Practical Cryptanalysis of a Public-key Encryption Scheme Based on Non-linear Indeterminate Equations at SAC 2017

Keita Xagawa (草川　恵太)

NTT Secure Platform Laboratories

2018/04/09

Agenda

Post-Quatnum Crypgraphy

IEC/Giophantus as Lattice-based PKE

Attack against IEC with $n = 80$

Attack against IEC with prime n

Summary

NIST PQC Round 1 Candidates

We have 69 candidates on 21 Dec. 2017.

Code, Lattice, MQ, Isogeny, SymKey, Others

PKE/KEM 49: BIG QUAKE, BIKE, CFPKM, Classic McEliece, Compact LWE, CRYSTALS-Kyber, DAGS, Ding Key Exchange, DME, ~~Edon-K~~, EMBLEM and R.EMBLEM, FrodoKEM, Giophantus, GuessAgain, Hila5, ~~HK17~~, HQC, KCL, KINDI, LAC, LAKE, LEDAkem, LEDApkc, Lepton, Lima, Lizard, LOCKER, LOTUS, McNie, Mersenne-756839, NewHope, NTRUEncrypt, NTRU-HRSS-KEM, NTRU Prime, NTS-KEM, Odd Manhattan, Ouroboros-R, Post-Quantum RSA-Encryption, QC-MDPC KEM, Ramstake, RLCE-KEM, Round2, RQC, ~~RVB~~, SABER, SIKE, ~~SRTPI~~, Three Bears, Titanium

Sig. 22: CRYSTALS-Dilithium, DME, DRS, DualModeMS, Falcon, GeMSS, Gravity-SPHINCS, Gui, HiMQ-3, LUOV, MQDSS, pqNTRUsign, Picnic, Post-Quantum RSA-Signature, pqsigRM, qTESLA, RaCoSS, Rainbow, ~~RankSign~~, SPHINCS+, ~~SRTPI~~, WalnutDSA

Summary

IEC/Giophantus proposes CPA/CCA-secure PKE
based on IE-LWE (= a special Module-LWE)

	n	$\deg X$
IEC in Aug. 2017	80	1 or 2
IEC in Sep. 2017	83	1 or 2
Giophantus in Dec. 2017	≥ 1201	1

Summary

IEC/Giophantus proposes CPA/CCA-secure PKE
based on IE-LWE (= a special Module-LWE)

	n	$\deg X$
IEC in Aug. 2017	80	1 or 2
IEC in Sep. 2017	83	1 or 2
Giophantus in Dec. 2017	≥ 1201	1

Akiyama et al. changed parameter values by reflecting our attacks.

- IEC in Aug. 2017
  - Key Recovery in ≈ 30 s $(\deg X = 1)$
  - Distinguishing in ≈ 0.5 s $(\deg X = 1)$
  - Distinguishing in ≈ 30 s $(\deg X = 2)$
- IEC in Sep. 2017
  - Plaintext Recovery in ≈ 17 h $(\deg X = 2)$
  - Distinguishing in ≈ 4 days for large $n \leq 110$ $(\deg X = 2)$

Agenda

Post-Quatnum Crypgraphy

IEC/Giophantus as Lattice-based PKE

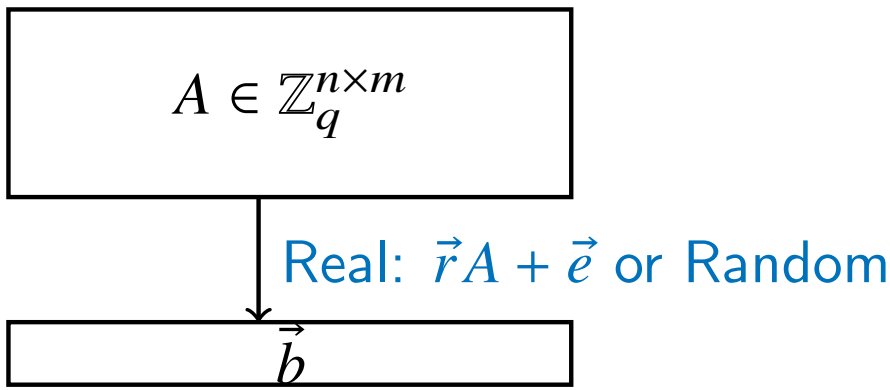
Attack against IEC with $n = 80$

Attack against IEC with prime n

Summary

LWE [Reg09]

