Proof of Proximity of Knowledge

Serge Vaudenay

EPFL
CH-1015 Lausanne, Switzerland
http://lasec.epfl.ch

Abstract. Public-key distance bounding schemes are needed to defeat relay attacks in payment systems. So far, only two such schemes exist, but fail to fully protect against malicious provers. In this paper, we solve this problem. We provide a full formalism to define the proof of proximity of knowledge (PoPoK). Protocols should succeed if and only if a prover holding a secret is within the proximity of the verifier. Like proofs of knowledge, these protocols must satisfy completeness, soundness (protection for the honest verifier), and security (protection for the honest prover). We construct ProProx, the very first fully secure PoPoK.

1 Introduction

Following the chess grandmaster problem, a dummy chess player can challenge two grandmasters in parallel (without letting them know) if they take different colors. This works by letting the dummy player relay the move of a grandmaster on one chess board to the other chess board against the other grandmaster and *vice versa*. In real life, *relay attacks* can be a serious threat against applications such as NFC-based payment: for small payments, there is typically no action required on the creditcard or smartphone (beyond approaching to the terminal) such as typing a PIN code. So, a man-in-the-middle adversary could just relay communications between the payment device of the victim and the terminal to make payments on the behalf of the holder. The limit of the speed of communication was proposed to solve this problem [3]. Brands and Chaum [9] introduced the notion of *distance-bounding protocol* to prove that a *prover* is close enough to a *verifier*. This relies on information being local and unable to travel faster than the speed of light. So, an RFID reader can identify when participants are close enough because the round-trip communication time in challenge/response rounds have been small enough. Although challenging from an engineering viewpoint, it is actually feasible to implement these protocols, as shown in [23,24,25]. Actually, some commercial NFC cards by NXP[1] are already supposed to implement "proximity checks against relay attacks" by "a precise time measurement of challenge-response pairs", although no public analysis is available so far.

The literature considers several threat models.

- *Relay attack*: an adversary relay messages between a far-away honest prover and a verifier, trying to make the verifier accept. This is extended by *Mafia fraud* [13] where the adversary can also modify messages. This is further extended by *Man-in-the-Middle attack* [5,7] where the attack follows a learning phase where the prover could be close-by. Another related threat model is the *Impersonation fraud* [1] where an adversary tries to impersonate the prover to the verifier.
- *Distance fraud* [9]: a far-away malicious prover tries to pass the protocol.
- *Terrorist fraud* [13]: a far-away malicious prover, with the help of an adversary, tries to make the verifier accept the adversary's rounds on his behalf, but without giving the adversary any advantage to later pass the protocol alone. This is extended by *Collusion fraud* [5,7] where the goal of the adversary is now to run a man-in-the-middle attack. Terrorist fraud is also related to

[1] See Mifare Plus X on http://www.nxp.com

the notion of *soundness* [26]: whenever the verifier accepts, there must be an extractor who can reconstruct the secret of the prover based on the view of all close-by participants, even after many iterations. An hybrid model between distance fraud and terrorist fraud is the one of *Distance hijacking* [12]: A far-away prover takes advantage of some honest, active provers to make the verifier accept.

There exist many (symmetric) distance-bounding protocols but so far only the SKI [4,5,6], the Fischlin-Onete protocol [16], and DB1 and DB2 [8] provide an all-encompassing proven security, i.e., they protect against all the above threats with a formal proof of security. (See [4, Section 2].)

As discussed herein, resistance to malicious provers (i.e., distance fraud, distance hijacking, terrorist fraud, collusion fraud, and non-soundness) is important, specially for non-repudiation. This is needed for contactless payment applications: If a customer can deny a payment by proving he was somewhere else, there is a liability issue. Making the scheme such that this type of fraud is impossible would certainly be an asset. It would strengthen trust and acceptance of this technology. So, there is a need for distance-bounding protocols protecting against all the above types of fraud.

Public-key distance bounding. In interactive proofs, the prover does not share a secret key with the verifier. The verifier only knows a public key. However, so far, only the following distance-bounding protocols are in the public key model: the Brands-Chaum protocol [9] (Fig. 4), the Bussard-Bagga protocol [10], and the Hermans-Peeters-Onete (HPO) protocol [21] (Fig. 5).[2] The Bussard-Bagga protocol was broken by Bay et al. [2] and none of the others protect against terrorist fraud. So, the problem of making a fully secure public-key distance-bounding protocol is still open.

Sometimes, secret key protocols are sufficient for practical applications. Indeed, to unlock a car or to open a door in a building with an RFID token, it may be reasonable (especially if symmetric distance-bounding protocols are more efficient) to assume that the RFID token shares his secret with the car or the door. However, when considering wireless payment systems, it is unreasonable to assume that the secret of the prover can be shared with all verifiers. When paying with an NFC credit card at the grocery shop, the cashier may sometimes be offline with the bank and not willing to stop business. To protect against relay attacks, we need the cashier to run a distance-bounding protocol from the public key of the payer only. So, there is a need for public-key distance bounding.

Contribution. In this paper, we provide a full model to formalize public-key distance-bounding and we specify our new primitive: the *proof of proximity of knowledge (PoPoK)*. It is based on a prover holding a secret x authenticating to a verifier knowing his public key y. Under honest execution, the verifier should accept if the prover is at a distance up to a bound B. Under adversarial environment, he should only accept if we can extract x from the view of all participants within a distance lower than B. Our model is pretty natural and nicely connects recent work on distance bounding (such as the SKI model [5,7]) and interactive proofs. Our formalism captures the notions of man-in-the-middle and of terrorist fraud and attacks by malicious provers. Then, we construct ProProx the very first fully secure PoPoK. It is based on the quadratic residuosity problem, using the Goldwasser-Micali encryption [19,20] and the Fiat-Shamir protocol [15].

Organization. In Section 2 we provide a full formal model for public-key distance bounding, mostly based on the SKI model, and define the PoPoK. We relate this to the state of the art and to the notion of interactive proofs. In Section 3 we propose ProProx, the very first fully secure PoPoK, and analyze it. In addition to man-in-the-middle and collusion frauds, we specifically cover distance frauds. We

[2] A variant of the HPO protocol offers anonymous authentication [17].

also discuss on concrete parameters and implementation. Some case studies illustrating the difficulty of constructing a PoPoK are put in Appendix C.

2 Model and Definitions

We refine the security definitions and other tools from the security models in [5,7,26]. Throughout this paper, we use the asymptotic complexity approach for security. Constructions depend on some security parameter λ which is omitted for more readability. A *constant* does not depend on λ, while parameters defining cryptographic constructions do. Algorithms will often run in probabilistic polynomial-time (PPT) in terms of λ. A real function $f(\lambda)$ is negligible if for any d, we have $f(\lambda) = O(\lambda^{-d})$, as $\lambda \to +\infty$. In this case we denote $f(\lambda) = \mathsf{negl}(\lambda)$. We also use the following notation:

$$\mathsf{Tail}(n,\tau,\rho) = \sum_{i=\tau}^{n} \binom{n}{i} \rho^i (1-\rho)^{n-i}$$

2.1 Computational, Communication, and Adversarial Models

In our settings, participants are interactive Turing machines running PPT algorithms.

We follow the communication model and adversarial model from Boureanu et al. [5,7]: we assume that participants have a *location* which is an element of a metric space $\mathcal{S}$, with a distance function d. If a participant π_1 at a location loc_1 executes a special command $\mathsf{send}(\pi_2, m)$ at time t to send a message m to a participant π_2 at location loc_2, the message m is received by π_2 at time $t + d(\mathsf{loc}_1, \mathsf{loc}_2)$. Furthermore, any malicious participant π_3 at some location loc_3 could see this message m at time $t + d(\mathsf{loc}_1, \mathsf{loc}_3)$. We assume no authentication: π_2 does not know if the message comes from π_1.

There is an exception preventing m from being delivered to π_2: if π_2 is honest and some (malicious) participant π_3 at some location loc_3 has sent a special signal $\mathsf{corrupt}(\pi_1, \pi_2)$ at time t', m is not delivered to π_2 if $t + d(\mathsf{loc}_1, \mathsf{loc}_2) \geq t' + d(\mathsf{loc}_3, \mathsf{loc}_2)$. This condition is a consequence of the information traveling with a speed limit: whenever a malicious participant π_3 corrupts a $\pi_1 \to \pi_2$ channel, π_2 will only receive the messages until his corruption signal emitted from π_3 reaches π_2.

Note that once the $\pi_1 \to \pi_2$ channel is corrupted, π_3 can still see the message m sent by π_1 and decide to send any m' to π_2, either depending on m if he waits to receive m, or not. The crux is that either m' is independent of m, or it is delivered at a different time, depending on the locations.

This model is only used to prove the following lemma which is taken from [7] and [8].

Lemma 1 (Fundamental Lemma). *Assume a multiparty protocol execution with a distinguished participant $\mathcal{V}$, the set* Far *of all participants within a distance to $\mathcal{V}$ larger than B, and the set* Close *of all other participants. At some time t in the execution, $\mathcal{V}$ broadcasts a message c and waits for a response r. We let* Acc *denote the event that r was received by $\mathcal{V}$ no later than time $t + 2B$. For each participant U, we denote by* View_U *his partial view just before time $t + d(\mathcal{V}, U)$, the time when U could see c. We say that a message from U is* independent[3] *(from c) if it is the result of applying the algorithm U on* View_U*, or on an earlier partial view. There exists an algorithm* Algo *such that if* Acc *occurs and r was sent by some $U \in$ Close, then $r = \mathsf{Algo}(\mathsf{View}_{\mathsf{Close}}, c, \mathsf{Other})$, where* $\mathsf{View}_{\mathsf{Close}}$ *is the list of all* View_C*, $C \in$ Close, and* Other *is the list of all messages from any $F \in$ Far which are independent from c, that at least one member $C \in$ Close could see (either because he was the destinator, or because he is malicious), and not already in any* View_C *(i.e., sent after time $t + d(\mathcal{V}, F)$). Furthermore, if* Acc *occurs and r was sent by some $U \in$ Far, then r is independent from c.*

[3] We stress that this notion of independence is *not* related to statistical independence. Our notion of independence means that the message is computed with data available before c has reached the location where the computation is done.

