4th ASIA PQC Forum

Indeterminate Equation Public-key Cryptosystem “Giophantus™”

Koichiro AKIYAMA
TOSHIBA Corporation

Joint work with
Yasuhiro Goto, Shinya Okumura, Tsuyoshi Takagi, Koji Nuida,
Goichiro Hanaoka, Hideo Shimizu, Yasuhiko Ikematsu

2018.06.29
Agenda

1. Design concept
2. Algorithm
3. Computational assumption
4. Cryptanalysis
5. Evaluating at one attack
6. Conclusion
To construct a public-key cryptosystem whose security depends on some non-linear problem.

Giophantus provides new variation of PQC which is located between multivariate & lattice based cryptosystem.
Section Finding Problem

Algebraic Surface Cryptosystem (ASC)

Indeterminate Equation Public-key Cryptosystem - Giophantus - (4th ASIA PQC Forum)

This problem is considered as a Diophantine problems on $F_p[t]$

Algebraic Surface

$X(x, y) = 0$ on $F_p[t]$

Section

$(x, y) = (u_x(t), u_y(t))$

$u_x(t), u_y(t) \in F_p[t]$

Algebraic Surface

public key

Section Finding Problem

Hard

Easy

secret key
Algebraic Surface Cryptosystem (Encryption)

Public-key: Algebraic surface

Message $M$ Embed to poly

Message poly. $m(x, y)$

Random bivariate poly $s(x, y)$

Random bivariate poly $r(x, y)$

Randomize (Add/Mult)

Same form

Same form

Same form

Same form

High speed encryption

$F_p[t]$ calculation

Cipher text

\[ c(x, y) = m(x, y)s(x, y) + X(x, y)r(x, y) \]
Algebraic Surface Cryptosystem (Decryption)

Cipher text

\[ c(x, y) = m(x, y)s(x, y) + X(x, y)r(x, y) \]

Secret key: section

\[ D: (x, y, t) = (u_x(t), u_y(t)) \]

Section substitution

\[ m(u_x(t), u_y(t))s(u_x(t), u_y(t)) \]

Factoring (univariate poly.)

Message poly.

\[ m(u_x(t), u_y(t)) \]

Solving linear equations

Message \( M \)
History & Progression of ASC

\[ c = m + Xr \]

multiple structure \[ c = m(t) + Xr(t) \]

3 variables \[ c = m(t) + Xr(t) + \ell \cdot e \]

noise addition

Eliminate mult. structure (noise added structure)
Small Solution Problem

The “small” solution $u_x(t), u_y(t)$ has coefficients are in the range of 0 to $\ell - 1$, where $\ell$ is small enough to $q$.

**Indeterminate Equation**

$X(x, y) = 0$ on $F_q[t]/(t^n - 1)$

**Small Solution**

$(x, y) = (u_x(t), u_y(t))$

$u_x(t), u_y(t) \in F_q[t]/(t^n - 1)$

**Section Finding Problem**

**Algebraic Surface**

$X(x, y) = 0$ on $F_p[t]$
Encryption/Decryption

Public key: Indeterminate Eq.

\[ R_q = F_q[t] / (t^n - 1) \]

\( \ell \): small integer

\[ X(x, y) = 0 \]

Message poly. \( m(t) \) (with small coefficients)

Embed to coeff.

Random bivariate poly. \( r(x, y) \)

Noise bivariate poly. (with small coefficients) \( e(x, y) \)

Encryption

\[ c(x, y) = m(t) + X(x, y)r(x, y) + \ell \cdot e(x, y) \]

Substitute

\[ m(t) + \ell \cdot e(u_x(t), u_y(t)) \]

Decryption

\[ R_q \mod \ell \]

Recover \( m(t) \)

\[ m(t) \]

Same Form

Secret key: Small Solution

\[ D : (x, y) = (u_x(t), u_y(t)) \]

Indeterminate Equation Public-key Cryptosystem - Giophantus - (4th ASIA PQC Forum)}

© 2014 Toshiba Corporation
\[ F_q[t] / (t^n - 1) \text{ calculation} \]

\[ (2t^2 + 3t + 4)(at^2 + bt + c) = dt^2 + et + f \]

\[ t^3 \equiv 1 \]

\[ (2t^2 + 3t + 4)at^2 = 2at^4 + 3at^3 + 4at^2 \]
\[ = 4at^2 + 2at + 3a \]

\[ (2t^2 + 3t + 4)bt = 2bt^3 + 3bt^2 + 4bt \]
\[ = 3bt^2 + 4bt + 2b \]

\[ (2t^2 + 3t + 4)c = 2ct^2 + 3ct + 4c \]

