PUF-based solutions for secure communication in Advanced Metering Infrastructure (AMI)

Mahshid Delavar[1], Sattar Mirzakuchaki[2], Mohammad Hassan Ameri[3], Javad Mohajeri[4]

[1,2] Department of Electrical Engineering, Iran University of Science and Technology (IUST), Narmak, Tehran, Iran

[3,4] Electronic Research Institute, Sharif University of Technology, Azadi, Tehran, Iran

[1]Corresponding Author: Mahshid Delavar

Tel.: +98 912 3110 969

Email: mdelavar@iust.ac.ir

[2]m_kuchaki@iust.ac.ir

[3]Ameri70@gmail.com

[4]mohajer@sharif.ir

Abstract: In this paper, by considering the constraints of Advanced Metering Infrastructure (AMI) systems, we propose an authenticated key exchange protocol and an authenticated message broadcasting protocol. The proposed protocols are based on two well-known protocols, Okamoto and Schnorr, and inherit their security features. For providing the security of the system against physical attacks, we utilize the Physical Unclonable Function (PUF) technology in communication parties. Thus, there is no need to store the secrets in the smart meters which can easily be corrupted. We show that the proposed authenticated key exchange protocol meets all the security requirements such as secure key generation, backward and forward secrecy and explicit authentication. Also, it is shown that the authenticated message broadcasting protocol is secure against corrupted smart meters. The proposed schemes are practical and efficient for providing a secure communication between parties. We believe that our proposed protocols are the best fit for an AMI system.

Keywords: Advanced Metering Infrastructure (AMI), Key Management, Physical Unclonable Function (PUF), message broadcasting, authentication, physical security**.**

1 Introduction

1.1 Background and Motivation

The growing population of the world leads to a greater increase in demand for energy. In addition, today's modern life expects a stable and sustainable supply of energy from power systems. One major solution to handle such a demand increase and satisfying the modernized world's requests is to manage a variety of energy resources in a sufficient way. This is out of the capability of existing power systems. As a result, the notion of smart grid is appeared. The smart grid has the potential to provide sufficient capacity, reliability, efficiency and sustainability. In comparison with the existing power system, the smart grid utilizes high speed and bidirectional communication technologies for connecting millions of power components. This results in a dynamic and interactive infrastructure with novel energy management capabilities. One example is Advanced Metering Infrastructure (AMI) [1].

Advanced metering infrastructure is an essential part of smart grid initiative which provides two-way communications between smart meters and the utility company. The AMI system makes the real-time transmission of power consumption of customers and their pricing information possible. It also enables remote control of residential appliances. In this system, customers are able to adjust their consumption according to pricing data. Moreover, the utility companies can handle overloads caused by peak electricity demands [2].

The AMI network uses wireless technology for communication. In spite of the advantages of wireless networks, they are inherently more vulnerable to several types of passive and active attacks, such as eavesdropping, denial of service and the attacks targeting data integrity and entity authentication. In addition, smart meters are located in physically insecure environments which increases the risk of physical attacks. As smart meters are in two way communication with the utility, the vulnerabilities of them can lead to gain access to the more critical parts of the AMI network. This may destruct the whole infrastructure. Since having a secure and reliable data communication is essential, providing the cyber and physical security becomes one of the major challenges in the AMI networks. Applying cryptographic primitive based approaches are essential to ensure the security requirements of an AMI network.

1.2 Challenging Issue

In an AMI system, most electronic devices including smart meters should support basic cryptographic capabilities. Any smart meter should have its own cryptographic keys. Dedicating a unique secret key to all or some groups of smart meters increase the risk of happening a “break-one break-everywhere scenario”[3]. Each AMI network consists of millions of smart meters. And therefore, we face with millions of keys. Thus, developing a secure key management scheme for this large amount of keys is crucial. Deployment of an insecure key management scheme will increase the possibility of key disclosure to attackers and will threaten the entire communications in the AMI network.

NISTIR 7628 has presented a guideline for smart grid cyber security in [3]. This guideline introduces secure management, scalability, efficiency and evolvability as the basic requirements of an efficient key management scheme for smart grid [1]. On the other hand, [4] addresses cryptographic key management issues related to AMI. According to [4], deployment of smart meters in unprotected or lightly protected environments, their long life span and resource constraints are the points which must be considered for designing a key management scheme for an AMI network.

In the conventional approaches, cryptographic keys and other secrets are stored in digital memories of smart meters. These memories are vulnerable against invasive attacks [5-8] which can be simply applied to unprotected smart meters [9].

Therefore, developing a secure key management scheme which can provide high level of physical security in the AMI networks is a challenging issue.

1.3 Literature Review

The proposed key management schemes for smart grid can be considered in three categories based on their approaches including: the symmetric key based schemes, the public key based schemes and the ones which use both of them.

