

Accountable Privacy Based on Publicly Verifiable Secret Sharing

Young-Sam, Kim*,**, Seung-Hyun, Kim**, Seung-Hun, Jin*,**

**The Dept. of Information Security, University of Science and Technology, Daejeon, Korea*

***ETRI, Daejeon, Korea*

kim03, ayo, jinsh@etri.re.kr

Abstract— As developing the internet a variety of services emerge and service providers serve services such as using users' private information. Service providers require many types of information related users even including sensitive private information to serve a service with high quality, but users are reluctant to disclose their private information. Because if the private information is leaked it will lead to an invasion of privacy of users and may arise some problems about users' life. Nevertheless, service providers want to collect the users' information because of increasing their efficiency of services. As a result, it brings about a conflict of the loss and gain between users and service providers.

Anonymity is one of the solutions. Anonymity can get rid of linkability between transaction and users' private information. Therefore, users can provide their private information without concerns about leaking it and service providers can collect many types of information and serve services with high quality. However, anonymity may be abused, and used to undermine the protection goal of accountability. Namely, a person who is assured anonymity may serve information which is not related him/her. It may be reduced the quality of services.

Revocation of anonymity can make up for weak point of anonymity. But when anonymity is revoked legal dispute may be arisen and there is a cost of time or money.

In this paper, we propose a scheme for accountable privacy using secret sharing and some cryptographic methods. The scheme we propose reduces a cost of revocation of anonymity because there is maybe no legal dispute and keeps anonymity more secure against collusion between service provider and revocation authority.

Keywords— Accountable Privacy, Personalized Service, Verifiable Secret Sharing, Revocation , Time Capsule

I. INTRODUCTION

A variety of services are currently on the internet since the web has emerged. The service providers have been collecting users' information to improve a quality of services. They want to collect the private and sensitive users' information for the personalized services. But users reluctant to provide their own private and sensitive information with service providers because the private information is so important to them and also imply a hazard of an invasion of privacy. Many solutions have been proposed before to solve the problem and anonymity is one of them.

There are many schemes for anonymity. [1],[3],[6],[7] provide anonymity as well as revocation of anonymity to protect that malicious people abuse the anonymity and provide wrong information. It needs for a ground to request revocation of anonymity. [3],[6],[7] are able to revoke the anonymity but may need for legal dispute. It may be arisen a cost of money and time. [1] has minimized the legal dispute as assured a basis of revocation(e.g. Time limit of performance of a duty). It means service providers can serve more practical anonymous services to users.

However, [1] has some problems as follow

- Revocation authority only has a key to revoke the anonymity. Therefore, revocation authority is required to absolutely safety and be trusted.
- A basis of revocation is a part of a key when making the revocation key. It means the revocation key can be changed by a basis of revocation so that it is required to rigorous protocol to create a key and a basis of revocation.

We use a secret sharing method to solve the first problem we mentioned above. One of the important factors about secret sharing method is trusted dealer. In this paper, a user who has a secret key distributes a secret key. i.e. a user is a dealer. This is obvious for users' privacy but if a user is malicious then he/she abuses their power so that provides wrong identity or information. To prevent this, we set a CA(Certificate Authority) and an IDP(Identity Provider) and use their certificates by signing the identity of users' public key with their secret key. CA issues a certificate for users' public key and IDP issues a certificate for users' identity and then SP(service provider) and RAs(revocation authorities) can believe that a user correctly distribute a piece of secret.

To solve the second problem, we do not use a basis of revocation when generating a user's secret key. A basis of revocation is just a basis of revocation. It is used when revocation authority have to judge whether a service provider's request is correct or not. As doing so, a step for generating a secret key can be simple and revocation of anonymity would be fair and clear as publicly announce a basis of revocation to a user and a SP as well as RAs.

In this paper, we apply a concept of time capsule in [1] and publicly verifiable secret sharing in [4] to propose secure and practical scheme.

II. RELATED WORKS

A study on anonymity has been conducting in many ways. In this chapter, we introduce and analysis the scheme for anonymity which is proposed before.

