Provably Secure Blind Signature Schemes

David Pointcheval
David.Pointcheval@ens.fr

Jacques Stern
Jacques.Stern@ens.fr

École Normale Supérieure
Laboratoire d'Informatique

http://www.ens.fr/~wwwgrecc

Summary

- Introduction: E-cash
- Blind Signatures
  - Definition
  - Examples
- Security
- Model
- Witness Indistinguishability
- The First Secure Schemes
  - Presentation
  - Result
- Conclusion

Electronic Cash

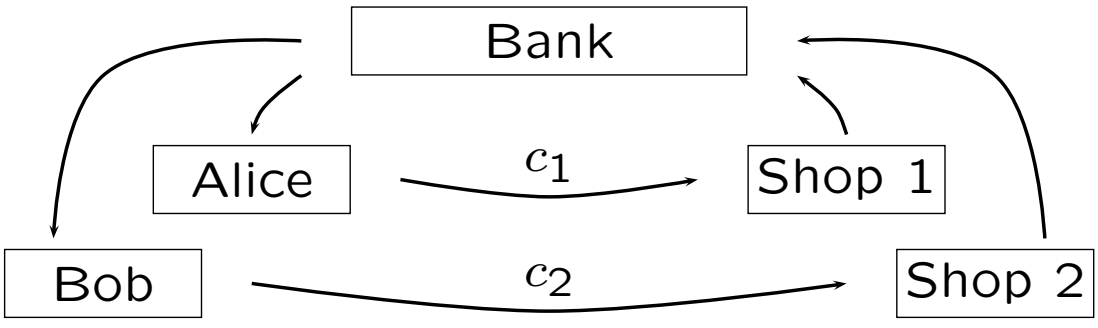
- **In the real world:**
  a coin is a piece of metal with a number, the amount, produced and certified by the Bank (or an authority).

  A coin is indistinguishable from another one.

- **In the electronic world:**
  a coin is a "random" number concatened with the amount, certified by the Bank.

  Two coins must be indistinguishable, even for the Bank.

Coins life



If the Bank can distinguish the coin it gave to Alice,
it knows that Alice went and spent money in Shop 1.

$\Longrightarrow$ Traceability of a coin.

Anonymity

respect of the private life $\Longrightarrow$ anonymity
untraceability $\Longrightarrow$ blind signatures

Blind Signatures

an authority helps a user to get a valid signature

the message and the signature
must remain unknown for the authority

An electronic coin is a "coin number"
certified by the Bank
such that the Bank doesnot know
the coin it gives nor the certificate.

Classical Examples

RSA Blind Scheme

Authority		Alice
public : $N = pq$ and e secret : $es = 1 \bmod \varphi(N)$		
		$r \in (\mathbb{Z}/N\mathbb{Z})^\star$
	$\xleftarrow{\quad m' \quad}$	$m' = r^e m \bmod N$
$\sigma' = m'^s \bmod N$	$\xrightarrow{\quad \sigma' \quad}$	
		$\sigma = r^{-1}\sigma' \bmod N$

σ is an unknown valid signature
of the unknown message m.

Used in the first E-cash systems.

Schnorr Blind Scheme

Bank		Alice
public : p, q, g, y secret : $y = g^{-x} \bmod p$ $k \in (\mathbb{Z}/q\mathbb{Z})^\star$ $r = g^k \bmod p$	$\xrightarrow{\quad r \quad}$	
		$\alpha, \beta \in \mathbb{Z}/q\mathbb{Z}$ $r' = r g^\alpha y^\beta \bmod p$ $e' = H(m, r')$
	$\xleftarrow{\quad e \quad}$	$e = e' - \beta \bmod q$
$s = k + ex \bmod q$	$\xrightarrow{\quad s \quad}$	
		$g^s y^e \stackrel{?}{=} r \bmod p$ $s' = s + \alpha \bmod q$

(r', s') is an unknown signature
of the unknown message m.

Security Properties

- $(\ell, \ell+1)$-forgery: after ℓ interactions with the Bank the attacker can forge $\ell+1$ message–signature valid pairs.
- One-more forgery: an $(\ell, \ell+1)$-forgery for some integer ℓ.

Attacks

- sequential attack: the attacker interacts sequentially with the signer.
- parallele attack: the attacker can initiate several interactions at the same time with the signer.

Context

- random oracle model [BR93]
- asymptotic framework of complexity theory

} as in [PS96]

- Since we want a secure signature scheme, we cannot simulate the signer without a secret key.

} $\neq$ [PS96]

$\Longrightarrow$ Witness indistinguishable protocols.

Witness Indistinguishability [FS90]

- several secret keys are associated to a same public one;
- communication tapes distributions are indistinguishable whatever the used secret key;
- two different secret keys associated to a same public key provide the solution of a difficult problem.

