Physical Unclonable Function Based Authentication Protocol for Unit IoT and Ubiquitous IoT

Min Zhao, Xuanxia Yao, Huansheng Ning
University of Science and Technology Beijing (USTB)
Beijing, 100083, China
ninghuansheng@ustb.edu.cn

Hong Liu
Research Institute, Run Technologies Company, Ltd.
Beijing 100192, China

***Abstract*—Unit and Ubiquitous IoT (U2IoT) is a typical IoT architecture for achieving comprehensive interactions of ubiquitous things. In U2IoT, security becomes a challenging issue due to objects' complicated interactive phases. The object in different phases of being mapped from the physical space to the cyber space has different security requirements. In this work, a concept of Object Life Cycle (OLC) is first proposed to describe the security requirements for the objects' physical access, cyberentity, and physical extinction phase in U2IoT. Meanwhile, considering the variety of objects and related diversity resources, Physical Unclonable Function (PUF) is introduced to design a lightweight mutual authentication protocol for a smart home scenario. The design correctness and formal security are proved based on the BAN-logic. It indicates that the proposed protocol satisfies the main security requirements for the object during the physical access phase.**

Keywords—Unit and Ubiquitous IoT, Physical Unclonable Function, Object Life Cycle, Authentication, BAN logic

I. INTRODUCTION

Internet of Things (IoT) is a system paradigm that combines a variety of sensing, networking, and computing equipment with the Internet, the aim of that whenever or wherever thing to thing, human to thing, human to human can widely and closely interconnect. It has wide applications including Smart City, Smart Grid, Intelligent Healthcare, and Intelligent Transportation. Researchers have provided various kinds of IoT architectures, including Unit and Ubiquitous IoT (U2IoT) [1], PECES [2], SENSEI [3], FIA [4] etc. Especially, the U2IoT architecture is a typical architecture for ubiquitous things and is established for the future IoT [1]. It refers to unit IoT as a single application and ubiquitous IoT aggregating multiple unit IoTs. Meanwhile, U2IoT shows some features, for example, 1) ubiquitous connection, things should connect into a network anytime, anywhere. 2) intelligent behavior, things have the ability of self-organization and self-adaptation. 3) green applications, resource-conserving is proposed to adapt to the sustainable development. 4) seamless connectivity, things or human can realize widely and closely interconnection. 5) thing-oriented services, automatic unmanned environment is developing with smart world. However, security issues under future IoT are becoming more important with the automatic and intelligent interaction of objects [5], [6], [7].

There are many works that focus on the IoT security issues [8], [9], [10], [11], [12]. The current solutions have the following main limitations: 1) Focusing on people attributes [6], [8] without emphasizing the devices' attributes (e.g., state, space-time, and interaction behavior). 2)Paying mainly attention to the specific application security [9], [10], and seldom considering the security issues during the mapping process from the physical world to the cyber word. 3) Lacking mutual authentication between the devices in certain heterogeneous networks [12], [17], [18]. Meanwhile, lightweight protocols become the trend for resource-constraint devices [11], [13]. Therefore, it is necessary to design an efficient authentication protocol to realize security protection for the U2IoT with objects' attributes considerations.

In the IoT applications, Physical Unclonable Function (PUF) can be applied for making an object's fingerprint. It means that a PUF expresses an instance-specific feature of a physical object with inherence and unclonability [14]. Existing PUF based security solutions are mainly applied in RFID systems [15], [16], [17], [18]. There are rare protocols that can realize mutual authentication among more than two PUF devices. The communication between two PUFs is not explored enough and lacks security protection for the Object Life Cycle (OLC).

In this paper, the main purpose is designed PUF based authentication protocol for smart devices in the physical access phase. The main contributions are as follows:

1) A new concept of OLC is proposed to describe the process of object from manufacture to discard in the U2IoT, and is for solving the security issues during physical-cyber space mapping.

2) PUF is used to implement authentication between smart devices. A mutual authentication protocol is designed for object in the physical accessing.

3) Dynamic IDs are applied to protect the security of device information.

The rest of the paper is organized as follows. Section II reviews the related work in authentication scheme for IoT. Section III presents the system model, and introduces the concept of OLC. Section IV describes the designed protocols. Design correctness and formal security is proved based on BAN logic in section V. Finally, section VI draws a conclusion.