A. Group Signature

David Chaum and Eugene van Heyst[6] first introduced a group signature. This scheme consists of many group members and one group manager. Group members only can generate a signature. Verifier can verify where the signature from but can't know the member who made the signature. Group manager who manages group members is able to revoke anonymity so users(prover or verifier) should trust him.

However, when revocation of anonymity is needed we need some legal dispute because a group manager needs some basis of revocation. So a prover and a verifier must consult about a basis of revocation and make a contract. But this is not technical but legal. If a conflict is arise between prover and a verifier it may brings about costs of money and time.

B. Ring Signature

Rivest, Shamir, Tauman[3] first introduced a ring signature which a shape of group is ring. It means there is no group manager so that absolute anonymity is assured. We need group member's public keys to generate ring signature. Group member's public keys are a factor that assures anonymity.

Revocation of anonymity is able to only prover who generates a signature because there is no group manager. It means there are no methods to enforce users' accountability.

C. Camenisch's Accountable Privacy

Camenisch, Groß, Heydt-Benjamin[1] proposed a scheme for accountable privacy. It assures that revocation of anonymity cryptographically so that a legal dispute is minimized. The scheme is constructed using many kind of cryptographic technique and a time capsule is generated by using verifiable encryption and identity based encryption. When a key to open a time capsule is generated, a time symbol is needed. It means revocation of anonymity is executed by technical method, not legal. [1] assume that there is a time server which is trusted to respond only current time. But when a user makes a time capsule, TLPD(time limit of performance of a duty) is needed. This is contradictory to assumption that a time server responds only current time. In addition, it is controversial how to get a time symbol corresponding TLPD for user, service provider, and a revocation authority.

III. CRYPTOGRAPHIC PRIMITIVE

A. Publicly Verifiable Secret Sharing

Shamir has proposed a (k, n) threshold scheme using polynomial interpolation named SS(secret sharing). SS is a method that is able to divide a secret to two or more pieces of secret so that protect a secret. 'n' is a total number of pieces and 'k' is the number of pieces which are needed to recover a secret. One of the problems in this scheme, a receiver of a piece of secret can't verify linkability between a piece and a secret.

Stadler has proposed a PVSS(Publicly Verifiable Secret Sharing) that a receiver of a piece of secret can verify that he/she received correct piece corresponding a secret. PVSS is based on polynomial interpolation and verifiable encryption. Steps of PVSS are following.

We assume that there are a dealer D , participant P_i who will receive a piece of secret, and a secret s . Let g, h be public elements, and $p, q = (p-1)/2$ be large primes. First, D chooses random numbers $x_i, i=1, \dots, n$, and $f_j, j=1, \dots, k-1$. Second, D calculates $S = g^s$ and $F_j = g^{f_j}, j=1, \dots, k-1$ and then publishes S and F_j . Third, D send s_i to each P using equation (1).

$$s_i = s + \sum_{j=1}^{k-1} f_j x_i^j \quad (1)$$

Fourth, D calculates $S_i = g^{s_i}$ and publishes it. Then each P can verify using equation (2) whether S_i is correct.

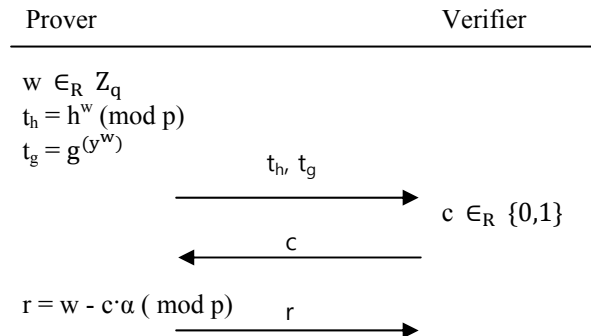
$$S_i = S \cdot \sum_{j=1}^{k-1} F_j^{(x_i^j)} \quad (2)$$

Now, each P can verify s_i is really come from s using formula $S_i = g^{s_i}$.

