K^{i-1} and the physical layer newly generated key $X^i, i > 0$ to generate a new chain key K^i, which is expressed as

$$K^i = K^{i-1} \oplus X^i \tag{20}$$

The physical layer updated key X^i continuously updates the chain key K^{i-1}. The chain key K^i not only contains the information of the physical layer updated key X^i, but also the information of the last chain key. It is determined by all previous physical layer generated keys, thus making the chain highly secure. More security analysis of PHYLOCK is in Section 5.2.

PHYLOCK operates iteratively by physical layer updated keys continuously generated from the wireless channel. The initial key K^0 pre-set by Alice and Bob provides the root of trust for authentication. The initial key K^0 guarantees the trustworthiness of the physical layer updated key X^1 and chain key K^1, and thus the subsequent physical layer updated keys $X^2, X^3 \ldots$ and chain keys $K^2, K^3 \ldots$. The trust relationship between Alice and Bob is passed along with the iterative process. Before PHYLOCK officially generates chain keys, PHYLOCK first performs the initialization phase. The initialization phase iterates m rounds to mask the initial key K^0 and protect K^0 from being leaked. Then, the physical layer updated keys are generated along the data transmission. The key generation rate of PHYLOCK depends on the generation rate of physical layer updated keys. There are many physical layer key generation schemes in the previous work to increase the key generation rate [39,40]. Finally, the chain keys $K^i, i = 1, 2, 3 \ldots$ generated by PHYLOCK are used for unconditional authentication. The procedure of PHYLOCK is summarized in Algorithm 1.

Algorithm 1 The procedure of unconditional authentication based on PHYLOCK.

Input: The initial key, K^0; The wireless channel state information, CSI_i;
Output: The chain keys, K^i;

1: Alice and Bob perform initial authentication through the initial key K^0;
2: Perform initialization phase of m rounds;
3: Alice and Bob probe the wireless channel state information CSI_i and generate physical layer updated key X_i, see Figure 5;
4: Generate the chain keys: $K^i = K^{i-1} \oplus X^i$;
5: Use the chain keys for message authentication according to the encoding rules $f(\cdot,\cdot)$;
6: Repeat Steps 3–5;
7: If the message authentication fails, Alice and Bob return to Step 2 and perform the initialization phase.

5.2. Security Analysis of PHYLOCK

The security of PHYLOCK is the basis for unconditional authentication. In this section, we conduct a security analysis of PHYLOCK. The security of PHYLOCK depends on the difficulty of Mallory to crack PHYLOCK. We consider three attack cases to illustrate the security of PHYLOCK. **Case 1:** Mallory obtains X^i or K^{i-1} to break PHYLOCK. This is possible, for example, if Mallory probes the same wireless channel and generates the same physical layer updated key X^i, or guessed the correct chain key K^{i-1} according to the current message. **Case 2:** Mallory gets both X^i and K^{i-1} to break PHYLOCK. **Case 3:** Mallory knows all X^i and K^i, and attempts to recover the initial key K^0. **Case 3** is similar to the known-plaintext attack in stream cipher and can be regarded as the worst attack case for PHYLOCK. The difficulty of these attacks is ascending. In addition to these three attack cases, we also discuss and simulate the performance of PHYLOCK under correlated channel attacks.

5.2.1. Analysis for Case 1

The security under **Case 1** means that Mallory can not reduce the uncertainty about K^i by knowing K^{i-1} or X^i. We need to prove the following equation holds:

$$H\left(K^i\right) = H\left(K^i|K^{i-1}\right) \tag{21}$$

$$H\left(K^i\right) = H\left(K^i|X^i\right) \tag{22}$$

Proposition 1. *For the chain key* $K^i = \left(k_1^i k_2^i \dots k_r^i\right)$ *and physical layer updated key* $X^i = \left(x_1^i x_2^i \dots x_r^i\right)$*, where r is the key length,* $x_j^i \in \{0,1\}, j = 1,2,\dots,r$ *is an independent and identically distributed (i.i.d) random variable whose probability distribution satisfies* $\Pr\left(x_j^i = 1\right) = \Pr\left(x_j^i = 0\right) = 0.5$*, then we get* $H\left(K^i\right) = H\left(K^i|K^{i-1}\right) = r$ *bits,* $H\left(K^i\right) = H\left(K^i|X^i\right) = r$ *bits.*