Matrix expression
\[
\begin{pmatrix}
4 & 3 & 2 \\
2 & 4 & 3 \\
3 & 2 & 4
\end{pmatrix}
\begin{pmatrix}
a \\
b \\
c
\end{pmatrix}
= \begin{pmatrix}
4a + 3b + 2c \\
2a + 4b + 3c \\
3a + 2b + 4c
\end{pmatrix}
t^2
t
t}
IE-LWE Problem/Assumption

\[ X \text{ : Irreducible polynomial with small zero point} \]
\[ Y \text{ : random bivariate polynomial} \]

Decision problem between the distribution \( (X, Xr + e) \) and the distribution \( (X, Y) \) called IE-LWE problem & assumption.

<table>
<thead>
<tr>
<th>Attack</th>
<th>Method</th>
<th>Infulluence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linear Algebra Attack (LAA)</td>
<td>( Z = Xr + e )</td>
<td>( \odot )</td>
</tr>
<tr>
<td>Key Recovery Attack (KRA)</td>
<td>( X(x, y) = 0 )</td>
<td>( \odot )</td>
</tr>
</tbody>
</table>

The lattice reduction technique can be applied to these attacks since these goals are common in finding small solutions.
Linear Algebra Attack (LAA)

\[ \sum_{(i,j) \in \Gamma_e} d_{ij} x^i y^j = \left( \sum_{(i,j) \in \Gamma_X} a_{ij} x^i y^j \right) \left( \sum_{(i,j) \in \Gamma_r} r_{ij} x^i y^j \right) + \sum_{(i,j) \in \Gamma_e} e_{ij} x^i y^j \quad \text{on } F_q[t] / (t^n - 1) \]

\[ \text{deg}_{xy} X = \text{deg}_{xy} r = 1 \]

\[ X(x, y) = a_{10} x + a_{01} y + a_{00} \]
\[ r(x, y) = r_{10} x + r_{01} y + r_{00} \]
\[ e(x, y) = e_{20} x^2 + e_{11} xy + e_{02} y^2 + e_{10} x + e_{01} y + e_{00} \]
\[ Z(x, y) = d_{20} x^2 + d_{11} xy + d_{02} y^2 + d_{10} x + d_{01} y + d_{00} \]

\[ \begin{align*}
    a_{10} r_{10} + e_{20} &= d_{20} \\
    a_{10} r_{01} + a_{01} r_{10} + e_{11} &= d_{11} \\
    a_{01} r_{10} + e_{02} &= d_{02} \\
    a_{10} r_{00} + a_{00} r_{10} + e_{10} &= d_{10} \\
    a_{01} r_{00} + a_{00} r_{01} + e_{01} &= d_{01} \\
    a_{00} r_{00} + e_{00} &= d_{00}
\end{align*} \]

Substitute & Compare

as \( F_q[t] / (t^n - 1) \)
LAA against IE-LWE (single term)

\[ a_{10}r_{10} + e_{20} = d_{20} \quad \text{on} \quad F_q[t]/(t^n - 1) \]

\[ a_{10}r_{10} + e_{20} + qu_{20} = d_{20} \quad \text{on} \quad \mathbb{Z}[t]/(t^n - 1) \]

Integerization

Linear Equation

\[
\begin{pmatrix}
A_{10} & I_n & qI_n
\end{pmatrix}
\begin{pmatrix}
r_{10} \\
e_{20} \\u_{20}
\end{pmatrix} =
\begin{pmatrix}
d_{20}
\end{pmatrix} \quad \text{on} \quad \mathbb{Z}
\]

Element of the \( e_{20} \) is small
LAA against IE-LWE (all terms)

