**SCIS 2011** The 2011 Symposium on Cryptography and Information Security
Kokura, Japan, Jan. 25-28, 2011
The Institute of Electronics, Information and Communication Engineers

# An efficient and privacy-preserving authentication protocol for HAN

Doyoung Chung * Made Harta Dwijaksara * Yijae Park * Jangseong Kim * Kwangjo Kim *

**Abstract**— The SG (Smart Grid) system provides advantages for its stakeholders, which can not only reduce wasted energy and maintenance cost but also increase reliability with transparency during delivering electricity from suppliers to customer. The HAN (Home Area Network), consisting of smart appliances, smart meter and management system, can enable an end-user to remotely control many digital appliances. However, anyone can easily eavesdrop communication between the components of the HAN due to wireless communication to support easy and quick connection. As a result, the adversary easily identify the type of appliances which belongs to the end-user by the energy consumption pattern. To prevent this, we propose a privacy-preserving authentication for HAN, which can support various security features such as mutual authentication, confidentiality, message integrity, anonymous communication, and resiliency against compromising smart meter.

**Keywords:** Smart grid, Home are network, Privacy, Authenticatoin

## 1 Introduction

The SG (Smart Grid), which is shown in Figure 1, provides advantages for its stakeholders (*i.e.,* supplier and end-user). It also reduces maintenance cost and increases reliability with transparency during delivering electricity from the suppliers to an end-user. An end-user also takes advantages from the SG. One of advantages in SG is that the appliances of a customer can operate when the price of electricity is counted to be cheap.

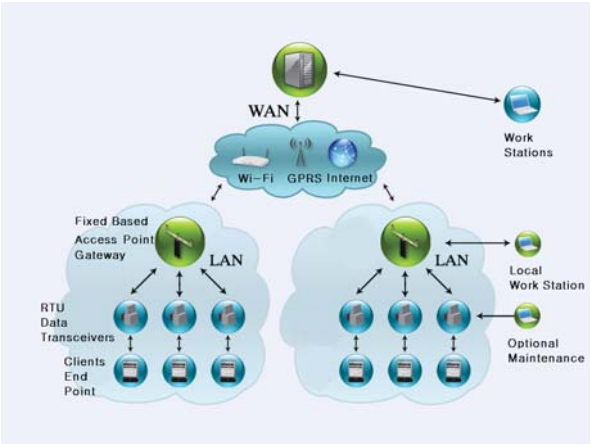


Figure 1: A configuration of SG [1]

Although wireless communication is necessary in order to support easy deployment in HAN, the adversary can easily obtain the private information(*i.e.,* life style, billing information, existence of an end-user in an accomodation, type of an appliance, *etc.*) of an end-user by eavesdropping.

The adversary can compromise the smart meter, because the smart meter is usually located on the outside of the accommodation. Thus, we should provide resiliency against compromising the smart meter.

However, some HAN devices (*e.g.,* smart appliances and smart meter) are constrained in their computing capabilities, primarily to keep costs down, which may limit the types and layers of security that could be applied [2]. Thus the authentication protocol for HAN should be lightweight.

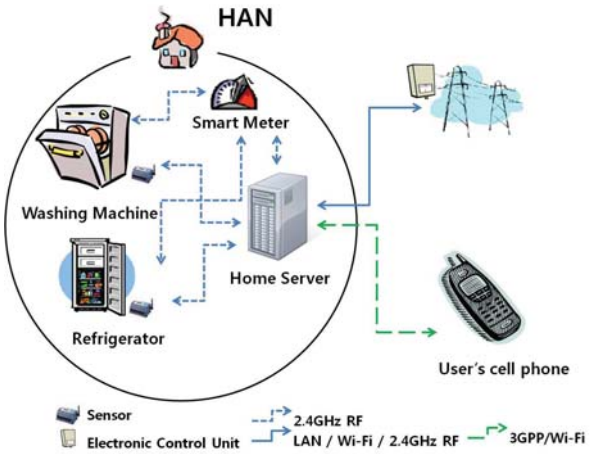


Figure 2: Our system model for HAN

We also consider scalability issue. Because an end-user may want to attach (or remove) a new smart appli-

* Korea Advanced Institute of Science & Technology, Dept. Computer Sience, 373-1 Guseong-dong, Yuseong-gu, Daejeon (Seoul 305-701 Korea), Rep of KOREA, (wordspqr, made.harta, krad, jskim.withkals, kkj@kaist.ac.kr)

ance in his HAN and replace his smart appliance with new one.

