A Provably Secure and Unlinkable Authentication System with Smart Cards

Nakamura, Toru
Graduate School of Information Science and Electrical Engineering, Kyushu University

Inenaga, Shunsuke
Faculty of Information Science and Electrical Engineering, Kyushu University

Ikeda, Daisuke
Faculty of Information Science and Electrical Engineering, Kyushu University

Baba, Kensuke
Faculty of Information Science and Electrical Engineering, Kyushu University

他

https://hdl.handle.net/2324/13299

A Provably Secure and Unlinkable Authentication System with Smart Cards

Toru Nakamura, Shunsuke Inenaga, Daisuke Ikeda,
Kensuke Baba, and Hiroto Yasuura

Graduate School/Faculty of Information Science and Electrical Engineering,
Kyushu University, Japan
`http://www.c.csce.kyushu-u.ac.jp`

Abstract. This paper proposes an identification scheme realizing an authentication system with smart cards. The proposed scheme satisfies the following properties simultaneously: security, unlinkability in multi-service environment and memory efficiency, although a system which satisfies only two of these properties can be constructed with trivial extensions of existing systems. However, to the best of our knowledge, there has not existed a system that satisfies all of these properties. Unlinkability in multi-service environment is a property of privacy protection such that user's actions or preferences are not linked by the adversary by analyzing logs from distinct service providers. We first present an identification scheme for multi-service environment, which utilizes pseudorandom functions. We then give a formal definition of unlinkability in multi-service environment, and prove that our scheme is secure, unlinkable and memory efficient.

Key words: identification, authentication, unlinkability, smart card

1   Introduction

Identity management systems and technologies, including authentication systems, are getting more and more essential for our life. In particular, authentication plays an important role to prevent impersonation attacks caused by ID-theft. Hence authentication systems must be secure against not only outside attackers but also malicious or careless insiders.

Of various ways of authentication, this paper focuses on authentication systems with smart cards which are more convenient to users than password-based authentication systems. Authentication in smart-card-based systems is realized by a proof of possession of secret information stored in the smart card of the user.

Privacy problems in identity management systems are also receiving increasing attention [1]. Due to the increase of data storage available and the progress of data mining technologies, it is becoming easier to analyze a user's action or preference from the user's service logs. This problem is more serious in multi-service environment since logs of the same user in distinct services may be linked by leakage of these logs or illegal coalition among distinct service providers. The property that a system can prevent this problem is called *unlinkability in multi-service environment* [2]. A naive solution to the problem is to use a unique ID (pseudonym) and secret-key for each service

provider. However, it is not desirable that the memory requirement for storing secret-keys and pseudonyms depends on the number of service providers due to restriction of the memory size in a smart card. Therefore, authentication systems with smart cards should be unlinkable in multi-service environment and the memory requirement should not depend on the number of service providers.

We show the summary of requirements for authentication systems with smart cards in this paper as follows;

- *Security*: any adversaries cannot impersonate a legal user even if the adversaries can use any information which service providers have.
- *Unlinkability*: any adversaries cannot link logs of the same user in distinct services even if the adversaries can collect these logs.
- *Memory Efficiency*: the amount of memory using our system does not depend on the number of service providers.

We construct our system based on *identification schemes* [3–5] and *pseudorandom functions* [5]. An identification scheme can be a way of secure authentication, and any strings can be used as secret-keys in the scheme. In our system, each user stores two functions in his/her smart card. One is used to generate his/her secret-key and the other is used to generate his/her pseudonym from a service ID. Hence the amount of memory does not depend on the number of service providers. We assume that two functions are values of two pseudorandom functions in our system in order to realize the property of unlinkability in multiservice environment. A pseudorandom function, which is a random variable whose values functions map strings to strings, is hard to distinguish from a truly random function.

It is shown that our scheme satisfies these requirements by a formal model based on Turing machines. We prove that our scheme is secure by using the formal definition of secure identification schemes [3, 5]. We also define the property of unlinkability in multi-service environment formally based on Turing machine, and prove that our scheme satisfies the property.

Applying our authentication system for multi-service environment, problems caused by server-side mistakes or weakness, such as impersonation and linkage of distinct service providers' logs, are prevented, hence the system is reliable for users and service providers can reduce the cost of identity management. In addition, our system is tolerant to the further increase of service providers, not only because the memory requirement for smart cards does not depend on the number of service providers, but also because the memory need not be rewritten every time a new service provider is introduced to the system.

This paper is organized as follows. Section 2 summarizes related work. In Section 3 we recall the identification scheme [5] which is viable and secure. We also introduce its slight modification which retains viability and security. In Section 4 we consider an extension of identification schemes to the case where there are multiple service providers, which uses random variables whose values are functions from strings to strings. We also develop a formal definition of unlinkability in multi-service environment. Section 5 proposes our identification scheme in multi-service environment which is viable, secure, and unlinkable. We also show that in our scheme the memory requirement for

users' smart card is independent of the number of service providers. Section 6 describes an example of implementation of our authentication system based on Schnorr's identification scheme and discuss overhead of computation time of our system. Section 7 concludes the paper.

