An Efficient Anonymous Group Identification Scheme with Short Secret Keys

Toshiyuki Isshiki
Keisuke Tanaka*
Department of Mathematical and Computing Sciences,
Tokyo Institute of Technology,
2-12-1 Ookayama Meguro-ku, Tokyo 152-8552, Japan

summary

We suggest to use short secret keys in the anonymous group identification scheme proposed by Lee, Deng, and Zhu [7] and prove that this scheme is secure under the discrete logarithm with short exponents assumption that solving the discrete logarithm problem modulo an n-bit prime p is hard even when the exponent is a small c-bit number. We show that the communication and the computation costs are lower than those of the Lee-Deng-Zhu scheme.

keywords

group identification, anonymous group identification, protocol, discrete logarithm

1 Introduction

Anonymous group identification scheme is a method that allows a member of group, say Alice convinces a verifier, say Bob that she is a member of the group without revealing any information about her identity in the group. A full and general solution to the problem of anonymous group identification has been presented by De Santis, Di Cresenzo, Persiano, and Yung [3] based on the closure properties of statistical zero-knowledge languages under monotone logic formula composition. Since the anonymity property often constrains the communication to heavily depend on the number of users in the group, communication cost is one of the most important measures for efficiency considerations. Motivated by the communication efficiency consideration, De Santis, Di Crescenzo, and Persiano [4] have developed elegant protocols minimizing the communication involved in the scheme (SCP scheme). The SCP scheme is based on the difficulty of factoring problem. Later, Cramer, Damgard, and Schoenmakers suggest a new general approach for proofs of partial knowledge independently [2]. Recently, Lee, Deng, and Zhu provided a 3-move anonymous group identification scheme (LDZ scheme) which is more efficient than the SCP scheme (with simple modification).

Incidentally, in [8], Patel and Sundaram constructed a pseudorandom generator based on the Blum-Micali generator. Their scheme is based on the assumption that solving the discrete logarithm problem modulo an n-bit prime p is hard even when the exponent is a small c-bit, where $c = \omega(\log n)$. This is called the *Discrete Logarithm with Short c-Bit Exponents* (c-DLSE) Assumption. Later, their construction was improved by Gennaro [5]. The DLSE assumption is also employed by Koshiba and Kurosawa [6].

*Supported in part by Grant-in-Aid for Scientific Research, Ministry of Education, Culture, Sports, Science, and Technology, 14780190

In this paper we suggest to use short secret keys in the LDZ scheme. We modify the LDZ scheme such that short secret keys are fit into it, and prove that this modified scheme is secure under the DLSE assumption while the original LDZ scheme is secure under the DL assumption that solving the discrete logarithm problem modulo an n-bit prime p is hard when the exponent is a n-bit number. We show that the communication and the computation costs are lower than the original scheme [7].

2 Preliminaries

2.1 Anonymous Group Identification Protocols

We briefly review the security definition on anonymous group identification protocols, introduced by De Santis, Di Crescenzo, and Persiano [4]. An anonymous identification scheme consists of two phases: the initial phase and the identification phase. Each user holds with a pair of the public key and the private key at the end of execution of the initial protocol. In the identification phase, a user tries to convince the verifier of some statement which certifies her knowledge of the secret key received in the initial phase. By INIT, we denote an initial protocol, and by (P, V), we denote a two-party protocol, where P is a proof algorithm executed by the prover and V is a verification algorithm executed by the verifier.

