Divertible Zero Knowledge Interactive Proofs and Commutative Random Self-Reducibility

Tatsuaki Okamoto *Kazuo Ohta*

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

Abstract

In this paper, a new class of zero knowledge interactive proofs, a *divertible* zero knowledge interactive proof, is presented. Informally speaking, we call (A,B,C), a triplet of Turing machines, a divertible zero knowledge interactive proof, if (A,B) and (B,C) are zero knowledge interactive proofs and B converts (A,B) into (B,C) such that any evidence regarding the relationship between (A,B) and (B,C) is concealed. It is shown that any *commutative random self-reducible* problem, which is a variant of the *random self-reducible* problem introduced by Angluin et al., has a divertible perfect zero knowledge interactive proof. We also show that a specific class of the commutative random self-reducible problems have *more practical* divertible perfect zero knowledge interactive proofs. This class of zero knowledge interactive proofs has two sides; one positive, the other negative. On the positive side, divertible zero knowledge interactive proofs can be used to protect privacy in networked and computerized environments. Electronic checking and secret electronic balloting are described in this paper to illustrate this side. On the negative side, identification systems based on these zero knowledge interactive proofs are vulnerable to an abuse, which is, however, for the most part common to all logical idenification schemes. This abuse and some measures to overcome it are also presented.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 134-149, 1990.

1. Introduction

In this paper, we consider the following question: Let (A, B) be a zero knowledge interactive proof (ZKIP) system regarding a problem, where A is a prover and B is a verifier. Can B prove this problem to another machine C in a zero knowledge manner under the condition that B does not leave any evidence of his utilizing A's power in order to prove it to C? In other words, this condition can be described as follows: B does not leave any evidence of the relationship between the A-B interactions and the B-C interactions. In many applications of this class of zero knowledge interactive proofs, this condition plays an essential role.

First, a new class of zero knowledge interactive proofs is defined, *divertible* zero knowledge interactive proofs, which satisfies the above-mentioned question. A new class of problems, *commutative random self-reducible (CRSR)* problems, are also defined. Basically, these are a variant of the *random self-reducible* problems introduced by Angluin et al., [AL] and Tompa et al., [TW]. We show that any CRSR problem has a divertible perfect zero knowledge interactive proof. We also show that a specific class of CRSR problems, *endomorphic CRSR (ECRSR)* problems, have *more practical (multi-keys and higher degree version)* divertible perfect zero knowledge interactive proofs.

Divertible zero knowledge interactive proofs have two sides; one positive, the other negative. On the positive side, this class of zero knowledge interactive proofs can be used to protect privacy in networked and computerized situations. For example, a blind digital signature scheme based on divertible zero knowledge interactive proofs can be constructed. The blind digital signature schemes based on the RSA scheme and the GMR scheme [GoMiRi] have been proposed for electronic check protocols and electronic secret ballot protocols [C1, C2, Oh2, Da]. However, the scheme based on the RSA is not provably secure against adaptive chosen message attacks and is not efficient. The scheme based on the GMR is provably secure against adaptive chosen message attacks under some reasonable assumptions but is not efficient. In contrast, our scheme, based on divertible zero knowledge interactive proofs, is provably secure against adaptive chosen message attacks under some assumptions [MS, S] and is efficient when some efficient problems (e.g., square root mod$N$) are used. In this paper, we show two applications of divertible zero knowledge interactive proofs: one for electronic checking, and the other for secret electronic balloting. As a different type of application, this class of zero-knowledge proofs can be used to construct subliminal-channel-free identification/signature systems based on zero-knowledge proofs in a manner similar to that shown by Desmedt et al., [DGB, De].

On the negative side, we show a new abuse of divertible zero knowledge interactive proofs, which is related to the *mafia fraud* described in [DGB]. These abuses, however, are for the most part common to all logical identification schemes, in which security depends only on secret information. In our abuse, Bob can pass himself off as Alice to anyone, when Alice proves her identity to Bob, and he conceals any evidence regarding the relationship between Bob's proof and Alice's proof. That is, although Bob proves himself to be Alice with Alice's help, he conceals any evidence that he used her help. To illuminate this situation, we discuss a number of measures for overcoming these abuses.

Note: The protocol described in [DGB] as a subliminal-channel-free identification system based on the Fiat-Shamir scheme satisfies the property of divertible zero knowledge inter-

active proofs. That is, although the notion of divertible zero-knowledge interactive proofs has not been proposed previously, an implementation of this class of zero knowledge interactive proofs based on the Fiat-Shamir scheme has been shown in [DGB], where this protocol corresponds to a protocol to be shown in Appendix B.

2. Divertible zero knowledge interactive proofs

There are two types of interactive proofs. One is an interactive proof *for membership in language L*, in which a membership of an instance in language L is demonstrated [GMR]. The other is an interactive proof *for possession of information*, in which a prover's possession of information is demonstrated [FFS, TW]. In this paper, we concentrate on the interactive proof for possession of information. The results in this paper can be applied to the interactive proof for language membership.

(A, B) is an interactive pair of Turing machines, where A is the prover, and B is the verifier [GMR, TM]. Let $T \in \{A, B\}$. $T(s)$ denotes T begun with s on its input work tape. $(A, B)(x)$ refers to the probability space that assigns to the string σ the probability that (A, B), on input x, outputs σ. $(\underline{A(s)},B(t))(x)$, A's history, denotes the triplet (x, s,ρ,m), where ρ is the finite prefix of A's random tape that was read, and m is the final content of the communication channel tape on which B writes. Similarly, $(A(s),\underline{B(t)})(x)$, B's history, denotes the triplet (x, t,ρ',m'), where ρ' is the finite prefix of B's random tape that was read, and m' is the final content of the communication channel tape on which A writes. B^A means B with oracle A, where B^A's oracle tapes correspond to B's communication channel tapes with A. $R \subseteq X \times Y$ is a relation.