The schemes presented in [10, 11] are in the first category. In [10] the authors developed a scheme that uses a Trusted Third Party (TTP) for key distribution, while the authors of [11] introduced a password-based authenticated symmetric key establishment without need to TTP. None of the introduced schemes are scalable.

The problem of scalability was solved in the public key based schemes. Most of introduced public key based schemes are certificate based [12] or identity based schemes [13-17]. The certificate based schemes need Public Key Infrastructure (PKI) which adds high computational and communication costs to the system [4] and the identity based schemes suffer from the key escrow problem.

In the third category, we can refer to [18] which has combined the symmetric key and elliptic curve public key techniques in its developed key management scheme. Moreover, this category includes several key management schemes [19-24] for Supervisory Control and Data Acquisition (SCADA).

The main vulnerability point of all the introduced works except [25] is smart meters which contains some important secrets and are located in insecure environment. In [25], the authors introduced a public key based scheme without using a PKI and utilized PUF's properties for providing the physical security of an AMI network. However, it suffers from some other security issues. In the AMI network, the utility is responsible for transmitting critical commands and messages to the smart meters. So, the authentication of the Utility by the smart meters is vital in these networks. The main drawback of the developed key management scheme in [25] is not addressing this crucial requirement. Furthermore, the scheme does not provide confidence that the other party gets the session key. The mentioned shortcomings are solved in our proposed protocols.

1.4 Our Contribution

In this paper, we propose new authenticated key exchange and message broadcasting protocols. The proposed protocols utilize Physical Unclonable Functions (PUFs). PUFs are new primitives to extract secrets from complex physical characteristics of Integrated Circuits (ICs) instead of storing them in a memory. PUFs utilize the random variations occurring during a fabrication process. Therefore, prediction or extraction of the produced secrets becomes extremely difficult. Also, since PUFs generate volatile secrets which only exist when the chip is running, physical security is significantly increased. In our proposed protocols, the PUF devices are embedded in both parties (Head-End System (HES) and Smart Meters (SMs)) and used for generating the secrets and random values.

The proposed authenticated key exchange protocol is based on Okamoto identification scheme which is provable secure. The scheme shows strong physical security and meets essential security requirements for a secure key management scheme such as mutual authentication, forward and backward secrecy, collusion resistance and so on. The authenticated message broadcasting protocol is based on the modified version of Schnorr zero-knowledge identification protocol. Also, the hash chain idea is utilized in this protocol [26]. In the proposed protocol, the Smart Meters (SMs) can authenticate both the HES and the critical commands broadcasted by HES.

OVERVIEW- The paper is organized as follows: Section II briefly describes AMI and its security requirements. In section III, we introduce the relevant cryptographic primitives. Our proposed protocols are introduced in section IV. Section V and section VI present the security analysis of the proposed protocols and a discussion about them, respectively. Finally, conclusion are drawn in section VII.

2 System Model

In this section, we describe a typical model of Advanced Metering Infrastructure (AMI) considered in this paper; also, its security requirements and system constraints are introduced.

2.1 System Components

An overall AMI model includes the smart meter, the network communication device and the head-end system [27, 28] (Fig. 1).

AMI Head-End System is located within the utility company. It is responsible for two-way communications with smart meters to gather data and send the executive commands. The system also remotely manages firmware updates, configuration changes, control and diagnostics.

Smart Meter is an electronic smart-metering device which has two-way communication with the head-end system.

It measures and records data such as energy usage and generation and transmits them to the utility.

Network Communications Device is an intermediate component between the smart meter and the head-end system which carries all the information exchanged between them. As this component does not play a security role in most of the introduced protocols and schemes, we do not consider it in our proposed protocols, as well.

2.2 Security Requirements

The AMI network like other communication networks must provide the following common security requirements [29].

Confidentiality - Smart meters store the information about customers' energy usage and their personal details which can be a potential point of attacks. Attackers who are able to access these data can use or change them to benefit themselves. They can also endanger victim consumers by analyzing and manipulating their energy usage. Therefore, confidentiality is an important issue in AMI systems.

Integrity **-** The exchanged data between the utilities and the customers must be checked for integrity. For example, in the direction from the customer to the utility, altering the energy usage by adversaries will lead to erroneous billing. In opposite direction, changing the control data from the utility to the customer can result in faults and major outages.

Availability **-** Availability is one of the most important security requirements in AMI systems. As the utilities depend upon smart meters to collect energy usage data, the meters must be available when the utilities request for the usage data.

Source authentication **-** authentication of smart meters to the utility and vice versa is extremely critical for granting access to resources in the AMI systems. In these systems, it must be ensured that resources are accessed only by the appropriate entities that are correctly identified. Otherwise, unauthorized parties can impersonate the utility or a smart meter and transmit the false data to the other party. In some cases, such as sending outage command from the utility to the smart meters, will cause irreversible damages to all the system.

