Parallel Divertibility of Proofs of Knowledge

(Extended Abstract)

L. Chen, I. B. Damgård and T. P. Pedersen*

Aarhus University, Denmark

Abstract. An interactive proof is transferred if a person, while interacting with the prover, convinces a (second) verifier of the statement. Divertible proof systems, first introduced by Desmedt et al., offer a more subtle way of transferring a proof: the messages are blinded such that neither the prover nor the second verifier can ever discover what is going on. While the ability to transfer (and divert) interactive proofs is useful in many situations it also has the disadvantage that the prover has less control over the use of the proofs. This paper investigates (and limits) the possibilities of transferring and diverting certain interactive proofs. In particular it is shown that zero-knowledge proof systems based on a polynomial number of sequential iterations of a three-move protocol cannot be transferred (and hence diverted) to two independent third parties even with just a very small (polynomial fraction) probability of success unless the proof is insecure for the prover. Furthermore, if the three move protocol in itself constitutes a witness hiding proof of knowledge it is shown that it cannot be diverted to two independent third parties simultaneously with overwhelming probability. This result rules out one possible attack on the blind signature scheme suggested by Ohta and Okamoto.

1 Introduction

Even though the prover in zero-knowledge proofs (see [GMR89]) does not reveal any information but the validity of the claim, the receiver (verifier) can easily transfer such proofs to another person online. This observation was used in [DGB88] to construct a so called mafia fraud against the Fiat-Shamir identification scheme ([FS87]). [DGB88] also showed how a warden by modifying (blinding) the messages sent forth and back between prover and verifier in this scheme can prevent these two persons from using it as a subliminal channel (see [Sim84]). Later, in [OO90], this was generalized to interactive proofs of knowledge (see [FFS88] and [TW87]), and the term "divertible interactive proofs" was adopted. For historical reasons the intermediary was still called a warden. Hence, a divertible proof system constitutes a three-party protocol involving the prover, P, the warden, W and the verifier V as illustrated in Figure 1.

[OO90] presented divertible proofs of knowledge for commutative, randomly self-reducible languages (a restriction of the class of randomly self-reducible languages including quadratic residuosity and group membership but excluding

* Funded by Carlsbergfondet

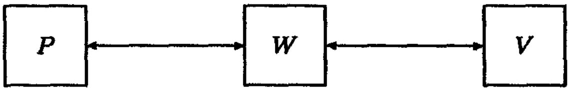

Fig. 1. Transferring a proof on-line.

graph isomorphism, see also [TW87]). These interactive proofs are also proofs of language membership and the divertible protocols work in that case as well with the notable difference that for the proofs of knowledge both warden and verifier are convinced, whereas in the proof of membership the warden is only convinced under a computational assumption (and the verifier unconditionally).

However, this does not mean that the warden in general cannot be convinced unconditionally in divertible proofs of membership: In Section 8 a two round (four move) divertible, perfect zero-knowledge proof of membership is presented in which both warden and verifier are convinced unconditionally.

Further work on divertible proofs in [BD91] has resulted in divertible proofs for graph isomorphism and (given a probabilistic encryption homomorphism) for every language in *NP* (more precisely for SAT). Recently, [ISS93] constructed divertible proofs for graph non-isomorphism and a general protocol for every language in *IP*. However, these constructions seem to use a weaker definition of divertibility, and furthermore, the result for *IP* allows the verifier to send information to the necessarily unbounded prover.

All divertible proofs in [DGB88], [OO90] and [BD91] deal with specific instances of a three move protocol in which on common input x, the prover sends the first and the third message, while the message from the verifier is a random challenge from a finite set E (this protocol may be repeated in order to constitute a proof system). The prover is either convincing the verifier that the common input, x, belongs to some given language, or that he knows a witness w such that $\mathcal{P}(x, w) = 1$, where $\mathcal{P}$ is a poly-time predicate.

The Fiat-Shamir identification protocol, for example, which was considered in [DGB88] consists of t sequential iterations of the basic protocol with $E = \{0,1\}^k$, while the signature scheme is based on a single iteration with $E = \{0,1\}^{tk}$, where t and k are security parameters.

While the ability to divert zero-knowledge proofs is very useful (e.g., to construct blind signatures and prevent subliminal channels), it also has the effect that the prover can never be sure who will be convinced by his proof. Thus the prover loses control over his proof. It is therefore important to investigate to which extent it is possible to transfer and divert interactive proofs.

The primary goal of this paper is to do this for the basic protocol described above when used in proofs of knowledge. It will be assumed that the protocol is secure for the prover in the sense that a polynomially bounded verifier cannot find a witness after a single execution (it is witness hiding, see [FS90][2]). This notion of security comprises all zero-knowledge protocols ([GMR89]).

[2] This is only defined for proofs of knowledge, but it extends to any protocol in which the prover's secret input and the common input satisfy a poly-time predicate.

