A Modification of the Fiat-Shamir Scheme

Kazuo Ohta *Tatsuaki Okamoto*

NTT Communications and Information Processing Laboratories
Nippon Telegraph and Telephone Corporation
1-2356, Take, Yokosuka-shi, Kanagawa-ken, 238-03, Japan

Abstract: Fiat-Shamir's identification and signature scheme is efficient as well as provably secure, but it has a problem in that the transmitted information size and memory size cannot simultaneously be small. This paper proposes an identification and signature scheme which overcomes this problem. Our scheme is based on the difficulty of extracting the L-th roots mod n (e.g., $L = 2 \sim 10^{20}$) when the factors of n are unknown. We define some variations of no transferable information and prove that the sequential version of our scheme is a zero knowledge interactive proof system and our parallel version satisfies these variations of no transferable information under some conditions. The speed of our scheme's typical implementation is at least one order of magnitude faster than that of the RSA scheme and is relatively slow in comparison with that of the Fiat-Shamir scheme.

1. Introduction

Fiat and Shamir have proposed an identification and signature scheme which is promising because it is efficient and provably secure against any active attack [FS]. Their scheme is based on the difficulty of extracting square roots mod n when the factors of n are unknown. The Fiat-Shamir scheme consists of sequential and parallel versions. Though their sequential version is a zero knowledge interactive proof system [FFS], the iteration number must be $O(\log_2 n)$ and the communication performance is therefore low. The parallel version is more efficient than the sequential version, and it is secure because it reveals no transferable information [FFS]. There is, however, a trade-off between the transmitted information size and memory size. That is, the probability of forgery is $1/2^{kt}$, where k denotes the number of secret information integers and the overall transmitted information size is proportional to t. For example, in order to attain the security level 2^{-20}, i.e., $tk = 20$, when we reduce the information size to $t = 1$, we must store twenty ($k = 20$) secret integers. When we store only one secret integer, $k = 1$, we must send twenty ($t = 20$) times as long a message. Therefore, the efficient parameter values, $t = k = 1$, cannot be used in their scheme.

In this paper, we propose an identification and signature scheme which over-

S. Goldwasser (Ed.): Advances in Cryptology - CRYPTO '88, LNCS 403, pp. 232-243, 1990.

comes the above mentioned problem. Our scheme is based on the difficulty of extracting the L-th roots mod n when factors of n are unknown. In our scheme, the third design parameter L is introduced in addition to the two parameters t and k which correspond to t and k of the Fiat-Shamir scheme. Here, the security level is represented as $L^{-t \cdot k}$. Therefore, the parameter values $t = k = 1$ are applicable in our scheme if the appropriate value for L is chosen, although our scheme is relatively slow in comparison with the Fiat-Shamir scheme. Hence our scheme is suitable for smart cards, because their memory amounts are restricted.

We define new security level notions of "transferable information *with a (strict) security level* ρ " and "transferable information *with a (strict) sharp-threshold security level* ρ ." We then prove that the sequential version of our scheme is a perfect zero knowledge interactive proof system for any L. We go on to prove that our parallel version reveals no transferable information with a strict security level $1/p'$, where p and q are factors of n, $p' = (L, p-1) > 1$, $p' \geq q' = (L, q-1)$, if the factoring is difficult and an additional condition holds, where (a, b) denotes the greatest common divisor of a and b. Finally we also prove that our parallel version releases no transferable information with a strict sharp-threshold security level $1/L$ when $(L, p-1) = L$ and an additional condition holds.

Although the idea of using higher roots was implied in [FS], [GQ1] and [GQ2], its security and parameter conditions were not formally discussed.

In the following sections, we consider a typical case where $k = 1$ for the sequential version and $k = t = 1$ for the parallel version. Our results are easily extended to cases where k and t have other values.

2. Some Number-Theoretic Results

First some number-theoretic results are shown concerning the modular L-th roots.

[Lemma 1] Let p be an odd prime, L be an integer ($L \geq 2$) and $p' = (L, p-1)$. If y is the L-th residue mod p, then there are p' integers x of the L-th root mod p of y such that $x^L \equiv y \pmod{p}$.

Proof Let g be a primitive element over a finite field $GF(p)$, let α satisfy $g^\alpha \equiv x \pmod{p}$ and let β satisfy $g^\beta \equiv y \pmod{p}$. Then $x^L \equiv y \pmod{p}$ implies $(g^\alpha)^L \equiv g^\beta \pmod{p}$. Here α satisfies $\alpha L \equiv \beta \pmod{p-1}$; therefore, it has p' solutions [HW, pp.51-52]. *Q.E.D.*

[Lemma 2] Let p be an odd prime, L be an integer ($L \geq 2$) , y be the L-th residue mod p and $p' = (L, p-1) \geq 2$. If $\{x_1, \ldots, x_{p'}\}$ is the set of the L-th roots mod p of y, then any pair (x_i, x_j) satisfies $x_i^{p'} \equiv x_j^{p'} \pmod{p}$ $(1 \leq i, j \leq p')$ and there is at least one pair (x_i, x_j) such that $i \neq j$ and $x_i^{p'-1} \not\equiv x_j^{p'-1} \pmod p$.

