情報保護學會論文誌
第16卷 第5號, 2006. 10

추적 가능한 가명 은밀 획득 프로토콜*

양 대 헌,[1†] 이 경 희[2‡]
[1]인하대학교 정보통신대학원, [2]수원대학교 전기공학과

Private Pseudonym Retrieval with Controlled Traceability

DaeHun Nyang[1†] KyungHee Lee[2‡]
[1]The Graduate School of Information Tech & Telecomm, InHa University
[2]Department of Electrical Engineering, The University of Suwon

요 약

가명을 이용한 시스템에서는 가명을 발급한 기관에게도 사용자의 익명성이 유지되어야 하며, 다만 정책적으로 사용자가 규칙을 어겼을 때는 가명으로부터 사용자의 신원정보를 추적할 수 있어야 한다. 이 논문에서는 m-out-of-n oblivious transfer와 cut-and-choose 기술을 이용하여 추적 가능한 가명 은닉 획득 프로토콜을 제안한다.

ABSTRACT

Pseudonyms must be maintained anonymously even to the organization that issues the pseudonyms, but when some event occurs that policy defines the real identity for the pseudonym must be able to be traced. We propose a private pseudonym retrieval protocol with controlled traceability using m-out-of-n oblivious transfer and cut-and-choose technique.

Keywords : Anonymity, Pseudonym, Oblivious Transfer, Credential, Cut and Choose

Ⅰ. Introduction

Most researches on pseudonym have focused on the unlinkability among pseudonyms in credential transfer, but our concern is a method to issue/retrieve pseudonyms privately with conditional traceability[3][4][6][7][9]. By "privately", we mean that even under inevitable exposure of implicit information about user's identity, user can obtain its pseudonyms without letting authorities know which pseudonyms that it will use in future transactions. In the conditional traceability setting, cooperation of pseudonym issuing authorities must enable judicial authority "trace" user's identity from the pseudonym when some "condition" is satisfied that policy defines. By accompanying a key with a pseudonym, user can prove its ownership of the pseudonym using an authentication protocol. Our contribution can be summarized as following:

(1) We provide a new direction to design a

접수일: 2006년 8월 31일; 채택일: 2006년 9월 25일
*이 논문은 2004년도 한국학술진흥재단의 지원에 의하여 연구되었음 (KRF-2004-015-D00389)
† 주저자: nyang@inha.ac.kr
‡ 교신저자: khlee@suwon.ac.kr

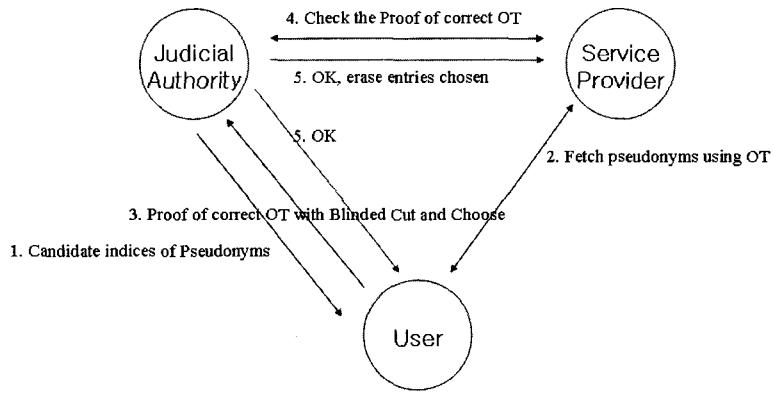

Fig. 1 Overview of Private Pseudonym Retrieval Protocol

pseudonym system using oblivious transfer that has not been used in accessing with pseudonyms.

(2) Using our pseudonym retrieval protocol as a primitive building block, more advanced protocols and systems requiring controlled anonymity can be developed. We show its applications in section 5.

II. Overview of Our Protocol

A private pseudonym retrieval protocol must achieve the following goals when a user is issued a pseudonym from a service provider:

(1) User must authenticate itself by real identity both to Service Provider and to Judicial authority when it is issued a pseudonym.

(2) Neither Service Provider nor Judicial authority can link a pseudonym with user's identity.

(3) If Judicial authority obtains specific information of user from Service Provider, it can trace user's real identity from the pseudonym concerned.

Our private pseudonym retrieval(PPR) protocol is mainly based on m-out-of-n oblivious transfer(or equivalently symmetric private information retrieval) and cut and choose technique.

Assume the following scenario: At the enrollment stage, user authenticates him both to judicial authority and to service provider with its real identity using some security token such as certificates. Interacting with judicial authority and service provider, user obtains a pseudonym and its corresponding authentication key pair without letting them know which pseudonym it has taken. At service provider, user would like to act as an entity with some pseudonyms and its corresponding authentication keys. Here, even service provider cannot link pseudonyms with the real identity that was used at enrollment stage. However, when some event occurs that policy defines, service provider would like to accuse him of violation and to punish him. At this stage, judicial authority will involve to identify him by combining its own information obtained at the enrollment stage and the information submitted by service provider. After identifying the misbehaving user, judicial authority can punish him without letting service provider know the real identity.

