Security Bounds for Parallel Versions of Identification Protocols

(Extended Abstract)

Lidong Chen, Ivan Damgård
Department of Mathematics
Aarhus University
Denmark

Abstract The security bounds we will define and discuss in this paper is an universal security measure for parallel versions of identification protocols. From this bound we can judge which of the security measures defined in [FFS],[FeS],[OO] are satisfied. The bounds are controllable in the sense that they are connected with a security parameter. When the bound is a "sharp-threshold" security bound, it is tight enough to describe the security of the protocol precisely. Using this bound, we discuss the generalized Fiat-Shamir identification scheme ID(L,k,t,n) which is defined in [CDL]. Under the assumption that there is no polynomial time algorithm of factoring, the parallel version of the scheme is secure in the sense that even cheating verifier B can get some information from the interacting with the prover, the information he get is absolutely useless for cheating.

1. Introduction

The zero-knowledge property is a perfect measure for the security of identification scheme. But in most cases, especially for parallel versions, we can not establish this property. Therefore many researchers have been trying to define other security measures to explore its security([FFS],[FeS],[OO]). The security bound we will give is a more universal one. From this bound we can judge that which of the security measures defined before is satisfied.

Because most discussions are developed for the generalized Fiat-Shamir identification scheme with four parameters ID(L,k,t,n) defined in [CDL], we first introduce it here.

The scheme assumes the existence of a trusted center as in Fiat-Shamir scheme. The center chooses and makes public a modulus n, where $n=pq$, p and q are odd primes, and a pseudorandom function f. The center produces $v_j = f(I, j)$, $j=1,2,\ldots,k$ for user U_I, such that for every v_j there exists s_j satisfying $s_j^L \cdot v_j \equiv 1 \bmod n$. $J=(v_1, v_2, \ldots, v_k)$ is public key. $S=(s_1, s_2, \ldots, s_k)$ is secret key. In the identification scheme, A want to prove to B that he is valid A, because he knows secret key S. The basic protocol is as follows:

1. A picks a random $r \in Z_n$, and sends

R.A. Rueppel (Ed.): Advances in Cryptology - EUROCRYPT '92, LNCS 658, pp. 461-466, 1993.

$$x \equiv r^L \bmod n$$

to B;

2. B sends a random vector $\mathbf{d}=(e_1, e_2, \ldots, e_k)$, $0 \le e_j \le L-1$, $j=1,2,\ldots,k$, to A;

3. A sends to B

$$y \equiv r \cdot \prod_{j=1}^{k} s_j^{e_j} \mod n;$$

4. B checks that if

$$x \equiv y^L \cdot \prod_{j=1}^{k} v_j^{e_j} \mod n.$$

Repeat the basic protocol t times. This 4 parameter identification scheme is called the ID(L,k,t,n) identification scheme.

Among all the security measures for identification schemes, what we are most interested in is the concept of security level defined in [OO]. Here after, we use $\bar{A}$, $\bar{B}$ to represent honest prover and verifier, and $\tilde{A}$, $\tilde{B}$, cheating prover and verifier, separately. A protocol (A,B) is said to release no transferable information with security level ρ, if after a polynomial number of executions of $(\bar{A}, \tilde{B})$, the probability of $(\tilde{A}, \bar{B})$ success is not larger than ρ.

First, ρ is a bound for security of the parallel version of identification protocol. Generally in a protocol, we take $|n|$ as security parameter. The larger $|n|$ is, the smaller the probability of an impersonation event is.

Second, ρ is a measure of the amount of information leaking during executing($\bar{A}, \tilde{B}$) in parallel, which is meaningful only when we compare it with the probability of one cheating prover's success. Generally, what a coalition can do is better than one cheating prover $\tilde{A}$ can do, because for a coalition, $\tilde{A}$ may use the information which was extracted by $\tilde{B}$ from executing $(\bar{A}, \tilde{B})$ polynomial number of times. But for one cheating prover, what he can do is just guessing the verifier's query in advance. Of course, we can consider $\tilde{A}$ and $\tilde{B}$ to be one person but play different roles at different protocols. The question is how much it is better. From the security point of view, it should not be "much" better, if we require that the protocol release no transferable information. The

extreme situation is another concept given by Ohta and Okamoto " the protocol (A,B) releases *no* transferable information with a strict sharp-threshold security level ρ " which means that what a coalition can do is "not" better than one cheating prover can. This concept may have some significance. But it is hard to find a general identification protocol ID(L,k,t,n) satisfying this condition. So we would like to give a more general concept and discuss it.

Now we give the definition of security bound.

Definition 1.1 The protocol $(\bar{A}, \bar{B})$ releases no transferable information with a security bound $\rho(|n|)$ if

1. It succeeds with probability 1;

2. For any coalition of polynomial time machines $\tilde{A}$, $\tilde{B}$,after a polynomial number of executions of $(\bar{A}, \tilde{B})$, the probability of $(\tilde{A}, \bar{B})$ success is not larger than or equal to $\rho(|n|)$.

The protocol $(\bar{A}, \bar{B})$ releases no transferable information with a sharp-threshold security bound $\rho(|n|)$ if it satisfies condition 1 and 2 above as well as the following condition:

3. If the probability of $\tilde{A}$ cheating $\bar{B}$ is $\rho_0(|n|)$, then

$$\lim_{n\to\infty} \frac{\rho(|n|)}{\rho_0(|n|)} - 1 = 0 .$$

2. Protocols with Controlable Security Bound

For protocol ID(L,k,t,n), we can prove that even the parallel versions of it can not be proved to be zero-knowledge protocol, if some information is leaked during the execution of it, the information the cheating verifier can get is useless for successfully cheating. More precisely, the information leaked during the execution can not make the probability of success increase nonnegligibly.

