Security Proofs for Signature Schemes

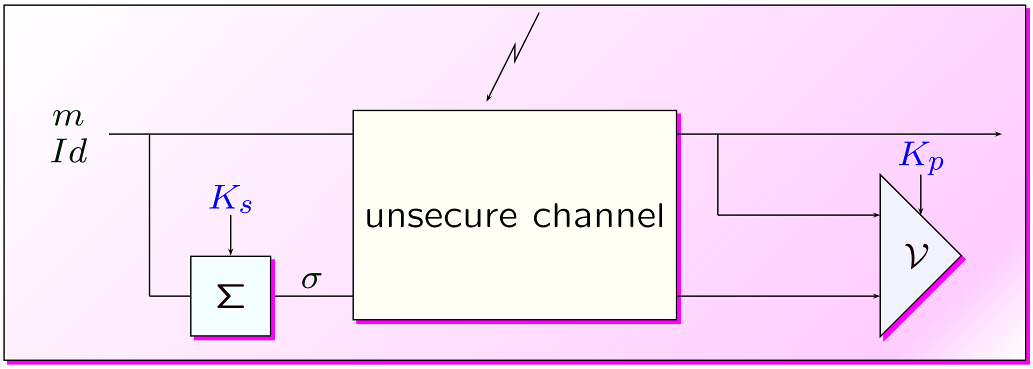
David Pointcheval
David.Pointcheval@ens.fr

Jacques Stern
Jacques.Stern@ens.fr

Laboratoire d'Informatique
École Normale Supérieure
45, rue d'Ulm
75230 PARIS CEDEX 05

Summary

Signature schemes

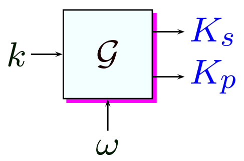
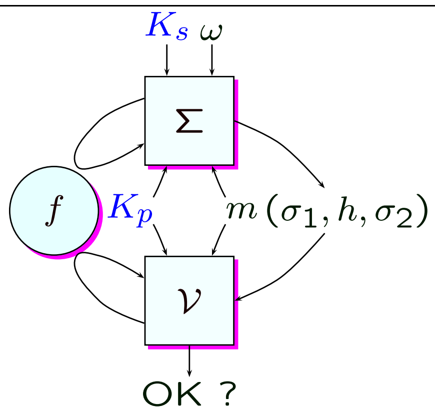


Proof of identity of the sender.

Security

No one can forge a valid pair (m, σ) = no existential forgery

The model (1)

Key generation	Signature and Verification
k is the security parameter  $n = \|K_p\|$	

- $\mathcal{G}$ and Σ are probabilistic algorithms: random tape ω
- $\mathcal{V}$ is deterministic

The model (2)

- Σ and $\mathcal{V}$ both use a hash function f
  with $f \in_R \{0,1\}^\ell \to \{0,1\}^k$, seen as a random oracle.
  (refer to Bellare & Rogaway ACM CCCS'93)

  $\longrightarrow$ validates cryptodesign
  (refer to Vaudenay's attack on DSS)

- Signatures are of the following form: $(m, \sigma_1, f(m, \sigma_1), \sigma_2)$

Assumptions

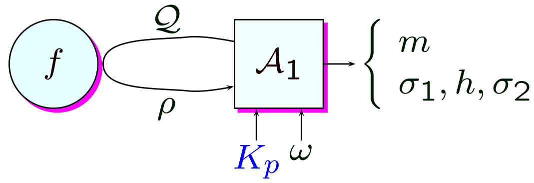
- $k(n) \gg \log n$

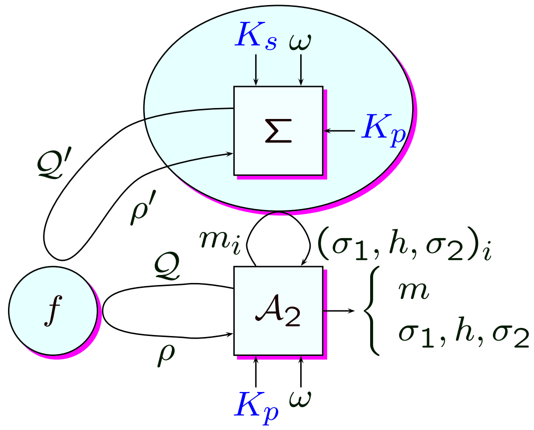
- Existential forgery:
  there is an attacker $\mathcal{A}$ which outputs proper signatures with probability $\varepsilon \geq \frac{1}{poly(n)}$ for infinitely many n's