Definition 1. An interactive triple of Turing machines (A, B, C) is a *divertible (computational/perfect)* zero knowledge interactive proof that the prover can compute some y satisfying $(x, y) \in R$, if the following conditions hold.

(i) (A, B^C) is a (computational/perfect) zero knowledge interactive proof that the prover can compute some y satisfying $(x, y) \in R$ [TW].

(ii) (B^A, C) is a (computational/perfect) zero knowledge interactive proof that the prover can compute some y satisfying $(x, y) \in R$.

(iii) Only A can compute some y satisfying $(x, y) \in R$.

(iv) For any prover A^* accepted by a valid verifier C, any verifier C^*, any $(x, y) \in R$, and any strings s and t, $((\underline{A^*(y, s)},B^{C^*(t)})(x)$, $(B^{A^*(y,s)},\underline{C^*(t)})(x))$ and $((\underline{A^*(y, s)},C)(x)$, $(A(y),\underline{C^*(t)})(x))$ are (polynomially indistinguishable/equivalent), where A is a valid prover.

3. Commutative random self-reducible problems and divertible perfect zero knowledge interactive proofs

3.1 Commutative random self-reducible

Definition 2. Let $\mathcal{N}$ be a countable infinite set. For any $N \in \mathcal{N}$, let $|N|$ denote the length of a suitable representation of N. For any $N \in \mathcal{N}$, let X_N, Y_N be finite sets, and

$R_N \subseteq X_N \times Y_N$ be a relation. Let

$$domR_N = \{x \in X_N \mid (x, y) \in R_N \text{ for some } y \in Y_N\}$$

denote the *domain* of R_N,

$$R_N(x) = \{y \mid (x, y) \in R_N\}$$

the *image* of $x \in X_N$, and

$$R_N(X_N) = \{y \mid (x, y) \in R_N, x \in X_N\}$$

the *image* of R_N.

R is *commutative random self-reducible (CRSR)* if and only if there is a polynomial time algorithm A that, given any inputs $N \in \mathcal{N}$, $x \in domR_N$, and $r \in R_N(X_N)$, outputs $x' = A(N, x, r) \in domR_N$ satisfying the following five properties.

R1. If r is randomly and uniformly chosen on $R_N(X_N)$, then x' is uniformly distributed over $domR_N$.

R2. There is a polynomial time algorithm that, given N, x, r, and any $y' \in R_N(x')$, outputs $y \in R_N(x)$.

R3. There is a polynomial time algorithm that, given N, x, r, and any $y \in R_N(x)$, outputs some $y' \in R_N(x')$. If, in addition, r is randomly and uniformly chosen on $R_N(X_N)$, then y' is uniformly distributed on $R_N(x')$.

R4. A law of composition $\bullet : R_N(X_N) \times R_N(X_N) \to R_N(X_N)$ is defined, and $(R_N(X_N), \bullet)$ is a commutative group. In addition, the following relation holds.

$$(x', y \bullet r) \in R_N$$

R5. There is a polynomial time algorithm that, given N, x, and x', outputs some $x^* \in domR_N$ such that $(x^*, r^{-1}) \in R_N$.

In the conditions for *CRSR* in Definition 2, R1-R3 are the same as those for *random self-reducible (RSR)* shown in [TW], but R4 and R5 are added. In CRSR, $r \in R_N(X_N)$ replaces $r \in \{0,1\}^\omega$ from RSR. Therefore, the set of CRSR relations is a subset of RSR relations.

Example 1. Let a function $f_N : Y \to X$ as follows:

(1) Laws of composition $* : X \times X \to X$ and $\circ : Y \times Y \to Y$ are defined, and $(X, *)$, $(Y, \circ)$ are commutative groups.

(2) f_N is homomorphic. That is,

$$f_N(y_1 \circ y_2) = f_N(y_1) * f_N(y_2),$$

where $y_1, y_2 \in Y$.

(3) f_N is regular. Here, f_N is regular [GKL] if there exists a function $m(\cdot)$ such that for every $x \in X$ the cardinality of $R_N(x)$ equals $m(|x|)$, where $R_N(x) = \{y \mid f_N(y) = x \in X, y \in Y\}$.

(4) For any $y \in Y$, if r is randomly and uniformly chosen on Y, then $y * r$ is uniformly distributed over Y.
(5) There are polynomial time algorithms to compute laws of composition $*$ and $\circ$, and to take inverses of these groups.

Then, the relation R is commutative random self-reducible, if

$$(x, f_N(x)) \in R_N,$$

$$domX_N = X,$$

$$R_N(X_N) = Y,$$

$$A(N, x, r) = x * f_N(r)$$

Example 2. The following three examples E1, E2, and E3 are random self-reducible. Among them, E1 and E2 are commutative random self-reducible, because they are included in Example 1. However, E3 is not commutative random self-reducible, because commutativity of a group for the condition R4 does not hold.

E1 (square roots mod$N$).

$$(x = y^2 \bmod N, y) \in R_N,$$

$$A(N, x, r) = r^2 x \bmod N.$$

E2 (discrete logarithms).

$$(x = a^y \bmod p, y) \in R_{(p,a)},$$

$$A((p, a), x, r) = a^r x \bmod p.$$

E3 (graph isomorphism).

$$(G' = \pi(G), \pi) \in R_G,$$

$$A(G, G', \phi) = \phi(G'),$$

where G and G' are graphs, and $\pi : G \to G'$ and $\phi : G' \to G$" are isomorphic transformations on graphs.

