mathematics

MDPI

Article

Improvement and Cryptanalysis of a Physically Unclonable Functions Based Authentication Scheme for Smart Grids

Masoumeh Safkhani [1], Nasour Bagheri [2], Saqib Ali [3], Mazhar Hussain Malik [4], Omed Hassan Ahmed [5], Mehdi Hosseinzadeh [6,*] and Amir H. Mosavi [7,8,9,*]

[1] Faculty of Computer Engineering, Shahid Rajaee Teacher Training University, Tehran 16788-15811, Iran
[2] Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran 16788-15811, Iran
[3] Department of Information Systems, College of Economics and Political Science, Sultan Qaboos University, Al Khoudh, Muscat P. C. 123, Oman
[4] School of Computing and Creative Technologies, College of Arts, Technology and Environment (CATE), University of the West of England, Frenchay Campus, Coldharbour Lane, Bristol BS16 1QY, UK
[5] Department of Information Technology, University of Human Development, Sulaymaniyah 0778-6, Iraq
[6] Pattern Recognition and Machine Learning Lab, Gachon University, 1342 Seongnamdaero, Sujeong-gu, Seongnam 13120, Republic of Korea
[7] John von Neumann Faculty of Informatics, Obuda University, 1034 Budapest, Hungary
[8] Institute of Information Engineering, Slovak University of Technology in Bratislava, 81243 Bratislava, Slovakia
[9] Institute of the Information Society, University of Public Service, 1083 Budapest, Hungary
* Correspondence: mehdi@gachon.ac.kr (M.H.); amirhosein.mosavi@stuba.sk (A.H.M.)

check for updates

Citation: Safkhani, M.; Bagheri, N.; Ali, S.; Hussain Malik, M.; Hassan Ahmed, O.; Hosseinzadeh, M.; Mosavi, A.H. Improvement and Cryptanalysis of a Physically Unclonable Functions Based Authentication Scheme for Smart Grids. *Mathematics* **2023**, *11*, 48. https://doi. org/10.3390/math11010048

Academic Editor: Jonathan Blackledge

Received: 5 October 2022
Revised: 13 December 2022
Accepted: 15 December 2022
Published: 23 December 2022

Abstract: Authentication protocols are often used in smart grids to deliver the necessary level of security. A huge number of clients in such a system, however, provides the attacker with the ability to clone them, for example. Device fingerprints, or Physically Unclonable Functions (PUF), have been investigated as an authentication feature to thwart such attacks. In order to accomplish the necessary security in smart grid neighborhood area network communications and to prevent unwanted physical access to smart meters, a former study designed a lightweight authentication system in this way. The suggested protocol uses PUFs to reduce physical attacks. As a consequence, the server/meter impersonation attack is one of the many assaults that this protocol is thought to be secure against. On the other hand, it is generally acknowledged that no security solution should be trusted unless its security has been verified by independent researchers. As a result, this paper assesses the security of this protocol against a typical adversary who has access to or influences over the messages carried over the public channel. This study demonstrates that the attacker is simply capable of impersonating the server for the meter and vice versa. In addition, the suggested attacks desynchronize them, making the adversary the only one capable of interacting with the meter in the role of the legal server rather than the latter. Each of the proposed attacks is extremely effective, and their success probability is almost 1. Finally, a modification is suggested that successfully fixes the protocol's security weaknesses. The security proof of the improved protocol has been done through the Scyther tool. The computational cost comparison shows that the overhead of the proposed protocol compared to the former scheme is 4.85%, while it withstands various attacks, including traceability, desynchronization, impersonation, man-in-the-middle, and secret disclosure attacks.

Keywords: Internet of things; IoT; smart grid; smart city; key agreement; physically unclonable functions; security

MSC: 94A60; 68M12; 68Pxx

1. Introduction

Smart grids play an important role in smart cities and are a promising technology for improving power system reliability, flexibility, and efficiency. Information and communication technologies are the basic infrastructure in a smart grid. However, assuming that the network is accessed and controlled by adversaries, this technology poses significant risks. To overcome such disadvantages, authentication protocols play an important role in determining whether a user is a friend or foe. An authentication protocol is a series of information exchanges between two or more parties to determine whether a specific party is legitimate or not. In distributed systems, such as Internet of Things (IoT) systems and smart grids, edge clients/devices are distributed throughout the field. Hence, it could not be possible to use physical protection in many cases, and, as a result, they are vulnerable to adversarial access. Such an adversary, for example, may read their memory and attempt to clone them. If there is a human involved in the authentication process, it is possible to use other factors to provide a higher level of security. Smart card-based user name and password, for example, may be used to increase the security in that case [1–4] or the user's biometrics [5–8]. However, the main challenge for employing multifactor authentication for many embedded devices, such as smart meters, is the fact that they should work 24/4 and be independent of the operator in many cases. Hence, researchers find a dual fingerprint for devices, which is known as a physically unclonable function (PUF) [9–14]. Although it could be a promising solution (assuming that PUFs behave fully reliable and randomly), the response is not entirely random, and the proposed protocol could be a target of modeling attacks [15–19], if the adversary accesses the PUF's input/output.

1.1. Motivation

Following the provided argument, to realize their full potential, smart grid applications require a dependable, lightweight, and fast authentication system [20]. One of the most difficult security challenges in the smart grid is protecting the meters, as well as embedded devices in general, from security breaches that could have disastrous consequences [21]. Among the various proposals to improve the security of smart grids, those that consider physical access to meters are more realistic and can achieve a higher level of security [22]. The reason is that the meters are distributed throughout the field, and an adversary can always access them to read their memory, for example, to clone them. As a result, security based on stored credentials could not withstand attacks based on such access. A common approach to providing security against this type of attack is multi-factor authentication, and among various approaches, using a physically unclonable function (PUF) as a hardware fingerprint has recently received a lot of attention [22]. However, such a solution should provide sufficient security requirements to be applicable to transferring sensitive data.

1.2. Challenge

A former study proposed a lightweight mutual authentication for smart grid neighborhood area network communications based on PUF [23]. Designers provided formal and informal security analysis and claimed protection against a variety of attacks, including impersonation. However, this protocol, similar to any other security solution, should be investigated independently to highlight its pros and cons. To the best of our knowledge, no independent detailed security analysis for this protocol has been reported in the literature. Hence, this paper is aimed at addressing this shortage by shedding light on its security.

1.3. Our Contribution

The main contribution of this paper is to shed light on the security of a PUF-based authentication protocol for smart grid applications, which has been recently proposed in a former study [23]. Although the protocol is very lightweight and has several interesting features that make it a good candidate for the target application, this paper shows that the adversary can easily impersonate the server or the meter and can also desynchronize them permanently. Following the proposed attack in this paper, the adversary could be the only entity that can communicate with the meter as the legitimate server. In addition, an amendment is proposed that effectively addresses the protocol's security flaws.

