The Study of Low-Level Authentication Mechanism Based on Physical Layer Characteristics

1st Kai Chen
China Telecom Stocks Co.,Ltd.
CT
Guangdong, China
chenk3.gd@chinatelecom.cn

2nd Longru Chen
China Telecom Stocks Co.,Ltd.
CT
Guangdong, China
chenlr5.gd@chinatelecom.cn

3rd Jianxian Lu
China Telecom Stocks Co.,Ltd.
CT
Guangdong, China
lujx5.gd@chinatelecom.cn

4th Gaoyuan Dai*
South China University Of Technology, China Telecom Stocks Co.,Ltd.
SCUT, CT
Guangdong, China
daigy.gd@chinatelecom.cn

5th Zhe Wang
China Telecom Stocks Co.,Ltd.
CT
Guangdong, China
wangz.gd@chinatelecom.cn

6th Liyang Yu
Beijing University of Posts and Telecommunications
BUPT
Beijing, China
yuliyang111@bupt.edu.cn

Abstract—**The advent of 5G networks brings about a monumental transformation. It is characterized by significantly larger bandwidth, lower latency transmission, and diverse connectivity of multi-type terminal devices. This paradigm shift in mobile communication technology introduces new challenges in network security. This paper introduces an authentication mechanism based on the physical layer attributes, leveraging Physical Unclonable Functions (PUFs) to address authentication and privacy protection for resource-constrained devices. The application of physical layer security techniques involves embedding authentication information within wireless communication signals. This augmentation enhances system security. However, challenges, including integration with novel transmission technologies, implementing secure transmission mechanisms across diverse network scenarios, and addressing emerging security threats, must be overcome. PUFs, known for their persistence, unclonability, and tamper-evident properties, have versatile applications across various domains. This study emphasizes the requirements of PUFs in 5G networks. It encompasses research areas such as secure key generation based on PUFs and key negotiation mechanisms rooted in wireless channel characteristics. These efforts aim to address specific scenarios and emerging security threats.**

Keywords-5 G; Physically Unclonable Functions; physical layer security

I. Introduction

With the rapid advancement of mobile communication technology, future mobile communication networks are poised for a monumental transformation in aspects such as network architecture, flexible connectivity, bandwidth, latency, and synchronization. As transmission bandwidth expands and latency diminishes, mobile terminal devices will exhibit characteristics of extensive connectivity and diverse types. Various network types will coexist, rendering network configurations more heterogeneous and diverse, while blurring the boundaries of security. Consequently, this will lead to an escalation in various forms of malicious attacks at both the mobile communication terminal and network layers, posing graver security challenges to the development of mobile communication.

Ensuring the security of mobile communication has always been a matter of great concern for users, enterprises, and nations. Enhancing the security of future mobile communication has risen to become a strategic requirement for various countries. Due to the open nature of wireless channels, air interface security forms the foundation of mobile communication security. The air interface security, also known as access domain security, primarily provides secure user access to services offered by the mobile communication system. It aims to prevent attacks on the wireless channel, such as eavesdropping on the wireless channel, physical layer signal attacks, random access Denial-of-Service (DOS) attacks, and flooding attacks in authentication protocols, among others. Generally speaking, air interface security needs to achieve the following objectives: 1) Authentication between users and the network; 2) Security of user data and signaling data transmitted over the wireless channel (confidentiality and integrity); 3) Confidentiality protection of user identity; 4) Confidentiality protection of user location; 5) Prevention of user tracking, and so forth.

To address the aforementioned issues and tackle the novel security threats [1] arising from the intricate wireless environments of the future, this paper proposes a foundational authentication mechanism based on the physical layer attributes. It employs Physical Unclonable Functions (PUFs) [2] to perform computations on the underlying hardware characteristic parameters, thereby resolving authentication and privacy protection concerns for resource-constrained devices.

II. Analysis of the Current Research Status

To ensure the security of the air interface in mobile communications, both the academic and industrial sectors have conducted extensive research and practical endeavors. As mentioned above, some research outcomes have already been adopted by mobile communication standards. A prevalent perspective in the study of communication systems is that the physical layer is primarily responsible for information transmission, while encryption, authentication, and other security mechanisms are executed by higher layers such as the data link, network, or application layers. These security protocols have become increasingly intricate. Despite the enhanced security offered by these schemes, they are often challenging to implement in practical scenarios, particularly in wireless communication systems like RFID. Leveraging certain attributes of the physical layer to delegate partial security functions to it can simplify these complex security protocols.