Proof Let g be a primitive element over $GF(p)$ and let α_i satisfy $g^{\alpha_i} \equiv x_i \pmod p$ $(1 \leq i \leq p')$. Since a congruence $x_i^L \equiv x_j^L \equiv y \pmod p$ implies $L(\alpha_i - \alpha_j) \equiv 0 \pmod{p-1}$, $p-1$ is a divisor of $L(\alpha_i - \alpha_j)$. Here p' is the greatest common divisor of L and $p-1$. Thus, $p-1$ is a divisor of $p'(\alpha_i - \alpha_j)$. Therefore, the congruence $p'\alpha_i \equiv p'\alpha_j \pmod{p-1}$ holds, and we finally obtain $x_i^{p'} \equiv (g^{\alpha_i})^{p'} \equiv (g^{\alpha_j})^{p'} \equiv x_j^{p'} \pmod p$ $(1 \leq i, j \leq p')$.

Assume that any x_i satisfies $x_i^{p'-1} \equiv z \pmod p$ $(1 \leq i \leq p')$. Thus, there are p' integers of the $(p'-1)$-th roots mod p of z. Here, the number of the $(p'-1)$-th roots mod p of z is at most $p'-1$ according to Lemma 1 because $(p'-1, p-1) \leq p'-1$. This is a contradiction. Therefore, there is at least one pair (x_i, x_j) such that $i \neq j$ and $x_i^{p'-1} \not\equiv x_j^{p'-1} \pmod p$. *Q.E.D.*

We classify the L-th roots mod n of 1 in order to calculate the probability of successfully factoring n.

[Definition 1] Let L be an integer $(L \geq 2)$ and n be a composite number which is the product of two odd primes p and q. Four types of the L-th roots mod n of 1 are defined as follows:

$$\begin{aligned} &\omega \text{ is } \mathit{Type1} \text{ if } \omega = [1, 1], \\ &\omega \text{ is } \mathit{Type2} \text{ if } \omega = [1, \omega_q], \\ &\omega \text{ is } \mathit{Type3} \text{ if } \omega = [\omega_p, 1], \\ &\omega \text{ is } \mathit{Type4} \text{ if } \omega = [\omega_p, \omega_q], \end{aligned}$$

where the notation $\omega = [a, b]$ means that ω satisfies the following congruences:

$$\omega \equiv \begin{cases} a \pmod p \\ b \pmod q, \end{cases}$$

and where ω_p satisfies $1 + \omega_p + \ldots + \omega_p^{L-2} + \omega_p^{L-1} \equiv 0 \pmod p$ and ω_q satisfies $1 + \omega_q + \ldots + \omega_q^{L-2} + \omega_q^{L-1} \equiv 0 \pmod q$.

[Lemma 3] Let L be an integer $(L \geq 2)$, n be a composite number which is the product of two odd primes p and q and ω be one of the L-th roots mod n of 1. Then,

$$\begin{aligned} \#\{\omega \mid \omega \text{ is } \mathit{type1}\} &= 1, \\ \#\{\omega \mid \omega \text{ is } \mathit{type2}\} &= q' - 1, \\ \#\{\omega \mid \omega \text{ is } \mathit{type3}\} &= p' - 1, \\ \#\{\omega \mid \omega \text{ is } \mathit{type4}\} &= (p'-1)(q'-1) \end{aligned}$$

where $p' = (L, p-1)$, $q' = (L, q-1)$, and $\#$ denotes the number of elements of a set.

Proof The following equation with respect to ω has p' solutions in $GF(p)$ according to Lemma 1: $1 - \omega^L \equiv (1-\omega)(1 + \omega + \ldots + \omega^{L-2} + \omega^{L-1}) \equiv 0 \pmod p$. Thus, $\#\{\omega_p \bmod p \mid 1 + \omega_p + \ldots + \omega_p^{L-2} + \omega_p^{L-1} \equiv 0 \pmod p)\} = p' - 1$. Similarly, $\#\{\omega_q$ mod

$q \mid 1+\omega_q+\ldots+\omega_q^{L-2}+\omega_q^{L-1} \equiv 0 \pmod q)\} = q'-1$. Moreover, $\#\{\,\omega \mid \#\{\omega \bmod p\} = \alpha$ and $\#\{\omega \bmod q\} = \beta\} = \alpha \cdot \beta$. Therefore, the above property is proven. *Q.E.D.*

[Theorem 1] Let L be an integer ($L \geq 2$), n be a composite number which is the product of two odd primes p and q, I be the L-th residue mod n, and AL be a probabilistic polynomial time algorithm which, given I and n, finds one of the L-th roots mod n of I with probability ($> 1/|n|^a$), where $|n|$ denotes the data length of n. If $(L, p-1) \neq 1$ or $(L, q-1) \neq 1$, then there exists a probabilistic polynomial time algorithm for factoring n using AL at most in $O(|n|^{a+2b})$ steps, where b satisfies $L = O(|n|^b)$.