1.4. Related Works

Following the protocol discussed in this paper, i.e., [23], nearly the same team of authors [24–26] and other researchers [27,28] proposed or analyzed new related schemes, which are worth noting in this section to highlight later advances in this field of research. Among those studies, [26] dedicated to designing a PUF on an FPGA. They specifically proposed an FPGA-based Anderson PUF and tested it on Spartan-6 family Xilinx XC6SLX9 FPGAs. Their finding shows that the proposed structure increases the unpredictability of the designed PUF while decreasing the required area overhead. Aghapour et al. proposed a lightweight protocol [25] that provides mutual authentication using a hash function as the main cryptographic primitive. Although the proposed protocol considered smart grid neighborhood area network communications, it does not employ PUF and by nature, any node can tamper with such an application. In addition, one of the messages is computed as $((m_i^j \oplus r_i^j)\|r_i^j) \oplus k_i^j$ where r_i^j is a random value, m_i^j is a data packet, and k_i^j is the latest shared key. The shared key is updated after each successful session, first by the smart meter SM_j and then by the gateway NG. However, assuming the adversary allows SM_j to receive the message properly and update its session key to k_{i+1}^j but blocks the sent message to NG, then they desynchronized because SM_j does not keep a copy of k_i^j. Even in that case, the protocol does not provide full security of k_i^j if it is assumed m_i^j has enough low entropy and can be predicted by the adversary because $m_i^j \oplus r_i^j \oplus r_i^j = m_i^j$. Hence the expected complexity of finding k_{i+1}^j is $min(2^{\mathcal{H}(m_i^j)+\frac{1}{2}\mathcal{H}(K_i^j)}, \mathcal{H}(K_i^j))$ while it should be $\mathcal{H}(K_i^j)$, where $\mathcal{H}(\cdot)$ denotes the entropy function. In a later research, Aghapour et al. [24] proposed another protocol for smart grid applications that again uses the hash function to provide desired security. An interesting feature of this protocol is the use of a hash key chain to provide forward secrecy. However, if the adversary has access to SM_j, it can tamper with it. In addition, in this protocol, the NG's command is sent in plain text, which may not be desirable in some applications. Baghestani et al. [27] recently examined the security of a proposed authentication protocol by Kumar et al. [29] and demonstrated that smart meters are traceable in that protocol. Besides that, they proposed an elliptic curve cryptography (ECC)-based authentication protocol for smart grid applications. However, ECC is very time-consuming and may not be applicable in constrained environments. In addition, it also does not provide security against cloning attacks because it does not use PUF. Moreover, it can not withstand advanced attacks such as key compromise impersonation. Among the most recent research in this field is [30], which proposes a lightweight PUF-based authentication protocol for smart grid applications. Although the proposed protocol has interesting features compared to other related works such as [31,32], it has two important drawbacks. First, in a part of the protocol, the meter identifier is sent over a public channel plain, which is enough to trace it and compromise its anonymity. The second drawback is sending the PUF's response to the network gateway. Hence, it could be a target for modeling attack by an insider.

Therefore, there is still enough room to do research in this field and design a secure protocol for smart grid applications. On the other hand, any new protocol should be evaluated by third parties to ensure its security, which emphasizes the necessity of this research and other related works.

1.5. Paper Organization

In the remainder of this article, the necessary notations and a description of the former protocol are provided in Section 2. Then, in Section 3, the conducted attacks against this protocol are introduced. In Section 4, the improved protocol and its evaluation are presented. Finally, the paper is concluded in Section 6.

2. Review of Former Scheme

Each phase of the former protocol, which has been proposed by Kaveh and Mosavi [23] and we call it KM-protocol, is briefly explained in the following section, using the list of notations in Table 1.

Table 1. Used notations.

Symbol	Description
C_i	i^{th} challenge of PUF
R_i	The response to C_i
CRP	A challenge-response pair
TS	Timestamp
SM	Smart-meter
NG	Neighborhood gateway
r	Random number
ID	The unique identifier
$h(\cdot)$	One-way hash functions
$A\|B$	Concatenation of the strings A and B
X_{LSW}	Assuming $X = A\|B$, $X_{LSW} = B$
$\oplus$	Bitwise XOR
r	Random number
D_j	Usage report of the SM$_j$

As previously stated, KM-protocol is a lightweight authentication protocol for smart grids. The proposed protocol takes into account a neighborhood area network (NAN) in which a neighborhood gateway (NG) collects electricity data from hundreds of smart meters (SM). To gain a better understanding of the PUF-based KM-protocol, it is explained how it works in this section, and then its vulnerabilities are shown in the following section. The KM-protocol is divided into two phases: secure installation and secure communication. Secure Installation Phase: A smart meter must be registered by a neighborhood gateway before communication begins. As a result, the smart meter first sends ID_j and a $CRP = (C_i, R_i)$ from the PUF function to NG, where $R_i = \text{PUF}_j(C_i)$. This data is saved in the database of the NG. As a result, the NG can use them in the authentication process, and the SM$_j$ deletes CRP from its memory.

Secure communication Phase: The following are the steps in the authentication process:

- Step one:
  1. The ID_j of the SM$_j$ is sent to the NG.
- Step two: The NG searches its database for a field that matches the ID_j received. If a duplicate item is discovered, then:
  1. It obtains the associated $CRP = (C_i, R_i)$ for the received ID_j and generates two random numbers, r^{N1} and r^{N2}.
  2. Then A and V are calculated as $A = R_i \oplus ((r^{N1} \oplus TS_{\text{NG}})\|r^{N2})$ and $V = h(R_i \oplus (TS_{\text{NG}}\|r^{N1}) \oplus (r^{N2}\|ID_j))$, where TS_{NG} is the timestamp of NG.
  3. NG replies $\{A, V, C_i\}$ to SM$_j$.
- Step three: Upon receiving the messages, given C_i, the SM$_j$ calculates $R_i = \text{PUF}_j(C_i)$ and obtains r^{N1} and r^{N2} from $A \oplus R_i$, where TS_{NS} should be almost similar with the SM$_j$'s timestamp TS_j. Afterwards, given r^{N1} and r^{N2}, it verifies V and if the verification is passed:
  1. By generating a random number r^{SM}, SM$_j$ calculates a new challenge as $C_{i+1} = h(r^{\text{SM}}, r^{N2})$.
  2. Based on the new response $h(R_{i+1}) = h(\text{PUF}_j(\text{C}_{i+1}))$, it generates $S = (h(R_{i+1}) \oplus (TS_j\|r^{N1})) \oplus R_i)$.

3. Then SM_j computes E and V' as $E = (D_j\|(r^{N1} \oplus r^{\text{SM}})) \oplus R_i$ and $V' = h(h(R_{i+1}) \oplus (TS_j\|ID_j) \oplus (r^{\text{SM}}\|D_j))$.
4. Finally it transfers $\{E, S, V'\}$ to NG and deletes all stored variables.

