An Authentication Protocol with Anonymity against Service Providers and the Central Manager

中村, 徹
九州大学大学院システム情報科学府/研究院

稲永, 俊介
九州大学大学院システム情報科学府/研究院

馬場, 謙介
九州大学附属図書館研究開発室

池田, 大輔
九州大学大学院システム情報科学府/研究院

他

出版情報：コンピュータセキュリティシンポジウム2010(CSS2010)予稿集, pp.585-590, 2010-10. 情報処理学会コンピュータセキュリティ研究会
バージョン：
権利関係：

中央機関とサービス提供者に対して匿名な認証プロトコル

中村　徹 †　　稲永　俊介 †　　馬場　謙介 ‡　　池田　大輔 †　　安浦　寛人 †

† 九州大学大学院システム情報科学 [府／研究院]
819-0395 福岡市西区元岡 744 番地

‡ 九州大学附属図書館研究開発室
812-8581 福岡市東区箱崎 6-10-1

{toru,inenaga,yasuura}@c.csce.kyushu-u.ac.jp
daisuke@inf.kyushu-u.ac.jp

baba@lib.kyushu-u.ac.jp

あらまし　本稿では，認証の度にサービス提供者が中央機関と通信を行うタイプの，マルチサービス環境の匿名認証システムに注目する．本稿の目的は，このようなシステムに対して，安全性とプライバシ保護に関する 4 つの要件，すなわち，**完全性**，**受動的内部攻撃者にへのなりすまし耐性**，**中央機関への匿名性**，**サービス提供者への匿名性**を満たす実用的なプロトコルの実現である．既存プロトコルは，複数データベース PIR という要素技術を用いて実現された．しかしながら複数データベース PIR では，同じデータベースの複製を用意し，さらにそれらのデータベースが互いに通信を行わないという前提が必要となる．本稿では，シングルデータベース PIR を用いた認証プロトコルを提案する．このプロトコルは，前述の前提が必要ないため，より実用的である．

An Authentication Protocol with Anonymity against Service Providers and the Central Manager

Toru Nakamura† Shunsuke Inenaga† Kensuke Baba‡ Daisuke Ikeda† Hiroto Yasuura†

†Graduate School/Faculty of Information Science and Electrical Engineering, Kyushu University
Moto'oka 744, Nishi-ku, Fukuoka 819-0395, Japan

{toru,inenaga,yasuura}@c.csce.kyushu-u.ac.jp
daisuke@inf.kyushu-u.ac.jp

‡Research and Development Division, Kyushu University Library
10-1, Hakozaki 6, Higashi-ku, Fukuoka, 812-8581, Japan

baba@lib.kyushu-u.ac.jp

Abstract　This paper focuses on authentication systems in multi-service environment, in which service providers communicate with the central manager in every authentication. The purpose of this paper is to realize a practical authentication protocol for such systems which satisfies four requirements for security and privacy protection, that is, *correctness*, *impersonation resistance against passive insider*, *anonymity against central manager*, and *anonymity against service providers*. The existing protocol consists of a multi-database PIR scheme, in which there are copies of the same database and none of these copies are allowed to communicate with each other. This paper proposes an authentication protocol which consists of the single-database PIR scheme. This protocol is more practical since using a single database implies the above-mentioned assumptions for multi-database PIR schemes are not required any more.

1　Introduction

With the increase of the number of services, users are forced to manage more pairs of a user ID and a password. Hence much attention is recently paid to *authentication systems in multi-service environment*, which enable each

user to have only a pair in order to use multiple services with a central manager. In this paper, we focus on issues about user privacy such that activity or preference of a user can be revealed by (1) service providers or (2) a central manager. In order to solve such issues, an authentication protocol with anonymity against (1) service providers and (2) a central manager is essential.

Authentication systems in multi-service environment can be classified according to which service providers must communicate with the central manager in every authentication. With respect to authentication systems without such communications, some protocols to realize the both kinds of anonymity are known, such as group signature schemes [3], anonymous credential schemes [2], and dynamic ID based anonymous authenticated key exchange schemes [7]. However, such protocols have a drawback that it is difficult for the central manager to deal with frequent queries to update the database of user information. Hence we focus on authentication systems with communications between service providers and the central manager. The requirements for an authentication system considered in this paper are the following.