Attacks

We will consider only
- No-message attacks
- Adaptively chosen message attacks

Attack I no-message attack	**Attack II** adaptively chosen message attack





Motivation

To provide proofs of security for signature schemes relatively to well-established difficult problems:
Existential forgery under such attacks is equivalent to difficult problems.

Example: Fiat-Shamir (with single key)

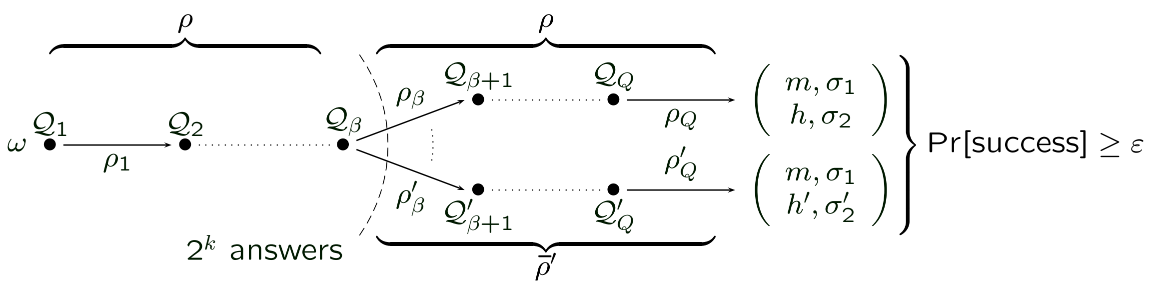
$\mathcal{G}$: $N = pq$ such that $|N| = n$
secrete key: $s \in_R \mathbb{Z}/N\mathbb{Z}$
public key: $v = s^2 \bmod N$

Σ : $r_1, \ldots, r_k \in_R \mathbb{Z}/N\mathbb{Z}$
$x_i = r_i^2 \bmod N$: $\sigma_1 = (x_1, \ldots, x_k)$
$e_1 \ldots e_k = f(m, \sigma_1)$
$y_i = r_i \cdot s^{e_i} \bmod N$: $\sigma_2 = (y_1, \ldots, y_k)$

Signature: $\big(m, (x_1, \ldots, x_k), e_1 \ldots e_k, (y_1, \ldots, y_k)\big)$

$\mathcal{V}$: $y_i^2 \stackrel{?}{=} x_i v^{e_i} \bmod N$
$e_1 \ldots e_k \stackrel{?}{=} f\big(m, (x_1, \ldots, x_k)\big)$

The forking lemma (1)



$\mathcal{A}$ is an attacker with probability of success, over ω, f and possibly K_p, greater that ε.

Oracle replay:
- play the attack with random ω and f
- select β at random
- replay the attack with the same ω and same $\beta - 1$ first answers, others are given at random

Application with Fiat-Shamir

In order to factor N:

- create a key pair (s, v) with $v = s^2 \bmod N$.
- apply the forking lemma to get
  $(m, \sigma_1, h, \sigma_2)$ and $(m, \sigma_1, h', \sigma_2')$. with $h \neq h'$
  if h and h' differ at i, say $h_i = 0$ and $h_i' = 1$
  then $y_i^2 = x_i$ and $(y_i')^2 = x_i v$
  hence $(y_i' y_i^{-1})^2 = v \bmod N$

Since algorithm cannot distinguish s from other roots, we can factor.

Conclusion: existential forgery of the Fiat-Shamir signature scheme, under a no-message attack, is equivalent to the factorization.