We illustrate our system model for HAN (Home Area Network) in Figure 2. Since services are provided to customers in the ubiquitous environment, the management system such as the home server is usually required. In addition, the end-user can remotely control his smart appliances through the home server and check his power bill and power consumptions of each smart appliances from outside of his accommodation. The smart meter gathers the information such as power consumption from the smart appliances and reports it to the home server.

In this paper, we suggest an efficient and privacy-preserving authentication protocol for HAN over the SG which satisfies the requirements mentioned above.

The rest of this paper is organized as follows: In Section 2, we discuss the related work in brief. Section 3 presents membership verification used in our protocol. In Section 4, we suggest our protocol in detail. Then, we analysis security analysis our protocol in Section 5. Finally, we conclude this paper in Section 6.

## 2 Related Work

### 2.1 Authentication for HAN over Smart Grid

Guidelines for Smart Grid Cyber Security published by NIST [3] says that, "Due to the relatively new technologies used in HANs, communication protocols have not yet stabilized as accepted standards, nor have their capabilities been proven through rigorous testing."

Moreover, the smart meter in HAN can be compromised by the adversary. The device is exposed to physical security threats such as poor maintenance, misusage, and theft.

### 2.2 BGN encryption [4]

In 2005, Boneh *et al.* [4] proposed a new homomorphic encryption scheme supporting unlimited additive operations and one multiplicative operation on encrypted data. The proposed encryption scheme enables one entity to evaluate the encrypted data without revealing the content of encrypted data. We review the BGN encryption scheme in brief.

In BGN encryption, all operations are done over two cyclic group $G$ and $G_1$ with the same order $n = q_1 q_2$ , where $q_1$ and $q_2$ are two large prime numbers.

The public key $PK_{BGN}$ is $g$ and $h = g^{\mu q_2}$ under the group $G$, where $\mu$ is a random integer. The encryption of $m_i$, $m_i + m_j$, and $m_i m_j$ can be computed as $g^{m_i} h^{r_i}$, $g^{m_i} h^{r_i} g^{m_j} h^{r_j}$ and $e(g^{m_i} h^{r_i}, g^{m_j} h^{r_j})$ where $T$ is a non-zero random number less than $q_2$, $m_i \in Z_T$ be i-th message, $r_i$ is i-th random number, and $e$ is a bilinear mapping from $G \times G$ to $G_1$. The expected decryption time using Pollard's lambda method is $\tilde{O}(\sqrt{|T|})$ although the authentication server has the private key, $SK_{BGN} = q_1$.

### 2.3 Membership verification

In 2008, Yau *et al.* [5] proposed an idea to convert the searching of the sets to an evaluation of polynomial representations of a given set [6, 7] using BGN encryption [4].

However, the proposed approach is not efficient in view of computational overhead. Denote $S_1$ and $S_2$ by a set of access keys and a set of keywords, respectively. Then, the end-user should compute $(|S_1| + |S_2| + 1)$ exponent multiplications and BGN encryptions per each query.

To reduce the computational overhead, Kim *et al.* [8] revised the definition of the polynomial presenting the sets and proposed new verification algorithm. The end-user should compute $(|S_2| + 1)$ BGN encryptions per each query. Also, Kim *et al.* suggested an idea to reduce the verification cost while providing a certain level of performance. This approach is more lightweight than the scheme by Yau *et al.* [5]. Their membership verification process requires some pairing computations and exponent multiplications.