- *Correctness*: if a user sends an authentication request with the valid password, every service provider accepts the request.
- *Impersonation resistance against passive insider* [1]: even if an adversary is a service provider, the adversary cannot impersonate a legitimate user.
- *Anonymity against service provider*: it is difficult for any service providers to obtain any information about a user ID.
- *Anonymity against central manager*: it is difficult for any central manager to obtain any information about a user ID.

There are few schemes which satisfy the previous requirements, as far as we know. Nakamura *et al.* [8] proposed an anonymous authentication protocol which satisfies all the requirements previously described. This protocol is based on *private information retrieval* (*PIR*) schemes [4][6]. Using a PIR scheme, a client can reconstruct an element from the answer which the database server has generated with the query, without the index of the element being revealed to the database server. The authentication protocol consists of a multi-database PIR scheme [4], in which there are copies of the same database and none of these copies are allowed to communicate with each other. However, such assumptions are not practical.

In this paper, we propose an authentication protocol with a single-database PIR scheme [6], which does not require copies of the same database. Our basic idea of realizing the authentication protocol is that a service provider reconstructs the information to verify a user from the central manager with single-database PIR scheme. However, original Kushilevitz and Ostrovsky's single-database PIR scheme requires an index to reconstruct the element from the answer, where indices correspond to user IDs. If the service provider can obtain the ID, it is impossible to realize anonymity against service providers. Hence the single-database PIR scheme cannot be applied to our protocol. In this paper, we use the special version of Kushilevitz and Ostrovsky's single-database PIR, in which an element of the database can be reconstructed without the index, in order to construct the authentication protocol which satisfies the all requirements previously described, called *Single-database PIR based Anonymous Authentication Protocol* (SPAAP for short).

SPAAP is more practical than the existing protocol [8] since using a single database implies the assumptions for multi-database PIR schemes are not required any more. Therefore, this paper contributes the development of anonymous authentication systems in which service providers need to communicate with the central manager from the view point of reducing some impractical assumptions.

[1] In this paper, a "passive and insider adversary" means that an adversary who is restricted to eavesdropping on messages that the service provider obtains.

2 Requirements of Anonymous Authentication Protocol

In this section, we introduce the authentication model which we assume in this paper and the definitions of the four requirements of anonymous authentication protocols.

2.1 Notations

Let $\mathbb{Z}$ denote the set of integers and $\mathbb{N}$ denote the set of natural numbers. For a finite set X, let $|X|$ denote the number of elements which X contains. For $x \in \mathbb{Z}$, let $\|x\|$ denote the binary length of x. For $k \in \mathbb{N}$, let $[k] = \{1, 2, ..., k\}$. For $a, b \in \mathbb{Z}$, let $a|b$ mean that b is divisible by a. Let $x \circ y$ be the concatenation of bit strings x and y. We denote any polynomial of $n \in \mathbb{N}$ by $p(n)$, and some polynomial by $\mathrm{poly}(n)$.

An *interactive Turing machine* (*ITM*) [5] is a Turing machine which has a pair of *communication tapes* in addition to a local input tape, a common input tape, an output tape, and a work tape. A *joint computation* of two ITMs is a sequence of pairs of the local configurations. The output of a joint computation is the output of one of the ITMs. The output of a Turing machine $\mathcal{A}$ on an input x is denoted by $\mathcal{A}(x)$. We denote by $\langle \mathcal{A}, \mathcal{B} \rangle$ a joint computation of Turing machines $\mathcal{A}$ and $\mathcal{B}$, and by $\langle \mathcal{A}(y), \mathcal{B}(z) \rangle(x)$ its output on a common input x, a local input y for $\mathcal{A}$, and a local input z for $\mathcal{B}$. We sometimes omit the brackets if the input is empty. In the rest of this paper, we sometimes call a Turing machine $\mathcal{A}$ an "algorithm" $\mathcal{A}$ and a joint computation $\langle \mathcal{A}, \mathcal{B} \rangle$ a "protocol" $\langle \mathcal{A}, \mathcal{B} \rangle$. The idea of a joint computation of two ITMs can be extended straightforwardly to that of three ITMs by two pairs of communication tapes.