2 Related Work

Password authentication and authenticated key agreement schemes with smart cards, in which the size of memory is independent of the number of service providers, have been proposed in [6–8]. All of these schemes can prevent eavesdropping adversaries from impersonating a legal user, however, they cannot prevent adversaries such as inside attackers who can get any information in server-side, from impersonating. Juang [6] and Hwang *et al.* [7] did not discuss privacy protection. There are some authentication schemes which are secure against these attacks, for example, authentication schemes based on public-key encryption, identification schemes based on zero knowledge proof or three-move identification schemes [3, 4] and so on. However, to the best of our knowledge, none of them discussed the relationship between these schemes and multi-service environment.

On privacy protection technologies for authentication system, there are two notions of anonymity from the viewpoint of authentication, called *weak anonymity* (*pseudonymity*) and *strong anonymity* (*unlinkability*). Weak anonymity is a property that although a service provider can know whether two trials to be authenticated are done by the same user or not, the service provider cannot know the identifier of user. Strong anonymity is a property that a service provider cannot determine whether two trials are done by the same user or not. Liao *et al.* [8] proposed an authentication and authenticated key agreement scheme with strong anonymity, however, the scheme is not secure against inside attackers as well as the previous schemes [6, 7]. Authentication schemes based on anonymous credentials [9, 10] or group signatures [11, 12] satisfy both unlinkability and security against inside attackers. However, the implementation cost is too high for smart-card-based systems and in authentication systems based on these schemes, the service providers cannot provide different services for each user. Nohara *et al.* [2] proposed the notion of unlinkability in multi-service environment, which is a kind of weak anonymity, however, the notion has not been defined in terms of computational complexity theory.

3 Identification Scheme

In this section, we explain the definition of identification schemes [5] and we discuss the viability and the security of identification schemes replacing the identification protocols with extended ones.

3.1 Definitions

An *interactive Turing machine* (ITM) is a multi-tape Turing machine with read-only input tapes, a read-and-write work tape, a write-only output tape, a pair of communication

tapes, and a read-and-write switch tape consisting of a single cell. One communication tape is read-only and the other is write-only.

Two ITMs A and B are said to be linked if

- an input tape of A coincides with an input of B,
- the read-only communication tape of A coincides with the write-only communication tape of B, and vice versa, and
- the switch tape of A coincides with that of B.

The shared input tape is called the *common input tape* of the two ITMs, while the other tapes are called a *auxiliary input tape*. A *joint computation* of two linked ITMs is a sequence of pairs of the local configurations (that is, the state, the contents of the tapes, and the positions of the heads) of the ITMs, where the configuration of one ITM is not modified when the configuration of the other ITM is modified, which is realized by the switch tape. The output of a joint computation is the content of the output tape of one of the ITMs.

The output of a Turing machine A on an input x is denoted by $A(x)$. We denote by $\langle A, B \rangle$ a joint computation of ITMs A and B, and by $\langle A(y), B(z) \rangle(x)$ its output on a common input x, an auxiliary input y for A, and an auxiliary input z for B. We sometimes omit the brackets if the input tapes are blank. In the rest of this paper, we sometimes call a Turing machine A an "algorithm" A, and a joint computation $\langle A, B \rangle$ a "protocol". If A is a probabilistic algorithm, $A_r(x)$ denotes the output of A on an input x and random coins r. We denote by $\mathrm{poly}()$ some fixed but unspecified polynomial, and $p(n)$ denotes any polynomial of $n \in \mathbf{N}$.

Definition 1. *An* identification scheme *is a pair of a probabilistic polynomial-time algorithm I and a protocol $\langle A, B \rangle$ of two probabilistic polynomial-time ITMs such that:*

- Viability: *For any $n \in \mathbf{N}$, any $\alpha \in \{0,1\}^n$ and any $s \in \{0,1\}^{\mathrm{poly}(n)}$,*

$$\Pr[\langle P(s), V \rangle(\alpha, I_s(\alpha)) = 1] = 1.$$

- Security: *For any pair of probabilistic polynomial-time ITMs B' and B'', any sufficiently large $n \in \mathbf{N}$, any $\alpha \in \{0,1\}^n$ and any z,*

$$\Pr[\langle B''(z, T_n), V \rangle(\alpha, I_{S_n}(\alpha)) = 1] < \frac{1}{p(n)},$$

where S_n is a random variable uniformly distributed over $\{0,1\}^{\mathrm{poly}(n)}$ and T_n is a random variable describing the output of $B'(z)$ after interacting with $P(S_n)$, on common input $(\alpha, I_{S_n}(\alpha))$, for polynomially many times.

Then, the string s is called a *secret-key*, the string α is called a *pseudonym*, the algorithm I is called a *verifying-key generating algorithm*, the output of I is called a *verifying-key*, and the protocol $\langle A, B \rangle$ is called an *identification protocol*.

3.2 Extension Based on Equality

In this section we show that our extended identification protocol is viable and secure.

For any protocol $\langle A, B \rangle$ and any input x, it is easy to see that there exists a protocol $\langle A, B \rangle$ such that

$$\langle A, B \rangle(x) = \langle A'(x), B'(x) \rangle.$$

In addition, it is easy to see that there exists a protocol (A'', B'') such that

$$\langle A'(x), B'(x) \rangle = \langle A''(x), B'' \rangle.$$

The next lemma follows from the above arguments.

