Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER Applied Mathematics and Computation 169 (2005) 1324–1331
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

Fail-stop blind signature scheme design based on pairings

Henry Ker-Chang Chang [a,*], Erl-Huei Lu [b], Pin-Chang Su [b]

[a] *Graduate Institute of Business Administration, Chang Gung University, Kwei-San, Tao-Yuan 333, Taiwan, ROC*
[b] *Department of Electrical Engineering, Chang Gung University, Kwei-San, Tao-Yuan, Taiwan, ROC*

Abstract

We propose a robust first-stop blind signature scheme that will work in any Gap Diffie–Hellman (GDH) group. It can be applied in more critical systems like e-voting, e-commerce and e-payment systems that need higher security against sophisticated attacks and can preserve participants' anonymity. Untracebility and unlinkability are the two main properties of real coins for successful electronic mimicking. Whenever a user is permitted to spend an e-coin, he must fulfill the blind signature requirements. Because of the GDH group structure and the base scheme, most of our constructions are simpler, more efficient and have more useful properties than similar existing constructions.

Keywords: First-stop; Blind signature; Gap-Diffie–Hellman; E-voting; E-commerce; E-payment system

* Corresponding author.
E-mail address: changher@mail.cgu.edu.tw (H. Ker-Chang Chang).

0096-3003/$ - see front matter
doi:10.1016/j.amc.2004.10.067

1. Introduction

A signature scheme is a method for signing a message stored in electronic form. As such, a signed message can be transmitted over a computer network. The digital signature is an essential component in cryptography. Depending on the application, digital signatures can provide the required cryptographic properties. Diffie and Hellman [1] introduced the digital signature concept in 1976. Rivest, Shamir and Adleman [2] proposed the first digital signature scheme in 1978. An RSA cryptosystem is based on the problem of factoring large integers and soon became the best known and most widely used digital signature scheme. Another type of digital signature scheme—based on the discrete analogue of the logarithm function—gave rise to a second current of research in computational number theory [3]. This stimulated a tremendous amount of research on the two subjects; factoring and the discrete logarithm problem. The security of a cryptosystem relies on this computational assumption. However, such signatures are only computationally secure for the signer because a forger could forge a signature with unlimited computational power. This means that there is no mechanism to protect a signer against a forged signature that has succeeded in signature verification.

To surmount this kind of bombardment, Waidner and Pfitzmann [4] proposed the first fail-stop signature scheme. A fail-stop signature can protect a signer against a forger even with unlimited computational power because of the possibility of finding the signer's right private key in the fail-stop signature is negligible [5]. The signer can stop the system if a forgery occurs in the fail-stop signature scheme. The signer is unconditionally secure and the recipient is cryptographically secure in the fail-stop signature scheme.

A blind signature scheme [6] allows users to blind the messages being signed and reshape the outside of signatures such that the signer cannot link the signatures and the users. This is a useful building block in applications where anonymity is one of the most significant considerations, such as electronic cash and electronic voting systems. A lot of work has been done in the field of blind signature schemes since Chaum [7–9]. Recently bilinear pairings have been found advantageous in designing various cryptographic schemes, especially for those using public keys, e.g. encryption [10] and signature [11]. Using GDH groups obtained from bilinear pairings, as a special case of our scheme. We designed a new blind signature scheme that requires less computational operations to achieve better performance.

The proposed method can provide "proof of forgery" for signers and guarantee "anonymity" for participants. It can provide more secure and efficient cryptographic primitives for applications in electronic payment systems. The background of our proposed scheme is introduced in Section 2. Section 3 describes a fail-stop blind signature scheme based on bilinear pairings.