II. RELATED WORK

Ning et al. [12] pointed out that previous solutions for IoT security are not competent. The security issues in the U2IoT architecture must be considered. The authors proposed a

hierarchical authentication scheme for the U2IoT, in which aggregated proofs were established for the anonymous data transmission, homomorphism functions were established to realize secure interactions, and lightweight mechanisms were established to complete mutual authentication.

Tuyls et al. [15] proposed PUF based off-line authentication for RFID-tags, which combined standard identification scheme and standard signature scheme. In the authentication, the tag generated a secret key by the response of PUF and helper data. Subsequently, the verifier authenticated the tag by its certificate and identity.

Kulseng et al. [16] pointed out that traditional cryptosystems are infeasible for the low-cost RFID systems. And the tags in RFID systems faced forgery, learning and tracking attacks. Therefore, the authors proposed tag search protocols based on Linear Feedback Shift Registers (LFSR) and PUF. They regarded the tags as PUF devices, used LFSR to realize the secure communication and used challenge-response pairs to implement the authentication of the tags' identities.

Van Herrewege et al. [19] established a mutual authentication scheme for RFID based on the reverse fuzzy extractor, which got rid of expensive error correction mechanism to meet resources-constrained PUF-enabled devices. The core of this authentication scheme corrected the reference response of the database to the measured response. In this scheme, the response was protected by the hash function, and the mutual authentication was realized by the hash value of the response.

Oztiirk et al. [20] presented a noisy PUF based authentication scheme for low-cost devices. It made the scheme lightweight by omitting the cryptographic hash functions, and it limited attacker to access challenge-response pairs by an internal secret vector to prevent the attacks from forging a reader. Generated response was used to demonstrate the identity of the tag.

Currently, PUF is widely applied to device authentication due to inherent advantages (e.g., light-weight, unpredictability, unclonability and tamper-proof). These schemes mainly realize authentication through challenge-response pairs (CRPs). However, most of them cannot protect information of CRPs and combine well with standard security technologies. In this work, a base point of elliptic curve and dynamic ID are applied to solve these problems.

III. SYSTEM MODEL

A. Object Life Cycle in U2IoT

In the U2IoT, there are three layers [7]: sensor and actuator layer, network layer and application layer. Things in the U2IoT exist in the physical world as physical objects and in the cyber world as cyber entities. Cyberentity interaction is divided into three phases: preactive phase, active phase and postactive phase. In this paper, the cyberentity interaction is extended around a physical object's lifecycle, and OLC is established with security requirements considerations.

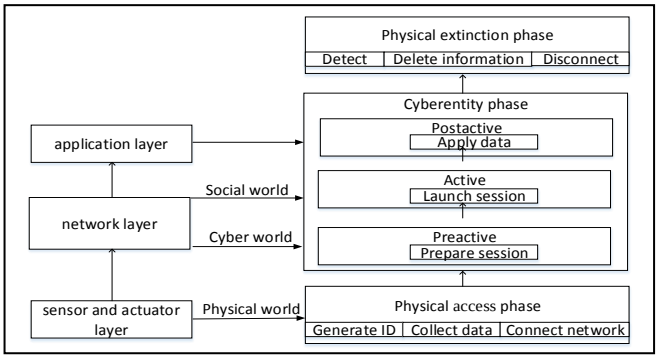

Fig. 1. Three phases of the OLC in the U2IoT.

Fig. 1. Show the three phases of OLC. Thereinto, physical access phase is the process from the physical world to the cyber world. Cyberentity phase is the period as cyber entity. Physical extinction phase is the state out of use.

Physical access phase mainly involves ID creation, response excitation and network access. The main requirements include: 1) Identification: An identity is created to uniquely identify the device, communicate with other devices, and prevent from forging and eavesdropping. 2) Mutual authentication: The illegal devices should not pass the verification and make sure only legal devices can access the network. Meanwhile, the network also is verified. 3) Forward security: Attackers cannot derive the CRPs in previous session since even if they know the corresponding CRPs of the current session. 4) Privacy preservation: The communication cannot disclose a device's privacy information (e.g., CRPs, attributes).