Cryptographic techniques play an important role in providing the first, second and forth requirements and designing a secure key management scheme is the fundamental part of any cryptographic mechanism which is considered in this paper.

2.3 System Constraints

For designing a secure key management scheme, the system's constraints should be considered. Therefore, we discuss some constraints of the AMI system in the following section [5, 30].

Physical environment - Smart meters which are one of the basic components of the AMI systems, are located in unprotected or lightly protected environments. They contain sensitive information such as cryptographic keys. Therefore physical protection of them must be considered in developing a key management scheme for AMI networks.

Life Span – Most of the AMI equipment, such as Smart Meters, have long life spans. A smart meter is expected to be functional for 15 years which is in contrast to the lifespan for most IT and telecommunications equipment (6 months to 2 years). Therefore, the cryptographic primitives and algorithms applied in the AMI networks must have long lifetimes. If the cryptographic algorithms are weakened by emerging new technologies or new cryptanalysis methods, the designed key management system must be upgradeable which includes updating all the cryptographic keys.

Communication Constraints – The bandwidth is a major constraint on many of the AMI endpoints and must be considered in designing the key management scheme for AMI. The functions of the cryptographic key management scheme such as key generation, key update, key revocation/suspension, and key distribution for potentially millions of cryptographic keys must be designed with a very low overhead.

Following, we present our proposed protocols which are designed by considering the mentioned constraints and provide the AMI security requirements. In these protocols, Physical Unclonable Functions (PUFs) are utilized for providing security against physical attacks. Designing the protocols based on Pedersen commitment and two well-known protocols, Okamoto and Schnorr, ensures the long time security of them. Also, as there is no need to implement a Public Key Infrastructure in our proposed protocols, they do not add high communication overhead to the system.

3 Building Blocks

This section is dedicated for introducing the cryptographic primitives used in the proposed protocols.

3.1 Physical Unclonable Functions (PUFs)

Physical Unclonable Function (PUF) is a physical entity that is tied to a device and gives unique characteristics to it such that its reproduction becomes practically impossible. A PUF shows different responses to different challenges and any attempts to tamper it, will affect on the behavior of the PUF and destroy it. An ideal PUF must have the following characteristics:

- Given a PUF device and a challenge C_i as input, must generate the same response R_i.
- Given a PUF device and a response R_i, it must be difficult to find the corresponding challenge C_i.
- Given a PUF device, two different challenges $C_1 \neq C_2$ must produce two different responses $R_1 \neq R_2$.
- Given a challenge C_i, two different PUFs must produce two different responses $R_i \neq R'_i$.

3.2 Pedersen Commitment

The *Pedersen commitment* [31] is an information-theoretically hiding commitment scheme which is based on the intractability of the discrete logarithm problem.

This scheme consists of the following three algorithms:

Setup **-** A Trusted Third Party (TTP) or one of the participants in the communication, chooses a multiplicative finite cyclic group G of large prime order p so that the computational Diffie-Hellman problem is hard in G. TTP chooses two generators g and h of G such that nobody knows $x = \log_g h$. It is not required that TTP knows the secret value x. Then, (G, p, g, h) are published by TTP as the public parameters.

Commit **-** The committer commits himself to a value $\alpha \in \mathbb{F}_p$ by choosing $\beta \in \mathbb{F}_p$ at random and computing the commitment $c = g^\alpha h^\beta \in G$.

Reveal **-** The committer reveals the values α and β to open the commitment c. The verifier checks whether $c = g^\alpha h^\beta$ or not.

3.3 Zero-Knowledge Proof (ZKP)

A Zero-Knowledge Proof (ZKP) is a two-party protocol which allows one party (the prover) to convince the other party (the verifier) that he knows some secrets which satisfy a given relation without revealing any information about them to the verifier [32]. Okamoto and Schnorr protocols are two ZKP protocols which are used in our authenticated key exchange and message broadcasting protocols, respectively. Both of the protocols are widely used and based on the hardness of the Discrete Logarithm Problem (DLP) on a cyclic group G of large prime order p. Okamoto protocol is provable secure [33, 34] and resistant against active and concurrent attacks [35]. Following, we describe how these protocols work.

3.3.1 Schnorr Protocol

In this protocol, the prover holds private knowledge of $x = \log_g y$ (where g is a generator of group G) and convince the verifier that he can open the commitment $y = g^x$ as follows [36]:

- The prover randomly chooses $r \in \mathbb{F}_p$, and sends $d = g^r$ to the verifier.

- The verifier replies a challenge value $e \in \mathbb{F}_p$ chosen at random.

- Upon receiving e, the prover computes $u = r + ex \ (mod\ p)$ and sends it to the verifier.

The verifier accepts the proof if and only if $g^u = dy^e$ in G.