Lemma 1. *For any identification protocol (P, V), any $n \in \mathbf{N}$, any $\alpha \in \{0, 1\}^n$ and any $s \in \{0, 1\}^{\mathrm{poly}(n)}$, there exists a protocol (P', V') such that*

$$\langle P(s), V \rangle(\alpha, I_s(\alpha)) = \langle P'(s, \alpha), V' \rangle(I_s(\alpha)).$$

For instance, the protocol $\langle A', B' \rangle$ can be constructed as follows:

1. P' is an ITM which reads α on the auxiliary input tape, writes α in the write-only communication tape, and then behaves in the same manner as P.
2. V' is a modification of V, which reads α on the read-only communication tape instead of reading α on the common input tape.

The identification protocol $\langle A', B' \rangle$ is called the *extended identification protocol* w.r.t. $\langle A, B \rangle$.

Lemma 2. *If $\langle A, B \rangle$ is an identification protocol, the extended identification protocol $\langle A', B' \rangle$ w.r.t. $\langle A, B \rangle$ satisfies the following property: for any pair of probabilistic polynomial-time ITMs B' and B'', any sufficiently large $n \in \mathbf{N}$, any $\alpha \in \{0, 1\}^n$ and any z,*

$$\Pr[\langle B''(z, T_n, \alpha), V' \rangle(I_{S_n}(\alpha)) = 1] < \frac{1}{p(n)},$$

where S_n is a random variable uniformly distributed over $\{0, 1\}^{\mathrm{poly}(n)}$ and T_n is a random variable describing the output of $B'(z)$ after interacting with $P'(S_n, \alpha)$, on common input $(I_{S_n}(\alpha))$, for polynomially times.

Proof. Assume that there exists a pair of probabilistic polynomial-time ITMs C' and C'' such that for an $\alpha' \in \{0, 1\}^n$ and a z',

$$\Pr[\langle C''(z', T_n', \alpha), V' \rangle(I_{S_n'}(\alpha')) = 1] \geq \frac{1}{p(n)},$$

where S_n' is a random variable uniformly distributed over $\{0, 1\}^{\mathrm{poly}(n)}$ and T_n' is a random variable describing the output of $C'(z')$ after interacting with $P'(S_n', \alpha')$ on the common input $(I_{S_n'}(\alpha'))$ for polynomially times. We can construct a pair of probabilistic polynomial-time ITMs D' and D'' such that:

1. D' is a modification of C', which reads α on the read-only communication tape instead of reading α.
2. D'' is an ITM which skips writing α on the write-only communication tape, and then behaves in the same manner as C''.

Then the distribution of the random variable T_n'', which is the output of D' after interacting with $P(S_n')$, equals the distribution of T_n'. According to previous 1 and 2, the pair of D' and D'' satisfies the following property:

$$\Pr[\langle D''(z', T_n'), V\rangle(\alpha, I_{S_n'}(\alpha')) = 1] \geq \frac{1}{p(n)}.$$

This is contradictory to the precondition that (P, V) is an identification protocol.

The next theorem follows from Lemma 1 and Lemma 2:

Theorem 1. *If a pair $(I, \langle A, B\rangle)$ is an identification scheme, then a pair of the verifying-key generating algorithm I and the extended identification protocol $\langle A', B'\rangle$ w.r.t. $\langle A, B\rangle$ satisfy the following properties:*

- *Viability: for any $n \in \mathbf{N}$, any $\alpha \in \{0,1\}^n$ and any $s \in \{0,1\}^{\mathrm{poly}(n)}$,*

$$\Pr[\langle P'(s, \alpha), V'\rangle(I_s(\alpha)) = 1] = 1.$$

- *Security: for any pair of probabilistic polynomial-time ITMs B' and B'', any sufficiently large $n \in \mathbf{N}$, any $\alpha \in \{0,1\}^n$ and any z,*

$$\Pr[\langle B''(z, T_n), V'\rangle(I_{S_n}(\alpha)) = 1] < \frac{1}{p(n)},$$

where S_n is a random variable uniformly distributed over $\{0,1\}^{\mathrm{poly}(n)}$ and T_n is a random variable describing the output of $B'(z)$ after interacting with $P'(S_n, \alpha)$ on common input $I_{S_n}(\alpha)$, for polynomially many times.

4 Extension of Identification Scheme for Multi-Service Environment

In this section, present the definition of identification schemes in multi-service environment, which are obtained by extending the identification schemes of Definition 1. The key is the use of random variables whose values are functions that map strings to strings. We also give a formal definition of *unlinkability in multi-service environment*.

4.1 Extension for Multi-Service Environment by Functions

In this paper, we consider random variables that take functions that map strings to strings as their values. For ease of explanation, we consider only length-preserving functions and we assume that the sample space of the random variable is $\{0,1\}^n$. Let F_n be a random variable whose values are functions that map n-bit strings to n-bit

strings, that is, the multi-set $\{f_s : \{0,1\}^n \to \{0,1\}^n\}_{s \in \{0,1\}^n}$ with s representing random coins. In the rest of paper, we also use the notation F_n as a probabilistic algorithm which outputs $f_s(x)$ on input x and random coins s, where the meaning will be clear from the context. We denotes $F_n(b)$ by $f_{U_n}(b)$ where U_n is a random variable uniformly distributed over $\{0,1\}^n$ since the random coins are random variables uniformly distributed over $\{0,1\}^n$.

