# A NEW ALGORITHM FOR THE VARIANTS OF ACD PROBLEM

Jung Hee Cheon, Wonhee Cho, Minki Hhan,
Minsik Kang, Jiseung Kim, Changmin Lee

ENS de Lyon

June 27, 2019

# Approximate Common-Divisor Problem[HG01]

**Partial Approximate Common Divisor problem(PACD):**

$$\begin{aligned} a_0 &= pq_0 \\ a_1 &= pq_1 + r_1 \equiv r_1 \bmod p \\ &\vdots \qquad\qquad \vdots \\ a_\ell &= pq_\ell + r_\ell \equiv r_\ell \bmod p \end{aligned}$$

where $p$ is a big secret prime and $r_i \ll p$.

**Question :** Given $(a_0, \ldots, a_\ell)$, Can we recover $p$ ?

**Answer :** SDA, OLA, Coppersmith Method

# Approximate Common-Divisor Problem[HG01]

**Partial Approximate Common Divisor problem(PACD):**

$$\begin{aligned} a_0 &= pq_0 \\ a_1 &= pq_1 + r_1 \equiv r_1 \bmod p \\ &\vdots \qquad\qquad \vdots \\ a_\ell &= pq_\ell + r_\ell \equiv r_\ell \bmod p \end{aligned}$$

where $p$ is a big secret prime and $r_i \ll p$.

**Question :** Given $(a_0, \ldots, a_\ell)$, Can we recover $p$ ?
**Answer :** SDA, OLA, Coppersmith Method

# Approximate Common-Divisor Problem[HG01]

**Application:**

- J.-S. Coron, A. Mandal, D. Naccache, M. Tibouchi. Fully homomorphic encryption over the integers with shorter public keys. CRYPTO 2011.
- J.-S. Coron, D. Naccache, M. Tibouchi. Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers. EUROCRYPT 2012.
- J. H. Cheon, D. Stehle. Fully Homomorphic Encryption over the Integers Revisited. EUROCRYPT 2015.

# Chinese Remainder Theorem-ACD Problem[CCK+13]

**CRT-ACD** (Simple version):

$$\begin{aligned} N &= \prod_{i=1}^{n} p_i \\ a_1 &\equiv r_{i1} \bmod p_i \\ &\vdots \\ a_\ell &\equiv r_{i\ell} \bmod p_i \end{aligned}$$

where $p_i$ are big secret primes ($\eta$-bit) and $r_{ij}$ ($\rho$-bit) $\ll p_i$.

**Question :** Given $(N, a_1, \ldots, a_\ell)$, Can we recover $p_i$ ?

**What if $n = 2$?**

# Chinese Remainder Theorem-ACD Problem[CCK+13]

**CRT-ACD** (Simple version):

$$\begin{aligned} N &= \prod_{i=1}^{n} p_i \\ a_1 &\equiv r_{i1} \bmod p_i \\ &\vdots \\ a_\ell &\equiv r_{i\ell} \bmod p_i \end{aligned}$$

where $p_i$ are big secret primes ($\eta$-bit) and $r_{ij}$ ($\rho$-bit) $\ll p_i$.

**Question :** Given $(N, a_1, \ldots, a_\ell)$, Can we recover $p_i$ ?
**What if $n = 2$?**

# Chinese Remainder Theorem-ACD Problem[CCK+13]

**Application:**

- J. H. Cheon, J.-S. Coron, J. Kim, M. S. Lee, T. Lepoint, M. Tibouchi, A. Yun. Batch Fully Homomorphic Encryption over the Integers. EUROCRYPT 2013.
- J.-S. Coron, T. Lepoint, M. Tibouchi, Practical Multilinear Maps over the Integers. CRYPTO13
- J.-S. Coron, T. Lepoint, M. Tibouchi, New Multilinear Maps Over the Integers. CRYPTO15

# Varinant of Chinese Remainder Theorem-ACD Problem

**CRT-ACD with a dual instance(CRT-ACDwDI):**

$$\begin{aligned} N &= \prod_{i=1}^{n} p_i \\ a_1 &\equiv r_{i1} \bmod p_i \\ &\vdots \\ a_\ell &\equiv r_{i\ell} \bmod p_i \\ D &= \sum_i d_i \cdot N/p_i \end{aligned}$$

where $p_i$ are big secret primes ($\eta$-bit) and $r_{ij}$ ($\rho$-bit), $d_i \ll p_i$.

