International Journal of Security and Its Applications
Vol. 10, No. 3 (2016), pp.193-204
http://dx.doi.org/10.14257/ijsia.2016.10.3.18

A Provably-Anonymous Authentication Scheme for Roaming Services

Junghyun Nam[1], Kim-Kwang Raymond Choo[2] and Juryon Paik[3,*]

[1]*Department of Computer Engineering, Konkuk University, Korea*
[2]*School of Information Technology & Mathematical Sciences, University of South Australia, Australia*
[3]*Department of Digital Information & Statistics, Pyeongtaek University, Korea*
jhnam@kku.ac.kr, raymond.choo@unisa.edu.au
jrpaik@ptu.ac.kr
**Corresponding author*

Abstract

In this work, we extend the widely accepted security model of Bellare, Pointcheval and Rogaway (2000) in order to prove the security of smart-card-based roaming authentication (SRA) schemes. More specifically, in this extended model, we provide formal definitions of authenticated key exchange and user anonymity for SRA schemes, in order to capture side-channel, offline dictionary, and other common attacks. We then present a new SRA scheme and prove its security in our extended model. To the best of our knowledge, our proposed scheme is the first provably-secure SRA scheme that achieves user anonymity. We conclude by demonstrating that our scheme is also computationally efficient relative to other similar published schemes without a security proof.

Keywords*: Authentication scheme, Roaming service, User anonymity, Smart card, Two-factor security*

1. Introduction

Advancements in mobile computing and other communications technologies have resulted in the increasing popularity of lightweight devices with wireless communication capabilities [1]. To fully enjoy the convenience of mobility, wireless devices travelling outside the geographical coverage of the home network should be provided with a seamless roaming service in the visited foreign network. Typically, there are three parties involved in a roaming process: *a mobile user*, *the foreign agent*, and *the home agent*. While security challenges in providing seamless roaming are not new, they are still a topic of current interest. More specifically, authenticated key exchange between a mobile user and a foreign agent should be achieved with the assistance of the home agent to prevent illegal usage of the network and to protect subsequent communications. The challenge of authenticated key exchange in mobile roaming systems is complicated by the need to ensure the anonymity of the mobile user is preserved. Anonymity is a property that is important not only in roaming services, but many other applications too (e.g. location-based services, anonymous web browsing, and e-voting).

Not surprising, roaming authentication schemes are a subject of active computer science research, and examples of roaming authentication schemes for smart cards include those presented in [2-19]. Smart-card-based schemes have attracted the attention of researchers due to their potential to be widely deployed. A key security requirement for such schemes is to guarantee that only a user who is in possession of both a smart card and the corresponding password can be authenticated by their home agent; thus,

ISSN: 1738-9976 IJSIA

establishing a session key with the foreign agent. A smart-card-based roaming authentication (SRA) scheme that meets this requirement is said to achieve *two-factor security*. To capture the notion of two-factor security, the adversary against SRT schemes is assumed to be able to either extract the sensitive information in the smart card of a mobile user possibly via a side-channel attack [20, 21] or learn the password of the mobile user through shoulder-surfing or by employing a malicious card reader, but not both. Clearly, there is no way to prevent the adversary from impersonating a mobile user if the information in the smart card and the password of the mobile user are both disclosed.

Designing roaming authentication (and other cryptographic) schemes and proving their security are, however, time-consuming and error-prone [22-25]. This is, perhaps, why most published schemes either provide no formal security proof [2, 3, 5, 7, 8, 11-16] or fail to achieve important security properties such as authentication, user anonymity, session-key security, two-factor security, and resistance against offline dictionary attacks [2, 3, 26, 4, 27, 6-8, 11, 12, 14-17]. Some schemes [4, 6, 9, 10, 17] have been proven secure using formal method tools, which is known to suffer from limitations such as undecidability and intractability. Thus, using such an approach could lead to a false positive result. At the time of research, Xie et al.'s (2014) scheme [18] is the only provably-secure SRT scheme proven secure, but it has not been proven to provide user anonymity.

Our contributions in this paper are two-fold:

1. We formulate a security model for the analysis of SRA schemes. Our model extends the widely accepted model of Bellare, Pointcheval and Rogaway [28] to incorporate user anonymity property and the notion of two-factor security. Note that the original Bellare-Pointcheval-Rogaway (BPR) model for authenticated key exchange (AKE) captures offline dictionary attacks and many other common attacks, and readers are referred to Ref. [29] to understand how a key exchange scheme that is not secure against an offline dictionary attack cannot achieve the AKE security in the BPR model. Our extension of the BPR model provides two security definitions, one for the AKE security and one for user anonymity. Both definitions capture the notion of two-factor security as they are defined considering the adversary's capability of corrupting users' smart cards. Authentication, session-key security, perfect forward secrecy, known-key security, and resistance against offline dictionary attacks by insiders/outsiders properties are implied by the AKE security.
2. We present the first SRA scheme whose AKE security as well as anonymity are formally proved in the extended model and random oracle model under the computational Diffie-Hellman (CDH) assumption. Our provably-secure scheme is also computationally efficient and, as we demonstrate in this paper, is among the best performing schemes that provide both anonymity and perfect forward secrecy.

