Preserving Forward Anonymity on Dynamic ID based Remote User Authentication Scheme

Ari Moesriami Barmawi and Fiky Y. Suratman

School of Computing, Telkom University, Indonesia
mbarmawi@melsa.net.id, fysuratman@gmail.com

Abstract: Recently, the use of smart cards in human life is increasing. One important aspect in implementing smart cards in human life is its security. Security should be considered because smart cards can contain important data that must be protected, and specific research is needed to address attacks against smart card. There are weaknesses in preserving forward anonymity on dynamic ID-based remote user authentication using smart cards as mentioned in Zhai et al. In their work, attacks that led to the failure of forward anonymity have been successfully carried out. This problem has already been overcome by Lee's scheme, with the probability of the forward anonymity failure was $½^{296}$ but the computation cost was still high. This research discussed about overcoming attacks that can lead to the failure of forward anonymity with probability of less than $½^{296}$ and has less computation cost. For this purpose, discrete log function and multiplicative inverse is introduced instead of using hash function and Diffie-Hellman method. Based on the discussion it is proven that these functions can preserve the forward anonymity with the probability of failure less than $½^{296}$.

Keywords: smart card; identity based; anonymity; hash; cyclic group

1. Introduction

Recently, the use of smart cards in human life is increasing. Smart cards are widely used in banking, commercial, business, government, health care, etc. In order to implement smart card in human life, there are several things to be considered including its profit, material or non-material benefit, obtained by users or systems. One important aspect in implementing smart cards in human life is its security. Security should be considered because smart cards can contain important data that must be protected, and leak insecurity can cause significant material losses to both users and systems. Based on the importance of the security aspects of smart card, specific research is needed to address attacks against smart card. There are weaknesses in preserving forward anonymity on dynamic ID-based remote user authentication using smart card as mentioned in [1,2,3]. Based on Zhai, et al. [3], attack that led to the failure of forward anonymity has been successfully carried out. This problem has already been overcome by Lee, et al. scheme, but the probability to failure the forward anonymity was still $½^{296}$, and the computation cost is still high. Therefore, this research discussed about overcoming the attacks that can lead to the failure of forward anonymity with probability of less than $½^{296}$ and has less computation cost. For overcoming the attack, discrete log function [4] and multiplicative inverse is proposed instead of using hash function and Diffie-Hellman method [5]. Based on the discussion it is proven that these function can overcome the attacks so that forward anonymity can be maintained.

2. Dynamic ID based Remote User Authentication Scheme (Wang. et. al) [6]

Dynamic ID based Remote User Authentication Scheme proposed by Wang et al. consists of four phases: registration phase, login phase, verification phase and password change phase. The first three phases in Wang, et.al scheme (i.e. registration, login and verification phase) are shown in Figure 1.

Since the presentation of Wang, et al. scheme needs several symbols for understanding the scheme presentation, symbols in Table. 1 should be consulted.

Received: December 7th, 2016. Accepted: December 28th, 2017
DOI: 10.15676/ijeei.2017.9.4.4

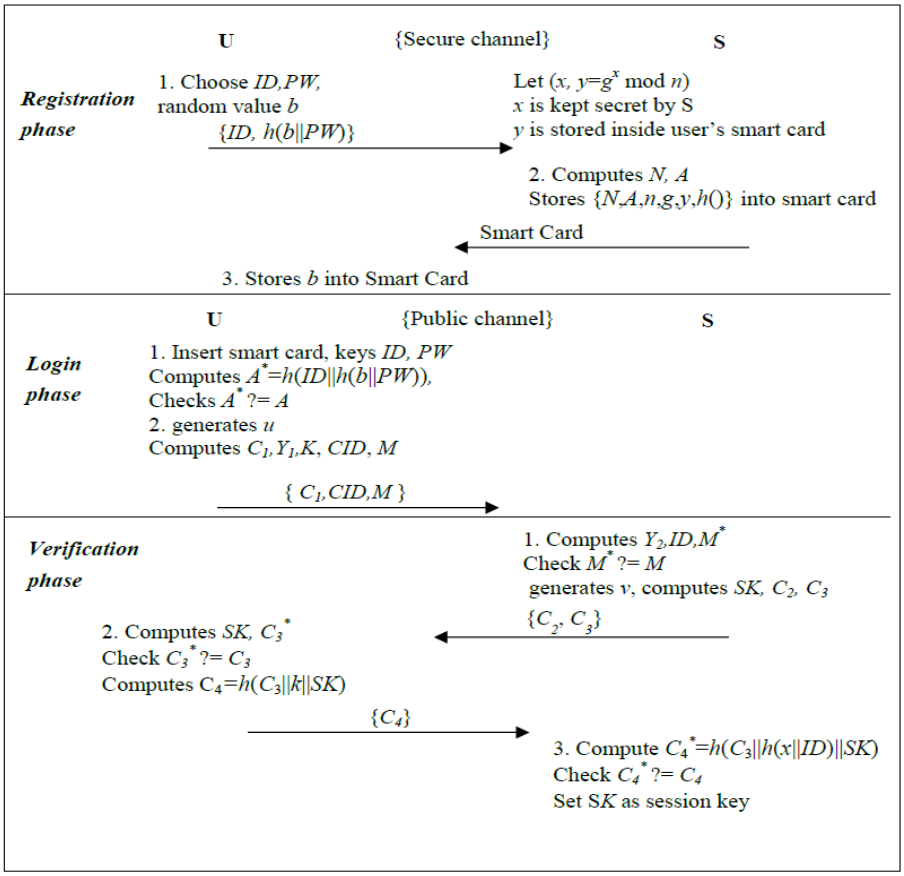

Figure 1. ID based remote user authentication scheme proposed by Wang, et.al.