To construct this private pseudonym retrieval protocol with controlled traceability, user authenticates himself both to judicial authority and to service provider using its certificate. (1) After establishing secure channels both with judicial authority and service provider, user retrieves candidate indices of pseudonyms of service provider. (2) User fetches (pseudonym, authentication key) pairs of candidate indices from service provider using m-out-of-n oblivious transfer. (3) User sends proof that it correctly fetches pseudonyms with candidate indices to judicial authority with blinded cut-and-choose technique. (4) Judicial authority checks the validity of proof to service provider. If valid, then judicial authority sends OK both to user and to service provider. Both at judicial authority and at service provider, all rest except one chosen blob(here, a pseudonym) must be marked as "used". (5) User now can use one remaining blob chosen as his pseudonym with its corresponding authentication key.

Ⅲ. Private Pseudonym Retrieval Protocol

3.1. Setup

Service provider prepares pseudonym pool $v1:(pID_{v1}, k_{v1}), v2:(pID_{V2}, k_{V2})\cdots \quad vn:(pID_{vn}, k_{vn})$, where vi is an index for the pair, pID_{v1} and k_{v1} are a pseudonym and its corresponding authentication key with index vi, respectively.

Judicial authority prepares index pool $(v1, unused), (v2, unused), \cdots, (vn, unused)$.

Player M authenticates himself both to judicial authority and to service provider and establishes secure channel with each authority using some security token and certificates.

3.2. Protocol action

(1) JA → M: JA randomly chooses an index list $L=\{v1, v2, \cdots, vm\}$, where indices in the index list must be "*unused*", and send it to M.

(2) M ↔ SP: M performs m-out-of-n oblivious transfer against SP to fetch m pseudonym pairs $[(pID_{v1}, k_{v1}), (pID_{v2}, k_{v2}), \cdots, (pID_{vm}, k_{vm})]$ that have the same indices in L. We can use the oblivious transfer protocol in [10].

(3) M → JA: Player sends $[(v1, E_{b1}(k_{v1})), (v2, E_{b2}(k_{v2})), \cdots, (vm, E_{bm}(k_{vm}))]$ to JA, where bi is a key to encrypt k_{vi}.

(4) JA → M: JA chooses randomly m-1 indices and requests decryption keys of those of M.

(5) M → JA: M sends blob decryption key $[b_1, b_2, \cdots b_{j-1}, b_{j+1}, \cdots b_m]$ to JA.

(6) JA ↔ SP: JA decrypts the blobs to validate by providing service provider $[(v1, k_{v1}), (v2, k_{v2}), \cdots, (vj-1, k_{vj-1}), (vj+1, k_{vj+1}), \cdots (vn, k_{vm})]$ list. Then, SP checks the validity of the index and the key pairs, and sends back its result to JA. Note that JA cannot know neither m-th pseudonym nor its authentication key.

(7) JA → M, SP: If all are valid, then JA sends OK both to SP and to M. SP will delete or mark "used" the m-1 entries and JA store (M, vj) pair in its storage. Also JA must convert the m indices into "*used*". If not, it sends ABORT to both of them. SP must delete or mark "*used*" the m entries known to M. Mismatch occurs because M fetches the different entries from what JA forces to choose. If mismatches occur p times, JA is able to find exactly m entries from M by asking M m correct pseudonym and key

pairs.

(8) Player M can now play as pID_{vj} with the corresponding authentication key k_{vj} with service provider.

Ⅳ. Security and Extension

SP cannot find out which pseudonym a user has because of oblivious transfer and cut and choose. Without cut and choose, SP can guess which pseudonym the connecting user fetches because JA requests validity of some index when the user is connecting. However, by applying cut and choose here, SP is not able to know the remaining pseudonym index. Also, JA does have only an index of pseudonym for the user, and thus, it cannot link pseudonym with user's identity.

If some event occurs that policy defines, SP sends corresponding user's (vi, pID_{vi}) pair to JA. JA then is able to match an entry with (M, vi) in its database. Even in this case, SP is not able to know who really violates rules.

Instead of revealing m-1 blobs, we can modify our protocol to reveal m-alpha blobs in the cut and choose stage. By doing so, user can get alpha pseudonyms, which is useful when a limited unlinkability(within alpha pseudonyms) must be maintained. However, revealing smaller part of blobs means that user has more probability to cheat by fetching different pseudonyms from those indexed by JA. To be safe from this reduction of blob opening, m also must be chosen larger proportionally. The probability that user succeeds to hide its choosing of a pseudonym that is not indexed by JA is

$$P_{cheat} = \binom{m-1}{m-\alpha} / \binom{m}{m-\alpha} = \frac{\alpha}{m}$$

Thus, sufficiently large m corresponding to alpha must be chosen considering the overhead of communication and security.

