Birational permutation による署名方式の非可換化について

橋本康史 （Yasufumi Hashimoto）
九州先端科学技術研究所

Ong-Schnorr-Shamir's (OSS) signature scheme (1984)

Keys: Primes p, q and $u \in (\mathbb{Z}/pq)^\times$ are secret, and $n = pq$ and $h := -u^{-2} \in (\mathbb{Z}/n)^\times$ are public.
Signature (x, y) **for a message** m**:** (r is random)

$$x := r^{-1}m + r, \quad y := u(r^{-1}m - r).$$

Verification: Check whether

$$x^2 + hy^2 \equiv 4m \bmod n. \tag{1}$$

This was broken by Pollard-Schnorr (1987) with the algorithm to solve (1) in (prob.) P-time without factoring n, based on

$$(x_1^2 + hy_1^2)(x_2^2 + hy_2^2) = (x_1x_2 - hy_1y_2)^2 + h(x_1y_2 + x_2y_1)^2.$$

Improvements.
1. Multivariate version [Shamir, 1993].
2. Quaternion (noncommutative) version [Satoh-Araki, 1997].

Birational permutation signature scheme [Shamir, 1993]

p, q: primes, $n := pq$,
Consider the following map ($l \geq 2$).

$$(\mathbb{Z}/n)^l \xrightarrow{A} (\mathbb{Z}/n)^l \xrightarrow{G} (\mathbb{Z}/n)^{l-1} \xrightarrow{B} (\mathbb{Z}/n)^{l-1},$$

Here A, B are invertible affine (linear) transforms,
$\mathbf{g} = (g_2, \cdots, g_l) := G(\mathbf{y})$ is as follows.

$$g_i(y_1, \cdots, y_i) := \begin{cases} y_1 y_2 & (i = 2), \\ v_i(y_1, \cdots, y_{i-1}) y_i + w_i(y_1, \cdots, y_{i-1}) & (i \geq 3), \end{cases}$$

where $v_i(y_1, \cdots, y_{i-1}) := \sum_{1 \leq j \leq i-1} v_j^{(i)} y_j$,
$w_i(y_1, \cdots, y_{i-1}) := \sum_{1 \leq j_1, j_2 \leq i-1} w_{j_1 j_2}^{(i)} y_{j_1} y_{j_2}$ with coefficients
$v_j^{(i)}, w_{j_1 j_2}^{(i)} \in \mathbb{Z}/n$.

Signature scheme

Keys: The secret keys are A, G, B and the public keys is $F(\mathbf{x}) = (B \circ G \circ A)(\mathbf{x})$.

Signature x for the message m $\in (\mathbb{Z}/n)^{l-1}$**:**

Calculate $\mathbf{m}' = (m'_2, \cdots, m'_l) := B^{-1}\mathbf{m}$,

Choose $y_1 \in (\mathbb{Z}/n)^\times$ randomly and determine $y_2, \cdots, y_l$ recursively by

$$y_i := \begin{cases} y_1^{-1} m'_2 & (i = 2), \\ v_i(y_1, \cdots, y_{i-1})^{-1}(m'_i - w_i(y_1, \cdots, y_{i-1})) & (i \geq 3). \end{cases}$$

Calculate $\mathbf{x} := A^{-1}\mathbf{y}$.

Verification: Verify whether $F(\mathbf{x}) = \mathbf{m}$.

This was broken by Coppersmith-Stern-Vaudenay.

$$[\text{Multivariate}] \overset{\text{lin. alg.}}{\longrightarrow} [\text{Binary (OSS)}]$$

Quaternion OSS signature scheme

Quaternion number: $\alpha := \alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3$, where $\alpha_j \in \mathbb{R}$ and $i_1^2 = i_2^2 = i_3^2 = -1$, $i_1 i_2 = i_3 = -i_2 i_1$.
The multiplication is non-commutative ($ab \neq ba$).

$$\alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 \leftrightarrow \begin{pmatrix} \alpha_0 + \alpha_1\sqrt{-1} & \alpha_2 + \alpha_3\sqrt{-1} \\ -\alpha_2 + \alpha_3\sqrt{-1} & \alpha_0 - \alpha_1\sqrt{-1} \end{pmatrix}.$$