First we consider the case where the cardinality of E is polynomial in $|x|$ and the protocol is repeated a polynomial number of times (e.g., resulting in a zero-knowledge proof). If a witness can be computed from the replies to two different challenges (see Property I in Section 4), it is shown that the warden cannot *transfer* the proof to two verifiers and succeed with non-negligible probability. This remains true if Property I is weakened (see Section 4.2). Next, if the cardinality of E is super-polynomial in $|x|$ (e.g., in parallel executions of the basic protocol), it is shown that the warden cannot *divert* the proof to two independent verifiers and succeed with "overwhelming probability". This second result can be used to rule out a possible attack on the blind signature scheme suggested in [OO90].

The paper is organized as follows. Section 2 introduces parallel divertibility and Section 3 the notation. The following two sections contain the main results: Section 4 for polynomially small challenge set, E, and Section 5 for larger challenge sets. Then the application to blind signatures and some extensions are described. Section 8 presents a divertible proof of language membership in which both warden and verifier are convinced unconditionally. Due to space limitations the proofs in this paper are only sketched. The complete proofs can be found in [Che94].

2 Transferability and Divertibility

This section first defines parallel transferability and divertibility and then it is shown that the ability to transfer (and hence divert) a proof can be decreased by repeating the protocol. Each participant will formally be modeled by an interactive, probabilistic (poly-time) Turing machine (see [GMR89]).

Divertible proofs of knowledge were defined formally in [OO90]. In the following this definition is extended to divertibility to many verifiers. First, however, the notion of *parallel transferability* is needed. Here, W is trying to transfer the proof to many verifiers, $V_1, V_2, \ldots, V_n$ ($n \in \mathbb{N}$) given only one interaction with P (see Figure 2). Thus $(n+1)$ pairwise protocols are involved. Extending [OO90], denote by $(P, W^{V_1,\ldots,V_n})$ the two party protocol between prover and warden, and by (W^P, V_i) that between warden and the i'th verifier ($i = 1, 2, \ldots, n$).

Definition 1. Let (P, V) denote a two-party protocol in which V ends up in one of two possible states: accept or reject. A (poly-time) warden W is said to n-transfer such a protocol with probability π, if the following holds. Let $V_1, \ldots, V_n$ denote the n verifiers and let the common input to $P, W, V_1, \ldots, V_n$ be denoted by x. Whenever P runs his part of (P, V) correctly (perhaps given an auxiliary input) and all V_i's run the protocol of V independently, each V_i will accept with probability at least $\pi(x)$ over the random coins of P, W and V_i.

- W is said to n-transfer a protocol if for every $c > 0$ and for $|x|$ sufficiently large $\pi(x) \geq 1 - |x|^{-c}$.
- W is said to weakly n-transfer the protocol if $\pi(x) \geq |x|^{-c}$ for some $c > 0$ and $|x|$ sufficiently large.

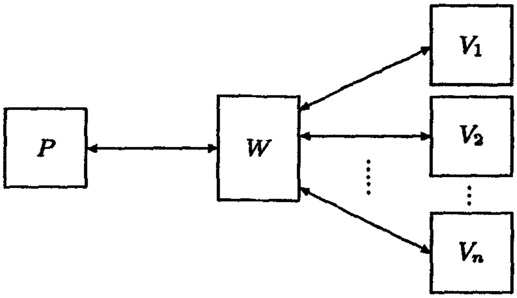

Fig. 2. Parallel transferability.

- The protocol (P, V) is called (weakly) n-transferable if there is a polynomial time warden, W, which (weakly) n-transfers it.

This definition encompasses "proof-systems", which satisfy completeness but not necessarily soundness. Every such proof is 1-transferable, because the warden can just forward P's messages to V and vice versa.

In a divertible proof the warden hides the relation between the messages, which the prover and the verifiers see — even if these deviate from the protocol. However, it will be required that the prover is able to send correct answers to the warden (it is not reasonable to expect the warden to transfer a proof, if he does not receive one).

Thus the notion of *view* is needed (see [GMR89]). Let A denote a possibly cheating participant having secret input s. Then $view_{A,B}(x, s)$ denotes the random coins used by A and the messages, which A receives during an execution of a two-party protocol with B on common input, x. Furthermore, $View_{A,B}(x, s)$ is the corresponding random variable whose distribution is induced by the random coins of B.

Definition 2. Let (P, V) be a proof of knowledge. (P, V) is said to be n-divertible if there is a polynomial time warden, W, such that

1. W n-transfers (P, V);
2. For any prover $\tilde{P}$ and any n verifiers $\tilde{V}_i$ $(i = 1, 2, \ldots, n)$ for which there is a $c > 0$ such that for $|x|$ sufficiently large $\tilde{P}$ convinces an honest verifier in (P, V) with probability at least $1 - |x|^{-c}$ the following holds:

$$(View_{\tilde{P},W}(x, s), View_{\tilde{V}_1,W}(x, s_1), \ldots, View_{\tilde{V}_n,W}(x, s_n))$$

has the same distribution as

$$(View_{\tilde{P},V}(x, s), View_{\tilde{V}_1,P}(x, s_1), \ldots, View_{\tilde{V}_n,P}(x, s_n))$$

for $|x|$ sufficiently large.

Using [GMR89], this definition extends to statistical and computational n-divertibility (however, in the case of computational n-divertibility the cheating provers and verifiers must be polynomially bounded).