3.3.2 Okamoto protocol

The Okamoto protocol may be viewed as a variation of Schnorr protocol [7]. In this protocol, the prover which holds the private knowledge of values α and β can convince the verifier that he/she can reveal the Pedersen commitment $c = g^{\alpha} h^{\beta}$ (where g and h are two generators of group G) as follows:

- The prover randomly chooses $y, s \in \mathbb{F}_p$ and sends $d = g^{y} h^{s} \in G$ to the verifier.
- The verifier sends a challenge value $e \in \mathbb{F}_p$ chosen at random.
- The prover returns $u = y + e\alpha \ (mod\ p)$, and $v = s + e\beta \ (mod\ p)$ to the verifier.
- The verifier accepts the proof if and only if $g^{u} h^{v} = d.c^{e}$ in G.

4 The Proposed Protocols

In this section, we introduce our proposed protocols including an authenticated key exchange protocol and an authenticated message broadcasting protocol.

Both of the protocols utilize a Physical Unclonable Function embedded in the head-end system (PUF_{HES}) and each Smart Meter (PUF_{SM_i}). The PUFs are used for generating the commitments and random numbers which are needed through running the protocols. Okamoto and Schnorr protocols are used in authenticated key exchange and authenticated message broadcasting protocols, respectively. The security of our schemes are based on discrete logarithm problem assumption.

The description of the proposed protocols is as follows.

4.1 Authenticated Key Exchange protocol

In this protocol, the Head-End System (HES) and the Smart Meter (SM) exchange a session key after authenticating each other. The protocol consists of four phases: Initialization, Registration, Mutual authentication and Key exchange (Fig. 2).

Initialization – In this phase, the Utility initializes the system by executing the setup phase of the Pedersen Commitment scheme. It defines cryptographic hash functions H_1, H_2, H_3: $H_1 \colon \{0,1\}^{t} \rightarrow \mathbb{F}_p$, $H_2 \colon \mathbb{F}_p \times \mathbb{F}_p \rightarrow \{0,1\}^{m}$, $H_3 \colon \mathbb{F}_p \times \{0,1\}^{m} \rightarrow \{0,1\}^{m}$ where *t* is the length of PUF responses and *m* is a security parameter. Also, it selects two challenges C_a and C_k which are applied to the PUFs implemented in the Head-End System (HES) and each Smart Meter (SM_i).

Registration – Before installation the Smart Meters in their locations and running the protocol, some secrets must be shared between the HES and SM_i. For satisfying this requirement, the following procedure is executed in the registration phase, assuming that the HES is in physical contact with SM_i.

1- Giving two challenges (C_a, C_k) to the PUF_{SM_i}, it generates the corresponding responses, $R_a^i = PUF_{SM_i}(C_a)$ and $R_k^i = PUF_{SM_i}(C_k)$. The same procedure is done with the PUF_{HES} by giving C_a as a challenge and producing $R_u = PUF_{HES}(C_a)$.

2- The cryptographic hash function H_1 is applied to all of the PUF responses to convert the vector responses of PUFs to a unique value in $\mathbb{F}_p$ for computing the commitments. Thus, the parameters α_i, β_i and γ are produced:
$\alpha_i = H_1(R_a^i)$, $\beta_i = H_1(R_k^i)$ and $\gamma = H_1(R_u)$. Then, β_i and h^{γ} are stored in the HES and SM_i, respectively.

3- Using the produced parameters, the Pedersen Commitments of the PUF responses are computed as follows: $com_i = g^{\alpha_i} h^{\beta_i}$, $com_{ui} = g^{\gamma} h^{\beta_i}$. com_i and com_{ui} are stored in the HES and SM_i, respectively.

Mutual Authentication – In this phase of the protocol, Okamoto protocol is used for mutual authentication between the HES and SM_i. Following procedure presents what is done in this phase:

1- SM_i chooses y, s at random and sends $d = g^{y} h^{s}$ to the HES.

2- Upon receiving d, the HES randomly chooses y', s' and e (as a challenge), computes $d' = g^{y'}h^{s'}$ and returns the tuple (d', e) to the SM_i.

3- SM_i chooses a random value e' (as a challenge), computes the values $u = y + e\alpha_i$ and $v = s + e\beta_i$ and sends the tuple (u, v, e') to the HES.

4- The HES authenticate the SM_i if and only if $g^u h^v = d(com_i)^e$.

5- The HES computes $u' = y' + e'\gamma$, $v' = s' + e'\beta_i$ and sends the tuple (u', v') to the SM_i.

6- Finally, SM_i authenticate the HES, if and only if $g^{u'}h^{v'} = d'(com_{ui})^{e'}$.

Key Exchange – After mutual authentication of the HES and SM_i, the key exchange phase is started as follows:

1- The long term key s_i is generated by applying H_2 to $(g^{\beta_i}, h^{\gamma})$. In each party, one of the parameters is already stored and the other one is computed online. Thus, there is no need to store the key, s_i, in the database.