Each P can prove that he/she has s_i to another person using verifiable encryption. First, each P chooses random secret value z and calculate public value $y = h^z \pmod{p}$. Second, P encrypt message s_i with random value α using equation (3).

$$(A, B) = (h^a, s_i^{-1} \cdot y^a) \pmod{p} \quad (3)$$

Finally, each P can verify that she/he has correct s_i using zero knowledge proof as follow.



$$t_h \stackrel{?}{=} h^r A^c \pmod{p}$$

$$t_g \stackrel{?}{=} \begin{cases} g^{(y^r)}, & \text{if } c = 0 \\ S^{(B \cdot y^r)}, & \text{if } c = 1 \end{cases}$$

The pieces of secret are able to be recovered if k or more pieces are in the one site. In the following equation (4), a solution of $f(0)$ is a secret s .

$$f(x) = \sum_{i=1}^k \left(s_i \cdot \prod_{\substack{j=1 \\ (i \neq j)}}^k \left(\frac{x - x_j}{x_i - x_j} \right) \right) \quad (4)$$

In this paper, we use stadler's PVSS, and (2, 2) threshold scheme to help understand.

IV. PROPOSED SCHEME

Our scheme keeps anonymity using PVSS and other cryptographic primitives. Plus, we protect user's abuse of anonymity to enforce their accountability. Camenisch's scheme, time capsule system, assures revocation of anonymity technically so that reducing a cost of money and time while some schemes proposed before may need to legal dispute. However, camenisch's scheme has some problems we mentioned in earlier chapter.

The scheme we propose uses a concept of time capsule and PVSS instead of trusted time server to solve the camenisch's problems. Therefore we achieve accountable privacy more practically.

A. Trust Model

In this chapter, we describe a role and trust model of the entities that consist of our scheme.

1) Revocation Authority1, 2 (RA1, RA2): RA1 and RA2 keep a piece of secret to open time capsule. They must not collude with each other and disclose a piece of secret unless some conditions (e.g. TLPD has passed) is satisfied. Moreover, they are honest to keep a TLPD and prove a piece of secret they keep.

2) Identity Provider (IDP): IDP keeps and provides users' identities. IDP authenticates users and provides an identity only if a user is authenticated. IDP also checks the time capsule if it has correct identity and then certifies the time capsule by signing with its private key. SP trust IDP.

3) CA (Certificate Authority): CA issues a certificate for a user. RA1, RA2 trust CA.

B. System Overview

The scheme we propose is constructed like figure 1.

1) Issue(Cert_{CA}(S)): CA authenticates a user and issues a certificate about user's public key S .

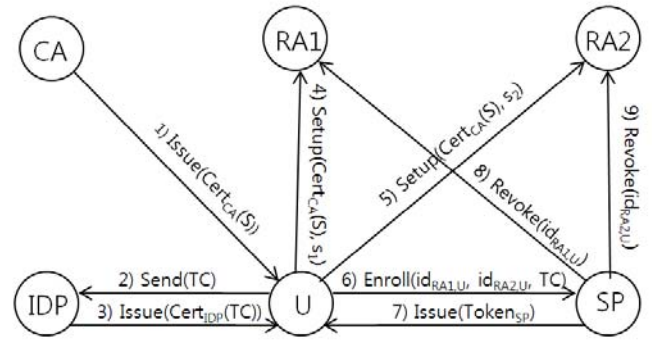


Figure 1. The flow of information during transactions

2) Send(TC): A U(user) encapsulates his/her identity with his/her secret key s , makes a TC (time capsule) and sends it to IDP.

3) Issue(Cert_{IDP}(TC)): IDP verifies a TC of a user and if it is verified then signs and sends a TC to U.

4) Setup(Cert_{CA}(S), s_1): U sends a piece of secret s_1 to RA1. RA1 verifies s_1 and then registers it. Then it issues $id_{RA1,U}$ to U.

5) Setup(Cert_{CA}(S), s_2): U sends a piece of secret s_2 to RA2. RA2 verifies s_2 and then registers it. Then it issues $id_{RA2,U}$ to U.

