FIDO Protocol Based on Physical Unclonable Functions and Its Application into Electronic Contract

Rui Xu\(^1\), Kun Liu\(^1\), Hua-Fei Yang\(^1\), Yue Fang\(^3\), Jia You\(^1,2\) and Feng Ma\(^1,2\)

\(^1\)NARI Group Corporation (State Grid Electric Power Research Institute), 211106 Nanjing, China; \(^2\)NARI Information Communication Science and Technology Co. Ltd., 210003 Nanjing, China; \(^3\)College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, 211106 Nanjing, China

Abstract. In this paper, the emerging Physical Unclonable Function (PUF) and Fast Identity Online (FIDO), are studied for the secure identification (ID) authentication of electronic contract. To solve the unstable response of PUF, error correction algorithms are applied. This paper proposes a high security authentication protocol, which is a FIDO protocol based on PUF. A comparison of the proposed protocol with three classical protocols is presented. The results shows that the proposed protocol has the advantages of anti-cloning and error-correcting compared with existing authentication protocols. Finally, the application of the FIDO protocol based on PUF into the electronic contract is also demonstrated.

1. Introduction

Electronic contracts are becoming popular as the trade can be done in a fast way [1-2]. However, there are several security issues that should be solved before deployment. One of the major issues is how to authenticate the online identification of the genuine trading party. The current authentication technologies generally use password and USB Key which cannot prevent cloning and key attack.

One of effective techniques to protect online ID is FIDO. FIDO [4] is an open standard protocol initiated by FIDO alliance which integrates biometric and asymmetric encryption technologies to ensure the security of user authentication.

Due to security, adaptability and privacy protection, combined with increasingly mature biometrics technology [10], FIDO may replace the traditional static/dynamic password verification method. FIDO has been supported by over 250 companies, including Google, Lenovo, Intel, PayPal and other major companies.

Recent years, Lenovo released the world's first PC with built-in support for FIDO certification standards [4]. Intel's 7th and 8th generation Core processors integrate FIDO protocols, allowing consumers to choose PayPal, Dropbox, Google, Facebook, etc. by fingerprint or two-factor authentication.

However, previous FIDO protocols are not unclonable on the physical level similar as most of conventional authentication. PUF is a special security primitive embedded in a physical object, which extracts random differences in the physical object and produces its unique response [5]. The key features of PUF are unclonable and low cost. Therefore, this paper proposes a FIDO protocol based on PUF and used for electronic contract as a FIDO device. Protocol framework and performance analysis
are presented in this paper. The results show that the proposed protocol has the advantages of anti-cloning and error-correcting compared with existing protocols.

The paper is organized as follows: Section 2 reviews FIDO and PUF in this work, including error correction scheme and classic PUF protocol. In Section 3, FIDO protocol based on PUF are proposed with performance analysis. In Section 4, a practical electronic contract application is presented. Finally, a conclusion is drawn in Section 5.

2. Background

2.1. FIDO
FIDO is a kind of multi-factor authentication technique [3], which combines several single-factor methods with higher security. FIDO protocols have two types: U2F (Universal 2nd Factor Protocol) and UAF (Universal Authentication Framework Protocol).

For the UAF protocol, all biometric data and private keys of the user are stored in the memory of the device and do not need to be transmitted to the server by the network. What the server needs to do is storing the user’s public key to complete the authentication process, which can reduce the risk of stolen authentication information.

U2F is proposed on the basis of compatibility with existing cryptographic authentication systems. Users are required to provide a U2F-compliant authentication device as a second authentication factor to ensure that the operation is secure enough for on-line operations requiring high security.

2.2. PUF
PUF [5] is a new concept in the field of hardware security, which has the characteristics of uniqueness and non-clonability. PUF is a security primitive usually embedded in an integrated circuit, which extracts random differences in the physical object and produces its unique response. According to the number of challenge and response pairs (CRPs), it can be divided into strong PUF and weak PUF [5-6], which are applied to low-cost authentication and security key generation. According to the circuit structure, it can be also divided into delay-based PUF and memory-based PUF [6].

Both weak and strong PUFs are used in the protocol proposed in this work. Since the response of weak PUF is vulnerable to the environment, it is necessary to use error correction method to eliminate these effects and generate stable keys.

The fuzzy extractor is an important concept of PUF error correction. The function of the fuzzy extractor is to correct the error of each extraction and restore it to the same value as when it was registered [7]. The fuzzy extractor of SRAM PUF mainly consists of two parts: the encoding phase and the decoding phase, as shown in Figure 1. The encoding phase uses the BCH coding [5] module with low complexity. In the encoding phase, the initial data $r$ generated by the weak PUF and challenge care input to the fuzzy extractor; the BCH encodes the data to generate help data $e$. In the decoding phase, the noisy data $r'$ and the help data $e$ are passed as input data to the extractor and performs a BCH decoding process, desirably restoring the data.

