EUROCRYPT 2012

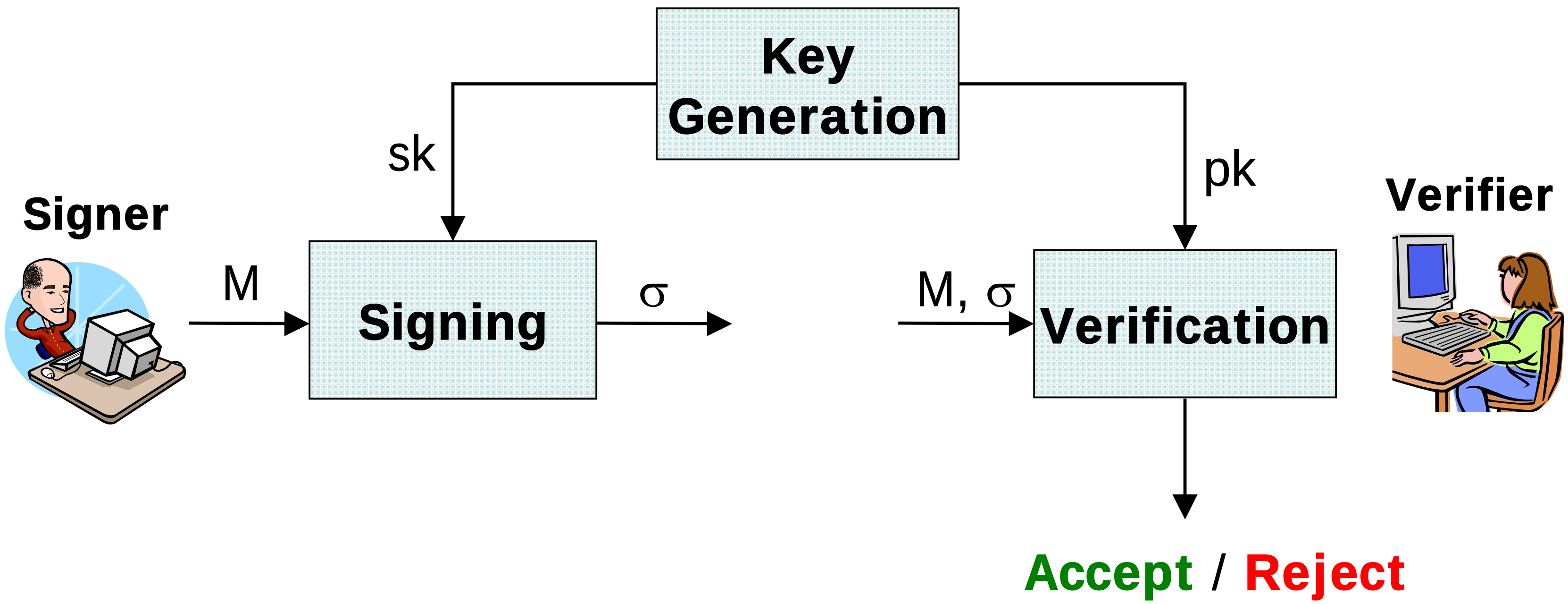
« Tightly-Secure Signatures from Lossy Identification Schemes »