Cyberentity phase involves the interactions of cyber entities, which includes parameter preparation, data transmission and data sharing. Thereinto, key distribution, access control, signature algorithms, data aggregation and intrusion detection can be used in this phase for security protection and privacy.

Physical extinction phase includes identity verification and access authorization revoking. The following requirements are considered. 1) Identity recognition: The fake/forged identity should be identified, and detect the identity that is no longer used. 2) Device identification: The device is out of use that should be affirmed and removed from the smart home. 3) Data elimination: If a smart device is used no longer. The related information should be cleared for data security protection. 4) Access control: The authorization of a smart device in the physical extinction phase should be canceled so that the devices cannot re-access the network.

Considering above security requirements, a physical unclonable function based authentication protocol is designed in the physical access phase for U2IoT. In addition, our protocol's lightweight and protection from bottom are appropriate for the characteristics of U2IoT.

B. Scenario Model

Fig.2. shows a specific scenario smart home which consists of wearable devices and five intelligent PUF devices: smart ring, intelligent lock, smart camera, intelligent light, smart toaster and smart TV. Besides, a home gateway is regarded as a data center, which can configure and store data into secure

database. The gateway is analogous to the management and data center (M&DC) in unit IoT for controlling smart devices. A smart ring controls or monitors other smart devices. Since there is usually more than one member in a home, the smart devices may be controlled by several smart rings. Meanwhile, one smart ring can exist in the home, and it also can be used for remote control.

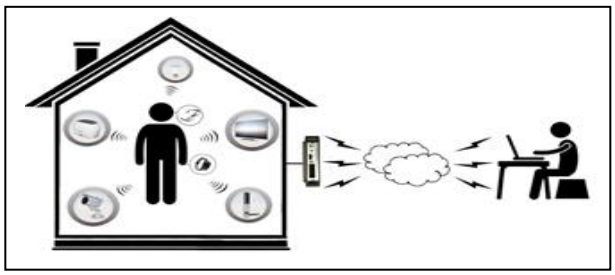

Fig. 2. Scenario model of the smart home.

IV. PROTOCOL DESCRIPTION

In this paper, an authentication protocol is designed for objects in the physical accessing phase， whose framework show in fig.3. .And TABLE 1 shows the main notations.

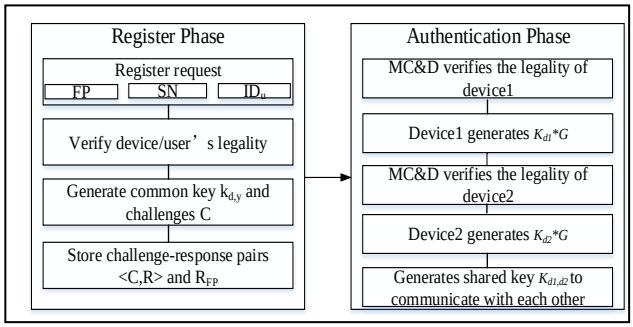

Fig. 3. framework for our protocol.

TABLE I. NOTATION AND SIGNIFICANCE

Notation	***Significance***
ID_x	The *ID* of x
r	A smart ring
l	A intelligent light
u	A legal user
d	A smart device in the home network
$<C,R>$	A pair of challenge response
C_x	A challenge for smart device x's PUF
R_x	A response corresponding to C_x from x's PUF
G	The base point of elliptic curve
p	A large prime number
n	The order of base point G
N_x	A random number for x
$K_{A,B}$	The shared key between A and B
SN	The serial number of a smart device
FP	The fingerprint or a unique secret data of a user
K_x	The partial key generated by the smart device x

A. Premises

For the sake of illustrating the protocols, there are several assumptions as follows.

1) The gateway is considered to be a trusted one in a home network, who is responsible for making access control on other entity and help other entity to do mutual authentication.

2) It is assumed that all the smart devices have the function of accepting input and the smart ring has the function of fingerprint recognition.

3) The legal users' fingerprints or unique secret data have been recorded in the gateway. Each legal user has a shared key $K_{u,g}$ with the gateway, which can be preloaded in the gateway in advance and can be changed offline or online in the future.