The following proposition is a collorary of Theorem 4 in [TW].

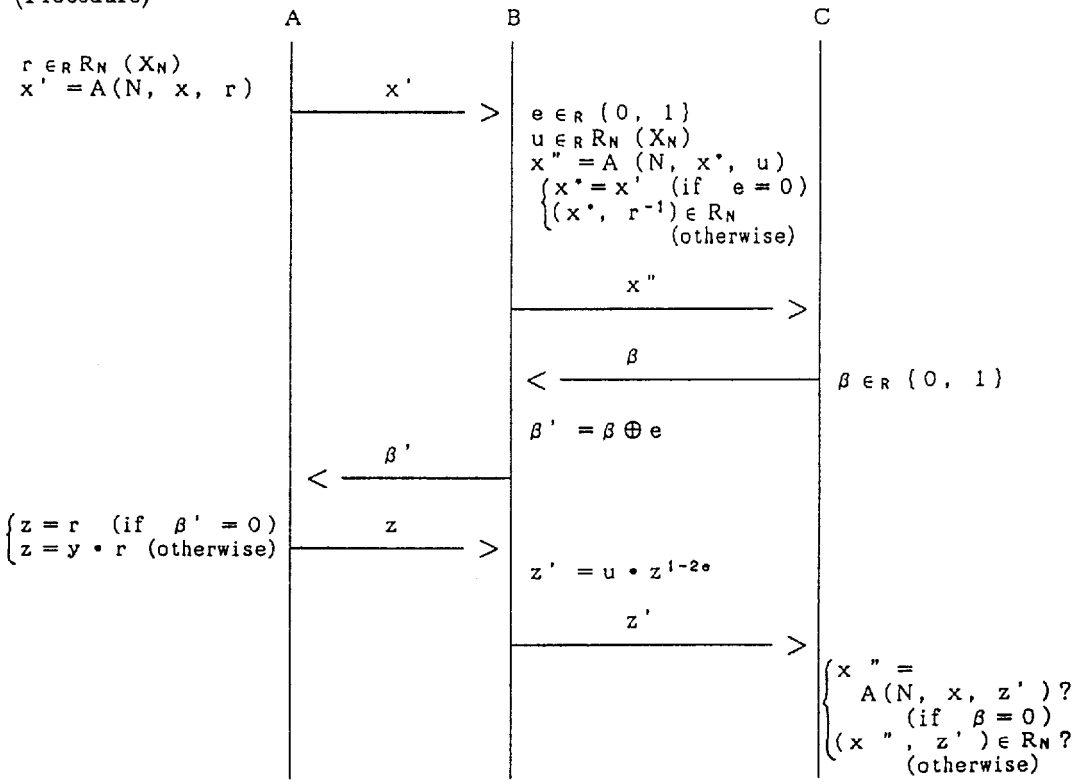
Proposition 1. On inputs N and x, there is a polynomial time perfect zero knowledge interactive proof that the prover can compute some y satisfying $(x, y) \in R_N$, if R satisfies the following conditions:

T0 R is CRSR.
T1 There is a probabilistic polynomial time algorithm that, given N, x', and y', determines whether $(x', y') \in R_N$.
T2 There is a probabilistic polynomial time algorithm that, given N, outputs random pairs $(x', y') \in R_N$ with x' uniformly distributed over $domR_N$ and y' uniformly distributed over $R_N(x')$.

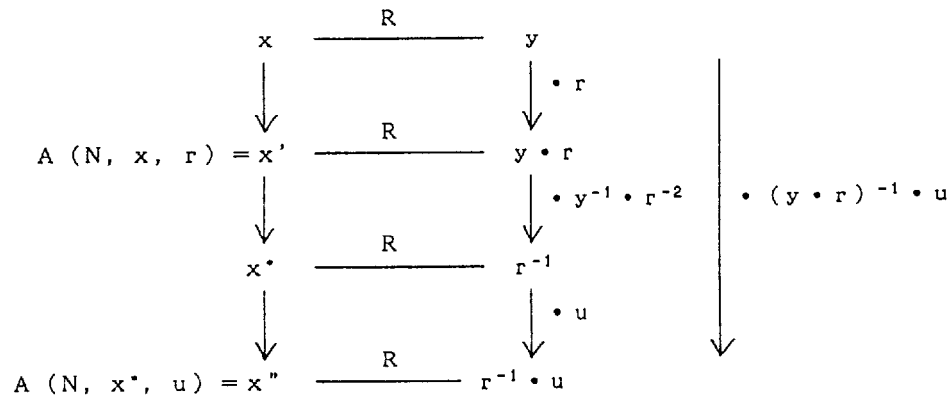
Theorem 1. Let the relation R be CRSR and satisfy T1 and T2. Then, on inputs N and x, there is a polynomial time divertible perfect zero knowledge interactive proof (A, B, C) that the prover can compute some y satisfying $(x, y) \in R_N$.

Proof Sketch:
We start by describing a construction of divertible perfect zero knowledge interactive proof (A, B, C) that the prover can compute some y satisfying $(x, y) \in R_N$.