The definition puts no restraints on the order of the messages which W sends to the n verifiers. For example, in one extreme, W first diverts the proof to V_1 and then, afterwards, to V_2 and so forth. In an other extreme W computes the messages to V_i depending on the messages from not only P, but the other verifiers as well.

Furthermore, it is an immediate consequence of the definitions that if a proof cannot be transferred then it cannot be diverted.

The following proposition shows that sequential iterations of a protocol can decrease the warden's chances of being successful.

Proposition 3. *Let (P, V) be an accept/reject protocol as in Definition 1, and let (P', V') denote the protocol consisting of K sequential iterations. Let $n \in \mathbb{N}$. If there is a warden which can n-transfer (P', V') with probability $p(k)$ on input x of length k, then there is a warden which after executing (P, V) with the prover expected $O(K/p(k))$ times can n-transfer (P, V) with probability at least $p(k)^{1/K}$.*

Furthermore, if (P, V) is zero-knowledge these initial iterations are not necessary.

3 Notation for the Protocols

As mentioned in the introduction, this paper only deals with three move proofs of knowledge of the poly-time predicate, $\mathcal{P}$. On common input x the prover has an auxiliary input, w, satisfying $\mathcal{P}(x, w) = 1$. The prover initially sends the message, a, to the verifier, and given the challenge $c \in E$ the prover sends the reply r. The verifier will accept if $p(x, a, c, r) = 1$, where p is a poly-time predicate.

The literature contains many examples of such three round protocols (e.g. the Fiat-Shamir scheme, proofs for graph isomorphism, group membership, equality of discrete logarithms, quadratic residuosity, see [FFS88, TW87, CEvdG87]).

The length of the common input, x, will often be denoted by k and called the security parameter. If $|E|$ is polynomial in k the basic protocol is usually repeated t times, where t is polynomial in k in order to obtain a proof system[3]. If these iterations are sequential, the resulting proof can be zero-knowledge, and if they are in parallel it is sometimes possible to obtain a witness-hiding proof (see [FS90]).

3.1 Transferring the Basic Protocol

As previously mentioned a warden can transfer proofs by just forwarding the messages between P and V. However, as the warden generally has many other possibilities the messages between W and V will be denoted by a_1, c_1 and r_1.

[3] $|S|$ denotes the cardinality of the finite set S.

Thus, the warden sends a_1 and r_1 to V and c to P. If ρ denotes the random bits of the warden, these messages are computed as

$$a_1 = f(x, a, \rho), \qquad c = g(x, a, c_1, \rho) \qquad \text{and} \qquad r_1 = h(x, a, c_1, r, \rho),$$

where f, g and h are poly-time computable functions. When the protocol is iterated, the warden may also use information from previous rounds when computing these messages. This extra input is omitted in this paper as it only shows up in the proof of Proposition 3.

We shall often consider the set of challenges from the verifier for which the warden can answer correctly given a correct reply from the prover. In general, the prover might choose between several such replies and it could be that the warden can only use some of these. Thus the set of challenges which the warden can answer may depend on both a and r chosen by the prover and ρ. It will be denoted by $S_{\rho,a,r}$ (S for success, the common input x is omitted):

Definition 4. Given three functions f, g, h as above. Then

$$S_{\rho,a,r} = \{c_1 \in E \mid p(x, a, g(x, a, c_1, \rho), r) = 1 \wedge$$
$$p(x, f(x, a, \rho), c_1, h(x, a, c_1, r, \rho)) = 1\}.$$

When considering the possibility of transferring the basic protocol to two verifiers (V_1 and V_2) in parallel the messages to and from V_i are denoted by (a_i, c_i, r_i) for $i = 1, 2$ and the warden uses the functions f_1, f_2, g and h:

$$\begin{aligned} a_1 &= f_1(x, a, \rho) \\ a_2 &= f_2(x, a, c_1, \rho) \\ c &= g(x, a, c_1, c_2, \rho) \\ (r_1, r_2) &= h(x, a, c_1, c_2, r, \rho) \end{aligned}$$

We allow the warden to compute the initial value a_2 to V_2 depending on the challenge c_1 from V_1. This is necessary as it is unreasonable to require any synchronization between the two independent verifiers V_1 and V_2 (V_1 may not be aware that there is another verifier). We also require that W receives a challenge from both verifiers before computing the challenge, c, to P. This makes the warden most general as the function g can always ignore some of its inputs.

Alternatively, the warden could postpone computing a_2 until it has received r from the prover. But, then the warden would be able to prove knowledge of a witness (and hence knowing one) after one execution of the protocol with P.

4 Polynomial Size E

This section considers the situation, where E is small. The infeasibility of 2-transferring the protocol will first be shown under the assumption that from correct answers to two different challenges it is possible to find a witness:

Property I.
There exists a polynomial time Turing machine, M, which given (x, a, c, r, c', r') satisfying

$$p(x,a,c,r) = 1 \quad \text{and} \quad p(x,a,c',r') = 1 \quad \text{and} \quad c \neq c'$$

as input, outputs w' such that $\mathcal{P}(x,w') = 1$.