Quaternion OSS signature scheme [Satoh-Araki, 1997]
$R := \{\alpha_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 \mid \alpha_i \in \mathbb{Z}/n\}$.
$\alpha^t := \alpha_0 + \alpha_1 i_1 - \alpha_2 i_2 + \alpha_3 i_3$.
Keys: $u \in R^\times$ is secret, $h := -(u^t)^{-1} u^{-1}$ is public.
Signature $(x_1, x_2) \in R^2$ **for a message** $m \in R$**:** (r is random)

$$x_1 := r^{-1} m + r^t, \quad x_2 := u(r^{-1} m - r^t).$$

Verification: Check whether

$$x_1^t x_1 + x_2^t h x_2 = 2(m + m^t) \quad \text{in } R.$$

The following relation used in Pollard-Schnorr's algorithm does not hold.

$$(x_1^2 + hy_1^2)(x_2^2 + hy_2^2) = (x_1x_2 - hy_1y_2)^2 + h(x_1y_2 + x_2y_1)^2.$$

Then the direct extension of PS-alg. is not valid.
However, Coppersmith (1999) broke it by using several special properties of the quaternion algebra.

$$[\text{A binary form/quaternion}] \overset{\text{prop. of quat.}}{\longrightarrow} [\text{Binary forms}/(\mathbb{Z}/n)]$$

The aim is to give further extensions of them.

Our generalization

K: an algebraic number field/$\mathbb{Q}$ with $[K:\mathbb{Q}] < \infty$,
$\mathcal{O}$: the integer ring of K,
p, q: two prime numbers (prime ideals), $n = pq$,
R: a noncommutative subring of $\mathrm{Mat}_s(\mathcal{O}/n)$ $(s \geq 1)$,
$\{\alpha_1, \cdots, \alpha_r\}$: a basis of R over $\mathbb{Z}/n$.

Consider the following map $(l \geq 2)$.

$$(\mathbb{Z}/n)^{rl} \xrightarrow{A} (\mathbb{Z}/n)^{rl} \to R^l \xrightarrow{G} R^{l-1} \to (\mathbb{Z}/n)^{r(l-1)} \xrightarrow{B} (\mathbb{Z}/n)^{r(l-1)},$$

Here A, B are invertible affine (linear) transforms,
$(\mathbb{Z}/n)^{rl} \to R^l$ is $\mathbf{y} = (y_{11}, \cdots, y_{1r}, y_{21}, \cdots, y_{lr}) \mapsto \tilde{\mathbf{y}} = (y_1, \cdots, y_l)$
where $y_i = y_{i1}\alpha_1 + \cdots y_{ir}\alpha_r$,
$\tilde{\mathbf{g}} = (g_2, \cdots, g_l) := G(\tilde{\mathbf{y}})$ is as follows.

$$\begin{aligned} & g_i(y_1, \cdots, y_i) \\ & := v_{i1}(y_1, \cdots, y_{i-1})^t y_i + y_i^t v_{i2}(y_1, \cdots, y_{i-1}) + w_i(y_1, \cdots, y_{i-1}), \end{aligned}$$

where $v_{i\delta}(y_1, \cdots, y_{i-1}) := \sum_{1 \le j \le i-1} v_{i\delta}^{(j)} y_j$ $(\delta = 1, 2)$,
$w_i(y_1, \cdots, y_{i-1}) := \sum_{1 \le j_1, j_2 \le i-1} y_{j_1}^t w_{j_1 j_2}^{(i)} y_{j_2}$ with coefficients
$v_{21}, v_{22}, v_{j1}^{(i)}, v_{j2}^{(i)}, w_{j_1 j_2}^{(i)} \in R$.

Signature scheme.
Keys: The secret keys are A, G, B and the public key is the quadratic form $F(\mathbf{x}) = (B \circ G \circ A)(\mathbf{x})$.
Signatures x for m $:= (m_{22}, \cdots, m_{lr})^t \in (\mathbb{Z}/n)^{r(l-1)}$**:**
Compute $\mathbf{m}' = (m'_{22}, \cdots, m'_{lr})^t = B^{-1}\mathbf{m}$,
Express $\mathbf{m}'$ as an element of R^{l-1}.
Choose $y_1 \in R$ randomly and determine $y_2, \cdots, y_l \in R$ recursively by solving $g_i(y_1, \cdots, y_i) = m'_i$.
Express $\mathbf{y} = (y_1, \cdots, y_l) \in R^l$ as an element of $(\mathbb{Z}/n)^{rl}$.
Calculate $\mathbf{x} = A^{-1}\mathbf{y}$.
Verification: Verify whether $F(\mathbf{x}) = \mathbf{m}$.