Construction: On inputs N and x, the (A, B, C) procedure is as follows.
The following procedure is repeated $t = O(|N|)$ times, where $x \in_R X$ denotes that x is uniformly and randomly chosen on X.
(Procedure)



(Relationship among variables when $e = 1$)



Correctness: Clearly, this construction satisfies conditions (i), (ii), and (iii) of Definition 1. Thus, we will show that the construction satisfies condition (iv). First, since e is uniformly and randomly chosen on $\{0,1\}$, then β' is uniformly distributed over $\{0,1\}$ independent from β. Since u is uniformly and randomly chosen on $R_N(X_N)$, then, from condition $R1$ of Definition 2, x" is uniformly distributed over $R_N(X_N)$ independent from x'. In addition, from condition $R3$ of Definition 2, z' is uniformly distributed over a set $Z' = \{z' \mid z' \text{ is validly verified by } C\}$. Thus, the construction satisfies condition (iv) of Definition 1. **QED**

The parallel version of the divertible zero knowledge interactive proof can be constructed in manners similar to those of the Fiat-Shamir scheme [FS, FFS]. (Here, its parallel version is not a zero knowledge interactive proof, but it has been proven to reveal no useful knowledge [FFS, OO, Ok].

3.2 Divertible zero knowledge interactive proof for digital signatures

An application to digital signatures of zero knowledge interactive proofs is shown in [FS, MS, GQ2, OO]. In this section, a blind digital signatures scheme is shown based on the divertible zero knowledge interactive proofs.

Definition 3. An interactive couple of Turing machines (A, B) is a *divertible (computational/perfect)* zero knowledge interactive proof for digital signatures, if the following conditions hold.

(i) (A, B) is a parallel version of (computational/perfect) zero knowledge interactive proof that the prover can compute some y satisfying $(x, y) \in R$.

(ii) B^A outputs a digital signature z of m based on the (computational/perfect) zero knowledge interactive proof with respect to $(x, y) \in R$, where m is a message chosen by B.

(iii) Only A can compute some y satisfying $(x, y) \in R$.

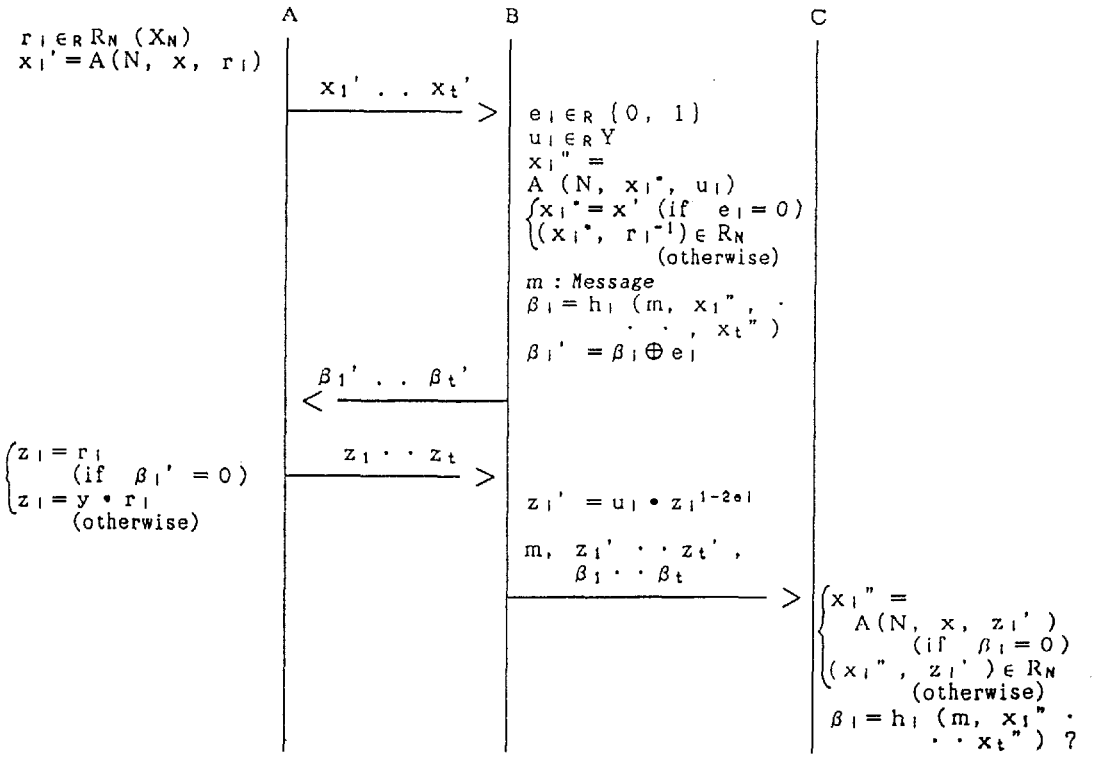
(iv) For any message m chosen by any party, any prover A^* accepted by a valid verifier C, and any string s, $((\underline{A^*(y,s)},B(m))(x)$, $Z(B^{A^*(y,s)})(m,x))$ and $((\underline{A^*(y,s)},C)(x)$, $Z(A(y))(m,x))$ are (polynomially indistinguishable/equivalent), where A is a valid generator of digital signatures based on the (computational/perfect) zero knowledge interactive proofs with respect to $(x, y) \in R$. $Z(T)(m, x)$ denotes the probability space that assigns to the signature z the probability that T outputs z, on input x and m.

Theorem 2. On inputs N and x, there is a polynomial time divertible perfect zero knowledge interactive proof for digital signatures (A, B) that the prover can compute some y satisfying $(x, y) \in R_N$, if the relation R is CRSR and satisfies T1 and T2'.

T2' There is a probabilistic polynomial time algorithm that, on input y', outputs x' satisfying $(x', y') \in R_N$. If, in addition, y' is randomly and uniformly chosen on $R_N(X_N)$, then x' is uniformly distributed on $domR_N$.

Proof Sketch:

Construction. On inputs N and x, the procedure of (A, B) is as follows.