Definition 1 (De Santis, Di Crescenzo, and Persiano [4]) *We define the security of an anonymous group identification scheme in the case that each user in the group shares common system public keys and the probability that one round execution of the protocol rejects an unqualified user is negligible. An anonymous identification scheme $\{INIT, (P, V)\}$ is secure if it satisfies:*

- *Correctness: For each user $U_i \in S$, $\Pr[(pk_1, \cdots, pk_m, sk) \leftarrow INIT(1^n) : (P(sk), V)(pk_1, \cdots, pk_m) = accept] = 1$;*
- *Soundness: For any user $U_i \notin S$ and any probabilistic polynomial-time algorithm P' which is an eavesdropping prover, the advantage of P': $\Pr[(pk_1, \cdots, pk_m) \leftarrow INIT(1^n) : (P'(\phi), V)(pk_1 \cdots, pk_m) = accept]$ is negligible, where ϕ indicates an empty string;*
- *Anonymity: For any user $U_i, U_j \in S$ and any probabilistic polynomial-time algorithm V', the probability space Π_1 and Π_2 are equal, where $\Pi_1 = [(pk_1, \ldots, pk_m, sk_i) \leftarrow INIT(1^n); t \leftarrow VIEW(P(sk_i), V')(pk_1, \cdots, pk_m) : t]$ and $\Pi_2 = [(pk_1, \ldots, pk_m, sk_j) \leftarrow INIT(1^n); t \leftarrow VIEW(P(sk_j), V')(pk_1, \cdots, pk_m) : t]$, where $t \leftarrow VIEW(A(y), B)(x)$ denotes that the transcript t has been generated through an execution of the protocol (A, B) with common input x and A's private input y.*

In the original definition on soundness in [4], the advantage of P': $|\Pr[(pk_1, \cdots, pk_m) \leftarrow \mathrm{INIT}(1^n) : (\mathrm{P}'(\phi), \mathrm{V})(pk_1, \cdots, pk_m) = accept]| = \frac{1}{2} - \epsilon$, where ϵ is negligible. However, their protocol actually satisfies the stronger definition described above without iteration. Thus, we require our method without iteration to satisfy this definition.

2.2 The Discrete Logarithm with Short Exponents Assumption

Let p be a prime. We denote by n the binary length of p. Then, $Z_p^* = \{x : 1 \leq x \leq p-1\}$ is a cyclic group under multiplication mod p. Let g be a generator of Z_p^*. Thus the function

$$\begin{gathered} f : Z_{p-1} \rightarrow Z_p^* \\ f(x) = g^x \bmod p \end{gathered}$$

is a permutation. The inverse of f (called the *discrete logarithm* function) is conjectured to be a function hard to compute. The best known algorithm to compute discrete logarithms is the so-called *index calculus* method [1] which however runs in time sub-exponential in n.

In some applications it is important to speed up the computation of the function $f(x) = g^x \bmod p$. One possible way to do this is to restrict its input to small values of x. Let c be an integer which we can think as depending on n ($c = c(n)$) . Assume now that we are given $y = g^x \bmod p$ with $x \leq 2^c$. It appears to be reasonable to assume that computing the discrete logarithm of y is still hard even if we know that $x \leq 2^c$. Indeed the running time of the index-calculus method depends only on the size n of the whole group. Depending on the size of c, different methods may actually be more efficient.

In the paper by Patel and Sundaram [8], it is explicitly conjectured that no such efficient algorithm that can compute the discrete log of $y = g^x \bmod p$ when $x \leq 2^c$, $c = \omega(\log n)$. This is called the *Discrete Logarithm with Short c-Bit Exponents* (c-DLSE) Assumption.

Assumption 2 (Patel and Sundaram [8])
Let PRIMES(n) be the set of n-bit primes and let $c = \omega(\log n)$. For every probabilistic polynomial-time Turing machine $\mathcal{I}$, for every polynomial $P(\cdot)$ and for sufficiently large n we have that

$$\Pr\left[\begin{array}{c} p \leftarrow PRIMES(n); \\ x \leftarrow R_c; \\ \mathcal{I}(p, g, g^x, c) = x \end{array}\right] \leq \frac{1}{P(n)}.$$

This assumption is somewhat supported by a result by Schnorr [9] who proves that no generic algorithm can compute c-bits discrete logarithms in less than $2^{\frac{c}{2}}$ generic steps. A generic algorithm is restricted to only perform group operations and cannot take advantage of specific properties of the encoding of group elements.

