Sound Proof of Proximity of Knowledge

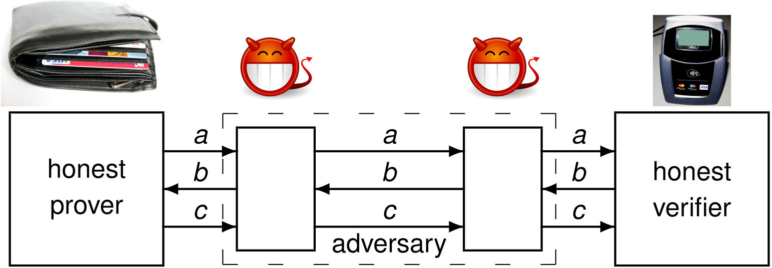
Serge Vaudenay

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

http://lasec.epfl.ch/

1. **Relay Attacks**
2. Formalism for Proofs of Proximity of Knowledge
3. ProProx

Relay Attacks



Relay Attacks in Real

- opening cars and ignition (key with no button)
- RFID access to buildings or hotel room
- toll payment system
- NFC credit card (for payment with no PIN)
- access to public transport
- ...

Using Round-Trip Time

- **Identification Tokens, or: Solving the Chess Grandmaster Problem**
  Beth-Desmedt CRYPTO 1990
- **Distance-Bounding Protocols**
  Brands-Chaum EUROCRYPT 1993

Basic Idea

Verifier		Prover
pick challenge		
start timer	challenge $\longrightarrow$	
stop timer	response $\longleftarrow$	
check timer and response		

Running at the speed of light: 10ns = round-trip of 2×1.5m...
$\rightarrow$ challenge and response are single bits
$\rightarrow$ we iterate many rounds

DB Protocol

Definition

A **distance-bounding protocol** is a tuple (Kgen, P, V, B), made of:

- a PPT algorithm $\mathsf{Kgen} \mapsto (\mathsf{pk}, \mathsf{sk})$;
- a PPT protocol $(P(\mathsf{sk}), V(\mathsf{pk}))$, where
  P is the **proving algorithm**,
  V is the **verifying algorithm**;
- a distance bound B.

At the end, $V(\mathsf{pk})$ sends $\mathsf{Out}_V = 1$ (**accept**) or $\mathsf{Out}_V = 0$ (**reject**).

Completeness: if P and V are at distance $< B$ and there is no malicious behavior, then $\Pr[\mathsf{Out}_V = 1] = 1$.

(could add variants allowing noise)

Experiments

- **instances** of **participants** with location
- **messages** are sent over an insecure broadcast channel and include a destinator
- a message sent at time t_{send} at loc_A is visible at loc_B at time $t_{\text{receive}} \geq t_{\text{send}} + d(\text{loc}_A, \text{loc}_B)$
- **honest** instances run a single P or a single V
- one **distinguished** instance of V; instances within a distance $\leq B$ are **close-by**; others are **far-away**
- honest instances only read messages sent to them
- a honest prover has **non-concurrent** instances
- a **malicious** instance at loc_M could act at time t_{act} to **block** messages from loc_A to loc_B received at time $t_{\text{receive}} \geq t_{\text{act}} + d(\text{loc}_M, \text{loc}_B)$

Security (for the Honest Prover)

Optimal Proximity Proofs

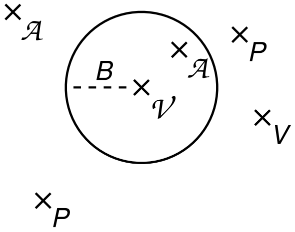
[Boureanu-Vaudenay Inscrypt 2014]

Definition (HP-security)

We say that a DB protocol is **HP-secure** if we have $\Pr[\mathcal{V} \text{ accepts}] = \text{negl}$ for any experiment $\exp(\mathcal{V})$ where

- the prover is honest,
- the prover instances are all far-away from $\mathcal{V}$,

captures man-in-the-middle, impersonation, relay attack, mafia fraud



DF-Resistance

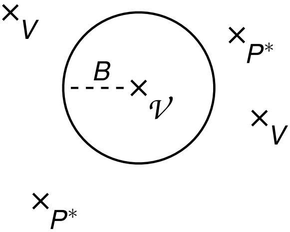
Optimal Proximity Proofs
[Boureanu-Vaudenay Inscrypt 2014]