2- For generating the session key k_i between the HES and SM_i, H_3 is applied to tuple (u, u', s_i) which u and u' are the random values computed in 3rd and 5th steps of the Mutual Authentication phase, respectively.

3- The HES selects a random value N_i and encrypts the value (N_i, u) by k_i. Then, $E_{k_i}(N_i, u)$ is sent to SM_i.

4- SM_i replies with $E_{k_i}(N_i + 1)$ to the HES.

If the 3rd and 4th steps of this phase is carried out successfully, the HES and SM_i can be sure that both of them have the same key (k_i). They can use the shared key to establish a secure communication with each other.

It must be noted that the same procedure can be done for creating the access level passwords.

4.2 Authenticated Broadcast Messaging Protocol

In addition to unicast messaging, the Head-End System sometimes needs to broadcast messages, such as firmware updates and control messages, to all of the Smart Meters [25].

We utilize hash chain idea and a modified version of Schnorr protocol for proposing an authenticated broadcast messaging protocol for the AMI systems. In the proposed protocol, the HES is authenticated by the Smart Meters; so, they can be assured that the received message is broadcasted by the HES. The protocol consists of three phases (Fig. 3):

Initialization – Similar to initialization phase of the authenticated key exchange protocol, the Utility initializes the system by executing the setup phase of the Pedersen Commitment scheme. Also, it defines $H_4\colon \{0,1\}^* \to \mathbb{F}_p$ and $H_5\colon \mathbb{F}_p \to \mathbb{F}_p$.

Registration – C_k is applied to PUF_{HES} to get its response, $R_u = PUF_{HES}(C_k)$. The parameter δ is generated by applying H_1 to R_u and the commitment $com_u = g^{\delta}$ is computed. Also, z_0 is generated by L times successive application of H_5 on δ (i.e. $z_0 = H_5^L(\delta) = \underbrace{H_5(H_5\left(H_5(\ldots(\delta))\right))}_{L\ times}$), where L can be the number of the messages which may be broadcasted along a specific duration. This number is in an acceptable range. For example, if we assume that at most 10 messages may be broadcasted to Smart Meters each day, the maximum number of broadcasting messages will be $10 \times 365 \times 10 = 36500$ for 10 years. In this case, the value of L will be 36500. Finally, com_u and z_0 are stored in all of the Smart Meters which are in connection with the HES.

Authentication – For broadcasting the message (M), the HES runs the Schnorr protocol to reveal its commitment to Smart Meters as follows:

1- The HES selects a random number r and generates z_j by $L - j$ times successive application of H_5 on δ and computes $y = g^r$. It, also, computes $c = H_4(M)$ and $w = r + z_j c\delta$. Then, the HES broadcasts the tuple (z_j, y, M, w) to the Smart Meters.

2- Each of the Smart Meters computes $c = H_4(M)$ and authenticates the HES and the received message if and only if $z_{j-1} = H_5(z_j)$ and $g^w = y(com_u)^{z_j c}$. Thus, the Smart Meters will be assured that the message is valid and broadcasted by the HES.

5 Security Analysis

The proposed protocols are based on the Okamoto and Schnorr protocols and can keep most of their benefits such as resistance against active and passive attacks. Also, because of utilizing Physical Unclonable Functions (PUFs) in both communicating parties, there is no need to store secret values securely. This solution makes the protocols strong against the physical attacks. In this section, we model an adversary and analyze the security of the proposed protocols. Dolev and Yao [37] proposed a framework to model behavior of an adversary in cryptographic protocols. In their framework, the adversary has the ability to record, delete, re-play, re-rout, re-order and re-schedule all the messages transmitted between the honest parties and the adversary [38]. Also, the main security requirement for authenticated key exchange protocols has been introduced by Bellare and Rogaway [39]. These are further refined by Bellare, Pointcheval and Rogaway [40] and Canetti and Krawczyk [41]. In their proposed adversary model, the adversary has full control on all the communications and can corrupt some of the parties. Also, the adversary pick out honest parties to take part in key-exchange sessions [42].

5.1 Adversary Model

We consider following adversary model for analyzing the security of our proposed protocols.

In this model, the adversary can be either one of the authorized meters that has been corrupted by a malicious adversary or an external adversary which performs attacks from outside of the network.

Objectives – The adversary perform an attack to Gain access to the system resources or any of the keys.

Capabilities – We assume the adversary has a complete knowledge about:

- The topology of the network
- The detail design of the proposed protocols
- The public parameters such as (G, p, g, h)
- The messages transmitted between two parties

Also, we assume that the adversary has physical access to all of the Smart Meters and can corrupt them.