In clear: r cannot depend on messages from a far away U which has been sent after U received c.

Proof. The case where r comes from $U \in \mathsf{Far}$ is easy: if r is computed at time t', we must have $t' \leq t + 2B - d(\mathcal{V},U)$. Since $d(\mathcal{V},U) > B$, we have $t' < t + d(\mathcal{V},U)$, so r is independent form c.

For the other case, we let Algo simulate each participant $C \in \mathsf{Close}$ between time $t + d(\mathcal{V},C)$ (to continue after View_C) and time $t + 2B - d(\mathcal{V},C)$ (after which it is too late to send a message to $\mathcal{V}$). The simulation of all participants is done in parallel, chronologically. The output of Algo is the first message r for $\mathcal{V}$ to arrive to $\mathcal{V}$.

We show by induction that the simulation cannot block: when Algo must simulate the computation of a message by some $C \in \mathsf{Close}$ at time $t' \leq t + 2B - d(\mathcal{V},C)$, the input to C are messages m which are either part of the input to Algo or which have been computed by Algo before. To prove this, we distinguish three cases. First, if m comes from a participant in Far, due to the distance constraint, it must be independent from c, so be part of w which is input to Algo. In the second case, m comes from $\mathcal{V}$. Since it is assumed that $\mathcal{V}$ does not send messages after c before r is received, m is either part of View_C or the message c itself, so part of the inputs of Algo in both cases. In the third case, m comes from $C' \in \mathsf{Close}$. It is either computable from $\mathsf{View}_{C'}$ or computed by C' after $\mathsf{View}_{C'}$ was closed but early enough to arrive at C at time t', so between time $t + d(\mathcal{V},C')$ and $t' - d(C,C')$. Since $t' \leq t + 2B - d(\mathcal{V},C)$, we have $t' - d(C,C') \leq t + 2B - d(\mathcal{V},C) - d(C,C') \leq t + 2B - d(\mathcal{V},C')$, so this message must have been computed in the simulation by Algo.

Finally, we observe that Algo returns r. Indeed, the message r to $\mathcal{V}$ must be among those which are computed by the simulation, due to the distance constraints. □

Participants can move, but not faster than communication. I.e., the location at time $t+1$ can only be at a distance up to 1 to the location at time t. For simplicity, we assume that far-away participants (as defined in Def. 3) remain far away during the entire execution.

We sometimes consider that when a honest participant receives a message from another honest participant, it may be subject to noise. As for malicious participants, we could assume that they use a better equipment which eliminates noise. Also: whenever the honest-to-honest communication is not time-sensitive, we may also assume that they use error correction means so that the communication is noiseless. Protocols shall thus make clear which messages may be subject to noise.

2.2 PoPoK: Proofs of Proximity of Knowledge

Definition 2 (Proof of proximity of knowledge). *A proof of proximity of knowledge (PoPoK) is a tuple $(\mathcal{K}, \mathsf{Kgen}, P, V, B)$, consisting of: a key space $\mathcal{K}$ depending on a security parameter λ, with elements of polynomially-bounded size in terms of λ; a PPT algorithm Kgen; a two-party PPT protocol $(P(x), V(y))$, where $P(x)$ is the* proving algorithm *and $V(y)$ is the* verifying algorithm*; a distance bound B. The algorithm Kgen maps the secret $x \in \mathcal{K}$ to a public key y.[4] y is given as input to all participants. At the end of the protocol, $V(y)$ sends a final message Out_V. He accepts ($\mathsf{Out}_V = 1$) or rejects ($\mathsf{Out}_V = 0$).*

The protocol must be such that when running $P(x)$ and $V(y)$ at locations within a distance up to B, in a noiseless environment, the verifier always accepts. This property is called completeness*.*

If the protocol specifies a list of time-critical challenge/response exchanges, we say that it is complete with noise probability p_{noise} *if, in an environment in which all challenge/response rounds are independently corrupted with probability p_{noise} and other exchanges are not subject to noise, the probability that the verifier accepts is $1 - \mathsf{negl}(\lambda)$.*

[4] This is without loss of generality: an algorithm $\mathsf{Gen}(\rho) = (K_p, K_s)$ making a public key K_p and a secret key K_s using coins ρ defines such $\mathsf{Kgen}(x) = y$ by letting $x = \rho$ and $y = K_p$.

The last part of this definition applies to protocols which identify well the challenge/response rounds.

We implicitly assume that (x,y) keys of honest provers are correctly registered using Kgen.

In practice, if we want to have $B = 10\text{m}$, assuming that an adversary can do computation in negligible time, the timer for receiving a response r to a challenge c in Lemma 1 should be limited to 67ns. So, a honest prover at a zero distance must respond within less than 67ns. This clearly excludes any cryptographic computation. This even excludes waiting for receiving several bits in a sequence since the typical time between two bits is of 1μs in wireless technologies. To be realistic, a PoPoK can only consider boolean (or very small) challenges and responses when it comes to use Lemma 1.

2.3 Cryptographic Properties of PoPoK in a Multiparty Setting

We adopt the multiparty setting from [8] and adapt it to public-key distance bounding.

As it is discussed in Example 19, we don't assume that instances reliably know their locations.

We consider a setting with participants which are called either *provers*, *verifiers*, or *others actors*. We assume only one verifier $\mathcal{V}$, without loss of generality. Indeed, we can take other verifiers as *other actors*. Similarly, we assume that provers correspond to the same identity so share the same secret x, without loss of generality. (Provers with other secrets are considered as *other actors*.) Other actors are malicious without loss of generality. The difference between malicious provers and malicious actors is in the input: malicious provers receive x while malicious actors only receive y.

We assume that participants run their algorithm only once. Since different participants may correspond to the same identity at different time and locations, multiple executions are modeled by multiple participants. Since honest provers correspond to the same person at different time and locations, we assume that honest provers never run concurrently. A malicious prover may however clone himself at different locations and run algorithms concurrently.

Definition 3 (Experiment). *An* experiment exp *for a PoPoK* $(\mathcal{K},\mathsf{Kgen},P,V,B)$ *is defined by several* participants *who are a* verifier $\mathcal{V}$*,* provers *from an ordered set* $\mathbf{P}$*, and other* actors *from a set* $\mathbf{A}$*. Participants which are within a distance of at most B to* $\mathcal{V}$ *are called* close-by *participants. Participants which are within a distance larger than B to* $\mathcal{V}$ *are called* far-away *participants. We say that the prover is* always far-away *if all participants in* $\mathbf{P}$ *are far away.*

We adopt a static *adversarial model: either the prover is honest and all participants in* $\mathbf{P}$ *run the* $P(x)$ *algorithm, or the prover is malicious, and they could run any PPT algorithm.*

If the prover is honest, the participants in $\mathbf{P}$ *are assumed to be* non-concurrent*: at each time, there is only one participant of* $\mathbf{P}$ *which is activated. When the active participant terminates, another participant of* $\mathbf{P}$ *is activated, following a sequence. This sequence is defined by the ordering of* $\mathbf{P}$*.*

At the beginning of the experiment, for malicious provers, (x,y) *is set arbitrarily. If the provers are honest,* $x \in \mathcal{K}$ *is randomly selected and* $y = \mathsf{Kgen}(x)$ *is computed. Then, x is given as input to participants in* $\mathbf{P}$*, while y is given as input to all participants.* $\mathcal{V}$ *runs* $V(y)$*. All participants are then activated and run concurrently. (If the prover is honest, only the first prover from* $\mathbf{P}$ *is activated with the other participants, other provers being activated sequentially.) The experiment terminates when* $\mathcal{V}$ *produces its final output* Out_V*.*

We want to protect the honest prover against abuse. For that, we formalize security as follows:

Definition 4 (Security of PoPoK). *A PoPoK* $(\mathcal{K},\mathsf{Kgen},P,V,B)$ *is* secure *if for any experiment* exp *where the prover is honest and always far-away from* $\mathcal{V}$*, we have* $\Pr[\mathsf{Out}_V = 1] = \mathsf{negl}(\lambda)$.

This definition clearly captures relay attacks, Mafia fraud [13], and man-in-the-middle attacks in general. Some models (like in [5,7]) distinguish a learning phase (with provers which could be close-by)

and an attack phase (with far-away provers). This could also be described in the above framework: we just simulate both phases in two different locations and time of the experiment and make the adversary of the (simulated) learning phase sends what he has learnt to the adversary of the (simulated) attack phase. (The target $\mathcal{V}$ would be the one from the attack phase. So, provers would still be all far away.) With our model, we also cover more general cases in which provers are being attacked in parallel at other locations. Our definition is thus much simpler, more natural, and more general than [5,7].

We now formalize the protection for the honest verifier. Intuitively, we want that if the proof is accepted, it must be because the information about the secret x is in the close-by neighborhood.

Definition 5 (Soundness of PoPoK). *A PoPoK* $(\mathcal{K}, \mathsf{Kgen}, P, V, B)$ *is* sound *if there exists a negligible function* $\gamma(\lambda)$ *such that for any experiment* exp *in which* $\mathcal{V}$ *accepts with probability* $\Pr[\mathsf{Succ}] \geq \gamma(\lambda)$*, there exists an algorithm* $\mathcal{E}$ *called* extractor*, with the following property.* exp *defines an oracle which simulates an execution of* exp *and returns the views of all participants which are close-by (excluding* $\mathcal{V}$*) and the transcript of the protocol seen by* $\mathcal{V}$*.* $\mathcal{E}$ *can invoke the oracle many times. Then,* $\mathcal{E}$ *finally outputs* x' *such that* $\mathsf{Kgen}(x') = y$*, using a time complexity of* $\frac{\mathsf{Poly}(\lambda)}{\Pr[\mathsf{Succ}]}$.