6) Enroll($id_{RA1,U}$, $id_{RA2,U}$, Cert_{CA}(S)): U sends $id_{RA1,U}$, $id_{RA2,U}$ to SP in order to use a service of anonymity. SP asks RA1 and RA2 that they keep a piece of secret of user. RA1 and RA2 can prove that they keep a piece of secret of user to SP using PVSS. If it is succeeded U and SP consult about TLPD and register it at RA1 and RA2. Finally, U sends a TC to SP. SP verifies a TC using IDP's public key.

7) Issue(Token_{SP}): After step 6), SP issues $Token_{SP}$ which can use a service of anonymity.

8) Roveke($id_{RA1,U}$): If U didn't perform his/her duty even though current date passed $TLPD$, SP can require RA1 to send a piece of secret. RA1 checks whether current date really passed $TLPD$, if so, RA1 sends s_1 , a piece of secret, to SP.

9) Roveke($id_{RA2,U}$): If U didn't perform his/her duty even though current date passed $TLPD$, SP can require RA2 to send a piece of secret. RA2 checks whether current date really passed $TLPD$, if so, RA2 sends s_2 , a piece of secret, to SP.

And now SP can recover a secret s with s_1 and s_2 so that a TC is opened by SP and user's identity is also disclosed.

C. Protocol Description

In this chapter, we describe parameters on each transaction we outline above and how to verify them. To avoid redundancy, some steps are omitted to describe.

First we assume that public parameter g , h and large prime p , $q = (p-1)/2$. A user's secret key is s and public key is $S = g^s$. They are used to encrypt or decrypt a TC .

1) Send(TC): U makes a TC with public key S like a following equation (5) and sends it to IDP.

$$TC = E(S, \text{identity}) \quad (5)$$

2) **Issue(Cert_{IDP}(TC))**: IDP can verify that a **TC** contains identity it issued before because it has **S** and identity of a user. If verification is succeeded, IDP signs a **TC** with its secret key like following equation (6) and sends it to U.

$$\text{Cert}_{IDP}(TC) = E(\text{sk}_{IDP}, TC) \quad (6)$$

3) **Setup(Cert_{CA}(S), s₁), Setup(Cert_{CA}(S), s₂)**: U chooses random value **x₁**, **x₂** and sends them to each of RAs. Then U divides a secret to two pieces **s₁**, **s₂** and calculates **S₁ = g^{s₁}**, **S₂ = g^{s₂}**. **S₁** and **S₂** are public parameter so anyone can know them. U sends **s₁**, **s₂** to RA1, RA2 respectively. RA1, RA2 verify a pieces they received using equation (2) and **Cert_{CA}(S)** respectively. If they are verified RA1 register **s₁** and RA2 register **s₂** and then each RA1, RA2 issues pseudonym **id_{RA1,U}** and **id_{RA2,U}** to U.

4) **Enroll(id_{RA1,U}, id_{RA2,U}, Cert_{CA}(S))**: SP can check that U registered correct pieces of secret to each RA. First SP asks RA1 and RA2 to check a piece of secret and then each of RAs verifiably encrypts its piece using equation (3). Suppose that RA1 chooses random value **α**, secret value **z₁**, and public value **y₁ = h^{z₁}** and RA2 chooses random value **β**, secret value **z₂**, and public value **y₂ = h^{z₂}**. Therefore each ciphertext is as follow.

$$RA1 : (A_1, B_1) = (h^{\alpha}, s_1^{-1} \cdot y_1^{\alpha}) \pmod{p} \quad (7)$$

$$RA2 : (A_2, B_2) = (h^{\beta}, s_2^{-1} \cdot y_2^{\beta}) \pmod{p} \quad (8)$$

RA1 and RA2 send their ciphertexts (7), (8) to SP. Now SP has parameters enough to verify that each of RAs have correct piece of secret. (SP has **S**, ciphertext (7), (8), **g**, **h**, **y₁**, **y₂**) RA1 and RA2 finally prove that they have a piece of secret using zero knowledge proof. If proof ends up successfully, U and SP consult about their **TLPD** (Time Limit of Performance of a Duty) and sends it to each RA. Each of RAs check **TLPD** received from U and SP respectively in order that U and SP has send correct **TLPD**. If each of **TLPDs** from U and SP are identical each RA register the **TLPD**. Next, U sends (6) to SP and then SP verifies it is really issued by IDP using IDP's public key

