Journal of Information Security and Applications 34 (2017) 84–91

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Establishing secure and anonymous communication channel: KEM/DEM-based construction and its implementation☆

Keita Emura[a,*], Akira Kanaoka[b], Satoshi Ohta[a], Takeshi Takahashi[a]

[a] National Institute of Information and Communications Technology, 4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
[b] Toho University, 2-2-1 Miyama, Funabashi-shi, Chiba 274-8510, Japan

ARTICLE INFO

Article history:
Available online 24 February 2017

Keywords:
Anonymous communication
Anonymous authentication
Secure channel
Key encapsulated mechanism
Data encapsulation mechanism
Group signature

ABSTRACT

Several cryptographic tools provide anonymity in a cryptographic sense, but solely using such a tool does not guarantee anonymity; for example, even if the underlying cryptographic primitives enable anonymity in some sense, a communication system using these tools may reveal the senders' IP address. Moreover, since a certificate of public key infrastructure contains information of a key holder, and that contradicts anonymity of the key holder, the certificate must be removed. Therefore, it seems difficult to check the validity of the public key in an anonymous environment. That is, constructing a secure and anonymous communication protocol, where end-to-end encryption and anonymous authentication are achieved simultaneously, is an important issue to be solved.

In ACM SAC 2014 (and IEEE Trans. Emerging Topics Comput. 2016), such a protocol was proposed, where it applies identity-based encryption (IBE) for packet encryption without contradicting anonymity. However, this protocol is inefficient and approximately 20 times slower than that of SSL communications because IBE requires heavy cryptographic pairing computations.

In this paper, we propose a more efficient, secure, and anonymous communication protocol, which achieves the same security level as the IBE-based protocol does. The protocol is exempted from pairing computation for establishing a secure channel by applying hybrid encryption instead of IBE. We implement the protocol and show that it is more efficient (overall approximately 1.2 times faster) than the IBE-based protocol. In particular, the decryption algorithm of our protocol is several hundred times faster than that of the IBE-based protocol. In our protocol, we employ the ElGamal KEM scheme and 128-bit AES as the underlying KEM and DEM schemes, respectively, and we have used the TEPLA library for the prototype implementation.

1. Introduction

Several cryptographic tools provide anonymity in a cryptographic sense, but solely using such a tool does not guarantee anonymity; for example, even if the underlying cryptographic primitives enable anonymity in some sense (e.g., group signature [2], key-private public key encryption [3], anonymous identity-based encryption [4], anonymous broadcast encryption [5] and so on), a communication system using these tools may reveal the senders' IP address. Then, the sender anonymity is never achieved even though cryptographic tokens (e.g., ciphertext or signature) do not reveal any sender information. Therefore, we need to consider not only the cryptographic building blocks but also communications for providing anonymous communications. Moreover, since a certificate of public key infrastructure contains information of a key holder, and that contradicts anonymity of the key holder, the certificate must be removed. Therefore, it seems difficult to check the validity of the public key in an anonymous environment. That is, constructing a secure and anonymous communication protocol, where end-to-end encryption and anonymous authentication are achieved simultaneously, is an important issue to be solved.

One candidate is to employ pseudonym certificates that hide information of key holders. For example, Whyte et al. [6] provided Security Credential Management System (SCMS), where pseudonym certificate authority issues certificates to vehicles frequently and vehicles are required to update their certificates. This system considers location privacy and prevents to link vehicles. Huang [7] also introduced pseudonym certificates for anonymous communications. Based on group signatures, several attempts for

☆ A preliminary version of this paper is presented in The 39th Annual International Computers, Software & Applications Conference, COMPSAC 2015 [1]. This is the full version.

* Corresponding author.
E-mail address: k-emura@nict.go.jp (K. Emura).

http://dx.doi.org/10.1016/j.jisa.2016.12.001
2214-2126/

adding anonymity to the standard X.509 certificates have already been made, e.g., [8–10].

A secure and anonymous communication protocol was proposed in [11,12], where a service provider (SP) sends encrypted content to a user while simultaneously and anonymously authenticating the user. The protocol employs identity-based encryption (IBE) [13] to encrypt contents without identifying key holders and employs a group signature [2] for anonymous user authentication. This protocol considers an intermediate proxy entity for establishing the anonymous communication. Briefly, a user randomly chooses a temporal ID for each session (as pseudonym), computes a group signature on this ID as its certificate, and sends it to the SP via the proxy. Unlike pseudonym certificates approaches [6,7], no authority is required for issuing certificates since each user can make a signature on behalf of the group. The SP encrypts a content by using IBE, and sends its ciphertext to the user via the proxy.

Our Motivation. Although the abovementioned IBE-based protocol simultaneously supports end-to-end encryption and anonymous authentication, its shortcoming is its efficiency. That is, the running time of the protocol is approximately 20 times slower than that of SSL communication (in our implementation result, See Section 4 for details). This delay is perceivable to users and decreases the usability of online services; thus, more efficient construction is needed in practice. Indeed, pairing (i.e., a bilinear map over elliptic curves) computations used in the protocol are the dominant factor of the computational costs. Moreover, though no authority is required for issuing certificates unlike pseudonym certificates approaches [6,7], IBE requires a trusted key generation center (KGC) that issues secret keys of users. If anyone can self-derive his/her private key for IDs chosen by them, then no security is guaranteed since anyone can obtain private keys of other users. Thus, such a KGC is indispensable in IBE systems. Nevertheless, it is desirable to remove trusted third parties as much as possible in practice. In addition to this, it is quite difficult to construct an efficient IBE scheme without pairings due to the impossibility results [14]. Therefore, if the paring computations of IBE need to be reduced, we need to investigate another method to realize a secure and anonymous communication protocol without using IBE.