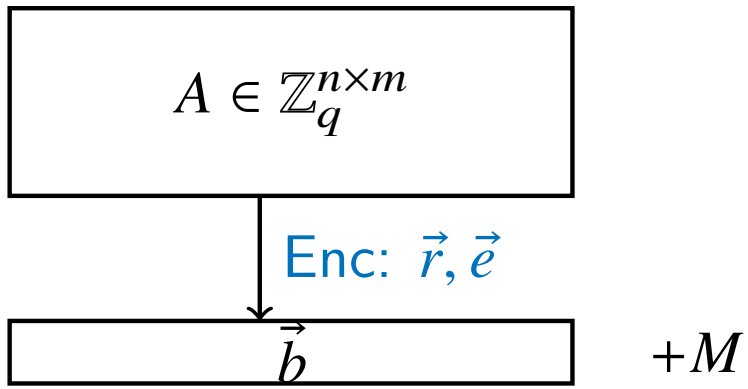
- Learning with Errors (LWE) Problem: Distinguishing
  - $(A, \vec{r}A + \vec{e})$ $(A \leftarrow \mathbb{Z}_q^{n \times m}, \vec{r} \leftarrow \mathbb{Z}_q^n, \vec{e} \leftarrow \chi^m)$
  - $(A, \vec{b})$ $(A \leftarrow \mathbb{Z}_q^{n \times m}, \vec{b} \leftarrow \mathbb{Z}_q^m)$



Example of χ: Discrete Gaussian

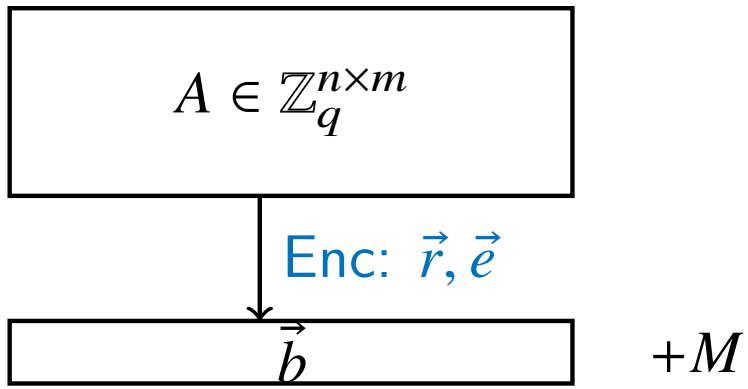
GPV-like PKE [GPV08]

ek $= A$, dk $= \vec{u}$ with $A \cdot \vec{u} = 0$, $\|\vec{u}\| \leq B$, and $u_0 = 1$
ct $= \vec{b} = \vec{r}A + p\vec{e} + (M, 0, \ldots, 0)$ with $\|\vec{e}\| \leq B$



GPV-like PKE [GPV08]

ek $= A$, dk $= \vec{u}$ with $A \cdot \vec{u} = 0$, $\|\vec{u}\| \leq B$, and $u_0 = 1$
ct $= \vec{b} = \vec{r}A + p\vec{e} + (M, 0, \ldots, 0)$ with $\|\vec{e}\| \leq B$

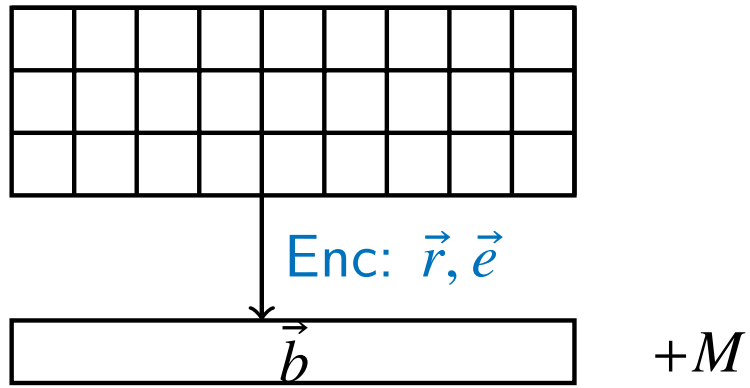


$$\begin{aligned}\vec{b} \cdot \vec{u}^\top &= M + (\vec{r}A + p\vec{e}) \cdot \vec{u}^\top \\ &= M + p\vec{e} \cdot \vec{u}^\top \ (\text{in } \mathbb{Z} \text{ if } p(1 + B^2) < q/2)\end{aligned}$$