Proof. First, we calculate the probability distribution of $\Pr\left(K^i\right)$.

$$\begin{aligned} &\Pr\left(k_j^i = 1\right) = \Pr\left(k_j^{i-1} \oplus x_j^i = 1\right) \\ &= \Pr\left(k_j^{i-1} = 1\right)\Pr\left(x_j^i = 0\right) + \Pr\left(k_j^{i-1} = 0\right)\Pr\left(x_j^i = 1\right) \\ &= 0.5\left(\Pr\left(k_j^{i-1} = 1\right) + \Pr\left(k_j^{i-1} = 0\right)\right) = 0.5 \end{aligned} \tag{23}$$

Similarly, we can get $\Pr\left(k_j^i = 0\right)$=0.5. Next, we calculate the conditional probability distribution $\Pr\left(K^i|K^{i-1}\right)$.

$$\begin{aligned}
&\Pr\left(k_j^i = 1 | k_j^{i-1}\right) \\
&= \Pr\left(k_j^{i-1} \oplus x_j^i = 1 | k_j^{i-1} = 0\right) \Pr\left(k_j^{i-1} = 0\right) + \\
&\Pr\left(k_j^{i-1} \oplus x_j^i = 1 | k_j^{i-1} = 1\right) \Pr\left(k_j^{i-1} = 1\right) \\
&= 0.5\left(\Pr\left(x_j^i = 1\right) + \Pr\left(x_j^i = 0\right)\right) = 0.5
\end{aligned} \tag{24}$$

Similarly, we can get $\Pr\left(k_j^i = 0 | k_j^{i-1}\right) = 0.5$. Since $\Pr(K^i) = \Pr(K^i | K^{i-1})$, K^i and K^{i-1} are independent of each other and (21) holds. Following the same derivation process, we can get $H(K^i) = H(K^i | X^i) = r$ bits. **Proposition 1** shows that Mallory can not decrease $H(K^i)$ by knowing K^{i-1} or X^i. This means that even if Mallory somehow obtains K^{i-1} or X^i, he still can not obtain any information about K^i. □

5.2.2. Analysis for Case 2

From the security analysis for **Case 1**, it is easy to find that Mallory must obtain both K^{i-1} and X^i to break K^i. However, due to the chain structure of PHYLOCK, the leakage of K^i does not affect other chain keys.

Proposition 2. *If Mallory gets both X^i and K^{i-1}, Mallory can only obtain K^i, but cannot get anything about the previous chain keys $K^{i-2}, K^{i-3} \ldots, i > 2$ and the following chain keys $K^{i+1}, K^{i+2} \ldots, i > 2$.*

Proof.

$$\begin{aligned}
&H(K^{i+1} | X^i K^{i-1} K^i) \\
&= H(K^i \oplus X^{i+1} | X^i K^{i-1} K^i) \\
&= H(K^0 \oplus X^1 \oplus \cdots \oplus X^{i+1} | K^0 \oplus X^1 \oplus \cdots \oplus X^i) \\
&= H(X^{i+1}) = r \; bits
\end{aligned} \tag{25}$$

Similarly,

$$\begin{aligned}
&H(K^{i-2} | X^i K^{i-1} K^i) \\
&= H(K^{i-1} \oplus X^{i-2} | X^i K^{i-1} K^i) \\
&= H(K^{i-1} \oplus X^{i-2} | K^{i-1}) \\
&= H(K^0 \oplus X^1 \oplus \cdots \oplus X^{i-2} | K^0 \oplus X^1 \oplus \cdots \oplus X^{i-1}) \\
&= H(X^{i-2}) = r \; bits
\end{aligned} \tag{26}$$

It can be derived from (25) and (26) that the disclosure of a certain chain key K^i does not affect the security of previous and following chain keys. Every chain key is updated by the corresponding physical layer updated key. Therefore, Mallory needs to know all the channel information state (CSI) to break PHYLOCK. However, it is difficult for Mallory to obtain the same CSI as Alice and Bob. □

5.2.3. Analysis for Case 3

In attack **Case 3**, we assume Mallory obtains all the $K^1, K^2, \ldots, K^i$. This is the worst attack case for PHYLOCK and Mallory attempts to recover K^0. If K^0 can be recovered, then PHYLOCK can be regarded as completely cracked by Mallory.