![Figure 1. Fuzzy extractor [7].](image-url)
2.3. Classic PUF Protocol

The conventional PUF protocol is implemented using only one unprotected strong PUF [8], as shown in Figure 2. The server collects CRPs during the registration phase and adds them to the database. During the verification process, the authentication device randomly selects challenge from the database and send it to the device to be authenticated. Then, the device generates a corresponding response according to the input signal and feeds back to the authentication device, and the authentication device compares the received response with the response in the database. The authentication successes if the response is the same. Considering strong PUFs are usually vulnerable to modeling attacks, combining PUF with other authentication technologies such as FIDO can improve system security.

![Figure 2. Classic PUF authentication protocol](image)

3. The proposed FIDO Protocol Based on PUF

3.1. A Framework Combing PUF and FIDO

The whole framework of combination of PUF and FIDO authentication include two process: the registration process and the identification process. The registration process is shown in Figure 3. The PUF registration process is as follows: the user opens the Uniform Resource Locator (URL), and the server returns the login form according to the https protocol; the user inputs the password and submits it to the server, and if the verification password is correct, the UAF registration request is triggered to the FIDO server. After that, the FIDO server generates a registration request and a random number, controls the weak PUF to generate authentication IDs, and sends the request, the random number together with the ID to the client in the form of an incentive. The FIDO client receives the signal to trigger the registration, verifies the user information, and then sends the data to the authenticator with the strong PUF. Finally, the generated registration response is sent to the FIDO server, and if the verification is successful, the registration process is completed.

![Figure 3. UAF authentication registration process based on PUF](image)

Figure 4 demonstrates the process of identification process. The FIDO server sends an authentication request message to the FIDO client, and the client transmits the message to the authenticator. The incentive information in the message generates a response message through the strong PUF; the FIDO server sends the response message to the FIDO server, and the server receives the message. Passed to the database where the registration information is stored for checksum comparison.
3.2. The formal improved FIDO protocol

After using the error correction scheme, an abstract description based on the PUF identity authentication protocol is shown in Fig. 5.

**Initialization**

\[ r_0 = \text{Hash}([\text{SPUF}(c_0)]) \]
\[ p_0 = \text{Gen}([\text{SPUF}(c_0)]) \]

**Verification**

\[ x \neq 0 \Rightarrow \text{WPUF}() \]
\[ r'_j = \text{Hash}(\text{Rep}([\text{SPUF}(c_j), p_j])) = c_j, c_k, p_j, p_k \]
\[ r'_k = \text{Hash}(\text{Rep}([\text{SPUF}(c_k), p_k])) \]
\[ \text{Judge } r'_j \oplus r'_k = x \]

Figure 4. UAF authentication identity process based on PUF

Figure 5. The proposed authentication protocol based on PUF

The protocol includes initialization and verification. Gen and Rep represent the generation and reproduction in the error correction process. Hash represents the process that converts a length of input into a fixed-length output through a hashing algorithm.

In the initialization, responses are generated by a random number generator. The generated responses are processed by a hash function and a code offset, respectively.

The verification first generates key \( x \) from the weak PUF. \( x \) is the result of two responses XOR. Restrictions \( x \neq 0 \) prevent an attacker from impersonating a server, selecting \( c_j = c_k \) and \( p_j = p_k \) to pass authentication. In order to avoid interference from replay attacks, the use of pseudorandom number generators that require secure non-volatile memory should be avoided, which would result in the advantages of PUF not being exhibited. Then look for \( r_j \) and \( r_k \) in the generated \( r_0 \), than make \( x \) equals the XOR of \( r_j \) and \( r_k \). Select \( p_j \) and \( p_k \) from \( p_0 \), select \( c_k \) and \( c_j \) from \( c_0 \) and send \( c_j, c_k, p_j, p_k \) to the client. Using the response \( c_j, c_k \) of the strong PUF summation and combining \( p_j, p_k \). Then the error-corrected result is processed using a hash function to obtain the final response \( r'_j, r'_k \). Finally, the result of the XOR of \( r'_j \) and \( r'_k \) is calculated, and judged whether it is equal to \( x \).

3.3. Performance Analysis

**Key Attack.** Due to the unclonability of the PUF, it is difficult for an attacker to obtain a key. The key generation depends on the weak PUF, which does not need to be separately configured with non-volatile memory and save hardware resources.

**Equipment Cloning.** The use of iris identification [11] or fingerprint identification [12] in the FIDO framework and PUF constitutes a multiple factor authentication approach, which means that even if the trusted hardware is lost, the attacker cannot steal security information or falsify the protocol. For
the very effective model attacking for Arbiter PUF, the FIDO protocol based on PUF uses hash function and XOR processing to confuse the CRPs, the attacker cannot directly use a certain number of CRPs to model, so the security of the system is obtained.