Our Contribution. In this paper, we point out that no IBE is required for constructing a secure and anonymous communication protocol, and we construct a more efficient protocol that achieves the same security level as the IBE-based protocol [11,12] does. By modifying the protocol syntax properly, we can apply the KEM/DEM framework [15][1] for establishing a secure channel instead of IBE; a session key is encapsulated by the KEM part, and the actual data is encrypted by the DEM part. That is, although the user additionally needs to compute a ciphertext by using the SP public key (which can be certified by a public key infrastructure) for establishing a secure channel, no pairing computation is required for decryption or encryption by the user or the SP, respectively. As a remark, the user's anonymity still holds since the certificate contains SP's information only and is independent of the user.

Moreover, we implement our protocol with the ElGamal KEM scheme (as the KEM part), AES (as the DEM part), the open-free variant of the Furukawa-Imai group signature scheme [11,12], and Simpleproxy [16]. Based on the implementation, we clarify that our protocol is more efficient than the IBE-based protocol. Concretely, our protocol is approximately 1.2 times faster than the original protocol. In particular, the decryption algorithm of our protocol is several hundred times faster than that of the previous protocol.

[1] KEM stands for Key Encapsulated Mechanism, and DEM stands for data encapsulation mechanism.

Organization. The rest of this paper is organized as follows: We define cryptographic tools (KEM/DEM and group signature) in Section 2. Next, we present an overview of the framework of our protocol, introduce our main idea called the dividing technique, and give the proposed protocol and its instantiation in Section 3. We evaluate the proposed scheme from the standpoints of performance and deployability in Section 4, and finally, we conclude this paper in Section 5.

2. Preliminaries: cryptographic tools

In this section, we define KEM/DEM [15] and open-free group signature [11,12]. For a set X and an element $x \in X$, $x \xleftarrow{\$} X$ implies that x is randomly chosen from X.

Definition 2.1 (Syntax of KEM)**.** The public-key encapsulation mechanism KEM consists of the following three algorithms $(\mathsf{KeyGen}_{\mathsf{KEM}}, \mathsf{EnCap}, \mathsf{DeCap})$:

- $\mathsf{KeyGen}_{\mathsf{KEM}}$: The key generation algorithm takes a security parameter k as input and outputs a pair of public key and decryption key (pk, dk).
- EnCap: The encapsulation algorithm takes pk as input and outputs an encapsulation C_{KEM} and a session key $K \in \mathsf{KeySp}(k)$, where $\mathsf{KeySp}(k)$ is a key space.
- DeCap: The decapsulation algorithm takes dk and C_{KEM} as input and outputs K or $\perp$.

Definition 2.2 (Syntax of DEM)**.** The data encapsulation mechanism DEM consists of the following two algorithms $(\mathsf{DEnc}, \mathsf{DDec})$:

- DEnc: The encryption algorithm takes a key $K \in \mathsf{KeySp}(k)$ and plaintext M as input and outputs a ciphertext C_{DEM}, where $\mathsf{KeySp}(k)$ is a key space.
- DDec: The decryption algorithm takes K and C_{DEM} as input and outputs M or $\perp$.

Definition 2.3 (Syntax of PKE)**.** The public-key encryption scheme PKE consists of the following three algorithms $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$:

- KeyGen: The key generation algorithm takes a security parameter k as input and outputs a pair of public key and decryption key (pk, dk).
- Enc: The encryption algorithm takes pk and a message M as input and outputs a ciphertext C.
- Dec: The decapsulation algorithm takes dk and C as input and outputs M or $\perp$.

Next, we construct a PKE scheme from KEM/DEM which is called hybrid encryption.

Construction 2.1 (Hybrid Encryption)**.**

- KeyGen: Run $(pk, dk) \leftarrow \mathsf{KeyGen}_{\mathsf{KEM}}(1^k)$ and output (pk, dk).
- Enc: Run $(C_{\mathsf{KEM}}, K) \leftarrow \mathsf{EnCap}(pk)$, compute $C_{\mathsf{DEM}} \leftarrow \mathsf{DEnc}(K, M)$, and output $C = (C_{\mathsf{KEM}}, C_{\mathsf{DEM}})$.
- Dec: Run $K \leftarrow \mathsf{DeCap}(dk, C_{\mathsf{KEM}})$, compute $M \leftarrow \mathsf{DDec}(K, C_{\mathsf{DEM}})$, and output M.

Next, we define IND-CPA security as follows:

Definition 2.4 (IND-CPA Security)**.**

- The challenger $\mathcal{C}$ runs $(pk, dk) \leftarrow \mathsf{KeyGen}_{\mathsf{KEM}}(1^k)$ and sends pk to the adversary $\mathcal{A}$.
- $\mathcal{A}$ sends M_0^* and M_1^*, where $|M_0^*| = |M_1^*|$ to $\mathcal{C}$. $\mathcal{C}$ flips a coin $b \xleftarrow{\$} \{0, 1\}$, computes $C^* := (C_{KEM}^*, C_{DEM}^*) \leftarrow \mathsf{Enc}(pk, M_b^*)$, and sends C^* to $\mathcal{A}$.
- Finally, $\mathcal{A}$ outputs a bit $b' \in \{0, 1\}$.