## 3 Our membership verification

We convert membership verification to set search by evaluating of a polynomial representing a given set [6, 7], where the set contains the service subscriber list. Compared to membership verification cost of the previous work [8], our membership verification cost is reduced to only one exponent operation. At this point, we claim that our membership verification is more efficient approach than the previous approaches.

### 3.1 Assumption and notations

We assume that the communication between the home server and appliances to be secure. Also, the home server issues a nonce $R_{HS}$ to the smart meter and shares a fresh session key $K_{HS,SM}$ when the smart meter becomes one entity in HAN. $g^{-\alpha r \cdot SK_{BGN}}$ , where $\alpha$ and $r$ are random integers, is stored in the smart meter for membership verification. Table 1 summarizes the notations used in this paper.

### 3.2 Polynomial generation

For a set $S_1 = \{w_1, w_2, \cdots, w_p\}$, a polynomial with degree $t$, $f(x)$ is defined as

$$f(x) = \begin{cases} E[-\alpha r, PK_{BGN}, G] & x = w_i \in S_1 \\ E[-r', PK_{BGN}, G] & x = w_i \notin S_1, \end{cases}$$

where $\alpha$, $r$, and $r'(r' \neq r)$ are random integers. Here, $w_i = E[-r', PK_{BGN}, G] = g^{-r} h^{R_i}$ is an authorized token of *i-th* appliance.

Given $x_i \in S_i = E[-r, PK_{BGN}]$ & $f(x) = x \times E[-(\alpha - 1)r, PK_{BGN}]$

Then, $f(x_i) = x_i \times E[-(\alpha - 1)r, PK_{BGN}] = E[-\alpha r , PK_{BGN}]$

Table 1: Notation

| | |
|---|---|
| $HS$ | Home Server |
| $APP$ | Appliance |
| $SM$ | Smart Meter |
| $PK_A$ | A public key of entity A |
| $SK_A$ | A private key of entity A |
| $PK_{BGN}$ | A public key under $BGN$ encryption [4] owned by $HS$ |
| $SK_{BGN}$ | A private key under $BGN$ encryption [4] owned by HS and distributed to SM |
| $E\{m, K_A\}$ | A message $m$ is encrypted by a symmetric key $K_A$ |
| $E[m, PK_{BGN}, G]$ | A message $m$ is encrypted by the public key $PK_{BGN}$ on cyclic group $G$ |
| $H(m)$ | A hash value of message $m$ using a hash function such as $SHA-1$ |
| $R_A, 1 \leq i \leq n$ | A series of 64-bit nonces generated by entity $A$ |

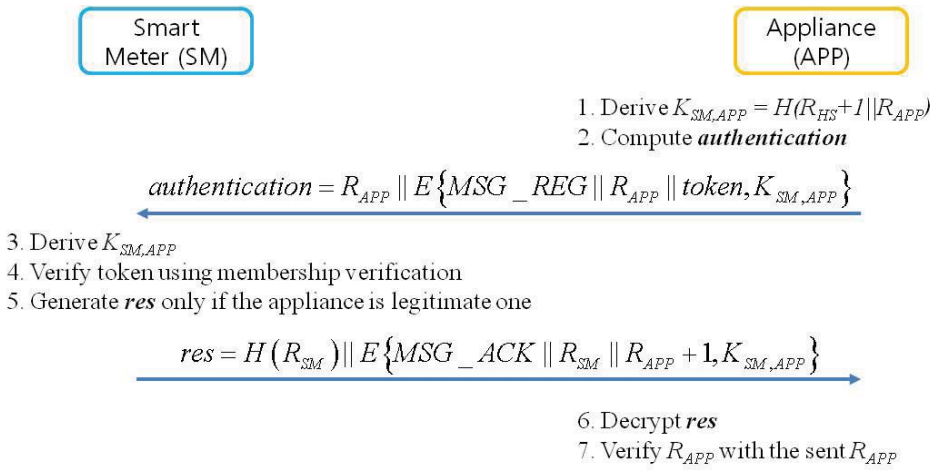


Figure 3: Appliance authentication

This computation presents an example of generating a polynomial. If the appliance exists in the set, the evaluation result of the given polynomial $f(x)$ is a fixed value $E[-\alpha r, PK_{BGN}, G]$ where $r$ is 0 to $2^{160}-1$. Therefore, we can verify whether the end-user exists in the subscriber list.