The forking lemma (2)

The probabilistic lemma

Let $A \subset X \times Y$ such that $\Pr[A(x, y)] \geq \varepsilon$
Then there exists $U \subset X$ such that

- $\Pr[x \in U] \geq \dfrac{\varepsilon}{2}$
- whenever $a \in U$, $\Pr[A(a, y)] \geq \dfrac{\varepsilon}{2}$

- there is a query index β such that Pr[success and β] $\geq \varepsilon/Q$
- using the previous lemma, we get a set Ω such that
  - $\Pr[(\omega, \rho) \in \Omega] \geq \varepsilon/2Q$
  - whenever $(\omega, \rho) \in \Omega$, $\Pr_{\overline{\rho}}$[success and β] $\geq \varepsilon/2Q$

The forking lemma (3)

With non-negligible probability, one gets

- good β
- $(\omega, \rho) \in \Omega$

And then, with random choice of $\bar{\rho}$ and $\bar{\rho}'$, with non-negligible probability:

- with answers $(\rho, \bar{\rho})$, the attacker outputs $(m, \sigma_1, h, \sigma_2)$ such that (m, σ_1) is the β^{th} query,
- with answers $(\rho, \bar{\rho}')$, the attacker outputs $(m, \sigma_1, h', \sigma_2')$,

With probability less than $2^{-k(n)}$, $h = h'$.

El Gamal

$\mathcal{G}$: p prime, and g generator of $(\mathbb{Z}/p\mathbb{Z})^\star$
secrete key: $x \in_R (\mathbb{Z}/(p-1)\mathbb{Z})^\star$
public key: $y = g^x \bmod p$

Σ : $k \in_R (\mathbb{Z}/(p-1)\mathbb{Z})^\star$
$r = g^k \bmod p$
solve $m = xr + ks \bmod (p-1)$

Signature: (m, r, s)

$\mathcal{V}$: $g^m \stackrel{?}{=} y^r r^s \bmod p$

Existential forgery

$$\begin{array}{ll} \text{choose} & e \in \mathbb{Z}/(p-1)\mathbb{Z} \\ & v = (\mathbb{Z}/(p-1)\mathbb{Z})^\star \\ \text{let} & r = g^e y^v \bmod p \\ & s = -rv^{-1} \bmod (p-1) \end{array}$$

(r, s) is a valid signature of the message
$m = es \bmod (p-1)$

Security Proofs for Signature Schemes

Modified El Gamal Signature

$\mathcal{G}$: p prime, and g generator of $(\mathbb{Z}/p\mathbb{Z})^\star$
secrete key: $x \in_R (\mathbb{Z}/(p-1)\mathbb{Z})^\star$
public key: $y = g^x \bmod p$

Σ : $k \in_R (\mathbb{Z}/(p-1)\mathbb{Z})^\star$
$r = g^k \bmod p$
solve $f(m,r) = xr + ks \bmod (p-1)$

Signature: $(m, r, f(m,r), s)$

$\mathcal{V}$: $g^{f(m,r)} \stackrel{?}{=} y^r r^s \bmod p$

First Result

For fixed α, an α-hard prime p is
a prime p such that $p-1=QR$
with Q prime and $R \leq |p|^{\alpha}$.

Existential forgery of the Modified El Gamal signature scheme, under a no-message attack, is equivalent to discrete logarithms with α-hard primes.

Proof (1)

By the forking lemma, we get (m, r, h, s) and (m, r, h', s') such that

$$h \neq h' \text{ and } \left\{ \begin{array}{rcl} g^{h} & = & y^{r} r^{s} \bmod p \\ g^{h'} & = & y^{r} r^{s'} \bmod p \end{array} \right.$$

Hence

$$g^{hs'-h's} = y^{r(s'-s)} \bmod p$$
$$g^{h-h'} = r^{s-s'} \bmod p$$

There are x and t such that $y = g^{x}$ and $r = g^{t}$, so

$$hs' - h's = xr(s'-s) \bmod (p-1)$$
$$h - h' = t(s-s') \bmod (p-1)$$

Proof (2)

h and h' come from the random oracle, we may assume
$h - h'$ prime to Q hence $s - s'$ prime to Q.