Thus, $M := (\vec{b} \cdot \vec{u}^\top \bmod^* q) \bmod p$

Module-LWE-based GPV-like PKE

$A \in \mathbb{Z}_q^{hn \times wn}$ is made from $a_{1,1}, \ldots, a_{h,w} \in \mathbb{Z}_q[t]/(t^n + 1)$
ek $= A$, dk $= \vec{u}$ with $A \cdot \vec{u} = 0$, $\|\vec{u}\| \leq B$, and $u_0 = 1$
ct $= \vec{b} = \vec{r}A + p\vec{e} + (M, 0, \ldots, 0)$ with $\|\vec{e}\| \leq B$

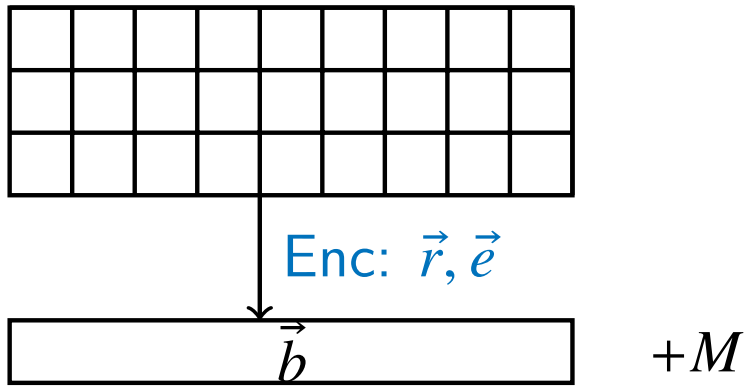


$$\begin{aligned} \vec{b} \cdot \vec{u}^\top &= M + (\vec{r}A + p\vec{e}) \cdot \vec{u}^\top \\ &= M + p\vec{e} \cdot \vec{u}^\top \ (\text{in } \mathbb{Z}) \end{aligned}$$

Thus, $M := (\vec{b} \cdot \vec{u}^\top \bmod^* q) \bmod p$

IEC/Giophantus

$A \in \mathbb{Z}_q^{hn \times wn}$ is made from few $a_{1,1}, \ldots, a_{h,w} \in \mathbb{Z}_q[t]/(t^n + 1)$
ek $= A$, dk $= \vec{u}$ with $A \cdot \vec{u} = 0$, $u_i \in [0, p)$, and $u_0 = 1$
ct $= \vec{b} = \vec{r}A + p\vec{e} + (M, 0, \ldots, 0)$ with $e_i \in [0, p)$



$$\begin{aligned} \vec{b} \cdot \vec{u}^\top &= M + (\vec{r}A + p\vec{e}) \cdot \vec{u}^\top \\ &= M + p\vec{e} \cdot \vec{u}^\top \ (\text{in } \mathbb{Z}) \end{aligned}$$

Thus, $M := (\vec{b} \cdot \vec{u}^\top \bmod q) \bmod p$

IEC ($\deg X = 1$)

- Key Generation
  - dk: "Short" $u_x, u_y \in \mathbb{Z}_q[t]/(t^n - 1)$
  - ek: $X(x, y) = a_{10}x + a_{01}y + a_{00}$
  - $a_{10}, a_{01} \leftarrow \mathbb{Z}_q[t]/(t^n - 1)$ and set $a_{00} = -(a_{10}u_x + a_{01}u_y)$
- Encryption: A plaintext is "short" $M \in \mathbb{Z}_q[t]/(t^n - 1)$
  - Choose random $r(x, y) = r_{10}x + r_{01}y + r_{00}$
  - Choose "short" $e(x, y) = e_{20}x^2 + \cdots + e_{00}$
  - A ciphertext is $c(x, y) = M + p \cdot e(x, y) + r(x, y) \cdot X(x, y)$