The protocols in [OO90] with $E = \{0,1\}$ and all protocols in [BD91] have this property. In section 4.2 this requirement will be relaxed.

4.1 The Basic Protocol Satisfies Property I

It will be shown that no warden can transfer the basic protocol to two verifiers and succeed for a large fraction of the possible challenges (Lemma 7). From this and Proposition 3 it follows that (zero-knowledge) proofs obtained by sequential iterations cannot be weakly 2-transferred (and hence, cannot be weakly n-transferred for $n \geq 2$). This is done in Theorem 8. We first need a lemma which links Property I to the following

Property II.
For any three functions (f, g, h) used by the warden to transfer the basic protocol to a single verifier the following holds. If for some $d > 0$ and k sufficiently large with probability at least k^{-d} there exist $c_1, c_1' \in S_{\rho,a,r}$ $(c_1 \neq c_1')$ such that

$$g(x,a,c_1,\rho) = g(x,a,c_1',\rho)$$

(the probability is over the choices of (a,r) by the prover and ρ), then there is an $e > 0$ and a probabilistic polynomial time verifier which can compute w' satisfying $\mathcal{P}(x,w') = 1$ with probability at least k^{-e} after one execution of the basic protocol.
This property says that no warden can compute correct responses to two different challenges from one execution of the basic protocol with P. Property II is an immediate consequence of Property I when $|E|$ is *polynomial* in k:

Lemma 5. *If the basic protocol satisfies Property I and $|E| \leq k^d$ for some integer d, then it satisfies Property II.*

Proof sketch. Assume the protocol satisfies Property I and let (f, g, h) be three poly-time functions as in Property II.

We will construct a polynomial time verifier, M, which extracts P's witness after one execution of the protocol. M computes, given a from the prover, its challenge as follows:

1. Choose a random string, ρ, of the proper length.
2. Choose a random pair $(c_1, c_1') \in E^2$ such that $g(x,a,c_1,\rho) = g(x,a,c_1',\rho)$ and let c denote this value.

Given r from the prover, M computes

$$r_1 = h(x, a, c_1, r, \rho) \qquad \text{and} \qquad r_1' = h(x, a, c_1', r, \rho).$$

Let $a_1 = f(x, a, \rho)$. If $p(x, a_1, c_1, r_1) = p(x, a_1, c_1', r_1) = 1$ then the machine guaranteed by Property I can be used to extract the witness. It is easy to see that M runs in polynomial time and it succeeds if and only if M guesses $c_1, c_1' \in S_{\rho,a,r}$ as required by Property II. Thus the witness can be extracted with probability at least a polynomial fraction. □

For the proof of our main result, we also need the following simple lemma.

Lemma 6. *Let E be a finite set, $D \subseteq E \times E$, $|D| \geq |E| + 1$, and σ a function from D to E. If σ has the property that*

$$\forall (x_1, y_1), (x_2, y_2) \in D : \; x_1 \neq x_2 \; \Rightarrow \; \sigma(x_1, y_1) \neq \sigma(x_2, y_2),$$

then there exist $(x, y_1), (x, y_2) \in D$, such that $y_1 \neq y_2$ and $\sigma(x, y_1) = \sigma(x, y_2)$.

Lemma 7. *If the basic protocol satisfies Property I, is witness hiding and $|E| \leq k^d$ for some integer d, then no polynomial time warden can transfer it to two verifiers, V_1 and V_2, in parallel and answer more than $1/|E|$ of the possible pairs of challenges with non-negligible probability.*

Proof sketch. The idea is that if a warden can answer more than $1/|E|$ of the possible pairs of challenges then, by Lemma 6 it can answer two different challenges from V_1 or V_2 using the same challenge to the prover. By Property I and Lemma 5 this contradicts the security of the prover in the basic protocol. □

The following theorem extends this lemma to cope with the application of the basic protocol to zero-knowledge proofs of knowledge.

Theorem 8. *Assume no polynomial time algorithm on input x can find w such that $\mathcal{P}(x, w) = 1$. Let (P, V) be a zero-knowledge proof of knowledge, in which the basic protocol is repeated t times where $1 < |E| < k^d$ for some d and $|E|^t$ grows faster than any polynomial in k. If the basic protocol satisfies Property I then (P, V) is not weakly 2-transferable.*

Proof sketch. The assumption implies that the basic protocol is witness hiding. By Lemma 7, for any warden the probability of success in transferring the proof in one iteration to two verifiers V_1 and V_2 is at most $1/|E|$. Thus the probability of success in t iterations is at most $(1/|E|)^t$ which by assumption is smaller than the inverse of any polynomial for k sufficiently large. □

4.2 Weakening Property I

Although Property I is satisfied by most known proofs of knowledge, it is quite restrictive. For example, it excludes proofs of knowledge in which $|E| = 5$ and a prover without knowing the witness can answer correctly on any two challenges, whereas answers to any three challenges allow a witness to be computed.

