Power Analysis on NTRU Prime

Wei-Lun Huang, Jiun-Peng Chen, Bo-Yin Yang

Academia Sinica, Taiwan

CHES 2020

Topics

- ❖ NTRU Prime
- ❖ A Brief Preview
- ❖ Correlation Power Analysis: vertical vs. horizontal in-depth
- ❖ Online Template Attacks
- ❖ Chosen-Input Simple Power Analysis
- ❖ Finale

Topics

- NTRU Prime
- A Brief Preview
- Correlation Power Analysis: vertical vs. horizontal in-depth
- Online Template Attacks
- Chosen-Input Simple Power Analysis
- Finale

Post-Quantum Cryptography (PQC)

- ❖ Shor's Algorithm
  - ➢ solving integer factorization and discrete logarithms efficiently
  - ➢ Quantum Computers: estimated as arriving in 10~20 years

- Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.

Post-Quantum Cryptography (PQC)

- Shor's Algorithm
  - solving integer factorization and discrete logarithms efficiently
  - Quantum Computers: estimated as arriving in 10~20 years

- The NIST PQC Standardization Project
  - key encapsulation mechanisms (KEM) + digital signatures
  - lattices / error correction codes / multivariate quadratic equations / ...

- Post-Quantum Cryptography | CSRC. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

NTRU Prime: lattice-based KEM

- Streamlined NTRU Prime / NTRU LPRime: 653 / 761 / 857

p and q prime; $R := \mathbb{Z}[x]/(x^p - x - 1)$
small: a ternary polynomial from R
short: **small** with exactly w nonzero coefficients
$R/3 := (\mathbb{Z}/3)[x]/(x^p - x - 1)$ and $R/q := (\mathbb{Z}/q)[x]/(x^p - x - 1)$

Alice		**Bob**
KeyGen		
small g s.t. g^{-1} in $R/3$ exists		
short $f \Rightarrow$ compute $f_{\text{inv}} := (3f)^{-1}$ in R/q	$\xrightarrow{\text{public key } h}$	
$h \leftarrow g \times f_{\text{inv}}$ in R/q		Encap
		short r as the session key
Decap	$\xleftarrow{\text{ciphertext } c}$	$c \leftarrow \text{Round}(h \times r)$ in R/q
$e \leftarrow c \times 3f$ in R/q		
$r \leftarrow e \times g^{-1}$ in $R/3$		

- Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU Prime: round 2.

Interesting Multiplication in NTRU Prime

- ❖ The Product Scanning Method
  - ➢ Inputs: known *c* in R/q and secret **short** *f*
  - ➢ Ouput: *e* = (*c* x *f*) mod *q*
  - ➢ `Decap` / `Encap` / `KeyGen` (only `ntrulpr*`)

$$
\begin{array}{rr}
 & -2x^2 + 3x - 5 \\
\times) & -1x^2 + 0x + 1 \\
\hline
 & -5 \\
 & \\
\hline
 & -5
\end{array}
$$

Side-Channel Informative: Least

- Michael Hutter and Erich Wenger. Fast Multi-Precision Multiplication for Public-Key Cryptography on Embedded Microprocessors.

Interesting Multiplication in NTRU Prime

- The Product Scanning Method
  - Inputs: known *c* in R/q and secret **short** *f*
  - Ouput: *e* = (*c* x *f*) mod *q*
  - `Decap` / `Encap` / `KeyGen` (only `ntrulpr`*)

$$
\begin{array}{rr}
 & -2x^2 + 3x - 5 \\
\times) & -1x^2 + 0x + 1 \\
\hline
 & +0 \quad -5 \\
 & +3 \qquad\; \\
\hline
 & +3 \quad -5
\end{array}
$$

Side-Channel Informative: **More**

Interesting Multiplication in NTRU Prime

❖ The Product Scanning Method

➢ Inputs: known *c* in R/q and secret **short** *f*

➢ Ouput: *e* = (*c* x *f*) mod *q*

➢ `Decap` / `Encap` / `KeyGen` (only `ntrulpr*`)

$$
\begin{array}{rrrr}
 & -2x^2 & +\,3x & -\,5 \\
\times) & -1x^2 & +\,0x & +\,1 \\
\hline
 & +5 & +0 & -5 \\
 & +0 & +3 & \\
 & -2 & & \\
\hline
 & +3 & +3 & -5
\end{array}
$$

Side-Channel Informative: Most

Interesting Multiplication in NTRU Prime

- ❖ The Product Scanning Method
  - ➢ Inputs: known *c* in R/q and secret **short** *f*
  - ➢ Ouput: *e* = (*c* x *f*) mod *q*
  - ➢ `Decap` / `Encap` / `KeyGen` (only `ntrulpr`*)

$$\begin{array}{rrrr}
 & -2x^2 & +3x & -5\\
\times) & -1x^2 & +0x & +1\\ \hline
 & +5 & +0 & -5\\
-3 & +0 & +3 & \\
+0 & -2 & & \\ \hline
-3 & +3 & +3 & -5
\end{array}$$