Discussions on the security

Let

$$\mathbf{x} \overset{A}{\longmapsto} \mathbf{y} \mapsto \tilde{\mathbf{y}} \overset{G}{\longmapsto} \tilde{\mathbf{g}} \mapsto \mathbf{g} \overset{B}{\longmapsto} \mathbf{f}.$$

Original Scheme.

Since $\mathbf{y} = A\mathbf{x}$, $g_i = \mathbf{y}^t G_i \mathbf{y}$ and $\mathbf{f} = B\mathbf{g}$, we have

$$f_i(\mathbf{x}) = \sum_{j=2}^{l} b_{ij} \mathbf{x}^t A^t G_j A \mathbf{x} = \mathbf{x}^t A^t \left(\sum_{j=2}^{l} b_{ij} G_j \right) A\mathbf{x} =: \mathbf{x}^t F_i \mathbf{x},$$

where $B = (b_{ij})_{2 \le i,j \le l}$.

Since

$$G_i = \begin{pmatrix} & & v_1^{(i)} \\ & W_i & \vdots \\ & & v_{i-1}^{(i)} \\ v_1^{(i)} \quad \cdots & v_{i-1}^{(i)} & \\ & & 0 \end{pmatrix} \qquad (W_i \in \mathrm{Mat}_{i-1}(\mathbb{Z}/n)),$$

we have

$$\sum_{j=2}^{l} b_{i_1 j} G_j - \lambda \sum_{j=2}^{l} b_{i_2 j} G_j =$$

$$\begin{pmatrix} & & (b_{i_1 l} - \lambda b_{i_2 l}) v_1^{(l)} \\ & * & \vdots \\ & & (b_{i_1 l} - \lambda b_{i_2 l}) v_{i-1}^{(i)} \\ (b_{i_1 l} - \lambda b_{i_2 l}) v_1^{(i)} & \cdots \quad (b_{i_1 l} - \lambda b_{i_2 l}) v_{i-1}^{(i)} & 0 \end{pmatrix}.$$

Then partial information $\{b_{i_1 l} b_{i_2 l}^{-1}\}$ of B is obtained by solving the equation $\det(F_{i_1} - \lambda F_{i_2}) = 0$ because
$\det(F_{i_1} - \lambda F_{i_2}) = (b_{i_1 l} - \lambda b_{i_2 l})^2 \times (\text{polyn. of } \lambda)$.
One can get other information little by little recursively and can reduce $\mathbf{f}(\mathbf{x})$ to simple equations like $(g_2, \cdots, g_l)$.

When R is commutative:
Consider A and B as transformations in R^l and R^{l-1}.
Then

$$f_i(\mathbf{x}) = \sum_{j=2}^{l} b_{ij} \mathbf{x}^t A^t G_j A \mathbf{x} = \mathbf{x}^t A^t \left(\sum_{j=2}^{l} b_{ij} G_j \right) A \mathbf{x} =: \mathbf{x}^t F_i \mathbf{x},$$

This can be broken similarly with generalized linear algebra over commutative ring.

When R is non-commutative:

Even if A, B are expressed as transformations in R^l and R^{l-1}, direct extension of the linear algebraic attack is difficult.

1.

$$f_i(\mathbf{x}) = \sum_{j=2}^{l} b_{ij} \mathbf{x}^t A^t G_j A \mathbf{x} \neq \mathbf{x}^t A^t \left(\sum_{j=2}^{l} b_{ij} G_j \right) A \mathbf{x}.$$

2. There are few convenient tools in the linear algebra over noncommutative rings such like the determinant which
(i) characterizes the linear independency of the column and row vectors, and
(ii) satisfies $\det(ab) = \det(a)\det(b)$.
In the noncommutative R,

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} := a_{11}a_{22} - a_{11}a_{21}a_{11}^{-1}a_{12}$$

satisfies (i), but does not (ii). (For larger size matrices, the determinants are much more complicated...)