Table 1. The notation used in Wang's, Lee's and proposed scheme

Symbol	Description
U	User
S	Remote Server
SC	Smart Card
ID,*id*	Identity of the user
PW, *Pw*	Password of the user
x	the secret key of remote server
$\oplus$	bit wise x-or operation
||	String Concatenation
A-->B: C	Message C transferred from A to B through public channel
A=> B: C	Message C transferred from A to B through secure channel
h, $\mathcal{H}i$, h	Hash function
Pw0	Initial password
K_s, *SK*	Session key

A. Registration Phase

We assume that user U and server S have established a secure channel. Let $y=g^x \bmod n$ where n is a larger prime (x, y) denote S's private key and its corresponding public key. U and S perform the following steps in registration phase.

Step 1: U chooses identity ID, password PW and a random value b. U sends $\{ID, h(b||PW)\}$ to S.

Step 2: S computes $N=h(b||PW)\oplus h(x||ID)$ and $A=h(ID||h(b||PW))$. S stores $\{N, A, n, g, y, h()\}$ on a smart card and sends it to U.

Step 3: U stores b into the smart card.

B. Login Phase

Step 1: U inserts the smart card and keys ID and PW. Then the smart card computes $A^*= h(ID||h(b||PW))$ and checks whether A^* is equal to the stored A. If they are not equal, the smart card terminates the session.

Step 2: The smart card generates a nonce u and computes $C_1=g^u \bmod n$, $Y1=y^u \bmod n$, $k=N\oplus h(b||PW)$, $CID=ID\oplus h(C1||Y1)$ and $M=h(CID||C1||k)$. U sends login request message $\{C1, CID, M\}$ to S.

C. Verification Phase

Step 1: Upon receiving the login message $\{C1, CID, M\}$, S computes $Y_2=(C1)^x \bmod n$, $ID= CID\oplus h(C_1||Y_2)$ and $M^*=h(CID||C1||h(x||ID))$ where x is its private key. S compares M^* with the received M. If they are not equal, the session is terminated. Otherwise, S generates a random number v and computes $SK=(C1)^v \bmod n$, $C2= g^v \bmod n$ and $C3=h(SK||C2||h(x||ID))$. Finally, S sends $\{C2, C3\}$ to U.

Step 2: Upon receiving $\{C_2, C_3\}$, U computes $SK=(C_2)^u \bmod n$, $C_3^*=h(SK||C_2||k)$, and checks C_3^* with C_3. If they are equal, U sets SK as the session key and sends $C_4= h(C_3||k||SK)$ to S.

Step 3: Upon receiving $C4$, S computes $C4^*= h(C3||h(x||ID)||SK)$ and then checks whether $C4^*$ is equal to $C4$. If the verification holds, S authenticates U and sets SK as their session key, otherwise the session is terminated.

3. Forward Anonymity-Preserving Secure Remote Authentication Scheme [16]

Using similar assumption to Wang scheme, Lee scheme [16] consisted of three phases: registration, login and verification as shown in Figure 2.

A. Registration Phase

This scheme is defined over a finite cyclic group $\mathbb{G}$ of prime order q with g as a generator. Hash functions $\{0,1\}^* \rightarrow \{0,1\}^{\ell_i}$ are denoted by $\mathcal{H}_i$, where $i \in \{0,1,2,3,4,5\}$ and ℓ_i is the output bit length of $\mathcal{H}_i$. Let $x, y=g^x \bmod p$ denote server S's private key and its corresponding public key. Suppose user U wishes to register his/her ID to server S. Then, the following operations are conducted.

Step 1: U chooses an id. U sends the chosen id to S.

Step 2: After receiving the registration request from U, Schooses two random numbers r and R, $ID=\mathcal{H}_0(\text{id})$, $V_U=\mathcal{H}_5(x||ID||R)$ and $V_U^\star=\mathcal{E}_{r||pw0}(V_U)$, where pw0 is the initial password. Then, S stores (ID, R) in the registration table.

Step 3: S stores $\{r, V_U, y, g, p, q, \mathcal{H}_i(i=0,1,2,3,4)(.)\}$ into the smart card. S sends the smart card along with $pw0$ to U.

B. Login Phase

Login phase consists of three steps that start from U receiving the smart card until the preparation of messages that will be sent for verification process.

Step 1: After receiving the smart card from S, U has to change the password immediately.

Step 2: U inserts the smart card into the card reader, inputs his/her ID and starts session with S.

Step 3: S chooses a random element b in $\mathbb{Z}_{q^*}$ and calculates $B=g^b \bmod p$. Server S sends S and B to U, where S is the server's identity.

Step 4: After receiving messages S and B from S, the smart card chooses a random element a in $\mathbb{Z}_{q^*}$ and calculates $A=g^a \bmod p$, $V_U=\mathcal{D}_{r||pw0}(V_U^*)$, $V_S=y^a \bmod p$, $K_U=B^a \bmod p$, $ID=\mathcal{H}_0(id)$, $ID^*=ID \oplus \mathcal{H}_3(A||B||V_S||K_U)$, and $M_U=\mathcal{H}_1(ID||S||A||B||V_U||V_S||K_U)$. U sends ID^*, A, and M_U to S.