4) Each smart device has a PUF. And the initial pairing between the new smart device and other smart devices or the gateway is accomplished with the help of a legal user. A secure sketch [21] used to recompile the responses from the same challenge to the same one is configured in the PUF devices

5）The device's *ID* is variable, and its generating process follows the following rules:

•The initial *ID* of a device is generated from its serial number *SN*, $ID=hash(SN)$.

•Subsequent *ID* is derived from the device's $<C,R>$.

•It is assumed that one $<C,R>$ pair is selected to generate the device's *ID*. The new $ID = h(R)$.

6) An elliptic curve $Ep(a,b)$ over finite field $Z_p = \{0,1,\ldots,p-1\}$is selected. p is a large prime. G is the base point of the elliptic curve. n is the order of G, which is a big integer. This elliptic curve is used to protect keys.

B. The Authentication protocol for the Physical Access Phase

Register phase: All smart devices want to join in the home network should register to the gateway. The register phase needs a legal user's participation so as to prove it is a legal device. The register phase done by a smart device itself consists of following 4 steps.

Step 1, the smart device or user sends a register request message "$E(K_{u,g},SN||FP||N_1)||ID_u||hash(N_1)$" to the gateway.

Step 2, the gateway decrypts "$E(K_{u,g},SN||FP||N_1)$" and checks whether the FP is a legal one of ID_u in its database and *SN* is not exist. If the *FP* is legal and SN doesn't exist, it generates a common key $K_{d,g}$ with the device and registers the SN in its database. Besides, the gateway generates a challenge set C of the smart device. Sends "$E(K_{u,g},FP||K_{g,d}||N_1||N_2||C)||hash(N_2)$" to the smart device.

Step 3, the smart device uses its PUF to generate responses R_{FP} according to the user's *FP*. And also produces responses according to the challenge set. Then sends "$E(K_{d,g},R_{FP}||N_1||N_2||<C,R>)$" to the gateway.

Step 4, the gateway decrypts "$E(K_{d,g},R_{FP}||N_1||N_2||<C,R>)$" and verifies the device by N_1 and N_2, if it passes the

verification, stores R_{FP} and these challenge response pairs in its database.

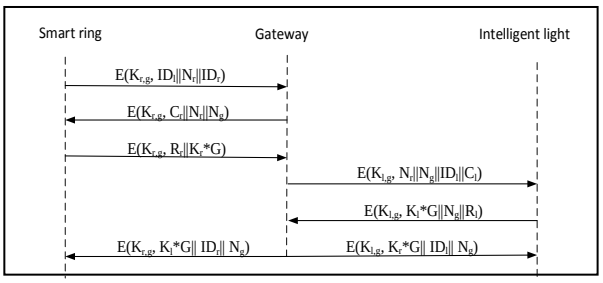

Fig. 4. Mutual authentication between smart ting and intelligent light.

Authentication phase: Any a smart device can join the home network to communicate with others after registering to the gateway. Before communicating with each other, mutual authentication and a shared key are necessary. We take the interaction between smart ring and intelligent light as an example to illustrate the mutual authentication protocol and key agreement, which is shown in Fig. 4.

Step 1, the smart ring generates a random number N_r and sends "$E(K_{r,g},ID_l ||N_r ||ID_r)$" to the gateway.

Step 2, the gateway choose a challenge C_r from the database according to ID_r and generates a random number N_g, sends "$E(K_{r,g},C_r ||N_r ||N_g)$" to the smart ring.

Step 3, the smart ring decrypts the message "$E(K_{r,g},C_r ||N_r ||N_g)$". If the N_r is correct, the gateway passes the authentication. And then it generates R_r, R_{Nr}, R_{Ng}, according to C_r, N_r and N_g respectively. Updates its ID with $hash(R_r)$, calculates $Kr=(R_{Nr}*R_{Ng}) \ mod \ p$, and sends "$E(K_{r,g},R_r ||K_r*G)$" to the gateway.

Step 4, the gateway decrypts the message "$E(K_{r,g},R_r ||K_r*G)$" and gets the R_r and K_r*G. The smart ring is authenticated by comparing the $< C_r,R_r >$ with the stored one, if they are identical, the smart ring passes the authentication. The gateway updates the smart ring's ID with $hash(R_r)$, and chooses a challenge C_l from the database and sends "$E(K_{l,g},N_r||N_g||ID_l||C_l)$" to the intelligent light or broadcasts it to the home network.