The remainder of this paper is structured as follows. The next section describes our extended model. In Section 3, we present our proposed scheme along with cryptographic primitives on which the security of our scheme relies. We conclude with a comparative efficiency and security of our scheme and other similar published schemes in Section 4.

2. Our Extended Security Model for SRA Schemes

Here we describe a security model extended from the BPR model [28] to capture the security properties of SRT schemes.

Participants and long-lived keys. Let HA be the home agent, FA be the foreign agent, $\boldsymbol{U}$ be the set of all mobile users registered with HA, and $\boldsymbol{E} = \boldsymbol{U} \cup \{HA\} \cup \{FA\}$. We assume that each entity $E \in \boldsymbol{E}$ is identified by a string, and E and ID_E are used

interchangeably to refer to this identifier string. To capture the notion of user anonymity, we also assume that: (1) each mobile user $MU \in \boldsymbol{U}$ has its pseudo identity PID_{MU} (in addition to its true identity ID_{MU}) and (2) the adversary $\boldsymbol{A}$ is given only PID_{MU} but not ID_{MU}. A mobile user MU may run multiple sessions of the authentication and key exchange protocol of the scheme (hereafter called the key exchange protocol or simply the protocol), either serially or concurrently, to establish a session key with FA. Thus, at any given time, there could be multiple instances of MU, HA and FA. We use Π_E^i to denote instance i of entity $E \in \boldsymbol{E}$. Instances of MU and FA are said to *accept* when they compute a session key in an execution of the protocol. We denote the session key of Π_E^i by sk_E^i. Before the protocol is ever executed, each $MU \in \boldsymbol{U}$ selects its private password pw_{MU} from the set of all possible passwords $\boldsymbol{PW}$ while HA generates a master secret x, establishes a shared secret k_{HF} with FA, and issues a smart card to each $MU \in \boldsymbol{U}$.

Partnering. Two instances are regarded as *partners* if they participate in a protocol execution and establish a (shared) session key, and these two instances share the same session identifier (sid). The latter is a unique identifier of a protocol session and usually defined as a function of the messages transmitted in the session. Let sid_E^i denotes the sid of instance Π_E^i, and two instances, Π_{MU}^i and Π_{FA}^j, are partners if (1) both instances have accepted and (2) $sid_{MU}^i = sid_{FA}^j$.

Adversary capabilities. The probabilistic polynomial-time (ppt) adversary, $\boldsymbol{A}$, is in complete control of communications between protocol participants. The adversary's capabilities are modeled using the below oracle queries, and the adversary does not need to know the true identity of a user to make oracle query to an instance of the user. We also remark that only the $Execute$ query models passive attacks against the protocol, and the $Send$, $Reveal$, $CorruptLL$, $CorruptSC$ queries model active attacks against the protocol.

- $Execute$ (Π_{MU}^i, Π_{FA}^j, Π_{HA}^k): This query executes a normal protocol run between Π_{MU}^i, Π_{FA}^j and Π_{HA}^k. Upon completion of the protocol execution, the transcript will be returned to $\boldsymbol{A}$.
- $Send$ (Π_E^i, *m*): Upon receiving *m*, the instance Π_E^i proceeds according to the protocol specification, and any output by Π_E^i is returned to $\boldsymbol{A}$. A query of the form $Send$ (Π_{MU}^i,start) prompts Π_{MU}^i to initiate the protocol.
- $Reveal$ (Π_E^i): This query captures the notion of known key security. Π_E^i, upon receiving the query and if it has accepted, returns the session key, sk_E^i, to $\boldsymbol{A}$.
- $CorruptLL$ (*E*): This query captures the notions of forward secrecy, unknown key share attacks and insider attacks. The adversary will receive the long-lived secrets of entity *E* as a result of this query.
- $CorruptSC$ (*MU*): This query, capturing the notion of two-factor security, results in the return of information stored on *MU*'s smart card.

