6-8 Secure and Anonymous Communication Technique

Keita EMURA and Takeshi TAKAHASHI

In this paper, we introduce our secure and anonymous communication technique which realizes secure communication and anonymous authentication simultaneously (this appears in IEEE Transactions on Emerging Topics in Computing 2015). As a remark, a simple combination of a secure communication technique and an anonymous authentication technique does not implement this functionality. For example, even if the underlying authentication scheme supports anonymity, additional values for communication, e.g., IP address, may detract anonymity, or public key certificate of public key infrastructure contradicts anonymity. In our protocol, we construct a secure and anonymous communication protocol by adequately combining cryptographic schemes (ID-based encryption and group signature) and anonymous communication protocols (Onion Routing). Its security is evaluated by using a standard provable security framework of cryptography.

1 Introduction

From the view point of privacy, some services are anonymously provided without identifying the user [1]. On the other hands, it sees not easy to check whether the anonymous user has a right to use the service or not due to anonymity. As a well-known cryptographic primitive providing anonymity, group signature is known [2]. The group manager issues a signing key to a signer, and the signer generates a signature. The verifier verifies a signature by using the group public key regardless of signers. So, the verification process does not identify the actual signer. In group signatures, a strong security level called unlinkability is required where no one, except the group manager, can distinguish whether two signatures are made by the same signer or not. As a remark, group signatures just guarantee that no personal information is revealed from signatures. That is, other information for communication may detract anonymity, e.g., IP address needs to be hidden when group signatures are sent. So, it seems natural to consider using a proxy entity between a user and a service provider (SP), such as Simpleproxy[3] and Tor[4]. In this usage, a group is regarded as a set of legitimate users who have rights to use the service. As a next step, we need to consider how to encrypt the content in such an anonymous environment. If a user has a public key, then the user is identified by its public key certificate.

In this paper, we introduce our secure and anonymous communication technique which realizes secure communication and anonymous authentication simultaneously[5]. In our protocol, we construct a secure and anonymous communication protocol by adequately combining cryptographic schemes (Identity-based encryption, IBE[6] and group signature) and anonymous communication protocols (Onion Routing). Its security is evaluated by using a standard provable security framework of cryptography.

2 Brief description of the protocol

We employ IBE as the underlying encryption scheme. In IBE, any value, typically identity of a user (for example, e-mail, name, and so on), can be regarded as a public key. A key generation center (KGC) issues a secret key to a user according to the identity of the user. We give a brief description of our protocol in Fig. 1. In our protocol, a user generates a random number TempID for each session, and computes a group signature σon TempID. The user sends (TempID, σ) to the SP via the proxy. The SP checks the signature σ, and if it is valid, then the SP encrypts the content by using TempID as a public key.

The SP can anonymously check whether a user has rights to use the service by verifying the signatureσ. Moreover, since σ is a signature for TempID, it is guaranteed that TempID is chosen by the user. In addition, due to the security of IBE (indistinguishability), no information of M is revealed from the ciphertext. See the detailed security proofs in [5].

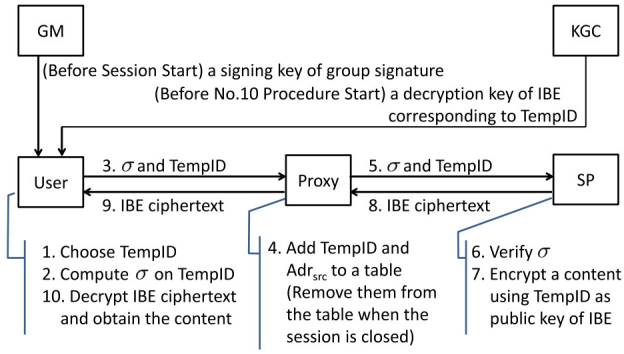

Fig. 1 A Brief Description of the proposed protocol [5,7]

3 Efficiency of the proposed protocol

Here, we introduce the efficiency evaluation given in [5]. We define the SendRequest algorithm (computation of a group signature, Fig. 1, procedure 2), the ValidityCheck algorithm (verifying the group signature, Fig. 1, procedure 6), the SendContent algorithm (encryption of the content by using IBE, Fig. 1, procedure 7), the GetContent algorithm (decryption of the ciphertext, Fig. 1, procedure 10) in [5]. We employ the Furukawa-Imai group signature scheme[8] (with a slight modification), and the Boneh-Franklin IBE scheme[6], and use the TEPLA library [9] (Table 1). Our implementation environment is as follows: Apple MacBookPro (processor: 2.6GHz Intel Core i7, Memory: 16GB, 1600 MHz DDR3, Darwin Kernel Version 13.1.0), and VMware (Fusion 6.0.2).