**Comparison of Authentication Protocols.** Table 1 compares the performance of basic PUF protocol, Controlled PUF protocol, FIDO and the protocol proposed in this paper. It can be seen from the table that the Basic PUF protocol and the Controlled PUF protocol respectively embed strong PUF and weak PUF to have anti-cloning characteristics, but neither of them has the function of error correction and the anti-noise ability is not so good. The FIDO protocol is difficult to be counterfeited due to the integration of one or more biometric technologies, but it lacks error correction modules and no PUF built-in. The proposed protocol combines the advantages of the basic PUF protocol and the FIDO protocol. At the same time, the application of strong PUF and weak PUF improves the security of the system, while the fuzzy extractor guarantees the robustness of the input data.

| Anti-cloning | Error-correction | Weak PUF | Strong PUF |
|--------------|------------------|----------|------------|
| Basic [9]    | ×                | ×        | ×          |
| Controlled [8]| ×                | √        | ×          |
| FIDO         |                  |          |            |
| This paper   |                  |          | √          |

**4. Electronic Contract Application**
The proposed FIDO protocol based on PUF has high security against attackers, which can be applied in electronic contract application. The device integrated the proposed protocol is part of the authentication system. When the device is inserted into the computer, the certification begins formally.

![Second Factor Authentication](image)

**Figure 6.** Identity factor authentication

The application can be performed as follows. The user logs in to the service platform for the first time. As shown in Figure 6, the user authenticates with the password and then sends a registration request to the FIDO server. The FIDO server interacts with the authentication to generate keys. The root key information is generated by the PUF protocol and the encrypted key is generated by using the related key algorithm to improve the security of the platform. The user logs in to the electronic subscription service platform and needs to complete the authentication through the protocol. A key handle is calculated by an encryption algorithm to obtain a signature key.

**5. Conclusion**
Electronic contract has become popular. However, one of the major issues is how to authentic the genius trading party. In this paper, PUF and FIDO are studied for secure ID authentication. We
proposed a FIDO protocol based on PUF and compared it with conventional protocols. The result shows that security scheme implemented by FIDO protocol based on physical unclonable functions improves the security of identity authentication. Electronic contract application is also provided to show the effectiveness of the proposed FIDO protocol based on PUF.

6. Acknowledgments
This work has been supported by grants from State Grid Corporation Science and Technology Project Funded "Key Technology Research on Trustworthy Identity Authentication of Grid Core Business" (52110418001L).

7. References
[1] P. R. Krishna and K. Karlapalem, Electronic Contracts, IEEE Internet Computing, vol. 12, no. 4, pp. 60-68, July-Aug, (2008).
[2] X. Yu, Y. Chai and Y. Liu, A Secure Model for Electronic Contract Enactment, Monitoring and Management, Second International Symposium on Electronic Commerce and Security, Nanchang, pp. 296-300, (2009).
[3] Bhargav-Spantzel A, Squicciarini A, Bertino E. Privacy preserving multi-factor authentication with biometrics. The Workshop on Digital Identity Management. DBLP. 63-72, (2006).
[4] K. Hu and Z. Zhang, Security Analysis of an Attractive Online Authentication Standard: FIDO UAF Protocol, China Communications, vol. 13, no. 12, pp. 189-198, December (2016).
[5] M. Yu and S. Devadas, Secure and Robust Error Correction for Physical Unclonable Functions, IEEE Design & Test of Computers, vol. 27, no. 1, pp. 48-65, Jan.-Feb, (2010).
[6] Suh G E, Devadas S. Physical Unclonable Functions for Device Authentication and Secret Key Generation. Design Automation Conference, (2007).
[7] Dodis Y, Ostrovsky R, Reyzin L, et al. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. Adv Eurocrypt, vol.38, pp. 97-139, (2004).
[8] Delvaux J, Peeters R, Gu D, et al. A Survey on Lightweight Entity Authentication with Strong PUFs. ACM Computing Surveys, vol.48, pp. 1-42, (2015).
[9] Bassil R, El-Beaino W, Kayssi A, et al. A PUF-based Ultra-lightweight Mutual-authentication RFID Protocol. Internet Technology and Secured Transactions, pp. 495 – 499, (2011).
[10] The next generation of identity authentication, http://www.sohu.com/a/204240481_490113.
[11] C. Tan and A. Kumar, Efficient and Accurate At-a-Distance Iris Recognition Using Geometric Key-Based Iris Encoding, IEEE Transactions on Information Forensics and Security, vol. 9, no. 9, pp. 1518-1526, Sept. (2014).
[12] X. Geng, Z. Zhou and K. Smith-Miles, Individual Stable Space: An Approach to Face Recognition Under Uncontrolled Conditions, IEEE Transactions on Neural Networks, vol. 19, no. 8, pp. 1354-1368, Aug. (2008).