Content Approval Systems with Expansions of a New Pair-Connected-Structured Aggregate Signature Scheme

Masaki Inamura, Department of Electrical Engineering, Graduate School of Engineering, Tokyo University of Science, Tokyo, Japan
Keiichi Iwamura, Department of Electrical Engineering, Graduate School of Engineering, Tokyo University of Science, Tokyo, Japan

ABSTRACT

In this study, the authors propose new aggregate signature schemes with pairing-based cryptography that can describe the pair-connected structure of signers and examples of new content approval systems with these schemes. Existing structured signature schemes are based on multisignature schemes, which are adapted for verification of a structure if all signers sign the same document. However, if each signer wants to sign a document different from those of other signers, another scheme that is based on an aggregate signature scheme is required. To resolve the above problem, a denoted connective signature is generated in this scheme and can be adapted for verification of variant structures with its expansion. In addition, the authors show examples of effective content approval systems, which can be realize with verifying not only who signs but also which division each of signers belongs to.

Keywords: Aggregate Signature, Digital Signature, Elliptic Curve, Gap Diffie-Hellman, Pairing

INTRODUCTION

Recently, the Internet has become more commonly used, and it has become possible for users to do their work more efficiently. An approval system for a draft proposal in business is one example of such improved efficiency that can be realized. Other example, which is an expression of copyright holders in contents, can also be adapted to one of copyright protection schemes.

For systems that handle work flow, it is important for managers to confirm the approvers of content, e.g., proposers and approvers of a draft proposal or copyright holders of multimedia content file. Digital signature schemes (Diffie & Hellman, 1976), e.g., RSA (Rivest, Shamir, & Adleman, 1978) or DSA (Romine, 2013), are generally used for confirmation of the approvers. However, you can only verify one person per signature file using these signature schemes.

DOI: 10.4018/ije.2013040102
There are usually plural approvers and many files of content, and so you must take a lot of time for confirmation of the approvers if you use these schemes. Therefore, an effective method is required to make those checks.

For this purpose, the multisignature scheme (Itakura & Nakamura, 1983) and derivative schemes (Okamoto, 1988; Harn, 1994) have been proposed as one of the promising mechanisms. Under this scheme, each member signs an objective document, and all members’ signatures are aggregated into one signature called a multisignature. A verifier can then understand all members, who sign this document, by verifying only the multisignature. Therefore, the signing cost is effectively minimized. Furthermore, a structured multisignature scheme (Burmester et al., 2000; Mitomi & Miyaji, 2000) is one of the best mechanisms and describes not only the member who signs the document but also the route that can be taken by the document using only multisignature verification. These multisignature schemes are used when all signers are signing the same document. On the other hand, if every signer signs a document different from those of other signers, e.g., the addition of information data to the distributed document because of alterations made to the document by each relay signer, an aggregate signature scheme is required. However, existing aggregate signature schemes do not extend to structured schemes.

In this study, we propose a structured aggregate signature scheme with a pairing-based cryptography called the BLS signature (Boneh, Lynn, & Shacham, 2001). Our contributions are described as follows:

- We propose an aggregate signature scheme that can express the pair-connected structured of signers.
- We verify that our proposed aggregate signature scheme is provably secure under the Gap Diffie-Hellman (GDH) assumption.
- We also implement a prototype and evaluate its computational performance. Furthermore, we propose examples of content approval systems using our new schemes and show the executable procedure of these examples.

**RELATED WORKS**

**BLS Signature Scheme**

Okamoto and Pointcheval defined a GDH class (Okamoto & Pointcheval, 2001). Consider a multiplicative cyclic group $G'$ with a prime order $p$. They defined two problems for Diffie-Hellman (DH) as follows:

- The computational DH (CDH) problem: For $a, b \in \mathbb{Z}_p^*$ and $g \in G'$, given $(g, g^a, g^b)$, compute $g^{ab}$.
- The decisional DH (DDH) problem: For $a, b, c \in \mathbb{Z}_p^*$ and $g \in G'$, given $(g, g^a, g^b, g^c)$, decide whether $c = ab$ or not.

Regarding the GDH class, it is defined such that the DDH problem is easy, whereas the CDH problem is hard.

The first example involving the use of such groups was given by Joux and Nguyen (Joux & Nguyen, 2001, 2003), and Boneh and Franklin showed that the GDH class can be structured over elliptic curves (Boneh & Franklin, 2001), by using pairing (Washington, 2008).

First, two problems for co-Diffie-Hellman (co-DH) over elliptic curves are defined as follows:

- The computational co-DH (co-CDH) problem: For $a \in \mathbb{Z}_p^*$, $g_1 \in G_1$ and $g_2 \in G_2$, given $(g_1, g_2, ag_1)$, compute $ag_2$.
- The decisional co-DH (co-DDH) problem: For $a, b \in \mathbb{Z}_p^*$, $g_1 \in G_1$ and $g_2 \in G_2$, given $(g_1, g_2, ag_1, bg_2)$, decide whether $a = b$ or not.
Establishing Service Management in SOA

[www.igi-global.com/article/establishing-service-management-soa/63013?camid=4v1a](www.igi-global.com/article/establishing-service-management-soa/63013?camid=4v1a)