3 The LDZ Scheme with Short Secret Keys

In this section, we present a modification of the LDZ efficient anonymous group identification scheme, in order to use short secret keys with length $c = \omega(\log n)$ instead of n.

Let n be a security parameter, $c = \omega(\log n)$, and p, q be two large primes such that $p - 1 = 2q$. Let G be a cyclic sub-group of Z_p^* with order q, and g be a generator of G. The system public key is (p, q, g) available to all group users. Let m be the number of members of the group. For $i = 1, \cdots, m$, each user U_i in the group chooses $x_i \in \{0, 1\}^c$ at random and computes $y_i := g^{x_i} \bmod p$. The public key is y_i and the secret key is x_i. The set $S := \{y_i, \cdots, y_m\}$ contains the information of all legal users.

To show the membership of the group anonymously (without loss of generality, we assume that the prover knows the secret information of y_1), one round of protocol is performed as follows.

Step 1 : The prover chooses $s \in Z_q$, $c_1, \cdots, c_m \in \{0, 1\}^c$ uniformly at random, then sends $u = g^s y_1^{c_1} \cdots y_m^{c_m} \bmod p$ to the verifier.

Step 2 : The verifier chooses $b \in \{0, 1\}^c$ uniformly at random and sends to the prover.

Step 3 : The prover sets d and r by the following way:

- If $b = c_1 \oplus \cdots \oplus c_m$, the prover sets

$$\begin{array}{rcl} d_j &=& c_j \ (j = 1, \ldots, m) \\ r &=& s. \end{array}$$

- If $b \neq c_1 \oplus \cdots \oplus c_m$, the prover sets

$$\begin{array}{rcl} d_j &=& c_j \ (j = 2, \ldots, m) \\ d_1 &=& b \oplus c_2 \oplus \cdots \oplus c_m \\ r &=& s + x_1(c_1 - d_1) \bmod q. \end{array}$$

and sends $(r, d_1, \ldots, d_m)$ to the verifier, where $a \oplus b$ denotes the bit-wise exclusive-or of a and b.

Step 4 : The verifier checks whether $b = d_1 \oplus \cdots \oplus d_m$ and $u = g^r y_1^{d_1} \cdots y_m^{d_m} \mod p$. If the both conditions hold, the verifier outputs *Accept*, else it outputs *Reject*.

4 Analysis

4.1 Security

Before going to correctness, soundness, and anonymity, we consider a direct attack against the secret key x_i using the public key y_i. Since $y_i = g^{x_i} \mod p$, finding x_i from y_i is hard from the c-DLSE assumption.

- Correctness: Correctness can be easily verified according to the definition.
- Soundness: Suppose there exists an unqualified user $U' \notin S$ and a probabilistic polynomial-time proof algorithm P' with non-negligible advantage to make the honest verifier accept, then there exists a polynomial-time algorithm P^* which solves the discrete logarithm with short exponents with non-negligible probability.

  Proof. We show an algorithm that takes (g, y) as input and produces the $\mathrm{DLSE}_g(y)$ as output (given access to a subroutine that breaks the protocol). Now P^* chooses randomly $i \in \{1, \cdots, m\}, r_1, \cdots, r_{i-1}, r_{i+1}, \cdots, r_m \in \{0,1\}^c$ and sets $y_i = y$ and $y_j = g^{r_j}$ $(j \neq i)$. By assumption, it follows P' is able to output $\{(u; r; (c_1, \cdots, c_m)), (u; r'; (c'_1, \cdot$ $P'(g, y_1, \cdots, y_m)$ with non-negligible probability such that $c_1 \oplus \cdots \oplus c_m \neq c'_1 \oplus \cdots \oplus c'_m$ and $u := g^r y_1^{c_1} \cdots y_m^{c_m} = g^{r'} y_1^{c'_1} \cdots y_m^{c'_m}$. Denote $d_i = c'_i - c_i$ $(1 \leq i \leq m)$. Hence with non-negligible probability, the adversary obtains the equation: $g^{r-r'} = y_1^{d_1} \cdots y_m^{d_m}$. It follows that $\mathrm{DLSE}_g(y) \cdot d_i = r - r' - (r_1 d_1 + \cdots + r_{i-1} d_{i-1} + r_{i+1} d_{i+1} + \cdots + r_m d_m) \mod q$. Hence the adversary is able to compute the discrete logarithm of any randomly given element y with non-negligible probability. This contradicts the hardness assumption of the discrete logarithm with short exponents.
- Anonymity: The distribution of the variable $r \leftarrow (r + (c_i - d_i)x_i) \mod q$ over Z_q (of the user U_i) and the distribution of the variable $r' \leftarrow (r' + (c_j - d_j)x_j) \mod q$ over Z_q (of the user U_j) are uniformly distributed if r and r' are chosen at random from Z_q. ∎