Proof Choose a random integer $y \in Z_n$, where Z_n denotes $\{0, \ldots, n-1\}$, calculate $z = y^L \bmod n$ and compute x which is one of the L-th roots mod n of z by using AL. Because the distribution of x doesn't depend on which y is selected, and because y is randomly selected, $\omega = x/y \bmod n$ is uniformly distributed. If ω is *type2* or *type3*, we can calculate the factors of n by computing $(\omega - 1, n)$. Note that when ω is *type1*, $(\omega - 1, n) = n$; and when ω is *type4*, $(\omega - 1, n) = 1$. The probability of $\{\ \omega$ is *type2* or *type3* $\}$ is $\frac{p'+q'-2}{p'q'}$ according to Lemma 3. Moreover, the inequation $\frac{p'+q'-2}{p'q'} \geq \frac{1}{p'q'}$ holds because of the assumption $(L, p-1) \neq 1$ or $(L, q-1) \neq 1$. The average number of iterations for deriving x from z using AL is $|n|^a$. The average number of iterations for selecting x such that ω is *type2* or *type3* is at most $p'q' = O(|I|^{2b})$. Therefore, the total average number of iterations for the factorization of n is at most $O(|n|^{a+2b})$. *Q.E.D.*

[Definition 2] Let p be a prime and $a \in GF(p)$. An index of a over $GF(p)$, $Ind_p(a)$, is defined as follows:

$$Ind_p(a) = \min\{m \mid a^m \equiv 1 \pmod p\}.$$

[Lemma 4] Let p be a prime, $J \in GF(p)$ be the p'-th residue mod p, where $(p', p-1) = p'$ and $p' = r_1 \cdot r_2$ ($r_1, r_2 > 1$), K be one of the r_1-th roots mod p of J, $v_i (i = 1, 2, \ldots, r_2)$ be the r_2-th roots of K, v_0 be one of the p'-th roots of J, and $\omega_i = v_i/v_0 \bmod p$. If there is an integer $\delta (> 1)$ which satisfies $(\delta, r_1) = 1$ and $(\delta, r_2) = \delta$, for any K and v_0, there is at least one pair (ω_i, ω_j) such that $Ind_p(\omega_i) \neq Ind_p(\omega_j)$.

Proof Let g be a primitive element over $GF(p)$, let α satisfy $g^{r_1 \cdot r_2 \cdot \alpha} \equiv J \pmod p$. Then,

$$K = g^{r_2 \cdot \alpha + (p-1) \cdot \frac{j_1}{r_1}} \bmod p,$$

where $0 \leq j_1 \leq r_1 - 1$. Thus,

$$v_i = g^{\alpha + (p-1) \cdot \frac{j_1 + i \cdot r_1}{r_1 \cdot r_2}} \bmod p,$$

where $0 \leq i \leq r_2 - 1$. Similarly,

$$v_0 = g^{\alpha + (p-1) \cdot \frac{j_0 + i_0 \cdot r_1}{r_1 \cdot r_2}} \bmod \ p.$$

Therefore,

$$\omega_i = g^{(p-1) \cdot \frac{(j_1 - j_0) + (i - i_0) \cdot r_1}{r_1 \cdot r_2}} \bmod \ p.$$

When $j_0 \neq j_1$, for any i_0, j_0 and j_1, there are two integers u $(-\delta < u < \delta)$ and v $(-r_1 < v < r_1)$ such that $(j_1 - j_0) + u \cdot r_1 = v \cdot \delta$, because $(r_1, \delta) = 1$. Put $i_1 = i_0 + u \bmod r_2$, then $(\omega_{i_1})^{\frac{r_1 \cdot r_2}{\delta}} \equiv g^{(p-1) \cdot v} \equiv 1 \pmod p$. Thus, $Ind_p(\omega_{i_1})$ divides $\frac{r_1 \cdot r_2}{\delta}$. On the other hand, there is an integer i_2 $(0 \leq i_2 \leq r_2 - 1)$ such that $(j_1 - j_0) + (i_2 - i_0) r_1 \not\equiv 0 \pmod \delta$, because $(r_1, \delta) = 1$ and $\delta \geq 2$. Thus, $Ind_p(\omega_{i_2})$ does not divide $\frac{r_1 \cdot r_2}{\delta}$. Therefore, $Ind_p(\omega_{i_1}) \neq Ind_p(\omega_{i_2})$. When $j_0 = j_1$, then $\omega_{i_0} = 1$ and $\omega_i \neq 1$ $(i \neq i_0)$. Therefore, $Ind_p(\omega_{i_0}) \neq Ind_p(\omega_i)$. *Q.E.D.*

3. Sequential Version

An identification scheme is proposed here in which a prover convinces a verifier that he is a real prover. Hereafter we denote a real prover as $\overline{A}$, an invalid prover as $\tilde{A}$, a real verifier as $\overline{B}$ and an invalid verifier as $\tilde{B}$.