### 3.3 Polynomial evaluation

For membership verification, an appliance submits $w_i$ to the membership verifier (*i.e.,* smart meter). Then, the membership verifier checks whether the appliance belongs to one of the end-user's appliances by computing $f(w_i)$. Only if $f(w_i) = -\alpha r$, the appliance is a legitimate one.

However, we want to hide the detailed information of membership function from the adversary. That's why the membership verifier performs the following steps:

$(S1) Compute\ C = w_i \times E[-(\alpha-1)r, PK_{BGN}, G]$
$(S2) Compare\ C^{SK_{BGN}}\ with\ the\ stored\ g^{-\alpha r \cdot SK_{BGN}}$

## 4 Our protocol

Our protocol consists of four phases such as appliance registration, appliance authentication, power request, and report. In the following, we describe our protocol in detail.

### 4.1 Appliance registration phase

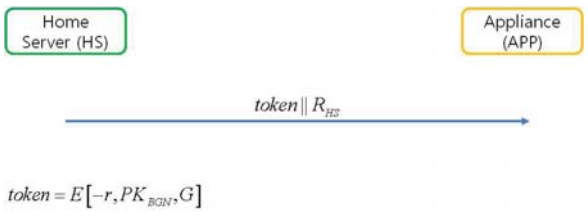


Figure 4: Appliance registration

Through the appliance registration phase, the home server issues proper $E[-r, PK_{BGN}, G]$ and $R_{HS}$ to the appliance for membership verification. Figure 4 shows the appliance registration phase.

### 4.2 Appliance authentication phase

In appliance authentication, the appliance authenticates itself using $E[-r, PK_{BGN}, G]$ and establishes a fresh session key $K_{SM,APP}$. As the smart meter and

