Slide 1

Secure digital signatures

with McEliece

and new records in short signatures

Nicolas T. Courtois[1,2], Matthieu Finiasz[1] and Nicolas Sendrier[1]

[1]INRIA Rocquencourt, France
[2]CP8 Crypto Lab, SchlumbergerSema, France

Full paper and info : `www.minrank.org/mceliece/`

Slide 2

Syndromes

Let H be a binary matrix $r \times n$.
Let x be a word in $GF(2)^n$.
$H \cdot x$ is called the **syndrome of x** (it has r bits).

The **S**yndrome **D**ecoding problem (SD)

SD - Find a word $\mathbf{x}$ of small weight $\leq$ some $\mathbf{t}$
with a given syndrome $Hx = \mathbf{y}$.

Hardness of the SD problem

$\diamondsuit$ NP-hard problem in general.
$\diamondsuit$ If $t << n$ all known attacks are **exponential** in about :

$$n^{t(1/2+o(1))}$$

[cf. Canteaut, Chabaud, Barg, Dumer, Stern, etc..]
$\approx \sqrt{\text{exhaustive search}}$, serious competitor to the EC.

Slide 3

Trapdoor functions based on SD

A code with **a decoding algorithm** due to a hidden algebraic structure.

Example :

Permuted binary Goppa codes. Exist for $n = 2^m$ and $r = tm$.
Trapdoor $\Rightarrow$ decoding of all syndromes of weight $\leq t$.

Structural attacks

Problem : Distinguish a permuted Goppa code from a random matrix of the same size. Best attack known :
[Sendrier 2000] : $tn^{t-2}(\log_2 n)^2$
Used in one of the oldest known public key schemes [1978] :

McEliece cryptosystem (Niederreiter variant)

Messages : n-bit words x of weight $\leq t$. Ciphertext = Hx.

Slide 4

McEliece in signature

$H\sigma = \text{SHA-1}(m)$???

Problem : The function $x \mapsto Hx$ is not surjective.
Only a tiny fraction of all syndromes are decodable.
Our solution : Randomized decoding :

$$H\sigma = \text{SHA-1}(m||Random)$$

Signature cost : $t!t^2(\log_2 n)^3$

Best attack : $n^{t(1/2+o(1))}$

Our discovery

Keep t small, $n = 2^{\mathcal{O}(t)}$, then it is **practical**, and the best attack is still **exponential** in the signature cost !

Slide 5

Courtois-Finiasz-Sendrier signature scheme [CFS]

Let $n = 2^m$, $m \geq \mathcal{O}(t)$, t grows slowly.

signature cost	$t!t^2(\log_2 n)^3$
signature length[1]	$(t-1)\log_2 n + \log_2 t$
verification cost[1]	$t \log_2 n$
public key size	$tn \log_2 n$
best decoding attack	$n^{t(1/2+o(1))}$
best structural attack	$tn^{t-2}(\log_2 n)^2$

[1] One error position omitted

Slide 6

Security Proofs for CFS

Proofs are very easy in the **random oracle model**.

♢ **Ressources of the Adversary :** Bounded by an exponentially growing expression $n^{t(1/2+o(1))}$.

⇒ concrete security by substitution (!).

♢**Adversarial Goal :** Compute a valid pair (message, signature).

♢ **Adversarial model :** Access to a signature oracle.

(Apparently) the strongest security notion known.

Main theorem 0.0.0.1 (Provable Security of CFS)
Any T-time algorithm A that forges a signature satisfies :

$$T \geq Min\,(T_{Goppa}, T_{SD})\,.$$

Slide 7

CFS in practice

Let $n = 2^{16}$, $m = 16$, $t = 9$.

signature time	30 s on a PC
signature length[1]	**87** bits
verification cost[1]	1 s on a PC
public key size	1 Mb
best decoding attack	2^{83}
best structural attack	2^{123}

[1] 3 error positions are omitted and recovered in signature verification

The shortest signature scheme known before : **128** bits with Quartz, based on the HFE family of trapdoor functions [Patarin 1996].

Slide 8

What signatures are the best ? Bad question

Use several algorithms and issue several certificates.

Programs, terminals and devices will have at least one common algorithm for few years.

Pro-active scenario : Invalidate some algorithms and introduce new ones.

Example, when 768-bit RSA is broken, the 1024-bit RSA expires.

Un example of combined certificate :

RSA + EC + McEliece = $1024 + 321 + 87$ bits.

RSA is slow and signatures are long, the rest is almost for free.