18 April 2012

Michel Abdalla
École normale supérieure & CNRS

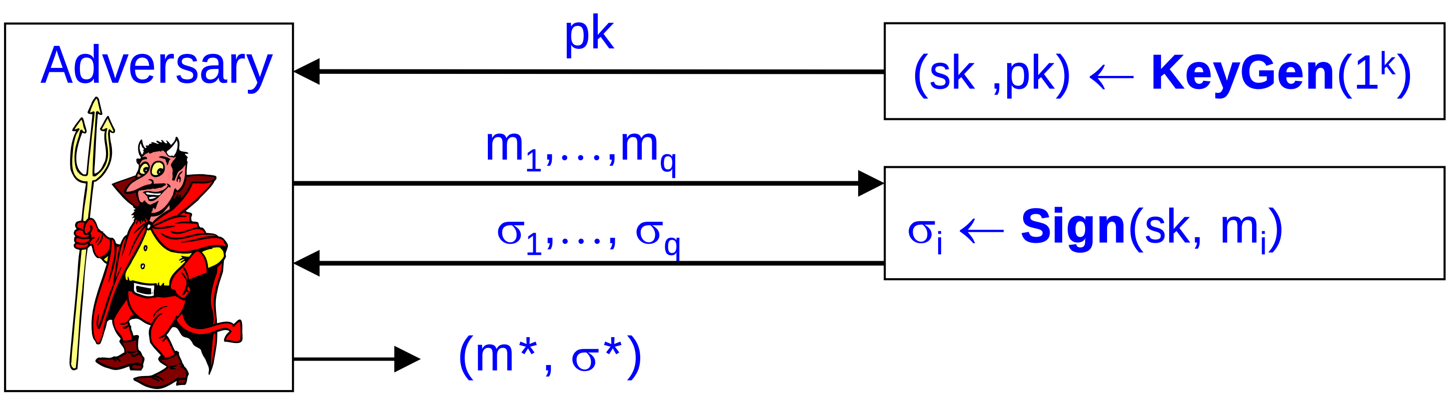
Joint work with
Pierre-Alain Fouque, Vadim Lyubashevsky and Mehdi Tibouchi

Signature schemes



Security of signature schemes

- Strong Existential unforgeability under chosen-message attacks [GMR88]