C. Verification Phase

Step 1: After receiving message $\{ID^*, A, M_U\}$ from U, S calculates $V_S=A_x \bmod p$, $K_S=A^b \bmod p$, $ID=ID^* \oplus \mathcal{H}_3(A||B||V_S||K_S)$. Furthermore, S checks the validity of ID based on the registration table by comparing ID obtained from U and ID in the list/table. If it is invalid, then the session is terminated. Otherwise, S calculates $V_U=\mathcal{H}_5(x||ID||R)$, where R is extracted from the entry corresponding to ID and checks whether $\mathcal{H}_1(ID||S||A||B||V_U||V_S||K_S)$ is equal to M_U or not. If they are not equal, the session is terminated. Otherwise, S calculates $M_S=\mathcal{H}_2(ID||S||A||B||V_U||V_S||K_S)$ and S sends M_S to U.

Step 2: After receiving message M_S from S, U verifies whether $\mathcal{H}_2(ID||S||A||B||V_U||V_S||K_U)$ is equal to M_S. If they are not equal, the session is terminated. Otherwise, the smart card and the server compute the common session key $sk_u=\mathcal{H}_3(ID||S||A||B||V_U||V_S||K_U)$, $sk_s=\mathcal{H}_3(ID||S||A||B||V_U||V_S||K_S)$ respectively.

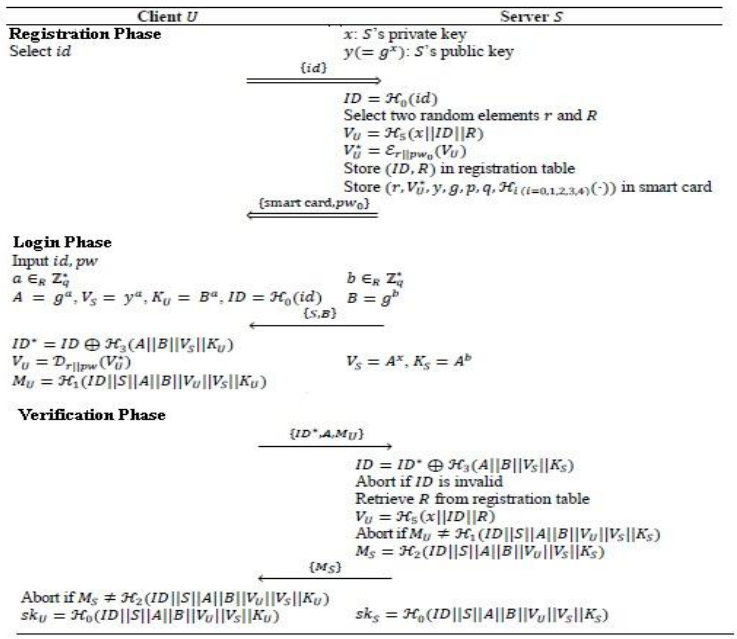

Figure 2. Forward Anonymity-Preserving Secure Remote Authentication Scheme

4. Failure to Achieve Forward Anonymity in Wang et al. Scheme [3] and Lee et al. [16]

This section discusses the detailed failure to achieve forward anonymity on Wang scheme [3] and Lee et al. scheme [16]. Failure analysis in this section was done by assuming that attacker may obtain the parameter stored in the smart card during its sending process. This assumption was held since there was a possibility that an attacker extract the parameter stored in the smartcard during the sending process, and this is the difference between assumption held in Wang's and Lee's scheme and the proposed scheme.

A. Failure to Achieve Forward Anonymity in Wang et al. Scheme [3]

Failure to achieve forward anonymity on Wang's Scheme is caused by the key values that have been compromised. In this case, the key value that has been compromised was the server's secret key *x* [3]. Although the session key is generated by Diffie-Hellman key agreement [5], Wang *et al.'s* dynamic ID scheme cannot provide forward anonymity, because the attacker may obtain the ID by tracing the exchanged message between the user and the server. Suppose the server's long-term key *x* is compromised, the attacker can derive the user's identity by tracing the previous sessions. The detailed attack is shown in Figure 3.

Step 1. The attacker recorded login request message $\{C_1, CID, M\}$ in previous sessions.

read x,i // assume x is compromised, i is the i-th record of view database
Read $C1_i$, CID_i, M_i) //i-th record from view database
$Y1_i = C1_i^x \bmod n$
$Z_i = h(C1_i \,||\, Y1_i)$
$ID_i = CID_i \oplus Z_i$
Return(ID_i)

Figure 3. Attack on Wang's Scheme

Step 2. The attacker computes $Y_1=(C_1)^x \bmod n$ using the compromised private key *x* and then obtains $ID = CID \oplus h(C_1||Y_1)$. Thus, Wang et al.'s scheme cannot possess anonymity once the server's long-term key *x* is compromised.

B. Probability of Forward Anonymity Failure in Lee. et al. Scheme [16]

Since the held assumption was that attacker may obtain the parameter stored in the smart card during its sending process, then Lee's scheme fails to achieve forward anonymity. This condition is occurred because by obtaining the parameters in the smart card, it means that the attacker obtains *r*, *pw*0 and V_U^* such that the attacker can reveal V_U. Since M_U and ID^* can be obtained by eavesdropping process, then using equation $M_U=\mathcal{H}_1(ID||S||A||B||V_U||V_S||K_U)$ and $V_S = A^x$, the attacker can guess $(ID||K_U)$. The guessed result should be checked with $ID=ID^* \oplus \mathcal{H}_3(A||B||V_S||K_U)$. If the result of equation $ID^*=ID \oplus \mathcal{H}_3(A||B||V_S||K_U)$ using the guessed *ID* is equal to ID^*, then the *ID* is revealed. In this case, the probability for attacking this scheme is equal to break the hash function. If Keccak hash function is used in this scheme, then the probability for attacking this scheme is less than 2^{-296} [17].