IEC ($\deg X = 1$)

- Key Generation
  - dk: "Short" $u_x, u_y \in \mathbb{Z}_q[t]/(t^n - 1)$
  - ek: $X(x, y) = a_{10}x + a_{01}y + a_{00}$
  - $a_{10}, a_{01} \leftarrow \mathbb{Z}_q[t]/(t^n - 1)$ and set $a_{00} = -(a_{10}u_x + a_{01}u_y)$
- Encryption: A plaintext is "short" $M \in \mathbb{Z}_q[t]/(t^n - 1)$
  - Choose random $r(x, y) = r_{10}x + r_{01}y + r_{00}$
  - Choose "short" $e(x, y) = e_{20}x^2 + \cdots + e_{00}$
  - A ciphertext is $c(x, y) = M + p \cdot e(x, y) + r(x, y) \cdot X(x, y)$

$$A = \begin{array}{c} \\ 1 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & x & y & x^2 & xy & y^2 \end{array} \\ \begin{pmatrix} A_{00} & A_{10} & A_{01} & & & \\ & A_{00} & & A_{10} & A_{01} & \\ & & A_{00} & & A_{10} & A_{01} \end{pmatrix} \end{array},$$

$$\vec{u} = \begin{array}{c} \\ 1 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & x & y & x^2 & xy & y^2 \end{array} \\ \begin{pmatrix} 1 & u_x & u_y & u_x^2 & u_x u_y & u_y^2 \end{pmatrix} \end{array}$$

PT-Recovery Attack against IEC ($\deg X = 1$)

- ek: $X(x, y) = a_{10}x + a_{01}y + a_{00}$
- ct: $c(x, y) = M + p \cdot e(x, y) + r(x, y) \cdot X(x, y)$

$$A = \begin{array}{c} \\ 1 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & x & y & x^2 & xy & y^2 \end{array} \\ \begin{pmatrix} A_{00} & A_{10} & A_{01} & & & \\ & A_{00} & & A_{10} & A_{01} & \\ & & A_{00} & & A_{10} & A_{01} \end{pmatrix} \end{array} \in \mathbb{Z}_q^{240 \times 480}$$

- Solve a 480-dim. CVP instance $(\Lambda_q(A), \vec{b})$,

$$\Lambda_q(A) = \{\vec{y} \in \mathbb{Z}^{480} \mid \exists \vec{r} \in \mathbb{Z}^{240} : \vec{r} \cdot A \equiv \vec{y}\},$$
$$\vec{b} = \vec{r} \cdot A + (p\vec{e} + (M, 0, \ldots, 0)) \bmod q$$

→ Success if the diff. is $p\vec{e} + (M, 0, \ldots, 0)$

→ But, (experimentally) hard for LLL/BKZ to find the diff.

Agenda

Post-Quatnum Crypgraphy

IEC/Giophantus as Lattice-based PKE

Attack against IEC with $n = 80$

Attack against IEC with prime n

Summary

Gentry's "Origami" Attack [Gen01]

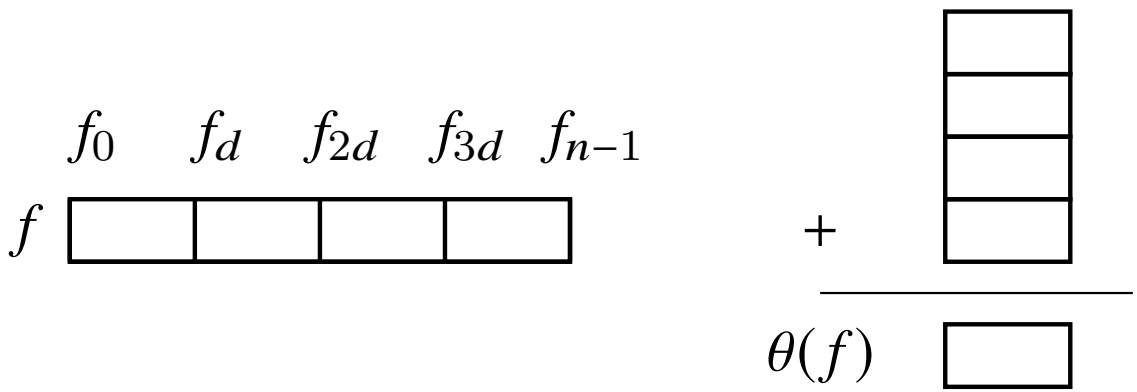
The core of his attack

If $d|n$,

$$\theta : \mathbb{Z}[t]/(t^n-1) \to \mathbb{Z}[t]/(t^d-1) : f = \sum_i f_i t^i \mapsto \sum_{i=0}^{d-1} \left(\sum_{j=0}^{n/d-1} f_{jd+i} \right) t^i$$