1. r also prime to Q $\Longrightarrow$ $x \mod Q$ $\Longrightarrow$ x
2. $r = bQ$ with b small $\Longrightarrow$ $t \mod Q$ $\Longrightarrow$ t

1. $\Pr[\mathcal{M}(g,y) \to x] \geq \frac{1}{poly(n)}$ $\Longrightarrow$ OK
2. $\Pr[\mathcal{M}(g,y) \to (b,t)] \geq \frac{1}{poly(n)}$ $\Longrightarrow$ bad case

Proof (3)

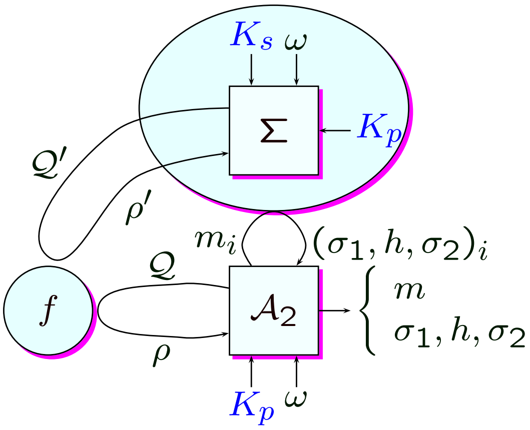
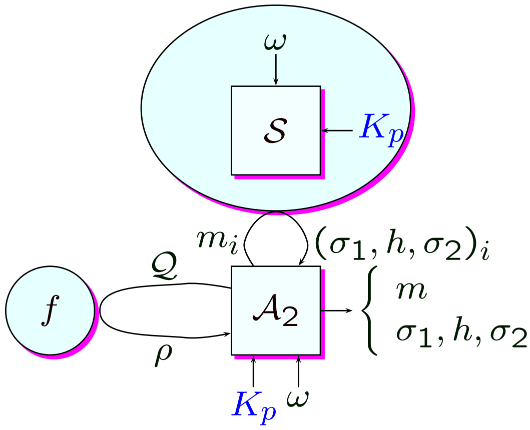
By trying (g^u, yg^v) for random u, v, it is well-known that if

$$\Pr_{\omega,g,y}[\mathcal{M}(g,y) \to x | y = g^x] \geq \frac{1}{poly(n)}$$

then we obtain a polynomial probabilistic Turing machine $\mathcal{M}'$
such that for every (g,y),

$$\Pr_{\omega}[\mathcal{M}'(g,y) \to x | y = g^x] \geq \frac{1}{poly(n)}$$

Adaptively Chosen Message Attack

Attacker II + Signer (Σ)	Attacker II + Simulator ($\mathcal{S}$)
	 We suppose $f(m_i, (\sigma_1)_i) = h_i\ \forall i$

If the legitimate signer can be simulated with an indistinguishable distribution, the collusion of the attacker and the simulator can solve the discrete logarithm problem.

Simulation

We assume that the output set H of random oracles contains a copy of $\mathbb{Z}/Q\mathbb{Z}$.

1. random choice of $u \in \mathbb{Z}/Q\mathbb{Z}$, $t \in (\mathbb{Z}/Q\mathbb{Z})^\star$ and $\ell \in (\mathbb{Z}/R\mathbb{Z})^\star$.
2. let $e = uR \bmod (p-1)$, $v = tR \bmod (p-1)$ and $r = (g^e y^v) g^{Q\ell} \bmod p$ until r is a generator.
3. mimicking the existential forgery in the subgroup generated by g^R, we need $s = -rv^{-1} \bmod Q$ and $h = -erv^{-1} \bmod Q$.
4. random choice of $h \bmod R$ such that $h \in H$.
5. exhaustive search over $s \bmod R$ such that $g^h = y^r r^s \bmod p$.

It is easy to see that it is a valid signature if $f(m, r) = h$.

Main Result

Consider an adaptively chosen message attack
in the random oracle model.

Existential forgery of the Modified El Gamal signature scheme is equivalent to discrete logarithms with α-hard primes.

Security Proofs for Signature Schemes

Conclusion

The forking lemma provides easy proofs of security for

1. the Fiat-Shamir signature scheme
2. the Schnorr signature scheme
3. . . .
   the transformation of any honest verifier zero-knowledge identification scheme
4. the modified El Gamal signature scheme

under an adaptively chosen message attack
in the random oracle model.