A. Air-port Security Mechanism Based on Physical Properties

Physical Layer Security [3][4][5] (PLS) leverages the diversity and time-variant nature of wireless channels, as well as the uniqueness and reciprocity of channels between legitimate communication parties. It explores intrinsic security mechanisms within wireless communication by capitalizing on the characteristics of signal propagation at the physical layer. A pivotal research focus within the realm of physical layer security is the development of physical layer authentication techniques [6].

Physical layer authentication technology primarily involves embedding identity authentication information into the wireless communication signals at the physical layer, thereby affecting identity verification within the physical layer. This technology operates transparently to upper-layer protocols, reducing the overhead of such protocols. Moreover, it mitigates identity authentication attacks directed at upper-layer protocols, thereby enhancing system security.

In the field of physical layer key generation technology, the primary focus is on methods where legitimate users at the transmitting and receiving ends can generate communication keys based on observations of the transmission link. This approach ensures that legitimate parties in communication can dynamically generate keys through the inherent randomness of the wireless channel, obviating the need for a central node for key distribution. Simultaneously, as long as the eavesdropper remains beyond the secure distance of the legitimate transmitting and receiving ends, they cannot access the channel characteristics associated with the legitimate link, thereby preventing them from obtaining the key.

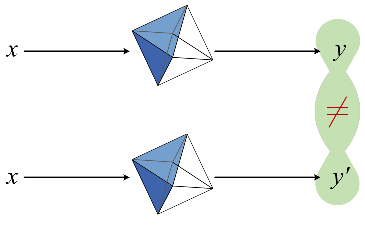


Figure 1. Example of a ONE-COLUMN figure caption.

The field of physical layer security has witnessed substantial progress over many years, yielding profound insights and effective methodologies for physical layer security technology. Nevertheless, the research in physical layer security is far from exhaustive. Particularly, with the rapid advancement of 5G wireless communication and networking technologies in recent years, wireless security confronts numerous pressing challenges, presenting new frontiers for traditional physical layer security techniques. These challenges manifest in several key aspects:

The collaborative investigation of physical layer security technology with novel transmission techniques. The emergence of 5G has introduced various new wireless transmission technologies, such as Massive Multiple Input and Multiple Output (MaMIMO), Millimeter Wave (mmWave) communication, Non-Orthogonal Multiple Access (NOMA), and Full-Duplex communication. While these technologies provide robust support for high-speed, large-scale, and low-latency wireless services in 5G, they do not inherently safeguard the secure transmission of information. Consequently, there is a need to synergize these technologies with physical layer security techniques to ensure information security while maintaining high-quality user services.

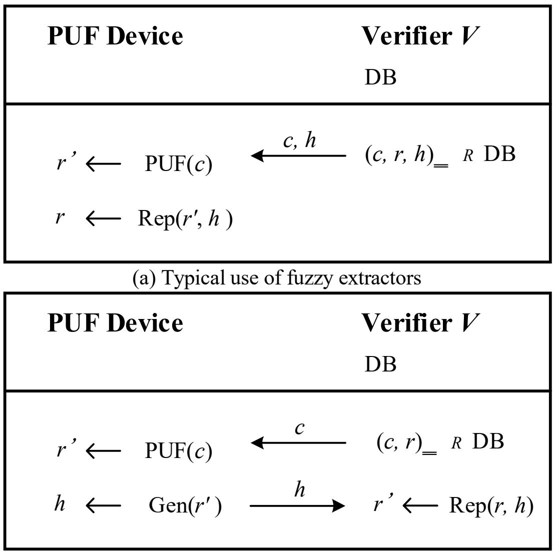
Security transmission mechanisms in novel wireless network scenarios. The development of 5G has given rise to diverse new wireless scenarios. Examples include the three defined by 5G: Enhanced Mobile Broadband Communication, Massive Machine-Type Communication, and Ultra-Reliable Low-Latency Communication. Additionally, specific network scenarios like Ad Hoc networks, heterogeneous networks, and vehicular networks have emerged. Different user requirements and wireless services characterize these distinct scenarios. As such, research on physical layer security technology must design corresponding security strategies tailored to the unique demands and business attributes of each scenario.

Physical layer security techniques addressing new security threats. The proliferation of diverse wireless technologies accompanying the advent of 5G, while enhancing the performance of legitimate users, also opens avenues for malicious users to exploit, potentially leading to more severe security threats. Consequently, physical layer security technology must be poised to counter potential new security threats, thereby establishing dependable security defenses.