Proposition 3. *If Mallory gets all $X^1, X^2, \ldots, X^i$ and $K^1, K^2, \ldots, K^i$, he still can not get any information about K^0 because of the initialization phase of PHYLOCK.*

Proof. The entropy of K^0 under **Case 3** is calculated as follows

$$\begin{aligned}
&H(K^0 | K^1 \ldots K^i X^1 \ldots X^i) \\
&= H(K^1 \oplus X^1 \oplus \tilde{X}^m \oplus \tilde{X}^{m-1} \oplus \cdots \oplus \tilde{X}^1 | K^1 \ldots K^i X^1 \ldots X^i) \\
&= H(\tilde{X}^m \oplus \tilde{X}^{m-1} \oplus \cdots \oplus \tilde{X}^1) = r \text{ bits} = H(K^0)
\end{aligned} \tag{27}$$

Mallory can not decrease the entropy of K^0 because the initialization phase masks K^0 well. □

5.2.4. Analysis for Correlated Channel Attack

Spatial decorrelation is essential to the security of physical layer key generation. However, some studies have shown that wireless channels may lose the characteristics of spatial decorrelation when Eve or Mallory is close enough to legitimate nodes or launches a pilot attack [41,42]. Traditional physical layer key generation schemes are vulnerable to correlated channel attacks. Fortunately, the proposed PHYLOCK can resist correlated channel attacks well. We assume Eve or Mallory already know a certain K^i and can generate keys $X_E^{i+j}, j = 1, 2, \ldots, n$ from wireless channels that are highly correlated to the physical layer update keys $X^{i+j}, j = 1, 2, \ldots, n$ in the subsequent. The key bit error probability (BER) [43] P_{AE} between $X_E^{i+j}, j = 1, 2, \ldots, n$ and $X^{i+j}, j = 1, 2, \ldots, n$ can be given according to the correlation coefficient. To simplify the analysis, we directly set the value of P_{AE} and keep unchanged with the iteration of PHYLOCK. After n iterations of PHYLOCK, the BER between K^{i+n} and K_E^{i+n} can be expressed as

$$BER\left(K^{i+n}, K_E^{i+n}\right) = \sum_{k=1,3,\ldots,2\left\lceil \frac{n}{2} \right\rceil - 1} C_n^k P_{AE}^k \cdot (1 - P_{AE})^{n-k} \tag{28}$$

$k = 1, 3, \ldots, 2\left\lceil \frac{n}{2} \right\rceil - 1$ is because the keys at the corresponding locations between K^{i+n} and K_E^{i+n} are inconsistent only when an odd number of key errors occur.

Figure 6 shows the BER between K^{i+n} and K_E^{i+n} versus the iterations of PHYLOCK. As the number of iterations n increases, the BER increases to 0.5 rapidly even if P_{AE} is small due to the strong correlation between the legitimate channel and illegitimate channel. This is because the iterative structure of PHYLOCK makes inconsistent keys constantly accumulate. BER approaches 0.5 after 10 iterations, which means that Eve or Mallory can obtain nothing about K^{i+n} even if the correlated channel attack is still ongoing. For traditional physical layer key generation schemes, they will always be threatened by correlated channel attacks. From the perspective of information theory, the iterative structure of PHYLOCK makes Eve or Mallory's uncertainty about the legitimate channel continue to accumulate.

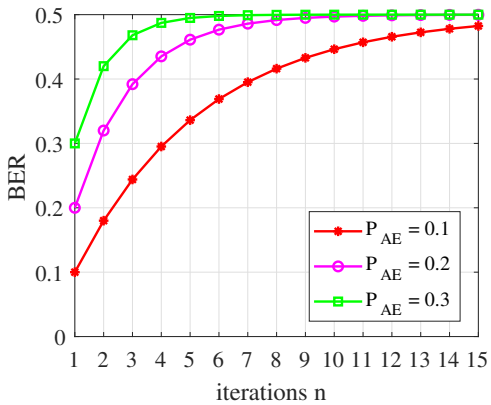

Figure 6. BER between K^{i+n} and K_E^{i+n} versus the iterations of PHYLOCK.

