Rank Preserving Code-based Signature

Terry S.C. Lau  C. H. Tan

Temasek Laboratories,
National University of Singapore

ISIT 2020
IEEE International Symposium on Information Theory
21–26 June 2020
1. Introduction and Motivation
2. Rank Preserving Signature Scheme
3. Security of RPS & Hard Problem Assumption
4. Performance of RPS
5. Conclusion
**Definition (Signature Scheme)**

A signature scheme consists of four algorithms:

- **Setup**(1^n): parameters
- **Keygen**(parameters): public verification key pk, secret signature key sk
- **Sign**(sk, m): signature σ on message m under sk
- **Verify**(pk, m, σ): check whether σ is valid on m
Overview for Code-based Signature

1. Hash-&-Sign Signature
2. Proof of Knowledge: Identification protocol → Signature
3. Schnorr-type Signature

Question: Can we construct other secure Schnorr-type Signature in code-based setting (with compact key sizes and signature sizes)?
Overview for Code-based Signature

1. Hash-\&-Sign Signature
2. Proof of Knowledge: Identification protocol $\rightarrow$ Signature
3. Schnorr-type Signature

<table>
<thead>
<tr>
<th>Metric</th>
<th>Scheme</th>
<th>$\text{size}_{pk}$</th>
<th>$\text{size}_{\sigma}$</th>
<th>SecCL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hamming</td>
<td>Persichetti’s OTS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RaCoSS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rank</td>
<td>TPL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RQCS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Durandal</td>
<td>15.25KB</td>
<td>4.06KB</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td>MURAVE</td>
<td>5.33KB</td>
<td>9.69KB</td>
<td>128</td>
</tr>
</tbody>
</table>

Question: Can we construct other secure Schnorr-type Signature in code-based setting (with compact key sizes and signature sizes)?
Overview for Code-based Signature

1. Hash-&-Sign Signature
2. Proof of Knowledge: Identification protocol $\rightarrow$ Signature
3. Schnorr-type Signature

<table>
<thead>
<tr>
<th>Metric</th>
<th>Scheme</th>
<th>$\text{size}_{pk}$</th>
<th>$\text{size}_{\sigma}$</th>
<th>$\text{Sec}_{\text{CL}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hamming</td>
<td>Persichetti’s OTS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RaCoSS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rank</td>
<td>TPL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RQCS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Durandal</td>
<td>15.25KB</td>
<td>4.06KB</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td>MURAVE</td>
<td>5.33KB</td>
<td>9.69KB</td>
<td>128</td>
</tr>
</tbody>
</table>

**Question:** Can we construct other secure Schnorr-type Signature in code-based setting (with compact key sizes and signature sizes)?
Some Terminology

\( \mathbb{F}_{q^m} \): finite field with \( q^m \) elements
Some Terminology

- $\mathbb{F}_{q^m}$: finite field with $q^m$ elements
- $P_k(X) \in \mathbb{F}_q[X]$: irreducible polynomial of degree $k$
Some Terminology

- $\mathbb{F}_{q^m}$: finite field with $q^m$ elements
- $P_k(X) \in \mathbb{F}_q[X]$: irreducible polynomial of degree $k$
- $g = (g_0, \ldots, g_{k-1}) \in \mathbb{F}_{q^m}^k \iff G(X) = \sum_{i=0}^{k-1} g_i X^i$
Some Terminology

- \( \mathbb{F}_{q^m} \): finite field with \( q^m \) elements
- \( P_k(X) \in \mathbb{F}_q[X] \): irreducible polynomial of degree \( k \)
- \( g = (g_0, \ldots, g_{k-1}) \in \mathbb{F}_{q^m}^k \iff G(X) = \sum_{i=0}^{k-1} g_i X^i \)
- \( g, h \in \mathbb{F}_{q^m}^k \): \( gh = G(X)H(X) \mod P_k(X) \)

\( \langle \cdot \rangle \): linear span of "\( \cdot \)"
Some Terminology

- $\mathbb{F}_{q^m}$: finite field with $q^m$ elements
- $P_k(X) \in \mathbb{F}_q[X]$: irreducible polynomial of degree $k$
- $g = (g_0, \ldots, g_{k-1}) \in \mathbb{F}_{q^m}^k$ $\implies$ $G(X) = \sum_{i=0}^{k-1} g_i X^i$
- $g, h \in \mathbb{F}_{q^m}^k$: $gh = G(X)H(X) \mod P_k(X)$
- $g \in \mathbb{F}_{q^m}^k$ is invertible if there exists $h \in \mathbb{F}_{q^m}^k$ such that $1 = gh = hg \mod P$. We denote $g^{-1} = h$
Some Terminology

- $\mathbb{F}_{q^m}$: finite field with $q^m$ elements
- $P_k(X) \in \mathbb{F}_q[X]$: irreducible polynomial of degree $k$
- $\mathbf{g} = (g_0, \ldots, g_{k-1}) \in \mathbb{F}_{q^m}^k \iff G(X) = \sum_{i=0}^{k-1} g_i X^i$
- $\mathbf{g}, \mathbf{h} \in \mathbb{F}_{q^m}^k$: $\mathbf{gh} = G(X)H(X) \mod P_k(X)$
- $\mathbf{g} \in \mathbb{F}_{q^m}^k$ is invertible if there exists $\mathbf{h} \in \mathbb{F}_{q^m}^k$ such that $1 = \mathbf{gh} = \mathbf{hg} \mod P$. We denote $\mathbf{g}^{-1} = \mathbf{h}$
- $\langle \cdots \rangle$ - linear span of “...”
Some Terminology

- $\mathbb{F}_{q^m}$: finite field with $q^m$ elements
- $P_k(X) \in \mathbb{F}_q[X]$: irreducible polynomial of degree $k$
- $g = (g_0, \ldots, g_{k-1}) \in \mathbb{F}_{q^m}^k \iff G(X) = \sum_{i=0}^{k-1} g_i X^i$
- $g, h \in \mathbb{F}_{q^m}^k$: $gh = G(X)H(X) \mod P_k(X)$
- $g \in \mathbb{F}_{q^m}^k$ is invertible if there exists $h \in \mathbb{F}_{q^m}^k$ such that $1 = gh = hg \mod P$. We denote $g^{-1} = h$
- $\langle \cdots \rangle$ - linear span of “\cdots”
- View $\mathbb{F}_{q^m} = \langle \beta_1, \ldots, \beta_m \rangle$ as $\mathbb{F}_q$-vector space
Some Terminology