Step 5, intelligent light decrypts "$E(K_{l,g},N_r||N_g||ID_l||C_l)$". If the ID_l is its current ID, the gateway passes light's authentication. It generates R'_{Nr}, R'_{Ng} and R_l according to N_r, N_g and C_l respectively. Updates its ID with $hash(R_l)$, calculates $K_l=(R'_{Nr}*R'_{Ng}) \ mod \ p$, and sends "$E(K_{l,g},K_l*G||N_g \ ||R_l)$" to the gateway.

Step 6, the gateway authenticates the intelligent light by comparing the $<C_l,R_l>$ with the stored one, if they are identical, the intelligent light passes the authentication. The gateway updates the smart light's ID with $hash(R_l)$. Sends "$E(K_{l,g},K_r*G||ID_l||N_g)$" to the intelligent light and "$E(K_{r,g},K_l *G|| ID_r||N_g)$" to the smart ring.

Step 7, the intelligent light decrypts "$E(K_{l,g},K_r*G|| ID_l||N_g)$". If the ID_l is its current ID, calculates $K_{r,l}= ((K_l *K_r)*G)_x$. The smart ring decrypts "$E(K_{r,g},K_l*G|| ID_r ||N_g)$". If the ID_r is its current ID, calculates $K_{r,l}=((K_l *K_r)*G)_x$. The subscript x denotes the x axis of point.

The mutual authentication and key agreement are done by the help of gateway. The authentication among other smart devices is similar to the authentication between smart ring and the intelligent light.

V. PROTOCOL ANALYSIS

A. Formal Analysis with BAN Logic

1) The messages for the authentication protocol in physical access phase

This protocol mainly involves three principals. A denotes smart ring, B denotes intelligent light, and S denotes the home gateway.

A->S: $\{ID_l, N_r, ID_r\}K_{r,g}$; S->A: $\{C_r, N_r, N_g\}K_{r,g}$;

A->S: $\{R_r, K_r*G\}K_{r,g}$; S->B: $\{N_r, N_g, ID_l, C_l\}K_{l,g}$;

B->S: $\{K_l*G, N_g, R_l\}K_{l,g}$; S->A: $\{K_l*G, ID_r, N_g\}K_{r,g}$;

S->B: $\{K_r*G, ID_l, N_g\}K_{l,g}$.

2) Message Formalization

Message formalization is used to idealize the protocol message.

M1 A->S: $\{N_r, A \xleftrightarrow{K_{r,g}} S\}K_{r,g}$;

M2 S->A: $\{N_r, S \xleftrightarrow{K_{r,g}} A\}K_{r,g}$;

M3 A->S: $\{R_r, K_r*G, A \xleftrightarrow{K_{r,g}} S\}K_{r,g}$;

M4 S->B: $\{ID_l, S \xleftrightarrow{K_{l,g}} B\}K_{l,g}$;

M5 B->S: $\{K_l*G, R_l, B \xleftrightarrow{K_{l,g}} S\}K_{l,g}$;

M6 S->A: $\{K_l*G, A \xleftrightarrow{K_{r,g}} S\}K_{r,g}$;

M7 S->B: $\{K_r*G, S \xleftrightarrow{K_{l,g}} B\}K_{l,g}$.

3) Initial Assumptions

In the authentication protocol, the devices in the smart home believe the numbers are random and the keys are secret. The shared keys only are known by corresponding two devices.

For A:

I1: $A|\equiv \#(N_r)$; I2: $A|\equiv A \xleftrightarrow{K_{r,g}} S$;

I3: $A|\equiv (S|\Rightarrow C_r)$; I4: $A|\equiv \#(N_c)$;

For B:

I5: $B|\equiv B \xleftrightarrow{K_{l,g}} S$; I6: $B|\equiv \#(N_g)$;

For S:

I7: $S \mid\equiv \#(N_g)$; I8: $S \mid\equiv A \xleftrightarrow{K_{r,g}} S$;

I9: $S \mid\equiv B \xleftrightarrow{K_{l,g}} S$; I10: $S \mid\equiv (A \mid\Rightarrow R_r)$.

4) Anticipant Goals

The anticipant goals indicate A believe B's identity and B believe A's identity.

