New Blind Signatures Equivalent to Factorization

David Pointcheval
David.Pointcheval@info.unicaen.fr

Université de Caen
GREYC
F – 14000 Caen

Jacques Stern
Jacques.Stern@ens.fr

École Normale Supérieure
Laboratoire d'Informatique
F – 75005 Paris

Summary

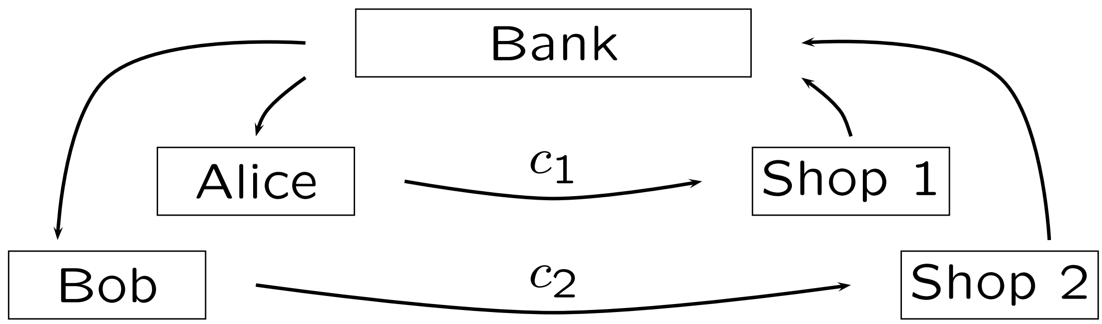
Electronic Cash

Electronic Cash = Electronic Version of Paper 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).

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

First Property of Paper Cash: Indistinguishability



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 $\neq$ Anonymity.

Anonymity

Respect of Private Life	$\Longrightarrow$	Anonymity
Untraceability	$\Longrightarrow$	Blind Signatures

Perfect Anonymity = Perfect Crimes
$\Longrightarrow$ appearance of revokable anonymity
(Third Trusted Party)

In any case: Blind Signatures

Blind Signatures

the Bank helps a user to get a valid signature

the message and the signature
must remain unknown for the Bank

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

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

Another well-known scheme is the Schnorr Blind one.

Second Property of Paper Cash: Unforgeability

One Coin *given* by the Bank = One Coin *spendable* in a Shop

$\Longrightarrow$ we want to avoid:

- $(\ell, \ell+1)$-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.
  ($\Longrightarrow$ low-rate withdrawal)

- parallele attack: the attacker can initiate several interactions at the same time with the signer.
  ($\Longrightarrow$ pratical attack due to the need of high-rate withdrawals)

New Blind Signatures Equivalent to Factorization

Previous Results

- adaptation of the Okamoto – Schnorr identification
  $\Longrightarrow$ a one-more forgery under a parallele attack is equivalent to the discrete logarithm problem.

- adaptation of the Okamoto – Guillou-Quisquater identification
  $\Longrightarrow$ a one-more forgery under a parallele attack is equivalent to the RSA problem.

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 Square Root Problem

$$\left.\begin{array}{c} x^2 = y^2 \bmod N \text{ where } N = pq \\ \text{with } x \text{ and } y \text{ in different classes} \\ \text{of quadratic residuosity} \end{array}\right\} \Longrightarrow \gcd(N, x-y) \in \{p, q\}.$$

Fiat − Shamir Blind Scheme (sketch)

(use of k secrets $S^{(1)}$, . . . , $S^{(k)}$).