Side-Channel Informative: Less

Interesting Multiplication in NTRU Prime

❖ The Product Scanning Method
  - ➢ Inputs: known *c* in R/q and secret **short** *f*
  - ➢ Ouput: *e* = (*c* x *f*) mod *q*
  - ➢ `Decap` / `Encap` / `KeyGen` (only `ntrulpr`*)

$$
\begin{array}{rrrrrr}
 & & & -2x^2 & +3x & -5 \\
\times) & & & -1x^2 & +0x & +1 \\
\hline
 & & & +5 & +0 & -5 \\
 & & -3 & +0 & +3 & \\
 & +2 & +0 & -2 & & \\
\hline
 & +2 & -3 & +3 & +3 & -5
\end{array}
$$

Side-Channel Informative: Least

Topics

- NTRU Prime
- A Brief Preview
- Correlation Power Analysis: vertical vs. horizontal in-depth
- Online Template Attacks
- Chosen-Input Simple Power Analysis
- Finale

Experiment Settings

- `sntrup761 Decap` on ARM Cortex-M4
  - p = 761, q = 4591, and w = 286
  - on STM32F303RCT7 and STM32F415RGT6

- STMicroelectronics. Datasheet - STM32F303xB STM32F303xC.
- STMicroelectronics. Datasheet - STM32F415xx STM32F417xx.

Experiment Settings

- `sntrup761 Decap` on ARM Cortex-M4
  - p = 761, q = 4591, and w = 286
  - on STM32F303RCT7 and STM32F415RGT6
- ChipWhisperer-Lite Two-Part Version
  - random input generation + measurement + data collection
- Statistical Analysis: in Python 3.6.1 or C++ on a MacBook Air

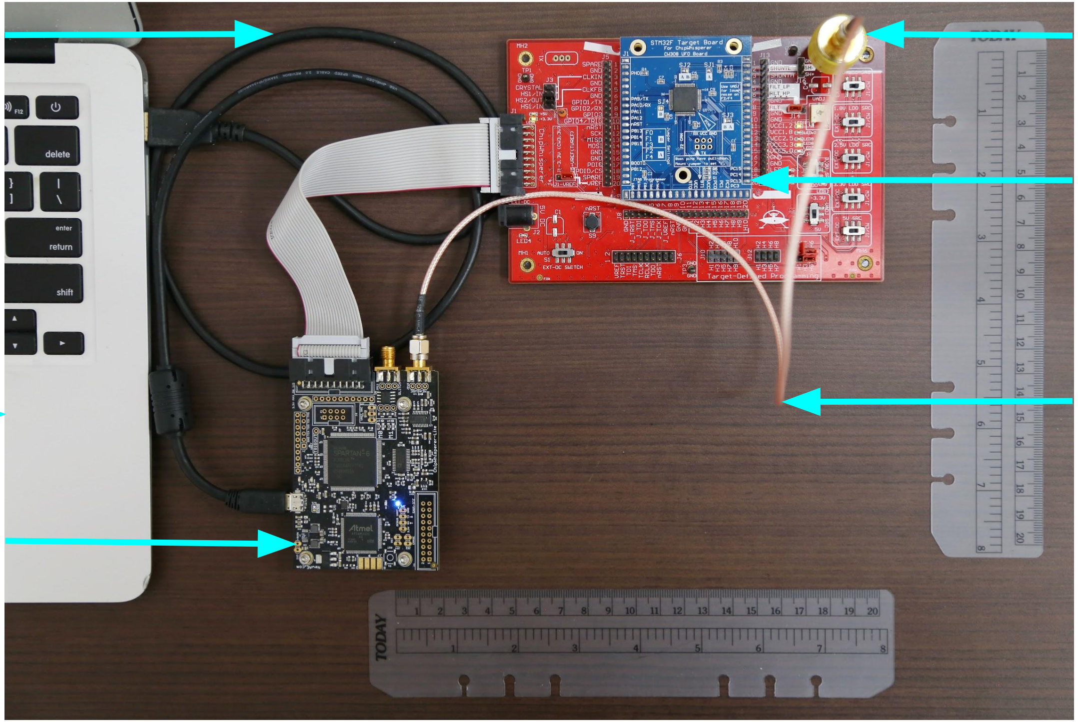
- ChipWhisperer-Lite (CW1173) Two-Part Version - NewAE Technology Inc. https://store.newae.com/chipwhisperer-lite-cw1173-two-part-version/

STM32F415RGT6 + ChipWhisperer-Lite

USB to PC

MacBook Air

Control Board



Mini-Circuits

SLP-10.7+

Target Board

at 7.38MHz

Coaxial Cable

- Low Pass Filter - Mini Circuits. https://www.minicircuits.com/pdfs/SLP-10.7+.pdf

Power Analysis Methods

CPA: Correlation Power Analysis

SPA: Simple Power Analysis

- ❖ Vertical CPA: robust and fast
- ❖ Horizontal In-Depth CPA: using one single short trace
- ❖ Online Template Attacks: fast profiling with few template traces
- ❖ Chosen-Input SPA: with the naked eye

Topics

- ❖ NTRU Prime
- ❖ A Brief Preview
- ❖ Correlation Power Analysis: vertical vs. horizontal in-depth
- ❖ Online Template Attacks
- ❖ Chosen-Input Simple Power Analysis
- ❖ Finale

- Mun-Kyu Lee et al. Countermeasures against Power Analysis Attacks for the NTRU Public Key Cryptosystem.
- Aydin Aysu et al. Horizontal Side-Channel Vulnerabilities of Post-Quantum Key Exchange Protocols.