5.2 Security Analysis: Authenticated Key Exchange Protocol

Considering the introduced adversary model, our authenticated key exchange protocol satisfies the following requirement:

5.2.1 Secure Key Generation

In the proposed protocol, the long term key (s_i) is generated by each of the communication parties (Smart Meters and HES). This is achieved through applying a secure hash function on $(g^{\beta_i}, h^{\gamma})$ where only one of the parameters β_i or h^{γ} is stored in each of communication parties and the other one is computed by the responses of party's PUF device at the moment. For example, in the HES side, β_i is stored in its database and γ is generated by its PUF.

The uniqueness of the PUF response to a specific challenge, applying a hash function and also, no need to store all the key materials, ensure the high security of the long term key (s_i).

Also, the session key (k_i) is created by applying a suitable hash function on tuple (u, u', s_i) where s_i and random values, u and u', are generated at the current session without storage requirement. Therefore, the session key is unpredictable, as well.

5.2.2 Key Freshness

Freshness requires that the session key is generated at the moment and no other party has used it before.

In our proposed protocol, the session key (k_i) is equal to $H_3(u, u', s_i)$ and is established at the moment between the HES and a Smart Meter. Thus, the session key is always fresh.

5.2.3 Forward and Backward Security

Forward and backward security means that a compromised session key only affect its session and does not put the other sessions in risk.

Similar to discussion on the previous requirements, since k_i is equal to $H_3(u, u', s_i)$ and u, u' are random values generated during each run of the authentication protocol, no information is leaked about the other session keys by compromising it.

5.2.4 Known Key Resilience

In each protocol with this property, the compromise of a session key in one session should not impose any information about the long term keys of other parties.

In the proposed protocol, the long term key $s_i = H_2(g^{\beta_i}, h^{\gamma})$ is only dependent on responses of the PUF_{HES} and the PUF_{SM_i} and k_i is equal to $H_3(u, u', s_i)$. The applied hash function, H_3, is one-way and non-invertible. Therefore, gaining access to the long term key by obtaining the session key is infeasible.

5.2.5 Collusion Resistance

The property requires that colluding users cannot obtain keys which they are not allowed to obtain individually.

The only parameter which is stored in each of the Smart Meters is h^{γ} and the other parameter, β_i, is computed by applying a hash function on the response of PUF_{SM_i} which is unique for each Smart Meter. Therefore, the generated $s_i = H_2(g^{\beta_i}, h^{\gamma})$ is unique for each Smart Meter and obtaining the information stored or produced in some of the Smart Meters does not leak any information about the long term and session keys of other Smart Meters.

5.2.6 Explicit Key Authentication

The property of explicit key authentication is obtained when one party is assured that only the other authenticated party really has knowledge or possession of the exchanged key. This property may be either mutual or unilateral.

In our proposed protocol, if mutual authentication phase is completed successfully, then the HES and the Smart Meter authenticate each other and produce a similar key based on the generated parameters. The key confirmation property is achieved by exchanging some encrypted messages between the HES and the Smart Meter. Thus, the explicit key authentication property is achieved by providing key authentication and key confirmation features.

5.3 Security Analysis: Authenticated Message Broadcasting Protocol

Our proposed protocol for message broadcasting is based on hash chain idea and a modified version of Schnorr protocol. This protocol authenticates the HES, which is responsible for broadcasting the critical commands to the smart meters. In this protocol, both of the HES and its broadcasted message are authenticated by the Smart Meters. Therefore, a dishonest party cannot impersonate himself as a HES.

An adversary must have δ to impersonate himself as HES. This parameter, δ, is equal to $H_1(PUF_{HES}(C_k))$ and can only be produced by the HES. In our adversary model, the adversary has not the capability of corrupting the HES, so, he/she can not obtain δ in this way. The stored or transmitted parameters which can be used by an adversary for obtaining δ are $com_u = g^{\delta}$, $z_0 = H_5^L(\delta)$, $z_j = H_5^{L-j}(\delta)$ and $w = r + z_j c\delta$ which obtaining δ from each of them is equal to solving the discrete logarithm problem or finding a preimage of the one-way hash function or solving a equation with two unknowns.

6 Discussion

As mentioned, developing a secure key management scheme for the AMI network is an important issue. To the best of our knowledge, there is no key establishment scheme in literatures which satisfy all the requirements of an appropriate one for the AMI. In all of the proposed schemes except [25], some important secret values are stored in the Smart Meters and since they are located in an insecure physical environment, they are considerably vulnerable to physical attacks. Although, the proposed scheme in [25] is immune against these attacks, it does not provide authentication of the HES, key confirmation between HES and Smart Meters and a solution for message broadcasting which are critical issues in the AMI networks.

Considering the system constraints and security requirements in the AMI networks and exploiting the intrinsic characteristics of PUF devices, we proposed a secure authenticated key exchange scheme and an authenticated message broadcasting protocol based on two well-known protocols: Okamoto and Schnorr.

The prototype implementation of PUF-enabled Smart Meters by Nabeel et al. [25] shows that the scheme is practical and efficient for providing a secure end-to-end communication.