- $TestAKE(\Pi_E^i)$: This query is used to *define* the indistinguishability-based security of session keys. If Π_E^i has accepted, then depending on a randomly chosen bit *b*, $\boldsymbol{A}$ is given either the real session key sk_E^i (if $b = 1$) or a random key drawn from the session-key space (if $b = 0$).
- $TestID(MU)$: This query is used to determine whether the protocol provides user anonymity (or not). Depending on a random bit *b* chosen by the oracle, $\boldsymbol{A}$ is given either MU's identity used in the protocol executions (if $b = 1$) or a random identity drawn from the identity space (if $b = 0$).

MU is corrupted if both $CorruptLL(MU)$ and $CorruptSC(MU)$ have been queried, and HA (resp. FA) is corrupted when $CorruptLL(HA)$ (resp. $CorruptLL(FA)$) is asked.

Authenticated key exchange (AKE). The AKE security of a key exchange protocol P also depends on the notion of *freshness*, where a fresh instance is one that holds a session key which should not be known to $\boldsymbol{A}$ (i.e. an unfresh instance is one whose session key, or some information about the key, is revealed).

Definition 1 (Freshness). An instance Π_E^i is fresh unless one of the following occurs:

1. $\boldsymbol{A}$ queries $Reveal(\Pi_E^i)$ or $Reveal(\Pi_{E'}^j)$, where $\Pi_{E'}^j$ is the partner of Π_E^i;
2. $\boldsymbol{A}$ queries $CorruptLL(FA)$ or $CorruptLL(HA)$ before Π_E^i accepts.
3. $\boldsymbol{A}$ queries both $CorruptLL(MU)$ and $CorruptSC(MU)$, for some $MU \in \boldsymbol{U}$, before Π_E^i accepts.

The AKE security of the protocol P is defined in the context of the following two-phase experiment:

Experiment $\boldsymbol{ExpAKE_0}$:

Phase 1. $\boldsymbol{A}$ makes any oracle queries at will, with the following restrictions:

1. No query to the $TestID$ oracle.
2. No $TestAKE(\Pi_E^i)$ query if the instance Π_E^i is not fresh.
3. No $Reveal(\Pi_E^i)$ query if $\boldsymbol{A}$ has already made a $TestAKE$ query to Π_E^i or $\Pi_{E'}^j$, where $\Pi_{E'}^j$ is the partner of Π_E^i.

Phase 2. Once $\boldsymbol{A}$ decides that Phase 1 is over, it outputs a bit b' as a guess on the hidden bit *b* chosen by the $TestAKE$ oracle. $\boldsymbol{A}$ is said to succeed if $b = b'$.

Let $SuccAKE_0$ be the event that $\boldsymbol{A}$ succeeds in the experiment $\boldsymbol{ExpAKE_0}$. Let $Adv_P^{AKE}(\boldsymbol{A})$ denote the advantage of $\boldsymbol{A}$ in breaking the AKE security of protocol P and be defined as $Adv_P^{AKE}(\boldsymbol{A}) = 2 \cdot \Pr_{P,\boldsymbol{A}}[SuccAKE_0] - 1$.

Definition 2 (AKE security). A key exchange protocol P is *AKE-secure* if $Adv_P^{AKE}(\boldsymbol{A})$ is negligible for any ppt adversary $\boldsymbol{A}$.

User anonymity. As we have previously noted, AKE security (Definition 2) does not imply user anonymity; thus, an AKE-secure key exchange protocol does not necessarily provide user anonymity. Hence, a new, separate definition is necessary to capture the user anonymity property. Our definition of user anonymity is based on the notion of cleanness.

Definition 3 (Cleanness). A mobile user MU is *clean* unless one of the following occurs:

1. $\boldsymbol{A}$ queries $\mathsf{CorruptLL}(HA)$.
2. $\boldsymbol{A}$ queries both $\mathsf{CorruptLL}(MU)$ and $\mathsf{CorruptSC}(MU)$.

In order to model user anonymity even against FA, Definition 3 does not restrict $\boldsymbol{A}$ from asking a $\mathsf{CorruptLL}$ query to FA.

We use the following experiment to formalize the user anonymity property:

Experiment $\boldsymbol{ExpID_0}$:

Phase 1. $\boldsymbol{A}$ is allowed to ask any oracle queries, except to the $\mathsf{TestAKE}$ oracle. In addition, $\boldsymbol{A}$ is neither allowed to make the $\mathsf{TestID}(MU)$ query when MU is not clean nor $\mathsf{CorruptLL}$ and $\mathsf{CorruptSC}$ queries against HA and MU if it has already made the $\mathsf{TestID}(MU)$ query.

Phase 2. $\boldsymbol{A}$ outputs a bit b' as a guess on the hidden bit b chosen by the TestID oracle, once it decides that Phase 1 is over.