We introduce *user IDs* and *service IDs*, which are n-bit strings corresponding uniquely to users and service providers, respectively. Let F_n and G_n be random variables that take functions mapping n-bit strings to n-bit strings as their values. For any user ID a and service ID b, $f_a(b)$ and $g_a(b)$ denote the secret-key and the pseudonym corresponding to a and b, respectively.

Then, we define *identification schemes in multi-service environment*, which is a quadruplet of a verifying-key generating algorithm I, an identification protocol $\langle P, V \rangle$, random variables F_n, and G_n. The definition of an identification scheme in multi-service environment is obtained by replacing a secret-key s and an pseudonym α in Definition 1 with $f_a(b)$ and $g_a(b)$, respectively. An identification scheme in multi-service environment clearly satisfies the property of viability in Definition 1.

4.2 Unlinkability in Multi-Service Environment

We also focus on a property related to privacy protection, *unlinkability in multi-service environment*. This property means that any adversaries cannot link logs of the same user in distinct services even if the adversaries can collect these logs. We assume that the adversaries can get pseudonyms and verifying-keys. We define this property as follows:

Definition 2. *An identification scheme in multi-service environment* $(I, \langle P, V \rangle, F_n, G_n)$ *has* unlinkability in multi-service environment *if for any probabilistic polynomial-time algorithm A, any sufficiently large* $n \in \mathbf{N}$ *and any* $b \neq b' \in \{0,1\}^n$,

$$\Pr[A(g_{U_n}(b), g_{U_n}(b')) = 1] - \Pr[A(g_{U_n}(b), g_{U'_n}(b'))] = 1| < \frac{1}{p(n)}$$

and

$$| \Pr[A(I_{f_{U_n}(b)}(g_{U_n}(b)), I_{f_{U_n}(b')}(g_{U_n}(b'))) = 1]$$
$$- \Pr[A(I_{f_{U_n}(b)}(g_{U_n}(b)), I_{f_{U'_n}(b')}(g_{U'_n}(b'))) = 1]| < \frac{1}{p(n)},$$

where U_n *and* U'_n *are random variables independently and uniformly distributed over* $\{0,1\}^n$.

As an example of "linkable" scheme, we consider an identification scheme in multi-service environment in which the same secret-key and pseudonym (we assume they are unique for each user ID) are used for all service providers. That is, we assume that for any random coins a, f_a and g_a output the same string on any input b. In this scheme, it is trivial to check whether or not two pseudonyms for distinct service providers correspond to the same user. For a more concrete example, assume an algorithm A' which outputs

1 if the first input equals the second input, and outputs 0, otherwise. It then holds that $\Pr[A'(g_{U_n}(b), g_{U_n}(b')) = 1] = 1$ and $\Pr[A'(g_{U_n}(b), g_{U'_n}(b')) = 1] < 1/p(n)$, hence this scheme does not have unlinkability in multi-service environment.

5 Identification Scheme Achieving Security, Unlinkability and Memory Efficiency

In this section, we propose an identification scheme in multi-service environment which realizes an authentication system satisfying security and unlinkability in multi-service environment by using *pseudorandom functions*. In this system, each user stores in his/her smart card two functions which pseudorandom functions take. In the authentication phase, the secret-key and pseudonym of each user for a service provider is computed by the two functions that take the service ID as their input. Then the user and the service providers execute the extended identification protocol with his/her secret-key and pseudonym. Let $\langle f \rangle$ be a description of a function f, and we assume any Turing machines can execute the function f if the machines are given the description $\langle f \rangle$.

We show an identification protocol $\langle P'', V' \rangle$ w.r.t. an extended identification protocol $\langle P', V' \rangle$ as follows:

- P'' is an ITM which first reads $\langle f_a \rangle$, and $\langle g_a \rangle$ on the auxiliary input tape, reads b on the common input tape, and then computes $f_a(b)$ and $g_a(b)$. Next, P'' reads $f_a(b)$ and $g_a(b)$ instead of reading the auxiliary input s, α, then behaves in the same manner as P'.

The identification protocol $\langle P'', V' \rangle$ is called *re-extended identification protocol* w.r.t. $\langle P, V \rangle$.

Our proposed identification scheme in multi-service environment is a quadruplet of a verifying-key generating algorithm I, a re-extended identification protocol $\langle P'', V' \rangle$, pseudorandom functions F_n, and G_n. In what follows, we show that our identification scheme achieves security, unlinkability in multi-service environment, and memory efficiency.

5.1 Pseudorandom Functions

A *pseudorandom function*, which is a random variable whose values are functions that map strings to strings, cannot be distinguished from a truly random function. As a notion of a pseudorandom function, Goldreich [5] is considering the set of the random variables F_n on the set of the functions from $\{0,1\}^n$ to $\{0,1\}^n$ for any natural number n. In this paper, we consider F_n for an n as a pseudorandom function.

For any oracle machine M and function f, let M^f denote the execution of M when given access to the oracle f.