**Question :** Given $(N, a_1, \ldots, a_\ell, D)$, Can we recover $p_i$ ?

**Answer :** Yes!

# Varinant of Chinese Remainder Theorem-ACD Problem

**CRT-ACD with a dual instance(CRT-ACDwDI):**

$$\begin{aligned} N &= \prod_{i=1}^{n} p_i \\ a_1 &\equiv r_{i1} \bmod p_i \\ &\vdots \\ a_\ell &\equiv r_{i\ell} \bmod p_i \\ D &= \sum_i d_i \cdot N/p_i \end{aligned}$$

where $p_i$ are big secret primes ($\eta$-bit) and $r_{ij}$ ($\rho$-bit), $d_i \ll p_i$.

**Question :** Given $(N, a_1, \ldots, a_\ell, D)$, Can we recover $p_i$ ?
**Answer :** Yes!

# Result

Current Status

- There are 3 types of algorithms for solving **PACD**
- Algorithms for **PACD** cannot be applied to **CRT-ACD**.
- There is no algebraic algorithm to solve the **CRT-ACD** problem.
  - It is not known which parameter is safe.
- **CRT-ACDwDI** is solved in polynomial time in $n, \eta$ [CHLRS15].

Our results

- We present an algorithm to solve the CRT-ACD problem
- It is solved in polynomial time if $n \leq \eta - 4 \cdot \rho$.
- We provide the first guideline to set $n$.

# Result

Current Status

- There are 3 types of algorithms for solving **PACD**
- Algorithms for **PACD** cannot be applied to **CRT-ACD**.
- There is no algebraic algorithm to solve the **CRT-ACD** problem.
  - It is not known which parameter is safe.
- **CRT-ACDwDI** is solved in polynomial time in $n, \eta$ [CHLRS15].

Our results

- We present an algorithm to solve the CRT-ACD problem
- It is solved in polynomial time if $n \leq \eta - 4 \cdot \rho$.
- We provide the first guideline to set $n$.

# Cryptanalysis of CRT-ACD

# Notation

Notation:

- $\mathrm{CRT}_{(p_i)}(r_i)$ defined as the unique integer in $\left(-\frac{1}{2}\prod_{i=1}^{n} p_i, \frac{1}{2}\prod_{i=1}^{n} p_i\right]$ which is congruent to $r_i \mod p_i$ for all $i \in \{1, \ldots, n\}$
- $N = \prod_{i=1}^{n} p_i$
- $\hat{p}_i = N/p_i$.

  Note that we assume $n = 2$ for the sake of simplicity. So we use the notation $\mathrm{CRT}_{(p_1,p_2)}(r_{i,1}, r_{i,2})$ as well.

# Definition of CRT-ACD and Dual instance

## Definition (CRT-ACD Problem, Simple version)

Let $p_1$ and $p_2$ be $\eta$-bit integers and $r_{i,1}$ and $r_{i,2}$ be $\rho$-bit integers with $\rho < \eta$. The CRT-ACD problem is:

Given many samples $\mathrm{CRT}_{(p_1,p_2)}(r_{i,1}, r_{i,2})$ and $N$, find $p_1$, $p_2$.