For experiments with a close-by prover, this is trivial (as x is in the view of the prover). For experiments with no close-by prover, close-by actors would extract the prover's credential in the case the verifier would accept due to the prover cheating from far away. For experiments with no close-by participant at all, the transcript as seen by $\mathcal{V}$ would leak. So, a malicious prover is bound to leak.

Clearly, our definition nicely connects the infamous terrorist-fraud resistance to the soundness of interactive proofs. To compare with the literature, we could see that terrorist frauds in our model make the secret leak instead of only making man-in-the-middle attack feasible as in the notion of collusion fraud proposed in [5,7], and on which the SKI protocol is based, or only making impersonation attack feasible as in [8]. Our soundness is thus stronger.

Our notion and the one of [8] are close to soundness as defined in [26], except that we no longer require $1/\Pr[\mathsf{Succ}]$ to be polynomial. Also, compared to [8], we no longer need the condition on the success of the experiment to extract and we call an oracle O many times instead of using m views.

Just like other notions of TF-resistance, soundness is incomparable with SimTF-security [14] or GameTF-security [16]. But SimTF-security has a single symmetric instance [16] which is not competitive (see [8,26]) and GameTF has no instance (the MSK instance from [16] is broken in [26]).

What is captured by the notion of soundness? In distance bounding, the regular distance fraud is the case where the verifier accepts, with a malicious prover, and all participants far-away. Our soundness definition implies in such a case an extractor based on the transcript only. So, our soundness and security definitions protect against distance fraud by warning that any attack would leak. If the malicious prover does not care about leaking, this line of defense does not work and we have to treat distance fraud specifically. For this reason, we specifically define resistance to distance fraud in Def. 6 below.

Similarly, distance hijacking is a more general case allowing some honest close-by participants but not the prover holding x. We could say that a malicious prover hijacking the distance is bound to leak his secret due to our soundness definition. Indeed, the distance hijacking scenario is less general than the case of terrorist fraud where some adversaries may be close to the verifier.

Why do we care about soundness? In practice, it is not quite clear which application *really* needs soundness. Indeed, the original motivation of distance-bounding was to protect against relay attacks, or more generally to man-in-the-middle attacks, where the prover is assumed to be honest. These are all covered by security following Def. 4. When we additionally want to protect against malicious provers, one may think that distance fraud resistance it is enough and not care about soundness.

History shows that more bizarre attack scenarios happen, such as distance hijacking and collusion fraud. As we have seen, our notion of soundness is strong enough to capture all these threat models. Finally, protection against malicious provers in general (what soundness captures) is really needed for applications requiring non-repudiation such as payment. A malicious prover who succeeds to make a payment by an unknown attack can deny having made the payment with an alibi for having been unable to do it honestly (e.g., by proving he could not be close to $\mathcal{V}$ at this time). Soundness could offer more confidence in that this situation could not happen. It could be an asset.

We mention that there are other techniques to protect against malicious provers, including making sure that provers are honest by relying on tamper resistance. But tamper resistant devices are always subject to side-channel attacks, so this may not be so easy to achieve. Also, we think that soundness nicely bridges to the theory of interactive proofs of knowledge where soundness is defined similarly.

There is however a risk in trying to make distance bounding sound. Like in [21], some authors argue that soundness weakens protocols. This is actually the case of [16] (as shown in [26]). Also, sometimes, poorly analyzed protocols aimed to be sound can be badly broken, like [10] (as shown in [2]). This requires soundness to be taken with a special care and to make correct full security proofs.

Definition 6 (Distance-fraud security). *A PoPoK* $(\mathcal{K}, \mathsf{Kgen}, P, V, B)$ *resists to* distance fraud *if for any experiment* exp *where all participants are far away from* $\mathcal{V}$*, we have that* $\Pr[\mathsf{Out}_V = 1] = \mathsf{negl}(\lambda)$.

3 ProProx: a PoPoK Scheme

3.1 Building Blocks

Perfectly binding bit commitment. Depending on the security parameter λ, we use a (multiplicative) group structure with two Abelian groups L and G and an element θ such that G is generated by L and θ, $\theta \notin L$, and L is the set of all squares of G. We further assume that it is easy to do group operations and comparisons in G and to sample elements in G uniformly.[5] Finally, we assume it is computationally hard to distinguish elements from L and from G.

We define $\mathsf{Com}(b;\rho) = \theta^b\rho^2$ for a bit b and a random $\rho \in G$, like in the Goldwasser-Micali cryptosystem [19,20]. So, Com is computationally hiding as defined by Def. 15. We will not require any secret key to extract b, although there *exists* a function Com^{-1} such that $\mathsf{Com}^{-1}(\mathsf{Com}(b;\rho)) = b$ for all $b \in \{0,1\}$ and $\rho \in G$. We will rather use the homomorphic properties of the commitment and prove the correct commitment in a zero-knowledge way. Def. 15 in appendix formally defines Com.

For instance, we can take a Blum integer N, i.e., $N = PQ$ for two distinct primes P and Q which are congruent to 3 modulo 4. We set L to the set of quadratic residues modulo N and θ a residue modulo N such that $\left(\frac{\theta}{P}\right) = \left(\frac{\theta}{Q}\right) = -1$. E.g., $\theta = -1$. The algorithm Com is given N and θ. We sample $r \in G$ by $r = \theta^b\rho^2 \bmod N$, for $b \in \mathbf{Z}_2$ and $\rho \in \mathbf{Z}_N^*$. Distinguishing G from L is the quadratic residuosity problem, which is supposed to be hard.

A zero-knowledge proof for z being a square. We use the Fiat-Shamir protocol [15]. Namely, we show that z is a commitment to zero with a witness ζ (i.e., $z = \zeta^2$) with the protocol from Fig. 3, based on a perfectly hiding trapdoor commitment. Concretely, we use Def. 16 and Def. 17 in appendix with an $\mathcal{NP}$ language L. This is the set of all squares. If $z = \zeta^2$, we say that z is a member of L with witness ζ.

The protocol of Fig. 3 in appendix is $\frac{1}{2}$-sound and zero-knowledge. It must be run k times in parallel to achieve a soundness level $\kappa = 2^{-k}$. We denote it by $\mathsf{ZKP}_\kappa(z : \zeta)$.

[5] So, we can sample an element of L uniformly by taking r^2 with r uniformly selected in G.

By using parallel composition, we extend the protocol to prove that $z_1, \ldots, z_k$ are some commitments to zero with witness $\zeta_1, \ldots, \zeta_k$ respectively, and denote it by $\mathsf{ZKP}_\kappa(z_1, \ldots, z_k : \zeta_1, \ldots, \zeta_k)$. I.e., it succeeds with probability up to κ if there exists i such that $z_i \notin L$.

(Perfectly binding) deterministic commitment. Given a hash function H making coins for Com, we define a deterministic commitment by $\mathsf{Com}_H(x) = (\mathsf{Com}(x_1; H(x,1)), \ldots, \mathsf{Com}(x_s; H(x,s)))$ for $x \in \mathbf{Z}_2^s$. We assume that Com_H is a one-way function. Def. 18 in appendix formally defines Com_H. For example, when H is a random oracle, we can easily show that Com_H satisfies Def. 18.

3.2 The ProProx Protocol

We define the ProProx protocol, as depicted on Fig. 1. We consider s (the size of the secret), n (the number of rounds), n' (the number of iterations), τ (the minimal number of correct rounds for acceptance) as functions in terms of the security parameter λ. We assume s, n, n' are asymptotically linear. We also use a vector $b \in \mathbf{Z}_2^s$ and a set $\mathcal{M}$ of $n \times s$ matrices μ. We consider the vector b as fixed in the protocol. For now on, b is not important. It will only appear in Lemma 13 to treat distance fraud. There, we will only require b to have a Hamming weight of $\left\lfloor \frac{n}{2} \right\rfloor$. A random matrix $\mu \in \mathcal{M}$ is multiplied to the secret vector x to produce an encoded *leak* $x' = \mu \times x$. It is meant to leak some information about x in the case of a collusion fraud. In what follows, we write $x'_i = \mu_i(x)$. I.e., μ_i is the ith row of μ.

We define the set $\mathcal{M}_{\mathsf{repeat}}$ of all $n \times s$ matrices μ in which all rows μ_i are identical. This is a repetition code applied to the leak $\mu_1(x)$. Our main instance of ProProx uses $\mathcal{M} = \mathcal{M}_{\mathsf{repeat}}$.[6]

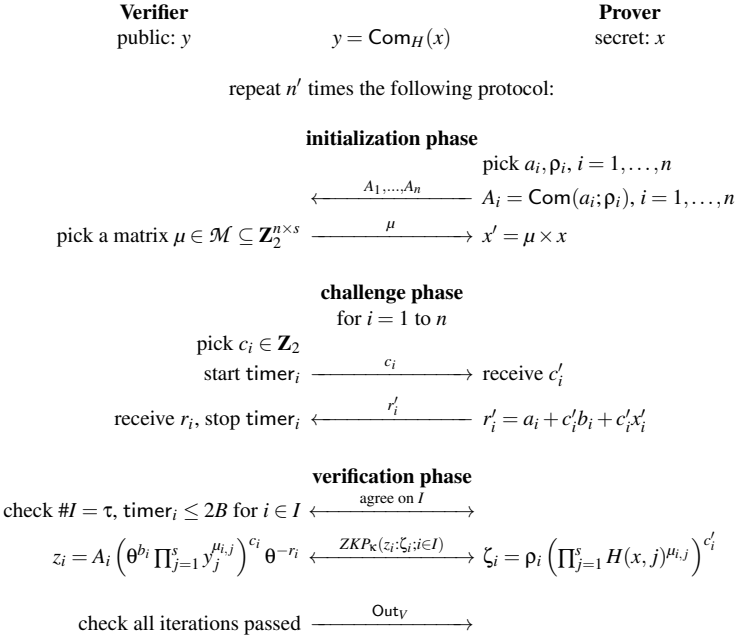

Fig. 1. ProProx: a Sound and Secure PoPoK.