G1: $A \mid\equiv S \mid\equiv N_r$, $S \mid\equiv R_r$, $B \mid\equiv ID_l$, $S \mid\equiv R_l$;

G2: $A \mid\equiv A \xleftrightarrow{K_{r,l}} B$, $B \mid\equiv A \xleftrightarrow{K_{r,l}} B$.

5) Logic Inference

Logic Inference is performed according to the rules of the BAN logic to demonstrate the correctness of the anticipant goals.

For G1:

(1) According to I2 and for the shared key, applying message meaning rule: $\frac{(A \mid\equiv (A \xleftrightarrow{K_{r,g}} S), A \triangleleft \{N_r\} K_{r,g})}{(A \mid\equiv S \mid\sim N_r)}$.

(2) According to I1, 1) and verification rule:

$\frac{(A \mid\equiv \#(N_r), A \mid\equiv S \mid\sim N_r)}{(A \mid\equiv S \mid\equiv N_r)}$, we obtain that $A \mid\equiv S \mid\equiv N_r$.

(3) Due to R_r generated by smart ring's PUF, it is random and unclonable, so $S \mid\equiv \#(R_r)$. For the shared key, applying message meaning rule: $\frac{(S \mid\equiv (A \xleftrightarrow{K_{r,g}} S), S \triangleleft \{R_r\} K_{r,g})}{(S \mid\equiv A \mid\sim R_r)}$.

(4) According to 3) and verification rule: $\frac{(S \mid\equiv \#(R_r), S \mid\equiv A \mid\sim R_r)}{(S \mid\equiv A \mid\equiv R_r)}$.

(5) According to I10, 4) and arbitration rule:

$\frac{(S \mid\equiv (A \mid\Rightarrow R_r), S \mid\equiv A \mid\equiv R_r)}{S \mid\equiv R_r}$, therefore we get that $S \mid\equiv R_r$.

(6) For the shared key, applying I5 and message meaning rule: $\frac{(B \mid\equiv (B \xleftrightarrow{K_{l,g}} S), B \triangleleft \{N_g, ID_l\} K_{l,g})}{(B \mid\equiv S \mid\sim (N_g, ID_l))}$.

(7) Applying I6 and the freshness rule: $\frac{(B \mid\equiv \#(N_g))}{(B \mid\equiv \#(N_g, ID_l))}$.

(8) Applying 6), 7) and the verification rule:

$\frac{(B \mid\equiv \#(N_g, ID_l), B \mid\equiv S \mid\sim (N_g, ID_l))}{(B \mid\equiv S \mid\equiv (N_g, ID_l))}$.

(9) According to 8) and belief rule: $\frac{(B \mid\equiv (N_g, ID_l))}{(B \mid\equiv ID_l)}$, so we obtain $B \mid\equiv ID_l$.

(10) Due to R_l generated by intelligent light's PUF, it is random and unclonable, so $S \mid\equiv \#(R_l)$. According to I9 and for the shared key, applying message meaning rule: $\frac{(S \mid\equiv (B \xleftrightarrow{K_{l,g}} S), S \triangleleft \{R_l\} K_{l,g})}{(S \mid\equiv B \mid\sim R_l)}$.

(11) According to I7, 10) and arbitration rule:

$\frac{(S \mid\equiv B \mid\Rightarrow R_l, S \mid\equiv B \mid\equiv R_l)}{(S \mid\equiv R_l)}$, we obtain that $S \mid\equiv R_l$.

For G2:

(1) According to G1, G realizes the authentication to A and B, also is the transmission center to all smart devices. So there are $A \mid\equiv (S \mid\Rightarrow K_l * G)$ and $B \mid\equiv (S \mid\Rightarrow K_r * G)$. According to the message, we can get $A \triangleleft \{K_l * G\} K_{r,g}$ and $B \triangleleft \{K_r * G\} K_{l,g}$.

(2) According to 1), I2 and I5, for the shared key, applying message meaning rule:

$\frac{(A \mid\equiv (A \xleftrightarrow{K_{r,g}} S), A \triangleleft \{K_l * G\} K_{r,g})}{(A \mid\equiv S \mid\sim K_l * G)}$ and $\frac{(B \mid\equiv (B \xleftrightarrow{K_{l,g}} S), B \triangleleft \{K_r * G\} K_{l,g})}{(B \mid\equiv S \mid\sim K_r * G)}$.