- Step four: After receiving the messages, by using R_i the NG obtains r^{SM}, D_j and $h(R_{i+1})$. Then in order to verify V', it computes $h(h(R_{i+1}) \oplus (TS_{\text{NG}}\|ID_j) \oplus (r^{\text{SM}}\|D_j))$. If the verification holds, the NG:
  1. Compares D_j with the existing report format. If the comparison holds, it accepts the messages.
  2. NG calculates $C_{i+1} = h(r^{\text{SM}}, r^{N2})$ as the new challenge and saves $(C_{i+1}, h(R_{i+1}))$ as a new CRP for the next authentication process.
  3. It accepts all messages and finishes a successful mutual authentication process.

Because the KM-protocol employs the concatenation ($\|$) and XOR ($\oplus$) operations in its computation, the given property in Equation (1) is recalled:

$$(x\|y) \oplus (u\|v) \quad = \quad (x \oplus u)\|(y \oplus v) \tag{1}$$

where x, y, u, and v are appropriate strings. This property is used in the proposed analysis.

3. Cryptanalysis of KM-Protocol

Although the designer of the KM-protocol [23] claimed optimum security against various attacks in the context, important attacks against the KM-protocol are presented in this section using the same adversarial model and an ideal PUF model. More specifically, assuming that the adversary eavesdrops and stores the sent messages from NG to SM_j, i.e., $A = R_i \oplus ((r^{N1} \oplus TS_{\text{NG}})\|r^{N2}$ and $V = h(R_i \oplus ((TS_{\text{NG}}\|r^{N1}) \oplus (r^{N2}\|ID_j)$. The timestamp in this message is TS_{NG}, which is known to all participants, including the adversary. Furthermore, assuming the adversary intends to impersonate NG to SM_j at a desired time TS'_{NG}, it computes $A' = A \oplus (\Delta TS_{\text{NG}}\|\Delta TS_{\text{NG}})$ and sends A', V, C_i to SM_j when SM_j sends its ID_j, where $\Delta TS = TS'_{\text{NG}} \oplus TS_{\text{NG}}$. It is obvious that:

$$\begin{aligned} A' &= R_i \oplus ((r^{N1} \oplus TS_{\text{NG}})\|r^{N2}) \oplus (\Delta TS\|\Delta TS) \\ &= R_i \oplus ((r^{N1} \oplus TS_{\text{NG}} \oplus (TS'_{\text{NG}} \oplus TS_{\text{NG}})\|(r^{N2} \oplus \Delta TS)) \\ &= R_i \oplus ((r^{N1} \oplus TS'_{\text{NG}})\|(r^{N2} \oplus \Delta TS)) \end{aligned} \tag{2}$$

After receiving the message, given C_i, the SM_j calculates R_i and obtains $r'^{N1} = r^{N1}$ and $r'^{N2} = r^{N2} \oplus \Delta TS$ from $A' \oplus R_i$, and verifies whether:

$$\begin{aligned} V &\overset{?}{=} h(R_i \oplus ((TS'_{\text{NG}}\|r'^{N1}) \oplus (r'^{N2}\|ID_j))) \\ &= h(R_i \oplus ((TS'_{\text{NG}}\|r^{N1}) \oplus ((r^{N2} \oplus \Delta TS)\|ID_j))) \\ &= h(R_i \oplus (((TS'_{\text{NG}} \oplus \Delta TS)\|r^{N1}) \oplus (r^{N2}\|ID_j)) \\ &= h(R_i \oplus ((TS_{\text{NG}}\|r^{N1}) \oplus (r^{N2}\|ID_j))) \\ &= V \end{aligned} \tag{3}$$

As a result, following Equations (2) and (3), the adversary will be authenticated by SM_j with a probability of '1', at any time TS'_{NG}. It shows that, contrary to what the designers claim, the KM-protocol is vulnerable to impersonation attacks.

Next, a SM_j impersonation attack is proposed that will desynchronize both SM_j and NG. Consider a valid session between SM_j and NG in which SM_j sends its ID_j to NG and receives $\{C_i, A, V\}$ and again SM_j computes and transfers $\{E, S, V'\}$. The adversary stores ID_j, $\{C_i, A, V\}$ and $\{E, S, V'\}$ but prevents NG form receiving $\{E, S, V'\}$, where $S = (R_{i+1} \oplus (TS_{\text{NG}}\|r^{N1})) \oplus R_i)$, $E = (D_j\|(r^{N1} \oplus r^{\text{SM}})) \oplus R_i$ and $V' = h(R_{i+1} \oplus$

$(TS_{\mathrm{NG}} \| ID_j) \oplus (r^{\mathrm{SM}} \| D_j))$. As a result, NG does not update its $CPR(C_i, R_i)$ record. The adversary then does the following procedure:

1. Sends ID_j to NG.
2. NG retrieves the related $CRP(C_i, R_i)$ and generates r'^{N1} and r'^{N2} and computes $\hat{A} = R_i \oplus ((r'^{N1} \oplus TS'_{\mathrm{NG}}) \| r'^{N2}$ and $V = h(R_i \oplus ((TS'_{\mathrm{NG}} \| r'^{N1}) \oplus (r'^{N2} \| ID_j)$ and replies $\{A, V, C_i\}$ to the SM$_j$, which is impersonated by the adversary.
3. The adversary computes $\hat{A} \oplus A = ((r'^{N1} \oplus r'^{N1}) \oplus (TS'_{\mathrm{NG}} \oplus TS_{\mathrm{NG}})) \| (r'^{N2} \oplus r'^{N2})$. Given that timestamp is a public value, the adversary can compute $\Delta TS = TS'_{\mathrm{NG}} \oplus TS$ and extract $\Delta_1 = r^{N1} \oplus r'^{N1}$ and $\Delta_2 = r^{N2} \oplus r'^{N2}$ from $\hat{A} \oplus A$. Next, the adversary computes $\hat{S} = S \oplus (\Delta TS \| \Delta_1)$, $\hat{E} = E \oplus (0 \| (\Delta TS \oplus \Delta_1))$ and returns $\{\hat{E}, \hat{S}, V'\}$ to NG.
4. NG obtains r'^{SM} as follows:

$$\begin{aligned} r'^{\mathrm{SM}} &= (\hat{E} \oplus R_i)_{LSW} \oplus r'^{N1} \\ &= ((r^{N1} \oplus r^{\mathrm{SM}})) \oplus (R_i)_{LSW}) \oplus (\Delta TS \oplus \Delta_1) \oplus (R_i)_{LSW}) \oplus r'^{N1} \\ &= ((r^{N1} \oplus r^{\mathrm{SM}})) \oplus (\Delta TS \oplus r^{N1} \oplus r'^{N1}) \oplus r'^{N1} \\ &= r^{\mathrm{SM}} \oplus \Delta TS \end{aligned} \tag{4}$$