Definition 9. The basic protocol is called an l-proof of knowledge ($1 \leq l < |E|$), if there exists a polynomial time Turing machine, M, which given (x, a) and $(c^{(j)}, r^{(j)})_{j=1,\ldots,l+1}$ satisfying

$$p(x, a, c^{(j)}, r^{(j)}) = 1 \qquad \text{for } j = 1, \ldots, l+1$$

and

$$c^{(j)} \neq c^{(j')} \qquad \text{for} \qquad 1 \leq j < j' \leq l+1$$

outputs a witness, w', satisfying $\mathcal{P}(x, w') = 1$.

By extending the previous proofs the following generalization to l-proofs can be obtained.

Theorem 10. *Let $n \in \mathbb{Z}$ be a constant (independent of k), and let $1 \leq l < |E|$. If $|E| < k^d$ for some integer d, no warden can answer more than $l^n|E|$ of the $|E|^n$ possible tuples of challenges with non-negligible probability, when trying to transfer the protocol to n verifiers.*

Proof sketch. The proof of this theorem follows that of Theorem 8 given the following observation. If the warden can answer more than $l^n|E|$ of the possible challenges, then he can answer two tuples of challenges, $(c_1, c_2, \ldots, c_n)$ and $(c'_1, c'_2, \ldots, c'_n)$, for which there is an i ($1 \leq i \leq n$) such that $c_i \neq c'_i$ and

$$c_j = c'_j \qquad \text{for } j = 1, 2, \ldots, i-1.$$

□

Example 1. For $n, l = 2$ and $|E| = 5$ the probability of success is at most $4/5$. Hence, in this case the proof cannot be 2-transferred with very high probability.

Example 2. For $n, l = 2$ and $|E| = 4$ this fraction is 1 — hence the theorem does not exclude 2-transferability in this case. However, the protocol cannot be 3-transferred: the probability of success is $2^3 4/4^3 = 1/2$.

5 The Basic Protocol is a Proof System

While the previous section assumed that $|E|$ is polynomial in k, this section considers the case where a single execution of the basic protocol constitutes a proof system. Hence, $|E|$ is larger than any polynomial for k sufficiently large. It will be shown that this protocol is not 2-divertible if it is witness hiding. In particular, this shows that the usual ways (e.g., as in [OO90]) of diverting instances of this protocol to a single verifier cannot be extended to parallel divertibility, if the warden still wants to be successful with overwhelming probability.

The proof in the previous section depends on E being of polynomial cardinality and we see no way to modify it to cope with larger E's. Therefore this section will use another technique, which neither seems to work for transferability nor seems to extend to weak divertibility (as will be pointed out). However, on the positive side the result in this section does not require the protocol to be an l-proof.

First, two lemmas are needed. Consider the situation where W tries to divert the proof to a single verifier, V. Lemma 11 below shows that W cannot use the same c in order to answer too many challenges from V. This lemma can be regarded as an extension of Lemma 5 to the case of large E.

Lemma 11. *For any warden given by (f, g, h) the following holds. If the protocol is a witness hiding proof of knowledge, then for all $d, e > 0$ the probability that there is an $c \in E$ such that*

$$|\{c_1 \in S_{\rho,a,r} \mid g(x, a, c_1, \rho) = c\}| > |E|/k^d$$

is at most k^{-e} for k sufficiently large. This probability is over the choices of (a, r) and ρ.

Proof. Let (f, g, h) be given and assume there are $d, e > 0$ such that for infinitely many values of k the cardinality of the above set is larger than $|E|/k^d$ with probability larger than k^{-e}. A verifier will be described which on input x of length such a k can find a witness after one execution of the protocol. As the protocol is a proof of knowledge it is sufficient to construct a verifier, M, which after a single execution can convince an honest verifier with probability at least $k^{-(e+2d)}$. M works as follows

1. Given a from the prover, compute $a_1 = f(x, a, \rho)$.
2. Choose $c_1 \in E$ at random and compute $c = g(x, a, c_1, \rho)$.
3. Get r from the prover and compute $r_1 = h(x, a, c_1, r, \rho)$.
4. If $p(x, a_1, c_1, r_1) = 0$ then stop.

Afterwards M, when acting as a prover, chooses a_1 in the first move, and given a challenge c_1' from the honest verifier returns $r_1' = h(x, a, c_1', r, \rho)$.

Clearly, M runs in polynomial time. In the following it will be shown that M convinces the verifier with probability at least $k^{-(e+2d)}$. Let for $c \in E$

$$E_c = \{c_1 \in S_{\rho,a,r} \mid g(x, a, c_1, \rho) = c\},$$

and let A denote the event that there is a c such that

$$|E_c| > |E|/k^d.$$

Now

$$\begin{aligned} Prob[V \text{ accepts}] &\geq Prob[V \text{ accepts} \mid A, c_1 \in E_c] Prob[c_1 \in E_c \mid A] Prob[A] \\ &\geq Prob[V \text{ accepts} \mid A, c_1 \in E_c] k^{-d} k^{-e} \\ &\geq Prob[c_1' \in E_c] k^{-(e+d)} \\ &\geq k^{-(e+2d)} \end{aligned}$$