If we consider the all equations

\[
\begin{pmatrix}
A_{10} & I_n & qI_n \\
A_{01} & A_{10} & I_n & qI_n \\
A_{00} & A_{10} & I_n & qI_n \\
A_{00} & A_{01} & I_n & qI_n \\
A_{00} & A_{00} & I_n & qI_n
\end{pmatrix}
= \begin{pmatrix}
\vdots \\
\vdots \\
\vdots \\
\vdots \\
\vdots \\
\end{pmatrix}
\begin{pmatrix}
r_{10} \\
r_{01} \\
r_{00} \\
e_{20} \\
e_{11} \\
e_{02} \\
e_{01} \\
e_{00} \\
u_{20} \\
u_{11} \\
u_{02} \\
u_{01} \\
u_{00}
\end{pmatrix}
\]

\[\mathcal{L}_{LAA}\]

where element of the \( e_{ij} \) is small

\[\text{rank}(\mathcal{L}_{LAA}) = 6n\]
Attack Improvement (by Xagawa)

\[ X(x, y) = a_{10}x + a_{01}y + a_{00} \]
\[ r(x, y) = r_{10}x + r_{01}y + r_{00} \]
\[ e(x, y) = e_{20}x^2 + e_{11}xy + e_{02}y^2 + e_{10}x + e_{01}y + e_{00} \]
\[ Z(x, y) = d_{20}x^2 + d_{11}xy + d_{02}y^2 + d_{10}x + d_{01}y + d_{00} \]

Substitute \( y = 0 \)

\[ X(x, 0) = a_{10}x + a_{00} \]
\[ r(x, 0) = r_{10}x + r_{00} \]
\[ e(x, 0) = e_{20}x^2 + e_{10}x + e_{00} \]
\[ Z(x, 0) = d_{20}x^2 + d_{10}x + d_{00} \]

\[
\begin{align*}
\text{rank}(\mathcal{L}_{LAA}') &= 3n \\
\end{align*}
\]
Key Recovery Attack  

Linear case

Small solution problem of Indeterminate. Eq.

Indeterminate Eq.  

\[ X(x, y) = 0 \]

Hard ★ Easy

Secret key

Public key

Small solution  

\[ (x, y) = (u_x(t), u_y(t)) \]

Polynomials with small coefficients

Linear Ind. Eq.

\[ X(x, y) = c_{10}x + c_{01}y + c_{00} = 0 \]

\[ R_q = F_q[t]/(t^n - 1) \]

Convert to  

\[ \mathbb{Z}[t]/(t^n - 1) \]

\[ c_{01}u_x + c_{10}u_y + qu = -c_{00} \]

Coefficient comparison

\[
\begin{pmatrix}
  u_x \\
  u_y \\
  u
\end{pmatrix}
\begin{pmatrix}
  C_{01} & C_{10} & qI
\end{pmatrix}
\begin{pmatrix}
  u_x \\
  u_y \\
  u
\end{pmatrix}
= -\begin{pmatrix}
  c_{00}
\end{pmatrix}
\]

\[ \mathcal{L}_{KRA} \]

Find a small solution  

\[ (\bar{u}_x, \bar{u}_y, \bar{u})^T \]
How to find a small solution

\[ \mathcal{L}_{KRA} \begin{pmatrix} u_x \\ u_y \\ u \end{pmatrix} = - (c_{00}) \]

Find \( \vec{v} \)

Generalize \( \vec{v} \pm \vec{w} \)

General solution

\[ \mathcal{L}_{KRA} (\vec{v} \pm \vec{w}) = -(c_{00}) \]

Shortest Vector problem: To find a small \( \vec{v} \pm \vec{w} \)

Closest Vector Problem: To find the closest \( \vec{w} \) to \( \vec{v} \)
Embedding Technique

Hermite normal form

\[ \mathcal{L}_{KRA} = \begin{pmatrix} I_n & B & C \\ O & qI_n & D \end{pmatrix} \]

\[ \mathcal{L}_{KRA} \begin{pmatrix} \vec{w}_x \\ \vec{w}_y \\ \vec{w}_c \end{pmatrix} = \begin{pmatrix} \vec{0} \end{pmatrix} \]

\( \mathcal{L}_{KRA} \) correspond to

\[ \mathcal{L}^+_K = \begin{pmatrix} I & B & \vec{0}^T \\ O & qI & \vec{0}^T \end{pmatrix} \begin{pmatrix} \vec{v}_x \\ \vec{v}_y \end{pmatrix} = \begin{pmatrix} \mu \end{pmatrix} \]

CVP

Embedding Technique

\( \text{rank}(\mathcal{L}'_{KRA}) = 2n \)

SVP

\( \text{rank}(\mathcal{L}^+_{KRA}) = 2n + 1 \)

A solution of

\[ \mathcal{L}_{KRA} \begin{pmatrix} \vec{v}_x \\ \vec{v}_y \\ \vec{v}_c \end{pmatrix} = -\begin{pmatrix} c_{00} \end{pmatrix} \]