It also obtains R'_{i+1} as follows:

$$\begin{aligned} R'_{i+1} &= \hat{S} \oplus (TS'_{\mathrm{NG}} \| r'^{N1}) \oplus R_i \\ &= (R_{i+1} \oplus (TS_{\mathrm{NG}} \| r^{N1})) \oplus R_i) \oplus (\Delta TS \| \Delta_1) \oplus (TS'_{\mathrm{NG}} \| r'^{N1}) \oplus R_i \\ &= R_{i+1} \end{aligned} \tag{5}$$

and verifies whether:

$$\begin{aligned} V' &\overset{?}{=} h(R_{i+1} \oplus (TS'_{\mathrm{NG}} \| ID_j) \oplus (r'^{\mathrm{SM}} \| D_j)) \\ &= h(R_{i+1} \oplus (TS'_{\mathrm{NG}} \| ID_j) \oplus ((r^{\mathrm{SM}} \oplus \Delta T) \| D_j)) \\ &= h(R_{i+1} \oplus ((TS'_{\mathrm{NG}} \oplus \Delta T) \| ID_j) \oplus ((r^{\mathrm{SM}}) \| D_j)) \qquad (6) \\ &= h(R_{i+1} \oplus (TS_{\mathrm{NG}} \| ID_j) \oplus (r^{\mathrm{SM}} \| D_j)) \\ &= V' \qquad (7) \end{aligned}$$

Following the driven values in Equations (4) and (5), the verification of Equation (7) is successful, and the adversary is authenticated as a legitimate SM$_j$, confirming that impersonation was successful.

Following the above attack, the adversary was successfully authenticated as a legitimate SM$_j$. NG, on the other hand, calculates $C_{i+1} = h(r'^{\mathrm{SM}}, r'^{N2})$ as a new challenge, saves (C_{i+1}, R_{i+1}) as a new CRP for the next authentication process, and deletes $CRP(C_i, R_i)$ from its database. It means that NG has a new $CRP(C_{i+1}, R_{i+1})$ that is almost certainly not a valid CPR for the embedded PUF within SM$_j$. Therefore, NG is no longer recognized as valid by SM$_j$, indicating that the adversary successfully desynchronized them. The adversary who stored A, V, and C_i is now the only entity that can communicate with SM$_j$ as a result of the proposed NG impersonation attack.

4. Proposed Protocol

In this section, the KM-protocol is modified as little as possible to counter the proposed attack in this paper, and the security and efficiency of the revised protocol are discussed in comparison to the original protocol.

Suggested Remedy

The main reason for carrying out the proposed attacks is the adversary's ability to manipulate messages via the XOR operation. Hence, to avoid the proposed attacks, it is recommended to overcome the adversary's current control over the transferred messages.

To be more precise, similar to the KM-protocol, the improved protocol also includes two phases: secure installation and secure communication. The secure installation phase is unaffected by the revised protocol, except that $(C_i, h(R_i))$ are sent to the NG instead of the KM-protocol's (C_i, R_i). However, the steps in the authentication process (authentication phase) is revised as follows:

- Step one:
  1. SM_j sends its ID_j to the NG, if it fails uses the ID_j^{old}.
- Step two: NG looks up the $CRP = (C_i, h(R_i))$ associated with the received ID_j and generates a random number r^N. Following that, A and V are calculated as $A = h(R_i) \oplus r^N$ and $V = h(h(R_i)\|TS_{\mathrm{NG}}\|r^N\|ID_j)$, where TS_{NG} is the NG timestamp. Then NG responds to SM_j with $A, V, C_i, TS_{\mathrm{NG}}$.
- Step three: When the messages are received, SM_j verifies the received TS_{NG} and, given C_i, calculates $h(R_i) = h(\mathrm{PUF}_j(C_i))$ and obtains $r^N = A \oplus h(R_i)$. Following that, it verifies V before generating a random number r^{SM} in order to calculate a new challenge as $C_{i+1} = h(r^{\mathrm{SM}}\|r^N)$. Then it computes $S = h(R_{i+1}) \oplus h(r^N\|TS_{\mathrm{NG}})$, $E = (D_j\|r^{\mathrm{SM}}) \oplus h(r^N\|h(R_{i+1})\|h(R_i)\|TS_{\mathrm{NG}})$, $ID_j^{new} = h(h(R_{i+1})\|C_{i+1})$ and $V' = h(h(R_{i+1})\|TS_{\mathrm{NG}}\|ID_j^{new}\|r^{\mathrm{SM}}\|D_j\|C_{i+1})$. Finally it transfers $\{E, S, V'\}$ to NG, stores new $ID_j^{new} = h(h(R_{i+1})\|C_{i+1})$ and deletes all stored variables, exclude ID_j^{new} and $ID_j^{old} = ID_j$.
- Step four: After receiving the messages, NG computes $h(R_{i+1}) = S \oplus h(r^N\|TS_{\mathrm{NG}})$ and $(D_j\|r^{\mathrm{SM}}) = E \oplus h(r^N\|h(R_{i+1})\|h(R_i)\|TS_{\mathrm{NG}})$, $C_{i+1} = h(r^{\mathrm{SM}}\|r^N)$ and $ID_j^{new} = h(h(R_{i+1})\|C_{i+1})$. Next it verifies whether $V' \stackrel{?}{=} h(h(R_{i+1})\|TS_{\mathrm{NG}}\|ID_j^{new}\|r^{\mathrm{SM}}\|D_j\|C_{i+1})$ to accept the messages. Then, NG stores ID_j^{new} and corresponding $(C_{i+1}, h(R_{i+1}))$ for the next authentication process.

The authentication phase of the improved protocol is depicted in Figure 1.

SM_j		NG
	$\xrightarrow{ID_j}$	
		Finds the associated $CRP = (C_i, h(R_i))$ for the received ID_j, generates r^N, calculates $A = h(R_i) \oplus r^N$ and $V = h(h(R_i) \| TS_{\mathrm{NG}} \| r^N \| ID_j)$; TS_{NG} is the timestamp of NG
	$\xleftarrow{A,V,C_i,TS_{\mathrm{NG}}}$	
Verifies the received TS_{NG}, calculates $h(R_i) = h(\mathrm{PUF}_j(C_i))$ and obtains $r^N = A \oplus h(R_i)$, generates r^{SM} to calculate a new challenge as $C_{i+1} = h(r^{\mathrm{SM}} \| r^N)$ and its related response $h(R_{i+1}) = h(\mathrm{PUF}_j(C_{i+1}))$. Then it computes $S = h(R_{i+1}) \oplus h(r^N \| TS_{\mathrm{NG}})$, $E = (D_j \| r^{\mathrm{SM}}) \oplus h(r^N \| h(R_{i+1}) \| h(R_i) \| TS_{\mathrm{NG}})$, $ID_j^{new} = h(h(R_{i+1}) \| C_{i+1})$ and $V' = h(h(R_{i+1}) \| TS_{\mathrm{NG}} \| ID_j^{new} \| r^{\mathrm{SM}} \| D_j \| C_{i+1})$ and stores $ID_j^{new} = h(h(R_{i+1}) \| C_{i+1})$ and deletes all stored variables, exclude ID_j^{new} and $ID_j^{old} = ID_j$		
	$\xrightarrow{E,S,V'}$	
		Computes $h(R_{i+1}) = S \oplus h(r^N \| TS_{\mathrm{NG}})$ and $(D_j \| r^{\mathrm{SM}}) = E \oplus h(r^N \| h(R_{i+1}) \| h(R_i) \| TS_{\mathrm{NG}})$, $C_{i+1} = h(r^{\mathrm{SM}} \| r^N)$ and $ID_j^{new} = h(h(R_{i+1}) \| C_{i+1})$. Next it verifies $V' \overset{?}{=} h(h(R_{i+1}) \| TS_{\mathrm{NG}} \| ID_j^{new} \| r^{\mathrm{SM}} \| D_j \| C_{i+1})$ to accept the messages and store ID_j^{new} and corresponding $(C_{i+1}, h(R_{i+1}))$ for the next authentication process

Figure 1. Mutual authentication phase of proposed protocol.