A trusted center publishes an integer L $(L \geq 2)$ and a modulus n which is the product of two secret large primes p and q. $\overline{A}$ publishes I which is calculated by $I = S^L \bmod n$ using a secret random integer $S \in Z_n$. Note that the difficulty of deriving S from I corresponds to that of breaking the RSA scheme [RSA] in the case where $(L, p-1) = 1$ and $(L, q-1) = 1$, and corresponds to the difficulty of factoring n in the case where $(L, p-1) \neq 1$ or $(L, q-1) \neq 1$ according to Theorem 1.

To generate and verify a proof of identity, the parties execute the following procedure. Repeat Steps 1 to 4 in sequence t times:

Step 1) $\overline{A}$ generates a random integer $R \in Z_n$ and sends $X = R^L \bmod n$ to $\overline{B}$.

Step 2) $\overline{B}$ sends a random integer $E \in Z_L$ to $\overline{A}$.

Step 3) $\overline{A}$ sends $Y = R \cdot S^E \bmod n$ to $\overline{B}$.

Step 4) $\overline{B}$ verifies that $Y^L \equiv X \cdot I^E \pmod n$.

Verifier $\overline{B}$ accepts prover $\overline{A}$'s proof of identity only if all the checks are successful t times. Note that there is no constraint on the relation among L, p and q.

The following theorem guarantees the security of our sequential version.

[Theorem 2] This protocol is an interactive proof system of knowledge of the S [FFS] which is perfect zero knowledge [GMW], when $t = O(|n|)$ and $L = O(1)$.

Proof (sketch) *Completeness:* To prove that $\overline{A}$'s proof always convinces $\overline{B}$, we evaluate the verification condition: $Y^L \equiv (R \cdot S^E)^L \equiv R^L (S^L)^E \equiv X \cdot I^E \pmod n$. Thus, the verifier accepts $\overline{A}$'s proof with probability 1.

Soundness: Our goal is to show that whenever $\overline{B}$ accepts $\tilde{A}$'s proof with non-negligible probability ($> 1/|n|^a$), a probabilistic polynomial time Turing machine M can output the S', which satisfies $S'^L \equiv I \pmod{n}$, with overwhelming probability.

Let T be the truncated execution tree of $(\tilde{A}, \overline{B})$ for input I and $\tilde{A}$'s random tape RA. A vertex is called "heavy" if it has more than $L/2$ sons. First, we prove that at least half the vertices in at least one of the levels in T must be heavy, then that M can find a heavy vertex in T with overwhelming probability, and finally that S' can be computed from the sons of any heavy vertex when a heavy vertex is found.

Let $\alpha_i = \beta_{i+1}/\beta_i$ where β_i means the number of vertices at level i in T. If $\alpha_i < (3/4)L$ for all $1 \leq i \leq t$, then the total number of leaves in $T(i.e., \beta_t = \alpha_1 \cdots \alpha_{t-1} \cdot \beta_1)$ is bounded by $(3/4)^{t-1}L^t$, which is a negligible fraction of the L^t possible leaves. Since we assume that this fraction is polynomial, $\alpha_i > (3/4)L$ for at least one level, which we denote i_0. Assume at least half the vertices at this level (i_0) are not heavy, then $\beta_{i_0+1} < \beta_{i_o} \cdot L - (\beta_{i_0}/2)(L/2) = (3/4)\beta_{i_0} \cdot L$, and $\alpha_{i_0} = \beta_{i_0+1}/\beta_{i_0} < (3/4)L$. Here $\alpha_{i_0} > (3/4)L$. This is a contradiction. Therefore, it is proven that at least half the vertices in at least one of the levels in T must be heavy.

In order to find a heavy vertex in T, M explores random paths in the untruncated tree by determining the degree of each vertex and restarts from the root whenever the path encounters an improperly answered query. Since a non negligible fraction ($> 1/|n|^a$) of leaves is assumed to survive the truncation, the average iteration number of the executions where the path reaches to the t-th level is $|n|^a(t \cdot L)$. Since there is at least one level in T where at least half the vertices are heavy, the average iteration number of the executions where M can find a heavy vertex is at most $2|n|^a(t \cdot L) = O(|n|^{1+a})$.

Finally, we will show how S' can be computed from the sons of any heavy vertex, when a heavy vertex is found. Let Q be the set of queries E which are properly answered by $\tilde{A}$. Assume that all pairs of integers $(E', E")$ satisfy $E" - E' > 1$ where $E', E" \in Q$. Since $\#Q > L/2$, the largest difference between elements in Q is at least L. Here $\#Z_L = L$ and the largest difference between elements in Z_L is at most $L - 1$. This is a contradiction. Therefore, it is proven that a set Q of more than $L/2$ integers of Z_L must contain at least one pair of integers (E_1, E_2) such that $E_1 - E_2 = 1$. Since these queries were properly answered, the following verification conditions hold, where $X_i = X$; $Y_i^L \equiv I^{E_i} \cdot X \pmod{n}$ $(1 \leq i \leq 2)$. From these equations, we obtain $S' = Y_1/Y_2 \bmod n$ which satisfies the relation $S'^L \equiv (Y_1/Y_2)^L \equiv I^{E_1 - E_2} \equiv I \pmod{n}$.

