Multi-Language Zero Knowledge Interactive Proof Systems

Kaoru KUROSAWA Shigeo TSUJII

Department of Electrical and Electronic Engineering,
Faculty of Engineering,
Tokyo Institute of Technology

2-12-1, Ookayama, Meguro-ku, Tokyo 152, JAPAN

Tel. +81-3-726-1111(Ext. 2577)
Fax +81-3-729-0685
E-mail kkurosaw@ss.titech.ac.jp or
kkurosaw%ss.titech.ac.jp@relay.cs.net

Abstract

Suppose that two ZKIPs are given for language L_1 and L_2. The total number of bits communicated is the sum of the two. This paper shows that it is possible to get the same effect in less amount of communication. We call such protocols "multi-language zero knowledge interactive proof systems".

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 339-352, 1991.

1 Introduction

In zero knowledge interactive proof systems (ZKIPs) [GMR89], a large amount of communication is the bottleneck. Suppose that Alice wants to convince Bob of two theorems in zero knowledge, such as z is a quadratic residue mod N and G is Hamiltonian. The easiest way is to concatenate the two ZKIPs. The total number of bits communicated is the sum of the two. It will be nice if Alice can do that in shorter conversation.

This paper shows that it is possible. Alice can convince Bob in zero knowledge that $x_1 \in L_1$ and $x_2 \in L_2$ independently, and the total number of bits communicated is less than the sum of the two. We call such protocols "multi-language zero knowledge interactive proof systems (MZKIP)".

The paper is organized in the following way: In section 2, the definition of ZKIP is reviewed. In subsection 3.1, Kurosawa's cryptosystem is shown. (This cryptosystem itself is interesting.) In subsection 3.2, we define conditioned QNR and present a ZKIP for that by using Kurosawa's cryptosystem. In section 4, the definition of MZKIP is given. In section 5, we show an example of MZKIP for conditioned QNR and Hamilton problem.

2 ZKIP

For the definition of ZKIP, we refer the reader to [GMR89].

(Definition)

(A, B) is an interactive proof system for L if we have the following.

(1) Completeness

For each k, for sufficiently large x in L, B accepts with probability at least $1 - |x|^{-k}$.

(2) Soundness

For each k, for sufficiently large x not in L, for any A', on input x to

(A', B), B accepts x with probability at most $|x|^{-k}$. (The probabilities here are taken over the coin tosses of A' and B)

Let P(U, C, x) be the probability that a poly-size circuit C_x outputs 1 on input a random string distributed according to U(x).

(Definition)

(A, B) is zero-knowledge on L for B' if there exists a probabilistic turing machine $M_{B'}$, running in expected polynomial time, such that, for all poly-size family of circuits C, for all constant $c > 0$ and all sufficiently long strings $x \in L$,

$$|P(View_{AB'}, C, (x, H)) - P(M_{B'}, C, (x, H))| < |x|^{-c}$$

where H is an extra input tape to B'.

(A, B) is zero-knowledge on L if it is zero-knowledge on L for all B'.

(Definition)

(A, B) is a zero-knowledge proof system for L if it is an interactive proof system for L and zero-knowledge protocol on L.

3 Kurosawa's cryptosystem

3.1 Proposed public key cryptosystem [KIT87]

RSA is not know to be as hard as factorization. Rabin's cryptosystem is as hard as factorization. However, it is not uniquely deciphered because four different plaintexts produce the same ciphertext. Williams showed that this disadvantage can be overcome if the secret two prime numbers, p and q, are chosen such that p=q=3 mod 4. In Kurosawa's cryptosystem,

(1) p and q are arbitrary.

(2) It is as hard as factorization.

(3) It is uniquely deciphered.

The cryptosystem is as follows.

(Secret key) Two prime numbers, p and q.

(Public key) R(=pq) and c, where

$$(c/p) = (c/q) = -1 \tag{1}$$

(Plaintext) M

(Ciphertext) (E, s, t), where

$$E = M + (c/M) \bmod R \tag{2}$$

$$s = \begin{cases} 0 & \text{if } (M/R) = 1 \\ 1 & \text{if } (M/R) = -1 \end{cases} \tag{3}$$

$$t = \begin{cases} 0 & \text{if } M < (c/M \bmod R) \\ 1 & \text{if } M > (c/M \bmod R) \end{cases} \tag{4}$$

(Decryption)

From eq.(2), we obtain

$$M^2 - EM + c = 0 \tag{5}$$

Let a_1 and a_2 be the roots of eq.(5) mod p, and b_1 and b_2 be the roots of eq.(5) mod q. ([R80] shows how to find them.) Then, eq.(5) mod R has the following four roots.

$$M_1 = [a_1, b_1], \quad M_2 = [a_2, b_2]$$

$$M_3 = [a_1, b_2], \quad M_4 = [a_2, b_1]$$

where $M_1 = [a_1, b_1]$ means

$$M_1 = a_1 \bmod p, \quad M_1 = b_1 \bmod q$$

The original plaintext M is one of the four roots. "s" and "t" tell which one the plaintext M is, as we will see.