5. Security and Cost Evaluation of the Improved Protocol

When the computations of V and V' in the KM-protocol and the proposed protocol are compared, it is clear that the main difference is that $\oplus$ is replaced with $\|$ and C_{i+1} is included in the computation of V'. These changes successfully prevent the proposed attacks. Following this fix, it is extremely difficult to impersonate NG or SM_j by replaying a message with a TS_{NG} timestamp at another TS'_{NG} timestamp. Furthermore, any change in A, E, or S affects $h(R_{i+1})$ or C_{i+1}, and V' is not verified by NG. Hence, the proposed meter impersonation attack will fail as well. On the other hand, the adversary cannot perform the proposed desynchronization attack if s/he cannot impersonate the meter SM_j. In the rest of this section, the security of the proposed protocol is presented in more detail. Through the analysis, an active adversary with access to the transferred messages over the public channels, i.e., $ID_j, E, S, V', A, V, C_i, TS_{\mathrm{NG}}$, is considered, where:

$$\begin{aligned}
A =& h(R_i) \oplus r^N \\
V =& h(h(R_i) \| TS_{\mathrm{NG}} \| r^N \| ID_j) \\
S =& h(R_{i+1}) \oplus h(r^N \| TS_{\mathrm{NG}}) \\
E =& (D_j \| r^{\mathrm{SM}}) \oplus h(r^N \| h(R_{i+1}) \| h(R_i) \| TS_{\mathrm{NG}}) \\
V' =& h(h(R_{i+1}) \| TS_{\mathrm{NG}} \| ID_j^{new} \| r^{\mathrm{SM}} \| D_j \| C_{i+1}) \\
C_{i+1} =& h(r^{\mathrm{SM}} \| r^N) \\
ID_j^{new} =& h(h(R_{i+1}) \| C_{i+1})
\end{aligned} \tag{8}$$

5.1. Replay Attack

Through a replay attack, the adversary aims to use an eavesdropped message from an early time at a later time to impersonate a protocol entity. The current timestamp is used in the computation of $V = h(h(R_i)\|TS_{\mathrm{NG}}\|r^N\|ID_j)$ and $V' = h(h(R_{i+1})\|\ TS_{\mathrm{NG}}\|ID_j^{new}\|r^{\mathrm{SM}}\|D_j\|C_{i+1}$ in the proposed protocol, similar to the KM-protocol. Hence, this protocol does not suffer from replay attacks.

5.2. Impersonation Attack

Given that it is not feasible to do a replay attack; the adversary should manipulate the transferred messages to do a successful impersonation attack. In order to impersonate NG, the adversary must return a valid tuple $(A, V, C_i, TS_{\mathrm{NG}})$, which corresponds to the current timestamp TS_{NG}. However, it is not possible to compute $V = h(h(R_i)\|TS_{\mathrm{NG}}\|r^N\|ID_j)$ without first knowing $h(R_i) = h(\mathrm{PUF}_j(C_i))$. However, the only way to get that value is from $A = h(R_i) \oplus r^N$, which is masked by a new random value, or from the previous $S = R_i \oplus h(r'^N\|TS'_{\mathrm{NG}})$, which is masked by r'^N once more. Hence, the adversary has no significant chance to impersonate NG. To impersonate SM, however, the adversary must return a valid set of $E, S,$ and V' for the given time TS_{NG}. On the other hand, $V' = h(h(R_{i+1})\|TS_{\mathrm{NG}}\|ID_j^{new}\|r^{\mathrm{SM}}\|D_j\|C_{i+1})$ and the adversary requires $h(R_{i+1}) = h(\mathrm{PUF}_j(C_{i+1}))$ to compute it. Given that the only way to get that value is via $A = h(R_i) \oplus r^N$ or $S = h(R_{i+1}) \oplus h(r^N\|TS_{\mathrm{NG}})$, that are masked, this protocol does not suffer from impersonation attacks.

5.3. Traceability and Anonymity

As long as the protocol's entities have not participated in a successful session, ID_j and C_i remain unaffected in the proposed protocol, but they will be randomized in the next session as $ID_j^{new} = h(h(R_{i+1})\|C_{i+1})$ and $C_{i+1} = h(r^{\mathrm{SM}}\|r^N)$. The adversary cannot track the target SM for an extended period of time because r^{SM} and r^N are also masked. Other parameters, such as E, S, V', A and V, are randomized by session-dependent ephemeral values and therefore cannot be traced. Hence, this protocol provides long-term untraceability.

5.4. Secret Disclosure Attack

In the proposed protocol, the secret parameter is the PUF's response and it is masked by ephemeral values through different sessions, i.e., $A = h(R_i) \oplus r^N$ and $S = R_i \oplus h(r'^N\|TS'_{\mathrm{NG}})$. Hence, the adversary has no chance to retrieve the PUF's response, which guarantees the protocol's security against secret disclosure attacks.

5.5. Man-in-the-Middle Attack

If the adversary is able to change the transferred messages without being detected, then it has conducted a successful man-in-the-middle attack. The structure of $V = h(h(R_i)\|TS_{\mathrm{NG}}\|r^N\|ID_j)$ and $V' = h(h(R_{i+1})\|TS_{\mathrm{NG}}\|ID_j^{new}\|r^{\mathrm{SM}}\|D_j\|C_{i+1})$ have been selected such that the integrity of the transferred messages is guaranteed. Therefore, the proposed protocol provides the desired security against man-in-the-middle attacks.