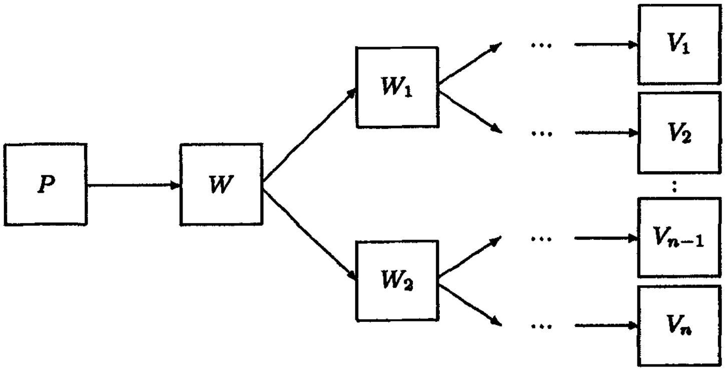

Fig. 3. Diverting a proof to many verifiers

The next lemma shows that if W can divert the proof to two persons in parallel, then she can divert it to any polynomial number of verifiers. This lemma fails in the case of weak divertibility.

Lemma 12. *If an interactive proof system is 2-divertible then it is also n-divertible for any n which is polynomial in k.*

Proof sketch. Let $n = n(k)$ be polynomial in k. The method for W to divert the proof to two verifiers can be used in a tree-like way to divert it to n verifiers as shown in Figure 3. The analysis of this can be found in [Che94]. □

Using these two lemmas the following can be proven

Theorem 13. *If the protocol is a witness hiding proof of knowledge then it is not 2-divertible.*

Proof sketch. As each element of E can be represented by a polynomial number of bits, the cardinality of E can be assumed to be at most $2^{q(k)}$ for some polynomial q. By Lemma 12 the proof is $q(k)$-divertible.

Let A_i denote the event that there is an $c \in E$ such that for more than $|E|/3$ of the possible challenges from the i'th verifier W can find an answer to this verifier given the prover's response to c. By Lemma 11 the probability of A_i is super-polynomially small. Hence, the probability of the event $A = A_1 \vee \ldots \vee A_{q(k)}$ is super-polynomially small as well (over the choice of a, r and ρ). Let Acc denote the event that all verifiers accept (distributed according to the random coins of all parties). Then

$$\begin{aligned} Prob[Acc] &= Prob[Acc \mid A]Prob[A] + Prob[Acc \mid \neg A]Prob[\neg A] \\ &\leq Prob[A] + Prob[Acc \mid \neg A] \end{aligned}$$

Now if $\neg A$ occurs then a given c cannot be used to answer more than a third of the possible questions from the i'th verifier. Hence, the probability that there is a c which can be used to answer all verifiers is at most

$$|E|3^{-q(k)} \leq \left(\frac{2}{3}\right)^{q(k)}.$$

This is also an upper bound on $Prob[Acc \mid \neg A]$. Thus the probability that all verifiers accept is super-polynomially small. Therefore, at least one verifier will not accept with probability polynomially close to 1.

□

6 Blind Signatures

This section applies the result in the previous section to the blind signatures suggested in [OO90].

Consider the situation where the basic protocol constitutes a proof of knowledge. Then the protocol can be used to construct a signature scheme by using the technique of Fiat and Shamir ([FS87]). Let H be a hash function as in that paper.

The public key is x and the secret key is the witness w. The signature on a message, $m \in \{0,1\}^*$, is

$$\sigma(m) = (a, r)$$

and it is correct if $p(x, a, c, r) = 1$ where $c = H(a, m)$.

If the basic proof is divertible, a blind signature can be constructed in an interactive protocol between signer and receiver as follows. The prover first computes a. The receiver finds $c_1 = h(m, a_1)$ and then computes c. Given r from the prover, the receiver finds r_1. The resulting signature on m is $\sigma(m) = (a_1, r_1)$.

This blind signature scheme is very difficult to analyze (its security depends very much on H). However, it would be easy to get two blind signatures from one execution of the protocol, if the proof could be diverted to two verifiers in parallel. It follows immediately from Theorem 13, that such an attack cannot succeed with probability close to 1.

7 Extensions

In some divertible proofs the warden is not interested in proving that he knows a witness to x, but rather to some transformation of x (e.g., in the case of square roots, the warden may want to prove that he knows a square root of r^2x for some number, r). The proofs in Section 4 and 5 also work in this more general scenario. More precisely, it can be shown that the warden cannot transform x to two other input values, x_1 and x_2 and use the prover's proof, unless he knows a witness to either x_1 or x_2. The details of this can be found in [Che94].

8 Convincing the Warden Unconditionally

This section presents a divertible zero-knowledge proof of membership, in which both warden and verifier are convinced unconditionally. The original proof system was suggested by Chaum and used to verify undeniable signatures in [Cha91].

Let p and q be primes such that q divides $p-1$. The common input is $(g, h, m, z) \in \mathbb{Z}_p^*$, each of order q. The prover knows $x = \log_g h$ and wants to show that $\log_g h = \log_m z$. The divertible proof system is shown in Figure 4.

Proposition 14. *The protocol in Figure 4 is a divertible proof.*

The proof is omitted. More interesting is the following

Proposition 15. *Even if P and V cooperate, the warden will not accept a false statement with probability larger than $(q-1)^{-1}$ (over his own coins).*

Proof sketch. In [Cha91] it is shown that if $\log_g h \neq \log_m z$ then the prover can only convince the warden if he can guess the value of a before sending h_1 and h_2.