Zero knowledge: Let $\tilde{B}$ be any polynomial expected time algorithm for the verifier. The simulator $M_{\tilde{B}}$ does the following:

```
repeat while $0 \leq c \leq t$
    begin
```

```
        choose $E' \in Z_L$ randomly and uniformly
        choose $Y = R \in Z_L$ randomly and uniformly
        $X = R^L / I^{E'} \pmod{n}$
        $\tilde{B}$ issues $E$
        if $E = E'$ then halt, $c = c + 1$ and output $(X, E, Y)$
    end
```

It can be demonstrated that $(\overline{A}, \tilde{B})(n, I)$ and $M_{\tilde{B}}(n, I)$ are identically distributed verifier's histories. For any verifier $\tilde{B}$, the probability that $E = E'$ is at least $1/L$. Thus, the average running time of this simulator $M_{\tilde{B}}$ is $O(t \cdot L)$, which is polynomial in $|n|$ based on our assumptions of the values of L and t. *Q.E.D.*

Remark: Evidently, we can extend the value of L to $O(|n|)$ in the above theorem.

4. Parallel Version

In this section, we consider a typical case where $k = t = 1$ and $p' = (L, p-1) > 1$ and $p' \geq q' = (L, q-1)$ for the parallel version. In this case, the difficulty of deriving S from I corresponds to that of factoring n according to Theorem 1. We define four security level notions of "transferable information with a (strict) security level ρ " and "transferable information with a (strict) sharp-threshold security level ρ ," which are more rigorous than the notion "transferable information" defined by [FFS].

[Definition 3] The protocol $(\overline{A}, \overline{B})$ releases *no transferable information with a security level ρ* if:

1. It succeeds with overwhelming probability.
2. There is no coalition of $\tilde{A}$, $\tilde{B}$ with the property that, after a polynomial number of executions of $(\overline{A}, \tilde{B})$, it is possible to execute $(\tilde{A}, \overline{B})$ with $c \cdot \rho$ probability of success, where c is an arbitrary real constant greater than 1.

The protocol $(\overline{A}, \overline{B})$ releases *no transferable information with a strict security level ρ* if:

1. It succeeds with overwhelming probability.

2'. There is no coalition of $\tilde{A}$, $\tilde{B}$ with the property that, after a polynomial number of executions of $(\overline{A}, \tilde{B})$, it is possible to execute $(\tilde{A}, \overline{B})$ with $c \cdot \rho$ probability of success, where c is $(1 + 1/|n|^d)$ and d is an arbitrary constant greater than 0.

The protocol $(\overline{A}, \overline{B})$ releases *no transferable information with a sharp-threshold security level ρ* if it satisfies conditions 1 and 2 above as well as the following condition:

3. The probability of $\tilde{A}$ cheating $\overline{B}$ is ρ.

The protocol $(\overline{A}, \overline{B})$ releases *no transferable information with a strict sharp-threshold security level ρ* if it satisfies conditions 1, 2' and 3.

It has been proven that Fiat-Shamir's parallel version of the identification scheme releases no transferable information with a sharp-threshold security level [FFS], but not with a *strict* sharp-threshold security level. The following theorem and corollary guarantee the security of our parallel version using the new notion, "transferable information with a *strict (sharp-threshold)* security level." The following results are easily extended to the situation where k and t have other values.

[Theorem 3] Let the parameters $k = t = 1$ and L satisfy $(L, p-1) = p' > 1$, $p' \geq (L, q-1) = q'$, and $L = O(1)$. When at least one of the following conditions C1, C2, C3, and C4 is satisfied, then the parallel version of our identification scheme releases no transferable information with a strict security level $1/p'$, if there is no probabilistic polynomial time algorithm of factoring.

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

C2. $q' = \prod_{i=1}^{M} q_i$, where q_i is a prime number, $q_i \neq q_j$ $(i \neq j)$, and $M \geq 1$.

C3. $q' = 1$.

C4. $(p', q') = 1$

Proof (sketch) Let $L = p' \cdot l_p$. To prove this theorem, we show that if $(\widetilde{A}, \overline{B})$ can be executed with probability $\varepsilon = c/p' = (1 + 1/|n|^d)/p'$ after $O(|n|^e)$ executions of $(\overline{A}, \widetilde{B})$, then n can be factored by a coalition of $\overline{A}, \widetilde{A}, \overline{B}$ and $\widetilde{B}$ at most in time $O(\|\widetilde{B}\| \cdot |n|^e + \|\widetilde{A}\| \cdot |n|^d)$ and with overwhelming probability, where d and e are positive constants, and $\|A\|$ and $\|B\|$ denote the time complexity of A and B.