- $\mathbb{F}_{q^m}$: finite field with $q^m$ elements
- $P_k(X) \in \mathbb{F}_q[X]$: irreducible polynomial of degree $k$
- $g = (g_0, \ldots, g_{k-1}) \in \mathbb{F}_{q^m}^k \implies G(X) = \sum_{i=0}^{k-1} g_i X^i$
- $g, h \in \mathbb{F}_{q^m}^k$: $gh = G(X)H(X) \mod P_k(X)$
- $g \in \mathbb{F}_{q^m}^k$ is invertible if there exists $h \in \mathbb{F}_{q^m}^k$ such that $1 = gh = hg \mod P$. We denote $g^{-1} = h$
- $\langle \cdots \rangle$ - linear span of “· · ·”
- View $\mathbb{F}_{q^m} = \langle \beta_1, \ldots, \beta_m \rangle$ as $\mathbb{F}_q$-vector space
- Let $x = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$. Support for $x$: $\text{supp}(x) = \langle x_1, \ldots, x_n \rangle$ - a vector subspace of $\mathbb{F}_{q^m}$
Some Terminology

- $\mathbb{F}_{q^m}$: finite field with $q^m$ elements
- $P_k(X) \in \mathbb{F}_q[X]$: irreducible polynomial of degree $k$
- $g = (g_0, \ldots, g_{k-1}) \in \mathbb{F}_{q^m}^k \iff G(X) = \sum_{i=0}^{k-1} g_i X^i$
- $g, h \in \mathbb{F}_{q^m}^k$: $gh = G(X)H(X) \mod P_k(X)$
- $g \in \mathbb{F}_{q^m}^k$ is invertible if there exists $h \in \mathbb{F}_{q^m}^k$ such that $1 = gh = hg \mod P$. We denote $g^{-1} = h$
- $\langle \cdots \rangle$ - linear span of “\cdots”
- View $\mathbb{F}_{q^m} = \langle \beta_1, \ldots, \beta_m \rangle$ as $\mathbb{F}_q$-vector space
- Let $x = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$. Support for $x$: $\text{supp}(x) = \langle x_1, \ldots, x_n \rangle$ - a vector subspace of $\mathbb{F}_{q^m}$
- Rank metric: $\text{rk}(x) = \dim(\text{supp}(x))$
Some Terminology

- $\mathbb{F}_{q^m}$: finite field with $q^m$ elements
- $P_k(X) \in \mathbb{F}_q[X]$: irreducible polynomial of degree $k$
- $g = (g_0, \ldots, g_{k-1}) \in \mathbb{F}_{q^m}^k \iff G(X) = \sum_{i=0}^{k-1} g_i X^i$
- $g, h \in \mathbb{F}_{q^m}^k$: $gh = G(X)H(X) \mod P_k(X)$
- $g \in \mathbb{F}_{q^m}^k$ is invertible if there exists $h \in \mathbb{F}_{q^m}^k$ such that $1 = gh = hg \mod P$. We denote $g^{-1} = h$
- $\langle \cdots \rangle$ - linear span of “$\cdots$”
- View $\mathbb{F}_{q^m} = \langle \beta_1, \ldots, \beta_m \rangle$ as $\mathbb{F}_q$-vector space
- Let $x = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$. Support for $x$:
  $\text{supp}(x) = \langle x_1, \ldots, x_n \rangle$ - a vector subspace of $\mathbb{F}_{q^m}$
- Rank metric: $\text{rk}(x) = \dim(\text{supp}(x))$
- $A = \langle a_1, \ldots, a_r \rangle$, $B = \langle b_1, \ldots, b_d \rangle$. Define product space $A.B = \langle a_1 b_1, \ldots, a_r b_d \rangle$. 
In RQCS: $pk = (H, s = (e_1, e_2)H^T)$ and $sk = (e_1, e_2)$ (low rank)
Schnorr Approach in Rank Metric: RQCS Signature

In RQCS: \( pk = (H, s = (e_1, e_2)H^T) \) and \( sk = (e_1, e_2) \) (low rank)

\[
\begin{align*}
\gamma & = (y_1, y_2)H^T \\
c & = \mathcal{H}(\gamma, m, pk) \\
z_1 & = y_1 + ce_1, \\
z_2 & = y_2 + ce_2
\end{align*}
\]

Signature leaks information from the secret key!
In RQCS: \( pk = (H, s = (e_1, e_2)H^T) \) and \( sk = (e_1, e_2) \) (low rank)

\[
\begin{align*}
\gamma &= (y_1, y_2)H^T \\
\mathbf{c} &= \mathcal{H}(\gamma, m, pk) \\
z_1 &= y_1 + ce_1, \\
z_2 &= y_2 + ce_2
\end{align*}
\]

\[
\sigma = (c, z_1, z_2)
\]

Compute \( \gamma = (z_1, z_2)H^T - cs \)

Check: i. \( c = \mathcal{H}(\gamma, m, pk) \)

ii. \( \text{rk}(z) \leq \text{rk}(y) + \text{rk}(c)\text{rk}(e) \)
In RQCS: \( \text{pk} = (H, s = (e_1, e_2)H^T) \) and \( \text{sk} = (e_1, e_2) \) (low rank)

\[
\begin{align*}
\gamma &= (y_1, y_2)H^T \\
c &= \mathcal{H}(\gamma, m, \text{pk}) \\
z_1 &= y_1 + ce_1 \\
z_2 &= y_2 + ce_2
\end{align*}
\]

\[
\sigma = (c, z_1, z_2)
\]

Compute \( \gamma = (z_1, z_2)H^T - cs \)