\( B, C, D \) Cyclic matrix

small integer
### Experimental results (LLL)

<table>
<thead>
<tr>
<th>n</th>
<th>q</th>
<th>rank</th>
<th>Norm1</th>
<th>Norm2</th>
<th>Gap</th>
<th>Norm1</th>
<th>result</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>33149</td>
<td>21</td>
<td>8</td>
<td>186</td>
<td>22</td>
<td>204</td>
<td>Success</td>
<td>0.02</td>
</tr>
<tr>
<td>20</td>
<td>131059</td>
<td>41</td>
<td>12</td>
<td>619</td>
<td>50</td>
<td>633</td>
<td>Success</td>
<td>0.09</td>
</tr>
<tr>
<td>30</td>
<td>293791</td>
<td>61</td>
<td>15</td>
<td>1416</td>
<td>97</td>
<td>1619</td>
<td>Success</td>
<td>0.26</td>
</tr>
<tr>
<td>40</td>
<td>521299</td>
<td>81</td>
<td>17</td>
<td>3236</td>
<td>191</td>
<td>3325</td>
<td>Success</td>
<td>0.76</td>
</tr>
<tr>
<td>50</td>
<td>813623</td>
<td>101</td>
<td>19</td>
<td>6013</td>
<td>315</td>
<td>6581</td>
<td>Success</td>
<td>1.77</td>
</tr>
<tr>
<td>60</td>
<td>1170751</td>
<td>121</td>
<td>21</td>
<td>11444</td>
<td>552</td>
<td>11738</td>
<td>Success</td>
<td>3.52</td>
</tr>
<tr>
<td>70</td>
<td>1592659</td>
<td>141</td>
<td>22</td>
<td>20796</td>
<td>943</td>
<td>20589</td>
<td>Success</td>
<td>6.45</td>
</tr>
<tr>
<td>80</td>
<td>2079401</td>
<td>161</td>
<td>24</td>
<td>37181</td>
<td>1563</td>
<td>37601</td>
<td>Success</td>
<td>10.74</td>
</tr>
<tr>
<td>90</td>
<td>2630917</td>
<td>181</td>
<td>25</td>
<td>66292</td>
<td>2641</td>
<td>65551</td>
<td>Success</td>
<td>57.79</td>
</tr>
<tr>
<td>100</td>
<td>3247243</td>
<td>201</td>
<td>27</td>
<td>106864</td>
<td>4026</td>
<td>110512</td>
<td>Success</td>
<td>318.16</td>
</tr>
<tr>
<td>110</td>
<td>3928361</td>
<td>221</td>
<td>28</td>
<td>186219</td>
<td>6724</td>
<td>201748</td>
<td>Success</td>
<td>788.46</td>
</tr>
<tr>
<td>120</td>
<td>4674289</td>
<td>241</td>
<td>29</td>
<td>307382</td>
<td>10474</td>
<td>313401</td>
<td>Success</td>
<td>1361.19</td>
</tr>
<tr>
<td>130</td>
<td>5484979</td>
<td>261</td>
<td>373397</td>
<td>574752</td>
<td>2</td>
<td>542968</td>
<td>Failure</td>
<td>2315.24</td>
</tr>
</tbody>
</table>

The norm of 1\textsuperscript{st} basis vector
The norm of 2\textsuperscript{nd} basis vector

Gap = Norm2 / Norm1

By Bai-Galbraith

\[ \left( \begin{array}{cc} I_n & A \\ O & qI_n \end{array} \right) \]

\[ \| \lambda_2(\mathcal{L}^+_{KRA}) \| \approx GH(\mathcal{L}'_{KRA}) \]

shortest vector
Experimental result (BKZ)

• We carried out a BKZ experiment by changing block size $\beta$

$$\log_2 || b_i^* ||$$

$$(b_1, b_2, \ldots, b_{2n+1})$$

$i = 2, \ldots, 2n - 1$

Sufficiently reduced basis of $L_{KRA}^+$
Gram-Schmidt orthonormalization

$$\approx$$

(*)Geometric series Assumption

| $\beta$ | slope   | y-int.  | $|| b_2^* || / || b_1^* ||$ | $|| b_2 || / || b_1 ||$ |
|---------|---------|---------|-----------------------------|-----------------------------|
| 10  | -0.0835 | 32.274  | 4320402                     | 4320505                     |
| 20  | -0.0749 | 31.228  | 1783504                     | 1783497                     |
The complexity of BKZ 2016 Estimate