2.2 Authentication Model

In this paper, we assume an authentication model which consists of the following three types of entities.

- **User**: Let m be the number of the users. Each user is assigned the unique *identifier* $i \in [m]$ and has a *password* $x_i \in \{0,1\}^\ell$ for a natural number ℓ. (Note that ℓ is a polynomial of a security parameter k.)
- **Service provider**: A *service provider* verifies whether the entity who has sent an authentication request is truly the legitimate user.
- **Central manager**: A *central manager* stores the sequence $x = (x_1, x_2, ..., x_n)$ of the passwords of the users. We assume that each password is a random string.

Throughout this paper, we assume that

- each user can communicate only with service providers,
- each service provider can communicate with users and the central manager, and
- the central manager can communicate only with service providers.

We define an authentication protocol as a joint computation $\langle \mathcal{P}, \mathcal{V}, \mathcal{M} \rangle$. $\mathcal{P}, \mathcal{V}$, and $\mathcal{M}$ mean the behaviors of a user, a service provider, and a central manager, respectively. $\mathcal{P}$ takes a pair of an identifier i and a *candidate password* $z \in \{0,1\}^m$ as inputs, and $\mathcal{M}$ takes x as an input. After running the authentication protocol, $\mathcal{V}$ outputs 1/0.

2.3 Requirements

We show the four requirements which an anonymous authentication protocol $\langle \mathcal{P}, \mathcal{V}, \mathcal{M} \rangle$ should satisfy as follows.

- *Correctness*: for any $k, \ell, m \in \mathbb{N}$, any $i \in [m]$, any $x = \{x_i \mid i \in [m], x_i \in \{0,1\}^\ell\}$,

$$\Pr[\langle \mathcal{P}(1^k, i, x_i), \mathcal{V}(1^k), \mathcal{M}(1^k, x) \rangle = 1] > 1 - \frac{1}{p(k)}.$$

- *Impersonation resistance against passive insider*: for any $k, \ell, m \in \mathbb{N}$ any $i \in [m]$, and any probabilistic polynomial-time algorithm $\mathcal{B}$,

$$\Pr[\langle \mathcal{B}(1^k, T_1), \mathcal{V}(1^k), \mathcal{M}(1^k, X) \rangle = 1] < \frac{1}{p(k)},$$

where X is a random variable uniformly distributed over $(\{0,1\}^\ell)^m$ and T_1 is a random variable which means a transcript of $\mathcal{V}$'s local tape and read tapes after running $\langle \mathcal{P}(i,x), \mathcal{V}, \mathcal{M}(x)\rangle$ where x is a sample from X.

- *Anonymity against central manager*: for any $k, \ell, m \in \mathbb{N}$, any $i, j \in [m]$, any $z, z' \in \{0,1\}^\ell$, and any probabilistic polynomial-time algorithm $\mathcal{B}$,

$$|\Pr[\mathcal{B}(1^k, T_2) = 1] - \Pr[\mathcal{B}(1^k, T_3) = 1]| < \frac{1}{p(k)},$$

where X is a random variable uniformly distributed over $(\{0,1\}^\ell)^m$ and T_2 is a random variable which means a transcript of $\mathcal{M}$'s local tape and read tapes after running $\langle \mathcal{P}(i,z), \mathcal{V}, \mathcal{M}(x)\rangle$ where x is a sample from X. Similarly, T_3 means a transcript after running $\langle \mathcal{P}(i,z'), \mathcal{V}, \mathcal{M}(x)\rangle$.