Theorem 2.1 Let $p' = (L,p-1) \geq q' = (L,q-1)$, $p'q' > 1$, $k = O(\log |n|)$. Then if one of the conditions C1, C2, (C3) is satisfied,the parallel version of ID(L,k,1,n) releases no transferable information with security bound

$$\frac{1}{(p')^k} + \frac{1}{|n|^c} \qquad \left(\frac{1}{(q')^k} + \frac{1}{|n|^c} \right)$$

for any positive constant c, if there is no probabilistic polynomial time algorithm of factoring n.

C1. $p' = \prod_{i=1}^{N} p_i$, where p_i is a prime, $p_i \neq p_j$ $(i \neq j)$, and $N \geq 1$.

C2. $(p', q') = 1$.

C3. $q' = \prod_{i=1}^{M} q_i$, where q_i is a prime, $q_i \neq q_j$ $(i \neq j)$, and $M \geq 1$.

Definition 1.1 can also be used to describe other protocols than those of Fiat-Shamir type. For example, we can use this definition to discuss the modified Schnorr scheme[BM] which can be proved releasing no transferable information with security bound $2^{-t} + |n|^{-c}$ for any constant c if there is no polynomial time algorithm of computing discrete logarithm. Here, t is the number of bits in the verifier's challenge.

As a security bound, $\rho(|n|)$ could be very loose so that no protocol can really be close to it. **Theorem 2.2** will point out which kind of the bounds are tight enough to describe the security of the protocols.

Theorem 2.2 The protocol ID(L,k,1,n) releases no transferable information with sharp-threshold security bound

$$\frac{1}{(p')^k} + \frac{1}{|n|^c} \qquad \left(\frac{1}{(q')^k} + \frac{1}{|n|^c} \right)$$

for any constant c satisfying

$$\lim_{|n| \to \infty} \frac{(p')^k}{|n|^c} = 0 \qquad \left(\lim_{|n| \to \infty} \frac{(q')^k}{|n|^c} = 0 \right) \qquad (1),$$

if there is no polynomial time algorithm of factoring n.

3. Connections to Other Definitions of Security

In this section , we would like to explore the relationship between security bounds and other security measures defined in [FFS], [FeS] and [OO]. From the following three theorems, it is reasonable to claim that the security bounds we have given are more universal compared with other security measures.

Theorem 3.1 If for any positive constant c, (A,B) releases no transferable information

with security bound

$$\rho(|n|) = \frac{1}{|n|^c},$$

then (A,B) is secure according to the definition given by Feige, Fiat and Shamir[FFS].

Theorem 3.2 If protocol (A,B) is a proof of knowledge, and satisfy the condition given in **Theorem 3.1**, then (A,B) is witness hiding according to the definition given by Feige and Shamir[FeS].

Theorem 3.3 If ρ is a constant, such that for any positive constant d, protocol (A,B) releases no transferable information with security bound

$$\rho(|n|) = \rho + \rho \cdot \frac{1}{|n|^d},$$

then it releases no transferable information with strict security level ρ according to the definition given by Ohta and Okamoto[OO].

4. Discussion

For convenience, we give a representation of the probability we will discuss here. Let

$$\rho_0 = \text{Prob}\{\ \tilde{A}\ \text{cheats}\ \bar{B}\ \}.$$

And let

$$\rho_{\tilde{A}\bar{B}} = \text{Prob}\{(\tilde{A}, \bar{B}) \text{ succeeds} \mid \text{after executing } (\bar{A}, \tilde{B}) \text{ polynomial number of times}\}$$

Obviously, if (A,B) is a zero knowledge protocol, $\rho_0 = \rho_{\tilde{A}\bar{B}}$ for any $\tilde{A}$ and $\tilde{B}$. But in most cases $\rho_0 < \rho_{\tilde{A}\bar{B}}$. The security bound $\rho(|n|)$ is a upper bound for $\rho_{\tilde{A}\bar{B}}$, i.e.which describes the amount of usable information leaking during excuting (A,B).

For protocol ID(L,k,1,n), under the assumption that there is no polynomial time algorithm of factoring n, for any $\tilde{A}, \tilde{B}$, $\rho_{\tilde{A}\bar{B}} - \rho_0 < \frac{1}{|n|^c}$ for any constant c, i.e. the increasing of probability gained by borrowing the information from executing $(\bar{A}, \tilde{B})$ is negligible.

Acknowledgements We would like to thank Peter Landrock for reading the manuscript and valuable comments.

References

[BM] E.F.Brickell, K.S.McCurley "An Interactive Identification Scheme Based on Discrete Logarithms and Factoring" The oringinal one is from Proc. of EUROCRYPT'90 pp 63-71. Here we refer to a new version of it.

[CDL] L.Chen, I.Damgård, P.Landrock "Extension and Analysis of Fiat-Shamir Identification Scheme" to appear.

[FFS] U.Feige, A.Fiat and A.Shamir "Zero-Knowledge Proofs of Identity" Journal Cryptology 1(2), 1988

[FeS] U.feige, A. Shamir " Witness Indistinguishable and Witness Hiding Protocols" Proc. of the 22nd ACM Symposium on Theory of Computing pp416-424

[OO] K.Ohta and T.Okamoto "A Modification of the Fiat Shamir Scheme" Proc. of CRYPTO'88 pp 232-243.