Available online at www.sciencedirect.com

ScienceDirect

Information Sciences 177 (2007) 5432–5440

INFORMATION SCIENCES
AN INTERNATIONAL JOURNAL

www.elsevier.com/locate/ins

A provably secure short signature scheme based on discrete logarithms

Zuhua Shao [*]

Department of Computer and Electronic Engineering, Zhejiang University of Science and Technology, No. 318, LiuHe Road, Hangzhou, Zhejiang 310023, PR China

Received 29 July 2005; received in revised form 25 May 2007; accepted 26 May 2007

Abstract

We propose a short signature scheme whose security is closely related to the discrete logarithm assumption in the random oracle model. The new scheme offers a better security guarantee than existing discrete-logarithm-based signature schemes. The main advantage of this scheme over the DSA signature scheme is that it has a one-fourth reduction in both the signature length and the verification computation; the level of security is preserved. The new short signatures are needed to low-bandwidth communication, low-storage and low-computation environments, and particularly applicable to smart cards and wireless devices.

Keywords: Short signature; Discrete logarithm; Random oracle model; Reductionist security proof

1. Introduction

In 1976, Diffie and Hellman invented the concept of the public key cryptography [10]. Since then, several public key cryptosystems, which can provide encryption and/or digital signatures, have been proposed. A digital signature is analogous to an ordinary hand-written signature, and is an evidence of the possession of an electronic document: a user's signature on a message *m* is a string which depends on *m* and on user's public key and private key in such a way that anyone can check validity of the signature by using the public key only.

One of the two most popular signature schemes is the RSA signature scheme [25], the security of which is based on the difficulty of factoring a large composite number. RSA provides relatively long signatures compared with the security it provides. The length of a signature is the same as the length of the modulus used.

[*] Tel.: +86 57185171332; fax: +86 57185121214.
E-mail address: zhshao_98@yahoo.com

doi:10.1016/j.ins.2007.05.039

Another popular signature scheme is the ElGamal type signature scheme [11]; its security is based on the difficulty of solving discrete logarithms. The original ElGamal signature scheme provides much longer signatures. The signature length is twice as long as the length of the modulus used. Schnorr and NIST independently demonstrated modifications to shorten ElGamal type signatures. The signature length of their modifications, called the Schnorr signature [26] and the DSA signature [18], was shortened to 320 bits, and is not related to the length of the modulus used. The signature length of elliptic curve variants of DSA, such as ECDSA, is also 320 bits long [20].

Short digital signatures are important in low-bandwidth communication, low-storage and low-computation environments. Short signatures are needed when printing a signature on a postage stamp, a commerce invoice or a bank bill. Short digital signatures are also needed when a human is asked to key in signatures manually. For instance, product registration systems often ask the users to key in a signature provided on a CD label. Short signatures are particularly applicable to wireless devices such as PDAs, cell phones, RFID chips and sensors, where battery life is the main limitation. Communicating even one bit of data needs to use significantly more power than executing a 32-bit instruction. Reducing the number of bits to communicate saves power and is important to increase battery life. Also, in many settings, communication is not reliable, and so the fewer the number of bits one has to transmit, the better. For such reasons, methods to construct a digital signature scheme yielding a shorter signature length and requiring less computation have attracted much attention.

A number of short signature schemes have been proposed to date. Some schemes tried to shorten the RSA-based signatures. Bellare and Rogaway [2] described a RSA-based signature scheme PSS that essentially combines optimal efficiency with attractive security properties. Granboulan [15] studied methods to generate the shortest possible signatures. He proposed a method named OPSSR that achieves a lower bound for message expansion. However, the signature length of these RSA-based signatures is still related to the length of the modulus used.

Several schemes have shown how to shorten the discrete-logarithm-based signatures while preserving the level of security. Naccache and Stern [17] proposed a variant of the DSA signatures to sign on postcards, where the signature length is approximately 240 bits. The technique they used for reducing the DSA signature length uses message recovery. In such systems, one encodes a part of the message into the signature, thus shortening the total length of the message-signature pair. For long messages, one can achieve a DSA signature length of 160 bits. However, for a very short message (e.g., 64 bits), the total length is still 320 bits. Moreover, when messages are not transmitted, the DSA signatures with message recovery are not any shorter than standard DSA signatures.

Subsequently, digital signature schemes with signature lengths shorter than 160 bits were proposed. Patarin et al. [22] introduced Quartz for standardization in the European Nessie project, achieving signatures of 128 bits with a claimed security level of 2^{80} [8]. The McEliece-based signature scheme CFS gave signatures of about 80 bits [9] but had a substantially bigger public key than Quartz. However, the two signature schemes are forms of the multivariant cryptography, not classical cryptography. Thus they are not efficient in terms of computation and storage.

The shortest signatures known in classical cryptography are based on Weil pairing and achieve signatures of 160 bits with the security level of 2^{80}. Boneh et al. [4] introduced a short signature scheme (BLS) from the Weil pairing-based under the computational Diffie–Hellman assumption on certain elliptic curves and hyperelliptic curves, whose signature lengths were about half the length of the DSA signature with the same level of security. Later, Boneh and Boyen [5] also proposed a new short signature scheme where signatures are almost as short as the BLS signature scheme without random oracles under a strong Diffie–Hellman problem assumption. Zhang et al. [29] improved the BLS scheme by replacing special hash functions with general cryptography hash functions such as SHA-1 [19] or MD5.

Recently, Zhang et al. [31] presented a new short signature scheme without random oracles, which is a variant of the Boneh and Boyen scheme [5]. Zhang et al. [30] proposed a new signature scheme that is existentially unforgeable under chosen-message attacks without random oracles. The security of their scheme depends on a new complexity assumption called the $k+1$ square roots assumption. Victor et al. [27] constructed three new short signature schemes and provided security proofs without random oracles. They are motivated, respectively, by the signatures introduced by Boneh and Boyen [5], Zhang et al. [30], and Camenisch and Lysyanskaya's [6] without random oracles.