5.3. Definition and Conditions of Unconditional Authentication

The analysis of the above two sections shows that we can generate one-time keys by PHYLOCK that makes unconditional authentication possible. In this section, we give the definition and framework of unconditional authentication in wireless communication and list the conditions for achieving unconditional authentication.

Definition 1. *For a wireless authentication system with appropriate encoding rules $f(\cdot,\cdot)$ and one-time keys generator PHYLOCK, if Mallory has unlimited computing resources and his probability of deception p_0 satisfies $p_0 = 2^{-\frac{1}{2}H(k)}$, then the system achieves unconditional authentication.*

Next, we list the conditions that need to be met to achieve unconditional authentication. Note that realization of unconditional authentication is when equality holds in (12). If equality is to hold in (12), all the inequalities used in proving **Theorem 1** must become equalities. We now review these inequalities to obtain requirements.

We first give three conditions that are most easily stated in the diagram, Figure 3.

(i) Every pair of bundles, from m_1 to c_1 and m_2 to c_2, with $m_1 \neq m_2$, has only one key in common.

(ii) Every bundle contains $2^{\frac{1}{2}H(k)}$ keys.

(iii) There are $2^{\frac{1}{2}H(k)}$ bundles at each m.

To prove (i), (ii), (iii), begin with (13). The equality $H(c'|m,c,m') = H(m',k|m,c,m')$ means that there is only one key k satisfied $c' = f(m',k)$ under the condition (m,c,m'). If for some (m,c,m'), more than one key k satisfied $c' = f(m',k)$, then the conditional entropy about c' is higher. Therefore, we have condition (i) hold.

The equation $p_0 = 2^{-\frac{1}{2}H(k)}$ means that there are $2^{\frac{1}{2}H(k)}$ possibles keys to satisfy $c = f(m,k)$, which proves (ii) every bundle contains $2^{\frac{1}{2}H(k)}$ keys. We can also derive condition (ii) from another perspective. The equality in (9) requires that the keys in any bundle from m to c be distributed equally over $2^U = 2^{\frac{1}{2}H(k)}$ images c' of any m'. Each of these keys leads from m' to a different c'(by (i)). Then, the bundle m to c has $2^{\frac{1}{2}H(k)}$ keys. Now, (iii) follows from (ii) because there are only $2^{H(k)}$ keys. Conditions (ii) and (iii) also guarantee $H(c|m) = \frac{1}{2}H(k)$, which is needed for equality in (17) and (19).

(i) requires a pair of keys $(k_1,k_2), k_1 \neq k_2$ to belong to at most one bundle. The number of pairs having a common bundle in one cluster is $C^2_{2^{\frac{1}{2}H(k)}} * 2^{\frac{1}{2}H(k)}$. The number of clusters is equal to the number of messages M. So the number of pairs of keys having a common bundle is $C^2_{2^{\frac{1}{2}H(k)}} * 2^{\frac{1}{2}H(k)} * M$. This number must be no larger than the unrestricted number of pairs of keys $C^2_{2^{H(k)}}$, thus

$$\begin{aligned} C^2_{2^{\frac{1}{2}H(k)}} * 2^{\frac{1}{2}H(k)} * M &\leq C^2_{2^{H(k)}} \\ M &\leq 2^{\frac{1}{2}H(k)} + 1 \end{aligned} \tag{29}$$

Follows (iii), the length of the code is expressed as $C = M * 2^{\frac{1}{2}H(k)}$.

(iv) The length of the message m is no more than half the length of the key and the length of the code.

From (iv) we know that $p_0 = 2^{-\frac{1}{2}H(k)}$ can only be achieved by severely restricting the length of messages m.

Last but most importantly, the key has to be changed for every piece of the message because only one key fits both $c = f(m,k)$ and $c' = f(m',k')$ [by (i)] and a second message with the same key would disclose the key.

(v) The key needs to be changed through our proposed PHYLOCK key generation architecture for every piece of the message.