5.6. Permanent De-Synchronization Attack

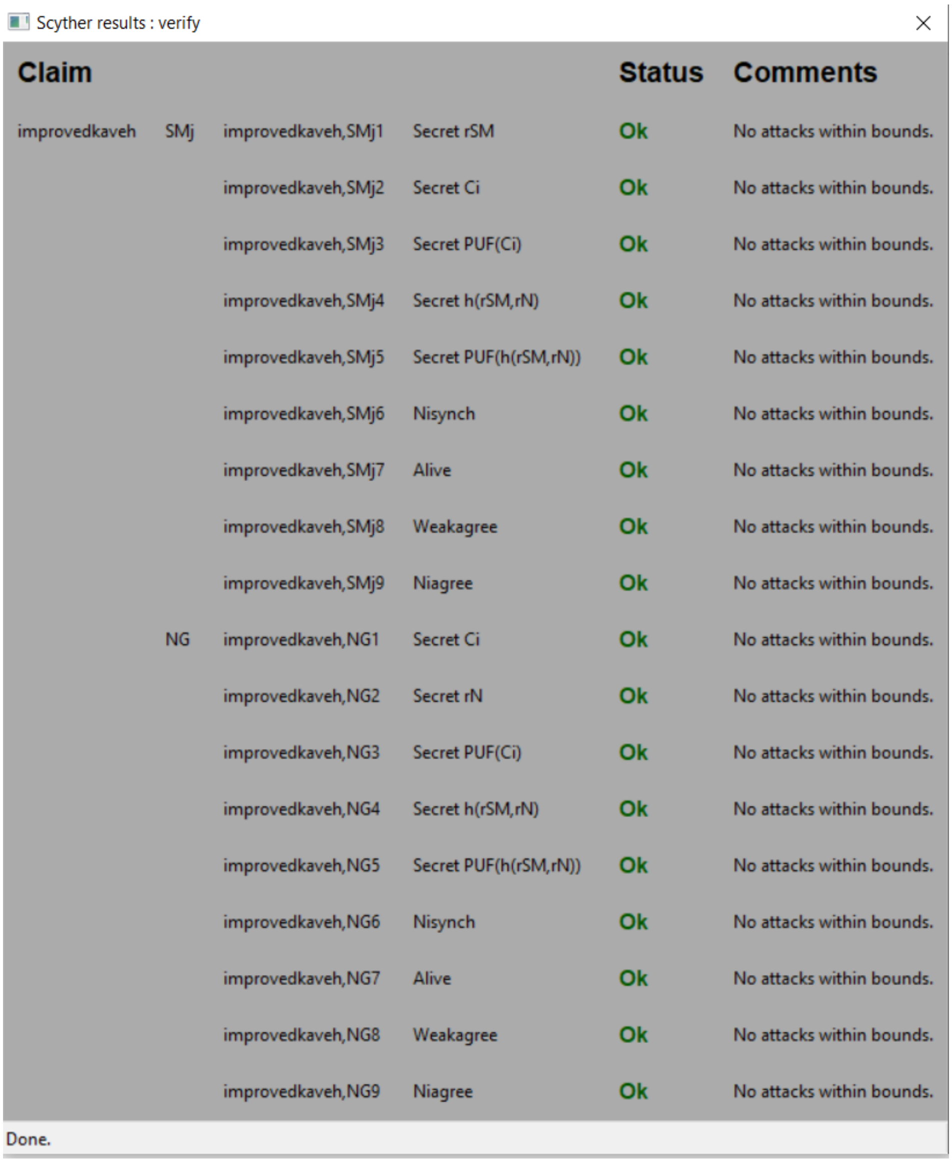
To do a permanent desynchronization attack, the adversary should successfully do an impersonation attack or act as a man-in-the-middle. Following Sections 5.2 and 5.5, the adversary has no chance to conduct such attacks. Hence, the proposed protocol resists permanent desynchronization attacks.

5.7. Modeling Attack

To do a modeling attack, the adversary needs access to several challenge/response pairs of the target PUF. Any adversary that monitors the channel has access to the challenges, but the responses are masked by ephemeral session-dependent values. Hence, such an adversary cannot model the embedded PUF. Because it has access to the exact response of PUF, a malicious NG can do this against the KM-protocol. However, in the proposed protocol, it has $h(R_i)$, not the exact R_i. Therefore, the proposed protocol does not suffer from a modeling attack.

5.8. Scyther

To verify the security of the proposed protocol formally, it has been modeled using SPDL and verified by the Scyther tool [33]. The evaluation results are represented in Figure 2, which confirms the security of the proposed protocol.



Claim				Status	Comments
improvedkaveh	SMj	improvedkaveh,SMj1	Secret rSM	Ok	No attacks within bounds.
		improvedkaveh,SMj2	Secret Ci	Ok	No attacks within bounds.
		improvedkaveh,SMj3	Secret PUF(Ci)	Ok	No attacks within bounds.
		improvedkaveh,SMj4	Secret h(rSM,rN)	Ok	No attacks within bounds.
		improvedkaveh,SMj5	Secret PUF(h(rSM,rN))	Ok	No attacks within bounds.
		improvedkaveh,SMj6	Nisynch	Ok	No attacks within bounds.
		improvedkaveh,SMj7	Alive	Ok	No attacks within bounds.
		improvedkaveh,SMj8	Weakagree	Ok	No attacks within bounds.
		improvedkaveh,SMj9	Niagree	Ok	No attacks within bounds.
	NG	improvedkaveh,NG1	Secret Ci	Ok	No attacks within bounds.
		improvedkaveh,NG2	Secret rN	Ok	No attacks within bounds.
		improvedkaveh,NG3	Secret PUF(Ci)	Ok	No attacks within bounds.
		improvedkaveh,NG4	Secret h(rSM,rN)	Ok	No attacks within bounds.
		improvedkaveh,NG5	Secret PUF(h(rSM,rN))	Ok	No attacks within bounds.
		improvedkaveh,NG6	Nisynch	Ok	No attacks within bounds.
		improvedkaveh,NG7	Alive	Ok	No attacks within bounds.
		improvedkaveh,NG8	Weakagree	Ok	No attacks within bounds.
		improvedkaveh,NG9	Niagree	Ok	No attacks within bounds.

Done.

Figure 2. Security evaluation of the proposed protocol using Scyther tool.

5.9. Cost Analysis

The computational cost of the improved protocol with KM-protocol and other related protocols for smart grids is compared and represented in this section. Through this analysis, $T_{E/D}$, T_H, T_{PUF}, $T_{GEN/REC}$, and T_{ECC} are used respectively to denote the computational time of a call to symmetric encryption/decryption, a one-way hash function, a PUF operation, the data generation and reproduction algorithm of the fuzzy extractor, and ECC point-multiplication. The expected time of those primitives is quoted from [30] and presented in Table 2, taking into account an embedded platform with a quad-core Cortex-A72

(ARM v8) 64-bit SoC at 1.5 GHz as NG and a MSP430FR5969 microcontroller as the meter. Since the PUF output is noisy, a fuzzy extractor should be used while regenerating the PUF response. Hence, to be fair, that time is added to the protocols whenever it is applicable, e.g., in the KM-protocol and the proposed protocol.

The details of each protocol computation and the approximate computation time based on the above-mentioned setup are provided in Table 3 and also depicted in Figure 3. Following the provided comparison, the overhead of the proposed protocol compared to the KM-protocol is only 4.85%, which is acceptable compared to the provided security level.

Table 2. Cost comparison of different primitives in micro-second, when a Quad-core Cortex-A72 (ARM v8) 64 bit SoC 1. 5GHz as NG and a MSP430FR5969-microcontroller as the meter1 [30].