Let SuccID_0 be the event that $\boldsymbol{A}$ succeeds in $\boldsymbol{ExpID_0}$ (i.e. $b = b'$). Then, we define the advantage of $\boldsymbol{A}$ in breaking user anonymity of protocol P as $\mathsf{Adv}_P^{ID}(\boldsymbol{A}) = 2 \cdot \Pr_{P,\boldsymbol{A}}[\mathsf{SuccID}_0] - 1$.

Definition 4 (User anonymity). A key exchange protocol P provides *user anonymity* if $\mathsf{Adv}_P^{ID}(\boldsymbol{A})$ is negligible for any ppt adversary $\boldsymbol{A}$.

3. Our Proposed Scheme

This section presents our proposed SRA scheme.

3.1. Preliminaries

Computational Diffie-Hellman (CDH) assumption. Let $\boldsymbol{G}$ be a cyclic group of prime order q, and g be an arbitrary generator of $\boldsymbol{G}$. (In practice, $\boldsymbol{G}$ could be either a multiplicative group over an ordinary finite field or an additive group on an elliptic curve, though it is written multiplicatively in this paper.) Informally stated, the CDH problem for $\boldsymbol{G}$ is to compute $g^{xy} \in \boldsymbol{G}$ when given two elements $(g^x, g^y) \in \boldsymbol{G}^2$, where x and y are chosen at random from $\boldsymbol{Z}_q^*$. We say that the CDH assumption holds in $\boldsymbol{G}$ if it is computationally infeasible to solve the CDH problem for $\boldsymbol{G}$. More formally, we define the advantage of an algorithm $\boldsymbol{A}$ in solving the CDH problem for $\boldsymbol{G}$ as $\mathsf{Adv}_{\boldsymbol{G}}^{CDH}(\boldsymbol{A}) = \Pr[\boldsymbol{A}(\boldsymbol{G}, g, g^x, g^y) = g^{xy}]$. We say that the CDH assumption holds in $\boldsymbol{G}$ if $\mathsf{Adv}_{\boldsymbol{G}}^{CDH}(\boldsymbol{A})$ is negligible for all ppt algorithms $\boldsymbol{A}$. We denote by $\mathsf{Adv}_{\boldsymbol{G}}^{CDH}(t)$ the maximum value of $\mathsf{Adv}_{\boldsymbol{G}}^{CDH}(\boldsymbol{A})$ over all algorithms $\boldsymbol{A}$ running in time at most t.

Message authentication codes. A message authentication code (MAC) scheme Σ is a pair of efficient algorithms (Mac, Ver) where: (1) Mac takes as input an ℓ-bit key k and a message m, and outputs a MAC (also known as a tag) σ; and (2) Ver takes as input a key k, a message m, and a MAC σ, and outputs 1 if σ is valid for m under k or outputs 0 if σ is invalid. Let $Adv_{\Sigma}^{CMA}(\boldsymbol{A})$ be the advantage of $\boldsymbol{A}$ in violating the strong existential unforgeability of Σ under an adaptive chosen message attack. More precisely, $Adv_{\Sigma}^{CMA}(\boldsymbol{A})$ is the probability that $\boldsymbol{A}$, who mounts an adaptive chosen message attack against Σ with oracle access to $Mac_k(\cdot)$ and $Ver_k(\cdot)$, outputs a message/tag pair (m, σ) such that: (1) $Ver_k(m, \sigma) = 1$ and (2) σ was not previously output by the oracle $Mac_k(\cdot)$ as a MAC on the message m. We say that the MAC scheme Σ is secure if $Adv_{\Sigma}^{CMA}(\boldsymbol{A})$ is negligible for every ppt adversary $\boldsymbol{A}$. Let $Adv_{\Sigma}^{CMA}(t)$ denote the maximum value of $Adv_{\Sigma}^{CMA}(\boldsymbol{A})$ over all adversaries $\boldsymbol{A}$ running in time at most t.

Symmetric encryption schemes. A symmetric encryption scheme Ω is a pair of efficient algorithms (Enc, Dec) where: (1) Enc takes as input an ℓ-bit key k and a plaintext message m, and outputs a ciphertext c; and (2) Dec takes as input a key k and a ciphertext c, and outputs a message m. We require that $Dec_k(Enc_k(m)) = m$ holds for all $k \in \{0,1\}^{\ell}$ and all $m \in \boldsymbol{M}$, where $\boldsymbol{M}$ is the plaintext space.

Cryptographic hash functions. Additionally, our scheme uses three cryptographic hash functions $F: \{0,1\}^* \rightarrow \{0,1\}^{\ell}$, $H: \{0,1\}^* \rightarrow \{0,1\}^{\kappa}$, and $I: \{0,1\}^* \rightarrow \{0,1\}^{\varepsilon}$, where ℓ is as defined for Σ and Ω, κ is the bit-length of session keys, and ε is the bit-length of SID_{MU} (see the registration phase of our scheme below). These hash functions are modelled as random oracles in our security proofs.