- *Anonymity against service provider*: for any $k, \ell, m \in \mathbb{N}$, any $i, j \in [m]$, any $z, z' \in \{0,1\}^\ell$, and any probabilistic polynomial-time algorithm $\mathcal{B}$,

$$|\Pr[\mathcal{B}(1^k, T_4) = 1] - \Pr[\mathcal{B}(1^k, T_5) = 1]| < \frac{1}{p(k)},$$

where X is a random variable uniformly distributed over $(\{0,1\}^\ell)^m$ and T_4 is a random variable which means a transcript of $\mathcal{V}$'s local tape and read tapes after running $\langle \mathcal{P}(i,z), \mathcal{V}, \mathcal{M}(x)\rangle$ where x is a sample from X. Similarly, T_5 means a transcript after running $\langle \mathcal{P}(i,z'), \mathcal{V}, \mathcal{M}(x)\rangle$.

3 Our Approach: SPAAP

In this section, we show the anonymous authentication protocol which satisfies all the requirements, called SPAAP. We construct SPAAP with a special version of Kushilevitz and Ostrovsky's single-database PIR schemes [6], in which an element of the database can be reconstructed without the index.

3.1 Kushilevitz and Ostrovsky's PIR scheme

For the ease of explanation, we assume that an element of a database is a bit, that is, a database is denoted by $x = x_1 \circ x_2 \circ \cdots \circ x_m \in \{0,1\}^m$. $\mathcal{W}_n$ is defined as follows:

$$\mathcal{W}_n(y) = \begin{cases} 0 & \text{if } \exists w \in \mathbb{Z}_n^* \text{ such that } w^2 = y \bmod n \\ 1 & \text{otherwise} \end{cases}.$$

Let $QR_n^{+1} = \{x \in \mathbb{Z}_n^{+1} | \mathcal{W}_n(x) = 0\}$ and $QNR_n^{+1} = \{x \in \mathbb{Z}_n^{+1} | \mathcal{W}_n(x) = 1\}$.

- *Query algorithm* $\mathcal{Q}(\cdot,\cdot)$: $\mathcal{Q}$ is a probabilistic algorithm which receives 1^k and an index $i \in [m]$ (k is a security parameter) as inputs. First, $\mathcal{Q}$ randomly chooses distinct primes α and β whose length is $k/2$. Next, $\mathcal{Q}$ uniformly and randomly chooses m numbers $y_1, ..., y_m \in \mathbb{Z}_n^{+1}$ such that y_j is an element of QR_n^{+1} if $j = i$, y_j is an element of QNR_n^{+1} otherwise, where $n = \alpha \cdot \beta$. Finally, $\mathcal{Q}$ outputs $y_1, ..., y_m$ as a query and (α, β) as a secret.

- *Answer algorithm* $\mathcal{A}(\cdot,\cdot,\cdot)$: $\mathcal{A}$ is a deterministic algorithm which receives 1^k, a database $x \in \{0,1\}^m$, and a query $y_1, ..., y_m \in \mathbb{Z}_n^{+1}$ as inputs. $\mathcal{A}$ computes

$$w_i = \begin{cases} y_i^2 & \text{if } x_i = 0 \\ y_i & \text{if } x_i = 1. \end{cases}$$

Then, $\mathcal{A}$ outputs as an answer

$$z = \prod_{i=1}^{m} w_i.$$

- *Reconstruct algorithm* $\mathcal{R}(\cdot,\cdot,\cdot)$: $\mathcal{R}$ is a deterministic algorithm which receives 1^k, a secret (α, β), and answer $z \in \mathbb{Z}_n^{+1}$ as inputs. $\mathcal{R}$ outputs 1 if $\mathcal{W}_n(z) = 1$, and outputs 0 otherwise.

The PIR scheme satisfies the following properties under the quadratic residuosity assumption.