(3) Due to the responses are random and unclonable, so $K_r=(R_{Nr} * R_{Ng})$ *mod p* and $K_l=(R'_{Nr} * R'_{Ng})$ *mod p* also are random. That is to say, $A \mid\equiv \#(K_l * G)$ and $B \mid\equiv \#(K_r * G)$.

(4) According to (2), (3), applying the verification rule:

$\frac{(A \mid\equiv \#(K_l * G), A \mid\equiv S \mid\sim K_l * G)}{(A \mid\equiv S \mid\equiv K_l * G)}$ and $\frac{(B \mid\equiv \#(K_r * G), B \mid\equiv S \mid\sim K_r * G)}{(B \mid\equiv S \mid\equiv K_r * G)}$.

(5) According to 1), there are $A \mid\equiv (S \mid\Rightarrow K_l * G)$ and $B \mid\equiv (S \mid\Rightarrow K_r * G)$. Applying arbitration rule:

$\frac{(A \mid\equiv (S \mid\Rightarrow K_l * G), A \mid\equiv S \mid\equiv K_l * G)}{(A \mid\equiv K_l * G)}$ and $\frac{(B \mid\equiv (S \mid\Rightarrow K_r * G), B \mid\equiv S \mid\equiv K_r * G)}{(B \mid\equiv K_r * G)}$.

(6) Because of $K_{r,l} = ((K_l * K_r) * G)_x$, A and B calculate $K_{r,l}$ by $K_l * G$ and $K_r * G$ respectively. Therefore, $A \mid\equiv K_{r,l}$ and $B \mid\equiv K_{r,l}$. That is to say, $A \mid\equiv A \xleftrightarrow{K_{r,l}} B$ and $B \mid\equiv A \xleftrightarrow{K_{r,l}} B$ are satisfied.

Therefore, the protocol is proven to be correct based on the BAN logic, and mutual authentication between smart devices and the gateway are also achieved.

B. Result Analysis

1) *ID Freshness*

A challenge is chosen randomly from database according to the corresponding device, and then stimulates its PUF to generate response. *ID* is calculated by *ID = h(R)*, which can be changed in the protocol. Therefore, *ID* is fresh and secure.

2) *Identity Identification*

IDs and keys are generated by PUF's response (e.g., *ID = h(R)*, $K_{r,l}=((K_l * K_r) * G)_x$ etc.). Due to the properties of PUF's responses, IDs and keys are unclonable and unpredictable, which can uniquely express a device. Any tries to invade the device that will change the results.

3) *Confidentiality*

The devices authenticate each other with the help of gateway, and this process is encrypted by keys, so transmitted message is secret. Besides, the common key for devices is concealed by the base point G of an elliptic curve, which protects key information from exposing outside. $K_{r,l}$ cannot be known and derived by adversary even the gateway.

4) *Attacks Analysis*

Firstly, the user's fingerprint or unique identifier is as a challenge. An attacker has not the corrected challenge to generate response, which can ensure that the illegal device cannot pass the verification. Second, CRPs are used to prevent impersonate attack. If a physical attacker attempts to probe or model PUF behavior, the challenge-response behavior will change largely. Third, all communications are completed through gateway. An adversary doesn't know which one is interacting. Therefore if an adversary eavesdrop the communication, he will not track any information about challenge-response pairs. Last, due to the random numbers (e.g., N_r, N_l, N_g), the adversary cannot carry out replay attack.

5) *Performance Analysis*

In the authentication protocol, the register phase can be completed offline or in advance, and a device only need register once. Therefore, we just need consider the computation complexity in authentication phase. As shown in TABLE Ⅱ, devices only require to compute K*G except encryption and decryption operations.

TABLE II. COMPUTATIONAL COMPLEXITY FOR AUTHENTICATION PROCESS

Principal	***Encryption***	***Decryption***	***Others***
Device1	2	2	1
Device2	1	2	1
MC&D	4	3	-

VI. CONCLUSION

In this paper, we propose the concept of OLC, identify the security requirements of OLC in the U2IoT and propose a PUF based mutual authentication protocol for the physical access phase. Authentication protocol is established to verify the identities of smart devices and the gateway, and it realizes the mutual authentication between smart devices and the gateway. Finally, BAN logic proof shows that it is theoretically correct and secure. The security analysis indicates that the protocols are satisfied the security requirements.