5. Proposed Scheme

For overcoming the problem in preserving forward anonymity when long term key has been compromised, modular power and multiplicative inverse has been proposed. The basic idea of modified Wang Scheme and Lee Scheme is that even if *x* were compromised, *ID* could not be revealed by the attacker, and the probability of Forward Anonymity Failure on Dynamic ID-based Remote User Authentication process is less than $½^{296}$ with less computation cost. Suppose the user *U* will access server *S* using smart card *SC*, then they have to execute the proposed scheme as shown in Figure 4. The difference between the proposed scheme and the other two previous schemes is shown in Table 2.

Table 2. The difference between Wang's, Lee's and the proposed method

Issues	Wang's	Lee's	Proposed method
Registration Process	*ID* and PW are determined by *U* in the registration Process. For camouflaging PW, *U* uses the concatenation function $h(b\|\|PW)$ where *b* is a number chosen by *U*.	*id* is determined by *U* in the registration process. However, *S* modified *id* into *ID* using equation $ID=\mathcal{H}_0(\text{id})$ while password $pw0$ is determined by *S* and are sent to the user *U* along with the smart card.	*ID* and *Pw* are determined by *U* in the registration Process. For camouflaging PW, *U* uses discrete log function $g^{b.Pw}$.
Session Key Generation	The session key is generated using Diffie-Hellman key exchange, where *U* sends $g^u \bmod n$ to *S*, and *S* sends $g^v \bmod n$ to *U*. The session key is $g^{uv} \bmod n$ (see chapter 3).	The session key is generated using a hash function of the concatenated variables $ID\|\|S\|\|A\|\|B\|\|V_U\|\|V_S\|\|K_U$ (see chapter 3).	The session key is generated using Diffie-Hellman key exchange, but instead of only based on the chosen random number of both parties, it was also based on the user password *Pw*.
Forward anonymity	The probability to fail the forward anonymity was equal to 1 (see section 4.1)	The probability to fail the forward anonymity was less than $1/2^{296}$ if Keccak Hash function was used (see section 4.2)	The probability to fail the forward anonymity was reduced and equal to the probability of obtaining *ID* less than $1/(u^u.2^{296})$, if Keccak Hash function was used *u* (*u* and *y* was discussed in section 6.1)
Computation cost (TE is time complexity for exponential operation, TC is symmetric encryption/decryption, and TH is the hash function.	6TE + 14 H (see chapter 7)	6TE + 1 TC + 10 TH (see chapter 7)	6TE + 6 TH (see chapter 7)

A. Registration Phase of Proposed Scheme

The protocol is defined over a finite cyclic group $G =< g >$of order *r*-bit integer number *n* which is equal to *pq* (where *p* and *q* are large primes). This group could be $G = Z_n^*$ where $Z_n^*=1, 2, ..., Ø(n)$ where $Ø(n)$ is the Euler Totient Function. We denote the group operation multiplicatively. Hash functions from $\{0, 1\}^* \rightarrow \{0, 1\}^l$ are denoted by *h*, where *l* is the bit length

of function output, e.g. $l = 256$ (by assuming that Keccak 256 is used). We also define a medium integer n, $28 \leq r < 256$, which determines the capacity of the pool of the (ID, PW) pair against offline guessing attack. Let (x, $y = g^x \bmod n$; $n=pq$) denote the server S's private key and its corresponding public key, where x is kept secret by S while y is stored inside each user's smart card and g is public.

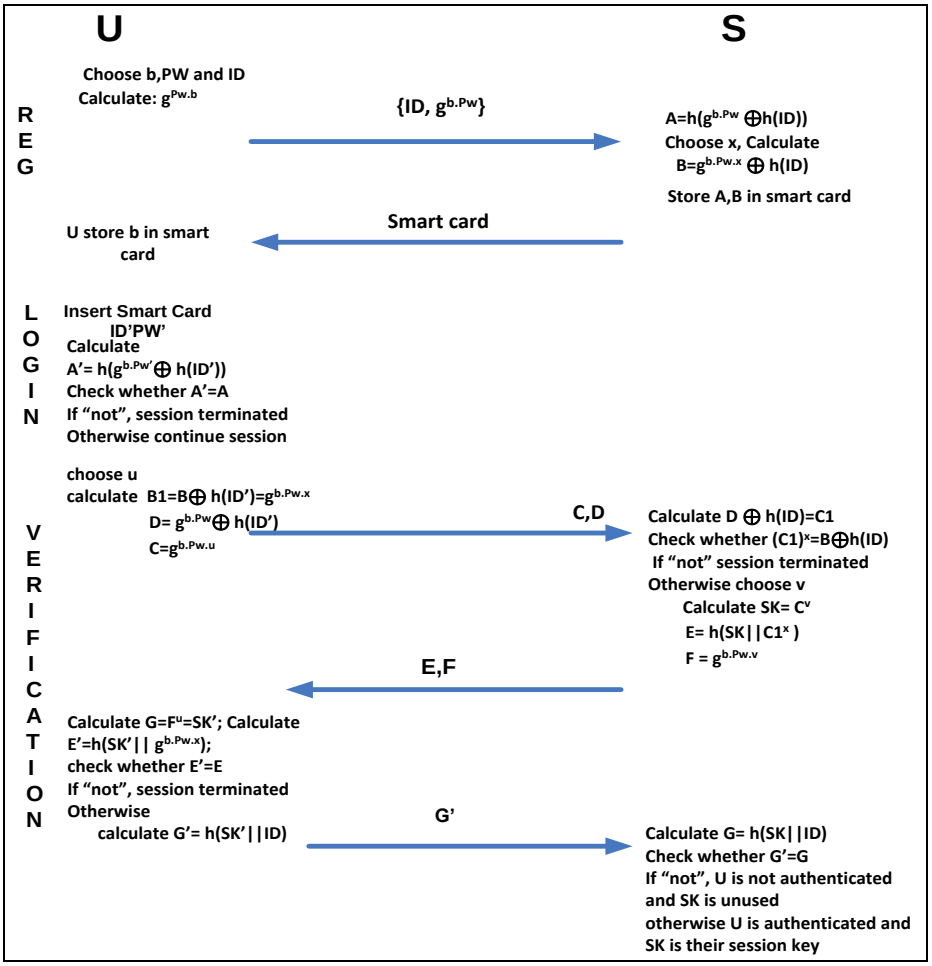

Figure 4. Proposed scheme

The registration phase involves the following operations:

Step 1. U chooses her identity ID, password PW and a random number b. U calculates $g^{b.Pw} \bmod n$

Step 2. $U \Rightarrow S$: $\{ID, g^{b.Pw} \bmod n\}$.

Step 3. On receiving the registration message from U at time T, S first checks whether is a registered user or not. If it is U's initial registration, S creates an entry for U in the account database and stores (ID, $T_{reg} = T$) in this entry. Otherwise, S updates the value of T_{reg} with T in the existing entry for U. Next, S computes $A=h(g^{b.Pw} \oplus h(ID))$, and calculates $B= g^{b.Pw.x} \bmod n \oplus h(ID)$. Store A, B in smart card.

Step 4. $S \Rightarrow U$: A smart card containing security parameters $\{B, A, y, n, h(\cdot),\}$.

Step 5. Upon receiving the smart card SC, U enters b into SC.

In this case Keccak-256 Hash Function [7] was used as the hash function, while the input of the hash function was 1600 bits, while the modulus number size was ≤ 256 bits.

B. Login Phase of Proposed scheme

When *U* wants to login to the system, the following operations will be performed:

Step 1. *U* inserts her smart card into the card reader and inputs *ID', Pw'*

Step 2. *SC* computes $A' = h(g^{b.Pw'} \bmod n \oplus h(ID'))$ and verifies the validity of *ID'* and *Pw'* by checking whether *A* equals to the stored *A*. If the verification holds, it implies *ID'= ID* and *Pw'= Pw*. Otherwise, the session is terminated.

Step 3. *SC* chooses a random number *u* and calculates $B1=B \oplus h(ID') = g^{b.Pw.x} \bmod n$, $C= g^{b.Pw.u.x} \bmod n$ and $D= g^{b.Pw.u} \bmod n \oplus ID'$

Step 4. $U \rightarrow S$: *{C, D}*.

C. Verification Phase of Proposed scheme

After receiving the login request, the server *S* performs the following process:

Step 1. *S* computes $g^{b.Pw.u} \bmod n = D \oplus h(ID) = C1$. Check whether $(C1)^x = C$. If they are "not equal", then the session will be terminated. Otherwise, chooses *v* and calculates $SK= C1^v \bmod n$; $E= h(SK|| C1)$ and $F = g^{b.P.wv} \bmod n$

Step 2. $S \rightarrow U$: {*E,F*}
Server calculates $G=F^u=SK'$ and $E'=h(SK'||g^{b.Pw.u})$. Check whether E'=E. If they are "not equal" then the session is terminated, otherwise calculates $G'= h(SK|| ID)$

Step 3. $U \rightarrow S$: {*G'*}

Step 4. Calculate $G= h(SK|| ID)$. Check whether $G'=G$, If they are "not equal", then *U* is not authenticated and *SK* is fake and unused. Otherwise *U* is authenticated and *SK* is their session key.

6. Security Analysis

Since the goal of the proposed method is to provide forward anonymity, then the security analysis concerning the forward anonymity will be evaluated. Since after modifying Wang's scheme, the security against impersonation attack should be maintained, then the evaluation against impersonation attack should be conducted.

A. Strength Analysis for Preserving Forward Anonymity

For evaluating the security of the proposed method, similar attack is applied on the Wang's scheme and the proposed method. The attack is shown in Figure 5.

```
read x,i      // assume x is compromised and i indicates the i-th records of view database
read (Ai, Bi, Ci, Di, Ei, Fi , Gi )   //i-th record from view database
C1i=  (Ci )^(x-1)
SKi=h-1 (split(E)[C1i])
IDi=h-1(split(Gi )[SKi]
Return(IDi)
```

Figure 5. Attack on Proposed Scheme

Step 1. The attacker recorded message {*A, B, C, D, E, F, G*} in previous sessions.

Step2. The attacker computes $C1=(C)^{\wedge}(x^{-1}) \bmod n$ using the compromised private key *x* and then obtains *SK* by calculating $SK=split(h^{-1}(E))[C1]$ where split(a)[b] means splitting a by applying b. In order to obtain *SK* the attacker should calculate the inverse of $h(E)$ and continued with $split(h^{-1}(E))[C1]$.

Step3. Finally the attacker obtained *ID* by calculating $h^{-1}(split(h^{-1}(G))[SK])$.