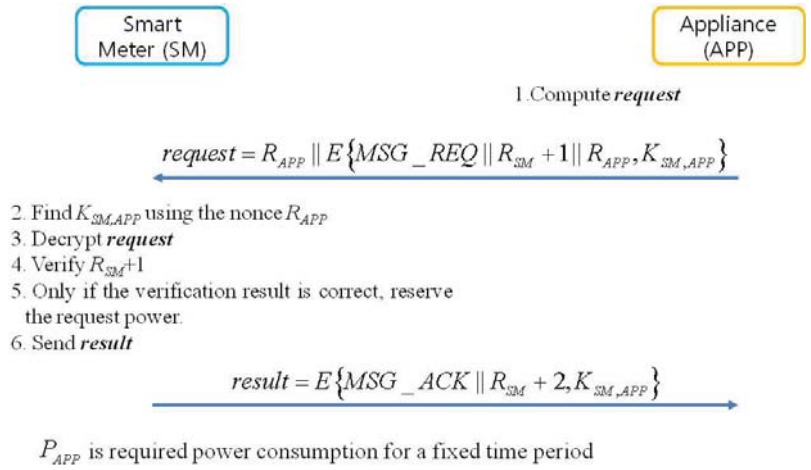


Figure 5: Power request

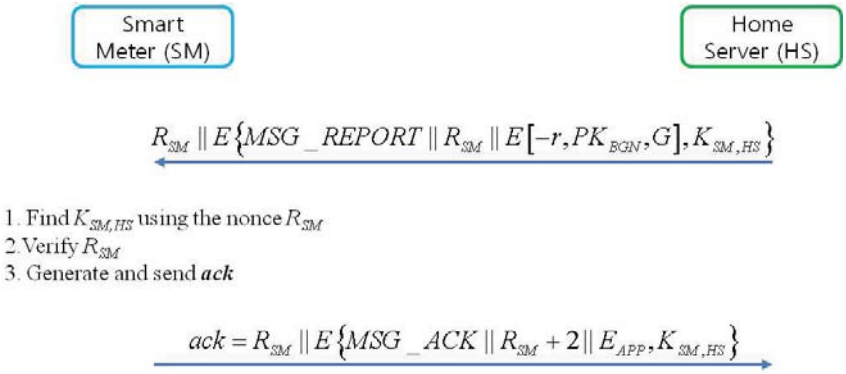


Figure 6: Report

appliance share $R_{HS}$, they can generates $K_{SM,APP}$. Using the key, we believe that the communication between the smart meter and appliance is secure.

Through membership verification discussed in Section 3, the smart meter checks whether the appliance is one of legitimate appliances owned by an end-user. Only if the computed result $C^{SK_{BGN}}$ is the same as the stored one in the memory, the smart meter can trust the appliance and send ***res*** to the appliance. This phase is shown in Figure 3.

### 4.3 Power request phase

The appliance sends a request to deal with the expected power consumption in a certain time period. Then, the smart meter verifies the received request, reserves proper power, and sends result to the appliance only if the verification result is correct. Figure 5 depicts the power request phase.

Although the end-user leaves his accommodation without plugging into the unused appliances, our protocol can minimize unnecessary power consumption of the unused appliances by adopting the time period.

### 4.4 Report phase

Since the end-user may want to observe the status of energy consumption, the home server should collect the expected power consumption from the smart meter.

Using the shared key $K_{SM,HS}$, the home server sends the request for collecting the expected power consumption of an appliance to the smart meter. Only if the received $R_{SM}$ is the same as the stored in the memory, the smart meter sends ***ack*** message to the home server.

Since $E[-r, PK_{BGN}, G]$ is used to identify the target appliance, the smart meter cannot identify what the appliance is.

## 5 Performance Analysis

Our protocol is targeting to use for commercial application, thus our protocol has to balance between strength of security and performance. To satisfy this purpose, the size of keys or nounce in our protocol are decided to provide the commercial level of security. For example, we use 128 bit key for symmetric encryption which follows the guidelines of NIST [3]. In Table 2, we define the size of nounce, symmetric key, keys for BGN encryption [4], *etc.*

Table 2: Storage Requirement

| | |
|---|---|
| Nonce | 64-bit |
| Symmetric Key | 128-bit |
| $E[-r, PK_{BGN}, G]$ | 512-bit |
| $E[-(\alpha-1)r, PK_{BGN}, G]$ | 512-bit |
| $PK_{BGN}$ | 512-bit |
| $SK_{BGN}$ | 512-bit |
| Name of Appliance | 1024-bit |
| Power Consumption | 32-bit |

### 5.1 Storage Overhead

Each entity requires storage to save persistent data or temporarily data for computaiton. This overhead is naturally proportional to the number of bits of each saved data. Thus we measure this overhead by count the number of bits requied to save each data.

The appliance has to store $R_{APP}$, $R_{HS}$, $R_{SM}$, $K_{SM,APP}$ and token. The nonces $R_{APP}$, $R_{HS}$ and $R_{SM}$ require 64-bit per each. $K_{SM,APP}$ requires 128-bit and the token requires 512-bit. Thus, $64+64+64+128+512 = 832(bit)$ of storage is required for the appliance.

| $R_{APP}$ | $K_{SM,APP}$ | Token | $R_{SM}$ |
|---|---|---|---|
| 0x32... | 0xFF2D1... | 512-bit | 0xAB... |
| 0x12... | 0xA32BC... | 512-bit | 0x0F... |
| | | | |
| | | | |
| | | | |
| | | | |

Figure 7: An example of memory image in Smart Meter

The smart meter has to store $E[-(\alpha-1)r, PK_{BGN}, G]$, $K_{SM,HS}$ and $R_{HS}$ to communicate with the home server and to do membership vertification. Moreover the smart meter has to store $R_{APP}$, $K_{SM,APP}$, token, and $R_{SM}$ per each appliance as depicted in Figure 7. The smart meter requires $512+128+64 = 704(bit)$ and $64+128+512+64 = 768(bit)$ per each appliance. Thus the total amount of bits required is $704(bit)+768(bit)\times(the\ number\ of\ appliances)$.