In our authentication model, Mallory can always intercept the current message and code. Then, Mallory can search the whole key space according to $c = f(m,k)$ and thus reduce the entropy of the key. According to **Definition 1**, the key entropy is halved by Mallory based on a pair of (m,c). If the key keeps unchanged, then Mallory would disclose the key by a second (m,c). Therefore, we must make (v) hold to achieve unconditional authentication. The strict conditions we listed above imply that unconditional authentication

is impractical, but we can compromise among three conflicting goals: small p_0, small $|K|$, and large $|M|$.

Finally, we give the framework of wireless unconditional authentication in Figure 7. Alice and Bob generate one-time keys through PHYLOCK, the structure of which is depicted in Figure 4. The chain keys K^i generated by PHYLOCK together with the message m generate authentication code c according to the encoding rules. The encoding rules must meet the conditions we discussed above. The data transmission and the procedure of authentication are integrated together.

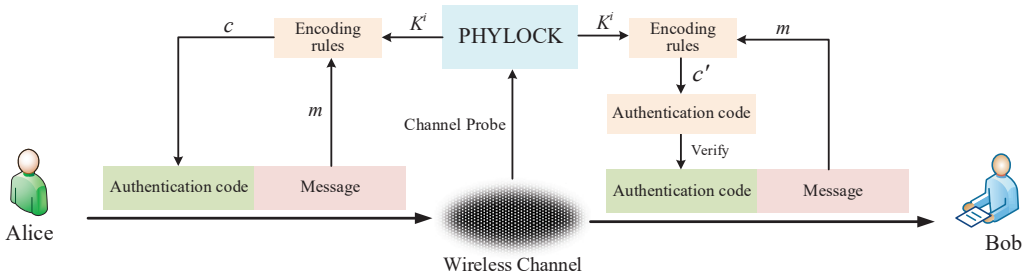

Figure 7. The framework of wireless unconditional authentication.

6. Conclusions

This paper analyzes unconditional authentication based on the physical layer offered chain key (PHYLOCK) in wireless communication. The chain key is generated through a chain structure iteratively. The initial key provides the root of trust and the chain key is updated by the physical layer updated key generated from the wireless channel. We conduct a security analysis of PHYLOCK and proves that it can provide one-time keys for unconditional authentication. Then, we analyze unconditional authentication from the perspective of information theory and the encoding rules that should be followed for unconditional authentication. However, the unconditional authentication framework we proposed is only applicable to wireless communications and the chain key rate depends on the entropy of the wireless channel and further limits the message rate. It can be inferred from the strict requirements of unconditional authentication that our framework is impractical, but provides theoretical guidance. The issue of authentication in the presence of wireless channel noise and channel coding is not addressed in this paper, which is our future research.

Author Contributions: Conceptualization, J.Y. and L.J.; Formal analysis, S.W.; Funding acquisition, K.H.; Investigation, X.H.; Methodology, S.W.; Supervision, K.H.; Writing—original draft, S.W.; Writing—review & editing, X.X. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China, grant number 61871404.

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

References

1. Shakiba-Herfeh, M.; Chorti, A.; Poor, H.V. Physical layer security: Authentication, integrity, and confidentiality. In *Physical Layer Security*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 129–150.
2. Yang, J.; Johansson, T. An overview of cryptographic primitives for possible use in 5G and beyond. *Sci. China Inf. Sci.* **2020**, *63*, 1–22. [CrossRef]
3. Bai, L.; Zhu, L.; Liu, J.; Choi, J.; Zhang, W. Physical layer authentication in wireless communication networks: A survey. *J. Commun. Inf. Netw.* **2020**, *5*, 237–264.
4. Simmons, G.J. Authentication theory/coding theory. In *Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1984; pp. 411–431.
5. Liu, Y.; Boncelet, C. The CRC-NTMAC for noisy message authentication. In Proceedings of the MILCOM 2005-2005 IEEE Military Communications Conference, Atlantic City, NJ, USA, 17–20 October 2005; pp. 2775–2781.

