Communications
in
Mathematical
Research
25(3)(2009), 265–276

XTR-Kurosawa-Desmedt Scheme*

Ding Xiu-huan, Fu Zhi-guo, and Zhang Shu-gong
(*School of Mathematics, Jilin University, Changchun, 130012*)

Communicated by Zou Yong-kui

Abstract: This paper proposes an XTR version of the Kurosawa-Desmedt scheme. Our scheme is secure against adaptive chosen-ciphertext attack under the XTR version of the Decisional Diffie-Hellman assumption in the standard model. Comparing efficiency between the Kurosawa-Desmedt scheme and the proposed XTR-Kurosawa-Desmedt scheme, we find that the proposed scheme is more efficient than the Kurosawa-Desmedt scheme both in communication and computation without compromising security.

Key words: XTR, Kurosawa-Desmedt scheme, adaptive chosen-ciphertext security, XTR-DDH assumption

2000 MR subject classification: 11T71, 12F05, 94A60

Document code: A

Article ID: 1674-5647(2009)03-0265-12

1 Introduction

XTR stands for "ECSTR", which is an abbreviation for Efficient and Compact Subgroup Trace Representation. It was proposed by Lenstra and Verheul in Crypto 2000 (see [1]). XTR is a novel method that makes use of traces to represent and calculate powers of elements of a subgroup of a finite field.

From a security point of view, XTR is a traditional discrete logarithm system: for its security it relies on the difficulty of solving discrete logarithm related problems in the multiplicative group of a finite field. Thus, XTR is not based on any new primitive or new allegedly hard problem — on the contrary, it is based on the primitive underlying the very first public key cryptosystem, the Diffie-Hellman key agreement protocol. Other advantages of XTR are its very fast parameter and key selection, small key sizes, and speed. Combined with its very easy programmability, this makes XTR an excellent public key system for a very wide variety of environments, ranging from smart cards to web servers, without the need to share system parameters with other users. For actual implementation results and comparisons with other cryptosystems, see [1].

*Received date: Sept. 8, 2008.
Foundation item: Supported partially by the National Grand Fundamental Research 973 Program (2004CB318000) of China.

The notion of the chosen-ciphertext security was introduced by Naor and Yung[2] and developed by Rackoff and Simon[3], and Dolev *et al.*[4]. In an adaptive chosen-ciphertext attack, the adversary is given access to a decryption oracle that allows him to obtain the decryptions of ciphertexts of his choosing. Intuitively, security in this setting means that an adversary obtains no information about encrypted messages, provided the corresponding ciphertexts are never submitted to the decryption oracle. For these reasons, the notion of the adaptive chosen-ciphertext security has emerged as the "right" notion of security for encryption schemes. Indeed it can be shown that in order to model encryption as a "secure envelope", then the encryption scheme used must be adaptive chosen-ciphertext secure.

A number of adaptive chosen-ciphertext secure cryptosystems have been proposed in the literature. Nowadays the most efficient adaptive chosen-ciphertext secure encryption scheme in the standard model is the one due to Kurosawa and Desmedt[5]. The Kurosawa-Desmedt scheme is secure under the Decisional Diffie-Hellman (DDH) assumption. The underlying group G is an Abelian group of order q, where q is a large prime. There are other choices for the group G.

In this paper we make a choice for the group G: a carefully chosen XTR group, namely a subgroup of prime order $q > 3$ of the order $p^2 - p + 1$ subgroup of $\mathrm{GF}(p^6)^*$, where p is a prime and $p \equiv 2 \bmod 3$. Under the XTR version of the DDH (XTR-DDH) assumption, we propose an XTR version of the Kurosawa-Desmedt scheme in the XTR group. Our scheme is secure against adaptive chosen-ciphertext attack under the XTR-DDH assumption in the standard model. Compared to the Kurosawa-Desmedt scheme, the XTR-Kurosawa-Desmedt scheme is more efficient than the Kurosawa-Desmedt scheme both in communication and computation of the same security level.

The organization of this paper is as follows. In Section 2, we first describe the XTR method and some algorithms which will be used in our proposed scheme. Then we describe the XTR-DDH assumption in Section 3. We propose the XTR-Kurosawa-Desmedt scheme, together with the security proof in Sections 4 and 5. Finally we consider the efficiency comparison between the proposed scheme and the Kurosawa-Desmedt scheme in Section 6.

2 XTR

2.1 Description of XTR

Let p be a prime equal to 2 modulo 3. The polynomial $X^2 + X + 1$ is thus irreducible over $\mathrm{GF}(p^2)$ and the roots α and α^p of this polynomial form an optimal normal basis for $\mathrm{GF}(p^2)$ over $\mathrm{GF}(p)$. Moreover, since $p \equiv 2 \bmod 3$, then

$$\alpha^i = \alpha^{i \bmod 3}.$$

It follows that

$$\mathrm{GF}(p^2) \cong \{x_1\alpha + x_2\alpha^2 : \alpha^2 + \alpha + 1 = 0,\ x_1, x_2 \in \mathrm{GF}(p)\}.$$

Each element of $\mathrm{GF}(p^2)$ can thus be represented as a couple (x_1, x_2), where $x_1, x_2 \in \mathrm{GF}(p)$. This representation allows very efficient arithmetic over $\mathrm{GF}(p^2)$ as shown in Lemma 2.2 in