4.2 Efficiency

Our scheme needs essentially m exponentiations modulo an n-bit prime p with c-bit exponent and one exponentiation modulo p with n-bit exponent for both the prover and the verifier, while the original LDZ scheme needs $(m + 1)$ exponentiation modulo p with n-bit exponent. In order to compare these costs, if we use the square and multiply algorithm for modular exponentiations (on average $1.5l$ modular multiplications are required for an l-bit exponent), our method requires about $1.5n + (1.5c + 1)m = O(n + cm)$ modular multiplications modulo p, while the LDZ scheme needs $1.5n(m + 1) + m = O(nm)$ modular multiplications modulo p. For example, if we set $c = (\log n)^2$, then our method is more efficient than the LDZ scheme. In particular, if we set $n = 1024$ and $c = (\log n)^2 = 100$, then the length of each secret key in our method is 100 bits, while that in the original LDZ scheme is 1024 bits.

The total communication cost of our scheme is $2n + (2m + 1)c$-bit, while that of the LDZ scheme is $(2m + 3)n$-bit. Furthermore the length of random tape for a prover in our scheme is $(n + mc)$-bit, while that of the LDZ scheme is $(m + 1)n$-bit.

5 Concluding Remarks

In this paper, we suggest to use short secret keys in the anonymous group identification scheme proposed by Lee, Deng, and Zhu and prove that this scheme is secure under the discrete logarithm with the DLSE assumption. Then we show that the communication and the computation costs are lower than those of the LDZ scheme. It might be interesting to find other protocols that can use the DLSE assumption.

References

[1] Adleman, L. A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In *IEEE FOCS* (1979), pp. 55–60.

[2] Cramer, R., Damgård, I. B., and Schoenmakers, B. Proof of partial knowledge and simplified design of witness hiding protocols. In *CRYPTO '94, Lecture Notes in Computer Science* (1994), vol. 839, pp. 174–187.

[3] De Santis, A., Di Crescenzo, G., Persiano, G., and Yung, M. On monotone formula closure of SZK. In *IEEE Symposium on Foundations of Computer Science* (1994), pp. 454–465.

[4] De Santis, A., Di Cresenzo, G., and Prisiano, G. Communication-eficient anonymous group identification. In *5th A.C.M. Conference on Computer and Communications Security(ACM CCS'98)* (1998), pp. 73–82.

[5] Gennaro, R. An improved pseudo-random generator based on discrete log. *CRYPTO 2000, Lecture Notes in Computer Science 1880* (2000), 469–481.

[6] Koshiba, T., and Kurosawa, K. Short exponent DDH. In *LA Symposium* (February 2003), pp. [25]–1–6.

[7] Lee, C. H., Deng, X., and Zhu, H. Design and security analysis of anonymous group identification protocols. In *Public Key Cryptography* (2002), vol. 2274 of *Lecture Notes in Computer Science*, Springer, pp. 188–198.

[8] Patel, S., and Sundaram, G. An efficient discrete log pseudo random generator. In *CRYPTO '98, Lecture Notes in Computer Science* (1998), vol. 1462, pp. 304–317.

[9] Schnorr, C. P. Security of almost ALL discrete log bits. In *ECCCTR: Electronic Colloquium on Computational Complexity, technical reports* (1998).