From eq.(5) and eq.(1), we obtain

$$(a_1/p)(a_2/p) = (c/p) = -1$$

We thus set

$$(a_1/p) = 1, \quad (a_2/p) = -1 \tag{6}$$

Similarly, we set

$$(b_1/q) = 1, \quad (b_2/q) = -1 \tag{7}$$

We then obtain

$$(M_1/R) = (M_1/p)(M_1/q) = (a_1/p)(b_1/q) = 1$$

Similarly, we obtain

$$(M_2/R) = 1$$

$$(M_3/R) = (M_4/R) = -1$$

Therefore, the receiver sees that

$$M = \begin{cases} M_1 \text{ or } M_2 & \text{if } s = 0 \\ M_3 \text{ or } M_4 & \text{if } s = 1 \end{cases} \tag{8}$$

Now, suppose that s=0. From eq.(5), we get

$$M_1 M_2 = [a_1 a_2, b_1 b_2] = [c, c] = c \bmod R$$

Hence

$$M_2 = c/M_1 \bmod R$$

Therefore, the receiver sees that

$$M = \begin{cases} min(M_1, M_2) & \text{if } t = 0 \\ max(M_1, M_2) & \text{if } t = 1 \end{cases} \tag{9}$$

When s=1,

$$M = \begin{cases} min(M_3, M_4) & \text{if } t = 0 \\ max(M_3, M_4) & \text{if } t = 1 \end{cases} \tag{10}$$

Thus, any ciphertext is uniquely deciphered.

It is clear that the cryptosystem is broken if one can factor R=pq. We will prove the converse.

[Lemma 1]

$$a_1 \neq a_2 \bmod p, \quad b_1 \neq b_2 \bmod q$$

(Proof)

It is clear from eq.(6) and eq.(7).

Q.E.D.

[Theorem 1]

Suppose that there exists a probabilistic polynomial time algorithm finding a plaintext from any ciphertext. Then, there exists a probabilistic polynomial time algorithm factoring R=pq.

(Proof)

Choose at random c such that (c/R)=1. Such c satisfies eq.(1) with probability 1/2. Let (R, c) be a public key of the cryptosystem.

Choose M randomly and compute M' as follows.

$$\begin{aligned} M &\rightarrow (E, s, t) \quad \text{(encryption)} \\ &\rightarrow (E, s', t) \\ &\rightarrow M' \qquad \text{(decryption)} \end{aligned} \tag{11}$$

where $s' = s + 1 \bmod 2$. Let $M = [f_1, g_1]$. Since $s' = s + 1 \bmod 2$,

$$M' = [f_1, g_2] \quad or \quad [f_2, g_1]$$

First, consider the case of $M' = [f_1, g_2]$. Then,

$$M - M' = [f_1, g_1] - [f_1, g_2] = [0, g_1 - g_2]$$

From lemma 1,

$$M - M' = 0 \bmod p, \quad M - M' \neq 0 \bmod q$$

Therefore,

$$gcd(M - M', R) = p.$$

The case of $[f_2, g_1]$ is similar.

Q.E.D.

[Theorem 2]

Suppose that there exists a probabilistic polynomial time algorithm finding a plaintext from 1/poly(n) of all ciphertexts, where $n = |R|$. Then, there exists a probabilistic polynomial time algorithm factoring R=pq.

3.2 Conditioned QNR

QNR (quadratic non-residue) is defined as follows.

$$QNR = \{(c, N) | (c/N) = 1, \quad N = \prod_i p_i^{e_i}, \quad (c/p_j) = -1 \text{ for some j.}\}$$

We define "conditioned QNR" as follows.

$$\text{conditioned QNR} = \{(c, N) | (c/N) = 1, \quad N = \prod_i p_i^{e_i},$$

$$(c/p_j^{e_j}) = -1 \text{ for some j.}\}$$

We present a ZKIP for conditioned QNR below.

Without loss of generality, let $(c/p_1^{e_1}) = -1$ and set $Q = N/p_1^{e_1}$. $x = [a, b]$ denotes

$$x = a \bmod Q, \quad x = b \bmod p_1^{e_1}$$

Repeat step 1-4 n times, where $n = |N|$.

(step 1)

A chooses a random number r and computes

$$y = r + (c/r) \bmod N$$

A sends y to B.

(step 2)

B sends randomly e=1 or -1 to A.