The computational constraints, storage constraints and life spans of Smart Meters were also considered in designing the protocols. Table 1 shows the necessary stored data in the HES and each Smart Meter. For running the authenticated message broadcasting protocol, a Smart Meter only needs to store two parameters and computes three modular exponentiations which is completely practical for it. Thus, the protocol can be classified in the category of efficient message broadcasting protocols. Also, running the authenticated key exchange protocol requires a Smart Meter to compute some hash functions and modular exponentiations and again, store only one parameter which is applicable for Smart Meters. We utilized Okamoto and Schnorr protocols in our proposed protocols which their security is based on Discrete Logarithm Problem (DLP) assumption. Therefore, the proposed protocols are secure in life span of Smart Meters as long as the quantum computers has not been appeared.

The security analysis of the proposed authenticated key exchange protocol shows that it provides all the requirements of a secure one. Also, we showed that our authenticated message broadcasting protocol is secure against corrupted Smart Meters.

7 Conclusion

Developing a secure key management scheme for the AMI network is a major challenge. In this paper, two cryptographic protocols are proposed for the Advanced Metering Infrastructure (AMI) systems. To the best of our knowledge, our proposed key establishment scheme is the first proposed method which satisfies all the requirements of an appropriate scheme for the AMI.

References

[1] W. Wang and Z. Lu, "Survey Cyber security in the Smart Grid: Survey and challenges," *Comput. Netw.*, vol. 57, pp. 1344-1371, 2013.

[2] P. Jokar, N. Arianpoo, and V. C. M. Leung, "A survey on security issues in smart grids," *Security and Communication Networks,* pp. n/a-n/a, 2012.

[3] U. NIST, "Guidelines for smart grid cyber security (vol. 1 to 3)," *NIST IR-7628, Aug,* 2010.

[4] EPRI, "Cryptographic Key Management (CKM) Design Principles for the Advanced Metering Infrastructure (AMI)," Electric Power Research Institute (EPRI) 1024431, 2012.

[5] R. Anderson and M. Kuhn, "Tamper resistance: a cautionary note," presented at the Proceedings of the 2nd conference on Proceedings of the Second USENIX Workshop on Electronic Commerce - Volume 2, Oakland, California, 1996.

[6] R. J. Anderson and M. G. Kuhn, "Low Cost Attacks on Tamper Resistant Devices," presented at the Proceedings of the 5th International Workshop on Security Protocols, 1998.

[7] B. Schoenmakers, "Cryptographic Protocols," ed, 2013.

[8] S. P. Skorobogatov, "Semi-invasive attacks-a new approach to hardware security analysis," *Technical report, University of Cambridge, Computer Laboratory,* 2005.

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

[10] X. Jinyue and W. Yongge, "Secure Key Distribution for the Smart Grid," *Smart Grid, IEEE Transactions on,* vol. 3, pp. 1437-1443, 2012.

[11] H. Nicanfar and V. C. M. Leung, "Smart grid multilayer consensus password-authenticated key exchange protocol," in *Communications (ICC), 2012 IEEE International Conference on*, 2012, pp. 6716-6720.

[12] L. Yee Wei, M. Palaniswami, G. Kounga, and A. Lo, "WAKE: Key management scheme for wide-area measurement systems in smart grid," *Communications Magazine, IEEE,* vol. 51, pp. 34-41, 2013.

[13] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Efficient Authentication and Key Management Mechanisms for Smart Grid Communications," *Systems Journal, IEEE,* vol. 8, pp. 629-640, 2014.

[14] H. Nicanfar, P. Jokar, and V. C. M. Leung, "Smart grid authentication and key management for unicast and multicast communications," in *Innovative Smart Grid Technologies Asia (ISGT), 2011 IEEE PES*, 2011, pp. 1-8.

[15] J. Kamto, Q. Lijun, J. Fuller, and J. Attia, "Light-weight key distribution and management for Advanced Metering Infrastructure," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, 2011, pp. 1216-1220.

[16] Z. Fangming, Y. Hanatani, Y. Komano, B. Smyth, S. Ito, and T. Kambayashi, "Secure authenticated key exchange with revocation for smart grid," in *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, 2012, pp. 1-8.

[17] K. Jincheol, A. Seongji, K. Youngeok, L. Kidong, and K. Sangjin, "Sensor network-based AMI network security," in *Transmission and Distribution Conference and Exposition, 2010 IEEE PES*, 2010, pp. 1-5.

[18] W. Dapeng and Z. Chi, "Fault-Tolerant and Scalable Key Management for Smart Grid," *Smart Grid, IEEE Transactions on,* vol. 2, pp. 375-381, 2011.

[19] C. Beaver, D. Gallup, W. Neumann, and M. Torgerson, "Key management for SCADA."

