Attack on an Identification Scheme Based on Gap Diffie-Hellman Problem

Zhen-Feng ZHANG Jing XU Deng-Guo FENG

State Key Laboratory of Information Security,
Institute of Software, Chinese Academy of Sciences, Beijing 100080, P.R.China
E-mail: zfzhang@is.iscas.ac.cn

Abstract. In [KK], a new identification scheme based on the Gap Diffie-Hellman problem was proposed at SCIS 2002, and it is shown that the scheme is secure against active attacks under the Gap Diffie-Hellman Intractability Assumption. Paradoxically, this identification scheme is totally breakable under passive attacks. In this paper, we show that any adversary holding only public parameters of the scheme can convince a verifier with probability 1.

Key words. identification scheme, Gap Diffie-Hellman problem, weil-pairing

1 Introduction

There is no doubt that identification schemes has been a very important and useful cryptographic tool. The identification scheme is an interactive protocol where a prover, $\mathcal{P}$, tries to convince a verifier, $\mathcal{V}$, of his identity. Only $\mathcal{P}$ knows the secret value corresponding to his public one, and the secret information allows to convince $\mathcal{V}$ of his identity.

Using the Weil-pairing, Boneh and Franklin [BF] and Boneh et al. [BS] suggested an efficient ID-based encryption scheme and short signature scheme, respectively. Recently, the weil-pairing has been proved to have many cryptographic applications. In [JN], Joux and Nguyen suggested that there exist groups in which the decisional Diffie-Hellman (DDH) problem is easy, although the computational Diffie-Hellman (CDH) problem is hard in a group. The DH problem on such a group is called the GDH problem. Based on such groups, M. Kim and K. Kim [KK] proposed a new identification scheme using weil-pairing, which was claimed to be the first identification scheme based on a Gap-problem published in the open literature, and the scheme was proved to be secure

against active attacks in their paper, if the GDH problem is hard. However, in this paper we show that this scheme is totally insecure even under the passive attack: an adversary can easily succeed in cheating a verifier, what he needed is only the public parameter of the identification scheme.

2 Definitions

2.1 Notions of Security

In general, an identification scheme $(\mathcal{G}, \mathcal{P}, \mathcal{V})$ consists of a probabilistic polynomial-time algorithm $\mathcal{G}$, and two probabilistic polynomial-time interactive algorithms $\mathcal{P}$ and $\mathcal{V}$ with the following properties [FF, Sh]:

1. The algorithm $\mathcal{G}$ is a key generation algorithm. It takes as input a string of the form 1^k, and outputs a pair of string (pk, sk). k is called a security parameter, pk is called a public key, and sk is called a secret key.

2. $\mathcal{P}$ receives as input the pair (pk, sk) and $\mathcal{V}$ receives as input pk. After an interactive execution of $\mathcal{P}$ and $\mathcal{V}$, $\mathcal{V}$ outputs either an 1 (indicating "accept") or a 0 (indicating "reject"). For a given pk and sk, the output of $\mathcal{V}$ at the end of this interaction is a probability space and is denoted by $< \mathcal{P}(pk, sk), \mathcal{V}(pk) >$.

3. A valid prover should always be able to succeed in convincing the verifier. Formally speaking, for all k and for all $(pk, sk) \in [\mathcal{G}(1^k)]$, there holds $< \mathcal{P}(pk, sk), \mathcal{V}(pk) >= 1$ with probability 1.

The weakest form of attack is a *passive attack*, where the adversary is not allowed to interact with the system at all before attempting an impersonation; the only available information to the adversary has is the public key of the prover.

An *active adversary* is a pair of probabilistic polynomial-time interactive algorithms $(\mathcal{A}_1, \mathcal{A}_2)$. For a given key pair (pk, sk), we denote by h the string $< \mathcal{P}(pk, sk), \mathcal{A}_1(pk) >$ output by $\mathcal{A}_1$ after interacting with $\mathcal{P}$ several times. The string h is used as input to $\mathcal{A}_2$ which attempts to convince $\mathcal{V}$. We denote by $< \mathcal{A}_2(h), \mathcal{V}(pk) >$ the output of $\mathcal{V}$ after interacting with $\mathcal{A}_2(h)$.

An identification scheme $(\mathcal{G}, \mathcal{P}, \mathcal{V})$ is secure against active attacks if for all adversaries $(\mathcal{A}_1, \mathcal{A}_2)$, for all constants $c > 0$, and for all sufficiently large k,

$$\Pr\left[\sigma = 1 \middle| (pk, sk) \longleftarrow \mathcal{G}(1^k);\ h \longleftarrow < \mathcal{P}(pk, sk), \mathcal{A}_1(pk) >;\ \sigma \longleftarrow < \mathcal{A}_2(h), \mathcal{V}(pk) > \right] < \frac{1}{k^c}.$$

2.2 The Weil-Pairing

The scheme of [KK] can make use of any bilinear map on an elliptic curve to construct a group G in which the CDH problem is intractable, but the DDH problem is tractable [JN, BF, BSL]. In particular, they make use of the Weil-pairing among bilinear maps.