Blobs in cut and choose stage are data that are hidden from JA, but actually it does not need to be hidden from JA because only the index and its authentication key for some pseudonym does not give any information that might be abused to JA. However, the authentication key for some identity(here, pseudonym) is usually known only to its owner, and so is our protocol.

Ⅴ. Applications

Persistent anonymity requires both impossibility of identity-pseudonym mapping and consistent use of a pseudonym. Thus, applications requiring the persistent anonymity are fit to our PPR protocol. Refer to [1] for more applications with detailed analysis requiring anonymity. Anonymous auction, anonymous email and anonymous publication are examples of applications requiring persistent anonymity. Besides those, followings are the main target of application of our PPR protocol.

(1) Anonymous certificate issuing

Very practical approaches to anonymous certificates/credentials without unlinkability have been suggested by [2] and [8]. Our scheme can be used to issue anonymous certificates/credentials while providing controlled traceability. After user obtains pseudonym with our PPR protocol, using the pseudonym, he can request to issue a certificate for his public key and the pseudonym to Certificate Authority. Here, the role of service provider can be transferred either to Registration Authority or to Certificate Authority. Certificates

obtained in this way are persistently anonymous, but at the time of violation, it can be used to trace its user's identity by judicial authority.

(2) Anonymous BBS

Many Internet BBS attracts people by their allowance of anonymity, but freedom of expression is sometimes abused. Thus, some extent of restriction is required. Our PPR protocol can play a role in anonymous BBS by issuing user a pseudonym. Violation of a regulation and a law at the BBS will cause involvement of judicial authority that is able to trace user's identity by the aid of BBS operator.

(3) Anonymous consulting/counseling

Medical or business consulting sometimes requires anonymity, but the history of consulting must be maintained by consultant. Also, in emergency case, the identity of consulter must be able to be revealed.

Ⅵ. Conclusion

We presented a method to retrieve privately a pseudonym from pseudonym pool. The protocol presents also the tracing algorithm for the pseudonym concerned. Our scheme has versatility in that it is applicable to various applications that require persistent anonymity such as anonymous certificate issuing, anonymous BBS, anonymous consulting. In our work, no special structure for pseudonyms is defined, but a pseudonym is just a random number. Therefore, we believe that our private pseudonym retrieval protocol can be incorporated into other anonymous credential systems supporting unlinkability for enhancing user's privacy.

References

[1] 박해룡, 김지현, 천동형, 전길수, 이재일, "프라이버시 보호를 위한 익명성 및 익명성 제어 모델 분석," 정보보호학회지 14권 6호, pp.14-27, December, 2004

[2] V. Benjumea, J. Lopez, J. Montegegro, and J. Troya, "A first approach to provide anonymity in attribute certicates," PKC 2004, Lecture Notes in ComputerScience, vol. 2947, Springer-Verlag, pp.402-415, 2004.

[3] J. Camenisch and E. Herreweghen, "Design and implementation of the Idemix anonymous credential system," ACM Conference on Computer and Communications Security, pp.21-30, 2002.

[4] J. Camenisch and A. Lysyanskaya, "Efficient non-transferable anonymous multishow credential system with optional anonymity revocation," Eurocrypt '01, Lecture Notes in Computer Science, vol. 2045, Springer-Verlag, pp.93-118, 2001.

[5] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 4, no. 2, February 1981.

[6] D. Chaum and J. Evertse, "A secure and privacy-protecting protocol for transmitting personal information between organizations," CRYPTO '86, Lecture Notes in Computer Science, vol. 263, Springer-Verlag, pp.118-167, 1987.

[7] L. Chen, "Access with pseudonyms," Cryptography: Policy and Algorithms, Lecture Notes in Computer Science, vol. 1029, Springer-Verlag, pp.232-243, 1995.

[8] T. Kwon, J. Cheon, Y. Kim and J. Lee, "Privacy Protection in PKIs: A Separation-of-Authority Approach," Work-

shop on Information Security Applications 2006, to appear.

[9] A. Lysyanskaya, R. Rivest, A. Sahai and S. Wolf, "Pseudonym systems," Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 1758, Springer-Verlag, 1999.

[10] Y. Mu, J. Zhang and V. Varadharajan, "m out of n oblivious transfer," In Proceedings of the 7th Australasian Conference on Information Security and Privacy (ACISP '02), volume 2384 of LNCS, pp. 395-405. Springer-Verlag, 2002.