Correctness. It can be proven in a manner similar to the proof of Theorem 1 that this construction satisfies conditions (i)-(iv) of Definition 3. **QED.**

Note: When we replace β_i by $x"_i$ $(i = 1, \ldots, t)$ as a part of signature information of m, we do not need to replace condition $T2$ by $T2'$.

4. Practical implementation of divertible zero knowledge interactive proofs

Some practical protocols such as multi-key version and higher degree version [C3, FS, FFS, GQ, OO, Oh1] have been proposed based on a basic zero knowledge proof protocol for quadratic residuosity [GMR] or discrete logarithm problem.

In this section, we show that a specific class of CRSR problems, *endomorphic CRSR (ECRSR)* problems, has multi-keys and higher degree version divertible zero knowledge interactive proofs.

Definition 4. For any $N \in \mathcal{N}$, let X_N be a finite set, and $R_N \subseteq X_N \times X_N$ be a relation. R is *endomorphic commutative random self-reducible (ECRSR)* if

(1) A law of composition $\bullet : X_N \times X_N \to X_N$ is defined, and $(X, \bullet)$ is a commutative group.

(2) $(x = y^L, y) \in R_N$, where $x \in X_N$, $y \in X_N$, L is an integer, and

$$y^L = \overbrace{y \bullet \cdots \bullet y}^{L \text{ times}}.$$

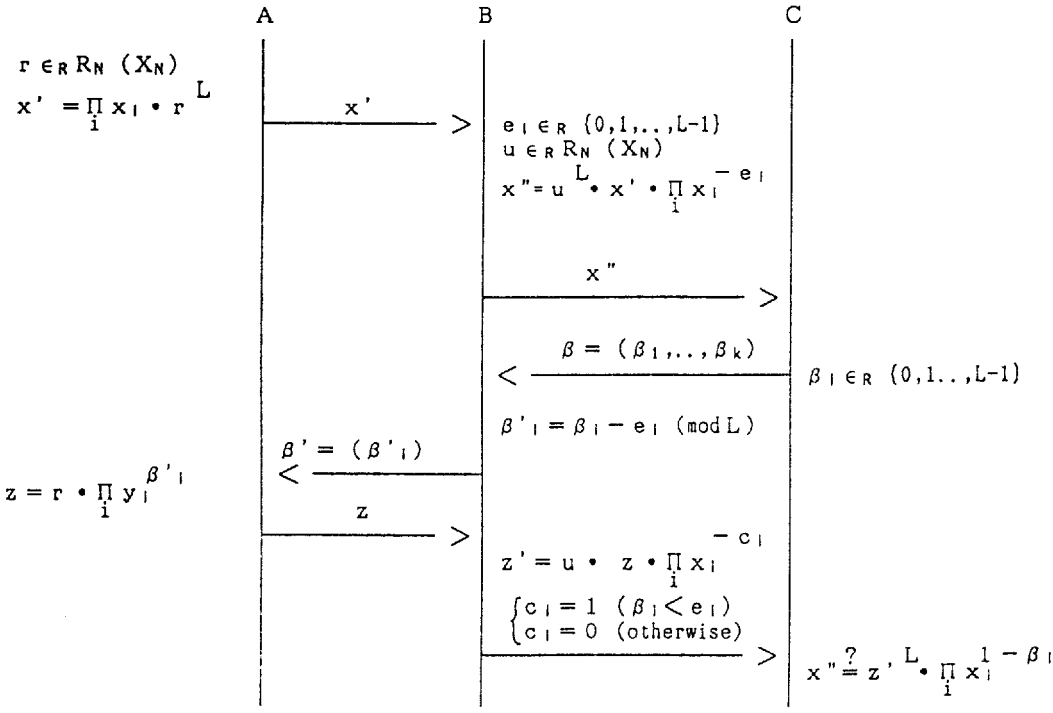
(3) There exists a function $m(\cdot)$ such that for every $x \in domR_N$ the cardinality of $R_N(x)$ equals $m(|N|)$.

(4) For any $y \in X_N$, if r is randomly and uniformly chosen on X_N, then $y \bullet r$ is uniformly distributed over X_N.

(5) There are polynomial time algorithms to compute the law of composition $\bullet$, and to take inverse of this group.

Here, using ECRSR relations, we show a protocol that is a divertible zero knowledge interactive proof with multi-keys and higher degree.

Protocol (multi-keys and higher degree version divertible zero knowledge interactive proof) On inputs N, L and $x_1, x_2, \ldots, x_k$, the following procedure is repeated $t = O(|N|)$ times.



Theorem 3. If the relation R is ECRSR, then this protocol is a polynomial time divertible perfect zero knowledge interactive proof that the prover can compute some y_i satisfying $(x_i, y_i) \in R_N$ for all $i \in \{1, 2, \ldots, k\}$.

Notes:
(1) Variations of this protocol are shown in Appendix B, which are based on the Fiat-Shamir type protocol (Appendix A).
(2) When $t = 1, k \cdot |L| = O(|N|)$, this protocol has not been proven to be zero knowledge, however, it has been proven to reveal no useful knowledge [FFS, OO, Ok].
(3) By combining the ideas shown in Section 3.2 and this section, we can easily construct multi-keys and higher degree version divertible perfect zero knowledge interactive proofs for digital signatures.

5. Applications

In this section, the positive properties of divertible zero knowledge interactive proofs are shown. They can be useful for electronic checking and secret electronic balloting. In these applications, divertible zero knowledge interactive proofs for digital signatures shown in Section 3.2 are used as follows:

(1) After authority A checks the identity of member B, A gives B his digital signature on a message made by B through the zero knowledge interactive proofs between A and B. However, A cannot see his own signature or the message that he signs. That is, A makes a blind signature.
(2) B presents A's signature on B's messsage to a verifier C. C checks whether the message was signed by A. However, C cannot determine who made the message.
(3) Even if A and C are colluding with each other, they cannot know who made B's message with A's signature. This is because there is no information that shows the relationship between the A-B interaction for the generation of A's signature and B's message with A's signature.