Based on the attack shown in Figure 5, it can be seen that for obtaining ID, the attacker should calculate the inverse of *x* and calculating the inverse of hash function *h.* For obtaining the inverse of *x*, the attacker should factor the modulus number *n*. Suppose Quadratic Sieve Algorithm [8]is used for factoring *n.* The algorithm works as follows:

1. Fix a factor base $F = \{p_1, p_2, \dots, p_m\}$.
2. Search for integers *r* such that $f(r) = r^2 - n$ is smooth over *F*. An integer *f(r)* is said to be smooth over a factor base *F*, if all primes which is a unique factor of *n*, are members of *F*.
3. Find a subset $U = \{r_1, r_2, \dots, r_N\}$ such that equations 1, 2 and 3 hold for *f.*

$$\forall i: f(r_i) = r_i^2 \equiv p_1^{e_{i1}} p_2^{e_{i2}} \dots p_m^{e_{im}} \bmod n \quad (1)$$

$$\forall j, 1 \le j \le m: \sum_{i=1}^{N} e_{ij} = 2.e_{i,} \quad for\ e_i \in Z \quad (2)$$

$$\prod_{i=1}^{n} f(r_i) = \prod_{i=1}^{N} r_i^2 \equiv (p_1^{e_{i1}} p_2^{e_{i2}} \dots p_m^{e_{im}})^2 \ mod\ n \quad (3)$$

Furthermore, define *x* and *y* as follows: $x = \prod_{i=1}^{N} r_i$ and $y = \prod_{i=1}^{m} p_i^{e_i}$.
Finally, find *x* and *y* which satisfy equation 4.

$$x^2 \equiv y^2 \bmod n \quad (4)$$

Using the following equation

$$x^2 = \prod_{i=1}^{N} r_i^2 \equiv \prod_{i=1}^{N} (r_i^2 - n) \equiv (\prod_{i=1}^{m} p_i^{e_i})^2 \equiv y^2 \bmod n \quad (5)$$

For simplicity, it can be assumed that the factor base consists of all primes $\le y$, (such that the algorithm consists of the following steps (the value of *y* will be determined later):

a. Find $(\pi(y) + 1)$integers $r_1, r_2 \dots r_{(\pi(y)+1)}$ (where $\pi(y)$, the number of primes less than *y*), such that$r_i^2 \bmod n$ can be written as a product of primes (and their powers) $\le y$.
b. Finding a subset *U* of these numbers, such that the product of these numbers is a perfect square (mod *n*).
c. If integers *x, y* is found such that $x \equiv \pm y \pmod n$ repeat the process.

Using this algorithm it can be shown that the probability to find an integer r_i, such that $r_i < n$ wherer_i^2can be written as the products of all primes less than *y* which is approximately equal to u^{-u} where $u = log\ n/log\ y$. Thus, for finding $(\pi(y) + 1))$ r_i's, $(\pi(y) + 1))u^u$ numbers should be randomly guessed. Since *u* depends on *y*, then if *y* is large, then u^{-u} is large, such that the probability of finding smooth r_i*'s* is high. However, if *y* is large then it takes more time for verifying whether r_i is actually smooth and for finding the subset *U* (see step 2). Conversely, if *y* is small, then the time for verifying whether r_i is actually smooth and for finding the subset *U* is low, but u^{-u} becomes small. Thus, it means that a lot of numbers should be guessed before we find r_i , that satisfies our conditions. Finally, *y* should be chosen from an intermediate range. Based on [8] the appropriate value of *y* is

$$y \approx \sqrt{\frac{\log n}{2k} log\ (log\ n)} \quad (6)$$

where $k \in Z$and $f(r+kp)^2 \equiv 0 \bmod p$ and *p* is a prime number in the factor base.

Finally, it can be concluded that the probability for obtaining the prime factors of *n* is approximately $u^{-u} = 1/(log\ n/log\ y)^{(log\ n/log\ y)} < 1$ since $log\ n/log\ y$ is greater than 1.

Since for obtaining *ID*, the attacker should at first obtain the inverse of the hash function, then the probability of obtaining the inverse should be observed. Since the probability for obtaining the inverse of a hash is less than is less than the probability for obtaining the collision

attack, then in this case the probability for obtaining the collision attack should be observed. Suppose keccak-256 is used, then it can be attacked by methods which were proposed by Dinur et al. [9,14], Naya-Plasencia et al. [13], Kolbl et al. [15] and Daemen et al. [17]. Assume that the attacker used an attack proposed by Daemen et al. [17] with probability of 2^{-296}, in the 24-round collision attack, then the probability of obtaining the collision is equal to 2^{-296}[17].Since the probability of obtaining the inverse of a hash value is always less than the probability for obtaining its collision, then the probability for obtaining the inverse of Keccak hash value is less than 2^{-296}. Thus, the probability for obtaining the user *ID* which depended on the probability of factoring the modulus number *n* and the probability for obtaining the inverse of the hash (less than the probability for obtaining the collision) is as follows

$$Pr_{ID} \approx (u^{-u})(m) \quad (7)$$

where *m* is the probability for obtaining the inverse of *H(ID)* which is less than the probability for obtaining the collision of Keccak-256, and u^{-u} is the probability for factoring the modulus number *n*.

In Wang's scheme, the probability for obtaining *ID* after *x* is compromised is 1, because the attacker can directly obtain *ID* after obtaining the message $\{C_1, CID, M\}$ and calculating $Y_1=(C_1)^x$ mod *n* using the compromised private key *x*, such that *ID* can be directly obtained by calculating $ID= CID \oplus h(C_1 \| Y_1)$.

Finally, it can be concluded that the proposed method is stronger compared with Wang's and Lee's Scheme, because the probability for obtaining *ID* using the proposed method is $(u^{-u})(m)$, while using Wang's scheme is 1 and using Lee's scheme is *m*.

B. Security Analysis against Impersonation Attack

The strategy for analyzing the security of the proposed method against impersonation attack, is by applying/inputting *ID'* and *Pw'* (fake *ID* and *Pw*) in the login phase, and observed the result of the scheme. The detailed impersonation attack is show in Figure 6. Impersonation attack is conducted by trying to insert fake *Pw* and *ID*. According to Figure 6, if the fake password *Pw* and *ID* are not equal with the original ones, then the session will be terminated, because A≠A' and $(C1)^x \neq C'$. For calculating the probability of succeeding in impersonation attack, we have to calculate the probability to obtain *ID'* and *Pw'* which is equal to *ID* and *Pw*.