We assume that the complexity for BKZ is as same as the LWE problem with

<table>
<thead>
<tr>
<th>parameters</th>
<th>meaning</th>
<th>Key recovery attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
<td>dimension</td>
<td>$n$</td>
</tr>
<tr>
<td>$m$</td>
<td>Number of samples</td>
<td>$2n$</td>
</tr>
<tr>
<td>$q$</td>
<td>modulus</td>
<td>$\sim 324n^2 + 72n + 15$</td>
</tr>
<tr>
<td>$\sigma$</td>
<td>standard deviation</td>
<td>1.12</td>
</tr>
</tbody>
</table>

Estimation for the root of Hermite factor for SVP

$$\delta_0 = (((\pi \beta)^{1/\beta} \beta / (2 \pi e))^{1/2(\beta - 1)})$$

2016 Estimate

$$\sqrt{\beta / (2n) \lambda_1 (\mathcal{L}_{KRA}^+)} \geq \delta_0^{2\beta - 2n} (\det \mathcal{L}_{KRA}^+)^{1/2n}$$

( where $\lambda_1 (\mathcal{L}_{KRA}^+) = \sqrt{5n / 2}$ holds )

Find a pair $(n, \beta)$ satisfied both conditions

Time complexity $8 \cdot 2n \cdot 2^{0.292\beta + 12.31}$
Parameter & Performance

In linear case, namely $\deg X(x,y)=1$, we choose the parameter $n$ by cryptanalysis based on the “2016 estimate”.

\[
\ell = 4
\]

<table>
<thead>
<tr>
<th>$k$</th>
<th>$n$</th>
<th>$q$</th>
<th>Public Key(KB)</th>
<th>Secret Key(KB)</th>
<th>Cipher Text(KB)</th>
<th>Key Gen (Mcycle)</th>
<th>Encrypt (Mcycle)</th>
<th>Decrypt (Mcycle)</th>
</tr>
</thead>
<tbody>
<tr>
<td>135</td>
<td>1201</td>
<td>467424413</td>
<td>15</td>
<td>0.6</td>
<td>29</td>
<td>93</td>
<td>179</td>
<td>336</td>
</tr>
<tr>
<td>196</td>
<td>1733</td>
<td>973190461</td>
<td>21</td>
<td>0.9</td>
<td>42</td>
<td>161</td>
<td>379</td>
<td>717</td>
</tr>
<tr>
<td>259</td>
<td>2267</td>
<td>1665292879</td>
<td>28</td>
<td>1.2</td>
<td>55</td>
<td>240</td>
<td>627</td>
<td>1187</td>
</tr>
</tbody>
</table>

$q$ is a prime next to

\[
\ell - 1 + \ell (\ell - 1) + 2 \ell (\ell - 1)^2 n + 3 \ell (\ell - 1)^3 n^2
\]

prime prime Small

High speed

CPU : Xeon E5-1620 3.6GHz
OS : Windows 7, 64bit
Memory : 32GB
Evaluating at one attack

---

**Decryption**

\[ c(x, y, t) = m(t) + X(x, y, t)r(x, y, t) + \ell \cdot e(x, y, t) \]

small solution

\[ X(x, y, t) = 0 \]

\[ (u_x(t), u_y(t)) = \left( \sum_{i=0}^{n-1} a_i t^i, \sum_{i=0}^{n-1} b_i t^i \right) \]

\[ 0 \leq a_i, b_i < \ell - 1 \]

\[ c(u_x(t), u_y(t), t) = m(t) + \ell \cdot e(u_x(t), u_y(t), t) \]

\[ \mathbb{Z}[t] \]

\[ c(u_x(t), u_y(t), t) \mod \ell = m(t) \]

---

**Attack**

\[ c(x, y, 1) = m(1) + X(x, y, 1)r(x, y, 1) + \ell \cdot e(x, y, 1) \]

small solution

\[ X(x, y, 1) = 0 \]

exhaustive search

\[ (s_x, s_y) = \]

\[ (u_x(1), u_y(1)) = \left( \sum_{i=0}^{n-1} a_i, \sum_{i=0}^{n-1} b_i \right) \]

\[ 0 \leq s_x, s_y < n(\ell - 1) \]

\[ c(s_x, s_y, 1) = m(1) + \ell \cdot e(s_x, s_y, 1) \]

\[ \mathbb{Z}[t] \]

\[ c(s_x, s_y, 1) \mod \ell = m(1) \mod \ell \]