Check: i. \( c = \mathcal{H}(\gamma, m, \text{pk}) \)

ii. \( \text{rk}(z) \leq \text{rk}(y) + \text{rk}(c)\text{rk}(e) \)

\[
\text{supp}(c) = \langle \gamma_1, \ldots, \gamma_r \rangle, \text{supp}(z) = \langle \mu_1, \ldots, \mu_t, \epsilon_1 \gamma_1, \ldots, \epsilon_w \gamma_r \rangle.
\]
Schnorr Approach in Rank Metric: RQCS Signature

In RQCS: \( pk = (H, s = (e_1, e_2)H^T) \) and \( sk = (e_1, e_2) \) (low rank)

\[
\begin{align*}
\gamma &= (y_1, y_2)H^T \\
c &= H(\gamma, m, pk) \\
z_1 &= y_1 + ce_1, \\
z_2 &= y_2 + ce_2 \\
\end{align*}
\]

\[
\sigma = (c, z_1, z_2)
\]

Compute \( \gamma = (z_1, z_2)H^T - cs \)

Check:

i. \( c = H(\gamma, m, pk) \)

ii. \( rk(z) \leq rk(y) + rk(c)rk(e) \)

\[
\mathrm{supp}(c) = \langle \gamma_1, \ldots, \gamma_r \rangle, \quad \mathrm{supp}(z) = \langle \mu_1, \ldots, \mu_t, \epsilon_1 \gamma_1, \ldots, \epsilon_w \gamma_r \rangle.
\]

Aim: Determine \( \mathrm{supp}(e) = \langle \epsilon_1, \ldots, \epsilon_w \rangle \)
Schnorr Approach in Rank Metric: RQCS Signature

In RQCS: \( pk = (H, s = (e_1, e_2)H^T) \) and \( sk = (e_1, e_2) \) (low rank)

\[
\begin{align*}
\gamma &= (y_1, y_2)H^T \\
c &= H(\gamma, m, pk) \\
z_1 &= y_1 + ce_1, \\
z_2 &= y_2 + ce_2 \\
\sigma &= (c, z_1, z_2)
\end{align*}
\]

Compute \( \gamma = (z_1, z_2)H^T - cs \)

Check:

i. \( c \equiv H(\gamma, m, pk) \)

ii. \( \text{rk}(z) \leq \text{rk}(y) + \text{rk}(c)\text{rk}(e) \)

\( \text{supp}(c) = \langle \gamma_1, \ldots, \gamma_r \rangle, \text{supp}(z) = \langle \mu_1, \ldots, \mu_t, \epsilon_1\gamma_1, \ldots, \epsilon_w\gamma_r \rangle. \)

Aim: Determine \( \text{supp}(e) = \langle \epsilon_1, \ldots, \epsilon_w \rangle \)

Using techniques from the decoding of Low Rank Parity Check (LRPC) codes, with high probability we have

\[
\bigcap_{i=1}^{r} \gamma_i^{-1} \cdot \text{supp}(z) = \bigcap_{i=1}^{r} \langle \gamma_i^{-1} \mu_1, \ldots, \gamma_i^{-1} \epsilon_w \gamma_r \rangle = \text{supp}(e)
\]
Schnorr Approach in Rank Metric: RQCS Signature

In RQCS: \( pk = (H, s = (e_1, e_2)H^T) \) and \( sk = (e_1, e_2) \) (low rank)

\[
\begin{align*}
\gamma &= (y_1, y_2)H^T \\
c &= \mathcal{H}(\gamma, m, pk) \\
z_1 &= y_1 + ce_1 \\
z_2 &= y_2 + ce_2
\end{align*}
\]

\( \sigma = (c, z_1, z_2) \)

Compute \( \gamma = (z_1, z_2)H^T - cs \)

Check:

i. \( c \stackrel{?}{=} \mathcal{H}(\gamma, m, pk) \)

ii. \( \text{rk}(z) \leq \text{rk}(y) + \text{rk}(c)\text{rk}(e) \)

\( \text{supp}(c) = \langle \gamma_1, \ldots, \gamma_r \rangle, \text{supp}(z) = \langle \mu_1, \ldots, \mu_t, \epsilon_1\gamma_1, \ldots, \epsilon_w\gamma_r \rangle \).

Aim: Determine \( \text{supp}(e) = \langle \epsilon_1, \ldots, \epsilon_w \rangle \)

Using techniques from the decoding of Low Rank Parity Check (LRPC) codes, with high probability we have

\[
\bigcap_{i=1}^{r} (\gamma_i^{-1} \cdot \text{supp}(z)) = \bigcap_{i=1}^{r} \langle \gamma_i^{-1}\mu_1, \ldots, \gamma_i^{-1}\epsilon_w\gamma_r \rangle = \text{supp}(e)
\]

Signature leaks information from the secret key!
In RQCS: $pk = (H, s = (e_1, e_2)H^T)$ and $sk = (e_1, e_2)$

$$
\begin{align*}
\gamma &= (y_1, y_2)H^T \\
c &= \mathcal{H}(\gamma, m, pk) \\
z_1 &= y_1 + ce_1, \quad z_2 = y_2 + ce_2 \\
\end{align*}
$$

$\sigma = (c, z_1, z_2)$
Idea for RPS

In RQCS: \( pk = (H, s = (e_1, e_2)H^T) \) and \( sk = (e_1, e_2) \)

\[
\begin{align*}
\gamma &= (y_1, y_2)H^T \\
c &= H(\gamma, m, pk) \\
z_1 &= y_1 + ce_1, \quad z_2 = y_2 + ce_2
\end{align*}
\]

\[
\sigma = (c, z_1, z_2)
\]

Idea: \( pk = \left(H \text{ gen. by } \left( h = e_1^{-1}e_2, h^{-1} \right) \right) \) and \( sk = (e_1, e_2) \)
Idea for RPS

In RQCS: $pk = (H, s = (e_1, e_2)H^T)$ and $sk = (e_1, e_2)$

\[
\begin{align*}
\gamma &= (y_1, y_2)H^T \\
c &= \mathcal{H}(\gamma, m, pk) \\
z_1 &= y_1 + ce_1, \quad z_2 = y_2 + ce_2
\end{align*}
\]

\[
\sigma = (c, z_1, z_2)
\]