Definition 3. *A random variable F_n, whose values are functions from $\{0,1\}^n$ to $\{0,1\}^n$, is called a* pseudorandom function *if for any probabilistic polynomial-time oracle machine M and any sufficiently large $n \in \mathbf{N}$,*

$$|\Pr[M^{F_n}(1^n) = 1] - \Pr[M^{H_n}(1^n) = 1]| < \frac{1}{p(n)},$$

where H_n is a random variable uniformly distributed over all functions from $\{0,1\}^n$ to $\{0,1\}^n$.

The following three lemmas are used to prove the security and unlinkability in multi-service environment of our identification scheme. The next lemma follows from Definition 3.

Lemma 3. *For any pseudorandom functions F_n, oracle reply $f_{U_n}(b)$ on any query $b \in \{0,1\}^n$, any probabilistic polynomial-time algorithm A and any $x \in \{0,1\}^n$,*

$$|\Pr[A(f_{U_n}(b), x) = 1] - \Pr[A(W_n, x) = 1]| < \frac{1}{p(n)}$$

where U_n and W_n are random variables independently and uniformly distributed over $\{0,1\}^n$.

Proof. The oracle reply given by H_n on a query $b' \in \{0,1\}^n$ is obviously uniformly distributed over $\{0,1\}^n$. Assume for contrary that there exists a probabilistic polynomial-time algorithm A' such that, for some $x' \in \{0,1\}^n$,

$$|\Pr[A'(f_{U_n}(b'), x') = 1] - \Pr[A'(W_n, x') = 1]| \geq \frac{1}{p(n)}.$$

Let M' be a probabilistic polynomial-time oracle machine which receives an oracle reply with a query b' then invokes A' on input the oracle reply and x'. Then we have that

$$|\Pr[M'^{F_n}(1^n) = 1] - \Pr[M'^{H_n}(1^n) = 1]| \geq \frac{1}{p(n)},$$

which contradicts to Definition 3 of pseudorandom functions.

The following lemma can be shown similarly to Lemma 3.

Lemma 4. *For any pseudorandom function F_n, oracle reply $f_{U_n}(b)$ on any query $b \in \{0,1\}^n$, any probabilistic polynomial-time algorithm A, B and any $x \in \{0,1\}^n$,*

$$|\Pr[A(B(f_{U_n}(b), x)) = 1] - \Pr[A(B(W_n, x)) = 1]| < \frac{1}{p(n)},$$

where U_n and W_n are random variables independently and uniformly distributed over $\{0,1\}^n$.

The following lemma can be shown similarly to Lemma 4 since any joint computation can be simulated by a probabilistic polynomial-time algorithm.

Lemma 5. *For any pseudorandom functions F_n and G_n, oracle replies $f_{U_n}(b)$ and $g_{U_n}(b)$ on any query $b \in \{0,1\}^n$, any probabilistic polynomial-time algorithm A, any protocol $\langle B, C \rangle$ of probabilistic polynomial-time ITMs and any $x \in \{0,1\}^n$,*

$$|\Pr[A(\langle B(f_{U_n}(b), x), C \rangle (g_{U_n}(b), y)) = 1] - \Pr[A(\langle B(W_n, x), C \rangle (X_n, y)) = 1]| < \frac{1}{p(n)},$$

where U_n, W_n and X_n are random variables independently and uniformly distributed over $\{0,1\}^n$.

5.2 Proof of Security

Recall the identification scheme $\langle P, V \rangle$ of Definition 1. Here, we show that an identification scheme in multi-service environment using pseudorandom functions as F_n and G_n satisfies security.

Theorem 2. *For any identification scheme in multi-service environment $(I, \langle P, V \rangle, F_n, G_n)$ such that F_n and G_n are pseudorandom functions, any pair of probabilistic polynomial-time ITMs B' and B'', any sufficiently large $n \in \mathbf{N}$, any $b \in \{0,1\}^n$ and any z,*

$$\Pr[\langle B''(z, T_n'), V \rangle(b, g_{U_n}(b), I_{f_{U_n}(b)}(g_{U_n}(b))) = 1] < \frac{1}{p(n)},$$

where U_n is a random variable uniformly distributed over $\{0,1\}^n$ and T_n' is a random variable describing the output of $B'(z)$ after interacting with $P(f_{U_n}(b))$, on common input $(b, g_{U_n}(b), I_{f_{U_n}(b)}(g_{U_n}(b)))$, for polynomially many times.

Let P^* be an ITM such that $T_n' = \langle P^*(f_{U_n}(b)), B' \rangle(b, g_{U_n}(b), I_{f_{U_n}(b)}(g_{U_n}(b)))$.