Next, we show the running time of our protocols as follows (Table 2). In the case of Simpleproxy, the running time of our protocol is approximately 20 times slower than that of SSL communication. This inefficiency is caused by the pairing computation that is not required in usual public key encryption, digital signature, and authentication (these are used in SSL). Nevertheless, it is particularly worth noting that our running time still fits inside the msec order. In a Tor network, data are communicated via several Tor routers. That is, different servers are chosen in each communication to hide source IP addresses, and this costs significantly. Moreover, communication among Tor routers is encrypted (note that this is not an end-to-end encryption, whereas our protocol establishes end-to-end secure channels and therefore, no Tor routers can reveal content information in our protocol). Because of this, the running time of Tor cases have a wider range at each execution, and we can interpret that the cost of all cryptographic operations are not dominant when Tor is used as the underlying proxy module.

Table 1 Running time (Algorithms) [5][7]

Algorithm	Entity	Time(msec)	Proxy Module
SendRequest	User	63.90	Simple Proxy
		62.50	Tor
ValidityCheck	SP	87.67	Simple Proxy
		89.40	Tor
SendContent	SP	87.36	Simple Proxy
		85.99	Tor
GetContent	User	52.17	Simple Proxy
		54.23	Tor

Table 2 Running time (1 Session) [5][7]

Scheme	Cryptographic Operations	Time(msec)	Proxy Module
None	-	2.55	Simple Proxy
	-	8375.48	Tor
SSL	Enc &Auth	14.22	Simple Proxy
		7750.00	Tor
Ours	Enc &Anon. Auth	293.53	Simple Proxy
		9755.53	Tor

4 Conclusion

In this paper, we introduce our secure and anonymous communication technique which realizes secure communication and anonymous authentication simultaneously. We have proposed more efficient protocol that does not use IBE. See the paper [10] for details. In actual systems, it is indispensable to provide revocation. However, it is difficult to decide whether an anonymous user has been revoked or not. Revocable group signature schemes, e.g.,[11] could be a solution. However, there is a room for improvement for its efficiency for the actual systems. We leave it as a future work.

References

1 Selected papers in anonymity. http://freehaven.net/
2 D. Chaum and E. van Heyst. Group signatures. In EUROCRYPT, pp.257–265, 1991.
3 Simpleproxy: Crocodile group software. http://www.crocodile.org/software.html.
4 Tor Project. Tor project: Anonymity online. https://www.torproject.org/.
5 Keita Emura, Akira Kanaoka, Satoshi Ohta, Kazumasa Omote, and Takeshi Takahashi, "Secure and Anonymous Communication Technique: Formal Model and Its Prototype Implementation," IEEE Trans., Emerging Topics Comput., 4(1), pp.88–101, 2016. (full version of [7])
6 D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," SIAM J. Comput., 32(3), pp.586–615, 2003.
7 Keita Emura, Akira Kanaoka, Satoshi Ohta, and Takeshi Takahashi, "Building secure and anonymous communication channel: formal model and its prototype implementation," ACM SAC 2014, pp.1641–1648, 2014.
8 Jun Furukawa and Hideki Imai, "An Efficient Group Signature Scheme from Bilinear Maps," IEICE Transactions 89-A(5), pp.1328–1338, 2006.
9 TEPLA, "University of Tsukuba Elliptic Curve and Pairing Library," [Online]. Available: http://www.cipher.risk.tsukuba.ac.jp/tepla/index_e.html, accessed Feb. 20, 2015.
10 Keita Emura, Akira Kanaoka, Satoshi Ohta, and Takeshi Takahashi, "A KEM/

DEM-Based Construction for Secure and Anonymous Communication," COMPSAC Workshops 2015, pp.680–681, 2015.
11 Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, and Yusuke Sakai, "Revocable Group Signature with Constant-Size Revocation List," Computer Journal, 58(10), pp.2698–2715, 2015.

Keita EMURA, Ph.D.

Senior Researcher, Security Fundamentals Laboratory, Cybersecurity Research Institute
Cryptography

Takeshi TAKAHASHI, Ph.D.

Senior Researcher, Cybersecurity Laboratory, Cybersecurity Research Institute
Cybersecurity, Network Security