Idea: $pk = \left(H \text{ gen. by } \begin{pmatrix} h = e_1^{-1}e_2, h^{-1} \end{pmatrix}\right)$ and $sk = (e_1, e_2)$

\[
\gamma = (y_1e_1, y_2e_2)H^T
\]
Idea for RPS

In RQCS: \( pk = (H, s = (e_1, e_2)H^T) \) and \( sk = (e_1, e_2) \)

\[
\begin{align*}
\gamma &= (y_1, y_2)H^T \\
c &= H(\gamma, m, pk) \\
z_1 &= y_1 + ce_1, \quad z_2 = y_2 + ce_2 \\
\end{align*}
\]

\[
\sigma = (c, z_1, z_2)
\]

Idea: \( pk = \left( H \text{ gen. by } \begin{pmatrix} h = e_1^{-1}e_2, h^{-1} \end{pmatrix} \right) \) and \( sk = (e_1, e_2) \)

\[
\begin{align*}
\gamma &= (y_1e_1, y_2e_2)H^T \\
s &= (u_1e_1, u_2e_2)H^T \\
\end{align*}
\]
Idea for RPS

In RQCS: \( pk = (H, s = (e_1, e_2)H^T) \) and \( sk = (e_1, e_2) \)

\[
\begin{align*}
\gamma &= (y_1, y_2)H^T \\
c &= \mathcal{H}(\gamma, m, pk) \\
z_1 &= y_1 + ce_1, \quad z_2 = y_2 + ce_2
\end{align*}
\]

\[\sigma = (c, z_1, z_2)\]

Idea: \( pk = \left( H \text{ gen. by } \left[ \begin{pmatrix} h &= e_1^{-1}e_2, h^{-1} \end{pmatrix} \right] \right) \) and \( sk = (e_1, e_2) \)

\[
\begin{align*}
\gamma &= (y_1e_1, y_2e_2)H^T \\
s &= (u_1e_1, u_2e_2)H^T \\
c &= \mathcal{H}(\gamma, s, m, pk)
\end{align*}
\]
Idea for RPS

In RQCS: \( pk = (H, s = (e_1, e_2)H^T) \) and \( sk = (e_1, e_2) \)

\[
\begin{align*}
\gamma &= (y_1, y_2)H^T \\
c &= \mathcal{H}(\gamma, m, pk) \\
z_1 &= y_1 + ce_1, \quad z_2 = y_2 + ce_2
\end{align*}
\]

\( \sigma = (c, z_1, z_2) \)

Idea: \( pk = \left( H \text{ gen. by } \left[ \begin{array}{c} h = e_1^{-1}e_2, h^{-1} \end{array} \right] \right) \) and \( sk = (e_1, e_2) \)

\[
\begin{align*}
\gamma &= (y_1e_1, y_2e_2)H^T \\
s &= (u_1e_1, u_2e_2)H^T \\
c &= \mathcal{H}(\gamma, s, m, pk) \\
z_1 &= (y_1 + cu_1)e_1, \\
z_2 &= (y_2 + cu_2)e_2
\end{align*}
\]
Idea for RPS

In RQCS: $pk = (H, s = (e_1, e_2)H^T)$ and $sk = (e_1, e_2)$

$$\gamma = (y_1, y_2)H^T$$
$$c = \mathcal{H}(\gamma, m, pk)$$
$$z_1 = y_1 + ce_1, \quad z_2 = y_2 + ce_2$$

\[ \sigma = (c, z_1, z_2) \]

\[ \gamma = (y_1e_1, y_2e_2)H^T \]
\[ s = (u_1e_1, u_2e_2)H^T \]
\[ c = \mathcal{H}(\gamma, s, m, pk) \]
\[ z_1 = (y_1 + cu_1)e_1, \]
\[ z_2 = (y_2 + cu_2)e_2 \]

\[ \sigma = (c, s, z_1, z_2) \]
Idea for RPS

In RQCS: $pk = (H, s = (e_1, e_2)H^T)$ and $sk = (e_1, e_2)$

$\gamma = (y_1, y_2)H^T$
$c = \mathcal{H}(\gamma, m, pk)$
$z_1 = y_1 + ce_1, \quad z_2 = y_2 + ce_2$

$\sigma = (c, z_1, z_2)$

Idea: $pk = \left( H \text{ gen. by } \begin{pmatrix} h = e_1^{-1}e_2, h^{-1} \end{pmatrix} \right)$ and $sk = (e_1, e_2)$

$\gamma = (y_1e_1, y_2e_2)H^T$
$s = (u_1e_1, u_2e_2)H^T$
$c = \mathcal{H}(\gamma, s, m, pk)$
$z_1 = (y_1 + cu_1)e_1,$
$z_2 = (y_2 + cu_2)e_2$

$\sigma = (c, s, z_1, z_2)$

The information on secret $E_1$ is hidden by the vector $y_1 + cu_1$
Idea for RPS

In RQCS: \( pk = (H, s = (e_1, e_2)H^T) \) and \( sk = (e_1, e_2) \)

\[
\begin{align*}
\gamma &= (y_1, y_2)H^T \\
c &= \mathcal{H}(\gamma, m, pk) \\
z_1 &= y_1 + ce_1, \quad z_2 = y_2 + ce_2 \\
\end{align*}
\]

\[\sigma = (c, z_1, z_2)\]

Idea: \( pk = \left( H \text{ gen. by } \begin{pmatrix} h = e_1^{-1}e_2, h^{-1} \end{pmatrix} \right) \) and \( sk = (e_1, e_2) \)

\[
\begin{align*}
\gamma &= (y_1e_1, y_2e_2)H^T \\
s &= (u_1e_1, u_2e_2)H^T \\
c &= \mathcal{H}(\gamma, s, m, pk) \\
z_1 &= (y_1 + cu_1)e_1, \\
z_2 &= (y_2 + cu_2)e_2 \\
\end{align*}
\]

\[\sigma = (c, s, z_1, z_2)\]

The information on secret \( E_1 \) is hidden by the vector \( y_1 + cu_1 \)
The information on secret \( E_2 \) is hidden by the vector \( y_2 + cu_2 \)
Idea for RPS