6. Fang, H.; Wang, X.; Hanzo, L. Adaptive trust management for soft authentication and progressive authorization relying on physical layer attributes. *IEEE Trans. Commun.* **2020**, *68*, 2607–2620. [CrossRef]
7. Tsudik, G. Message authentication with one-way hash functions. *ACM SIGCOMM Comput. Commun. Rev.* **1992**, *22*, 29–38. [CrossRef]
8. Dodis, Y.; Kiltz, E.; Pietrzak, K.; Wichs, D. Message authentication, revisited. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 355–374.
9. Xie, N.; Zhang, S.; Liu, A.X. Physical-layer authentication in non-orthogonal multiple access systems. *IEEE/ACM Trans. Netw.* **2020**, *28*, 1144–1157. [CrossRef]
10. Zhang, P.; Shen, Y.; Jiang, X.; Wu, B. Physical layer authentication jointly utilizing channel and phase noise in MIMO systems. *IEEE Trans. Commun.* **2020**, *68*, 2446–2458. [CrossRef]
11. Xiao, L.; Sheng, G.; Wan, X.; Su, W.; Cheng, P. Learning-based PHY-layer authentication for underwater sensor networks. *IEEE Commun. Lett.* **2018**, *23*, 60–63. [CrossRef]
12. Yang, J.; Ji, X.; Huang, K.; Chen, Y.; Xu, X.; Yi, M. Unified and fast handover authentication based on link signatures in 5G SDN-based HetNet. *IET Commun.* **2019**, *13*, 144–152. [CrossRef]
13. Pan, F.; Pang, Z.; Wen, H.; Luvisotto, M.; Xiao, M.; Liao, R.F.; Chen, J. Threshold-free physical layer authentication based on machine learning for industrial wireless CPS. *IEEE Trans. Ind. Inform.* **2019**, *15*, 6481–6491. [CrossRef]
14. Choi, J. A Coding Approach With Key-Channel Randomization for Physical-Layer Authentication. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 175–185. [CrossRef]
15. Xiao, L.; Reznik, A.; Trappe, W.; Ye, C.; Shah, Y.; Greenstein, L.; Mandayam, N. PHY-authentication protocol for spoofing detection in wireless networks. In Proceedings of the 2010 IEEE Global Telecommunications Conference GLOBECOM, Miami, FL, USA, 6–10 December 2010; pp. 1–6.
16. Shan, D.; Zeng, K.; Xiang, W.; Richardson, P.; Dong, Y. PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1817–1827. [CrossRef]
17. Wu, X.; Yang, Z.; Ling, C.; Xia, X.G. Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 6611–6625. [CrossRef]
18. Yu, J.; Hu, A.; Li, G.; Peng, L. A multi-sampling convolutional neural network-based RF fingerprinting approach for low-power devices. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 29 April–2 May 2019; pp. 1–6.
19. Luo, Y.; Hu, H.; Wen, Y.; Tao, D. Transforming device fingerprinting for wireless security via online multitask metric learning. *IEEE Internet Things J.* **2019**, *7*, 208–219. [CrossRef]
20. Ding, L.; Wang, S.; Wang, F.; Zhang, W. Specific emitter identification via convolutional neural networks. *IEEE Commun. Lett.* **2018**, *22*, 2591–2594. [CrossRef]
21. Ramadhani, F.; Ramadhani, U.; Basit, L. Combination of Hybrid Cryptography In One Time Pad (OTP) Algorithm And Keyed-Hash Message Authentication Code (HMAC) In Securing The Whatsapp Communication Application. *J. Comput. Sci. Inf. Technol. Telecommun. Eng.* **2020**, *1*, 31–36. [CrossRef]
22. Saldamli, G.; Ertaul, L.; Shankaralingappa, A. Analysis of lightweight message authentication codes for IoT environments. In Proceedings of the 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), Rome, Italy, 10–13 June 2019; pp. 235–240.
23. Chen, D.; Cheng, N.; Zhang, N.; Zhang, K.; Qin, Z.; Shen, X. Multi-message authentication over noisy channel with polar codes. In Proceedings of the 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Orlando, FL, USA, 22–25 October 2017; pp. 46–54.
24. Chen, D.; Zhang, N.; Cheng, N.; Zhang, K.; Qin, Z.; Shen, X. Physical layer based message authentication with secure channel codes. *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 1079–1093. [CrossRef]
25. Jin, L.; Hu, X.; Sun, X.; Lou, Y.; Huang, K.; Zhong, Z.; Xu, X. Native Security Scheme Based on Physical Layer Chain Key for Encryption and Authentication. In Proceedings of the 2021 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), Nanjing, China, 9–29 March 2021; pp. 1–7. [CrossRef]
26. Ye, H.; Li, G.Y.; Juang, B.H. Power of deep learning for channel estimation and signal detection in OFDM systems. *IEEE Wirel. Commun. Lett.* **2017**, *7*, 114–117. [CrossRef]
27. Ma, W.; Qi, C.; Zhang, Z.; Cheng, J. Sparse channel estimation and hybrid precoding using deep learning for millimeter wave massive MIMO. *IEEE Trans. Commun.* **2020**, *68*, 2838–2849. [CrossRef]
28. Zhang, J.; Rajendran, S.; Sun, Z.; Woods, R.; Hanzo, L. Physical layer security for the Internet of Things: Authentication and key generation. *IEEE Wirel. Commun.* **2019**, *26*, 92–98. [CrossRef]
29. Smith, R.E. A contemporary look at Saltzer and Schroeder's 1975 design principles. *IEEE Secur. Priv.* **2012**, *10*, 20–25. [CrossRef]
30. Gilbert, E.N.; MacWilliams, F.J.; Sloane, N.J. Codes which detect deception. *Bell Syst. Tech. J.* **1974**, *53*, 405–424. [CrossRef]
31. Gorbenko, I.; Kuznetsov, A.; Lutsenko, M.; Ivanenko, D. The research of modern stream ciphers. In Proceedings of the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, Ukraine, 10–13 October 2017; pp. 207–210.
32. Manifavas, C.; Hatzivasilis, G.; Fysarakis, K.; Papaefstathiou, Y. A survey of lightweight stream ciphers for embedded systems. *Secur. Commun. Netw.* **2016**, *9*, 1226–1246. [CrossRef]