B. Studies Based on Physically Unclonable Functions

The concept of Physical Unclonable Function (PUF) was first introduced by Pappu from MIT in 2001 [7]. In simple terms, it is a random function computed from underlying hardware characteristics, as illustrated in Fig. 1 [8]. The cubic structure in the middle is regarded as the PUF function, where x and y represent the input and output of the PUF. x can also be considered as a stimulus. By utilizing the inevitable random differences in the inherent physical structure of the PUF, an unpredictable response y is generated.

The work of Gassend et al. during the period of 2002-2005 [9][10] demonstrated that PUF cannot be accurately replicated simply, nor can it be predicted or duplicated. Even when using the same hardware, there exist variations in the manufacturing process and associated delays, making it impossible to produce a functionally identical result as the first implementation. For example, as shown in Figure 1, even with the same hardware and input x, the resulting y' is unlikely to be identical to y. Additionally, PUF can be implemented through specialized customization, requiring fewer gate circuits compared to traditional encryption functions. In 2012, Nithyanand provided a description of PUF attributes [11], as follows:



(a) Typical use of fuzzy extractors

(b) The Concept of Reverse Fuzzy Extractor

Figure 2. Two applications of fuzzy extractors.

1) Persistence and Unpredictability: The response (Ri) to certain stimuli or challenges (Ci) is random and unpredictable. However, over extended observations, the response to the same challenge remains consistent.

2) Unclonable: Without a genuine PUF, obtaining the corresponding Ri for a specific Ci is infeasible. In other words, given a PUF, an attacker cannot construct another PUF' that produces identical responses to each challenge as the original PUF.

3) Tamper Evident: Attempting to tamper with the behavior of the PUF will alter its stimulus-response behavior, making it easily detectable.

These characteristics of PUF align precisely with the properties required for cryptographic primitives in secure protocol design. Consequently, PUF is employed in various domains including Intellectual Property (IP) protection for integrated circuits [12][13][14], device authentication [15][16][17][18], key generation [19][20][21], trusted computing [22], and digital rights protection [23] [24].

III. Research on Secure Key Generation Algorithm Based on Physically Unclonable Functions

Traditional security solutions relying on cryptographic algorithms require a physical entity to execute the encryption algorithm and store the key. Common physical entities include encryption cards and smart cards. Fundamentally, the traditional approach involves storing a secure key in non-volatile storage units (such as EEPROM) to enable the use of cryptographic primitives (such as digital signatures and encryption) for safeguarding sensitive information. However, this method exhibits numerous evident flaws. For instance, recently proposed non-invasive and invasive physical tampering techniques (e.g., microwave probing attacks and side-channel attacks) can allow attackers to obtain the digital key stored in non-volatile storage units, rendering the security mechanisms associated with cryptographic algorithms ineffective.

With the introduction and in-depth research of PUFs, researchers have proposed that PUFs can serve as cryptographic primitives for generating secure volatile keys. Firstly, since the randomness in PUFs is permanently embedded in the subtle physical structure of the chip, the traditional non-volatile storage step is unnecessary. PUFs can derive a secure key within a specified time frame and erase it after use, eliminating the need for permanent digital storage. This restricts the time frame for extracting the key from the device, making PUFs resilient against probing attacks and other potential side-channel attacks. Secondly, a key generated by a PUF is intimately tied to the physical hardware embedding the PUF, endowing the entire hardware with physical unclonability. Furthermore, due to the randomness of the digital circuit for key generation caused by inevitable manufacturing variations, explicit key programming steps are unnecessary, simplifying key distribution. Finally, the tamper-evident property of PUFs can be utilized to provide tamper-evident key storage.

Among the currently published lightweight security protocols, the predominant employment of cryptographic assumptions still revolves around traditional cryptographic assumptions. Due to the impractical resource requirements, in terms of storage and computational power, of implementing traditional cryptographic algorithms in low-cost tags, there is a pressing need for new cryptographic assumptions. Combining the latest mathematical models of Physical Unclonable Functions (PUFs) and drawing inspiration from current approaches advocating enhanced PUF security through the addition of logical control functionalities, the search for novel cryptographic assumptions based on PUF is underway. These assumptions serve as the foundational elements for constructing secure systems based on PUFs.