Given any pair of unusually successful programs $\widetilde{A}$ and $\widetilde{B}$, we start the factorization by executing $(\overline{A}, \widetilde{B})$ $O(|n|^e)$ times and relaying a transcript of the communication to $\widetilde{A}$. Since $\overline{A}$ itself can be used in this part and its time complexity $\|\overline{A}\|$ is assumed to be dominated by $\|\widetilde{B}\|$, these executions require $O(\|\widetilde{B}\| \cdot |n|^e)$.

The possible outcomes of the executions of $(\widetilde{A}, \overline{B})$ can be summarized in a large Boolean matrix H whose rows correspond to all possible choices of RA. Its columns correspond to all the possible choices L of RB, and its entries are 1 if $\overline{B}$ accepts $\widetilde{A}$'s proof, and 0 if otherwise.

To factor n, the coalition tries to find at least $(l_p + 1)$ 1's along the same row in H. We call a row "heavy" if the number of 1's along it is at least $l_p + 1$. Assume that at least $1/c$ of the 1's in H are not located in heavy rows. Then the fraction of non-heavy rows in H, which we denote τ, is estimated as follows: $\tau > \frac{\varepsilon \cdot L \cdot 1/c}{l_p} = 1$. This is a contradiction. Therefore, at least $(1 - 1/c)$ of the 1's in H are located in heavy rows. We thus adopt the following strategy:

1. Probe $O(1/\varepsilon)$ random entries in H.

2. After the first 1 is found, probe $l_p O(1/\varepsilon)$ random entries along the same row. Because $\frac{1}{1-1/c} = \frac{c}{c-1} = 1 + |n|^d$, we can find a heavy row with constant probability in just $\frac{c}{c-1} \cdot \{O(\frac{1}{\varepsilon}) + l_p \cdot O(\frac{1}{\varepsilon})\} = \frac{c}{c-1} \cdot \{(1 + l_p) O(\frac{1}{\varepsilon})\} < O(|n|^d)$ probes. Again we assume that $\|\overline{B}\|$ is dominated by $\|\widetilde{A}\|$, and thus the time complexity of this part of

the algorithm is at most $O(||\widetilde{A}|| \cdot |n|^d)$.

Next, we will prove that n can be factored by a coalition of $\overline{A}, \widetilde{A}, \overline{B}$ and $\widetilde{B}$ in polynomial time and with probability at least $1/p'$, when the coalition finds at least $(l_p + 1)$ 1's along the same row in H.

Let Q be the set of queries E which are properly answered by $\widetilde{A}$. Assume that all pairs of queries (E', E") satisfy E" − E'≥ p' where E', E" $\in Q$. Since $\#Q \geq (l_p + 1)$, the largest difference between elements in Q is at least $l_p \cdot p' = L$. Here $\#Z_L = L$ and the largest difference between elements in Z_L is at most $L - 1$. This is a contradiction. Therefore, it is proven that a set Q of at least $(l_p + 1)$ integers of Z_L must contain at least one pair of integers (E_1, E_2) such that $E_1 - E_2 < p'$.

Let (X, E_1, Y_1) and (X, E_2, Y_2) be the two 1's in Q , i.e., the two possible outcomes of the execution of $(\widetilde{A}, \overline{B})$, that satisfy $E_1 - E_2 < p'$. Since (X, E_1, Y_1) and (X, E_2, Y_2) satisfy the equation $(Y_1/Y_2)^L \equiv I^{E_1 - E_2} \pmod n$, thus $Y_1/Y_2 \bmod n$ is one of the L-th roots mod n of $I^{E_1-E_2} \bmod n$, and $S^{E_1-E_2} \bmod n$ is also one of the L-th roots mod n of $I^{E_1-E_2} \bmod n$, where S is known by $\overline{A}$.

We claim that from the X's and Y's sent by $\overline{A}$ during the execution of $(\overline{A}, \widetilde{B})$ even an infinitely powerful $\widetilde{B}$ cannot determine which L-th root mod n of I $\overline{A}$ acturally uses. This can be shown as follows: let ω be one of the L-th roots mod n of 1, then $S' = \omega \cdot S$ is another L-th root mod n of I other than S. If $\overline{A}$ replaces S with S', $\overline{A}$ produces the same X, Y with the same probability distribution, shown as follows: $X \equiv R^L \equiv (R \cdot \omega^{-E})^L \pmod n$ and $Y \equiv S^E \cdot R \equiv S'^E (R \cdot \omega^{-E}) \pmod n$. Since the R's are randomly chosen, $\overline{A}$ produces the same X, Y values with the same probability distribution in both cases. Therefore, during the executions of $(\overline{A}, \widetilde{B})$ $\overline{A}$ cannot leak to $\widetilde{B}$ which L-th root mod n of $I^{E_1-E_2} \bmod n$ he can compute from the S he knows. Thus, we have proven that the L-th roots mod n of $I^{E_1-E_2} \bmod n$ which are known by $\overline{A}$ and computed by a coalition of $\widetilde{A}$, $\overline{B}$ and $\widetilde{B}$ are totally independent.