For succeeding in impersonation attack, $C1^x=C$, and $G= h(SK \| ID)$ should be hold. Since for calculating *C* the attacker should obtain the value *Pw* from *B* (where $B=g^{bPwX} \bmod n \oplus h(ID)$), then the probability for obtaining *Pw* is equal to the calculation of discrete log of $g^{bPw.x} \bmod n$ which is a hard problem even if the attacker knows *x*and *b*. Furthermore, the attacker should obtain the value of *ID* for calculating *D*. *ID* can be obtained from *B*, by obtaining $g^{bPw.x} \bmod n$ first, then the probability of obtaining *ID* depends on the probability for obtaining *Pw*. In other words, the probability for obtaining *ID* and *Pw* is equivalent with the discrete logarithm problem which is a hard problem.

7. Computation Cost Evaluation

This section discussed the computation cost comparison between Wang's, Lee's and the proposed scheme. These three schemes used three computations: exponential operation, symmetric encryption/decryption, and hash function. Suppose TE, T_S, and TH, denote the time complexity for exponential operation, symmetric encryption/decryption, and hash function, respectively. Based on Figure 1, Wang's scheme uses 6 exponential processes and 14 hash processes, or the computation complexity was 6 T_E + 14 T_H. Based on Figure 2, Lee's scheme uses 6 exponential processes, 1 symmetric encryption-decryption process, and 10 hash processes, or the computation complexity was 6 T_E + 10 T_H.

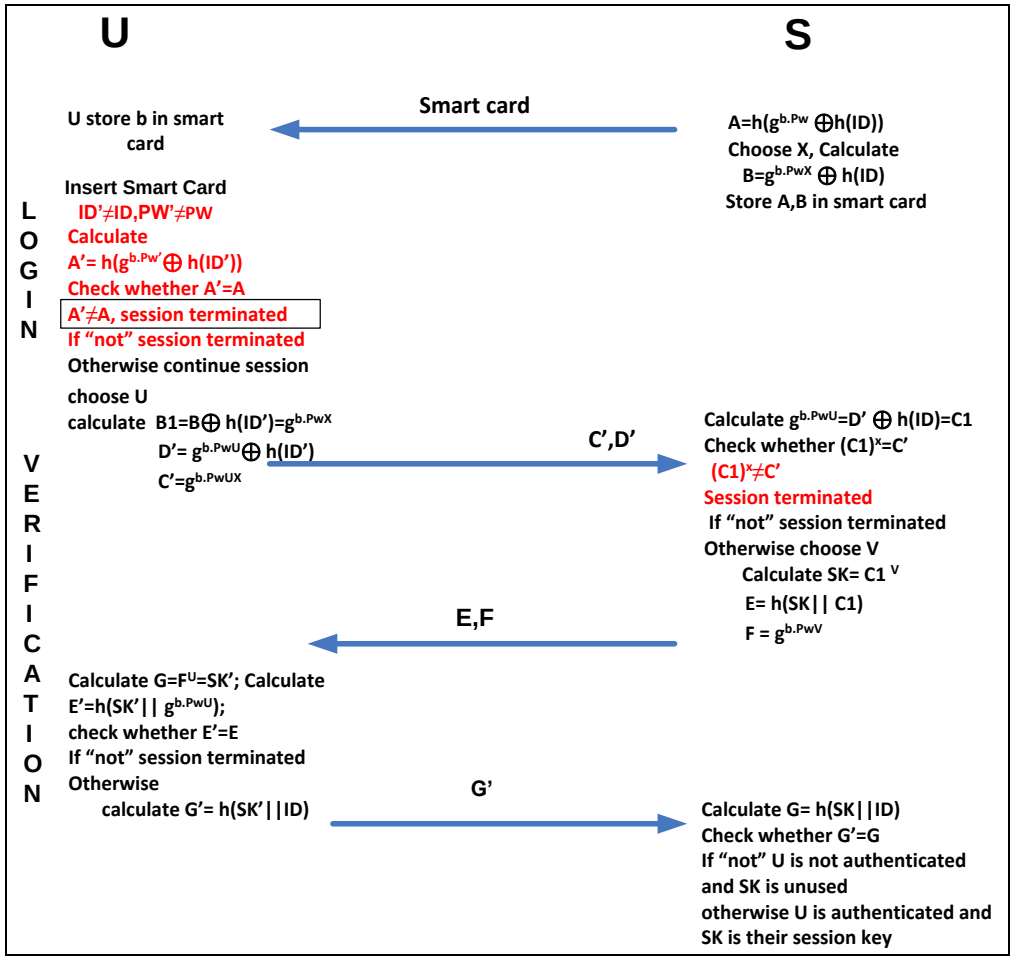

Figure 6. Impersonation Attack

The proposed scheme uses 6 exponential processes and 6 hash processor the computation complexity was $6T_E + 6T_H$.The result of the evaluation is shown in Table 3.

Table 3. Computation cost comparison.

Name of the Scheme	Cost for Exponential operation	Cost for encryption/decryption	Cost for hash function evaluation	Total Computation Cost
Wang's	6		14	$6\ T_E + 14\ T_H$
Lee's	6	1	10	$6\ T_E + 1\ T_C + 10T_H$
Proposed	6		6	$6\ T_E + 6\ T_H$

Finally, it can be concluded that for succeeding the impersonation attack on the proposed method, the attacker should solve the hard problem. In other word, the scheme is secure against impersonation attack.