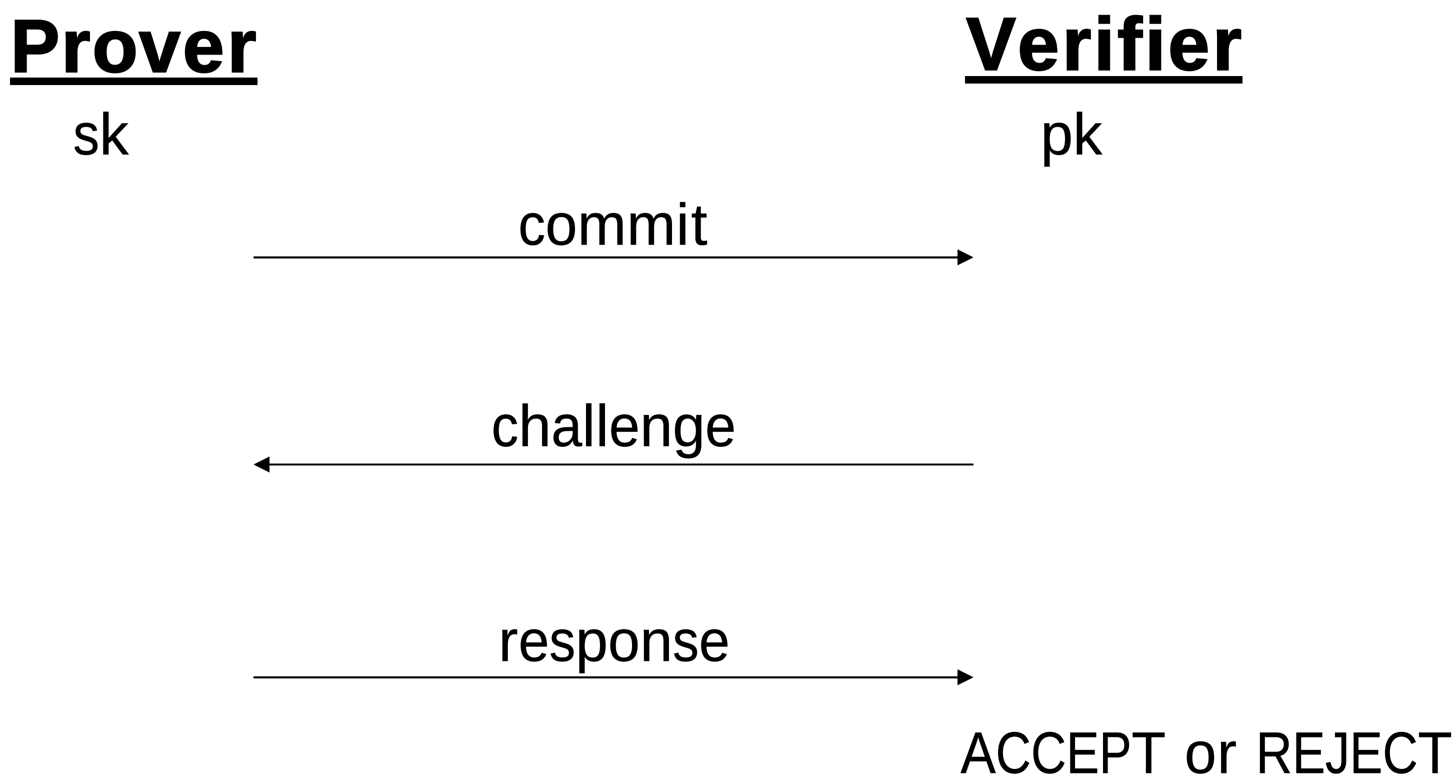


- Adversary wins if **Verify(pk,m*,σ*)=Accept** and **(m*, σ*)** was not previously queried

Common methods for obtaining signature schemes

- Full Domain Hash
  - Let (f,f^{-1}) be a trapdoor one-way permutation
  - Let H be a random oracle
  - $\sigma = f^{-1}(H(m))$
- Identification-based signatures
  - Start with a “secure” identification scheme
  - Make it non-interactive with the help of a random oracle

Canonical identification scheme



Fiat-Shamir transform

Prover

sk

Verifier

pk

commit

challenge =

H(message,commit)

response

ACCEPT or REJECT

Tightness of security reductions

- What do we mean by tightness?
  - [BR96]: Adversary against scheme can be transformed into an adversary against underlying assumption with similar success probability and time complexity
- Can help set parameters for the scheme

FDH and alternatives with tight security

- PSS - probabilistic signature scheme [BR96]
- Magic bit by Katz and Wang [KW03]
- Goh and Jarecki CDH-based scheme [GJ03]
- Kakvi and Kiltz [KK12]

On the exact security of identification-based signatures

- If the ID scheme is secure against passive adversaries, then the signature scheme is existentially unforgeable [AABN02]
  - $\varepsilon_{sig}(k) \approx \mathbf{q_H} \times \varepsilon_{id}(k) + \mathrm{negl}(k)$
  - Proof of passive security of the ID scheme is usually based on rewinding
- Direct proofs based on the forking lemma also lose a $\mathbf{q_H}$ factor [PS96]

Fiat-Shamir alternatives with tight security

- Katz-Wang DDH-based signature scheme [KW03]
  - Uses the Fiat-Shamir heuristic based on a proof of membership for the language $\{g,h,g^r,h^r\}$ instead of a proof of knowledge
  - Has a tight reduction to a decisional Diffie-Hellman problem

Our results

- **We extend the results by Katz and Wang to other settings**
  - New schemes based on the decisional short-discrete-log problem, Ring-LWE, and subset sum
- **A generic proof of security based on *lossy identification schemes***
  - Refines the results in [AABN]: No q_H factor
  - Formalizes the intuition behind the Katz-Wang signature scheme