Primetive	SM (μs)	NG (μs)
$T_{E/D}$	83.75	16.9
T_H	262	25.1
T_{PUF}	22.5	0.5
T_{GEN}	8912.8	1968
T_{REC}	3,2891. 8	8806

Table 3. Cost comparison of different protocols versus the proposed protocols.

	[31]		[32]		[30]		[23]		**0 urs**	
	SM	**NG**	**SM**	**NG**	**SM**	**NG**	**SM**	**NG**	**SM**	**NG**
E/D	0	0	0	0	1	5	0	0	0	0
H	4	5	3	9	4	12	2	3	6	6
PUF	2	0	1	0	2	2	2		2	0
GEN	0	1	0	0	0	2	0	0	0	0
REC	1	0	1	0	1	1	1	0	1	0
Time	34,389.8	2093.5	33,902.8	225.9	34,473.55	13,128.7	33,865.8	75.3	35,437.8	150.6
Total	36,483.3		34,128.7		47,602.25		33,941.1		35,588.4	

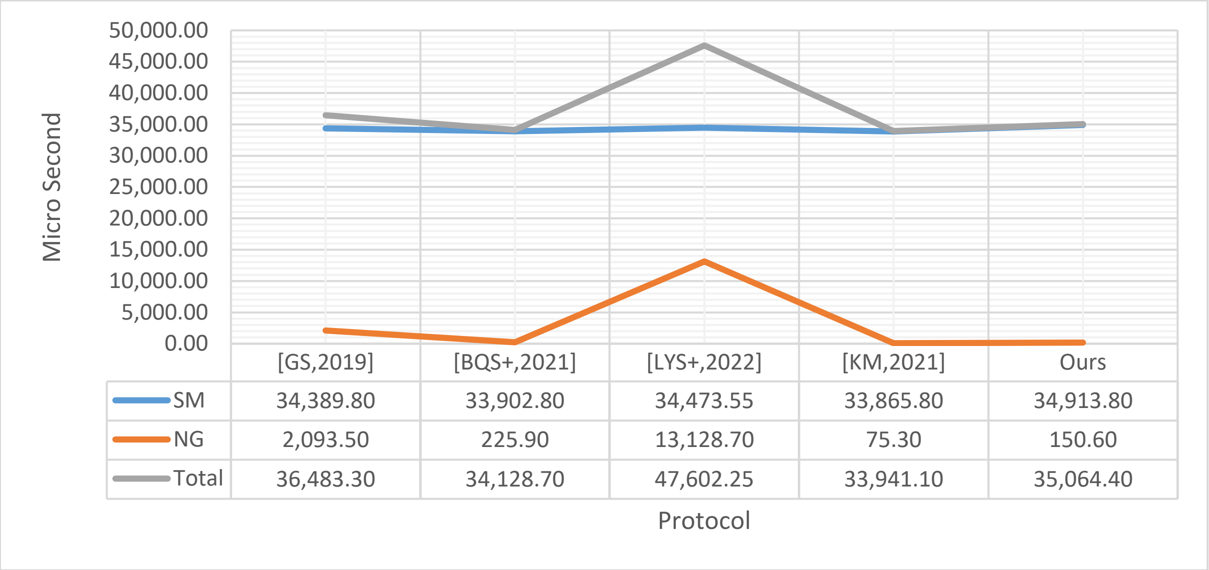


Figure 3. Comparison of the computational cost of the proposed protocol and related protocols ([GS,2019] [31]; [BQS+,2021] [32]; [LYS+,2022] [30]; [KM,2021] [23]; Ours: Figure 1).

6. Conclusions

This paper proposes several successful and efficient attacks against a recently proposed PUF-based protocol for smart grid applications, i.e., KM-protocol. The adversary can impersonate any protocol party, such as NG or SM$_j$, after monitoring a KM-protocol session and initiating another consequence session. Furthermore, following the proposed "SM" impersonation attack, "NG" and "SM" will be permanently desynchronized. The legitimate NG, on the other hand, can no longer communicate with the target SM$_j$, whereas the adversary can communicate with SM$_j$ at any time.

Minor changes to the KM-protocol were proposed to counter the proposed attacks and remedy the KM-protocol, which almost entirely prevent the aforementioned flaws at insignificant extra cost when compared to the original protocol.

It is worth noting that the KM-protocol sends the meter identifier, i.e., ID_j, over the public channel, which allows for a traceability attack and compromises the meter's anonymity. This attack was taken into account in the proposed alternative; however, it is still possible to trace a meter as long as it has not participated in a successful session of the protocol. One simple solution is to mask its identifier in the first step, such as by sending $SID_j = h(ID_j \| TS_j)$. Although the such protocol provides anonymity in this manner, the outcome is not scalable. It is possible to revise the protocol to provide scalability as well, but this will increase the protocol's cost, so it is left for future work.

Author Contributions: N.B.: Conceptualization, Methodology, Validation, Writing; M.S.: Experimentation, Validation, Writing—review & editing, S.A. Conceptualization, Methodology, Experimentation, Validation, Writing—review & editing, M.H.M.: Experimentation, Validation, review & editing, O.H.A.: Experimentation, Validation, Writing—review & editing; M.H.: Methodology, Designing, Experimentation, Validation, Supervision, Review, Funding & editing; A.H.M.: Experimentation, Designing, Validation, Writing—review & editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: For any supplementary material, please contact the corresponding authors.

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

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
SG	Smart Grid
NAN	Neighborhood Area Network
SM	Smart Meter
NG	Neighborhood Gateway
PUF	Physically Unclonable Function
CRP	A Challenge-Response Pair
TS	Timestamp
ID	The unique identifier

References

1. Juang, W.S.; Chen, S.T.; Liaw, H.T. Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards. *IEEE Trans. Ind. Electron.* **2008**, *55*, 2551–2556. [CrossRef]
2. Tsai, J.L.; Lo, N.W.; Wu, T.C. Novel Anonymous Authentication Scheme Using Smart Cards. *IEEE Trans. Ind. Inform.* **2013**, *9*, 2004–2013. [CrossRef]
3. Shunmuganathan, S.; Saravanan, R.D.; Palanichamy, Y. Secure and Efficient Smart-Card-Based Remote User Authentication Scheme for Multiserver Environment. *Can. J. Electr. Comput. Eng.* **2015**, *38*, 20–30. [CrossRef]
4. Odelu, V.; Das, A.K.; Goswami, A. A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1953–1966. [CrossRef]