Let E be a elliptic curve over a base field K, and G_1 and G_2 be two cyclic groups of order q for some large prime p. The Weil pairing is defined by a bilinear map e:

$$e : G_1 \times G_1 \longrightarrow G_2,$$

where G_1 corresponds to the additive group of points of E/K, and G_2 corresponds to the multiplicative group of an extension field $\bar{K}$ of K.

For any $P, Q \in G_1$, the Weil pairing e has the following properties of *Identity, Alternation, Bilinearity, and Non-degeneracy.* Moreover, there exists efficient algorithms to compute $e(P, Q)$ for any $P, Q \in G_1$.

3 Identification Scheme of SCIS02

For security parameter k, a pair of secret and public parameters of the identification scheme is generated as follows.

Key Generation.

On input k, the key generation algorithm $\mathcal{G}$ works as follows:

1. Generates two cyclic groups G_1 and G_2 of order m for some large prime p and a bilinear map $e : G_1 \times G_1 \rightarrow G_2$.

2. Generates an arbitrary generator $P \in G_1$.

3. Chooses randomly $a, b, c \in \mathbf{Z}_m^*$ and computes $v = e(P, P)^{abc}$.

4. The public parameter is $\mathbf{Pub} = \{G_1, G_2, P, aP, bP, cP, e, v\}$, and the corresponding secret parameter is $\mathbf{Sec} = \{a, b, c\}$.

Protocol actions between $\mathcal{P}$ and $\mathcal{V}$.

The identification scheme includes several rounds, each of these is performed as follows:

1. $\mathcal{P}$ chooses $r_1, r_2, r_3 \in \mathbf{Z}_m^*$ at random, then computes $x = e(P, P)^{r_1 r_2 r_3}$, $Q_1 = r_1 P$, $Q_2 = r_2 P$, and $Q_3 = r_3 P$, and sends $< x, Q_1, Q_2, Q_3 >$ to $\mathcal{V}$.

2. $\mathcal{V}$ picks $\omega \in \mathbf{Z}_m^*$ at random, and sends ω to P.

3. $\mathcal{P}$ computes $y = e(\omega P, P)^{abc} e(P, P)^{r_1 r_2 r_3}$ and sends it to $\mathcal{V}$; $\mathcal{V}$ accepts if $y = v^{\omega} x$, and rejects otherwise.

In [KK], it is proved that the above identification scheme is secure against active attacks, under the Gap Diffie-Hellman Intractability Assumption.

4 Attack

Here we show that the above identification scheme is totally breakable under the weakest and simple passive attack: any adversary holding public parameters of the scheme can successfully

convince a verifier.

Let the key generation be as in section 3. Let $\mathcal{A}$ be a passive adversary who holding public key parameter $\mathbf{Pub} = \{G_1, G_2, P, aP, bP, cP, e, v\}$ only. $\mathcal{A}$ can convince a verifier as following:

1. First, $\mathcal{A}$ randomly chooses $r_1, r_2, r_3 \in \mathbf{Z}_m^*$, and computes $x = e(P,P)^{r_1 r_2 r_3}$, $Q_1 = r_1 P$, $Q_2 = r_2 P$, and $Q_3 = r_3 P$, and sends $< x, Q_1, Q_2, Q_3 >$ to $\mathcal{V}$.

2. Then $\mathcal{V}$ will pick $\omega \in \mathbf{Z}_m^*$ at random, and send ω to $\mathcal{A}$.

3. Note that the public parameter v is publicly available, the adversary $\mathcal{A}$ simply computes $y = v^{\omega} x$ and sends it to $\mathcal{V}$.

Then it is easy to see that the verifier $\mathcal{V}$ then will surely accept with probability 1 .

It is easy to see that the above attack is totally a passive attack. This attack also works for the generalized identification scheme described in [KK]. In fact, the failure of this identification scheme lies in that it does not bind a prover with his private key, hence an adversary can easily cheat a verifier, even without interaction with honest prover holding private keys.

References

[BF] D. Boneh and M. Franklin, "ID-based encryption from the Weil-pairing", Advances in Cryptology-Crypto2001, LNCS 2139, Springer-Verlag, pp. 213-229, 2001.

[BS] D. Boneh, H. Shacham, and B. Lynn, "Short signatures from the Weil-pairing", Advances in Cryptology-Asiacrypt2001, LNCS 2248, Springer-Verlag, pp.514-532, 2001.

[FF] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity", J. Cryptology, 1: 77-94, 1988.

[JN] A. Joux and K. Nguyen, "Seperating decision Diffie-Hellman from Diffie-Hellman in cryptographic groups", J. Cryptology Online First, available from http://eprint.iacr.org/2001/003.

[KK] Myungsun Kim and Kwangjo Kim, A., "A New Identification Scheme based on the Gap Diffie-Hellman Problem", The 2002 Symposium on Cryptography and Information Security Shirahama, Japan, Jan. 29-Feb.1, 2002

[Sh] V. Shoup, "On the security of a practical identification scheme", J. Cryptology 12: 247-260, 1999.