## Definition (Dual instance, Simple version)

Let $p_1$ and $p_2$ be parameters of CRT-ACD problem. Dual instance of CRT-ACD is defined as an integer that is expressed in the following form.

$$D = \sum_{i}^{n} d_i \cdot \hat{p}_i = d_1 \cdot p_2 + d_2 \cdot p_1,$$

where $|d_i| \leq 2^{\eta - 3\rho - \log n} = 2^{\eta - 3\rho - \log 2}$.

# Attack Outline

Our results

- We present an algorithm to solve the CRT-ACD problem

Our algorithm consists of 2 steps

- The first step is to obtain a dual instance only from the CRT-ACD samples.
- Using the previous algorithm for CRT-ACDwDI, all the factors $p_i$ can be recovered.

# Observation

Put $b_j := \mathrm{CRT}_{(p_1,p_2)}(r_{j,1}, r_{j,2}) = p_1 \cdot q_{j,1} + r_{j,1} = p_2 \cdot q_{j,2} + r_{j,2}$.
For any dual instance $d = d_1 \cdot \hat{p}_1 + d_2 \cdot \hat{p}_2$, the followings hold:

$$\begin{aligned}
[d \cdot b_j]_N &\equiv [d_1 \cdot \hat{p}_1 \cdot (p_1 \cdot q_{j,1} + r_{j,1}) + d_2 \cdot \hat{p}_2 \cdot (p_2 \cdot q_{j,2} + r_{j,2})]_N \\
&\equiv [d_1 \cdot \hat{p}_1 \cdot r_{j,1} + d_2 \cdot \hat{p}_2 \cdot r_{j,2}]_N \\
&= d_1 \cdot \hat{p}_1 \cdot r_{j,1} + d_2 \cdot \hat{p}_2 \cdot r_{j,2} \ \textbf{Small!} \text{ compared to } N
\end{aligned}$$

$$\because |d_i| \leq 2^{\eta - 3\rho - \log 2}, \quad |\textstyle\sum_{i=1}^{2} d_i \cdot r_{j,i} \cdot \hat{p}_i| \leq 2^{2\eta - 2\rho} \ll N/2$$

# Step 1: How to find a dual instance

Consider a lattice $\mathcal{L}$ generated by the following matrix:

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ b_1 & N & 0 & 0 & 0 \\ b_2 & 0 & N & 0 & 0 \\ b_3 & 0 & 0 & N & 0 \\ b_4 & 0 & 0 & 0 & N \end{pmatrix}$$

- $([d]_N, [d \cdot b_1]_N, [d \cdot b_2]_N, [d \cdot b_3]_N, [d \cdot b_4]_N)^T$ is a short vector in a lattice $\mathcal{L}$ if $d$ is a dual instance.
- We will show that the first entry of any short vectors in a lattice $\mathcal{L}$ is a dual instance.

# Step 1: Idea Sketch

Let $\mathbf{E} = (E_1, E_2, E_3, E_4, E_5)^T$ be a lattice point of $\mathcal{L}$. We hold:

- For any element $E_1 \in \mathbb{Z}$ can be written as $e_1 \cdot \hat{p}_1 + e_2 \cdot \hat{p}_2$.
- $E_i = [E_1 \cdot b_i]_N = e_1 \cdot r_{i,1} \cdot \hat{p}_1 + e_2 \cdot r_{i,2} \cdot \hat{p}_2 \bmod N$.

Hence, we have the following relation:

$$\begin{aligned} \mathbf{E} &= (E_1, E_2, E_3, E_4, E_5) \\ &= (e_1, e_2) \cdot \begin{pmatrix} \hat{p}_1 & 0 \\ 0 & \hat{p}_2 \end{pmatrix} \cdot \begin{pmatrix} 1 & r_{1,1} & r_{2,1} & r_{3,1} & r_{4,1} \\ 1 & r_{1,2} & r_{2,2} & r_{3,2} & r_{4,2} \end{pmatrix} \\ &= E \cdot \hat{P} \cdot R \bmod N \end{aligned}$$

We want to show that $\|E \cdot \hat{P} \bmod N\|_\infty$ is small. It implies that $\|E\|_\infty$ is small.