3.2. Description of the Scheme

The public system parameters for our scheme include: (1) a cyclic group $\boldsymbol{G}$ of prime order q, and a generator g of group $\boldsymbol{G}$, (2) a MAC scheme $\Sigma = (Mac, Ver)$, (3) a symmetric encryption scheme $\Omega = (Enc, Dec)$, and (4) three hash functions F, H and I. These public system parameters are fixed during initialization and are known to all network participants. As part of the initialization, HA selects the master secret key $x \in \boldsymbol{Z}_q^*$, computes the corresponding public key $X = g^x$, and shares an ℓ-bit secret key k_{HF} with FA.

3.2.1. Registration Phase

A mobile user MU registers itself with the home agent HA as follows:

1. MU chooses its identity ID_{MU} and password pw_{MU}, and submits ID_{MU} to HA via a secure channel.
2. HA computes $SID_{MU} = Enc_{F(x)}(ID_{MU} \| ID_{HA})$ and issues MU a smart card loaded with $\{SID_{MU}, X, ID_{HA}, \boldsymbol{G}, g, \Sigma, \Omega, F, H, I\}$.
3. MU replaces SID_{MU} with $TID_{MU} = SID_{MU} \oplus I(ID_{MU} \| pw_{MU})$.

3.2.2. Authentication and Key Exchange Phase

Whenever MU roams in a foreign network, it needs to perform this phase with FA and HA to gain access to the network - see Figure 1:

Step 1. MU inserts its smart card into a card reader, and inputs its identity ID_{MU} and password pw_{MU}. Next, MU retrieves the current timestamp T_1, chooses a random number $a \in Z_q^*$, and computes

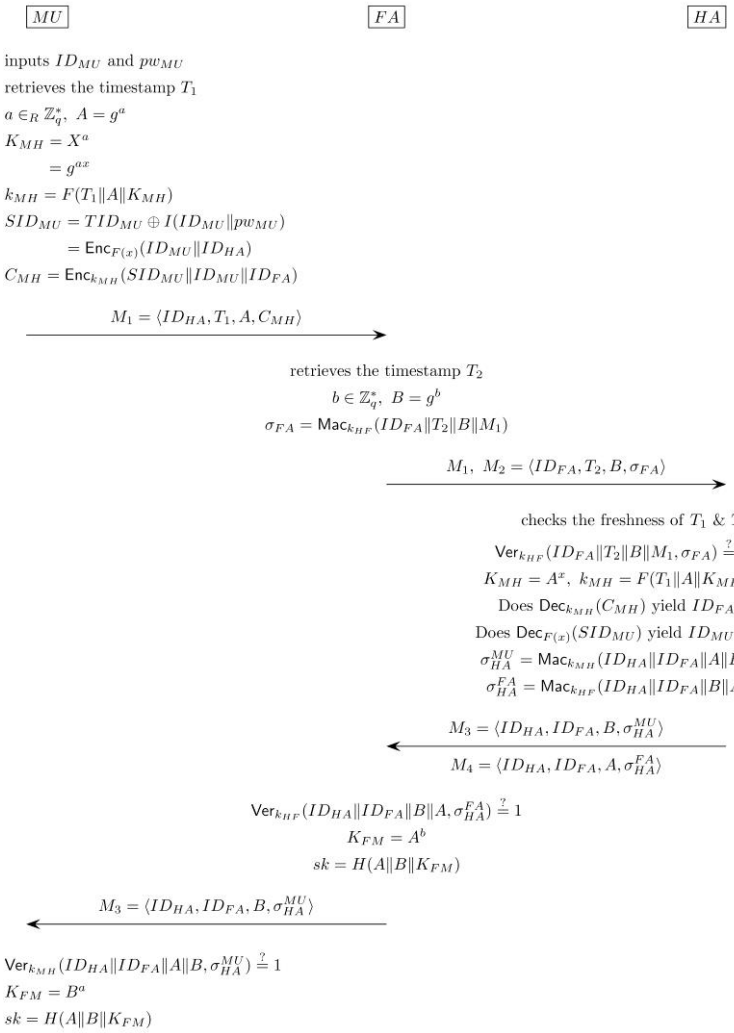

Figure 1. The Authentication and Key Exchange Phase of Our Proposed Scheme.

$$A = g^a,$$

$$K_{MH} = X^a,$$

$$k_{MH} = F(T_1 \| A \| K_{MH}),$$

$$SID_{MU} = TID_{MU} \oplus I(ID_{MU} \| pw_{MU}) = Enc_{F(x)}(ID_{MU} \| ID_{HA}),$$

$$C_{MH} = Enc_{k_{MH}}(SID_{MU} \| ID_{MU} \| ID_{FA}).$$

Then, MU sends $M_1 = \langle ID_{HA}, T_1, A, C_{MH} \rangle$ to FA.