The prover holds a secret $x \in \mathbf{Z}_2^s$ and the public key is $y = \mathsf{Com}_H(x)$. We iterate n' times the following protocol. First, the prover selects n bits $a_1, \ldots, a_n \in \mathbf{Z}_2$ and commits to them using some

[6] The notion of *leak* and the *leakage scheme* $\mathcal{M}_{\mathsf{repeat}}$ are taken from SKI [5,7].

fresh coins $\rho_1, \ldots, \rho_n$, respectively. So, $A_i = \mathsf{Com}(a_i; \rho_i)$, $i = 1, \ldots, n$. The A_i's are sent to the verifier who selects $\mu \in \mathcal{M}$ and sends it to the prover. The prover then computes $x' = \mu(x)$.

In the challenge phase, we have n time-critical rounds. These rounds may be subject to noise. The verifier picks a challenge $c_i \in \mathbf{Z}_2$ at random and sends it to the prover. The prover receives c_i' (which may be different, due to noise). He computes his response $r_i' = a_i + c_i' b_i + c_i' x_i'$ and sends it back to the verifier at once. The verifier receives r_i. The verifier measures the elapsed time timer_i taken to receive r_i after c_i was sent. Below, p_{noise} is the probability that some noise corrupts a challenge/response round. We assume that the noise corrupts each round independently.

The $c_i' \mapsto r_i'$ function maps one bit to one bit. Its table could be precomputed to save time. Furthermore, these $c_i' \mapsto r_i'$ rounds could be run by analog circuits to avoid many communication delays.

In the verification phase, the prover and the verifier determine a set I of τ round indices which they believe are correct. The way this agreement is done is not important (as long as the prover does not leak). Then, the verifier checks whether I has cardinality τ and the corresponding timers are small enough. If this fails, the verifier rejects. As a concrete instance for I agreement, we suggest that the prover sends (through the lazy noiseless channel) the c' and r' to the verifier. The verifier then takes the first τ rounds for which $c_i = c_i'$, $r_i = r_i'$, and $\mathsf{timer}_i \leq 2B$ to define I and sends I to the prover. If there are not enough correct rounds, the protocol aborts.

Next, the prover and the verifier run the interactive proof ZKP_κ to show that the responses r_i's are consistent with the A_i's and y_j's. Namely, for $i \in I$, they compute

$$z_i = A_i \left(\theta^{b_i} \prod_{j=1}^{s} y_j^{\mu_{i,j}} \right)^{c_i} \theta^{-r_i} \quad , \quad \zeta_i = \rho_i \left(\prod_{j=1}^{s} H(x,j)^{\mu_{i,j}} \right)^{c_i'}$$

Since $A_i = \theta^{a_i} \rho_i^2$, $y_j = \theta^{x_j} H(x,j)^2$, and $x_i' = \sum_{j=1}^{s} \mu_{i,j} x_j$, it is easy to verify that $r_i = a_i + c_i b_i + c_i x_i'$ is equivalent to the existence of ζ_i such that $z_i = \zeta_i^2$. That is, $z_i \in L$. If this fails, the protocol aborts. If no iteration aborts, the verifier accepts and sends $\mathsf{Out}_V = 1$. Otherwise, he sends $\mathsf{Out}_V = 0$.

3.3 Analysis

We first define the required properties on the $\mathcal{M}$ set.

Definition 7 ($\mathcal{M}$-set). *Given parameters s, n, δ, ε, q, (s, n, and q being polynomially bounded) and a function F on $\{0,1\}^s$, we say that a set $\mathcal{M}$ of $n \times s$ Boolean matrices is a (δ, q, ε)-set with hint F if there exist three PPT algorithms* Decode, ExtractFromSample, *and* ExtractFromOracle *such that:*

- *for all x, $y = F(x)$, $\mu \in \mathcal{M}$, ξ such that the Hamming distance between ξ and $\mu(x)$ is at most $\delta - 1$, we have* $\mathsf{Decode}(\xi, y) = \mu(x)$*;*
- *for all x, $y = F(x)$,* $\Pr[\mathsf{ExtractFromSamples}(\mu^1, \mu^1(x), \ldots, \mu^q, \mu^q(x), y) = x] \geq \frac{1}{2}$ *where $\mu^1, \ldots, \mu^q \in \mathcal{M}$ are randomly picked and independent;*
- *for all i, x, $y = F(x)$, given an oracle $O(\mu)$ such that for $\mu \in \mathcal{M}$ uniformly distributed,* $\Pr[O(\mu) = \mu_i(x)] \geq \frac{1}{2} + \varepsilon$*, we have* $\Pr[\mathsf{ExtractFromOracle}^O(i, y) = x] \geq \frac{1}{2}$.

What we want is to be able to decode $\mu(x)$ from a noisy version ξ, to make $\mu(x)$ leak. We want to have an extraction of x from a limited number of correct samples $(\mu, \mu(x))$, and also an extraction of x from a single bit of a polynomial number of samples $(\mu_i, \mu_i(x))$ which may be noisy.

We note that if $\mathcal{M}$ is a (δ, q, ε)-set with hint F, there must exist some μ, x_0, and x_1 such that $\mu(x_0) \neq \mu(x_1)$ (otherwise, no ExtractFromSamples would exist). Clearly, there is some ξ within a distance up to $\lceil \frac{n}{2} \rceil$ to both $\mu(x_0) = 0$ and $\mu(x_1) = 1$. So, $\delta \leq \lceil \frac{n}{2} \rceil$. We achieve this upper bound with $\mathcal{M}_{\mathsf{repeat}}$ as the following lemma shows.

Lemma 8. *If* Com_H *is perfectly binding, for any constant* $\varepsilon > 0$, $\mathcal{M}_{\mathsf{repeat}}$ *is a* $(\lceil \frac{n}{2} \rceil, s, \varepsilon)$*-set with hint* Com_H.

Proof. Clearly, if ξ has a Hamming distance up to $\lceil \frac{n}{2} \rceil - 1$ to $\mu(x)$, then the majority of the bits of ξ is equal to every $\mu_j(x)$. So, we can compute $\mathsf{Decode}(\xi, y) = \mu(x)$ by majority decoding. The hint y is not used here.

Given s samples $\mu^1, \ldots, \mu^s \in \mathcal{M}_{\mathsf{repeat}}$, the probability that they span a space of dimension at least $s-1$ is larger than $\frac{1}{2}$. So, if we only have $s-1$ linearly independent vectors μ_1^i, we can solve the system and deduce two possible values for x. The right one is obtained by checking the hint (which is non-ambiguous since Com_H is perfectly binding). So, this defines $\mathsf{ExtractFromSamples}$ to extract x from s samples with probability at least $\frac{1}{2}$.

Given an oracle $O(\mu)$ producing b such that $\Pr[b = \mu_i(x)] \geq \frac{1}{2} + \varepsilon$, we can use the Goldreich-Levin polynomial algorithm [18] which extracts a list of size $O(\varepsilon^{-2})$ containing x with probability at least $\frac{1}{2}$. Clearly, we can test each of these values with the non-ambiguous hint y. So, we can isolate x. □

Theorem 9. *We assume that* n *is linear in* λ *and that* $\frac{\tau}{n} < 1 - p_{\mathsf{noise}} - \varepsilon$ *for some constant* ε*. Under the assumption that* Com *is a homomorphic bit commitment [Def. 15] and that* ZKP_κ *is complete [Def. 16], the ProProx protocol is a PoPoK when the challenge/response rounds are subject to a noise level of* p_{noise} *[Def. 2].*

We further assume that n' *is linear in* λ *and that* $\frac{\tau}{n} \geq 1 - (\frac{1}{2} - 2\varepsilon)\frac{\delta}{n}$ *and* $\frac{\tau}{n} \geq \frac{3}{4} + \varepsilon$*, for some parameter* δ*. Under the assumption that* $\mathcal{M}$ *is a* (δ, q, ε)*-set with hint* Com_H*, that* Com *is a perfectly binding, computationally hiding, and homomorphic bit commitment [Def. 15], that* Com_H *is one-way [Def. 18], and that* ZKP_κ *is a* κ*-sound [Def. 16] computationally zero-knowledge [Def. 17] proof of membership for* $\kappa = \mathsf{negl}(\lambda)$*, the ProProx protocol is a sound [Def. 5] and secure [Def. 4] PoPoK.*

We note that for $\delta \leq \frac{n}{2}$, $\frac{\tau}{n} \geq 1 - (\frac{1}{2} - 2\varepsilon)\frac{\delta}{n}$ implies $\frac{\tau}{n} \geq \frac{3}{4} + \varepsilon$. So this latter condition is only to be checked for n odd and $\delta = \lceil \frac{n}{2} \rceil$.

Proof. Proving completeness is straightforward: when $\frac{\tau}{n} < 1 - p_{\mathsf{noise}} - \varepsilon$, we have less than τ noiseless rounds with probability $1 - \mathsf{Tail}(n, \tau, 1 - p_{\mathsf{noise}}) < e^{-2\varepsilon^2 n}$ due to the Chernoff-Hoeffding bound (see Appendix A), which is negligible. Then, the completeness failure is bounded by

$$p_{\mathsf{Comp}} = 1 - \mathsf{Tail}\,(n, \tau, 1 - p_{\mathsf{noise}})^{n'} \tag{1}$$

which is also negligible. We prove in Lemma 10 that ProProx is sound. We prove in Lemma 11 that ProProx is zero-knowledge. This is finally used to prove in Lemma 12 that ProProx is secure. □

Lemma 10 (Soundness). *We assume that* n *is linear in* λ *and that* $\frac{\tau}{n} \geq 1 - (\frac{1}{2} - 2\varepsilon)\frac{\delta}{n}$ *for some constant* ε *and some parameter* δ*. Under the assumption that* $\mathcal{M}$ *is a* (δ, q, ε)*-set with hint* Com_H*, that* Com *is a perfectly binding homomorphic bit commitment, and that* ZKP_κ *is a* κ*-sound proof of membership for* $\kappa = \mathsf{negl}(\lambda)$*, the ProProx protocol is a sound proof of proximity.*

Proof. We fix the random coins of participants other than $\mathcal{V}$. We define $p_B = \mathsf{Tail}(\delta, \tau - n + \delta, \frac{1}{2})$. We assume that we have an experiment making $\mathcal{V}$ accept with probability $p \geq \gamma$ where

$$\gamma = (\kappa + (1 - \kappa) q . p_B)^{n'} \tag{2}$$

Since $\frac{\tau - n + \delta}{\delta} \geq \frac{1}{2} + 2\varepsilon$, we have $p_B \leq e^{-8\varepsilon^2 n}$ due to the Chernoff-Hoeffding bound (see Appendix A), which is negligible. So, γ is negligible.