Consider $\tilde{\mathbf{g}}_i = \tilde{\mathbf{y}}^t G_i \tilde{\mathbf{y}}$.
Put

$$\begin{aligned}\tilde{\mathbf{y}} =& y^{(1)}\alpha_1 + \cdots + y^{(r)}\alpha_r, & y^{(k)} \in (\mathbb{Z}/n)^l,\\ G_j =& G_j^{(1)}\alpha_1 + \cdots + G_j^{(r)}\alpha_r, & G_j^{(k)} \in \mathrm{Mat}_{l-1}(\mathbb{Z}/n).\end{aligned}$$

We have

$$\tilde{g}_i = \tilde{\mathbf{y}}^t G_i \tilde{\mathbf{y}} = \sum_{k_1,k_2,k_3=1}^{r} (y^{(k_1)})^t G_i^{(k_2)} y^{(k_3)} (\alpha_{k_1}^t \alpha_{k_2} \alpha_{k_3}).$$

Put $c_{k_1k_2k_3}^{(k)} \in \mathbb{Z}/n$ s.t. $\alpha_{k_1}^t \alpha_{k_2} \alpha_{k_3} = c_{k_1k_2k_3}^{(1)}\alpha_1 + \cdots + c_{k_1k_2k_3}^{(r)}\alpha_r$.

$$\begin{aligned}\tilde{g}_i &= \sum_{k=1}^{r}\left[\sum_{k_1,k_2,k_3=1}^{r} c_{k_1k_2k_3}^{(k)} (y^{(k_1)})^t G_i^{(k_2)} y^{(k_3)}\right]\alpha_k\\ &= \sum_{k=1}^{r}\left[\sum_{k_1,k_3=1}^{r} (y^{(k_1)})^t \left[\sum_{k_2=1}^{r} c_{k_1k_2k_3}^{(k)} G_i^{(k_2)}\right] y^{(k_3)}\right]\alpha_k.\end{aligned}$$

We have

$$\tilde{g}_i = \sum_{k=1}^{r} \left[\mathbf{y}^t G_{i,k} \mathbf{y} \right] \alpha_k,$$

where

$$G_{i,k} = \left(\sum_{k_2=1}^{r} c^{(k)}_{k_1 k_2 k_3} G^{(k_2)}_i \right)_{1 \le k_1, k_3 \le r}$$

$$= \left(\begin{pmatrix} W^{(k_1,k_3)}_{i,k} & \\ & 0 \end{pmatrix} \right)_{1 \le k_1, k_3 \le r}, \quad W^{(k_1,k_3)}_{i,k} \in \mathrm{Mat}_i(\mathbb{Z}/n).$$

This seems to be much more complicated than the original scheme.
But be care that there might be many $c^{(k)}_{k_1 k_2 k_3} = 0$.
Consider several examples.

Example 1. $R = \mathrm{Mat}_s(\mathbb{Z}/n)$

The basis is $\{e_{ij}\}_{1 \le i,j \le s}$ where $e_{ij} :=$ $\begin{array}{c} \\ i \\ \\ \end{array}\begin{array}{c} \begin{array}{c} j \end{array} \\ \begin{pmatrix} \cdots & 1 \\ & \end{pmatrix} \end{array}$.

Since

$$e_{i_1 j_1} e_{i_2 j_2} = \begin{cases} e_{i_1 j_2} & (j_1 = i_2), \\ 0 & (\text{otherwise}), \end{cases}$$

most $c^{(k)}_{k_1 k_2 k_3}$ are vanished.

$$\mathrm{Prob}(c \neq 0) := \frac{\#\{c^{(k)}_{k_1 k_2 k_3} \neq 0\}}{\#\{(k_1, k_2, k_3, k)\}} = \frac{1}{s^4}.$$

The quadratic forms are simple for the number of parameters ($r = s^2$).

Consider the following simplest case.
$R = \mathrm{Mat}_2(\mathbb{Z}/n)$, $x_1^t x_1 + x_2^t h x_2 = m$ with $h^t = h$ and $m^t = m$.
Put $h = (h_{ij})$, $m = (m_{ij})$ and take

$$x_1 = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}, \quad x_2 = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}.$$

The equation $x_1^t x_1 + x_2^t h x_2 = m$ gives

$$\begin{aligned} a_{11}^2 + h_{11} b_1^2 &= m_{11}, \\ a_{11} a_{12} + h_{12} b_1 b_2 &= m_{12}, \\ a_{12}^2 + a_{22}^2 + h_{22} b_2^2 &= m_{22}. \end{aligned}$$

The above can be solved by twice Pollard-Schnorr's algorithms.
The case of general $R = \mathrm{Mat}_s(\mathbb{Z}/n)$ is similarly.
There are many parameters which do not contribute to the security.

Example 2. Quaternion version

$$R = \left\{ \begin{pmatrix} w & z \\ -\bar{z} & \bar{w} \end{pmatrix} \;\middle|\; w, z \in \mathbb{Z}[\sqrt{-1}]/n \right\} = < i_0 = 1, i_1, i_2, i_3 >_{\mathbb{Z}/n},$$

where $i_1^2 = i_2^2 = i_3^2 = -1$ and $i_1 i_2 = i_3 = -i_2 i_1$.