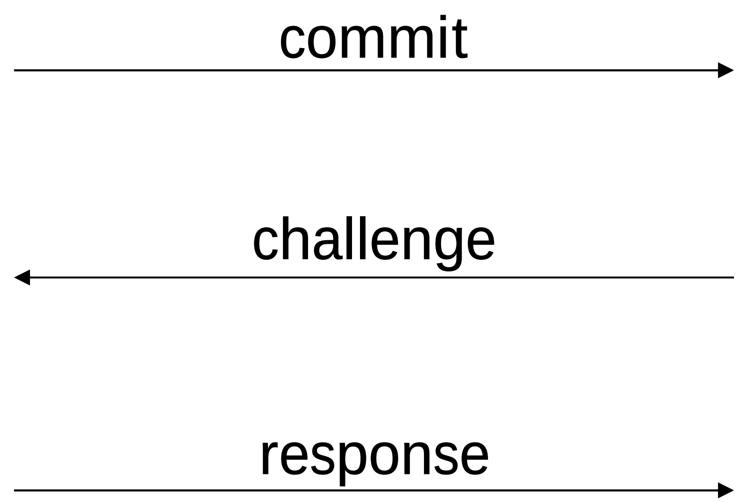
Plan

- Introduction
- **Identification schemes**
- Lossy identification schemes
- Instantiations of lossy ID schemes
- Concluding remarks

Canonical identification scheme

<u>Prover</u> **<u>Verifier</u>**

sk pk



ACCEPT or REJECT

Passive security for ID schemes

- Let $Tr_{pk,sk,k}()$ be a transcript generation oracle
- Passive security experiment

  Exp(A,KG,Tr)
  - $(pk,sk) \leftarrow KG(1^k)$
  - $(cmt,st) \leftarrow A^{Tr()}(pk)$
  - $ch \leftarrow \{0,1\}^{C(k)}$
  - $rsp \leftarrow A(st,ch)$
  - Return Ver(cmt,ch,rsp)
- Exp(A,KG,Tr) outputs 1 with negl. probability

Security of the Fiat-Shamir transform

- **Theorem [AABN02]**: If **ID** is ε_{id}-secure against passive impersonations, then **SIG**=FS[**ID**] is ε_{sig}-existentially unforgeable

$$\boldsymbol{\varepsilon_{sig}} \leq q_h \times \boldsymbol{\varepsilon_{id}} + \mathrm{negl}(k)$$

Lossy identification schemes

- $\exists$ an alternate (lossy) key generation
- Properties:
  - ρ**-completeness**: a valid proof gets accepted
  - ε_s**-simulatable**: transcript can be efficiently simulated without the secret key
  - ε_k**- key indistinguishable**: cannot distinguish lossy keys from normal keys
  - ε_l**- lossy**: an unbounded adversary cannot succeed in breaking the ID scheme when pk is lossy

Security of the Fiat-Shamir transform

- **Theorem**: If **ID** is a $(\rho,\varepsilon_s,\varepsilon_k,\varepsilon_l)$-lossy identification scheme, then **SIG**= FS[**ID**] is ε_{sig}-existentially unforgeable

$$\boldsymbol{\varepsilon_{sig}} \leq \boldsymbol{\varepsilon_k} + q_{sig}\,\varepsilon_s + q_h\,\varepsilon_l + \mathrm{negl}(k)$$

Security of the Fiat-Shamir transform

- **Theorem**: If **ID** is a $(\rho,\varepsilon_s,\varepsilon_k,\varepsilon_l)$-lossy identification scheme, then **SIG**= FS[**ID**] is ε_{sig}-existentially unforgeable

$$\boldsymbol{\varepsilon_{sig}} \leq \boldsymbol{\varepsilon_k} + q_{sig}\,\varepsilon_s + q_h\,\varepsilon_l + \mathrm{negl}(k)$$

- **Theorem [AABN02]**: If **ID** is ε_{id}-secure against passive impersonations, then **SIG**= FS[**ID**] is ε_{sig}-existentially unforgeable

$$\boldsymbol{\varepsilon_{sig}} \leq q_h \times \boldsymbol{\varepsilon_{id}} + \mathrm{negl}(k)$$

Proof idea

- **Use transcripts to simulate signing oracle**
  - Let m be in the sign query
  - Given (cmt,ch,rsp) $\neq(\perp,\perp,\perp)$, set H(cmt,m)=ch
  - Collision probability is negligible due to cmt min-entropy
  - Return σ=(cmt,rsp) as the signature