# Step 1: Idea Sketch

Let $\mathbf{E} = (E_1, E_2, E_3, E_4, E_5)^T$ be a lattice point of $\mathcal{L}$. We hold:

- For any element $E_1 \in \mathbb{Z}$ can be written as $e_1 \cdot \hat{p}_1 + e_2 \cdot \hat{p}_2$.
- $E_i = [E_1 \cdot b_i]_N = e_1 \cdot r_{i,1} \cdot \hat{p}_1 + e_2 \cdot r_{i,2} \cdot \hat{p}_2 \bmod N$.

Hence, we have the following relation:

$$\begin{aligned} \mathbf{E} &= (E_1, E_2, E_3, E_4, E_5) \\ &= (e_1, e_2) \cdot \begin{pmatrix} \hat{p}_1 & 0 \\ 0 & \hat{p}_2 \end{pmatrix} \cdot \begin{pmatrix} 1 & r_{1,1} & r_{2,1} & r_{3,1} & r_{4,1} \\ 1 & r_{1,2} & r_{2,2} & r_{3,2} & r_{4,2} \end{pmatrix} \\ &= E \cdot \hat{P} \cdot R \bmod N \end{aligned}$$

We want to show that $\|E \cdot \hat{P} \bmod N\|_\infty$ is small. It implies that $\|E\|_\infty$ is small.

# Step 1: Idea Sketch

We obtain the inequality as follows:

$$\begin{aligned} \|E \cdot \hat{P} \bmod N\|_\infty &= \|\mathbf{E} \cdot R^{-1} \bmod N\|_\infty \leq \|\mathbf{E} \cdot R^{-1}\|_\infty \\ &\leq \|\mathbf{E}\|_\infty \cdot \|R^{-1}\|_\infty \cdot n, \end{aligned}$$

where $R^{-1}$ is a right inverse of $R$.

We show that the smallness of

- $\|\mathbf{E}\|_\infty$ with a lattice reduction algorithm. (It is possible when $n \leq \eta - 4 \cdot \rho$.)
- $\|R^{-1}\|_\infty$ with Gaussian Heuristics.

From the equation, the size of $e_i \cdot \hat{p}_i$ is bounded for all $i$.

# Result

Let $n, \eta, \rho$ be parameters of the CRT-ACD Problem. When $2n$ instances are given, we can find a dual instance under the condition

- $n \leq \eta - 4\rho$ in polynomial time with LLL algorithm
- $n \leq \frac{\beta - 1}{2 \log \beta} \cdot (\eta - 4\rho)$ in $2^{O(\beta)}$ time with BKZ algorithm

# Experimental Results

| CRT-ACD | $\eta$ | $\rho_{\max}$[1] | time |
|---|---|---|---|
| Our result | 150 | 70 | 5m |
| | 300 | 110 | 1h |
| | 450 | 190 | 2h |
| | 600 | 300 | 3.1h |
| | 750 | 370 | 4.1h |
| | 900 | 450 | 6.2h |
| | 1500 | 700 | 10h |

Here the number of prime factors, $n$, is set to be 50.

[1] The $\rho_{max}$ value corresponding to $\eta$ is the maximum $\rho$ value on which the experiment succeeded.

# Step2 [CHLRS15]

- Product of $b = \mathrm{CRT}_{(p_i)}(r_i)$ and $d = e_1 \cdot p_2 + e_2 \cdot p_1$:

$$[b \cdot d]_N \quad = \quad e_1 \cdot r_1 \cdot p_2 + e_2 \cdot r_2 \cdot p_1. \qquad \textbf{(an integer equation!)}$$

- We can compute it with $b_1 \cdot b_2 \cdot b_3 \cdot d$:

$$[b_1 \cdot b_2 \cdot b_3 \cdot d]_N = r_{11} r_{12} r_{13} e_1 p_2 + r_{21} r_{22} r_{23} e_2 p_1$$

$$= \quad \begin{pmatrix} r_{11} & r_{21} \end{pmatrix} \cdot \begin{pmatrix} r_{13} & \\ & r_{23} \end{pmatrix} \cdot \begin{pmatrix} e_1 p_2 & \\ & e_2 p_1 \end{pmatrix} \cdot \begin{pmatrix} r_{12} \\ r_{22} \end{pmatrix}.$$

for $b_i = \mathrm{CRT}(r_{ij})$.