When utilizing PUFs for key generation, the PUF's response values need to be reliable and reproducible, while also exhibiting unpredictability. However, because of the inherent noise in PUFs and the fact that response values are not uniformly random, existing solutions often incorporate a Fuzzy Extractor to achieve this. The role of a Fuzzy Extractor is to obtain a consistent output from two slightly differing input data sets, and the output data exhibits a well-distributed uniformity. A typical Fuzzy Extractor comprises two stages: the Generation phase denoted as Gen, where h = Gen(r), and the Regeneration phase denoted as Rep, where r = Rep(r' ,h). Two applications of a Fuzzy Extractor are illustrated in Fig. 2.

IV. Key Negotiation Mechanism Based on Wireless Channel Characteristics

Addressing the diversity and time variability of the wireless channel, as well as the uniqueness and reciprocity of the legitimate communication channels, this research explores intrinsic security mechanisms in wireless communication starting from the characteristics of wireless signal propagation. The technological evolution of the new air interface of 5G creates favorable conditions for fundamentally resolving the risk of signal leakage brought about by open wireless transmission. The employment of technologies such as Massive MIMO, high-frequency bands, and large bandwidth in 5G enriches the intrinsic security elements contained in wireless resources, making their extraction more convenient and facilitating the realization of physical layer security. This paves the way for new approaches in physical layer security. Additionally, these security mechanisms naturally coexist with communication processes and signal processing technologies, enabling synchronized evolution and integrated development with 5G's new air interface technologies.

In the research on physical layer key generation technology, private channel characteristics of both communicating parties are utilized to extract the "fingerprint" of the wireless channel. This provides a means for the real-time generation of rapidly updated keys without the need for distribution. The characteristics of wireless propagation can serve as a public information source for secure key agreement protocols. Due to the unpredictable signal attenuation and electromagnetic wave interactions, the wireless channel between two legitimate users represents a common source of randomness. This randomness can be used to independently generate a key, which is then agreed upon through public discussion. Specific research areas include 1) Random information sharing (e.g., probing communication channels); 2) Optimizing channel selection; 3) Information reconciliation, correcting mismatches due to asymmetric channels, noise, interference, and temporarily distant half-duplex communication; and 4) Privacy removal, preprocessing public sequences containing private data to reduce information leakage on public channels, thereby generating secure keys.

The following are the basic operational methods for the research on key negotiation mechanisms based on wireless channel characteristics.

Firstly, confirm the wireless channel characteristic parameters, i.e., which channels can be used for key generation. Known channel characteristic parameters include small-scale fading channel characteristics, such as CSI and RSS. It is essential to ensure that these features are shared random information between the communicating nodes.

Secondly, select dominant features. As we are researching air interface security, in an open wireless environment, attackers are likely to have the capability to eavesdrop on wireless channel characteristics. Therefore, identifying a feature that provides a legitimate user with an advantage over an eavesdropper prevents malicious acquisition of communication keys.

Next, reconcile public features. Some features on the wireless channel can be considered static, while many features are dynamically changing, influenced by noise and time. Although keys negotiated between nodes should change with variations in the wireless channel, this change should not occur too frequently. When certain feature parameters in the channel undergo small changes, the negotiated key should remain unchanged. Hence, we need to determine how to reconcile some public features to ensure that the results are consistent when changes occur within defined feature variations.

Finally, conduct research on key generation algorithms. After confirming multiple wireless channel characteristics and reconciliation schemes, this project will establish a key generation algorithm. This algorithm should ensure the removal of information about these characteristics themselves (to prevent privacy leakage). A simple approach is to directly perform key generation through a hash function. However, to ensure that the keys generated by both communicating parties are identical, the reconciliation scheme must be incorporated into the key generation algorithm.

V. Conclusion

The underlying authentication mechanism based on physical layer characteristics and Physical Unclonable Function (PUF) technology demonstrates significant prospects and application potential in the 5G environment. With the rapid development of mobile communication technology, future mobile communication networks will undergo substantial changes, encompassing various requirements such as network architecture, flexible connectivity, bandwidth, and latency. This leads to a sharp increase in the scale of connected terminal devices, resulting in a more heterogeneous and diversified network topology, while blurring the boundaries of security perimeter.

References

[1] Yadav A, Kumar S, Singh J. A review of physical unclonable functions (pufs) and its applications in iot environment[J]. Ambient Communications and Computer Systems: Proceedings of RACCCS 2021, 2022: 1-13.