is a ring homomorphism.

The dim.: $n \to d$ and the norm: $a \to \leq (n/d)a$.



PT-Recovery Attack on IEC ($\deg X = 1$)

- ek: $X(x, y) = a_{10}x + a_{01}y + a_{00}$
- ct: $c(x, y) = M + p \cdot e(x, y) + r(x, y) \cdot X(x, y)$

$$A = \begin{array}{c} \\ 1 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & x & y & x^2 & xy & y^2 \end{array} \\ \begin{pmatrix} A_{00} & A_{10} & A_{01} & & & \\ & A_{00} & & A_{10} & A_{01} & \\ & & A_{00} & & A_{10} & A_{01} \end{pmatrix} \end{array} \in \mathbb{Z}_q^{240 \times 480}$$

- Solve a 480-dim. CVP instance $(\Lambda_q(A), \vec{b})$,

$$\Lambda_q(A) = \{\vec{y} \in \mathbb{Z}^{480} \mid \exists \vec{r} \in \mathbb{Z}^{240} : \vec{r} \cdot A \equiv \vec{y}\},$$
$$\vec{b} = \vec{r} \cdot A + (p\vec{e} + (M, 0, \ldots, 0)) \bmod q$$

$\rightarrow$ Success if the diff. is $p\vec{e} + (M, 0, \ldots, 0)$

- But, (experimentally) hard for LLL/BKZ to find the diff.

“Origami” Dist. Attack on IEC ($\deg X = 1$)

- ek: $X(x, y) = a_{10}x + a_{01}y + a_{00}$
- ct: $c(x, y) = M + p \cdot e(x, y) + r(x, y) \cdot X(x, y)$

"Origami" Dist. Attack on IEC ($\deg X = 1$)

- ek: $X(x, y) = a_{10}x + a_{01}y + a_{00}$
- ct: $c(x, y) = M + p \cdot e(x, y) + r(x, y) \cdot X(x, y)$
- Let $d = 10$ and apply $\theta : \mathbb{Z}[t]/(t^{80} - 1) \to \mathbb{Z}[t]/(t^{10} - 1)$

$$A' = \begin{array}{c} \\ 1 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & x & y & x^2 & xy & y^2 \end{array} \\ \begin{pmatrix} A'_{00} & A'_{10} & A'_{01} & & & \\ & A'_{00} & & A'_{10} & A'_{01} & \\ & & A'_{00} & & A'_{10} & A'_{01} \end{pmatrix} \end{array} \in \mathbb{Z}_q^{30\times 60}$$

- Solve a 60-dim. CVP instance $(\Lambda_q(A'), \vec{b}')$

$$\Lambda_q(A') = \{\vec{y} \in \mathbb{Z}^{60} \mid \exists \vec{r} \in \mathbb{Z}^{30} : \vec{r} \cdot A' \equiv \vec{y}\},$$

$$\vec{b}' = \vec{r}' \cdot A' + (p\vec{e}' + (M', 0, \ldots, 0)) \bmod q$$

"Origami" Dist. Attack on IEC ($\deg X = 1$)

- ek: $X(x, y) = a_{10}x + a_{01}y + a_{00}$
- ct: $c(x, y) = M + p \cdot e(x, y) + r(x, y) \cdot X(x, y)$
- Let $d = 10$ and apply $\theta : \mathbb{Z}[t]/(t^{80} - 1) \to \mathbb{Z}[t]/(t^{10} - 1)$

$$A' = \begin{array}{c} \\ 1 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & x & y & x^2 & xy & y^2 \end{array} \\ \begin{pmatrix} A'_{00} & A'_{10} & A'_{01} & & & \\ & A'_{00} & & A'_{10} & A'_{01} & \\ & & A'_{00} & & A'_{10} & A'_{01} \end{pmatrix} \end{array} \in \mathbb{Z}_q^{30\times 60}$$