Step 2. FA retrieves the current timestamp T_2, chooses a random number $b \in \mathbf{Z}_q^*$, and computes

$$B = g^b,$$

$$\sigma_{FA} = Mac_{k_{HF}}(ID_{FA} \| T_2 \| B \| M_1).$$

FA then sends $M_2 = \langle ID_{FA}, T_2, \mathrm{B}, \sigma_{FA} \rangle$ and M_1 to HA.

Step 3. HA verifies that (1) T_1 and T_2 are fresh and (2) $Ver_{k_{HF}}(ID_{FA} \| T_2 \| B \| M_1, \sigma_{FA}) = 1$. If either verification fails, HA aborts the session. Otherwise, HA computes $K_{MH} = A^x$ and $k_{MH} = F(T_1 \| A \| K_{MH})$, decrypts C_{MH} with key k_{MH}, and checks if the decryption produces the same ID_{FA} as in M_2. HA aborts if the check fails. Otherwise, HA decrypts SID_{MU} with key $F(x)$ and checks if this decryption yields the same ID_{MU} as produced through the decryption of C_{MH}. When both IDs match, HA computes $\sigma_{HA}^{MU} = Mac_{k_{MH}}(ID_{HA} \| ID_{FA} \| A \| \quad B)$ and $\sigma_{HA}^{FA} = Mac_{k_{HF}}(ID_{HA} \| ID_{FA} \| B \| A)$, and sends $M_3 = \langle ID_{HA}, ID_{FA}, B, \sigma_{HA}^{MU} \rangle$ and $M_4 = \langle ID_{HA}, ID_{FA}, A, \sigma_{HA}^{FA} \rangle$ to FA.

Step 4. FA verifies that $Ver_{k_{HF}}(ID_{HA} \| ID_{FA} \| B \| A, \sigma_{HA}^{FA}) = 1$. If the verification fails, FA aborts the session. Otherwise, FA forwards M_3 to MU, and computes the shared secret $K_{FM} = A^b$ and the session key $sk = H(A \| B \| K_{FM})$.

Step 5. MU computes $K_{FM} = B^a$ and $sk = H(A \| B \| K_{FM})$ if $Ver_{k_{MH}}(ID_{HA} \| ID_{FA} \| A \| B, \sigma_{HA}^{MU}) = 1$, and aborts the session, otherwise.

3.2.3. Password Update Phase

Our scheme is design to facilitate cyber hygiene by allowing mobile users to change their passwords anytime.

1. MU inserts smart card into a card reader and enters ID_{MU}, current password pw_{MU}, and new password pw'_{MU}.
2. The smart card computes $TID'_{MU} = TID_{MU} \oplus I(ID_{MU} \| pw_{MU}) \oplus I(ID_{MU} \| pw'_{MU})$ and replaces TID_{MU} with TID'_{MU}.

4. Concluding Remarks

In this paper, we proposed an extension of the model of Bellare, Pointcheval and Rogaway [28] in order to formally capture security requirements for smart-card-based roaming authentication (SRA) schemes. This allows us to formally define user anonymity and the AKE security, while capturing the notion of two-factor security. We also proved the security of our proposed SRA scheme in the extended model, which demonstrated that the scheme achieves user anonymity and AKE security.

Table 1. Comparative Summary: Efficiency and Security

Scheme	Computation		Security proof	
	MU	$MU + FA + HA$	AKE	Anonymity
Our scheme	$3E + 1S + 1M + 3H$	$6E + 3S + 6M + 6H$	Yes	Yes
XHBDW [18]	$3E + 2S + 4H$	$6E + 7S + 8H$	Yes	No
XHTBY [17]	$3E + 2S + 4H$	$8E + 9S + 8H$	Computer security approach	No
HKKL [16]	$3E + 2S + 7H$	$6E + 9S + 12H$	No	No

E: modular exponentiation/scalar-point multiplication
S: symmetric encryption/decryption
M: MAC generation/verification
H: hash function evaluation