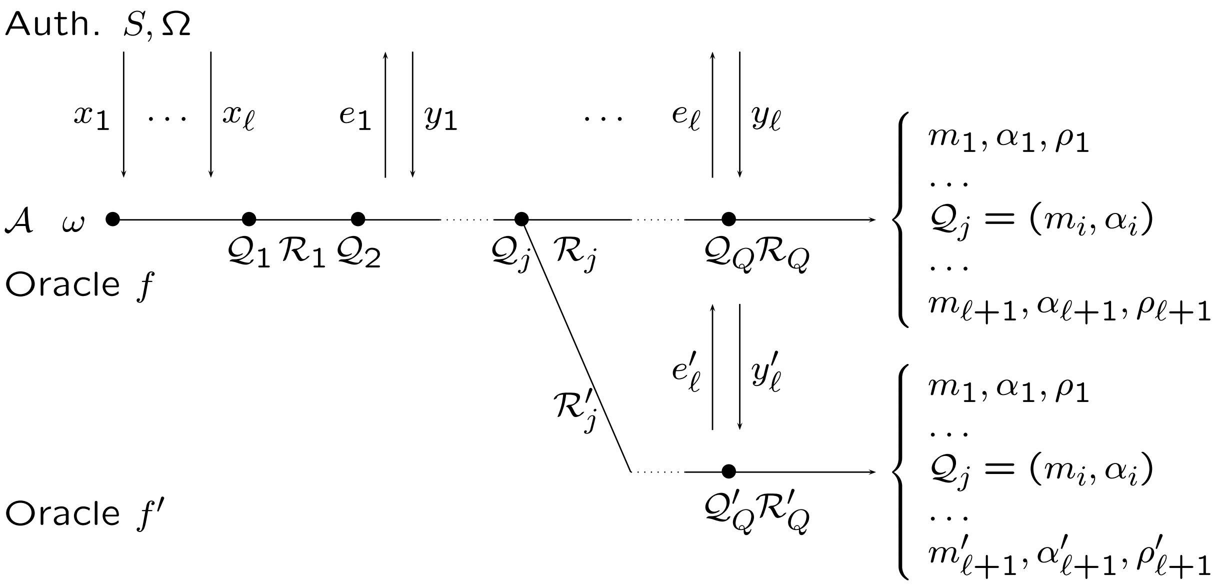
Authority		Alice
	$N = pq$, product of 2 large primes	
S, $V = S^2 \bmod N$		
$t \in (\mathbb{Z}/N\mathbb{Z})^\star$		
$x = t^2 \bmod N$	$\xrightarrow{x}$	
		$\beta \in (\mathbb{Z}/N\mathbb{Z})^\star$, $\gamma \in \mathbb{Z}/2\mathbb{Z}$
		$\alpha = x\beta^2 V^\gamma \bmod N$
		$\varepsilon = H(m, \alpha) \in \{0, 1\}$
	$\xleftarrow{e}$	$e = \varepsilon \oplus \gamma \bmod N$
$y = tS^e \bmod N$	$\xrightarrow{y}$	
		$y^2 \overset{?}{=} xV^e \bmod N$
		$\rho = y\beta V^{\gamma \text{ and } \varepsilon} \bmod N$

$(m, \alpha, \varepsilon, \rho)$ s.t. $\rho^2 = \alpha V^\epsilon \bmod N$ with $\varepsilon = H(m, \alpha)$.

Security 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 Factorization Problem
can be solved in Polynomial Time.

Forking Lemma



Forking Lemma (2)

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

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

$$\begin{aligned} \text{and} \quad \alpha_i &= \rho_i^2 / V^{\varepsilon_i} \bmod N \\ &= {\rho'_i}^2 / V^{\varepsilon'_i} \bmod N \end{aligned}$$

with $\varepsilon_i = 1$ and $\varepsilon'_i = 0$.

If we let $S' = \rho_i / \rho'_i \bmod N$,
then, $V = {S'}^2 \bmod N$.

Forking Lemma (3)

Since the communication tape follows a distribution
independent of the secret key used by the authority,
with good probability, S and S' are in distinct classes
of quadratic residuosity

$\Longrightarrow$ factorization of N.

Technical proof: study of the quadratic residuosity of some variables.

Ong − Schnorr Blind Scheme

Authority		Alice
$N = pq$, product of 2 large primes		
S, $V = S^{2^k} \bmod N$		
$t \in (\mathbb{Z}/N\mathbb{Z})^\star$		
$x = t^{2^k} \bmod N$	$\xrightarrow{x}$	
		$\beta \in (\mathbb{Z}/N\mathbb{Z})^\star$, $\gamma \in \mathbb{Z}/2^k\mathbb{Z}$
		$\alpha = x\beta^{2^k}V^\gamma \bmod N$
		$\varepsilon = H(m, \alpha)$
	$\xleftarrow{e}$	$e = \varepsilon + \gamma \bmod 2^k$
$y = tS^e \bmod N$	$\xrightarrow{y}$	
		$y^{2^k} \stackrel{?}{=} xV^e \bmod N$
		$\tau = (\varepsilon + \gamma) \div 2^k$
		$\rho = y\beta V^\tau \bmod N$

$(m, \alpha, \varepsilon, \rho)$ s.t. $\rho^{2^k} = \alpha V^\epsilon \bmod N$ with $\varepsilon = H(m, \alpha)$.

Security Result

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

Sequential! Why?

- we choose S and let $V = S^{2^{k-\lambda}}$
  with 2^λ polynomial and $\lambda < k$;
- we simulate the answers of the authority
  (as in the Shoup's proof – Eurocrypt'96)
  $\Longrightarrow$ reset in case of failure (2^λ resets on average)
  $\Longrightarrow$ cannot reply successfully to several queries at the same time;

New Blind Signatures Equivalent to Factorization

Conclusion

Another time, we see the importance of the "forking lemma":

$\Longrightarrow$ the first blind signature schemes equivalent to factorization.

- an efficient one, secure against sequential attacks
- a less efficient one, secure against parallel attacks