[2] Anandakumar N N, Hashmi M S, Tehranipoor M. FPGA-based Physical Unclonable Functions: A comprehensive overview of theory and architectures[J]. Integration, 2021, 81: 175-194.

[3] Al-Meer A, Al-Kuwari S. Physical unclonable functions (PUF) for IoT devices[J]. ACM Computing Surveys, 2023, 55(14s): 1-31.

[4] Vijay V, Chaitanya K, Pittala C S, et al. Physically unclonable functions using two-level finite state machine[J]. Journal of VLSI circuits and systems, 2022, 4(01): 33-41.

[5] Gao B, Lin B, Pang Y, et al. Concealable physically unclonable function chip with a memristor array[J]. Science advances, 2022, 8(24): eabn7753.

[6] Gebali F, Mamun M. Review of physically unclonable functions (pufs): structures, models, and algorithms[J]. Frontiers in Sensors, 2022, 2: 751748.

[7] Pappu R, Recht B, Taylor J, et al. Physical one-way functions[J]. Science, 2002, 297(5589): 2026-2030.

[8] Dachman-Soled D, Fleischhacker N, Katz J, et al. Feasibility and Infeasibility of Secure Computation with Malicious PUFs[M]//Advances in Cryptology–CRYPTO 2014. Springer Berlin Heidelberg, 2014: 405-420.

[9] Gassend B, Clarke D, Van Dijk M, et al. Controlled physical random functions[C]. Computer Security Applications Conference, 2002. Proceedings. 18th Annual. IEEE, 2002: 149-160.

[10] Lim D, Lee J W, Gassend B, et al. Extracting secret keys from integrated circuits[J]. Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, 2005, 13(10): 1200-1205.

[11] Nithyanand R, Solis J. A theoretical analysis: Physical unclonable functions and the software protection problem[C]. Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012: 1-11.

[12] Guajardo J, Kumar S S, Schrijen G, Tuyls P. FPGA intrinsic PUFs and their use for IP protection. In Proc. the 9th International

Workshop on Cryptographic Hardware and Embedded Systems, Sept. 2007:63-80.

[13] Zhang J, Wu Q, Lyu Y, et al. Design and implementation of a delay-based PUF for FPGA IP protection[C]. Computer-Aided Design and Computer Graphics (CAD/Graphics), 2013 International Conference on. IEEE, 2013: 107-114.

[14] Guajardo J, Kumar S S, Schrijen G J, et al. Brand and IP protection with physical unclonable functions[C]. Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on. IEEE, 2008: 3186-3189.

[15] Puntin D, Stanzione S, Iannaccone G. CMOS unclonable system for secure authentication based on device variability[C]. Solid-State Circuits Conference, 2008. ESSCIRC 2008. 34th European. IEEE, 2008: 130-133.

[16] Suh G E, Devadas S. Physical unclonable functions for device authentication and secret key generation[C]. Proceedings of the 44th annual Design Automation Conference. ACM, 2007: 9-14.

[17] Majzoobi M, Rostami M, Koushanfar F, et al. Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching[C]. Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012: 33-44.

[18] Majzoobi M, Koushanfar F. Time-bounded authentication of FPGAs[J]. Information Forensics and Security, IEEE Transactions on, 2011, 6(3): 1123-1135.

[19] Lim D, Lee J W, Gassend B, et al. Extracting secret keys from integrated circuits[J]. Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, 2005, 13(10): 1200-1205.

[20] Suh G E, Devadas S. Physical unclonable functions for device authentication and secret key generation[C]. Proceedings of the 44th annual Design Automation Conference. ACM, 2007: 9-14.

[21] Maes R, Van Herrewege A, Verbauwhede I. Pufky: A fully functional puf-based cryptographic key generator[M]. Cryptographic Hardware and Embedded Systems–CHES 2012. Springer Berlin Heidelberg, 2012: 302-319.

[22] Suh G E, O'Donnell C W, Devadas S. Aegis: A single-chip secure processor[J]. Design & Test of Computers, IEEE, 2007, 24(6): 570-580.

[23] Alkabani Y, Koushanfar F. Active control and digital rights management of integrated circuit IP cores[C]. Proceedings of the 2008 international conference on Compilers, architectures and synthesis for embedded systems. ACM, 2008: 227-234.

[24] Koushanfar F. Provably secure active IC metering techniques for piracy avoidance and digital rights management[J]. Information Forensics and Security, IEEE Transactions on, 2012, 7(1): 51-63.