- *correctness*: for any $k, m \in \mathbb{N}$, any $x = \{x_i \mid i \in [m], x_i \in \{0,1\}^{\mathrm{poly}(k)}\}$, and any $i \in [m]$,

$$\Pr[\mathcal{R}(1^k, \mathcal{Q}^2(1^k, i), \mathcal{A}(x, \mathcal{Q}^1(1^k, i))) = x_i] > 1 - \frac{1}{p(k)}. \quad (1)$$

- *privacy*: for any $k, m \in \mathbb{N}$, any $i, j \in [m]$, and any probabilistic polynomial-time algorithm $\mathcal{B}$,

$$|\Pr[\mathcal{B}(1^k, \mathcal{Q}^1(1^k, i)) = 1] - \Pr[\mathcal{B}(1^k, \mathcal{Q}^1(1^k, j)) = 1]| < \frac{1}{p(k)}. \quad (2)$$

We prove the following lemma with respect to the PIR scheme.

Lemma 1 *If $(\mathcal{Q}, \mathcal{A}, \mathcal{R})$ is the previous described PIR scheme, the following proposition holds: for any $k, m \in \mathbb{N}$, any $i, j \in [m]$, and any probabilistic polynomial-time algorithm $\mathcal{B}$,*

$$\Pr[\mathcal{B}(1^k, \mathcal{Q}^2(1^k, i), \mathcal{A}(1^k, X, \mathcal{Q}^1(1^k, i))) = 1] - \Pr[\mathcal{B}(1^k, \mathcal{Q}^2(1^k, j), \mathcal{A}(1^k, X', \mathcal{Q}^1(1^k, j))) = 1] = 0,$$

where X, X' are random variables uniformly and independently distributed over $\{0,1\}^m$.

The detail of this proof is skipped due to lack of space.

3.2 SPAAP

We use a public-key encryption scheme and a random oracle as a hash function in order to construct SPAAP.

We show the definition of a public-key encryption scheme [5] as follows.

Definition 1 *A public-key encryption scheme is a triple $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ of probabilistic polynomial-time algorithms satisfying the following conditions.*

- *On input 1^k, algorithm $\mathcal{G}$ outputs a pair of bit strings.*
- *For any pair of (e, d) in the range of $\mathcal{G}(1^k)$, and any $\gamma \in \{0,1\}^*$,*

$$\Pr[\mathcal{D}(d, \mathcal{E}(e, \gamma)) = \gamma] = 1. \quad (3)$$

- *For any $k \in \mathbb{N}$ any $x, y \in \{0,1\}^{\mathrm{poly}(k)}$, and any probabilistic polynomial-time algorithm $\mathcal{B}$,*

$$|\Pr[\mathcal{B}(\mathcal{G}^1(1^k), \mathcal{E}(\mathcal{G}^1(1^k), x)) = 1] - \Pr[\mathcal{B}(\mathcal{G}^1(1^k), \mathcal{E}(\mathcal{G}^1(1^k), y)) = 1]| < \frac{1}{p(k)}. \quad (4)$$

In this paper, we assume that we can regard any hash function as a random oracle [1]. This assumption is called the *random oracle assumption*. We show the behavior of a random oracle as follows. For the ease of explanation, we assume that the random oracle outputs m bit strings on inputs ℓ bit strings, where ℓ and m are polynomials of a security parameter k.

1. The random oracle receives $x \in \{0,1\}^\ell$ as inputs.
2. The random oracle randomly chooses a function $\mathcal{H}_i$ from the all functions $\mathcal{H} = \{\mathcal{H}_1, \mathcal{H}_2, \ldots, \}$ which map $\{0,1\}^\ell$ to $\{0,1\}^m$.
3. The random oracle outputs $\mathcal{H}_i(x)$.

The following lemma holds.

Lemma 2 *For any $k \in \mathbb{N}$, any $x, y \in \{0,1\}^{\mathrm{poly}(k)}$ $(x \neq y)$, and probabilistic polynomial-time algorithm $\mathcal{B}$,*

$$|\Pr[\mathcal{B}(1^k, \mathcal{H}(x)) = 1] - \Pr[\mathcal{B}(1^k, \mathcal{H}(y)) = 1] = 0.$$

SPAAP $\langle \mathcal{P}, \mathcal{V}, \mathcal{M} \rangle$, which satisfies the all requirements is shown as follows, where $(\mathcal{Q}, \mathcal{A}, \mathcal{R})$ is the Kushilevitz and Ostrovsky's PIR scheme which described in the previous section.