Keygen: \( pk = (h) \) and \( sk = (e_1, e_2) \)

Sign: \( \sigma = (c, s, z_1, z_2) \)
Idea for RPS

<table>
<thead>
<tr>
<th>Keygen: ( pk = (h) ) and ( sk = (e_1, e_2) )</th>
<th>Sign: ( \sigma = (c, s, z_1, z_2) )</th>
</tr>
</thead>
</table>

Verify\((pk, m, \sigma)\): Compute

\[
\vartheta_{m,k} = \min\{m - 1, k - 1\}, \quad \gamma = (z_1, z_2)H^T - cs.
\]
Idea for RPS

Keygen: \( pk = (h) \) and \( sk = (e_1, e_2) \)

Sign: \( \sigma = (c, s, z_1, z_2) \)

Verify(\( pk \), \( m \), \( \sigma \)): Compute

\[ d_{m,k} = \min\{m - 1, k - 1\}, \quad \gamma = (z_1, z_2)H^T - cs. \]

Check whether

- \( c = \mathcal{H}(\gamma, s, m, pk) \)
Idea for RPS

**Keygen:** \( pk = (h) \) and \( sk = (e_1, e_2) \)

**Sign:** \( \sigma = (c, s, z_1, z_2) \)

**Verify**(\( pk, m, \sigma \)): Compute

\[
\vartheta_{m,k} = \min\{m - 1, k - 1\}, \quad \gamma = (z_1, z_2)H^T - cs.
\]

Check whether

- \( c = H(\gamma, s, m, pk) \)
- \( \text{rk}(z_1) = (r_{y_1} + r_{u_1})r_{e_1}, \text{rk}(z_1h) = (r_{y_1} + r_{u_1})r_{e_2} \)
- \( \text{rk}(z_2) = (r_{y_2} + r_{u_2})r_{e_2}, \text{rk}(z_2h^{-1}) = (r_{y_2} + r_{u_2})r_{e_1} \)
Idea for RPS

Keygen: \( pk = (h) \) and \( sk = (e_1, e_2) \)

Sign: \( \sigma = (c, s, z_1, z_2) \)

Verify\((pk, m, \sigma)\): Compute

\[\varrho_{m,k} = \min\{m - 1, k - 1\}, \quad \gamma = (z_1, z_2)H^T - cs.\]

Check whether

- \( c = \mathcal{H}(\gamma, s, m, pk) \)
- \( \text{rk}(z_1) = (r_y + r_u) e_1, \text{rk}(z_1h) = (r_y + r_u) e_2 \)
- \( \text{rk}(z_2) = (r_y + r_u) e_2, \text{rk}(z_2h^{-1}) = (r_y + r_u) e_1 \)
- \( \text{rk}(s) = r_u e_2 + r_u e_1, \text{rk}(sh) \geq \varrho_{m,k}, \text{rk}(sh^{-1}) \geq \varrho_{m,k} \)
- \( \text{rk}(\gamma) = r_y e_2 + r_y e_1, \text{rk}(\gamma h) \geq \varrho_{m,k}, \text{rk}(\gamma h^{-1}) \geq \varrho_{m,k} \)
Idea for RPS

Keygen: \( pk = (h) \) and \( sk = (e_1, e_2) \)

Sign: \( \sigma = (c, s, z_1, z_2) \)

Verify(\( pk, m, \sigma \)): Compute

\[ \varrho_{m,k} = \min\{m - 1, k - 1\}, \quad \gamma = (z_1, z_2)H^T - cs. \]

Check whether

- \( c = \mathcal{H}(\gamma, s, m, pk) \)
- \( \text{rk}(z_1) = (r_{y_1} + r_{u_1})r_{e_1}, \text{rk}(z_1h) = (r_{y_1} + r_{u_1})r_{e_2} \)
- \( \text{rk}(z_2) = (r_{y_2} + r_{u_2})r_{e_2}, \text{rk}(z_2h^{-1}) = (r_{y_2} + r_{u_2})r_{e_1} \)
- \( \text{rk}(s) = r_{u_1}r_{e_2} + r_{u_2}r_{e_1}, \text{rk}(sh) \geq \varrho_{m,k}, \text{rk}(sh^{-1}) \geq \varrho_{m,k} \)
- \( \text{rk}(\gamma) = r_{y_1}r_{e_2} + r_{y_2}r_{e_1}, \text{rk}(\gamma h) \geq \varrho_{m,k}, \text{rk}(\gamma h^{-1}) \geq \varrho_{m,k} \)

Rank Preserving Signature (RPS): set \( r_{e_1} = r_{e_2} \),
Idea for RPS

Keygen: \( pk = (h) \) and \( sk = (e_1, e_2) \)

Sign: \( \sigma = (c, s, z_1, z_2) \)

Verify\((pk, m, \sigma)\): Compute

\[
\vartheta_{m,k} = \min\{m - 1, k - 1\}, \quad \gamma = (z_1, z_2)H^T - cs.
\]

Check whether

- \( c = \mathcal{H}(\gamma, s, m, pk) \)
- \( \text{rk}(z_1) = (r_{y_1} + r_{u_1})r_{e_1}, \text{rk}(zh) = (r_{y_1} + r_{u_1})r_{e_2} \)
- \( \text{rk}(z_2) = (r_{y_2} + r_{u_2})r_{e_2}, \text{rk}(z_2h^{-1}) = (r_{y_2} + r_{u_2})r_{e_1} \)
- \( \text{rk}(s) = r_{u_1}r_{e_2} + r_{u_2}r_{e_1}, \text{rk}(sh) \geq \vartheta_{m,k}, \text{rk}(sh^{-1}) \geq \vartheta_{m,k} \)
- \( \text{rk}(\gamma) = r_{y_1}r_{e_2} + r_{y_2}r_{e_1}, \text{rk}(\gamma h) \geq \vartheta_{m,k}, \text{rk}(\gamma h^{-1}) \geq \vartheta_{m,k} \)

Rank Preserving Signature (RPS): set \( r_{e_1} = r_{e_2} \), then\( \text{rk}(z) = \text{rk}(zH^T) \), i.e., rank of the signature is preserved.
### Problem (Rank Syndrome Decoding (RSD) Problem)

Let $H$ be a full rank $(n - k) \times n$ matrix over $\mathbb{F}_{q^m}$, $s \in \mathbb{F}_{q^m}^{n-k}$ and $r$ an integer. The RSD$\gamma_H(q, m, n, k, r)$ is to determine a vector $x \in \mathbb{F}_{q^m}^n$ such that $xH^T = s$ and $\text{rk}(x) = r$. 