The home server has to store $R_{HS}$, $R_{SM}$ and $K_{SM,HS}$. Moreover the home server has to store token, name of appliance, and power consumption per each appliance as depicted in Figure 8. The home server requires $64+64+128 = 256(bit)$ and $(512+1024+32 = 1568(bit)$ per each appliancce. Thus the total amount of bits required is $256(bit)+1568(bit)\times(the\ number\ of\ appliances)$.

| Token | Name of APP | Power Consumption |
|---|---|---|
| 0x35A... | TV | 40 Wh |
| 0x00F... | Air Conditioner | 521 Wh |
| 0x121... | Dish washer | 0 Wh |
| 0x698... | Refrigerator | 85 Wh |
| | | |
| | | |
| | | |

Figure 8: An example of memory image in Home Server

### 5.2 Computational Cost

We analyze the computational cost in hash operation, symmetric key operation, exponent multiplication and exponent addition. In Table 3, we summarize the computational cost for each phase and each entity.

#### 5.2.1 Appliance registration phase

In appliance registration phase, the home server computes $E[-r, PK_{BGN}, G]$. To compute this polynomial, 2 exponent multiplications and 1 exponent addition is required.

#### 5.2.2 Appliance authentication phase

In appliance authentication phase, the appliance computes $R_{HS}||E\{MSG\_REG||R_{APP}||token, K_{SM,APP}\}$. To derive $K_{SM,APP}$, 1 hash operation is required, and to send $R_{HS}||E\{MSG\_REG||R_{APP}||token, K_{SM,APP}\}$ 1 symmetric encryption is required.

The smart meter should perform 1 symmetric key operation to decrypt the message. It also performs 1 hash operation to derive $K_{SM,APP}$. For membership verification, it should perform 1 exponent multiplication and 1 exponent addition.

It performs 1 symmetric encryption and 1 hash operation for $H(R_{SM})||E\{MSG\_ACK||R_{SM}||R_{APP}+1, K_{SM,APP}\}$. When the appliance receives this message, it performs 1 symmetric key operation and 1 hash operation to reveal the content of the message.

Thus during the appliance authentication phase, the smart meter requires 2 hash operations, 2 symmetric key operations, 1 exponent multiplication and 1 exponent addition. The appliance requires 2 hash operations and 2 symmetric key operations.

#### 5.2.3 Power request phase

In power request phase, the appliance and the smart meter communicate via symmetric encrypted messages. Thus each entity performs 2 symmetric key operations to decrypt and encrypt messages.

#### 5.2.4 Report phase

In report request phase, the smart meter and the home server communicate via symmetric encyprted message. $R_{SM}||E\{MSG\_REPORT||R_{SM}||E[-r, PK_{BGN}, G], K_{SM,HS}\}$ is sent by the home server to the smart meter. To encypt this message the home server performs

Table 3: Computational cost

| Phase | Entity | Hash | Symmetric key | Exponent multiplication | Exponent addition |
|---|---|---|---|---|---|
| Registration | HS | 0 | 0 | 2 | 1 |
| | APP | 0 | 0 | 0 | 0 |
| Authentication | SM | 2 | 2 | 1 | 1 |
| | APP | 2 | 2 | 0 | 0 |
| Power request | SM | 0 | 2 | 0 | 0 |
| | APP | 0 | 2 | 0 | 0 |
| Report | HS | 0 | 2 | 0 | 0 |
| | SM | 0 | 2 | 0 | 0 |

1 symmetric key operation, and the smart meter performs 1 symmetric key operaiton to decrypt this message.