1. $\mathcal{M}$ computes $(e, d) \leftarrow \mathcal{G}(1^k)$ and publishes e.
2. $\mathcal{P}$ computes $(q, s) \leftarrow \mathcal{Q}(1^k, i)$ and sends $(\mathcal{E}(e, q), s)$ to $\mathcal{V}$.
3. $\mathcal{V}$ sends $\mathcal{E}(e, q)$ to $\mathcal{M}$.
4. $\mathcal{M}$ obtains q by decrypting $\mathcal{E}(e, q)$. $\mathcal{M}$ randomly chooses $c \in \{0,1\}^\ell$ and for any $j \in [m]$ computes $x'_j \leftarrow \mathcal{H}(x_j, c)$. Let $x' = (x'_1, x'_2, \ldots, x'_m)$. $\mathcal{M}$ computes $a \leftarrow \mathcal{A}(1^k, x', q)$ and sends (c, a) to $\mathcal{V}$.

5. $\mathcal{V}$ computes $x_i' \leftarrow \mathcal{R}(1^k, s, a) = \mathcal{H}(x_i, c)$ and sends c to $\mathcal{P}$.

6. $\mathcal{P}$ computes $z' \leftarrow \mathcal{H}(z, c)$ and sends z' to $\mathcal{V}$.

7. $\mathcal{V}$ outputs 1 if $z' = x_i'$, and outputs 0 otherwise.

3.3 Security Analysis

Theorem 1 *SPAAP has correctness, impersonation resistance against passive insider, anonymity against central manager, and anonymity against service providers under the quadratic residuosity assumption and the random oracle assumption.*

proof: We show only the outlines of the proofs. As for correctness, it can be proven by Inequation (1) and Equation (3). We show the others by contradiction. As for impersonation resistance against passive insider, it can be proven by Inequality (4) and the basic property of a random oracle. As for anonymity against central manager, it can be proven by Inequation (2). As for anonymity against service provieders, it can be proven by Inequation (4), Lemma 1, and the basic property of a random oracle. □

4 Conclusions

In this paper, we proposed SPAAP, which consists of the special version of the single-database PIR scheme proposed by Kushilevitz and Ostrovsky, in which an element of the database can be reconstructed without the index. We proved that SPPAP satisfies all the requirements; correctness, impersonation resistance against passive insider, anonymity against central manager, and anonymity against service providers under the quadratic residuosity assumption and the random oracle assumption. SPAAP is more practical than the existing protocol [8] since using a single database implies the assumptions for multi-database PIR schemes are not required any more.

Acknowledgements

This work was in part supported by CREST-DVLSI of JST. We are grateful for their support.

References

[1] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *In Proc. 1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM Press, 1993.

[2] J. Camenisch and A. Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In *Advances in Cryptology — CRYPTO 2002*, LNCS, pages 101–120. Springer-Verlag, 2002.

[3] D. Chaum and E. van Heyst. Group signatures. In *Advances in Cryptology - EUROCRYPT 1991*, volume 547 of *LNCS*, pages 257–270. Springer-Verlag, 1991.

[4] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan. Private information retrieval. *Jornal of the ACM*, 45:965–982, 1998.

[5] O. Goldreich. *Foundations of Cryptography.* Cambridge University, 2001.

[6] E. Kushilevitz and R. Ostrovsky. Replication is not needed: Single database, computationally-private information retrieval. In *the 38th Annual Symposium on Foundations of Computer Science*, pages 364–373, 1997.

[7] Y.-P. Liao and S.-S. Wang. A secure dynamic ID based remote user authentication scheme for multi-server environment. *Computer standards and interfaces*, 31(1):24–29, 2009.

[8] T. Nakamura, S. Inenaga, D. Ikeda, K. Baba, and H. Yasuura. Anonymous authentication systems based on private information retrieval. In *The First Conference on 'Networked Digital Technologies'(NDT2009)*, pages 53–58, 2009.