Table 1 summarizes the computational requirements and the security proofs for existing SRA schemes that provide both user anonymity and perfect forward secrecy. Although the XHBDW scheme [18] was designed to work in an additive group on an elliptic curve, we do not differentiate between modular exponentiations and scalar-point multiplications in our efficiency comparison since one can easily derive an elliptic curve version of other schemes by replacing a modular exponentiation with a scalar-point multiplication. For example, the cyclic prime-order group $\boldsymbol{G}$ used in our scheme can be replaced with an additive group on an elliptic curve as mentioned in Section 3.1. Modular exponentiation is more expensive than other operations considered in Table 1, such as symmetric encryption/decryption, MAC generation/verification, and hash function evaluation. The total number of modular exponentiations required in XHTBY [17] is 8 while the number is reduced to 6 in the other schemes. Our scheme is comparable to the XHBDW scheme, since a MAC generation/verification is almost as fast as a hash function evaluation and a symmetric encryption/decryption is usually more expensive than a hash function evaluation (see http://www.cryptopp.com/benchmarks.html for Crypto++ benchmarks for some of the most commonly used cryptographic algorithms, such as HMAC, SHA1, DES and AES). The XHBDW scheme may be efficient, but it is proven secure in a model that captures only the AKE security and not user anonymity. To the best of our knowledge, our scheme is the first provably-secure SRA scheme that achieves both AKE security and user anonymity.

Acknowledgements

This paper was supported by Konkuk University in 2015.

References

[1] Y. Yang, J. Lu, K. K. R. Choo and J. Liu, "On lightweight security enforcement in cyber-physical systems", International Workshop on Lightweight Cryptography for Security and Privacy - LightSec,LNCS, vol. 9542, **(2015)**, pp. 97-112.
[2] C. Lee, M. Hwang and I. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments", IEEE Transactions on Industrial Electronics, vol. 53, no. 5, **(2006)**, pp. 1683-1687.

[3] C. Wu, W. Lee and W. Tsaur, "A secure authentication scheme with anonymity for wireless communications", IEEE Communications Letters, vol. 12, no. 10, **(2008)**, pp. 722-723.
[4] C. Chang, C. Lee and Y. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks", Computer Communications, vol. 32, no. 4, **(2009)**, pp. 611-618.
[5] J. Lee and T. Kwon, "Secure authentication scheme with improved anonymity for wireless environments", IEICE Transactions on Communications, vol. E94.B, no. 2, **(2011)**, pp. 554-557.
[6] C. Chen, D. He, S. Chan, J. Bu, Y. Gao and R. Fan, "Lightweight and provably secure user authentication with anonymity for the global mobility network", International Journal of Communication Systems, vol. 24, no. 3, **(2011)**, pp. 347-362.
[7] D. He, M. Ma, Y. Zhang, C. Chen and J. Bu, "A strong user authentication scheme with smart cards for wireless communications", Computer Communications, vol. 34, no. 3, **(2011)**, pp. 367-374.
[8] J. Xu, W. Zhu and D. Feng, "An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks", Computer Communications, vol. 34, no. 3, **(2011)**, pp. 319-325.
[9] Y. Chen, S. Chuang, L. Yeh and J. Huang, "A practical authentication protocol with anonymity for wireless access networks", Wireless Communications and Mobile Computing, vol. 11, no. 10, **(2011)**, pp. 1366-1375.
[10] D. He, S. Chan, C. Chen, J. Bu and R. Fan, "Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks", Wireless Personal Communications, vol. 61, no. 2, **(2011)**, pp. 465-476.
[11] C. Li and C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications", Mathematical and Computer Modelling, vol. 55, no. 1-2, **(2012)**, pp. 35-44.
[12] H. Mun, K. Han, Y. Lee, C. Yeun and H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks", Mathematical and Computer Modelling, vol. 55, no. 1-2, **(2012)**, pp. 214-222.
[13] K. Son, D. Han and D. Won, "A privacy-protecting authentication scheme for roaming services with smart cards", IEICE Transactions On Communications, vol. E95-B, no. 5, **(2012)**, pp. 1819-1821.
[14] W. Jeon, J. Kim, J. Nam, Y. Lee and D. Won, "An enhanced secure authentication scheme with anonymity for wireless environments", IEICE Transactions on Communications, vol. E95-B, no. 7, **(2012)**, pp. 2505-2508.
[15] Q. Jiang, J. Ma, G. Li and L. Yang, "An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks", Wireless Personal Communications, vol. 68, no. 4, **(2013)**, pp. 1477-1491.
[16] D. He, N. Kumar, M. Khan and J. Lee, "Anonymous two-factor authentication for consumer roaming service in global mobility networks", IEEE Transactions on Consumer Electronics, vol. 59, no. 4, **(2013)**, pp. 811-817.
[17] Q. Xie, B. Hu, X. Tan, M. Bao and X. Yu, "Robust anonymous two-factor authentication scheme for roaming service in global mobility network", Wireless Personal Communications, vol. 74, no. 2, **(2014)**, pp.601-614.
[18] Q. Xie, D. Hong, M. Bao, N. Dong and D. Wong, "Privacy-preserving mobile roaming authentication with security proof in global mobility networks", International Journal of Distributed Sensor Networks, vol. 2014, **(2014)**.
[19] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments", IEEE Transactions on Consumer Electronics, vol. 50, no. 1, **(2004)**, pp. 230-234.
[20] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis", Advances in Cryptology - CRYPTO, LNCS vol. 1666, **(1999)**, pp. 388-397.
[21] T. Messerges, E. Dabbish and R. Sloan, "Examining smart-card security under the threat of power analysis attacks", IEEE Transactions on Computers, vol. 51, no. 5, **(2002)**, pp. 541-552.
[22] K. K. R. Choo, C. Boyd and Y. Hitchcock, "Errors in computational complexity proofs for protocols", Advances in Cryptology-ASIACRYPT, LNCS, vol. 3788, **(2005)**, pp. 624-643.
[23] J. Nam, J. Paik and D. Won, "A security weakness in Abdalla et al.'s generic construction of a group key exchange protocol", Information Sciences, vol. 181, no. 1, **(2011)**, pp. 234-238.
[24] J. Nam, K. K. R. Choo, M. Kim, J. Paik and D. Won, "Dictionary attacks against password-based authenticated three-party key exchange protocols", KSII Transactions on Internet and Information Systems, vol. 7, no. 12, **(2013)**, pp. 3244-3260.
[25] J. Nam, K. K. R. Choo, M. Kim, J. Paik and D. Won, "Efficient and anonymous two-factor user authentication in wireless sensor networks: Achieving user anonymity with lightweight sensor computation", PLOS ONE, vol. 10, no. 4, **(2015)**.
[26] P. Zeng, Z. Cao, K. K. R. Choo and S. Wang, "On the anonymity of some authentication schemes for wireless communications", IEEE Communications Letters, vol. 13, no. 3, **(2009)**, pp. 170-171.
[27] T. Youn, Y. Park and M. Li, "Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks", IEEE Communications Letters, vol. 13, no. 7, **(2009)**, pp. 471-473.
[28] M. Bellare, D. Pointcheval and P. Rogaway, "Authenticated key exchange secure against dictionary attacks", Advances in Cryptology-EUROCRYPT, LNCS, vol. 1807, **(2000)**, pp. 139-155.
[29] J. Nam, K. K. R. Choo, J. Paik and D. Won, "Password-only authenticated three-party key exchange proven secure against insider dictionary attacks", The Scientific World Journal, **(2014)**.