33. Courtois, N.T.; Meier, W. Algebraic attacks on stream ciphers with linear feedback. In *International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 345–359.
34. Lano, J.; Mentens, N.; Preneel, B.; Verbauwhede, I. Power analysis of synchronous stream ciphers with resynchronization mechanism. *Int. J. Intell. Inf. Technol. Appl.* **2008**, *1*, 327–333.
35. Zeng, K. Physical layer key generation in wireless networks: Challenges and opportunities. *IEEE Commun. Mag.* **2015**, *53*, 33–39. [CrossRef]
36. Jiao, L.; Wang, N.; Wang, P.; Alipour-Fanid, A.; Tang, J.; Zeng, K. Physical layer key generation in 5G wireless networks. *IEEE Wirel. Commun.* **2019**, *26*, 48–54. [CrossRef]
37. Aldaghri, N.; Mahdavifar, H. Physical layer secret key generation in static environments. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2692–2705. [CrossRef]
38. 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.
39. Li, G.; Hu, A.; Zhang, J.; Peng, L.; Sun, C.; Cao, D. High-agreement uncorrelated secret key generation based on principal component analysis preprocessing. *IEEE Trans. Commun.* **2018**, *66*, 3022–3034. [CrossRef]
40. Ji, Z.; Yeoh, P.L.; Zhang, D.; Chen, G.; Zhang, Y.; He, Z.; Yin, H.; Li, Y. Secret key generation for intelligent reflecting surface assisted wireless communication networks. *IEEE Trans. Veh. Technol.* **2020**, *70*, 1030–1034. [CrossRef]
41. Huang, K.W.; Wang, H.M. Intelligent reflecting surface aided pilot contamination attack and its countermeasure. *IEEE Trans. Wirel. Commun.* **2020**, *20*, 345–359. [CrossRef]
42. Xu, W.; Yuan, C.; Xu, S.; Ngo, H.Q.; Xiang, W. On pilot spoofing attack in massive MIMO systems: Detection and countermeasure. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 1396–1409. [CrossRef]
43. Hu, X.; Jin, L.; Huang, K.; Ma, K.; Xiao, S. A Secure Communication Scheme Based on Equivalent Interference Channel Assisted by Physical Layer Secret Keys. *Secur. Commun. Netw.* **2020**, *2020*, 1–15. [CrossRef]