We take the viewpoint of $\mathcal{V}$. Since we have a perfectly binding commitment, the value y_j uniquely defines $x_j = \mathsf{Com}^{-1}(y_j)$, and the value of A_i uniquely defines $a_i = \mathsf{Com}^{-1}(A_i)$. This further uniquely defines $x' = \mu(x)$. The purpose of the proof is to show that we can compute x. If $\mathcal{V}$ accepts with probability p, since all iterations are independent (as we fixed the coins which are not from $\mathcal{V}$), there must exist i' such that the i'th iteration pass with probability $p_{i'}$ such that $p_{i'} \geq p^{\frac{1}{n'}}$. Due to the κ-soundness of ZKP_κ (Def. 16), the statement that for any $i \in I$, $z_i \in L$ is valid with probability at least $p' = \frac{p_{i'}-\kappa}{1-\kappa} \geq q.p_B$. In the case where the statement holds, we deduce that for all $i \in I$, z_i is a commitment to zero. Due to the homomorphic property of Com, we know that z_i is the commitment to $a_i + c_i b_i + c_i x'_i - r_i$. So, we deduce that $r_i = a_i + c_i b_i + c_i x'_i$ for all $i \in I$ with probability at least $p' \geq q.p_B$.

Thanks to Lemma 1, when r_i comes from a close-by participant, we can write

$$r_i = \mathsf{Algo}(\mathsf{View}_i, c_i, \mathsf{Other}_i)$$

with View_i the partial view (before being able to see c_i) of close-by participants and messages Other_i independent (in the sense of Lemma 1) from c_i coming to these participants from far-away. Note that both View_i and Other_i can be computed from the final views of the close-by participants. So, we can compute the guess $\xi_i = \mathsf{Algo}(\mathsf{View}_i, 1, \mathsf{Other}_i) - \mathsf{Algo}(\mathsf{View}_i, 0, \mathsf{Other}_i) - b_i$ for x'_i. If we have two correct answers r_i to the challenges 0 and 1, then $\xi_i = x'_i$. But wrong answers may give wrong guesses for x'_i.

Note that if the answer r_i comes to $\mathcal{V}$ from far-away, we can still apply Lemma 1 and deduce that the answer is the same for $c_i = 0$ and $c_i = 1$: we have $\xi_i = -b_i$.

Let R_i be the number of challenge values for which the answer is correct in round i. If $R_i = 2$, we have $\xi_i = x'_i$. If $R_i = 1$, we have $\xi_i \neq x'_i$. Let $\mathcal{R}$ be the set of all $R = (R_1, \ldots, R_n)$ such that the number of i's with $R_i = 2$ is at most $n - \delta$. For $R \notin \mathcal{R}$, we can decode: we can compute more than $n - \delta$ values x'_i correctly, so have less than δ incorrect ones, so apply $\mathsf{Decode}(\xi, y)$ and obtain $\mu(x)$. Let S be the event that at least τ rounds give a correct answer. Clearly, $\Pr[S] \geq p'$. Clearly, $p_B = \max_{R \in \mathcal{R}} \Pr[S|R]$ (for $n - \delta$ values i such that $R_i = 2$ and δ values i such that $R_i = 1$). For $R \in \mathcal{R}$, we have $\Pr[S, R] \leq p_B \Pr[R]$. So, $\Pr[R \notin \mathcal{R}|S] \geq 1 - \frac{p_B}{p'} \geq 1 - \frac{1}{q}$. This means that given that $\mathcal{V}$ accepts, we extract $\mu(x)$, with probability at least $1 - \frac{1}{q}$.

We iterate $O(\frac{1}{p})$ times until one experiment succeeds, get the views and transcript and extract a pair $(\mu, \mu(x))$. (Note that μ is available from the transcript.) This generate a vector of n' samples $(\mu, \mu(x))$ (with possible error). We iterate q times to generate q vectors of samples. We obtain the existence of a coordinate i' in which we can read q samples with no errors with probability at least $(1 - \frac{1}{q})^q$, which is constant. When there is no error, $\mathsf{ExtractFromSamples}$ succeeds to extract x with constant probability. If the extraction fails, we can just iterate. With a constant number of iterations, we finally extract x. □

Lemma 11 (Zero-knowledge). *Under the assumption that* Com *is a computationally hiding bit commitment and that* ZKP_κ *is a computationally zero-knowledge proof of membership, The ProProx protocol is zero-knowledge following Def. 17.*

Proof. We have to prove that, given two participants $P(x)$ and $V^*(y, \mathsf{aux})$, there exists a simulator $S(y, \mathsf{aux})$ such that $V^*(y, \mathsf{aux}) \leftrightarrow P(x)$ produces a view of $V^*(y, \mathsf{aux})$ which is computationally indistinguishable from the output of $S(y, \mathsf{aux})$. Clearly, we can assume without loss of generality that $n' = 1$. We will actually construct a sequence of simulations. We define an interactive $V'(y, \mathsf{aux})$ to replace $V(y, \mathsf{aux})$, and some interactive $P'(x)$ and P'' to replace $P(x)$.

We denote $\bar{z} = (z_i)_{i\in I}$ and $\bar{\zeta} = (\zeta_i)_{i\in I}$. We split $V^*(y,\mathsf{aux})$ into two protocols $V_1(y,\mathsf{aux})$ and $V_2(\bar{z},\mathsf{aux}')$, where V_1 mimics V^* until the $\mathsf{ZKP}_\kappa(\bar{z}:\bar{\zeta})$ protocol must start. Actually, V_2 executes only $\mathsf{ZKP}_\kappa(\bar{z}:\bar{\zeta})$ where aux' is the final view of $V_1(y,\mathsf{aux})$. The final view of $V_2(\bar{z},\mathsf{aux}')$ is of form $v=(\bar{z},\mathsf{aux}',t)$. We write $g(v)=(\mathsf{aux}',t)$, which is the final view of $V^*(y,\mathsf{aux})$. Similarly, we split $P(x)$ into $P_1(x)$ and $P_2(x,u)$ where (x,u) is the view of $P_1(x)$. Clearly, running either $V^*(y,\mathsf{aux}) \leftrightarrow P(x)$ and taking the final view of V^*, or $V_1(y,\mathsf{aux}) \leftrightarrow P_1(x)$, $V_2(\bar{z},\mathsf{aux}') \leftrightarrow P_2(x,u)$, then taking $g(v)$ is the same. This simulation is illustrated on the left-hand side of Fig. 2.

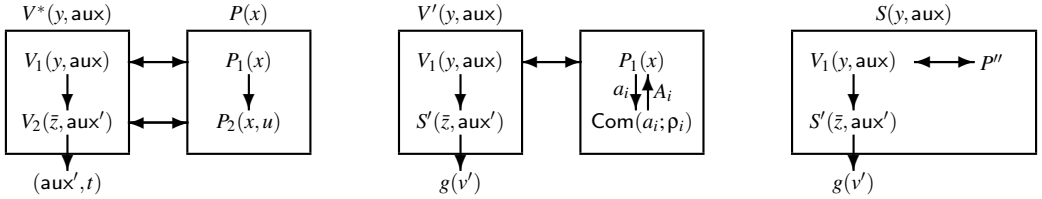

Fig. 2. Applying a ZK Reduction.

First, $V'(y,\mathsf{aux})$ runs a simulation of $V_1(y,\mathsf{aux})$ interacting with $P_1(x)$. Then, $V'(y,\mathsf{aux})$ runs the simulator $S'(\bar{z},\mathsf{aux}')$ of the $\mathsf{ZKP}_\kappa(\bar{z}:\bar{\zeta})$ protocol associated to the verifier $V_2(\bar{z},\mathsf{aux}')$. Let v' be the output of $S'(\bar{z},\mathsf{aux}')$. Finally, $V'(y,\mathsf{aux})$ produces $g(v')$ as an output. This simulation is illustrated on the middle of Fig. 2. Due to the zero-knowledge property of $\mathsf{ZKP}_\kappa(\bar{z}:\bar{\zeta})$, v' is computationally indistinguishable from the final view of $V_2(\bar{z},\mathsf{aux}')$. So, the final view of $V'(y,\mathsf{aux})$ in $V'(y,\mathsf{aux}) \leftrightarrow P_1(x)$ and the final view of $V^*(y,\mathsf{aux})$ in $V^*(y,\mathsf{aux}) \leftrightarrow P(x)$ are indistinguishable.

Note that $P_1(x)$ makes no longer extra use of the coins ρ_i's (as $P_2(x,u)$ does in ZKP_κ). So, the commitment can be outsourced to a challenger playing the real-or-random hiding game for Com. We modify $P_1(x)$ into an algorithm $P'(x)$ who sets A_i to the commitment to some random bit instead of a_i, and stops before ZKP_κ. Thanks to the hiding property of Com, the output of $V'(y,\mathsf{aux}) \leftrightarrow P_1(x)$ and of $V'(y,\mathsf{aux}) \leftrightarrow P'(x)$ are indistinguishable.

Finally, r'_i in $P'(x)$ is now uniformly distributed and independent from all the rest, so we change $P'(x)$ into an algorithm P'' which sends a random r'_i instead. Note that P'' no longer needs x. So, the view of V^* in $V^*(y,\mathsf{aux}) \leftrightarrow P(x)$ and the output of $V'(y,\mathsf{aux}) \leftrightarrow P''$ are indistinguishable. This defines a simulator $S(y,\mathsf{aux})$, as illustrated on the right-hand-side of Fig. 2.