---

Ward Beullens, Wouter Castryck and Frederik Vercauteren consider this relation leads to breaking IND-CPA.
But the attack does not always work. Because,

\[ c(s_x, s_y, 1) = m(1) + \ell \cdot e(s_x, s_y, 1) \]

\[ c(s_x, s_y, 1) \mod \ell = m(1) \mod \ell \]

\[ c(u_x(t), u_y(t), t) = m(t) + \ell \cdot e(u_x(t), u_y(t), t) \]

\[ c(u_x(t), u_y(t), t) \mod \ell = m(t) \]

\[ q \] must be larger than

\[ (\ell - 1)n + 2(\ell - 1)^2 n^2 + 3(\ell - 1)^3 n^3 \]

\[ q \] is a prime next to

\[ \ell - 1 + \ell(\ell - 1) + 2\ell(\ell - 1)^2 n + 3\ell(\ell - 1)^3 n^2 \]

in appropriate parameters

<table>
<thead>
<tr>
<th>n</th>
<th>The minimum required q</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>scheme</td>
</tr>
<tr>
<td>1201</td>
<td>467424413</td>
</tr>
<tr>
<td>1733</td>
<td>973190461</td>
</tr>
<tr>
<td>2267</td>
<td>1665292879</td>
</tr>
</tbody>
</table>

\[ c(s_x, s_y, 1) \mod \ell = m(1) \mod \ell \]

is not always satisfied!
Experimental Result  (parameter using fixed q)

However, we fix the parameter $q = 2^{31} - 1$ for optimal implementation.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$c(s_x, s_y, 1) \mod \ell$</th>
<th>Distinguishing Advantage(*)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1201</td>
<td>703</td>
<td>1167</td>
</tr>
<tr>
<td>1733</td>
<td>36852</td>
<td>28222</td>
</tr>
<tr>
<td>2267</td>
<td>24747</td>
<td>25522</td>
</tr>
</tbody>
</table>

$Distinguishing Advantage = \text{Pr(2 most likely value)} - \text{Pr(2 least likely value)}$

Here we set $m(1) \mod \ell = 1$

**Random**

<table>
<thead>
<tr>
<th>$c(s_x, s_y, 1) \mod \ell$</th>
<th>Distinguishing Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>24844</td>
<td>24900</td>
</tr>
<tr>
<td>25038</td>
<td>24946</td>
</tr>
<tr>
<td>25094</td>
<td>25056</td>
</tr>
</tbody>
</table>

Evaluating at one attack almost works the scheme with parameter used in optimal implementation.


Experimental Result (appropriate parameter)

For appropriate parameter, we employ minimum q which leads non-error decryption.

<table>
<thead>
<tr>
<th>n</th>
<th>q</th>
<th>( c(s_x, s_y, l) \mod \ell )</th>
<th>Distinguishing Advantage(*)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0 1 2 3</td>
<td></td>
</tr>
<tr>
<td>1201</td>
<td>467424413</td>
<td>24769 25113 25559 24559</td>
<td>0.01344</td>
</tr>
<tr>
<td>1733</td>
<td>973190461</td>
<td>25136 25035 25008 24821</td>
<td>0.00342</td>
</tr>
<tr>
<td>2267</td>
<td>1665292879</td>
<td>25117 24791 25021 25071</td>
<td>0.00376</td>
</tr>
</tbody>
</table>

Random

<table>
<thead>
<tr>
<th>( c(s_x, s_y, l) \mod \ell )</th>
<th>Distinguishing Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 3</td>
<td></td>
</tr>
<tr>
<td>24873 24922 25144 25061</td>
<td>0.0041</td>
</tr>
<tr>
<td>24883 24945 25032 25140</td>
<td>0.00344</td>
</tr>
<tr>
<td>25121 25114 24970 24795</td>
<td>0.0047</td>
</tr>
</tbody>
</table>

The distinguishability strongly depends on the public key. We need to consider about how to detect weak keys.
Conclusion

- We proposed a new variant of PQC called “Giophantus” which is located between Multivariate and Lattice based.

- We found the secure parameters by 2016 estimate.

- Giophantus requires short secret key in size and short process time.

- Evaluate at one Attack does not always work on Giophantus.
  - parameter used for optimization: almost works
  - appropriate parameter: depends on the public-key