Definition

We say that a DB protocol **resists to distance fraud** if for any distinguished experiment $\exp(\mathcal{V})$ where

- there is no participant close to $\mathcal{V}$,

we have $\Pr[\mathcal{V} \text{ accepts}] = \text{negl.}$



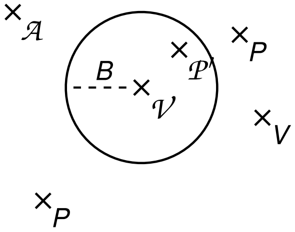
DH-Security (Distance Hijacking)

Private and Secure Public-Key Distance Bounding: Application to NFC Payment [Vaudenay FC 2015]

Definition (DH-security)

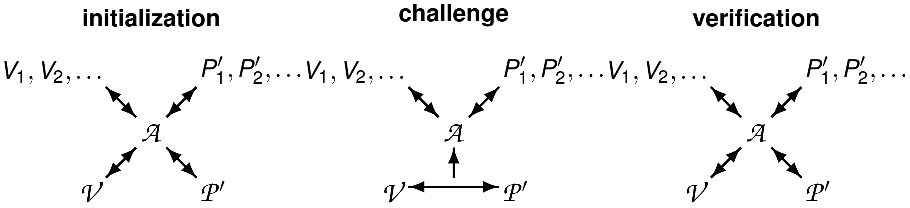
A DB protocol with initialization, challenge, and verification phases is **DH-secure** if for any $\exp(\mathcal{V})$ we have $\Pr[\mathcal{V} \text{ accepts } P'] = \text{negl}$ where

- there are two provers P and P' (with their own keys)
- P' is honest with a distinguished instance $\mathcal{P}'$
- $\mathcal{V}$ and $\mathcal{P}'$ run their challenge phase with matching conversations



DH-Security

the definition boils down to the following scenario with a regular communication model



Soundness

Definition (Soundness)

We say that a DB protocol is *p*-**sound** if for any distinguished experiment $\exp(\mathcal{V})$ in which $\Pr[\mathcal{V}\text{ accepts}] > p$, there exists a PPT algorithm $\mathcal{E}$ called **extractor**, with the following property.
By $\mathcal{E}$ running experiment $\exp(\mathcal{V})$ several times, in some executions denoted $\exp_i(\mathcal{V})$, we have that $\mathcal{E}(\text{View}_1, \ldots) = s$ such that (pk, s) is a possible output of Kgen with expected complexity $\text{poly}/(\Pr[\mathcal{V}\text{ accepts}] - p)$.
View_i denotes in $\exp_i(\mathcal{V})$

- the view of all close-by participants (except $\mathcal{V}$)
- the transcript seen by $\mathcal{V}$

captures terrorist fraud

State of Affair

protocol	Secure	DF	DH	Sound	Privacy	Strong p.	Efficient
Brands-Chaum	☺	☺	☹	☹	☹	☹	☺
DBPK-Log		!☹!		!☹!	☹	☹	☹
HPO	☺	☺	☹	☹	☺	☹	☺
GOR	☺	☺	☹	☹	!☹!	!☹!	☹
privDB	☺	☺	☺	☹	☺	☺	☺
ProProx	☺	☺	☺	☺	☹	☹	☹
eProProx	☺	☺	☺	☺	☺	☺	☹
Eff-pkDB	☺	☺	☺	☹	☹	☹	☺
Eff-pkDB^p	☺	☺	☺	☹	☺	☺	☺

ProProx (Variant I, Noiseless)