- Solve a 60-dim. CVP instance $(\Lambda_q(A'), \vec{b}')$

$$\Lambda_q(A') = \{\vec{y} \in \mathbb{Z}^{60} \mid \exists \vec{r} \in \mathbb{Z}^{30} : \vec{r} \cdot A' \equiv \vec{y}\},$$
$$\vec{b}' = \vec{r}' \cdot A' + (p\vec{e}' + (M', 0, \ldots, 0)) \bmod q$$

$\to$ We can find the diff. $= p\theta(\vec{e}) + (\theta(M), 0, \ldots, 0)$

- This leaks $\theta(M) \bmod p$!

Demo.

Agenda

Post-Quatnum Crypgraphy

IEC/Giophantus as Lattice-based PKE

Attack against IEC with $n = 80$

Attack against IEC with prime n

Summary

PT-Recovery Attack on IEC ($\deg X = 1$)

- The "origami" attack seems not work if n is prime (Note: Castryck and Vercauteren showed a dist. attack when $d = 1$ and $q = 2^{31} - 1$ for Giophantus)
- Is there another good subring?

PT-Recovery Attack on IEC ($\deg X = 1$)

- The "origami" attack seems not work if n is prime (Note: Castryck and Vercauteren showed a dist. attack when $d = 1$ and $q = 2^{31} - 1$ for Giophantus)
- Is there another good subring?
- Fixing $y = 0$ yields a subring $R[x]$!
- Let us consider

$$\pi : R_{n,q}[x, y] \to R_{n,q}[x] : f(x, y) \mapsto f(x, 0)$$

- The problem is finding M from

$$X(x, 0) = a_{10}x + a_{00}$$
$$c(x, 0) = M + p \cdot e(x, 0) + r(x, 0) \cdot X(x, 0)$$

Subring Attack on IEC ($\deg X = 1$)

- Apply $\pi : R_{n,q}[x, y] \to R_{n,q}[x]$

Subring Attack on IEC ($\deg X = 1$)

- Apply $\pi : R_{n,q}[x, y] \to R_{n,q}[x]$
- ek′: $X(x, 0) = a_{10}x + a_{00}$
- ct′: $c(x, 0) = M + p \cdot e(x, 0) + r(x, 0) \cdot X(x, 0)$

$$A = \begin{array}{c} \\ 1 \\ x \\ y \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & x & y & x^2 & xy & y^2 \end{array} \\ \begin{pmatrix} A_{00} & A_{10} & A_{01} & & & \\ & A_{00} & & A_{10} & A_{01} & \\ & & A_{00} & & A_{10} & A_{01} \end{pmatrix} \end{array} \in \mathbb{Z}_q^{240\times 480}$$

$$\to A' = \begin{array}{c} \\ 1 \\ x \end{array} \begin{array}{c} \begin{array}{ccc} 1 & x & x^2 \end{array} \\ \begin{pmatrix} A_{00} & A_{10} & \\ & A_{00} & A_{10} \end{pmatrix} \end{array} \in \mathbb{Z}_q^{160\times 240}.$$

Subring Attack on IEC ($\deg X = 1$)

- Apply $\pi : R_{n,q}[x, y] \to R_{n,q}[x]$
- ek: $X(x, 0) = a_{10}x + a_{00}$
- ct: $c(x, 0) = M + p \cdot e(x, 0) + r(x, 0) \cdot X(x, 0)$

$$A' = \begin{array}{c} \\ 1 \\ x \end{array} \begin{array}{c} \begin{array}{ccc} 1 & x & x^2 \end{array} \\ \begin{pmatrix} A_{00} & A_{10} & \\ & A_{00} & A_{10} \end{pmatrix} \end{array} \in \mathbb{Z}_q^{160 \times 240}.$$

- Solve a 240-dim. CVP instance $(\Lambda_q(A'), \vec{b}')$

$$\Lambda_q(A') = \{\vec{y} \in \mathbb{Z}^{240} \mid \exists \vec{r} \in \mathbb{Z}^{160} : \vec{r} \cdot A' \equiv \vec{y}\},$$
$$\vec{b}' = \vec{r}' \cdot A' + (p\vec{e}' + (M', 0, \ldots, 0)) \bmod q$$

$\to$ Success if the diff. $= p\pi(\vec{e}) + (M, 0, \ldots, 0)$

- Unfortunately, (experimentally) hard for LLL/BKZ to find the diff if $\deg X = 1$.