Next, we will prove that n can be factored with probability at least $1/p'$ using $S^{E_1-E_2} \bmod n$ and $Y_1/Y_2 \bmod n$, if at least one of the conditions C1, C2, C3, and C4 is satisfied, even if the value of $Y_1/Y_2 \bmod n$ is biased. Let $\omega = \frac{S^{E_1-E_2}}{Y_1/Y_2} \bmod n$ and $\omega = [\omega_p, \omega_q]$. When C1 is satisfied, the probability of successfully factoring n using ω is at least $1/p'$. This is because: if $Ind_p(\omega_p) < Ind_q(\omega_q)$, then $\omega^{Ind_p(\omega_p)} \bmod n$ is *Type2*, and if $Ind_p(\omega_p) > Ind_q(\omega_q)$, then $\omega^{Ind_q(\omega_q)} \bmod n$ is *Type3*. Therefore, when $Ind_p(\omega_p) \neq Ind_q(\omega_q)$, the probability of successfully factoring n using ω is 1. Here, we will show that the probability of $Ind_p(\omega_p) \neq Ind_q(\omega_q)$ is at least $1/p'$. Let $p' = r_1 \cdot r_2$ such that $r_1 = (p', E_1 - E_2) < p'$, $\{v_1, \cdots, v_{r_2}\} = \{S'^{E_1-E_2} \bmod p \mid S'$ is the L-th root mod n of $I\}$ and $v_0 = \frac{Y_1}{Y_2} \bmod p$, then $(r_1, r_2) = 1$ because of C1, and $r_2 \geq 2$ because of Lemma 2. Therefore, there is at least one pair $(\omega_{p,i}, \omega_{p,j})$ satisfying $Ind_p(\omega_{p,i}) \neq Ind_p(\omega_{p,j})$ according to Lemma 4, where $\omega_{p,i} = v_i/v_0 \bmod p$ $(i = 1, \cdots, r_2)$. When

C2 is satisfied, change the role of p and q in the C1 case. When C3 is satisfied and $\omega \neq 1$, then ω is *Type3* because $\omega = [\omega_p, 1]$ where $\omega_p \neq 1$. Since $\#\{S'^{E_1 - E_2} \bmod p \mid S'$ is the L-th root mod n of $I\} \geq 2$, the probability of successfully factoring n using ω is at least $1/2$. When C4 is satisfied and $\omega \neq 1$, then $\omega^{q'} \bmod n$ is *Type3* because $\omega^{q'} = [\omega_p, 1]$ where $\omega_p \neq 1$. Since $\#\{S'^{E_1 - E_2} \bmod p \mid S'$ is the L-th root mod n of $I\} \geq 2$, the probability of successfully factoring n using ω is at least $1/2$. Therefore, the probability of successfully factoring n using ω is at least $1/p'$.

Finally, We will prove that n can be factored by a coalition of $\overline{A}, \widetilde{A}, \overline{B}$ and $\widetilde{B}$ at most in time $p'\{O(\|\widetilde{B}\| \cdot |n|^e) + O(\|\widetilde{A}\| \cdot |n|^d)\} = O(\|\widetilde{B}\| \cdot |n|^e + \|\widetilde{A}\| \cdot |n|^d)$ and with overwhelming probability. When for any $f (1 \leq f < p')$, $\omega^f \bmod n$ is *Type1* or *Type4*, n cannot be factored. Then, $\overline{A}$ selects another S' randomly and calculates $I' = S'^L \bmod n$, and the coalition goes through the same procedure to factor n. The procedure is repeated until n can be factored. The average number of iterations is at most p'. *Q.E.D.*

Remark: Evidently, we can extend the value of L to $O(|n|)$ in the above theorem. However, from the practical viewpoint, it is essential that the security level is a constant value, or a non asymptotic value. Therefore, the condition of Theorem 3 for the order of L is optimal.

[Corollary] Let the parameters $k = t = 1$ and L satisfy $(L, p-1) = L$, and $L = O(1)$. If at least one of the conditions C1,C2,C3, and C4 is satisfied, then the parallel version of our identification scheme releases no transferable information with a strict ***sharp-threshold*** security level $1/L$, if there is no probabilistic polynomial time algorithm of factoring.

Proof It is proven that this protocol releases no transferable information with a strict security level $1/L$ because $(L, p-1) = L$ and because of Theorem 3. Here, $\widetilde{A}$ can cheat $\overline{B}$ with probability $1/L$ because $\widetilde{A}$ can guess RB with probability $1/L$. *Q.E.D.*

5. Applications

Signature scheme A triplet (M, E, Y) is sent as the signed message, where M is a message, h is a public pseudo-random function and $E = h(M, X) \in Z_L$, to turn the identification scheme into a signature scheme. Y here is the same as in Step 3 of the identification scheme.