Thus it is sufficient to show that if W chooses r, t'', a'', b'' uniformly at random then given $c', c, h_1, h_2, h_1', h_2', a', b'$ all values of a but one can occur (and with the same probability).

Given a pair (a, b) such that $c = g^a m^b$. Let $m = g^d$, $h_1 = g^{d_1}$ and $h_1' = g^{d_2}$. Similarly, let $z = h^e$, $h_2 = h^{e_1}$ and $h_2' = h^{e_2}$. Then all information about the secret choices of the warden is contained in the following four equations:

$$\begin{aligned}(d_2 - t'')r &= d_1 - (a'' + db'')\\ (e_2 - t'')r &= e_1 - (a'' + eb'')\\ a'' &= a - a'r\\ b'' &= b - b'r.\end{aligned}$$

It has to be shown that these equations always have at least one solution for r, t'', a'', b''. Subtracting the second from the first gives

$$(d_2 - e_2)r = d_1 - e_1 - (d-e)b''.$$

This implies

$$(d_2 - e_2)r = d_1 - e_1 - (d-e)(b - b'r)$$

and thus

$$(d_2 - e_2 - (d-e)b')r = d_1 - e_1 - (d-e)b \qquad (*)$$

We now distinguish two cases. First, if $d_2 - e_2 - (d-e)b' = 0$, then for any $r \in \mathbb{Z}_q^*$, a'', b'', t'' can be determined by

$$\begin{aligned}(d_2 - t'')r &= d_1 - (a'' + db'')\\ a'' &= a - a'r\\ b'' &= b - b'r.\end{aligned}$$

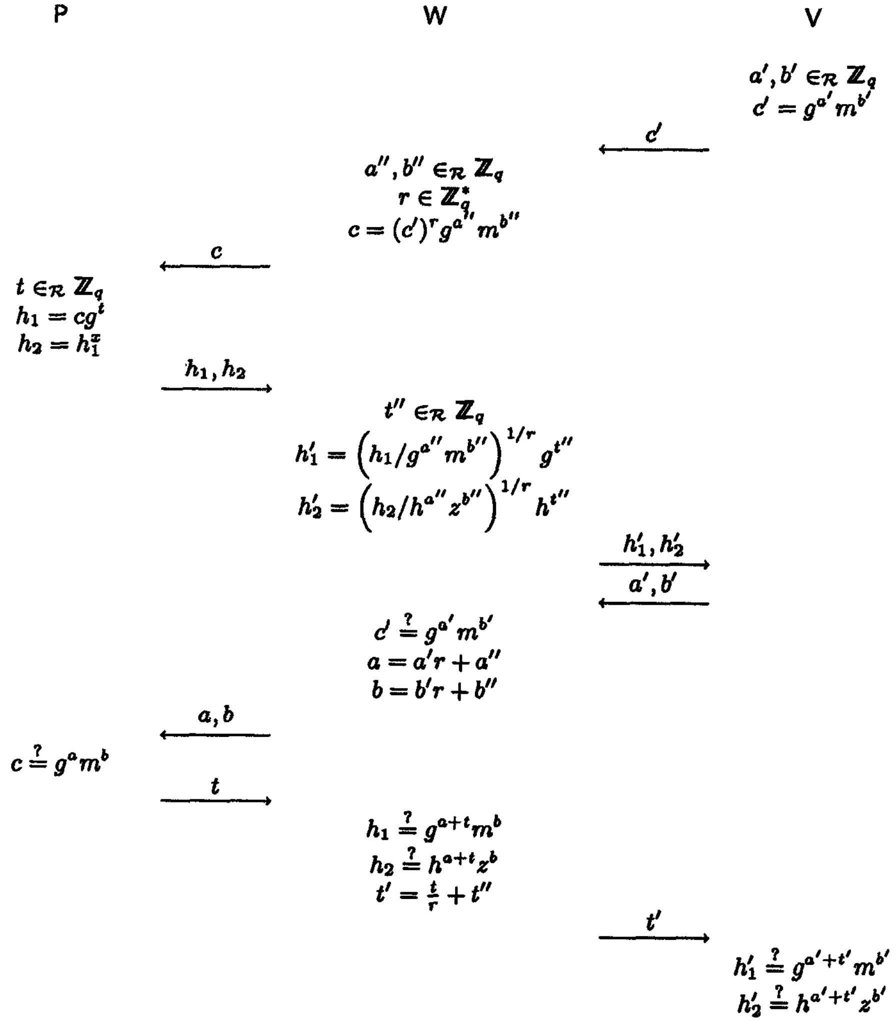
P
W
V
$a', b' \in_{\mathcal{R}} \mathbb{Z}_q$
$c' = g^{a'} m^{b'}$
c'
$a'', b'' \in_{\mathcal{R}} \mathbb{Z}_q$
$r \in \mathbb{Z}_q^*$
$c = (c')^r g^{a''} m^{b''}$
c
$t \in_{\mathcal{R}} \mathbb{Z}_q$
$h_1 = cg^t$
$h_2 = h_1^x$
h_1, h_2
$t'' \in_{\mathcal{R}} \mathbb{Z}_q$
$h_1' = \left(h_1/g^{a''} m^{b''}\right)^{1/r} g^{t''}$
$h_2' = \left(h_2/h^{a''} z^{b''}\right)^{1/r} h^{t''}$
h_1', h_2'
a', b'
$c' \overset{?}{=} g^{a'} m^{b'}$
$a = a'r + a''$
$b = b'r + b''$
a, b
$c \overset{?}{=} g^a m^b$
t
$h_1 \overset{?}{=} g^{a+t} m^b$
$h_2 \overset{?}{=} h^{a+t} z^b$
$t' = \frac{t}{r} + t''$
t'
$h_1' \overset{?}{=} g^{a'+t'} m^{b'}$
$h_2' \overset{?}{=} h^{a'+t'} z^{b'}$