Subring Attack on IEC ($\deg X = 2$)

- Apply $\pi : R_{n,q}[x, y] \to R_{n,q}[x]$
- ek: $X(x, 0) = a_{20}x^2 + a_{10}x + a_{00}$
- ct: $c(x, 0) = M + p \cdot e(x, 0) + r(x, 0) \cdot X(x, 0)$

$$A' = \begin{array}{c} \\ 1 \\ x \\ x^2 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & x & x^2 & x^3 & x^4 \end{array} \\ \begin{pmatrix} A_{00} & A_{10} & A_{20} & & \\ & A_{00} & A_{10} & A_{20} & \\ & & A_{00} & A_{10} & A_{20} \end{pmatrix} \end{array} \in \mathbb{Z}_q^{240\times 400}.$$

Subring Attack on IEC ($\deg X = 2$)

- Apply $\pi : R_{n,q}[x, y] \to R_{n,q}[x]$
- ek: $X(x, 0) = a_{20}x^2 + a_{10}x + a_{00}$
- ct: $c(x, 0) = M + p \cdot e(x, 0) + r(x, 0) \cdot X(x, 0)$

$$A' = \begin{array}{c} \\ 1 \\ x \\ x^2 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & x & x^2 & x^3 & x^4 \end{array} \\ \begin{pmatrix} A_{00} & A_{10} & A_{20} & & \\ & A_{00} & A_{10} & A_{20} & \\ & & A_{00} & A_{10} & A_{20} \end{pmatrix} \end{array} \in \mathbb{Z}_q^{240\times 400}.$$

- Solve a 400-dim. CVP instance $(\Lambda_q(A'), \vec{b}')$

$$\Lambda_q(A') = \{\vec{y} \in \mathbb{Z}^{400} \mid \exists \vec{r} \in \mathbb{Z}^{240} : \vec{r} \cdot A' \equiv \vec{y}\},$$
$$\vec{b}' = \vec{r}' \cdot A' + (p\vec{e}' + (M', 0, \ldots, 0)) \bmod q$$

Subring Attack on IEC ($\deg X = 2$)

- Solve a 400-dim. CVP instance $(\Lambda_q(A'), \vec{b}')$

$$\Lambda_q(A') = \{\vec{y} \in \mathbb{Z}^{400} \mid \exists \vec{r} \in \mathbb{Z}^{240} : \vec{r} \cdot A' \equiv \vec{y}\},$$
$$\vec{b}' = \vec{r}' \cdot A' + (p\vec{e}' + (M', 0, \ldots, 0)) \bmod q$$

$\longrightarrow$ We can find the diff. $= p\pi(\vec{e}) + (M, 0, \ldots, 0)$ in 17 hours!

- because q is too big to make IEC perfectly correct.

Agenda

Post-Quatnum Crypgraphy

IEC/Giophantus as Lattice-based PKE

Attack against IEC with $n = 80$

Attack against IEC with prime n

Summary

Summary

IEC/Giophantus proposes CPA/CCA-secure PKE
based on IE-LWE (= a special Module-LWE)

	n	$\deg X$
IEC in Aug. 2017	80	1 or 2
IEC in Sep. 2017	83	1 or 2
Giophantus in Dec. 2017	≥ 1201	1

They changed parameter values by reflecting our attacks.

- The origami attacks on IEC in Aug. 2017
  - Key Recovery in ≈ 30 s $(\deg X = 1)$
  - Distinguishing in ≈ 0.5 s $(\deg X = 1)$
  - Distinguishing in ≈ 30 s $(\deg X = 2)$
- The subring attacks on IEC in Sep. 2017
  - Plaintext Recovery in ≈ 17 h $(\deg X = 2)$
  - Distinguishing for large $n \geq 100$