When the above-described digital signature protocol is used for an electronic checking protocol, A is a banker, B a customer and C the owner of a shop. A gives B a check, after A checks the identity of B. B uses the check at C's shop, where C checks the validity of the check. Even if A and C are in collusion with each other, they cannot know who used the check at C's shop. This protocol is useful for privacy protection regarding this customer's activities.

On the other hand, when this digital signature protocol is used for a secret ballot, A is a ballot publisher, B a voter, and C a ballot counter. After A checks the validity of B based on voter registration records, A signs (stamps) the outside of an unopened envelope that contains a ballot for B and a facing piece of carbon paper. B takes B's ballot with the carbon image of A's signature out of the envelope, and sends it to C. C counts it, after C checks the validity of the carbon image of the signature on the ballot. Even if A and C are in collusion with each other, they cannot know whose ballot it is. Therefore, the privacy of each voter is guaranteed.

The above check protocol and secret ballot protocol were proposed in [C1, C2, Oh2]. However, the digital signatures used in these protocols are the RSA scheme or an RSA-like

scheme. Hence, these protocols are not provably secure and are not efficient. In contrast, when divertible zero knowledge interactive proofs for digital signatures are used for these protocols, they are provably secure under some conditions and are efficient if square root mod$N$ is adopted as a proof problem.

6. Abuses and the protective measures

In this section, we turn to the negative side of divertible zero knowledge interactive proofs. We show some abuses and a number of measures to counter them.

6.1 Abuses

(1) Identification based on divertible zero knowledge interactive proofs

Let us explain our abuse by using an example similar to that shown in [DGB]. A(lice) identifies herself to B(ob). B impersonates A and claims to be A. Then, C(harlie) checks the identity of B who is claiming to be A. Even if A and C are aware of the abuse, they cannot obtain any evidence but the relationship between the time when A claimed to be A and that B claimed to be A. To make it easier understand, we assume B and C are the owners of a restaurant and a jewelry shop with electronics payment respectively, where customers can pay electronically. A is a customer of B's restaurant. At the moment that A is ready to pay and to prove her identity to B, B determines to buy an expensive thing at C's shop, and C is starting to check B's (in fact A's) identity. While C is checking the identity of B, B is checking the identity of A, where the interaction between A and B is affected by the interaction between B and C and vice-versa. In this abuse, B leaves no evidence that proves the relationship between the A-B interaction and the B-C interaction.

(2) Digital signatures based on divertible zero knowledge interactive proofs

By using the divertible zero knowledge interactive proof, we can construct an abuse of digital signatures, as described below.

A identifies herself to B. B tries to forge A's signature on any message made by B. Then, C checks the validity of the forged signature, which , B is claiming, was generated by A. Even if A and C are aware of the abuse, they cannot obtain evidence of it. For illustrative purposes, consider an example similar to that in (1). B is a shop owner, and C is a banker. A is a customer of B's shop. While B is checking the identity of A, B is forging A's signature on a promissory note to C's bank written by B. Here, B's interaction with A is determined according to the promissory note. In this abuse, B leaves no evidence which proves the relationship between the A-B interaction and the signature message forged by B.

6.2 Protective measures

Here, we show two types of measures to protect against the above-described abuses; operational measures and algorithmic measures. Note that in the applications shown in Section 5, only operational measures can be used to counter these abuses, because algorithmic measures cannot used without losing the positive properties of divertible zero knowledge interactive proofs.

(1) Operational measures

Regarding the abuse in identification, essentially there is no operational protective measure except using a unique physical description as mentioned in [DGB]. In order to protect against the abuse in digital signatures, using a key for digital signatures different from that for identification is effective. Then, even if a forged signature message from Alice is made by Bob through the abuse described in Section 6.1, she can claim that the signature is invalid, although it is valid with respect to her identification key.

(2) Algorithmic measures

For these divertible perfect zero knowledge interactive proofs, it is essential that a verifier can determine the values of random bits to be sent to a verifier. Therefore, there are algorithmic measures in which the values are not determined by only the verifier. Two measures are shown in the following.

(i) Measure 1

In the first measure, the values of random bits to be sent from a verifier to a prover are determined by the cooperation of the verifier and the prover. Here, the values cannot be controlled by either the prover alone or the verifier alone. A coin flipping protocol for two persons has been shown in [B, BL]. In this measure, the previous perfect zero knowledge interactive proofs are used, replacing the verifier's coin flips with two people's coin flips. The other procedures in the divertible perfect zero knowledge interactive proofs are the same.

(ii) Measure 2

Recently, non-interactive zero knowledge proofs have been proposed [BFM, DMP]. In these zero knowledge proofs, the prover and verifier share common random bits before the prover starts the proofs. Therefore, these proofs are algorithmic measures to protect against this abuse, because the common random bits are not determined only by the verifier.

7. Open problems

Many problems regarding the divertible zero knowledge interactive proofs remain open. Here, we introduce some typical ones:

(1) What class of relations has divertible zero knowledge interactive proofs except CRSR relations? (Do all NP relations have divertible zero knowledge interactive proofs?)

(2) What class of relations has divertible *perfect* zero knowledge interactive proofs except CRSR relations? (Do all RSR relations have divertible perfect zero knowledge interactive proofs?)