After receives this message, the smart meter responses to the home server by send $R_{SM}||E\{MSG\_ACK||R_{SM}+2||E_{APP}, K_{SM,HS}\}$. This message also requires 1 symmetric key operation to encrypt, and another 1 symmetric key operation to decrypt. Thus the computational cost for the smart meter and the home server is 2 symmetric operations for each.

### 5.3 Communication Cost

To illustrate the efficiency of our protocol, we analyze each phase in detail. Using the message size defined in Table 2, we compute the message size. In Table 4, we summarize the computational cost for each phase and each entity.

Table 4: Communication cost

| Phase | Entity | Message size (bit) |
|---|---|---|
| Registration | HS | 576 |
| | APP | 0 |
| Authentication | SM | 704 |
| | APP | 416 |
| Power request | SM | 128 |
| | APP | 320 |
| Report | HS | 704 |
| | SM | 196 |

#### 5.3.1 Appliance registration phase

The home server sends $token||R_{HS}$ to the appliance. The token is 512-bit length and $R_{HS}$ is 64-bit length. Thus 576-bit is communication cost for the home server.

#### 5.3.2 Appliance authentication phase

As each appliance sends $R_{HS}||E\{MSG\_REG||R_{APP}||token, K_{SM,APP}\}$, the message size is $64 + E\{8 + 64 + 512\} = 64+640 = 704(bit)$. So, the computational cost for the appliance is 704 bit.

The smart meter sends $H(R_{SM})||E\{MSG\_ACK||R_{SM}||R_{APP}+1, K_{SM,APP}\}$ to the appliance, the message size is $160 + E\{8 + 64 + 64\} = 160 + 256 = 416(bit)$. Thus the computational cost for the smart meter is 416 bit.

#### 5.3.3 Power request phase

As each appliance sends $R_{APP}||E\{MSAG\_REQ||R_{SM}+1||R_{APP}, K_{SM,APP}\}$, the message size is $64+E\{8+64+64\} = 64 + 256 = 320(bit)$ length, and the computational cost for the appliance is 320 bit.

$E\{MSG\_ACK||R_{SM}+2, K_{SM,APP}\}$ is sent by the smart meter to the appliance, the message size is $E\{8+64\} = 128(bit)$. Thus the computational cost for the smart meter is 128 bit.

#### 5.3.4 Report phase

The home server sends $R_{SM}||E\{MSG\_REPORT||R_{SM}||E[-r, PK_{BGN}, G], K_{SM,HS}\}$ to the smart meter, the message size is $64 + E\{8 + 64 + 512\} = 64 + 640 = 704(bit)$. The smart meter replies $R_{SM}||E\{MSG\_ACK||R_{SM}+2||E_{APP}, K_{SM,HS}\}$ to the home server, the message size is $64 + E\{8 + 64 + 32\} = 64 + 128 + 196(bit)$. Thus the communication cost for the home server is 704 bit and that for the smart meter is 196 bit.

## 6 Security Analysis

### 6.1 Mutual authentication

Entity which participated in communication has shared key for each other. For detail, the home server and smart meter have shared key $K_{SM,HS}$ and the smart meter and each appliance have shared key $K_{SM,APP}$. By using shared key, entities which participated in communication can authenticate mutually.

### 6.2 Confidentiality and Integrity

All messages are encrypted by a fresh session key. Only the entity (*i.e.,* smart appliance and smart meter) having the session key can identify the contents of an encrypted message. Thus we can provide confidentiality. Also the integrity of message is confirmed by comparing nonces concatenated in front of message and nonces which have encrypted in a message.

### 6.3 Anonymity

Although the outsider including the adversary can easily eavesdrop the communications over HAN, he cannot reveal the content of message because the message is encrypted.