Given $\gamma = (y_1e_1, y_2e_2)H^T$. Aim: Determine $(y_1e_1, y_2e_2)$. 

### Problem (Ideal LRPC Codes Support Recovery (I-LRPC SR))

Given a polynomial $P_k \in \mathbb{F}_{q^m}[X]$ of degree $k$ and $h = x - 1y \in \mathbb{F}_{q^m}^k$. The I-LRPC SR problem is to determine the vectors $x$ and $y$ such that $\text{rk}(x, y) = d$. 

Given $h = e_1 - 1e_2$. Aim: Determine $(e_1, e_2)$. 


Problem (Rank Syndrome Decoding (RSD) Problem)

Let $H$ be a full rank $(n - k) \times n$ matrix over $\mathbb{F}_{q^m}$, $s \in \mathbb{F}_{q^m}^{n-k}$ and $r$ an integer. The $\text{RSD}_H(q, m, n, k, r)$ is to determine a vector $x \in \mathbb{F}_{q^m}^n$ such that $xH^T = s$ and $\text{rk}(x) = r$.

Given $\gamma = (y_1e_1, y_2e_2)H^T$. Aim: Determine $(y_1e_1, y_2e_2)$. 
Problem (Rank Syndrome Decoding (RSD) Problem)

Let $H$ be a full rank $(n - k) \times n$ matrix over $\mathbb{F}_{q^m}$, $s \in \mathbb{F}_{q^m}^{n-k}$ and $r$ an integer. The RSD$_H(q, m, n, k, r)$ is to determine a vector $x \in \mathbb{F}_{q^m}^n$ such that $xH^T = s$ and $\text{rk}(x) = r$.

Given $\gamma = (y_1 e_1, y_2 e_2)H^T$. Aim: Determine $(y_1 e_1, y_2 e_2)$.

Problem (Ideal LRPC Codes Support Recovery (I-LRPC.SR))

Given a polynomial $P_k \in \mathbb{F}_q[X]$ of degree $k$ and $h = x^{-1}y \in \mathbb{F}_{q^m}^k$. The I-LRPC.SR problem is to determine the vectors $x$ and $y$ such that $\text{rk}(x, y) = d$. 

Security of RPS Signature (1)
Problem (Rank Syndrome Decoding (RSD) Problem)

Let $H$ be a full rank $(n - k) \times n$ matrix over $\mathbb{F}_{q^m}$, $s \in \mathbb{F}_{q^m}^{n-k}$ and $r$ an integer. The $\text{RSD}_H(q, m, n, k, r)$ is to determine a vector $x \in \mathbb{F}_{q^m}^n$ such that $xH^T = s$ and $\text{rk}(x) = r$.

Given $\gamma = (y_1 e_1, y_2 e_2)H^T$. Aim: Determine $(y_1 e_1, y_2 e_2)$.

Problem (Ideal LRPC Codes Support Recovery (I-LRPC.SR))

Given a polynomial $P_k \in \mathbb{F}_q[X]$ of degree $k$ and $h = x^{-1}y \in \mathbb{F}_{q^m}^k$. The I-LRPC.SR problem is to determine the vectors $x$ and $y$ such that $\text{rk}(x, y) = d$.

Given $h = e_1^{-1}e_2$. 

Security of RPS Signature (1)
### Problem (Rank Syndrome Decoding (RSD) Problem)

Let $H$ be a full rank $(n - k) \times n$ matrix over $\mathbb{F}_{q^m}$, $s \in \mathbb{F}_{q^m}^{n-k}$ and $r$ an integer. The RSD$_H(q, m, n, k, r)$ is to determine a vector $x \in \mathbb{F}_{q^m}^n$ such that $xH^T = s$ and $\text{rk}(x) = r$.

Given $\gamma = (y_1e_1, y_2e_2)H^T$. Aim: Determine $(y_1e_1, y_2e_2)$.

### Problem (Ideal LRPC Codes Support Recovery (I-LRPC.SR))

Given a polynomial $P_k \in \mathbb{F}_q[X]$ of degree $k$ and $h = x^{-1}y \in \mathbb{F}_{q^m}^k$. The I-LRPC.SR problem is to determine the vectors $x$ and $y$ such that $\text{rk}(x, y) = d$.

Given $h = e_1^{-1}e_2$. Aim: Determine $(e_1, e_2)$.
Problem (Rank Support Basis Decomposition (RSBD) Problem)

Let $X \subset \mathbb{F}_{q^m}$ be an $rd$-dimensional product space such that $X = A.B$, where $A \in \text{Gr}(r, \mathbb{F}_{q^m})$ and $B \in \text{Gr}(d, \mathbb{F}_{q^m})$. The RSBD problem is to determine bases for $A$ and $B$ such that $X = A.B$, $\dim(A) = r$ and $\dim(B) = d$. 
Problem (Rank Support Basis Decomposition (RSBD) Problem)

Let $X \subset \mathbb{F}_{q^m}$ be an $rd$-dimensional product space such that $X = A.B$, where $A \in \text{Gr}(r, \mathbb{F}_{q^m})$ and $B \in \text{Gr}(d, \mathbb{F}_{q^m})$. The RSBD problem is to determine bases for $A$ and $B$ such that $X = A.B$, $\dim(A) = r$ and $\dim(B) = d$.

Given $z_i = (y_i + cu_i)e_i$. 
Problem (Rank Support Basis Decomposition (RSBD) Problem)

Let \( X \subset \mathbb{F}_{q^m} \) be an \( rd \)-dimensional product space such that \( X = A.B \), where \( A \in \text{Gr}(r, \mathbb{F}_{q^m}) \) and \( B \in \text{Gr}(d, \mathbb{F}_{q^m}) \). The RSBD problem is to determine bases for \( A \) and \( B \) such that \( X = A.B \), \( \dim(A) = r \) and \( \dim(B) = d \).