ACKNOWLEDGMENT

This work was funded by National Natural Science Foundation of China (61471035, 61601129), Fundamental Research Funds for the Central Universities (06105031), and Beijing Municipal Organization Department Talents Project (201500002685XG245).

REFERENCES

[1] H. Ning, "Unit and Ubiquitous Internet of Things". CRC Press, Taylor & France Group, 2013.

[2] Pervasive computing in embedded systems. FP7. http://www.ict-peces.eu (accessed November 14, 2011).

[3] SENSEI: Integrating the physical with the digital world of the network of the future. FP7. http://www.ict-sensei.org (accessed August 2, 2012).

[4] Future Internet assembly: European future Internet portal—The information hub for European R&D activities on the Internet of the future. http://www.future-internet.eu/home-/future-internet-assembly.html (accessed August 2, 2012).

[5] B. Guo, D. Zhang, Z. Yu, Y. Liang, Z. Wang, and X. Zhou, "From the Internet of Things to Embedded Intelligence," World Wide Web Journal (WWWJ), vol. 16, no. 4, pp. 399-420, 2013.

[6] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146-164, 2015.

[7] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the Internet of Things," Computer, pp. 46-53, 2013.

[8] G. Sun, S. Huang, W. Bao, Y. Yang, and Z. Wang, "A privacy protection policy combined with privacy homomorphism in the Internet of Things," in 2014 23rd International Conference on Computer Communication and Networks (ICCCN), 2014, pp. 1-6.

[9] J.-L. Hou and K.-H. Yeh, "Novel authentication schemes for IoT based healthcare systems," International Journal of Distributed Sensor Networks, vol. 2015, p. 5, 2015.

[10] F. V. Meca, J. H. Ziegeldorf, P. M. Sanchez, O. G. Morchon, S. S. Kumar, and S. L. Keoh, "HIP security architecture for the IP-based internet of things," in Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on, 2013, pp. 1331-1336.

[11] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," IEEE Sensors Journal, vol. 13, no. 10, pp. 3711-3720, 2013.

[12] H. Ning, H. Liu, and L. T. Yang, "Aggregated-proof based hierarchical authentication scheme for the internet of things," IEEE Transactions on Parallel and Distributed Systems, vol. 26, pp. 657-667, 2015.

[13] Q. Li, H. Liu, H. Ning, Y. Fu, S. Hu, and S. Yang, "Supply and Demand Oriented Energy Management in the Internet of Things," Advances in Internet of Things, vol. 6, p. 1, 2016.

[14] M. Roel, "Physically unclonable functions: Constructions, properties and applications," Ph. D. thesis, Dissertation, University of KU Leuven, 2012.

[15] P. Tuyls and L. Batina, "RFID-tags for Anti-Counterfeiting," in Cryptographers' Track at the RSA Conference, 2006, pp. 115-131.

[16] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight secure search protocols for low-cost RFID systems," in Distributed Computing Systems, 2009. ICDCS'09. 29th IEEE International Conference on, 2009, pp. 40-48.

[17] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight mutual authentication and ownership transfer for RFID systems," in INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1-5.

[18] L. Peng, W. Ru-chuan, S. Xiao-yu, and C. Long, "Privacy Protection Based on Key-changed Mutual Authentication Protocol in Internet of Things," in China Conference Wireless Sensor Networks, 2013, pp. 345-355.

[19] A. Van Herrewege, S. Katzenbeisser, R. Maes, R. Peeters, A.-R. Sadeghi, I. Verbauwhede, et al., "Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs," in International Conference on Financial Cryptography and Data Security, 2012, pp. 374-389.

[20] E. Öztürk, G. Hammouri, and B. Sunar, "Towards robust low cost authentication for pervasive devices," in Pervasive Computing and Communications, 2008. PerCom 2008. Sixth Annual IEEE International Conference on, 2008, pp. 170-178.

[21] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," SIAM journal on computing, vol. 38, pp. 97-139, 2008.