On the other hand, the smart meter cannot distinguish the type of appliance. Through our membership

verification, the smart meter only verifies whether the device is owned by the end-user or not. Also, the smart meter cannot reveal the power consumption of each devices. Because the smart meter does not have any information which relationship about the token and the smart appliances. However, as the adversary infers the power consumption of each smart appliance from the power consumption of each token, our protocol employs periodic change of the token owned by each device.

As a result, we believe that our protocol can support anonymity of an end-user from the insiders and outsiders.

### 6.4 Resiliency against compromising smart meter

Although the adversary cannot access the home server of the target end-user, he may compromise the smart meter in HAN. Through compromising the smart meter, the adversary can obtain useful information.

However, in our protocol the adversary cannot identify the type of appliance used in HAN through the stored information in smart meter. Because the token $E[-r, PK_{BGN}, G]$, which is used to authenticate the smart appliances, only indicates that the appliance is owned by an end-user. The relationship between the token and target appliance is only known to the home server. Moreover, the adversary cannot identify the target appliance of the token in polynomial time since the BGN encryption requires the $\tilde{O}(\sqrt{|T|})$ time for decryption although the adversary has the private key, $SK_{BGN} = q_1$ [4]. From these observations, we provide resiliency against compromising the smart meter.

## 7 Conclusion

In this paper, we propose an efficient privacy-preserving authentication for HAN over the SG. As explained before our protocol satisfies the security requirements such as mutual authentication, confidentiality, message integrity, anonymous communication, and resiliency against compromising smart meter. We analyze the security of our protocol in Section 6.

In our protocol, the storage overhead for each appliance is $O(1)$. Since the storage overhead for the home server and the smart meter are $O(L)$ where L is the number of appliances, thus we believe that our protocol is an efficient approach. The number of appliances in the house of an end-user does not exceed 20. But the home server and the smart meter have ability to remain enough storage.

By considering the computational capability of each component (*i.e.*, appliance, home server, and smart meter), the heavy computations such as exponent multiplication and exponent addition are delivered to the home server and smart meter. The appliance only requires hashing and symmetric key operations, which are believed to be lightweight computations compared to the exponent multiplication and exponent addition. Since the registration and the authentication phases are performed very few times, we believe that our protocol is to be lightweight.

In the view of communication cost, each entity is required to send its own message less than 1,024 bit. From this point, we believe that our protocol is efficient in terms of communication overhead.

In the future, we will analyze the security and performance of our membership verification protocol in a rigorous way. We also expand these protocol to more general ways for authentication under unbalanced computing environment, especially for the situation that the information about entity has to be bailed from authentication server.

## References


[1] MTR, "Smart Grid Wireless Solutions," *Internet*, http://www.mtrcom.com

[2] P. McDaniel, and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *Security & Privacy, IEEE, 2009*, pp. 75-77

[3] NIST, *Guidelines for Smart Grid Cyber Security*, vol 1-3

[4] D. Boneh, E.-J. Goh and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," *Theory of Cryptography (TCC '05), LNCS 3378, Feb. 2005*, pp. 325-341

[5] S. S. Yau and Y. Yin, "Controlled Privacy-preserving Keyword Search," *Proc. of ACM Symposium on Information, Computer & Communications Security (ASIACCS '08), Mar. 2008*, pp. 321-324.

[6] M. J. Freedman, K. Nissim and B. Pinkas, "Efficient Private Matching and Set Intersection," *Advanced in Cryptography - EUROCRYPT '04, LNCS 3027, May 2004*, pp. 1-19.

[7] L. Kissner and D. X. Song, "Privacy-preserving Set Operations," *Advances in Cryptology - CRYPTO '05, LNCS 3621, Aug. 2005*, pp. 241-257.

[8] Jangseong Kim, Joonsang Baek, Kwangjo Kim, and Jianying Zhou, "A Privacy-Preserving Secure Service Discovery Protocol for Ubiquitous Computing Environments," *Proc. of EuroPKI 2010, Sep. 23-24, 2010, Athens, Greece.*