(step 3)

A computes

$$x = \begin{cases} r & \text{if } (r/N) = e \\ [r, c/r] & \text{if } (r/N) = -e \end{cases} \tag{12}$$

A sends x to B.

(step 4)

B checks that

$$y = x + (c/x) \bmod N$$

$$(x/N) = e$$

(Remarks)

1. The validity of the above protocol is proved by using the same discussion of 3.1.

2. The number of bits communicated is 1/n of [GMR89].

3. The above ZKIP is also an Arthur-Merlin game.

4 Multi-language zero knowledge interactive proof systems

4.1 Probabilities and bit complexity

ZKIPs require a large amount of bits communicated so that the probabilities of soundness and zero-knowledgeness get sufficiently small. In other words, such probabilities are functions of the number of bits communicated.

Let F(=(A, B)) be a ZKIP for L. Let x be an input to F.

(Definition)

Let a_i (and b_i) be the i-th message of A(and B) Let

$$H_n \stackrel{\triangle}{=} \{x | x \in \{0,1\}^*, |x| = n\}$$

Then, we define

$$t(F,n) \stackrel{\triangle}{=} \max |b_1| + |a_1| + \ldots$$

where the maximum is taken over all $x \in H_n$ and the coin tosses of A and B.

(Definition)

$$P_*(F,x) \stackrel{\triangle}{=} \max \text{ Pr (B accepts } x)$$

where the maximum is taken over all A' and the coin tosses of A' and B.

(Definition)

$$P_z(F,x) \stackrel{\triangle}{=} \max_{B'} \min_{M_{B'}} \max_{C} |P(View_{AB'}, C, (x,H)) - P(M_{B'}, C, (x,H))|$$

4.2 Multi-language zero knowledge interactive proof systems

Suppose that two languages are given, $L_1 \subseteq \{0,1\}^*$ and $L_2 \subseteq \{0,1\}^*$. Let K(=(A, B)) be an interactive protocol with an input $x = (x_1, x_2)$, where $|x_1| = |x_2|$. B accepts nothing, x_1, x_2 or both x_1 and x_2.

(Definition)

We say that K is a concatenatable ZKIP (CZKIP) for L_1 and L_2 if we have the following.

(1) Completeness

If $x_i \in L_i$, B accepts x_i with probability at least $1 - |x_i|^{-k}$ for all k and x_i large enough, where i=1, 2.

(2) Soundness

If $x_i \notin L_i$, then for any A', B accepts x_i with probability at most $|x_i|^{-k}$ for all k and x_i large enough, where i=1, 2.

(3) Zero-knowledgeness

K is zero-knowledge on L, where $L \stackrel{\triangle}{=} \{(x_1,x_2)|x_1 \in L_1 \text{ and } x_2 \in L_2\}$.

(Remarks)

1. The completeness is independent of the other x_i. The soundness is also.

2. Therefore, CZKIP is different from a ZKIP for

   $L = \{(x_1,x_2)|x_1 \in L_1 \text{ and } x_2 \in L_2\}$ or $L = \{(x_1,x_2)|x_1 \in L_1 \text{ or } x_2 \in L_2\}$

Let K(=(A, B)) be a CZKIP for L_1 and L_2. Let $x(=(x_1,x_2))$ be an input to K.

(Definition)

Let a_i (and b_i) be the i-th message of A(and B). Let

$$H'_n \triangleq \{(x_1, x_2) | x_i \in \{0,1\}^*, |x_1| = |x_2| = n\}$$

Then, we define

$$t'(K, n) \triangleq \max |b_1| + |a_1| + \ldots$$

where the maximum is taken over all $(x_1, x_2) \in H'_n$ and the coin tosses of A and B.

(Definition)

$$P'_*(K, x) \triangleq \max \Pr \text{ (B accepts } x_i)$$

where the maximum is taken over all A' and the coin tosses of A' and B.

(Definition)

$$P'_z(K, x) = \max_{B'} \min_{M_{B'}} \max_{C} |P(View_{AB'}, C, (x, H)) - P(M_{B'}, C, (x, H))|$$

Let K be a CZKIP for L_1 and L_2. Let F_i be a ZKIP for L_i, i=1, 2.

(Definition)

We say that K is a multi-language ZKIP (MZKIP) for F_1 and F_2 if we have the following. Let $x = (x_1, x_2)$, $|x_1| = |x_2| = n$. Then, for sufficiently long n,

1. $t'(K, n) < t(F_1, n) + t(F_2, n)$ for any n.
2. $P'_*(K, x_i) < P_*(F_i, x_i)$ if $x_i \notin L_i$
3. $P'_z(K, x) \leq \max(P_z(F_1, x_1), P_z(F_2, x_2))$
   if $x_i \in L_i$ for i=1, 2.