5. Badhib, A.; Alshehri, S.; Cherif, A. A Robust Device-to-Device Continuous Authentication Protocol for the Internet of Things. *IEEE Access* **2021**, *9*, 124768–124792. [CrossRef]
6. Zhang, R.; Xiao, Y.; Sun, S.; Ma, H. Efficient Multi-Factor Authenticated Key Exchange Scheme for Mobile Communications. *IEEE Trans. Dependable Secur. Comput.* **2019**, *16*, 625–634. [CrossRef]
7. Ryu, J.; Oh, J.; Kwon, D.; Son, S.; Lee, J.; Park, Y.; Park, Y. Secure ECC-Based Three-Factor Mutual Authentication Protocol for Telecare Medical Information System. *IEEE Access* **2022**, *10*, 11511–11526. [CrossRef]
8. Liu, Z.; Guo, C.; Wang, B. A Physically Secure, Lightweight Three-Factor and Anonymous User Authentication Protocol for IoT. *IEEE Access* **2020**, *8*, 195914–195928. [CrossRef]
9. Adeli, M.; Bagheri, N.; Martín, H.; Peris-Lopez, P. Challenging the security of "A PUF-based hardware mutual authentication protocol". *J. Parallel Distrib. Comput.* **2022**, *169*, 199–210. [CrossRef]
10. Cao, J.; Li, S.; Ma, R.; Han, Y.; Zhang, Y.; Li, H. RPRIA: Reputation and PUF-Based Remote Identity Attestation Protocol for Massive IoT Devices. *IEEE Internet Things J.* **2022**, *9*, 19174–19187. [CrossRef]
11. Aminian Modarres, A.M.; Sarbishaei, G. An Improved Lightweight Two-Factor Authentication Protocol for IoT Applications. *IEEE Trans. Ind. Inform.* **2022**, 1–11. [CrossRef]
12. Cho, Y.; Oh, J.; Kwon, D.; Son, S.; Lee, J.; Park, Y. A Secure and Anonymous User Authentication Scheme for IoT-Enabled Smart Home Environments Using PUF. *IEEE Access* **2022**, *10*, 101330–101346. [CrossRef]
13. Li, S.; Zhang, T.; Yu, B.; He, K. A Provably Secure and Practical PUF-Based End-to-End Mutual Authentication and Key Exchange Protocol for IoT. *IEEE Sens. J.* **2021**, *21*, 5487–5501. [CrossRef]
14. Lounis, K.; Zulkernine, M. T2T-MAP: A PUF-Based Thing-to-Thing Mutual Authentication Protocol for IoT. *IEEE Access* **2021**, *9*, 137384–137405. [CrossRef]
15. Xu, Y.; Lao, Y.; Liu, W.; Zhang, Z.; You, X.; Zhang, C. Mathematical Modeling Analysis of Strong Physical Unclonable Functions. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2020**, *39*, 4426–4438. [CrossRef]
16. Shi, J.; Lu, Y.; Zhang, J. Approximation Attacks on Strong PUFs. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2020**, *39*, 2138–2151. [CrossRef]
17. Zhang, J.; Shen, C.; Guo, Z.; Wu, Q.; Chang, W. CT PUF: Configurable Tristate PUF Against Machine Learning Attacks for IoT Security. *IEEE Internet Things J.* **2022**, *9*, 14452–14462. [CrossRef]
18. Uddin, M.; Majumder, M.B.; Rose, G.S. Robustness Analysis of a Memristive Crossbar PUF Against Modeling Attacks. *IEEE Trans. Nanotechnol.* **2017**, *16*, 396–405. [CrossRef]
19. Liu, J.; Zhao, Y.; Zhu, Y.; Chan, C.H.; Martins, R.P. A Weak PUF-Assisted Strong PUF With Inherent Immunity to Modeling Attacks and Ultra-Low BER. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2022**, *69*, 4898–4907. [CrossRef]
20. Patil, V.C.; Kundu, S. Realizing Robust, Lightweight Strong PUFs for Securing Smart Grids. *IEEE Trans. Consumer Electron.* **2022**, *68*, 5–13. [CrossRef]
21. Boyapally, H.; Mathew, P.; Patranabis, S.; Chatterjee, U.; Agarwal, U.; Maheshwari, M.; Dey, S.; Mukhopadhyay, D. Safe is the New Smart: PUF-Based Authentication for Load Modification-Resistant Smart Meters. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 663–680. [CrossRef]
22. Mall, P.; Amin, R.; Das, A.K.; Leung, M.T.; Choo, K.R. PUF-Based Authentication and Key Agreement Protocols for IoT, WSNs, and Smart Grids: A Comprehensive Survey. *IEEE Internet Things J.* **2022**, *9*, 8205–8228. [CrossRef]
23. Kaveh, M.; Mosavi, M.R. A Lightweight Mutual Authentication for Smart Grid Neighborhood Area Network Communications Based on Physically Unclonable Function. *IEEE Syst. J.* **2020**, *14*, 4535–4544. [CrossRef]
24. Aghapour, S.; Kaveh, M.; Martín, D.; Mosavi, M.R. An Ultra-Lightweight and Provably Secure Broadcast Authentication Protocol for Smart Grid Communications. *IEEE Access* **2020**, *8*, 125477–125487. [CrossRef]
25. Aghapour, S.; Kaveh, M.; Mosavi, M.R.; Martín, D. An Ultra-Lightweight Mutual Authentication Scheme for Smart Grid Two-Way Communications. *IEEE Access* **2021**, *9*, 74562–74573. [CrossRef]
26. Lotfy, A.; Kaveh, M.; Martín, D.; Mosavi, M.R. An Efficient Design of Anderson PUF by Utilization of the Xilinx Primitives in the SLICEM. *IEEE Access* **2021**, *9*, 23025–23034. [CrossRef]
27. Baghestani, S.H.; Moazami, F.; Tahavori, M. Lightweight Authenticated Key Agreement for Smart Metering in Smart Grid. *IEEE Syst. J.* **2022**, *16*, 4983–4991. [CrossRef]
28. Zerrouki, F.; Ouchani, S.; Bouarfa, H. PUF-based mutual authentication and session key establishment protocol for IoT devices. *J. Ambient. Intell. Humaniz. Comput.* **2022**, 1–19.. [CrossRef]
29. Kumar, P.; Gurtov, A.V.; Sain, M.; Martin, A.P.; Ha, P.H. Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks. *IEEE Trans. Smart Grid* **2019**, *10*, 4349–4359. [CrossRef]
30. Liu, F.; Yan, Y.; Sun, Y.; Liu, J.; Li, D.; Guan, Z. Extremely Lightweight PUF-based Batch Authentication Protocol for End-Edge-Cloud Hierarchical Smart Grid. *Secur. Commun. Netw.* **2022**, *2022*, 9774853. [CrossRef]
31. Gope, P.; Sikdar, B. Privacy-Aware Authenticated Key Agreement Scheme for Secure Smart Grid Communication. *IEEE Trans. Smart Grid* **2019**, *10*, 3953–3962. [CrossRef]

32. Badar, H.M.S.; Qadri, S.; Shamshad, S.; Ayub, M.F.; Mahmood, K.; Kumar, N. An Identity Based Authentication Protocol for Smart Grid Environment Using Physical Uncloneable Function. *IEEE Trans. Smart Grid* **2021**, *12*, 4426–4434. [CrossRef]
33. Cremers, C. CISPA. Available online: https://people.cispa.io/cas.cremers/publications/index.html (accessed on 17 December 2022)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.