Fig. 4. Convincing verifier and warden unconditionally.

It follows immediately, that also the equation

$$(e_2 - t'')r = e_1 - (a'' + eb'')$$

will be satisfied. Secondly, if $d_2 - e_2 - (d - e)b' \neq 0$, then r is determined by $(*)$. As the warden chooses $r \neq 0$ the prover and verifier know that

$$b = \frac{d_1 - e_1}{d - e}$$

(and the corresponding value of a) is not possible. But for all other values t'', a'', b'' can be determined as in the first case.

As the prover chooses d_1 and e_1, he can always make sure that one of the q possible (a, b) pair will not occur. □

9 Conclusion and Open Problems

An example of a divertible proof has shown that it is possible to make divertible proofs in which the warden cannot be cheated into accepting a false statement.

We have shown that zero-knowledge proofs based on the basic three round protocol cannot be transferred to two independent verifiers simultaneously. If the basic protocol constitutes a witness hiding proof in itself, it cannot be diverted to two independent verifiers with overwhelming probability.

It would be interesting to improve the analysis of the latter case and obtain a result just as strong as in the former. Furthermore, it is an interesting open problem to extend the results in this paper to general proofs of knowledge (not only proofs based on the three round protocol).

References

[BD91] M. Burmester and Y. Desmedt. All Languages in NP Have Divertible Zero-Knowledge Proofs and Arguments under Cryptographic Assumptions. In *Advances in Cryptology - proceedings of EUROCRYPT 90*, Lecture Notes in Computer Science, pages 1 – 10, 1991.

[CEvdG87] D. Chaum, J.-H. Evertse, and J. van de Graaf. An improved protocol for demonstrating possession of a discrete logarithm and some generalizations. In *Advances in Cryptology - proceedings of EUROCRYPT 87*, Lecture Notes in Computer Science, pages 127–141, 1987.

[Cha91] D. Chaum. Zero-knowledge undeniable signatures. In *Advances in Cryptology - proceedings of EUROCRYPT 90*, Lecture Notes in Computer Science, pages 458 – 464. Springer Verlag, 1991.

[Che94] Chen Lidong. *Witness Hiding Proofs and Applications*. PhD thesis, Aarhus University, Mathematics Institute, 1994.

[DGB88] Y. Desmedt, C. Goutier, and S. Bengio. Special Uses and Abuses of the Fiat-Shamir Passport Protocol. In *Advances in Cryptology - proceedings of CRYPTO 87*, Lecture Notes in Computer Science, pages 21 – 39. Springer-Verlag, 1988.

[FFS88] U. Feige, A. Fiat, and A. Shamir. Zero-knowledge proofs of identity. *Journal of Cryptology*, 1(2):77–94, 1988.

[FS87] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology - proceedings of EUROCRYPT 86*, Lecture Notes in Computer Science, pages 186 – 194. Springer-Verlag, 1987.

[FS90] U. Feige and A. Shamir. Witness indistinguishable and witness hiding protocols. In *Proceedings of the 22nd Annual ACM Symposium on the Theory of Computing*, pages 416 – 426, 1990.

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. *SIAM Journal of Computation*, 18(1):186–208, 1989.

[ISS93] T. Itoh, K. Sakurai, and H. Shizuya. Any Language in *IP* Has a Divertible ZKIP. In *Advances in Cryptology - proceedings of ASIACRYPT 91*, Lecture Notes in Computer Science, pages 382 – 397. Springer-Verlag, 1993.

[OO90] T. Okamoto and K. Ohta. Divertible Zero Knowledge Interactive Proofs and Commutative Random Self-Reducibility. In *Advances in Cryptology - proceedings of EUROCRYPT 89*, Lecture Notes in Computer Science, pages 134 – 149. Springer-Verlag, 1990.

[Sim84] G. J. Simmons. The Prisoner's Problem and the Subliminal Problem. In *Advances in Cryptology - proceedings of CRYPTO 83*, pages 51 – 67, 1984.

[TW87] M. Tompa and H. Woll. Random self-reducibility and zero knowledge interactive proofs of possession of information. In *Proceedings of the 28th IEEE Symposium on the Foundations of Computer Science*, pages 472–482, 1987.