- **Replace pk with lossy public key lpk**
  - Probability of success changes by at most $\varepsilon_k + q_s\varepsilon_s$
  - Success probability is at most $q_h\varepsilon_l$ when key is lossy
  - q_h factor is due to guess of hash query used in the forgery

Plan

- Introduction
- Identification schemes
- Lossy identification schemes
- **Instantiations of lossy ID schemes**
- Concluding remarks

DDH-based ID scheme [KW03]

Prover	$\mathbf{G} = \langle g \rangle$, $\lvert G \rvert = q$	**Verifier**
$sk = x \in Z_q$		$pk=(g,h,y_1=g^x,y_2=h^x)$
$r \leftarrow Z_q$ $A \leftarrow g^r$; $B \leftarrow h^r$	A, B $\longrightarrow$	
	$\longleftarrow$ c	$c \leftarrow Z_q$
$s \leftarrow cx + r$	s $\longrightarrow$	Accept if • $A\, y_1^c = g^s$ • $B\, y_2^c = h^s$

Security of DDH-based ID scheme

- 1-complete since ID scheme never aborts
- Simulatability follows from ZK property
  - Choose $c \in Z_q$ and $s \in Z_q$
  - Set $A=g^s y_1^{-c}$ and $B=h^s y_2^{-c}$
- Key indistinguishability follows from DDH assumption
- Lossiness
  - pk is not a DH tuple
  - Given A and B, there exists at most one c for which there exists a response s s.t. $Ay_1^c=g^s$ and $By_2^c=h^s$

Short-discrete-log based ID scheme

Prover	**G**,p,g	**Verifier**
sk= $x \in \{0,...,2^c-1\}$		pk= g^x
$y \leftarrow \{0,\ldots,2^{k+k'+c}-1\}$ $u \leftarrow g^y \bmod p$	u →	
	← e	$e \leftarrow \{0,\ldots,2^k-1\}$
$z \leftarrow ex + y$ if $z \notin \{2^{k+c},\ldots,2^{k+k'+c}-1\}$ $z \leftarrow \perp$	z →	Accept if • $z \in \{2^{k+c},\ldots,2^{k+k'+c}-1\}$ • $g^z\, pk^e = u$

Subset-sum-based ID scheme

Prover	$\mathbf{G},p,g$	**Verifier**
$sk = \mathbf{X} \leftarrow \{0,1\}^{n \times k}$		$pk = (\mathbf{a} \in Z_M^n,\ \mathbf{t} = \mathbf{a}^T\mathbf{X} \bmod M)$
$\mathbf{y} \leftarrow \{-kn,\ldots,kn\}^n$ $u \leftarrow \langle \mathbf{a},\mathbf{y} \rangle \bmod M$	u →	
	← $\mathbf{c}$	$\mathbf{c} \leftarrow \{0,1\}^k$
$\mathbf{z} \leftarrow \mathbf{X}\mathbf{c} + \mathbf{y}$ if $\mathbf{z} \notin \{-kn+k,\ldots,kn-k\}^n$ $\quad \mathbf{z} \leftarrow (\perp,\ldots,\perp)$	$\mathbf{z}$ →	Accept if • $\mathbf{z} \in \{-kn+k,\ldots,kn-k\}^n$ • $\langle \mathbf{a},\mathbf{z} \rangle - \langle \mathbf{t},\mathbf{c} \rangle = u \bmod M$

Plan

- Introduction
- Lossy identification schemes
- Security of Fiat-Shamir transform
- Instantiations of lossy ID schemes
- **Concluding remarks**

Concluding remarks

- **We extended results by Katz and Wang to other settings**
  - New schemes based on the decisional short-discrete-log problem, Ring-LWE, and subset sum
- **Provided a tight and generic security proof based on *lossy identification schemes***
- **Security holds in the quantum-accessible random oracle model**
  - Our reductions are history-free []