Proof. For any probabilistic algorithm A, there exists deterministic algorithm A' outputs $A'(r, x) = A_r(x)$ on input x and outcome random coins r. According to Lemma 4, it holds that for any probabilistic polynomial-time algorithm A,

$$|\Pr[A(\langle P^*(f_{U_n}(b)), B' \rangle(b, g_{U_n}(b), I_{f_{U_n}(b)}(g_{U_n}(b)))) = 1]$$
$$- \Pr[A(\langle P^*(U_n), B' \rangle(b, g_{U_n}(b), I_{U_n}(g_{U_n}(b)))) = 1]| < \frac{1}{p(n)}.$$

That is, for any probabilistic polynomial-time algorithm A,

$$|\Pr[A(T_n') = 1] - \Pr[A(T_n) = 1]| < \frac{1}{p(n)},$$

where $T_n = \langle P^*(U_n), B' \rangle(g_{U_n}(b), I_{U_n}(g_{U_n}(b)))$. Therefore, by Lemma 5,

$$|\Pr[\langle B''(z, T_n'), V \rangle(b, g_{U_n}(b), I_{f_{U_n}(b)}(g_{U_n}(b))) = 1]$$
$$- \Pr[\langle B''(z, T_n), V \rangle(g_{U_n}(b), I_{U_n}(g_{U_n}(b))) = 1]| < \frac{1}{p(n)}.$$

According to the definition of security in Definition 1,

$$\Pr[\langle B''(z, T_n), V \rangle(g_{U_n}(b), I_{U_n}(g_{U_n}(b))) = 1] < \frac{1}{p(n)},$$

hence
$$\Pr[\langle B''(z, T_n'), V \rangle(b, g_{U_n}(b), I_{f_{U_n}(b)}(g_{U_n}(b))) = 1] < \frac{1}{p(n)}.$$

The next theorem follows from Theorem 1 and Theorem 3:

10

Theorem 3. *If a pair $(I, \langle P, V \rangle)$ is an identification protocol, then our proposed identification scheme in multi-service environment, which is a quadruplet of I, re-extended identification protocol $\langle P'', V' \rangle$ w.r.t. $\langle P, V \rangle$ and pseudorandom functions F_n, and G_n, satisfies the following properties:*

- Viability*: for any $n \in \mathbf{N}$, any $a \in \{0,1\}^n$ and any $b \in \{0,1\}^n$,*

$$\Pr[\langle P'(\langle f_a \rangle, \langle g_a \rangle), V' \rangle (b, I_{f_a(b)}(g_a(b))) = 1] = 1.$$

- Security*: for any pair of probabilistic polynomial-time ITMs B' and B'', any sufficiently large $n \in \mathbf{N}$, any $b \in \{0,1\}^n$ and any z,*

$$\Pr[\langle B''(z, T_n'), V' \rangle (b, I_{f_{U_n}(b)}(g_{U_n}(b))) = 1] < \frac{1}{p(n)},$$

where U_n is a random variable uniformly distributed over $\{0,1\}^n$ and T_n' is a random variable describing the output of $B'(z)$ after interacting with $P'(\langle f_{U_n} \rangle, \langle g_{U_n} \rangle)$, on common input b and $I_{f_{U_n}(b)}(g_{U_n}(b))$, for polynomially many times.

5.3 Proof of Unlinkability in Multi-Service Environment

Our proposed identification scheme in multi-service environment satisfies unlinkability in multi-service environment.

Theorem 4. *Our proposed identification scheme in multi-service environment $(I, \langle P'', V' \rangle, F_n, G_n)$ has unlinkability in multi-service environment.*

Proof. According to Lemma 3,

$$|\Pr[A(g_{U_n}(b), g_{U_n}(b')) = 1] - \Pr[A(g_{U_n}(b), X_n) = 1]| < \frac{1}{p(n)} \qquad (1)$$

and

$$|\Pr[A(g_{U_n}(b), g_{W_n}(b')) = 1] - \Pr[A(g_{U_n}(b), Y_n) = 1]| < \frac{1}{p(n)}, \qquad (2)$$

where U_n, W_n, X_n, and Y_n are random variables independently and uniformly distributed over $\{0,1\}^n$. X_n and Y_n are the same distribution, hence

$$|\Pr[A(g_{U_n}(b), X_n) = 1] - \Pr[A(g_{U_n}(b), Y_n) = 1]| < \frac{1}{p(n)}. \qquad (3)$$

According to Inequalities 1, 2, and 3,

$$|\Pr[A(g_{U_n}(b), g_{U_n}(b')) = 1] - \Pr[A(g_{U_n}(b), g_{W_n}(b'))] = 1| < \frac{1}{p(n)}.$$

In a similar way, according to Lemma 4,

$$|\Pr[A(I_{f_{U_n}(b)}(g_{U_n}(b)), I_{f_{U_n}(b')}(g_{U_n}(b'))) = 1]$$
$$- \Pr[A(I_{f_{U_n}(b)}(g_{U_n}(b)), I_{X_n}(Y_n)) = 1]| < \frac{1}{p(n)} \qquad (4)$$

11

and

$$| \Pr[A(I_{f_{U_n}(b)}(g_{U_n}(b)), I_{f_{W_n}(b')}(g_{W_n}(b'))) = 1]$$
$$- \Pr[A(I_{f_{U_n}(b)}(g_{U_n}(b)), I_{Z_n}(Q_n)) = 1]| < \frac{1}{p(n)}, \quad (5)$$

where U_n, W_n, X_n, Y_n, Z_n and Q_n are random variables independently and uniformly distributed over $\{0,1\}^n$. X_n, Y_n, Z_n and Q_n are the same distribution, hence

$$| \Pr[A(I_{f_{U_n}(b)}(g_{U_n}(b)), I_{X_n}(Y_n)) = 1]$$
$$- \Pr[A(I_{f_{U_n}(b)}(g_{U_n}(b)), I_{Z_n}(Q_n)) = 1]| < \frac{1}{p(n)}. \quad (6)$$