Overall, the advantage to distinguish is bounded by

$$p_{\mathsf{ZK}} = n'(p_{\mathsf{ZKP}} + p_{\mathsf{Com}}) \tag{3}$$

where p_{ZKP} is the advantage to distinguish the ZK simulation from real in the ZKP protocol and p_{Com} is the bound on the hiding property of Com. □

Lemma 12 (Security). *We assume that n' is linear and that $\frac{\tau}{n} \geq \frac{3}{4}+\varepsilon$ for some constant ε. Under the assumption that $\mathcal{M}$ is a (δ,q,ε)-set with hint Com_H, that Com is a perfectly binding, and computationally hiding bit commitment, that Com_H is one-way, and that ZKP_κ is a κ-sound computationally zero-knowledge proof of membership for $\kappa = \mathsf{negl}(\lambda)$, the ProProx protocol is secure following Def. 4.*

Proof. We consider an experiment exp with a honest always far-away prover. Let p be the probability that $\mathcal{V}$ accepts in one of the n' iterations. We want to show that $p = 1-\Omega(1)$ so that $p^{n'} = \mathsf{negl}(\lambda)$. For this, we construct a polynomial extractor for the secret x in the bad case that the ith round of one

iteration has a correct answer with probability larger than $\frac{3}{4}+\frac{\varepsilon}{2}$. Then, we apply the zero-knowledge property of the protocol to deduce an algorithm to invert Com_H using ExtractFromOracle. Finally, the one-wayness of Com_H allows us to conclude that each round passes with probability bounded by $\frac{3}{4}+\frac{\varepsilon}{2}$ for all i, except in the negligible bad cases. So, for $\frac{\tau}{n} \geq \frac{3}{4}+\varepsilon$, each iteration must fail with probability $\Omega(1)$.

Like in the proof of Lemma 10, the view of $\mathcal{V}$ uniquely defines the x_i's, a_i's, and x_i''s due to the perfectly binding property. Thanks to soundness, in each of the n' independent iterations, $r_i = a_i + c_i b_i + c_i x_i'$ for all $i \in I$ with probability at least $p' = \frac{p-\kappa}{1-\kappa}$. (See the proof of Lemma 10.)

We let $i \in \{1,\ldots,n\}$ be fixed. We apply Lemma 1 and write $r_i = \mathsf{Algo}(\mathsf{View}_i, c_i, \mathsf{Other}_i)$. The values View_i and Other_i are independent (in the sense of Lemma 1) of c_i. We let $p_i(x)$ be the probability (over all coins except the selection of x) that $r_i = a_i + c_i b_i + c_i x_i'$. We let Bad be the set of all x for which $p_i(x) \geq \frac{3}{4}+\frac{\varepsilon}{2}$. We want to show that $\Pr[x \in \mathsf{Bad}]$ is negligible.

Assuming $x \in \mathsf{Bad}$, we construct an online extractor playing with $P(x)$ in an interactive game such that, given μ random, it computes correctly $\mu_i(x)$ with probability at least $\frac{1}{2}+\varepsilon$. We do it as follows: The extractor simulates the experiment (with $\mathcal{V}$ selecting μ) to $P(x)$ and computes Algo, View_i, and Other_i following Lemma 1. Then, this extractor computes

$$\xi_i = \mathsf{Algo}(\mathsf{View}_i, 1, \mathsf{Other}_i) - \mathsf{Algo}(\mathsf{View}_i, 0, \mathsf{Other}_i) - b_i$$

Thanks to View_i and Other_i being independent from c_i, we need not rewind any $P(x)$: the extraction is straightline!

Let p_2 be the probability that $\mathsf{Algo}(\mathsf{View}_i, 1, \mathsf{Other}_i) = a_i + b_i + x_i'$ and $\mathsf{Algo}(\mathsf{View}_i, 0, \mathsf{Other}_i) = a_i$. We have $\Pr[\xi_i = x_i'] \geq p_2$ and $p_i(x) \leq \frac{1}{2}(1-p_2)+p_2$. So, $\Pr[\xi_i = x_i'] \geq 2p_i(x)-1$. Due to badness, we have $p_i(x) \geq \frac{3}{4}+\frac{\varepsilon}{2}$ and we obtain that $\Pr[\xi_i = \mu_i(x)] \geq \frac{1}{2}+\varepsilon$. So, we have our online oracle O.

We can now apply $\mathsf{ExtractFromOracle}^O(i,y)$ extraction to obtain x with probability at least $\frac{1}{2}$. This defines a polynomial algorithm to invert Com_H in the $x \in \mathsf{Bad}$ case. This algorithm is still playing with $P(x)$.

We now apply the zero-knowledge property from Lemma 11 to transform the online extractor in a standalone algorithm based on y only. Note that we assumed non-concurrency of the honest provers, so there is no problem is applying the rewinding simulator iteratively for all instances of the prover. We obtain a polynomial inversion algorithm for Com_H working with probability at least $\frac{1}{2} - \mathsf{negl}(\lambda)$ when $x \in \mathsf{Bad}$. So, it works for x random with probability at least $\frac{1}{2}\Pr[x \in \mathsf{Bad}] - \mathsf{negl}(\lambda)$. Due to the one-wayness of Com_H [Def. 18], this probability must be negligible. We deduce $\Pr[x \in \mathsf{Bad}] = \mathsf{negl}(\lambda)$.

The expected number of correct rounds, which is $\sum_i p_i(x)$, is at least $p'\tau$. So, $p' \leq \frac{n}{\tau}\left(\frac{3}{4}+\frac{\varepsilon}{2}\right) + \Pr[x \in \mathsf{Bad}]$. Since we assumed $\frac{\tau}{n} \geq \frac{3}{4}+\varepsilon$ with ε constant, we have $p' = 1-\Omega(1)$, so $p = 1-\Omega(1)$. Since n' is linear, $p^{n'} = \mathsf{negl}(\lambda)$.

Finally, by taking $\varepsilon = \frac{\tau}{n} - \frac{3}{4}$, the attack works with a probability bounded by

$$p_{\mathsf{Sec}} = \left(\kappa + (1-\kappa)\left(\frac{\frac{3}{4}+\frac{\varepsilon}{2}}{\frac{3}{4}+\varepsilon} + n(p_{\mathsf{OW}} + p_{\mathsf{ZK}}.\#\mathsf{Provers})\right)\right)^{n'}$$

where p_{OW} is the one-wayness of Com_H, p_{ZK} comes from Eq. (3), and #Provers is the number of provers in the experiment. If $\mathcal{M}$ is a $(\delta, q, \frac{\tau}{n} - \frac{3}{4})$-set, we can lower ε and obtain

$$p_{\mathsf{Sec}} = \left(\kappa + (1-\kappa)\left(\frac{1}{2} + \frac{3}{8} \times \frac{n}{\tau} + n(p_{\mathsf{OW}} + p_{\mathsf{ZK}}.\#\mathsf{Provers})\right)\right)^{n'} \tag{4}$$

Note that we could not have used the extractor from Lemma 10 since it is not guaranteed to work in polynomial time. Conversely, we could not have used the above extractor for Lemma 10 since the prover is malicious there and leaks on purpose, so we could not use the zero-knowledge argument. □

Note that a malicious prover can run a distance fraud when $\mu(x) = -b$, as r_i no longer depends on c_i. For $\mu \in \mathcal{M}_{\mathsf{repeat}}$ and $b = 0$, this happens with probability $\frac{1}{2}$ in each of the n' iterations. It is even worth if $x = 0$ (as allowed in the malicious prover model) as the distance fraud always works. The is no contradiction with soundness (note that the protocol is also sound for $n' = 1$): an observer seeing the verifier accepts can deduce that $\mu(x)$ is likely to be zero. So, the malicious prover leaks.

To have distance fraud resistance (even for $n' = 1$), we adopt the following trick taken from DB2 [8]: we select a vector b with Hamming weight $\left\lfloor \frac{n}{2} \right\rfloor$ so that half of the rounds will really use c_i. Actually, b has a maximal distance to the code generated by $\mathcal{M}_{\mathsf{repeat}}$.

Lemma 13 (DF-Resistance). *We assume that n is linear and that $\frac{\tau}{n} \geq \frac{3}{4} + \varepsilon$ for some constant ε and that the vector b has a Hamming weight of $\left\lfloor \frac{n}{2} \right\rfloor$. Under the assumption that* Com *is a perfectly binding bit commitment and that ZKP_κ is a κ-sound computationally zero-knowledge proof of membership for $\kappa = \mathsf{negl}(\lambda)$, the ProProx protocol with $\mathcal{M} = \mathcal{M}_{\mathsf{repeat}}$ resists to distance fraud following Def. 6.*

This generalizes to any $\mathcal{M}$ by having b to a distance at least D to the codes generated by all $\mu \in \mathcal{M}$, as long as $2^{-n'D}$ is negligible.