Since $i_{k_1}^t i_{k_2} i_{k_3} = \pm i_j$ for some $j = 0, \cdots, 3$,

$$c^{(k)}_{k_1 k_2 k_3} = \begin{cases} \pm 1 & \text{one of } k = 0, \cdots, 3, \\ 0 & \text{otherwise,} \end{cases}$$

$$\mathrm{Prob}(c \neq 0) = \frac{1}{4}.$$

Example 3. An example of 3×3 matrix versions

Let

$$g_1 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad g_2 := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad g_3 := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$
$$g_4 := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad g_5 := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Put $R =< g_1, \cdots, g_5 >_{\mathbb{Z}/n} \subset \mathrm{Mat}_3(\mathbb{Z}/n)$.
The identity is $I = g_1 + g_2 + g_3 - g_4 - g_5$.
$S_3 := \{I, g_1, \cdots, g_5\}$ is the symmetric group of degree 3.
$g_{k_1}^t g_{k_2} g_{k_3}$ is one of $g_1, \cdots, g_5$ or I.

$$\mathrm{Prob}(c \neq 0) \sim \frac{1}{3}.$$

Remarks on these constructions of R

In the quaternion case and S_3 case, R is written by
$R := \{\sum_{g\in G} a_g g \mid a_g \in \mathbb{Z}/n\}$ with the group

$$G = \begin{cases} \{\pm 1, \pm i_1, \pm i_2, \pm i_3\} & \subset \mathrm{Mat}_2(\mathbb{Z}[\sqrt{-1}]/n), \\ \{I, g_1, \cdots, g_5\} & \subset \mathrm{Mat}_3(\mathbb{Z}/n). \end{cases}$$

These are generalized as follows.
G: a (nonabelian) finite group in $\mathrm{Mat}_s(\mathcal{O})$ for some $K(\supset \mathcal{O})$,
$G' = \{g_1, \cdots, g_r\}$: a subset of G s.t. $g_1, \cdots, g_r$ are lin. indep.
and any $g \in G$ is lin. comb. of $g_1, \cdots, g_r$ over $\mathbb{Z}$.
$R(G) := \{\sum_{g\in G'} a_g g \mid a_g \in \mathbb{Z}/n\}$ is a subring of $\mathrm{Mat}_s(\mathcal{O}/n)$.

$$\mathrm{Prob}(c \neq 0) \geq \frac{1}{\#G'} \qquad \left(G' = G \Rightarrow \mathrm{Prob}(c \neq 0) = \frac{1}{\#G'}\right).$$

Possibility.

Since maximal compact groups in $\mathrm{Mat}_s(\mathbb{C})$ are isom. to $U(s) := \{g \in \mathrm{Mat}_s(\mathbb{C}) \mid \bar{g}^t g = I\}$, any finite group in $\mathrm{Mat}_s(\mathbb{C})$ is discrete subgroup of $U(s)$ up to isom.
For $s = 2$,

$$U(2) = \left\{ \rho \begin{pmatrix} w & z \\ -\bar{z} & \bar{w} \end{pmatrix} \;\middle|\; w, z, \rho \in \mathbb{C}, |\rho| = 1, |w|^2 + |z|^2 = 1 \right\}.$$

$R(G)$ with $G \subset U(2)$ is similar to the quaternion R.
If the quaternion case would be broken then other cases of $R(G) \subset \mathrm{Mat}_2(\mathcal{O}/n)$ might be broken similarly.

In fact, OSS with such $R(G)$ can be broken similarly by Coppersmith's attack to the quaternion OSS.

Note that if $R \subset \mathrm{Mat}_s(\mathcal{O}/n)$ with odd $s \geq 3$ and factoring $n = pq$ is infeasible, then C's attack is not valid to OSS.

Conclusion

Problem. Which R and which properties of R give high security of the signature scheme?

1. "$\mathrm{Prob}(c \neq 0)$ is larger" is better?

If $\mathrm{Prob}(c \neq 0)$ is larger, the quadratic forms seem to be more complicated....

2. More detail distribution of $c^{(k)}_{k_1 k_2 k_3}$?

If the distribution has "symmetricity", there might be attacks using the symmetricity (e.g. commutative case).

If the distribution has a strong bias, there might be attacks like "diff. attack".

3. Any other ...?