(3) What class of relations has *multi-keys or higher degree version* divertible zero knowledge interactive proofs except ECRSR relations? (Do all CRSR relations have multi-keys or higher degree version divertible zero knowledge interactive proofs?)

Acknowledgements: The authors would like to thank Prof. Adi Shamir for his valuable suggestions, especially on the formal definition of divertible zero knowledge interactive proofs. They would also like to thank Prof. Yvo Desmedt for informing them of the related protocols in [DGB].

References

[AFK] M.Abadi, J.Feigenbaum and J.Kilian, "On Hiding Information from an Oracle," STOC pp.195-203 (1987)

[AL] D.Angluin and D.Lichtenstein, "Provable Security of Cryptosystems: a Survey," Technical Report TR-288, Yale University (1983)

[B] M.Blum, "Coin Flipping by Telephone: A Protocol for Solving Impossible Problems," Compcon, pp133-137 (1982)

[BFM] M.Blum, P.Feldman and S.Micali, "Non-Interactive Zero-Knowledge and Its Applications," STOC, pp.103-112 (1988)

[BL] M.Ben-Or and N.Linial, "Collective Coin Flipping, Robust Voting Schemes and Minima of Banzhaf Values," FOCS, pp.408-416 (1985)

[C1] D.Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," Comm. of the ACM, 28, 10, pp.1030-1044 (1985)

[C2] D.Chaum, "Blinding for Unanticipated Signatures," Eurocrypto'87 (1987)

[C3] D.Chaum, "An Improved Protocol for Demonstrating Possession of Discrete Logarithms and Some Generalizations," Eurocrypto'87 (1987)

[Da] I.B.Damgård, "Payment Systems and Credential Mechanisms with Provable Security against Abuse by Individuals," Crypto'88 (1988)

[De] Y.Desmedt, "Subliminal-Free Authentication and Signature," Eurocrypto'88 (1988)

[DGB] Y.Desmedt, C.Goutier and S.Bengio, "Special Uses and Abuses of the Fiat-Shamir Passport Protocol," Crypto'87 (1987)

[DMP] A.DeSantis, S.Micali and G.Persiano, "Non-Interactive Zero-Knowledge Proof Systems," Crypto'87 (1987)

[FFS] U.Feige, A.Fiat and A.Shamir, "Zero Knowledge Proofs of Identity," STOC, pp.210-217 (1987)

[FS] A.Fiat and A.Shamir, "How to Prove Yourself," Crypto'86 (1986)

[GKL] O.Goldreich, H.Krawczyk, and M.Luby, "On the Exixtence of Pseudorandom Generators," Crypto'88 (1988)

[GMR] S.Goldwasser, S.Micali, and C.Rackoff, "Knowledge Complexity of Interactive Proofs," STOC, pp291-304 (1985)

[GMW] O.Goldreich, S.Micali, and A.Wigderson, "Proofs that Yield Nothing But their Validity and a Methodology of Cryptographic Protocol Design," FOCS, pp.174-187 (1986)

[GoMiRi] S.Goldwasser, S.Micali, and R.Rivest, "A Paradoxical Solution to the Signature Problem," FOCS, pp.441-448 (1984)

[GQ1] L.C.Guillou, and J.J.Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessors Minimizing Both Transmission and Memory," Eurocrypto'88 (1988)

[GQ2] L.C.Guillou, and J.J.Quisquater, "A "Paradoxical" Identity-Based Signature Scheme Resulting from Zero-Knowledge," Crypto'88 (1988)

[MS] S.Micali, and A.Shamir, "An Improvement of The Fiat-Shamir Identification and Signature Scheme," Crypto'88 (1988)

[Oh1] K.Ohta, "Efficient Identification and Signature Schemes," Electronics Letters, 24, 2, pp.115-116 (1988)

[Oh2] K.Ohta, "An Electrical Voting Scheme Using a Single Administrator" (in Japanese), Spring Conference of IEICE Japan, A-294 (1988)

[Ok] T.Okamoto "Proofs that Release No Use Knowledge and Their Applications," to appear

[OO] K.Ohta, and T.Okamoto "A Modification of the Fiat-Shamir Scheme," Crypto'88 (1988)

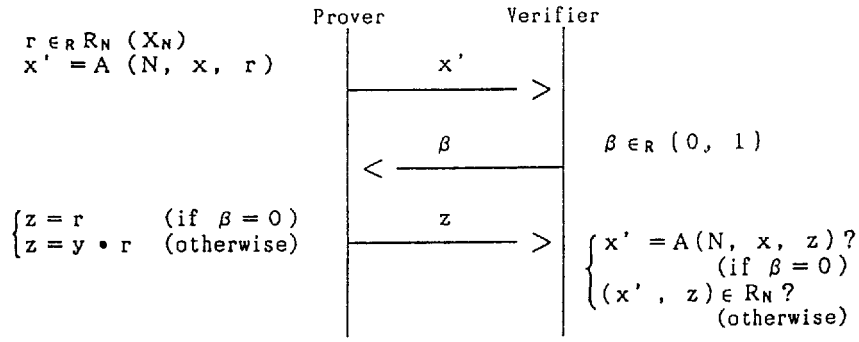
[S] A.Shamir, Private Communication (1988)

[TW] M.Tompa and H.Woll, "Random Self-Reducibility and Zero Knowledge Interactive Proofs of Possession of Information," FOCS, pp472-482 (1987)