(Remark)

MZKIPs for more than two languages are defined in a similar way.

5 Examples of MZKIP

5.1 Conditioned QNR + Hamiltonian

Let

$L_1 = \{(c, N) |$ c is a conditioned QNR mod N $\}$

$L_2 = \{$a graph G$|$ G is Hamiltonian $\}$

$ZKIP_1$ = the ZKIP for L_1 given in 3.2.

$ZKIP_2$ = the ZKIP for L_2 given by [B87].

We present a MZKIP for $ZKIP_1$ and $ZKIP_2$. Let

S = a Hamilton tour of G.

$n = |N| = m(m-1)/2$

where m is the number of nodes of G.

(step 1)

A publicizes a one way permutation f.

Repeat step 2-5 n times.

(step 2)

A permutes the nodes of G by a random permutation π. Let the incidence matrix of the resulted graph be $D = \{d_{ij}\}$. A chooses random numbers r_{ij} such that

$$(r_{ij} + c/r_{ij} \bmod N) = d_{ij} \bmod 2$$

A computes

$$g_{ij} = f(r_{ij} + c/r_{ij} \bmod N)$$

and send $\{g_{ij}\}$ to B.

(step 3)

B chooses (e_1, e_2) at random and sends it to B, where

$$e_1 = 1 \text{ or } -1, \quad e_2 = 0 \text{ or } 1$$

(step 4)

A computes

$$x_{ij} = \begin{cases} r_{ij} & \text{if } (r_{ij}/N) = e_1 \\ [r_{ij}, \quad c/r_{ij}] & \text{if } (r_{ij}/N) = -e_1 \end{cases}$$

If $e_2 = 0$, A sends π and $\{x_{ij}\}$ to B.

If $e_2 = 1$, A sends $\pi(S)$ and those x_{ij} such that edge ij is in $\pi(S)$.

(step 5)

B checks what he received.

(Remarks)

1. It is easily verified that the above protocol satisfies the conditions of MZKIP.

2. The number of bits communicated is nearly the same as that of $ZKIP_2$. That of $ZKIP_1$ is saved.

3. e_i is a question for L_i, i=1, 2.

4. If $(c, \quad N) \notin L_1$ and $G \in L_2$, B accepts only G with overwhelming probability, and vice versa.

5.2 Other examples

The following ZKIPs are known.

$ZKIP_3$: $L_3 =$ {$(z, N)|z$ is a quadratic residue mod N } [GMR89]

$ZKIP_4$: $L_4 =$ {$(z, a, p)|z = a^z \bmod p$}[TW87]

$ZKIP_5$: $L_5 =$ {$N|p^i$ divides N and p^{i+1} does not,
where $p = 3 \bmod 4$ is prime and i is odd } [B82]

$ZKIP_6$: $L_6 =$ {3-colorable graph } [GMW87]

$ZKIP_7$: $L_7 =$ {SAT} [BCC88]

A MZKIP is obtained for any one of ($ZKIP_1$, $ZKIP_3$, $ZKIP_4$, $ZKIP_5$) and any one of ($ZKIP_2$, $ZKIP_6$, $ZKIP_7$). A MZKIP for $ZKIP_3$ and $ZKIP5$ is also possible.

6 Summary

This paper proposed the notion of "multi-language zero-knowledge interactive proof systems". Some examples were given.

It will be a further work to clarify what kinds of ZKIPs can be combined so that the MZKIP is obtained.

References

[B82] Blum: " Coin flipping by telephone", IEEE, COMPCON, pp.133-137 (1982)

[B86] Blum: " How to prove a theorem so no one else can claim it Proc. International Congress of Mathematics, pp.1444-1451 (1986)

[BCC88] Brassard, Chaum and Crepeau: " Minimum disclosure proofs of knowledge", JCSS, pp.156-166 (1988)

[GMR89] Goldwasser, Micali and Rackoff: " The knowledge complexity of interactive proof systems", SIAM J. on Comp. vol.18, No.1, pp.186-208 (1989)

[GMW86] Goldreich, Micali and Wigderson: " How to prove all NP-statements in zero knowledge, and a methodology of cryptographic protocol design", Crypt'86, pp.171-185 (1986)

[KIT87] Kurosawa, Itoh and Takeuchi: " Public key cryptosystem using a reciprocal number with the same intractability as factoring a large number", Electronics Letters, vol.23, No.15, pp.809-810 (1987), CRYPTOLOGIA, vol.XII, No.4, pp.225-233 (1988)

[R80] Rabin: " Probabilistic algorithms in finite fields", SIAM J. Comput. 9, pp.273-280 (1980)

[TW87] Tompa and Woll: " Random self reducibility and zero knowledge interactive proofs of possession of information", FOCS, pp.472-482 (1987)