Verifier		**Prover**
public: pk	$\mathsf{pk} = \mathsf{Com}_H(\mathsf{sk})$ $(\mathsf{pk}_j = \mathsf{Com}(\mathsf{sk}_j; H(\mathsf{sk}, j)))$	secret: sk

initialization phase

for $i = 1$ to n and $j = 1$ to s

Verifier		Prover
(b: a vector of weight $\frac{n}{2}$)		pick $a_{i,j} \in \mathbf{Z}_2$, $\rho_{i,j}$
	$\xleftarrow{A_{i,j}}$	$A_{i,j} = \mathsf{Com}(a_{i,j}; \rho_{i,j})$

challenge phase

for $i = 1$ to n and $j = 1$ to s

Verifier		Prover
pick $c_{i,j} \in \mathbf{Z}_2$		
start timer$_{i,j}$	$\xrightarrow{c_{i,j}}$	receive $c'_{i,j}$
receive $r_{i,j}$, stop timer$_{i,j}$	$\xleftarrow{r'_{i,j}}$	$r'_{i,j} = a_{i,j} + c'_{i,j} b_i + c'_{i,j} \mathsf{sk}_j$

verification phase

Verifier		Prover
check timer$_{i,j} \leq 2B$		
$z_{i,j} = A_{i,j} \left(\theta^{b_i} \mathsf{pk}_j\right)^{c_{i,j}} \theta^{-r_{i,j}}$	$\xleftrightarrow{ZKP_\kappa(z_{i,j} : \zeta_{i,j}; i,j)}$	$\zeta_{i,j} = \rho_{i,j} H(\mathsf{sk}, j)^{c'_{i,j}}$
	$\xrightarrow{\mathrm{Out}_V}$	

Security of ProProx Variant I

Theorem

If $n = \Omega(\lambda)$ and

- Com *is a perfectly binding, computationally hiding, and homomorphic bit commitment,*
- Com_H *is one-way,*
- ZKP_κ *is a complete κ-sound computationally zero-knowledge proof of membership for $\kappa = \mathrm{negl}(\lambda)$,*

then the protocol is a ***sound*** *and* ***secure*** *PoPoK.*
Furthermore, the protocol is ***DF-*** *and* ***DH-resistant****.*

Proof Technique

- sk is uniquely defined by pk
- given a constant w, we construct a straightline extractor which takes the view of the experiment and returns s such that

$$\Pr[\mathsf{Out}_V = 1, d_H(\mathsf{sk}, s) > w] \leq \left(\frac{1}{2}\right)^{(w+1)\left\lceil \frac{n}{2} \right\rceil} + \kappa$$

  if ZKP is κ-sound. So, if an experiment succeeds with a higher probability, we extract a secret w-close to sk
- we prove the protocol is zero-knowledge
- soundness comes from the extractor (+ enumerate all w-close strings)
- for HP-security, we use the extractor then apply the ZK simulator to show that we can invert Com_H
- DF- and DH-resistance are proven directly

Parameters (Variant I, noiseless)

bound	s	n	w	p_{DF}	p_{Sec}	p_{Sound}	p_{DH}
proven	81	2	41	2^{-22}	2^{-22}	2^{-22}	2^{-22}
empirical	80	2		2^{-80}	2^{-160}	2^{-80}	2^{-160}

proven bounds

$$p_{\text{DF}} = \left(\frac{1}{2}\right)^{s\lfloor \frac{n}{2} \rfloor} + \kappa$$

$$p_{\text{Sec}} = \left(\frac{1}{2}\right)^{(w+1)\lceil \frac{n}{2} \rceil} + \kappa + \text{negl}$$

$$p_{\text{Sound}} = \left(\frac{1}{2}\right)^{(w+1)\lceil \frac{n}{2} \rceil} + \kappa$$

$$p_{\text{DH}} = \left(\frac{1}{2}\right)^{wn} + \kappa$$

empirical bounds

$$p_{\text{DF}} = \left(\frac{1}{2}\right)^{s\lfloor \frac{n}{2} \rfloor}$$

$$p_{\text{Sec}} = \left(\frac{1}{2}\right)^{sn}$$

$$p_{\text{Sound}} = \left(\frac{1}{2}\right)^{s\lfloor \frac{n}{2} \rfloor}$$

$$p_{\text{DH}} = \left(\frac{1}{2}\right)^{sn}$$

Observation (Waste)

- we need $s \geq \lambda$ (otherwise, exhaustive search within less than 2^λ)
- our results need $n = \Omega(\lambda)$

☹ so $\Omega(\lambda^2)$ rounds?!?