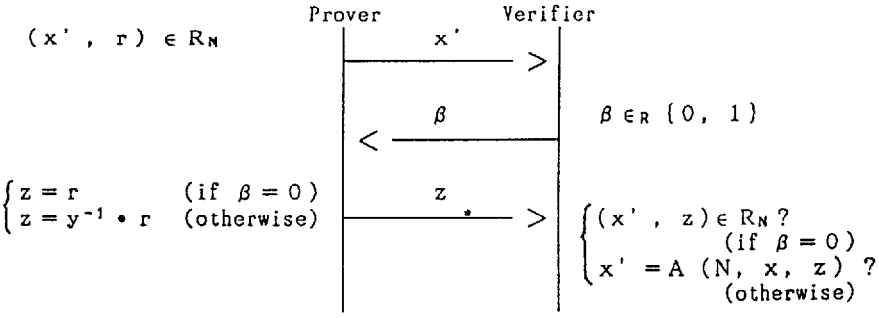
Appendix A

In this appendix, we show two types of perfect zero knowledge interactive proofs based on the commmutative-random self-reducible relation. One is the Tompa-Woll type [TW], and the other is the Fiat-Shamir type. Although all of the protocols shown in this paper are based on the Tompa-Woll type, we can construct similar protocols based on the Fiat-Shamir type, including the multi-keys and higher degree versions (Appendix B).

(Tompa-Woll type)



(Fiat-Shamir type)



Appendix B

In this appendix, we show some protocols of divertible zero knowledge interactive proofs based on the Fiat-Shamir type (Appendix A), including the multi-keys and higher degree versions.

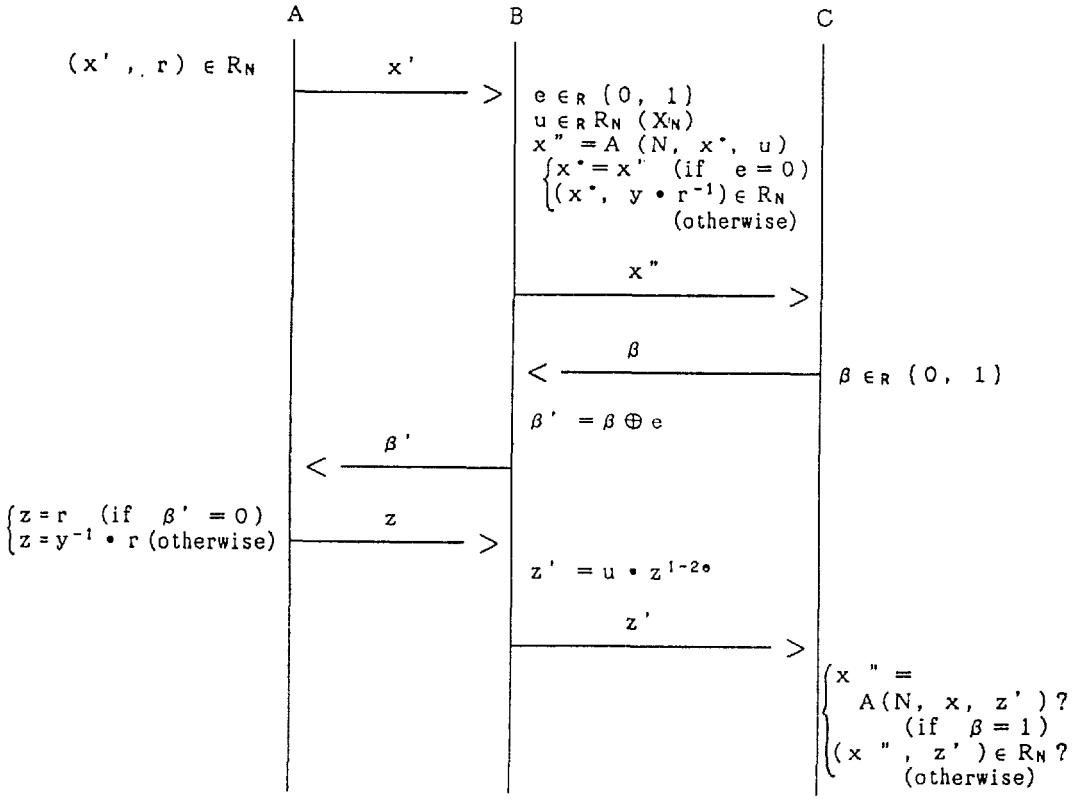
Protocol B1 is the Fiat-Shamir type of the protocol shown in the proof of Theorem 1 (basic version). In this protocol, we must replace condition R5 with R5' shown as follows:

R5'. There is a polynomial time algorithm that, given N, x, and x', outputs some $x^* \in dom R_N$ such that $(x^*, y \bullet r^{-1}) \in R_N$.

Protocol B2 is the Fiat-Shamir type of the protocol shown in Section 4 (multi-keys and higher degree version). The protocol described in [DGB] as a subliminal-channel-free identification system based on the Fiat-Shamir scheme corresponds to the quadratic version of Protocol B2.

(Protocol B1)

On inputs N and x, the following procedure is repeated $t = O(|N|)$ times.



(Protocol B2)

On inputs N, L and $x_1, x_2, \ldots, x_k$, the following procedure is repeated t times.

Note: We can replace $x'' = u^L \bullet x' \bullet \prod_i x_i^{-e_i}$, $z = r \bullet \prod_i y_i^{-\beta'_i}$, $z' = u \bullet z \bullet \prod_i x_i^{-c_i}$, and $x'' = z'^L \bullet \prod_i x_i^{\beta_i}$ with $x'' = u^L \bullet x' \bullet \prod_i x_i^{e_i}$, $z = r \bullet \prod_i y_i^{\beta'_i}$, $z' = u \bullet z \bullet \prod_i x_i^{e_i}$, and $x'' = z'^L \bullet \prod_i x_i^{-\beta_i}$.