N-Party authentication scheme N-party identification and signature protocol based on the Fiat-Shamir scheme was proposed by [BLY]. However, in the Fiat-Shamir scheme a large memory ($k \approx 100$) is required. Our parallel version is suited to their protocol with only one secret integer and $\log_2 L \approx 100$.

6. Efficiency

In this section, we focus on a typical implementation of our parallel version.

Secret memory size This scheme requires $|n|$ bits of secret information S, while the Fiat-Shamir scheme requires $k\ |n|$ bits of secret information. The proposed scheme is therefore more efficient than the Fiat-Shamir scheme when $k \geq 2$.

Transmission efficiency $(2|n| + |L|)$ bits are transmitted in this scheme, while $(2t|n| + kt)$ bits are transmitted in the Fiat-Shamir scheme. Note that when $t = 1$ is used in the Fiat-Shamir scheme, the k value must be large.

Processing speed The amount of processing needed for this scheme is compared with the RSA [RSA] and Fiat-Shamir schemes using the average number of modular multiplications required to generate or verify a proof of identity.

The RSA scheme requires $(3|n|)/2$ steps, the Fiat-Shamir scheme requires $t(k+2)/2$ steps, and the proposed scheme requires $(5l+2)/2$ steps where $L = 2^l$. For example, when $tk = l = 20$, our parallel version requires 51 steps, while the Fiat-Shamir scheme requires 11 steps (where $k = 20, t = 1$) to 30 steps (where $k = 1, t = 20$), and the RSA scheme requires 768 steps where $|n| = 512$.

When a prover uses a secret integer S satisfying $I^{-1} \equiv S^L \bmod n$, a verifier checks whether $Y^L \cdot I^E \equiv X \pmod{n}$ holds. The computations of Y^L and I^E can be combined, i.e., according to the value of E, a verifier can repeatedly square the results of the intermediate calculation, or square those results multiplied by I, as appropriate. This improved calculation requires $3l/2$ steps in the verification; for example, 30 steps are required when $l = 20$.

7. Conclusion

Combining our scheme with the Fiat-Shamir scheme provides greater flexibility because three appropriate design parameters of transmitted information size, memory size and speed can be selected.

The parallel version described in Section 4 is more efficient than the Fiat-Shamir scheme from the standpoint of transmitted information size and secret information size, because it corresponds to $t = k = 1$ in their scheme. It is about one order of magnitude faster than the RSA scheme and is relatively slow in comparison with the Fiat-Shamir scheme. Our sequential and parallel versions are also shown to have the same security characteristics as the Fiat-Shamir scheme.

Finally, we conclude with an open problem relating to the security level: when $(L, p-1) = p' < L$ and at least one of conditions C1,C2,C3, and C4 is satisfied, does the parallel version of our identification scheme release no transferable information with a strict *sharp-threshold* security level $1/p'$, if there is no probabilistic polynomial time algorithm of factoring ?

Acknowledgements

The authors would like to thank Adi Shamir and Kenji Koyama for their participation in valuable discussions. In particular, we owe the improved calculation in *Section 6* to Adi Shamir.

References

[BLY] Brickell, E., Lee, P. and Yacobi, Y.: "Secure Audio Teleconference," Advances in Cryptology - Crypto'87, Lecture Notes in Computer Science 293, 1988, pp.429-433

[FS] Fiat, A. and Shamir, A.: "How to Prove Yourself: Practical Solution to Identification and Signature Problems," Advances in Cryptology - Crypto'86, Lecture Notes in Computer Science 263, 1987, pp.186-199

[FFS] Feige, U., Fiat, A. and Shamir, A.: "Zero Knowledge Proofs of Identity," Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, pp.210-217

[GMR] Goldwasser, S., Micali, S. and Rackoff, C.: "Knowledge Complexity of Interactive Proof Systems," Proceedings of the 17th Annual ACM Symposium on Theory of Computing, 1985, pp.291-304

[GMW] Goldreich, O., Micali, S. and Wigderson, A.: "Proofs that Yield Nothing but Their Validity and a Methdology of Cryptographic Protocol Design," Proceedings of the 27th Annual Symposium on Foundations of Computer Science, 1986, pp.174-197

[GQ1] Guillou, L.C., and Quisquater, J.J.: "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Tranamission and Memory," Eurocrypt'88 Abstracts, 1988, pp.71-75

[GQ2] Guillou, L.C., and Quisquater, J.J.: "A Paradoxical Identity-Based Signature Scheme Resulting from Zero-Knowledge," These Proceedings, 1988

[OO] Ohta, K. and Okamoto, T.: "Practical Extension of Fiat-Shamir Scheme," Electron.Lett., 24, No. 15, 1988, pp.955-956

[HW] Hardy, G.H. and Wright, E.M.: "An Introduction to the Theory of Numbers," Fifth edition, Oxford University Press, New York, 1978

[RSA] Rivest, R.L., Shamir, A. and Adleman, L.: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communication of the ACM, Vol. 21, No. 2, 1978, pp.120-126