Example: the Bi-Discrete Logarithm Problem

$$y = g^r h^s = g^{r'} h^{s'} \bmod p$$
$$\text{with } r \neq r' \bmod q$$
$$\Longrightarrow h = g^{-(r-r')/(s-s')} \bmod p.$$

Okamoto–Schnorr Blind Scheme

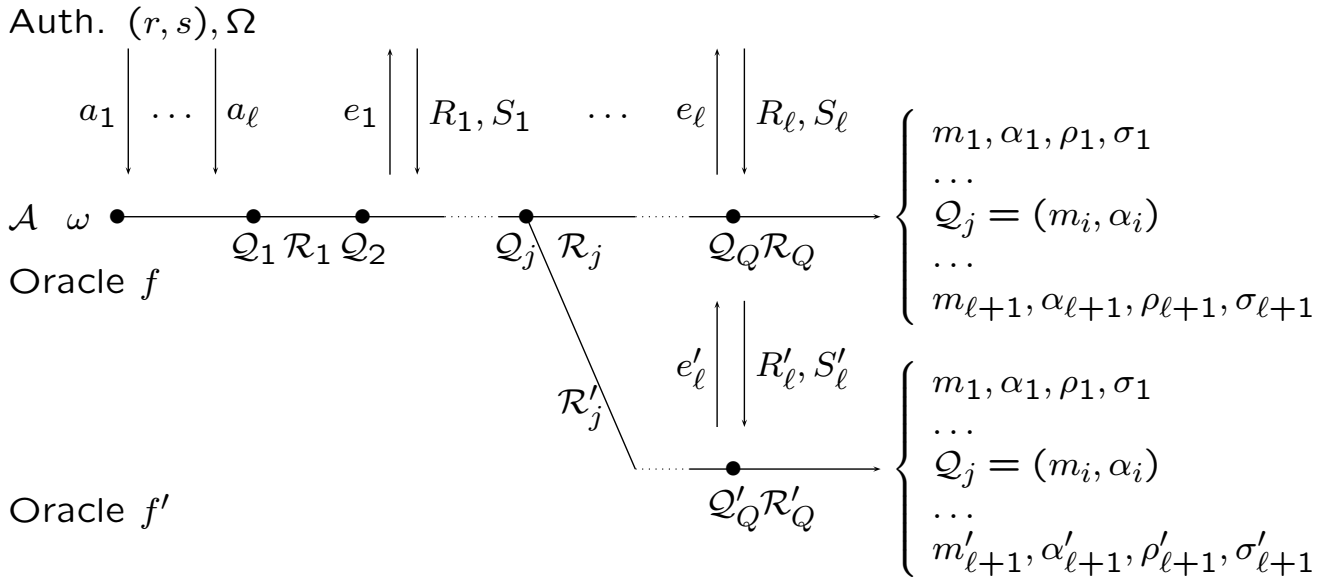
Authority		Alice
public : p, q, g, h, y		
secret : $y = g^{-r}h^{-s} \bmod p$		
$t, u \in (\mathbb{Z}/q\mathbb{Z})^\star$		
$a = g^t h^u \bmod p$	$\xrightarrow{\quad a \quad}$	
		$\beta, \gamma, \delta \in \mathbb{Z}/q\mathbb{Z}$
		$\alpha = a g^\beta h^\gamma y^\delta \bmod p$
		$\varepsilon = H(m, \alpha)$
	$\xleftarrow{\quad e \quad}$	$e = \varepsilon - \delta \bmod q$
$R = t + er \bmod q$		
$S = u + es \bmod q$	$\xrightarrow{\quad R, S \quad}$	
		$g^R h^S y^e \stackrel{?}{=} a \bmod p$
		$\rho = R + \beta \bmod q$
		$\sigma = S + \gamma \bmod q$

$(m, \alpha, \varepsilon, \rho, \sigma)$ s.t. $\alpha = g^\rho h^\sigma y^\varepsilon \bmod p$ with $\varepsilon = H(m, \alpha)$.

Main Result

If there exists a Probabilistic Polynomial Turing Machine
which can perform a one-more forgery,
with non-negligible probability,
even under a parallele attack,
then the Discrete Logarithm Problem
can be solved in Polynomial Time.

Forking Lemma



Forking Lemma (2)

We play the attack with random (r, s), Ω, ω and f
and replay with (r, s), Ω, ω
but f' which differs from f at the j^{th} answer.

With non-negligible probability,
there exists i such that $\mathcal{Q}_j = (m_i, \alpha_i)$

$$\text{and } \alpha_i = g^{\rho_i} h^{\sigma_i} y^{\varepsilon_i} \bmod p$$
$$= g^{\rho'_i} h^{\sigma'_i} y^{\varepsilon'_i} \bmod p$$

with $\varepsilon_i \neq \varepsilon'_i \bmod q$.

Then, with $r' = (\rho'_i - \rho_i)/(\varepsilon'_i - \varepsilon_i) \bmod q$
and $s' = (\sigma'_i - \sigma_i)/(\varepsilon'_i - \varepsilon_i) \bmod q$,

$$y = g^{-r'} h^{-s'} \bmod p.$$

Forking Lemma (3)

Since the communication tape follows a distribution independent of the secret key used by the authority, with high probability, $r \neq r' \bmod q$

$$\Longrightarrow \log_g h.$$

"Proof"

With a valid signature $(m_i, \alpha_i, \varepsilon_i, \rho_i, \sigma_i)$

$$\begin{aligned} \alpha_i &= g^{\rho_i} h^{\sigma_i} y^{\varepsilon_i} \bmod p \\ &= g^{\rho_i - r\varepsilon_i} h^{\sigma_i - s\varepsilon_i} \bmod p. \end{aligned}$$

We have to study the random variables

$$\chi_i = \rho_i - r\varepsilon_i \bmod q.$$

Conclusion

The forking lemma provides easy proofs of security for
Blind Signature Schemes derivated from
Witness Indistinguishable identification protocols, like

- the Okamoto–Schnorr scheme equivalent to the DL problem
- the Okamoto–GQ scheme equivalent to the RSA problem

It opens a way towards provably secure E-cash systems.