Given \( z_i = (y_i + cu_i)e_i \).

Aim: Let \( T_i = \text{supp}(y_i + cu_i) \). Then we have \( Z_i = T_i.E_i \).

Determine \( T_i \) and \( E_i \) such that

\[
Z_i = T_i.E_i, \quad \dim(T_i) = r_{y_i} + r_{u_i}, \quad \dim(E_i) = r_{e_i}.
\]
We define a new problem:

**Problem (Rank Vector Decomposition (RVD) Problem)**

Let $X \in \text{Gr}(r_1, F_{q^m})$, $Y \in \text{Gr}(r_2, F_{q^m})$ and $Z \in \text{Gr}(r_3, F_{q^m})$ such that $X \cap Y = 0$ and $Z \cap Y = 0$. Given $a = x + y$ and $b = y + z$ such that $x \in X^k$, $y \in Y^k$, $z \in Z^k$, $r_1 + r_2 < m$, $r_2 + r_3 < m$ and $r_1 + r_2 + r_3 \geq m$. The RVD$_{a,b}$ problem is to determine the unique pair $(Y, y)$ such that $a = x + y$ and $b = y + z$. 
We define a new problem:

**Problem (Rank Vector Decomposition (RVD) Problem)**

Let \( X \in \text{Gr}(r_1, \mathbb{F}_{q^m}) \), \( Y \in \text{Gr}(r_2, \mathbb{F}_{q^m}) \) and \( Z \in \text{Gr}(r_3, \mathbb{F}_{q^m}) \) such that \( X \cap Y = 0 \) and \( Z \cap Y = 0 \). Given \( a = x + y \) and \( b = y + z \) such that \( x \in X^k \), \( y \in Y^k \), \( z \in Z^k \), \( r_1 + r_2 < m \), \( r_2 + r_3 < m \) and \( r_1 + r_2 + r_3 \geq m \). The RVD\(_{a,b} \) problem is to determine the unique pair \((Y, y)\) such that \( a = x + y \) and \( b = y + z \).

Given \( z_1 h = y_1 e_2 + c u_1 e_2 \) and \( cs = c u_1 e_2 + c u_2 e_1 \).
We define a new problem:

**Problem (Rank Vector Decomposition (RVD) Problem)**

Let $X \in \text{Gr}(r_1, \mathbb{F}_{q^m})$, $Y \in \text{Gr}(r_2, \mathbb{F}_{q^m})$ and $Z \in \text{Gr}(r_3, \mathbb{F}_{q^m})$ such that $X \cap Y = 0$ and $Z \cap Y = 0$. Given $a = x + y$ and $b = y + z$ such that $x \in X^k$, $y \in Y^k$, $z \in Z^k$, $r_1 + r_2 < m$, $r_2 + r_3 < m$ and $r_1 + r_2 + r_3 \geq m$. The RVD$_{a,b}$ problem is to determine the unique pair $(Y, y)$ such that $a = x + y$ and $b = y + z$.

Given $z_1 h = y_1 e_2 + cu_1 e_2$ and $cs = cu_1 e_2 + cu_2 e_1$.

**Aim:** Let $v = y_1 e_2$, $w = cu_1 e_2$ and $t = cu_2 e_1$. Then we have $a = v + w$ and $b = w + t$. 
We define a new problem:

**Problem (Rank Vector Decomposition (RVD) Problem)**

Let $X \in \text{Gr}(r_1, \mathbb{F}_{q^m})$, $Y \in \text{Gr}(r_2, \mathbb{F}_{q^m})$ and $Z \in \text{Gr}(r_3, \mathbb{F}_{q^m})$ such that $X \cap Y = 0$ and $Z \cap Y = 0$. Given $a = x + y$ and $b = y + z$ such that $x \in X^k$, $y \in Y^k$, $z \in Z^k$, $r_1 + r_2 < m$, $r_2 + r_3 < m$ and $r_1 + r_2 + r_3 \geq m$. The RVD$_{a,b}$ problem is to determine the unique pair $(Y, y)$ such that $a = x + y$ and $b = y + z$.

Given $z_1 h = y_1 e_2 + cu_1 e_2$ and $cs = cu_1 e_2 + cu_2 e_1$.

**Aim:** Let $v = y_1 e_2$, $w = cu_1 e_2$ and $t = cu_2 e_1$. Then we have $a = v + w$ and $b = w + t$. Determine $w$ so that the above holds.
We define a new problem:

**Problem (Rank Vector Decomposition (RVD) Problem)**

Let \( X \in \text{Gr}(r_1, \mathbb{F}_{q^m}) \), \( Y \in \text{Gr}(r_2, \mathbb{F}_{q^m}) \) and \( Z \in \text{Gr}(r_3, \mathbb{F}_{q^m}) \) such that \( X \cap Y = \emptyset \) and \( Z \cap Y = \emptyset \). Given \( a = x + y \) and \( b = y + z \) such that \( x \in X^k \), \( y \in Y^k \), \( z \in Z^k \), \( r_1 + r_2 < m \), \( r_2 + r_3 < m \) and \( r_1 + r_2 + r_3 \geq m \). The RVD\(_{a,b}\) problem is to determine the unique pair \((Y, y)\) such that \( a = x + y \) and \( b = y + z \).

Given \( z_1 h = y_1 e_2 + cu_1 e_2 \) and \( cs = cu_1 e_2 + cu_2 e_1 \).

Aim: Let \( v = y_1 e_2 \), \( w = cu_1 e_2 \) and \( t = cu_2 e_1 \). Then we have \( a = v + w \) and \( b = w + t \). Determine \( w \) so that the above holds.