[20] R. Dawson, C. Boyd, E. Dawson, J. M. Gonz, #225, and l. Nieto, "SKMA: a key management architecture for SCADA systems," presented at the Proceedings of the 2006 Australasian workshops on Grid computing and e-research - Volume 54, Hobart, Tasmania, Australia, 2006.

[21] C. Donghyun, K. Hakman, W. Dongho, and K. Seungjoo, "Advanced Key-Management Architecture for Secure SCADA Communications," *Power Delivery, IEEE Transactions on,* vol. 24, pp. 1154-1163, 2009.

[22] C. Donghyun, L. Sungjin, W. Dongho, and K. Seungjoo, "Efficient Secure Group Communications for SCADA," *Power Delivery, IEEE Transactions on,* vol. 25, pp. 714-722, 2010.

[23] H. Wenbo, H. Ying, R. Sathyam, K. Nahrstedt, and W. C. Lee, "SMOCK: A Scalable Method of Cryptographic Key Management for Mission-Critical Wireless Ad-Hoc Networks," *Information Forensics and Security, IEEE Transactions on,* vol. 4, pp. 140-150, 2009.

[24] L. Nian, Z. Jianhua, and L. Wenxia, "Toward Key Management for Communications of Wide Area Primary and Backup Protection," *Power Delivery, IEEE Transactions on,* vol. 25, pp. 2030-2032, 2010.

[25] M. Nabeel, S. Kerr, D. Xiaoyu, and E. Bertino, "Authentication and key management for Advanced Metering Infrastructures utilizing physically unclonable functions," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, 2012, pp. 324-329.

[26] A. Perrig, R. Canetti, D. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol," ed, 2002.

[27] O. Consortium, "Report on the identification and specification of functional, technical, economical and general requirements of advanced multi-metering infrastructure, including security requirements," ed: Deliverables, 2009.

[28] ASAP-SG, "Security profile for Advanced Metering Infrastructure," The Advanced Security Acceleration Project (ASAP-SG) Version 2.1, 2012.

[29] S. Ganguly, S. Panda, A. C. Dhandapani, and G. Mallappan, "Efficient encryption and key management in advanced metering infrastructure," ed, 2011.

[30] X. Wang, W. Gu, K. Schosek, and S. Chellappan, "Sensor network configuration under physical attacks," *International Journal of Ad Hoc and Ubiquitous Computing,* vol. 4, pp. 174-182, 2009.

[31] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology—CRYPTO'91*, 1992, pp. 129-140.

[32] E. Bangerter, J. Camenisch, S. Krenn, A.-R. Sadeghi, and T. Schneider, "Automatic Generation of Sound Zero-Knowledge Protocols," *IACR Cryptology ePrint Archive,* vol. 2008, p. 471, 2008.

[33] Y. Seurin, "On the exact security of schnorr-type signatures in the random oracle model," in *Advances in Cryptology–EUROCRYPT 2012,* ed: Springer, 2012, pp. 554-571.

[34] T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," in *Advances in Cryptology—CRYPTO'92*, 1993, pp. 31-53.

[35] P. Kitsos and Y. Zhang, *RFID security: techniques, protocols and system-on-chip design*: Springer, 2008.

[36] U. Maurer, "Unifying zero-knowledge proofs of knowledge," in *Progress in Cryptology–AFRICACRYPT 2009*, ed: Springer, 2009, pp. 272-286.

[37] D. Dolev and A. C. Yao, "On the security of public key protocols," *Information Theory, IEEE Transactions on,* vol. 29, pp. 198-208, 1983.

[38] H. Nicanfar and V. C. Leung, "Multilayer consensus ECC-based password authenticated key-exchange (MCEPAK) protocol for smart grid system," *Smart Grid, IEEE Transactions on,* vol. 4, pp. 253-264, 2013.

[39] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in *Advances in Cryptology—CRYPTO'93*, 1994, pp. 232-249.

[40] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Advances in Cryptology—Eurocrypt 2000*, 2000, pp. 139-155.

[41] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Advances in Cryptology—EUROCRYPT 2001*, ed: Springer, 2001, pp. 453-474.

[42] K. Lauter and A. Mityagin, "Security analysis of KEA authenticated key exchange protocol," in *Public Key Cryptography-PKC 2006*, ed: Springer, 2006, pp. 378-394.

Table 1. The Data Stored in The Head-End System (HES) and each Smart Meter (SM_i)

	The Head-End System (HES)	Smart Meter i (SM_i)
Authenticated Key Exchange Protocol	$\boldsymbol{\beta_i}$, $\boldsymbol{com_i}$ ($\boldsymbol{i = 1, 2, \dots, n}$), $\boldsymbol{n}$ is the number of smart meters	$\boldsymbol{com_{ui}}, \boldsymbol{h^{\gamma}}$
Authenticated Message Broadcasting Protocol	-	com_u, z_0