According to Inequalities 4, 5, and 6,

$$| \Pr[A(I_{f_{U_n}(b)}(g_{U_n}(b)), I_{f_{U_n}(b')}(g_{U_n}(b'))) = 1]$$
$$- \Pr[A(I_{f_{U_n}(b)}(g_{U_n}(b)), I_{f_{W_n}(b')}(g_{W_n}(b'))) = 1]| < \frac{1}{p(n)}.$$

5.4 Memory Efficiency

The auxiliary input tape of P'' of our proposed identification scheme corresponds to the memory of each smart card of our authentication system. The memory efficiency of identification schemes is defined as follows:

Definition 4. *An identification scheme in multi-service environment is said to be* memory-efficient *if the length of the auxiliary input tape of P'' is independent of the number of service providers.*

Since the lengths of descriptions $\langle f_a \rangle$, and $\langle g_a \rangle$ of functions f_a and g_a are independent of the number of service providers, we have the following theorem:

Theorem 5. *Our proposed identification scheme $(I, \langle P'', V' \rangle, F_n, G_n)$ is memory-efficient.*

6 An Example of Implementation

In this section, we show an example of implementation of our authentication system. The system is based on Schnorr's identification scheme [4], and uses one-way hash functions instead of pseudorandom functions. We then estimate an overhead with respect to the run time of our scheme.

6.1 Schnorr's Identification Scheme

As an example of identification schemes, we introduce the scheme proposed by Schnorr [4]. The scheme is a three-move identification scheme based on the discrete logarithm problem. Bellare and Paracio [13] showed that the scheme is secure against an active attack

on the assumption that the one more inversion problem for discrete logarithm is hard in terms of an interactive computation.

The verifying-key generating algorithm in the Schnorr identification scheme outputs (p, q, g, X) on an input $s \in \{0, 1\}^k$ for a security parameter $k \in \mathbf{N}$, where p is a prime number such that $2^{k-1} \leq p < 2^k$, q is a prime divisor of $p - 1$, g is a generator of a subgroup of $\mathbf{Z}_p^*$ of order q, and X is $g^s \bmod p$. In our authentication system, (p, q, g) is regarded as common parameters and (p, q, g) can be computed independently of X. Hence the verifying-key generating algorithm can be divided into the algorithm C, which outputs (p, q, g) on input 1^k, and the algorithm I', which outputs X on input s.

The identification protocol is shown as follows:

1. P chooses $y \in \mathbf{Z}_q$ randomly, computes $g^y \bmod p$, and send the result as Y to V;
2. V chooses $c \in \mathbf{Z}_q$ randomly and sends c to P;
3. P computes $y + cs \bmod q$ and sends the result as z to V;
4. V outputs 1 if $g^z = YX^c \pmod{p}$, and 0 otherwise.

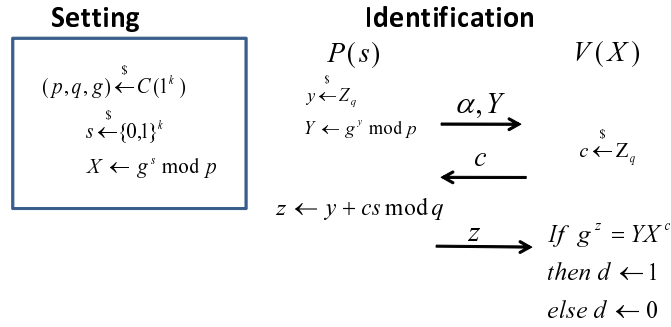Fig.1 shows Schonorr identification scheme.

Fig. 1. Schnorr's Identification scheme.

6.2 The Authentication System

Let $\{u_1, u_2, \ldots, u_\ell\}$ be the set of *users* and $\{s_1, s_2, \ldots, s_m\}$ the set of *service providers*. Each user secretly stores his/her user ID in his/her smart card. Let $\{a_1, a_2, \ldots, a_\ell\}$ be the set of user IDs. A user u_i is associated with his user ID a_i, and for any i, j such that $i \neq j$, $u_i \neq u_j$. Each service provider is labeled by his service ID, which is the public identifier. Let $\{b_1, b_2, \ldots, b_m\}$ be the set of the service IDs. A service provider s_j is associated with his service ID b_j, and for any i, j such that $i \neq j$, $s_i \neq s_j$.

We use one-way hash functions in place of pseudorandom functions. More concretely, $h(0 \parallel a \parallel b)$ and $h(1 \parallel a \parallel b)$ are used as $f_a(b)$ and $g_a(b)$ in the system respectively, where h denotes a one-way hash function and $\parallel$ denotes concatenation.

In our authentication system, there is a *manager M*, which manages information of the system and sets up several parameters. First, we show the preparation procedure which is operated by M before authentication.

– **Startup:**M chooses a security parameter $k \in \mathbf{N}$, and computes (p, q, g).
– **Registration of Users:**When a new user u_i requests to join in the system, M issues a smart card which stores $a_i \in \{0, 1\}^k$ chosen randomly and (p, q, g) to u_i.
– **Registration of Services:**When a new service provider s_j requests to join in the system, M sends $b_j \in \{0, 1\}^k$ chosen randomly and (p, q, g) to s_j. Then M computes pairs $(h(0 \parallel a_i \parallel b_j), h(1 \parallel a_i \parallel b_j))$ for all i, and sends pairs $(h(1 \parallel a_i \parallel b_j), g^{h(0\|a_i\|b_j)} \bmod p)$ for all i.