Our best solving complexity to solve RVD\(_{a,b}(q, m, k, r_1, r_2, r_3)\) is

\[
O \left( (\min\{r_1, r_3\} + r_2)^3 k^3 q^{r_2(r_1+r_2+r_3-m)} \right).
\]
Parameters for RPS Signature

Keygen: \( pk = (h) \) and \( sk = (e_1, e_2) \)

Sign: \( \sigma = (c, s, z_1, z_2) \)

<table>
<thead>
<tr>
<th>Schemes</th>
<th>size pk</th>
<th>size sk</th>
<th>size ( \sigma )</th>
<th>Sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPS-C1</td>
<td>443 B</td>
<td>74 B</td>
<td>4.027 KB</td>
<td>128</td>
</tr>
<tr>
<td>RPS-C2</td>
<td>494 B</td>
<td>79 B</td>
<td>5.993 KB</td>
<td>192</td>
</tr>
<tr>
<td>MURAVE-1</td>
<td>5.33 KB</td>
<td>1.24 KB</td>
<td>9.69 KB</td>
<td>128</td>
</tr>
<tr>
<td>Durandal-I</td>
<td>15.25 KB</td>
<td>2.565 KB</td>
<td>4.06 KB</td>
<td>128</td>
</tr>
<tr>
<td>cRVDC</td>
<td>0.152 KB</td>
<td>0.151 KB</td>
<td>22.48 KB</td>
<td>125</td>
</tr>
<tr>
<td>CVE</td>
<td>7.638 KB</td>
<td>0.210 KB</td>
<td>436.6 KB</td>
<td>80</td>
</tr>
</tbody>
</table>
Parameters for RPS Signature

Keygen: \( pk = (h) \) and \( sk = (e_1, e_2) \)

Sign: \( \sigma = (c, s, z_1, z_2) \)

We consider \( q = 2, \, r_{e_1} = r_{e_2}, \, r_{y_1} = r_{u_2} \) and \( r_{y_2} = r_{u_1} \).

Table: Parameters and Comparisons with Other Rank-based Signatures

<table>
<thead>
<tr>
<th>Schemes</th>
<th>size_{pk}</th>
<th>size_{sk}</th>
<th>size_{\sigma}</th>
<th>Sec_{CL}</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPS-C1</td>
<td>443 B</td>
<td>74 B</td>
<td>4.027 KB</td>
<td>128</td>
</tr>
<tr>
<td>RPS-C2</td>
<td>494 B</td>
<td>79 B</td>
<td>5.993 KB</td>
<td>192</td>
</tr>
<tr>
<td>MURAVE-1</td>
<td></td>
<td></td>
<td>5.33 KB</td>
<td>128</td>
</tr>
<tr>
<td>Durandal-I</td>
<td></td>
<td></td>
<td>15.25 KB</td>
<td>128</td>
</tr>
<tr>
<td>cRVDC</td>
<td></td>
<td></td>
<td>0.152 KB</td>
<td>125</td>
</tr>
<tr>
<td>CVE</td>
<td></td>
<td></td>
<td>7.638 KB</td>
<td>80</td>
</tr>
</tbody>
</table>
Parameters for RPS Signature

Keygen: \( pk = (h) \) and \( sk = (e_1, e_2) \)  
Sign: \( \sigma = (c, s, z_1, z_2) \)

We consider \( q = 2, \ r_{e_1} = r_{e_2}, \ r_{y_1} = r_{u_2} \) and \( r_{y_2} = r_{u_1} \).

Table: Parameters and Comparisons with Other Rank-based Signatures

<table>
<thead>
<tr>
<th>Schemes</th>
<th>size(_{pk})</th>
<th>size(_{sk})</th>
<th>size(_{\sigma})</th>
<th>Sec(_{CL})</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPS-C1</td>
<td>443 B</td>
<td>74 B</td>
<td>4.027 KB</td>
<td>128</td>
</tr>
<tr>
<td>RPS-C2</td>
<td>494 B</td>
<td>79 B</td>
<td>5.993 KB</td>
<td>192</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Schemes</th>
<th>size(_{pk})</th>
<th>size(_{sk})</th>
<th>size(_{\sigma})</th>
<th>Sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPS-C1</td>
<td>0.443 KB</td>
<td>0.074 KB</td>
<td>4.027 KB</td>
<td>128</td>
</tr>
<tr>
<td>MURAVE-1</td>
<td>5.33 KB</td>
<td>1.24 KB</td>
<td>9.69 KB</td>
<td>128</td>
</tr>
<tr>
<td>Durandal-I</td>
<td>15.25 KB</td>
<td>2.565 KB</td>
<td>4.06 KB</td>
<td>128</td>
</tr>
<tr>
<td>cRVDC</td>
<td>0.152 KB</td>
<td>0.151 KB</td>
<td>22.48 KB</td>
<td>125</td>
</tr>
<tr>
<td>CVE</td>
<td>7.638 KB</td>
<td>0.210 KB</td>
<td>436.6 KB</td>
<td>80</td>
</tr>
</tbody>
</table>
Summary & Future Work

1. Schnorr Signature in Rank Metric
   - Adaptations and Challenges
Summary & Future Work

1. Schnorr Signature in Rank Metric
   - Adaptations and Challenges

2. RPS Signature Scheme

Security of RPS

New problem: RVD

Performance of RPS

parameters comparison

Future Work

Hardness of RVD (other attacks)?

Applications of RVD in public-key cryptography
Summary & Future Work

1. Schnorr Signature in Rank Metric
   - Adaptations and Challenges

2. RPS Signature Scheme

3. Security of RPS
   - Security Analysis
   - New problem: RVD

Future Work

- Hardness of RVD (other attacks)?
- Applications of RVD in public-key cryptography
Summary & Future Work

1. Schnorr Signature in Rank Metric
   - Adaptations and Challenges

2. RPS Signature Scheme

3. Security of RPS
   - Security Analysis
   - New problem: RVD

4. Performance of RPS
   - parameters comparison
Summary & Future Work

1. Schnorr Signature in Rank Metric
   - Adaptations and Challenges

2. RPS Signature Scheme

3. Security of RPS
   - Security Analysis
   - New problem: RVD

4. Performance of RPS
   - Parameters comparison

5. Future Work
   - Hardness of RVD (other attacks)?
   - Applications of RVD in public-key cryptography
Question?

Please contact us at
tsltlsc@nus.edu.sg
tsltch@nus.edu.sg