Proof. Due to the perfectly binding property, the view of $\mathcal{V}$ uniquely defines x_i, a_i, and x'_i. Thanks to Lemma 1, r_i is independent (in the sense of Lemma 1) from c_i. So, for $b_i \neq \mu_i(x)$ (which happens for half of the rounds), we have that $\Pr[r_i = a_i + c_i b_i + c_i x'_i] = \frac{1}{2}$. So, the probability that the statement in ZKP_κ holds is bounded by $\mathsf{Tail}(\lfloor \frac{n}{2} \rfloor, \tau - \lceil \frac{n}{2} \rceil, \frac{1}{2})$ which is negligible for $\frac{\tau}{n} \geq \frac{3}{4} + \varepsilon$. Due to the fact that ZKP_κ is sound, the verifier accepts in one iteration with probability bounded by $\kappa + (1 - \kappa)\mathsf{Tail}(\lfloor \frac{n}{2} \rfloor, \tau - \lceil \frac{n}{2} \rceil, \frac{1}{2})$. Finally, the attack succeeds with probability bounded by

$$p_{\mathsf{DF}} = \left(\kappa + (1-\kappa)\mathsf{Tail}\left(\left\lfloor \frac{n}{2} \right\rfloor, \tau - \left\lceil \frac{n}{2} \right\rceil, \frac{1}{2} \right) \right)^{n'} \tag{5}$$

which is also negligible. □

3.4 A Variant for Noiseless Communications

The protocol could be simplified in noiseless environment. For this, we would take $\tau = n = s$ and the set $\mathcal{M}_{\mathsf{rotate}}$ of the n matrices μ making a circular rotation of x (i.e., the identity matrix with a circular rotation of its columns). We can easily see that $\mathcal{M}_{\mathsf{rotate}}$ is a $(\delta, 1, \varepsilon)$-set with hint Com_H for any *constant* $\delta > 0$ and $\varepsilon > 0$: we can decode a constant number of errors in ξ with a hint y by exhaustive search, we can clearly extract x from one sample $(\mu, \mu(x))$..., and we can extract x from random μ_i and noisy bits $b = \mu_i(x)$ with y by majority decoding. There is clearly no need to agree on I which is always the full set $I = \{1, \ldots, s\}$. The protocol is much simpler.

3.5 Concrete Parameters

The proven bounds (2), (4), and (5) may not be tight. The best known attacks correspond to

$$p_{\mathsf{DF}} = \mathsf{Tail}\left(\left\lfloor \frac{n}{2} \right\rfloor, \tau - \left\lceil \frac{n}{2} \right\rceil, \frac{1}{2} \right)^{n'} \quad , \quad p_{\mathsf{Sec}} = \mathsf{Tail}\left(n, \tau, \frac{1}{2} \right)^{n'} \quad , \quad p_{\mathsf{TF}} = \mathsf{Tail}\left(\left\lceil \frac{n}{2} \right\rceil, \tau - \left\lfloor \frac{n}{2} \right\rfloor, \frac{1}{2} \right)^{n'}$$

The DF attack consists of guessing c_i in half of the rounds for which $\mu(x) \neq b_i$. The MF attack follows the post-ask strategy: the adversary first guesses the answers to all challenges then play with the prover with the same challenges. The TF attack consists of giving a table of all $c'_i \mapsto r'_i$ which is corrupted in half of the rounds. So, we could also use these empirical values for the security to derive concrete parameters.

As concrete parameters, we could suggest $s = 80$ bits as the size of the secret and a modulus N of 2048 bits. Then, we look for n, n', and τ which minimize the total number of rounds nn' while keeping $p_{\mathsf{comp}} \approx 1 - 2^{-7}$ and different objectives: we propose several vectors of parameters to reach the online security of either 2^{-20} (*high*) or 2^{-10} (*low*), with *proven* bounds or *empirical* bound, and with either $p_{\mathsf{noise}} = 1\%$ or the noiseless variant from Section 3.4.

security	bounds	p_{noise}	n	n'	τ	nn'	p_{comp}	p_{DF}	p_{Sec}	p_{TF}
high	proven	0.01	37	168	33	6216	$1-2^{-7}$	2^{-1010}	2^{-20}	2^{-63}
high	empirical	0.01	76	1	73	76	$1-2^{-7}$	2^{-24}	2^{-20}	2^{-24}
low	proven	0.01	37	84	33	3108	$1-2^{-8}$	2^{-505}	2^{-10}	2^{-31}
low	empirical	0.01	48	1	45	48	$1-2^{-9}$	2^{-12}	2^{-10}	2^{-12}
high	proven	0	2	104	2	208	1	2^{-103}	2^{-20}	2^{-103}
high	empirical	0	7	7	7	49	1	2^{-20}	2^{-20}	2^{-28}
low	proven	0	2	52	2	104	1	2^{-51}	2^{-10}	2^{-51}
low	empirical	0	5	5	5	25	1	2^{-10}	2^{-10}	2^{-15}

Clearly, there are some reasonable parameters to consider for implementation. ProProx may be hard to implement on NFC credit cards, but, at least all vectors in the noiseless variant and all vectors with the empirical bounds are feasible for implementation on an NFC smartphone for payment applications.

4 Conclusion

We proposed ProProx, the very first PoPoK addressing soundness. It is provably secure. Conceptually, we believe it could integrate well in an infrastructure for contactless payments. A remaining challenge is to construct a more efficient PoPoK. Another open question would be to have a tight security proof for ProProx.

References

1. G. Avoine, A. Tchamkerten. An Efficient Distance Bounding RFID Authentication Protocol: Balancing False-Acceptance Rate and Memory Requirement. In *Information Security ISC'09*, Pisa, Italy, Lecture Notes in Computer Science 5735, pp. 250–261, Springer-Verlag, 2009.
2. A. Bay, I. Boureanu, A. Mitrokotsa, I. Spulber, S. Vaudenay. The Bussard-Bagga and Other Distance-Bounding Protocols under Attacks. In *INSCRYPT'12*, Beijing, China, Lecture Notes in Computer Science 7763, pp. 371–391, Springer-Verlag, 2012.
3. T. Beth, Y. Desmedt. Identification Tokens or: Solving The Chess Grandmaster Problem. In *Advances in Cryptology CRYPTO'90*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 537, pp. 169–176, Springer-Verlag, 1991.
4. I. Boureanu, A. Mitrokotsa, S. Vaudenay. Secure & Lightweight Distance-Bounding. In *Lightweight Cryptography for Security and Privacy LightSec'13*, Gebze, Turkey, Lecture Notes in Computer Science 8162, pp. 97–113, Springer-Verlag, 2013.
5. I. Boureanu, A. Mitrokotsa, S. Vaudenay. Practical & Provably Secure Distance-Bounding. Eprint technical report, 2013. http://eprint.iacr.org/2013/465.pdf
6. I. Boureanu, A. Mitrokotsa, S. Vaudenay. Towards Secure Distance Bounding. In *Fast Software Encryption'13*, Singapore, Lecture Notes in Computer Science 8424, pp. 55–67, Springer-Verlag, 2013.

7. I. Boureanu, A. Mitrokotsa, S. Vaudenay. Practical & Provably Secure Distance-Bounding. To appear in the proceedings of ISC'13.
8. I. Boureanu, S. Vaudenay. Optimal Proximity Proofs. Eprint technical report, 2014. http://eprint.iacr.org/2014/693.pdf
9. S. Brands, D. Chaum. Distance-Bounding Protocols (Extended Abstract). In *Advances in Cryptology EUROCRYPT'93*, Lofthus, Norway, Lecture Notes in Computer Science 765, pp. 344–359, Springer-Verlag, 1994.
10. L. Bussard, W. Bagga. Distance-Bounding Proof of Knowledge to Avoid Real-Time Attacks. In *IFIP TC11 International Conference on Information Security SEC'05*, Chiba, Japan, pp. 223–238, Springer, 2005.
11. H. Chernoff. A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on the sum of Observations. *Annals of Mathematical Statistics*, vol. 23 (4), pp. 493-507, 1952.
12. C.J. F. Cremers, K.B. Rasmussen, B. Schmidt, S. Čapkun. Distance Hijacking Attacks on Distance Bounding Protocols. In *IEEE Symposium on Security and Privacy S&P'12*, San Francisco, California, USA, pp. 113–127, IEEE Computer Society, 2012.
13. Y. Desmedt. Major Security Problems with the "Unforgeable" (Feige-)Fiat-Shamir Proofs of Identity and How to Overcome Them. In *Congress on Computer and Communication Security and Protection Securicom'88*, Paris, France, pp. 147–159, SEDEP Paris France, 1988.
14. U. Dürholz, M. Fischlin, M. Kasper, C. Onete. A Formal Approach to Distance-Bounding RFID Protocols. In *Information Security ISC'11*, Xi'an, China, Lecture Notes in Computer Science 7001, pp. 47–62, Springer-Verlag, 2011.
15. A. Fiat, A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Advances in Cryptology CRYPTO'86*, Santa Barbara, California, U.S.A., Lecture Notes in Computer Science 263, pp. 186–194, Springer-Verlag, 1987.
16. M. Fischlin, C. Onete. Terrorism in Distance Bounding: Modelling Terrorist-Fraud Resistance. In *Applied Cryptography and Network Security ACNS'13*, Banff AB, Canada, Lecture Notes in Computer Science 7954, pp. 414–431, Springer-Verlag, 2013.
17. S. Gambs, C. Onete, J.-M. Robert. Prover Anonymous and Deniable Distance-Bounding Authentication. In *ACM Symposium on Information, Computer and Communications Security (ASIACCS'14)*, Kyoto, Japan, pp. 501–506, ACM Press, 2014.
18. O. Goldreich, L. Levin. A Hard-Core Predicate for all One-Way Functions. In *Proceedings of the 21st ACM Symposium on Theory of Computing*, Seattle, Washington, U.S.A., pp. 25–32, ACM Press, 1989.
19. S. Goldwasser, S. Micali. Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information. In *Proceedings of the 14th ACM Symposium on Theory of Computing*, San Fransisco, California, U.S.A., pp. 365–377, ACM Press, 1982.
20. S. Goldwasser, S. Micali. Probabilistic Encryption. *Journal of Computer and System Sciences*, vol. 28, pp. 270–299, 1984.
21. J. Hermans, R. Peeters, C. Onete. Efficient, Secure, Private Distance Bounding without Key Updates. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks WISEC'13*, Budapest, Hungary, pp. 195–206, ACM, 2013.
22. W. Hoeffding. Probability Inequalities for Sums of Bounded Random Variables. *Journal of the American Statistical Association*, vol. 58, pp. 13–30, 1963.
23. A. Ranganathan, N.O. Tippenhauer, B Škorić, D. Singelée, S. Čapkun. Design and Implementation of a Terrorist Fraud Resilient Distance Bounding System. In *Computer Security - ESORICS'12*, Pisa, Italy, Lecture Notes in Computer Science 7459, pp. 415–432, Springer-Verlag, 2012.
24. A. Ranganathan, B. Danev, S. Čapkun. Low-Power Distance Bounding. Available as CoRR 1404.4435 technical report, Cornell University 2014. http://arxiv.org/abs/1404.4435
25. K.B. Rasmussen, S. Čapkun. Realization of RF Distance Bounding. In *USENIX Security Symposium (USENIX'10)*, Washington, DC, USA, pp. 389–402, USENIX, 2010.
26. S. Vaudenay. On Modeling Terrorist Frauds. In *Provable Security ProvSec'13*, Melaka, Malaysia, Lecture Notes in Computer Science 8209, pp. 1–20, Springer-Verlag, 2013.