Next, we show the identification protocol in the system as follows.

1. u_i sends an authentication query to s_j.
2. s_j sends b_j to u_i.
3. u_i computes a pair $(h(0 \parallel a_i \parallel b_j), h(1 \parallel a_i \parallel b_j))$ and sends $h(1 \parallel a_i \parallel b_j)$ to s_j.
4. s_j specifies collesponding $g^{h(0\|a_i\|b_j)} \bmod p$ from $h(1 \parallel a_i \parallel b_j)$.
5. u_i and s_j follow Schnorr's identification scheme.

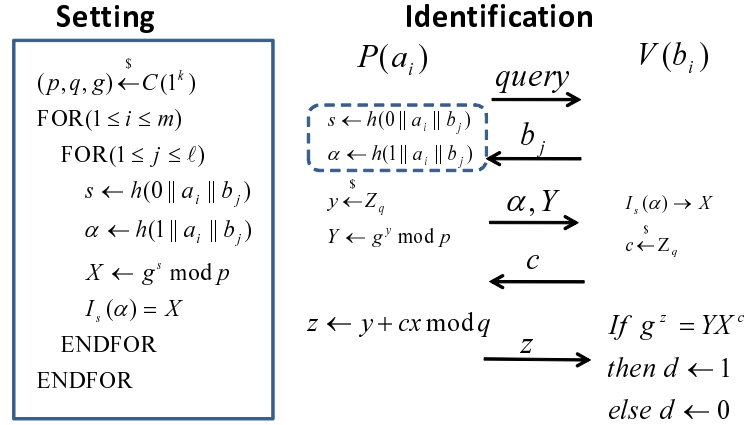The outline of the identification protocol in our authentication system is shown in Figure. 2.

Fig. 2. Our identification scheme based on Schnorr's identification scheme.

6.3 Discussion

A naive scheme realizing unlinkability in multi-service environment is to store his/her secret-keys and pseudonyms which are randomly chosen as a table in his/her smart card.

Using our scheme, the amount of memory is independent of the number of the service providers, however, two more hash computations are required compared to the naive scheme.

In our authentication system, $f_a(b)$ is defined as $h(0 \parallel a \parallel b)$. Assuming that a random variable on the set $\{f_a\}_{a \in \{0,1\}^n}$ can be regarded as a pseudorandom function, our authentication system satisfies secure and unlinkable in multi-service environment.

7 Conclusions

In this paper we proposed a secure and unlinkable authentication system with smart cards in multi-service environment. Our system is based on a non-trivial extension of the identification scheme [5] to the case where multiple service providers use the authentication system. Due to the use of pseudorandom functions, the memory requirement for each smart card is independent of the number of service providers. This is a remarkable advantage when a huge number of services utilize the system. We show an example of our system based on Schnorr's identification scheme, in which pseudorandom functions are replaced with one-way hash functions.

References

1. Hansen, M., Schwartz, A., Cooper, A.: Privacy-enhancing identity management. IEEE Security and Privacy **3** (2008) 38–45
2. Nohara, Y., Inoue, S., Yasuura, H.: Toward unlinkable ID management for multi-service environments. In: Proc. 3rd PerCom Workshops. (2005) 115–119
3. Feige, U., Fiat, A., Shamir, A.: Zero-knowledge proofs of identity. Journal of Cryptology **1**(2) (1988) 77–94
4. Schnorr, C.P.: Efficient signature generation by smart cards. Journal of Cryptology **4**(3) (1991) 161–174
5. Goldreich, O.: Foundations of Cryptography. Cambridge University (2001)
6. Juang, W.S.: Efficient multi-server password authenticated key agreement using smart cards. IEEE Transactions on Consumer Electronics **50** (2004) 251–255
7. Hwang, R.J., Shiau, S.H.: Provably efficient authenticated key agreement protocol for multi-servers. The Computer Journal **50** (2007) 602–615
8. Liao, Y.P., Wang, S.S.: A secure dynamic ID based remote user authentication scheme for multi-server environment. Computer standards and interfaces (2007)
9. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Advances in Cryptology - EUROCRYPT 2001. Volume 2045 of LNCS., Springer-Verlag (2001) 93–118
10. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Advances in Cryptology - CRYPTO 2004. Volume 3152 of LNCS., Springer-Verlag (2004) 56–72
11. Chaum, D., van Heyst, E.: Group signatures. In: Proc. EUROCRYPT'91. Volume 547 of LNCS., Springer-Verlag (1991) 257–270
12. Ateniese, G., Camenisch, J., Joye, M., Tsudik, G.: A practical and provably secure coalition-resistant group signature scheme. In: Proc. CRYPTO'00. Volume 1880 of LNCS., Springer-Verlag (2000) 255–270

13. Bellare, M., Palacio, A.: GQ and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In: Advances in Cryptology - CRYPTO 2002. LNCS, Springer-Verlog (2002)