8. Conclusion

Based on the discussion concerning the security analysis, it can be concluded that forward anonymity can be maintained by introducing discrete logarithm problem into dynamic identity

based authentication scheme. The analysis showed that the probability for obtaining the identity using proposed scheme is $(u^{-u})(m)$ which is less than the probability in Wang and Lee scheme. The computation cost of the proposed method is 6 T_E+ 6 T_H which is less than the computation cost of Wang's and Lee's scheme as well, while maintaining the security against impersonation attack.

9. References

[1]. Martínez-Peláez, R. &Rico-Novella, F., Weaknesses of an Improvement Authentication Scheme using Smart Cards, *IACR Cryptology e-Print Archive*, 2012

[2]. Kim, H., Cryptanalysis of Modified Dynamic ID-based User Authentication Scheme Resisting Smart-Card-Theft Attack, *International Journal of Mathematical Analysis*, 8(49), pp. 2413-2419, 2014.

[3]. Zhai, J., Cao, T., Chen, X and Huang, S., Security on dynamic ID-Based Authentication Schemes, International Journal of Security and Its Applications: 9(1) , pp.387-396, 2015.

[4]. Bach, E., Discrete Logarithm and Factoring, *Technical Report, University of California*, Berkeley, 1984

[5]. W. Diffie and M. E. Hellman, New Directions in Cryptography, *IEEE Transactions on Information Theory*, Vol. IT.22, No.6, November, 1976.

[6]. Ding Wang, Ping Wang, Chun-guang Ma, and Zhong Chen, Robust Smart Card based Password Authentication Scheme against Smart Card Security Breach, *Cryptology ePrint Archive*: Report 2012/439

[7]. G. Bertoni, J. Daemen, M. Peeters, G.V. Assche, Keccak Sponge Function Family, Main Document, Version 1.2, April 2009,

[8]. J. Hoffstein, J. Pipher, J.H. Silverman, An Introduction to Mathematical Cryptography, Springer, 2008.

[9]. Dinur, O. Dunkelman, and A. Shamir, Collision Attacks on Up to 5 Rounds of SHA-3 Using Generalized Internal Differentials, *Fast Software Encryption*, pp. 219-240, January 2014.

[10]. Smart, N.P., Cryptography Made Simple, ed. 1, Springer International Publishing, 2016.

[11]. Granger, R., Kleinjung, T. & Zumbr¨agel, J., On the discrete logarithm problem in finite fields of fixed characteristic, IACR e-Print, *International Association of Cryptologic Research*, 685, 2015.

[12]. Stern, J., Evaluation Report on the Discrete Logarithm Problem over finite fields, Technical Report, Cryptrec, Japan, 1027, 2001

[13]. Naya-Plasencia, M., Rock, A., and Meier, W., Practical Analysis of Reduced-Round Keccak, Indocrypt, Volume 7107 of the series Lecture Notes in Computer Science pp. 236-254, 2011

[14]. Dinur, I., Dunkelman, O., and Shamir. A., New attacks on Keccak-224 and Keccak-256, IACR e-Print, *International Association of Cryptologic Research*, 624, 2011.

[15]. Kolbl, S., Mendel, F., Nad, T., Schlaffer, M., Differential Cryptanalysis of Keccak Variants, Cryptography and Coding, Volume 8308, of the series Lecture Notes in Computer Science pp. 141-157, 2013.

[16]. Hanwook Lee, Junghyun Nam, Moonseong Kim and Dongho Won, Forward Anonymity-Preserving Secure Remote Authentication Scheme, *Ksii Transactions on Internet and Information Systems* Volume 10, No. 3, Mar, pp.1289-1310, 2016.

[17]. Daemen, J., and Assche, G. v., Differential propagation analysis of Keccak, Fast Software Encryption, March 19-21, 2012.

Ari Moesriami Barmawi received B.Sc from the Department of Electrical Engineering, Bandung Institute of Technology, Indonesia in 1985, M.Sc and Ph.D from the Department of Computer Science, Keio University, Japan in 1997 and 2001 respectively. Her research interests are Cryptography, Steganography, and Artificial Intelligence. She is a member of IEEE and IACR (International Association of Cryptography Researcher). Now she is the head of Intelligence, Multimedia and Computation research group in Telkom University Bandung. She is the TPC of IEEE and ACM Conferences.

Fiky Y. Suratman was born in Jakarta, Indonesia, in 1976. He received Bachelor Degree from Engineering Physics and Master Degree from School of Electrical and Informatics (STEI), Institut Teknologi Bandung, Bandung, Indonesia in 1998 and 2006, respectively. He was awarded scholarship from German Academic Exchange Service (DAAD) to continue his study at Technische Universitaet Darmstadt (TU-Darmstadt), Germany, until he recived his Dr.-Ing. Degree (PhD) in 2014. Early placement in industry (Astra Microtronics Technology) from 1998 to 2001, was then followed by lectureship in Universitas Komputer Indonesia (UNIKOM). In 2007, he joined the Faculty of Electrial Engineering, Institut Teknologi Telkom (now Universitas Telkom) as a faculty member. He is the head of Master Degree of Electrical Engineering, Telkom University since 2014. He is a member of IEEE (Signal Processing Soiciety and Communications Society), and since 2016 he is the chair of Signal Processing Society (SPS) Indonesia Chapter. Dr. Fiky was the TPC chair for Asia Pasific Conference on Wireless and Mobile (APWiMob) 2016 held in Bandung Indonesia, and was the the chair for International Conference on Signal and Systems (ICSIGSYS) 2017 held in Bali Indonesia. His research interest lies on Statistical Signal Processing and Radar Signal Processing.