A Useful Bounds

We recall here some useful bound on the tail of the binomial distribution.

Lemma 14 (Chernoff-Hoeffding bound [11,22]). *For any ε, n, τ, q such that $\frac{\tau}{n} < q - \varepsilon$, we have $\mathsf{Tail}(n,\tau,q) > 1 - e^{-2\varepsilon^2 n}$. For $\frac{\tau}{n} > q + \varepsilon$, we have $\mathsf{Tail}(n,\tau,q) < e^{-2\varepsilon^2 n}$.*

B Definitions

Definition 15 (Bit commitment). *A bit commitment consists of a PPT algorithm* Com *taking as input* λ*, a bit* $b \in \mathbf{Z}_2$*, and some random* $\rho \in G$*. It computes* $\mathsf{Com}(b;\rho) \in G$*. We define the following properties:*

- *homomorphic: for all* $b, b' \in \mathbf{Z}_2$ *and* $\rho, \rho' \in G$*,* $\mathsf{Com}(b;\rho)\mathsf{Com}(b';\rho') = \mathsf{Com}(b+b';\rho\rho')$*;*
- *perfectly binding: for all* $b, b' \in \mathbf{Z}_2$ *and* $\rho, \rho' \in G$*,* $\mathsf{Com}(b;\rho) = \mathsf{Com}(b';\rho')$ *implies* $b = b'$*;*
- *computationally hiding: for* ρ *random, the distributions of* $\mathsf{Com}(0;\rho)$ *and* $\mathsf{Com}(1;\rho)$ *are computationally indistinguishable.*

Definition 16 (Sound proof of membership). *An interactive proof for a language* L *is a pair of protocols* $(P(\zeta), V(z))$ *of PPT algorithms such that*

- completeness*: for any* $z \in L$ *with witness* ζ*,* $\Pr[\mathsf{Out}_V = 1 : P(\zeta) \leftrightarrow V(z)] = 1$*;*
- κ-soundness*: for any* $z \notin L$ *and any algorithm* P^* *then* $\Pr[\mathsf{Out}_V = 1 : P^* \leftrightarrow V(z)] \leq \kappa$*.*

Definition 17 (Zero-knowledge protocol). *A protocol* $(P(\zeta), V(z))$ *for a language* L *is computationally zero-knowledge for* $P(\zeta)$ *if for any PPT interactive machine* $V^*(z, \mathsf{aux})$ *there exists a PPT algorithm* $S(z, \mathsf{aux})$ *and a negligible* ε *such that for any PPT distinguisher, any* $(z : \zeta) \in L$*, and any* aux*, the advantage for distinguishing the final view of* $V^*(z, \mathsf{aux})$ *in* $P(\zeta) \leftrightarrow V^*(z, \mathsf{aux})$ *and the output of* $S(z, \mathsf{aux})$ *is bounded by* ε*.*

Definition 18 (One-way function). *We consider a function* Com *taking as input* λ *and a message* $x \in \mathbf{Z}_2^s$ *which is computable in deterministic polynomial time. The function is one-way if for any algorithm receiving* $\mathsf{Com}(x)$*, for* $x \in \mathbf{Z}_2^s$ *random, the probability that it outputs* x *is negligible.*

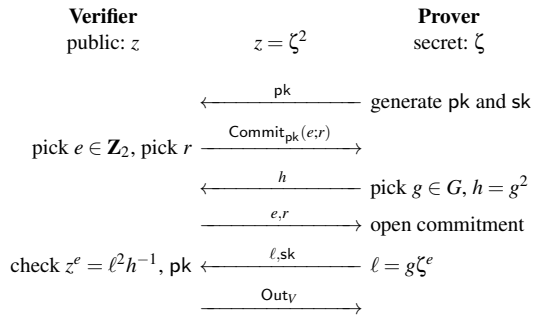

Fig. 3. $\mathsf{ZKP}(z : \zeta)$: a Sound and Zero-Knowledge Proof for z Being a Square based on a trapdoor commitment Commit.

C Case Studies

Example 19. Imagine a protocol in which the prover signs his location (with a challenge), then the verifier checks if this location is close enough. Obviously, this protocol is not sound since a malicious prover could claim to be anywhere. It may not be secure either *in practice*, since an adversary could make the honest prover believe that he is somewhere else. He could just relay GPS, WiFi, or cellular network signals. So, we rather consider protocols not assuming they reliably know their location.

Example 20. We consider a very simple protocol in which a verifier sends a random bitstring as a challenge and the prover must return at once a valid signature of it. This protocol suffers from many problems. First of all, it may not be sound, except if we could make the signature somehow extractable (i.e., we could extract the secret from the view of any signing algorithm). Second, sending a bitstring as a challenge must be done "at once" as we cannot afford loosing time by sending bits sequentially. This requires to send all bits in parallel. Finally, the signature operation would take too much time on any commercial device to make the protocol work with a B low enough. Indeed, the crucial problem in making a PoPoK scheme is to remove all computation from the time-critical challenge-response exchange and to split it into boolean challenge-response rounds.

Example 21. We recall the Brands-Chaum protocol [9] on Fig. 4. It is based on a commitment scheme and a signature scheme. The Brands-Chaum protocol is not sound if the signature resists chosen-message attacks: a far-away malicious prover can let a close-by actor run the protocol then sign the transcript for him.

Example 22. We recall the Hermans-Peeters-Onete protocol [21] on Fig. 5. It is based on the one-more discrete logarithm problem and the decisional Diffie-Hellman problem over elliptic curves. We can easily see that it is not sound. Indeed, the adversary can just relay messages between the prover and the verifier and run the challenge phase after being given the vectors a'_0 and a'_1. These vectors do not leak any sensitive information.

Example 23. We can easily construct a PoPoK based on a symmetric distance bounding protocol by making the shared secret used in distance-bounding be the result on a public-key based key agreement. However, this construction does not provide soundness since leaking the shared secret does not imply leaking the secret key.

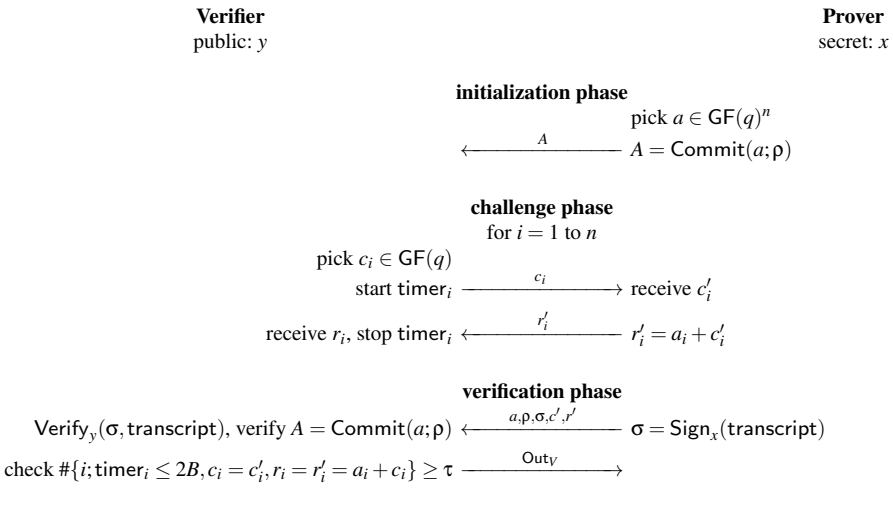

Fig. 4. The Brands-Chaum Protocol [9].

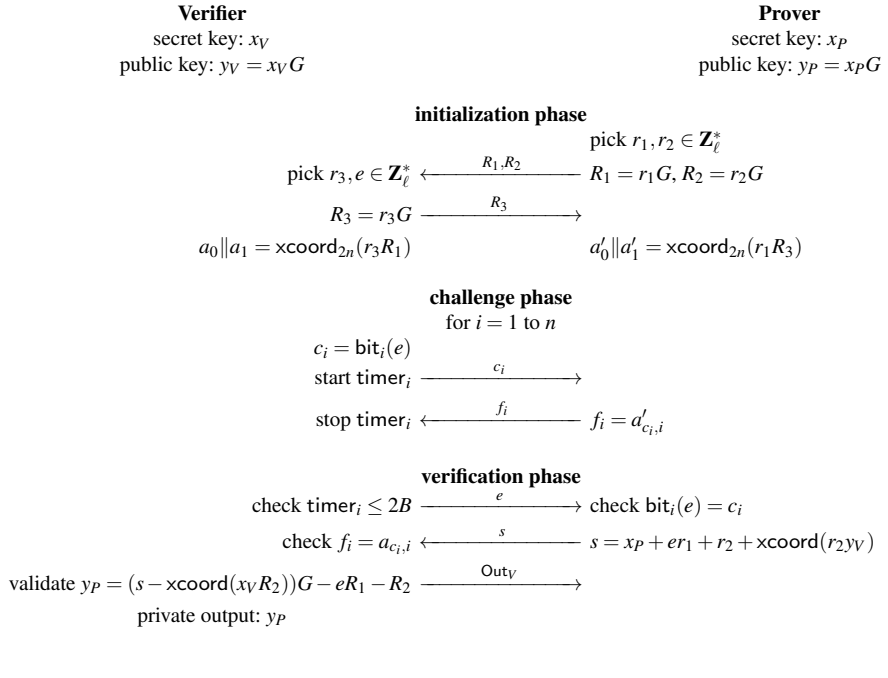

Fig. 5. The Hermans-Peeters-Onete Protocol [21].