☺ when it comes concrete, $n = 2$ is enough

- we need n even (to select a string of weight $\frac{n}{2}$)

☹ so, 160 rounds for an 80-bit security...

- let's try variants when we do not need a string of weight $\frac{n}{2}$

ProProx (Variant II, Noiseless, with $n = 1$)

Verifier	$\mathsf{pk} = \mathsf{Com}_H(\mathsf{sk})$	**Prover**
public: pk	$(\mathsf{pk}_j = \mathsf{Com}(\mathsf{sk}_j; H(\mathsf{sk}, j)))$	secret: sk
	initialization phase	
		pick a_j, ρ_j, $j = 1, \ldots, s$
	$\xleftarrow{A_1, \ldots, A_s}$	$A_j = \mathsf{Com}(a_j; \rho_j)$
pick $b \in \mathbf{Z}_2^s$	$\xrightarrow{b}$	
	challenge phase	
	for $j = 1$ to s	
pick $c_j \in \mathbf{Z}_2$		
start timer$_j$	$\xrightarrow{c_j}$	receive c'_j
receive r_j, stop timer$_j$	$\xleftarrow{r'_j}$	$r'_j = a_j + c'_j b_j + c'_j \mathsf{sk}_j$
	verification phase	
check timer$_j \leq 2B$		
$z_j = A_j \left(\theta^{b_j} \mathsf{pk}_j\right)^{c_j} \theta^{-r_j}$	$\xleftrightarrow{ZKP_\kappa(z_j:\zeta_j;j)}$	$\zeta_j = \rho_j H(\mathsf{sk}, j)^{c'_j}$
	$\xrightarrow{\mathsf{Out}_V}$	

Security of ProProx Variant II

Theorem

If $n = \Omega(\lambda)$ *and*

- Com *is a perfectly binding, computationally hiding, and homomorphic bit commitment,*
- Com_H *is one-way,*
- ZKP_κ *is a complete* κ*-sound computationally zero-knowledge proof of membership for* $\kappa = \mathsf{negl}(\lambda)$*,*

then the protocol is a ***sound*** *and* ***secure*** *PoPoK.*
Furthermore, the protocol is ***DF-*** *and* ***DH-resistant****.*

bad news: does not work with $n = 1$

Exact Security with $n = 1$

1. use instead $s = \Omega(\lambda)$ (we have $s \geq \lambda$ anyway)
2. use an exact w (non-constant)
   - take any w such that $\sum_{i=0}^{w} \binom{s}{i} < 2^{\lambda}$
   - string extraction with $p_{\text{Sound}} = \left(\frac{1}{2}\right)^{w+1} + \kappa$
   - $w = \frac{\lambda}{\log s}$ is ok

polynomial vs non-polynomial -style security does not work
but we can allow the extractor to run in complexity 2^{λ}

Parameters (Variant II, noiseless, with $n = 1$)

bound	s	n	w	p_{DF}	p_{Sec}	p_{Sound}	p_{DH}
proven	81	1	41	2^{-22}	2^{-22}	2^{-22}	2^{-22}
empirical	80	1		2^{-33}	2^{-80}	2^{-80}	2^{-80}

proven bounds

$$p_{DF} = \left(\frac{3}{4}\right)^{s} + \kappa$$

$$p_{Sec} = \left(\frac{1}{2}\right)^{w+1} + \kappa + \text{negl}$$

$$p_{Sound} = \left(\frac{1}{2}\right)^{w+1} + \kappa$$

$$p_{DH} = \left(\frac{1}{2}\right)^{w} + \kappa$$

empirical bounds

$$p_{DF} = \left(\frac{3}{4}\right)^{s}$$

$$p_{Sec} = \left(\frac{1}{2}\right)^{s}$$

$$p_{Sound} = \left(\frac{1}{2}\right)^{s}$$

$$p_{DH} = \left(\frac{1}{2}\right)^{s}$$

Conclusion

- soundness fills the gap between TF and interactive proofs
- first public-key DB protocol which is sound
- also DH-resistant
- not really efficient
- no privacy (but stay tuned...)