Authors

Junghyun Nam, He received the B.E. degree in Information Engineering from Sungkyunkwan University, Korea, in 1997. He received his M.S. degree in Computer Science from University of Louisiana, Lafayette, in 2002, and the Ph.D. degree in Computer Engineering from Sungkyunkwan University, Korea, in 2006. He is now an associate professor in Konkuk University, Korea. His research interests include cryptography and computer security.

Kim-Kwang Raymond Choo, He received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He is currently an associate professor at the University of South Australia, and a visiting expert at INTERPOL Global Complex for Innovation. He was named Winner of the 2015 Cybersecurity Educator of the Year – APAC, and one of 10 Emerging Leaders in the Innovation category of The Weekend Australian Magazine / Microsoft's Next 100 series in 2009. He is also the recipient of various awards including ESORICS 2015 Best Research Paper Award, Winning Team of Germany's University of Erlangen-Nuremberg (FAU) Digital Forensics Research Challenge 2015, 2014 Highly Commended Award by Australia New Zealand Policing Advisory Agency, 2010 Australian Capital Territory Pearcey Award, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award for the best (sole-authored) paper published in the 2007 volume of The Computer Journal. Most recently in 2015/6, he serves as a guest editor in a number of journals including ACM Transactions on Internet Technology, ACM Transactions on Embedded Computing Systems, IEEE Transactions on Big Data, and IEEE Transactions on Dependable and Secure Computing.

Juryon Paik, She received the B.E. degree at Information Engineering from Sungkyunkwan University, Korea, in 1997. After graduating the undergraduate course she worked at the Samsung SDS for about one year. She received her M.E. and Ph.D. degrees in Computer Engineering from Sungkyunkwan University in 2005 and 2008, respectively. She was a Research Professor at the Department of Computer Engineering, Sungkyunkwan University from Apr. 2012 to Feb. 2016. During that time she was devoted to researching the xml and big data mining. Also, she was a Program Committee member for DTA 2098. Currently, she is an Assistant Professor at the Department of Digital Information & Statistics, Pyeongtaek University. Her research interests include XML mining, big data mining, semantic mining, information retrieval, and web search engines.