# Step2 [CHLRS15]

- Product of $b = \mathrm{CRT}_{(p_i)}(r_i)$ and $d = e_1 \cdot p_2 + e_2 \cdot p_1$:

$$[b \cdot d]_N \quad = \quad e_1 \cdot r_1 \cdot p_2 + e_2 \cdot r_2 \cdot p_1. \qquad \textbf{(an integer equation!)}$$

- We can compute it with $b_1 \cdot b_2 \cdot b_3 \cdot d$:

$$[b_1 \cdot b_2 \cdot b_3 \cdot d]_N = r_{11} r_{12} r_{13} e_1 p_2 + r_{21} r_{22} r_{23} e_2 p_1$$

$$= \quad \begin{pmatrix} r_{11} & r_{21} \end{pmatrix} \cdot \begin{pmatrix} r_{13} & \\ & r_{23} \end{pmatrix} \cdot \begin{pmatrix} e_1 p_2 & \\ & e_2 p_1 \end{pmatrix} \cdot \begin{pmatrix} r_{12} \\ r_{22} \end{pmatrix}.$$

for $b_i = \mathrm{CRT}(r_{ij})$.

# Build Equations

- Changing the indices $j$ and $k$, compute $[b_j \cdot b_k \cdot b_3 \cdot d]_N$, and compose a matrix $W_1$

$$W_1 = \begin{pmatrix} r_{11} & r_{21} \\ r_{12} & r_{22} \end{pmatrix} \cdot \begin{pmatrix} r_{13} & \\ & r_{23} \end{pmatrix} \cdot \begin{pmatrix} e_1 p_2 & \\ & e_2 p_1 \end{pmatrix} \cdot \begin{pmatrix} r_{12} & r_{11} \\ r_{22} & r_{21} \end{pmatrix}.$$

$$= \hat{R} \cdot \mathrm{diag}((r_{13})e_1 p_2, (r_{23})e_2 p_1) \cdot R$$

**It is a matrix composed of secret parameter!**

# Build Equations

- By removing $b_3$

$$[b_1 \cdot b_2 \cdot b_3 \cdot d]_N \rightarrow [b_1 \cdot b_2 \cdot d]_N,$$

we obtain

$$W_2 \quad = \quad \hat{R} \cdot \mathrm{diag}(e_1 p_2, e_2 p_1) \cdot R$$

- $W_1$ and $W_2$ are of the same form except for the middle matrix.

$$W_1 \cdot W_2^{-1} \quad = \quad \hat{R} \cdot \mathrm{diag}(r_{13}, r_{23}) \cdot \hat{R}^{-1}.$$

Its eigenvalues are $r_{13}, r_{23}$.

# Solve Equations

- Recover $p_i$: By definition,
  - $p_1$ divides $b_3 - r_{13}$ and $N = p_1 \cdot p_2$.

  Hence, one can recover $p_1$ by computing GCD.

- By repeating this, we can find all the secret $p_i$'s.

# Summary

- We present a reduction from **CRT-ACD** problem to **CRT-ACDwDI** problem
- Combining the previous result, we solve the **CRT-ACD** problem under some constraints.
- We also provide an algorithm for distinguishing between **CRT-ACD** instnaces and random instances. Please refer to our paper.
- It would be an interesting problem to extend solvable parameter conditions.

Thank you

for your attention.