5) **Revoke(id_{RA1,U}, Revoke(id_{RA2,U}))**: SP require each RA to a piece of secret to get a user's real identity. RA1 and RA2 retrieve user's **TLPD** using **id_{RA1,U}** and **id_{RA2,U}** respectively and compare them with current date. If current date passed **TLPD** (**TLPD** < current date), RA1 and RA2 send their pieces of secret to SP. SP now can recover a secret to open a **TC** and finally get a user's real identity.

V. CONCLUSIONS AND FUTURE WORKS

In this paper, we propose a scheme for accountable privacy using a concept of time capsule. In addition, we propose a method for revocation of anonymity that a user and a SP(service provider) can accept without legal dispute and improve a security of scheme using PVSS(publicly verifiable secret sharing).

We are supposed that CA, RA, IDP should operate in compliance with proposed trust model. A user has made an important role in the proposed scheme. Trust model and our scheme enforce to perform honestly on a user. It is systemically and cryptographically enforced so SP and other entities can trust that a user behave honestly and verify of course. On the other hand, SP may also be malicious. SP can ignore a contract with a user (e.g. TLPD(Time Limit of Performance of a Duty)) and require a piece of secret to each RA. However, it can be rejected by RA because RA knows TLPD which a user and a SP set before. Plus there can be two or more RAs to prevent the collusion. In proposed scheme, we consider only two RAs for convenience but it would be varied according to (k, n) threshold scheme.

The proposed scheme is able to provide secure service of anonymity as describe above. One of the future works is that we need to implement user agent because a user have to do many tasks in the proposed scheme. The other is the proposed scheme is inefficient when there are many SPs. Suppose that a user is provided a service of anonymity with only one key pair. Hence, a user's anonymity may be revoked in all SPs even though a user did not perform his/her duty of only one SP. To solve this problem, a user has to manage different keys with each SP and RAs also have to manage the users' key pairs. Therefore some changes are needed in our scheme later.

ACKNOWLEDGMENT

The authors wish to thank people who work at Authentication Research Team, ETRI, Korea, which have helped us to improve the paper.

REFERENCES

- [1] Jan Camenisch, Thomas Groß, and Thomas S.Heydt-Benjamin, "Rethinking Accountable Privacy Supporting Services", DIM2008, 2008.
- [2] Y.K. Lee, S.W. Han, S.J. Lee, B.H. Chung, D.H. Nyang, and T.K.Kwon, "The Technology and Trend of Anonymous Authentication", The Analysis of Electronic and Telecommunication Trend Vol. 23, ETRI, August, 2008.
- [3] Ronald L. Rivest, Adi Shamir, and Yael Tauman, "How to Leak a Secret," ASIACRYPT2001, LNCS 2248, pp. 552-565, 2001.
- [4] Markus Stadler, "Publicly Verifiable Secret Sharing", EUROCRYPT'96, volume 1070 of LNCS, pp. 190-199, 1996
- [5] Adi Shamir, "How to Share a Secret", ACM '79, 1979
- [6] David Chaum, and Eugene van Heyst, "Group Signatures", EUROCRYPT'91, 1991
- [7] Jan Camenisch, and Markus Stadler, "Efficient Group Signature Schemes for Large Groups", CRYPTO'97, 1997
- [8] S.J. Park, S.M. Park, D.H. Won, and D.H. Kim, "An Efficient Verifiable Escrowed Signature and Its Applications", Korea Institute of Information Security & Cryptology, volume 8, December, 1998
- [9] Jan Camenisch, and Ivan B. Damgard, "Verifiable Encryption and Applications to Group Signatures and Signature Sharing", BRICS, December, 1998
- [10] Mike Burmester, Yvo Desmedt, Rebecca N. Wright, and Alec Yasinsac, "Accountable Privacy", Security Protocol 2004, LNCS 3957, pp.83-95, 2006