Efficient code-based one-time signature from automorphism group

Philippe Gaborit, and **Julien Schrek**

University of Limoges, France

8 mai 2012

Signature with codes

1. ZK-based signature : Stern authentication scheme '93
   1. SternDC : very good security reduction
   2. very small size of key : $\sim 500b$
   3. fast
   4. large signature : $\sim 150kb$
2. Courtois-Finiasz-Sendrier signature '01
   1. security : reasonable but extreme parameters
   2. very large key : 8Mb
   3. very slow
   4. very small size of signature : 80b
3. Kabatiansky-Krouk-Smeets scheme '97
   1. security : probably sure but unclear practically
   2. few-times scheme
   3. fast
   4. average size of keys : 200kb, signature length : moderate $\sim 3000b$

Interest of one-time signature

• Interest of few-times signature $\rightarrow$ transformation in multi-times via hash-trees

$\rightarrow$ In that case : signature size in mutli-time = size of key of one time signature

$\rightarrow$ SternDC signature 150kb $\rightarrow$ one should search for one-time schemes with smaller size of keys.

KKS scheme

Idea : construct a matrix of predefined syndrome matrix that the signer is able to invert

Description

H a random (or QC) $n \times k$ public matrix, G a private $k' \times n$ matrix with only n' non null columns.

A public matrix of syndromes $F = H.G^t$ (F is a $k \times k'$ matrix). $2^{k'}$=number of possible signature $\rightarrow k' \geq 160$.

Public key : (H,F), Private key : G

Signature :

- m $\rightarrow$ hash(m)=x $\in F_2^{k\prime}$, signature=xG

Verification :

$H.(xG)^t = F.x^t + weight(x) \sim \frac{n'}{2}$

Comments on KKS

1. clearly linear, one time or more ?
2. Security ? Cayrel-Otmani-Vergnaud '07 ; BarretoMisoczki '10 (reduction ? ? ?)
3. Intrinsic problem 1 : $k' \geq 160 \rightarrow$ large size of key ¿ 200kb.
4. Intrinsic problem 2 : the scheme is linear : makes attacks more effective
5. The weight of the signature is controlled by the fact that G has weight at most n' (n average n'/2)
6. recent attack Otmani-Tillich (PQC 2011) attack all parameters using the fact that the support of the potential errors is small.

New approach with syndrome

Definition (syndrome compatibility)

For G a permutation group on k positions and $H = (I|H_1|H_2|\cdots|H_{r-1})$ a $k \times rk$ parity check matrix of a certain code, we say that the permutation group G is *syndrome compatible* with H if for any g in G there exists a $k \times k$ matrix L_g such that for any $1 \leq i \leq r-1$ we have $H_i.\pi_g = L_g.H_i$. The matrix L_g is called the compatible matrix of g for H.

Proposition

If a permutation group G is syndrome compatible with H then for any x in F_2^n and any $g \in G$:

$$H.(x.\Pi_g)^t = L_g.(H.x^t).$$

Example

Example

Group G of circular permutations of length k. This group is syndrome compatible with a $k \times 2k$ matrix $H = (I|H_1)$ - H_1 a random circular matrix.

Circular permutations commute with cyclic matrices we get $L_g = \pi_g^{-1}$.

Idea : from one given syndrome that one is able to invert, one is able to construct several syndrome also invertible (in that case by permutation).

Key generation algorithm for the one-time signature algorithm

- **Public data** A permutation group G syndrome compatible with a parity check matrix H.
- **Key generation**
Private key : $x_1, x_2, ..., x_l$ random words of weight close to t.
Public key : the associated syndromes $s_i = H.x_i^t$.

One-time signature algorithm with syndrome compatibility

Entry : m a message to sign.

1. **Signature**
   1. Pick j a random element between 1 and 2^s.
   2. To any message m one associates through the hash function $h(m \| i)$, l elements $a_1, a_2, ..., a_l$ with $1 \leq a_i \leq |G|$.
   3. Compute the word $sign = \sum_{i=1}^{l} x_i.\Pi_{\phi(a_i)}$.
   4. If $weight(sign) > w$ or if the number of common coordinates between $x_i.\Pi_{\phi(a_i)}$ and $sign$ is greater than t, return to 1.
   5. Output the signature $(sign, j)$.
2. **Verification**
   1. Compute the a_i from m and j
   2. Verify that : $H.sign^t = \sum_{i=1}^{l} L_{\phi(a_i)} s_i$ and that $weight(sign) \leq w$.

Démonstration.

The verification works since for any i,
$H.(x_i.\Pi_{\phi(a_i)})^t = L_{\phi(a_i)}(H.x_i^t) = L_{\phi(a_i)}.s_i$. □

Quadratic double circulant codes

There exist special matrices such that the permutation which acts is large :

$$B_p = (U_p|V_p) = \left(\begin{array}{c|c|c|c} 0 & 0\cdots 0 & 1 & 1\cdots 1 \\ \hline 1 & & 0 & \\ \vdots & I & \vdots & M_p \\ 1 & & 0 & \end{array}\right)$$

M_p : circulant matrix of quadratic residues.

Proposition

The group $PSL_2(p)$ of order $\frac{(p-1)p(p+1)}{2}$ is syndrome compatible with the matrix B_p.

Security

Security arguments :

1. no linearity, the '1' of the secret keys can be in any column $\rightarrow$ resistance to Otmani-Tillich attack
2. one does not know how to decode this family of code
3. when a signature is given, there is always a part of each x_i coordinates which vanishes, an attacker will always have to recover them, as soon as this number is bigger than 30 it becomes very hard.

Parameters

- **Quasi-cyclic scheme** : G=cyclic shifts of length k. Take $k = 6007, r = 3, l = 12$, weight of $x_i = 260$, upper weight of signature w=2690, number of common bits $t < 260 - 40 = 220$. public key=72kb, signature :18000b.
- **Quadratic double circulant codes** : $G = PSL_2(p)$. Take $p = 3413, l = 5$, weight of $x_i = 338$, upper weight of signature=1385. number of common bits $t < 338 - 58 = 280$. Public key :18kb,signature size :6800b.

Conclusion

Efficient scheme which can be used with hash-trees to obtain 2^{20} possible signature of size $28kb$. Security probably better than KKS because of non-linearity, but relying on a specific class of codes : the Quadratic Residue codes, but not decodable for more than 40 years.