Vertical CPA

e_{p-1} initialized to be 0

$$\boxed{\begin{aligned}&+c_0 \times 0\\&\vdots\\&+c_{p-1-b_w} \times f_{b_w}\\&+c_{p-1-b_w+1} \times 0\\&\vdots\\&+c_{p-1-b_{w-1}-1} \times 0\\&+c_{p-1-b_{w-1}} \times f_{b_{w-1}}\\&+c_{p-1-b_{w-1}+1} \times 0\\&\vdots\\&+c_{p-1-b_1-1} \times 0\\&+c_{p-1-b_1} \times f_{b_1}\\&\vdots\\&+c_{p-1} \times 0\end{aligned}}$$

$$e_{p-1,1} = (c_{p-1-b_w} \times f_{b_w}) \bmod q$$

$$e_{p-1,2} = (c_{p-1-b_w} \times f_{b_w} + c_{p-1-b_{w-1}} \times f_{b_{w-1}}) \bmod q$$

$$\approx$$

$$\begin{aligned}e_{p-1,w} = (&c_{p-1-b_w} \times f_{b_w}\\&+ c_{p-1-b_{w-1}} \times f_{b_{w-1}}\\&\vdots\\&+ c_{p-1-b_1} \times f_{b_1}) \bmod q\end{aligned}$$

Vertical CPA

Reveal f_{b_w} and $f_{b_{w-1}}$ at a time.

e_{p-1} initialized to be 0

$$\boxed{\begin{array}{l} + c_0 \times 0 \\ \vdots \\ + c_{p-1-b_w} \times f_{b_w} \\ + c_{p-1-b_w+1} \times 0 \\ \vdots \\ + c_{p-1-b_{w-1}-1} \times 0 \\ + c_{p-1-b_{w-1}} \times f_{b_{w-1}} \\ + c_{p-1-b_{w-1}+1} \times 0 \\ \vdots \\ + c_{p-1-b_1-1} \times 0 \\ + c_{p-1-b_1} \times f_{b_1} \\ \vdots \\ + c_{p-1} \times 0 \end{array}}$$

likely to confuse with c_{p-1-b_w}

$$e_{p-1,1} = (c_{p-1-b_w} \times f_{b_w}) \bmod q$$

$$e_{p-1,2} = (c_{p-1-b_w} \times f_{b_w} + c_{p-1-b_{w-1}} \times f_{b_{w-1}}) \bmod q$$

$$\approx$$

$$e_{p-1,w} = (c_{p-1-b_w} \times f_{b_w} + c_{p-1-b_{w-1}} \times f_{b_{w-1}} \\ \vdots \\ + c_{p-1-b_1} \times f_{b_1}) \bmod q$$

Vertical CPA

Reveal f_{b_w} and $f_{b_{w-1}}$ at a time.

Reveal $f_{b_{w-2}}, \ldots, f_{b_1}$ one by one.

e_{p-1} initialized to be 0

$$\boxed{\begin{aligned}
&+ c_0 \times 0\\
&\vdots\\
&+ c_{p-1-b_w} \times f_{b_w}\\
&+ c_{p-1-b_w+1} \times 0\\
&\vdots\\
&+ c_{p-1-b_{w-1}-1} \times 0\\
&+ c_{p-1-b_{w-1}} \times f_{b_{w-1}}\\
&+ c_{p-1-b_{w-1}+1} \times 0\\
&\vdots\\
&+ c_{p-1-b_1-1} \times 0\\
&+ c_{p-1-b_1} \times f_{b_1}\\
&\vdots\\
&+ c_{p-1} \times 0
\end{aligned}}$$

likely to confuse with c_{p-1-b_w}

$$e_{p-1,1} = (c_{p-1-b_w} \times f_{b_w}) \bmod q$$

$$\begin{aligned} e_{p-1,2} = (&c_{p-1-b_w} \times f_{b_w}\\ &+ c_{p-1-b_{w-1}} \times f_{b_{w-1}}) \bmod q\end{aligned}$$

$$\approx$$

$$\begin{aligned} e_{p-1,w} = (&c_{p-1-b_w} \times f_{b_w}\\ &+ c_{p-1-b_{w-1}} \times f_{b_{w-1}}\\ &\vdots\\ &+ c_{p-1-b_1} \times f_{b_1}) \bmod q\end{aligned}$$

In-Depth CPA

- Vertical CPA: one coefficient at a time with multiple short traces
  - How to squeeze more information from each short trace?

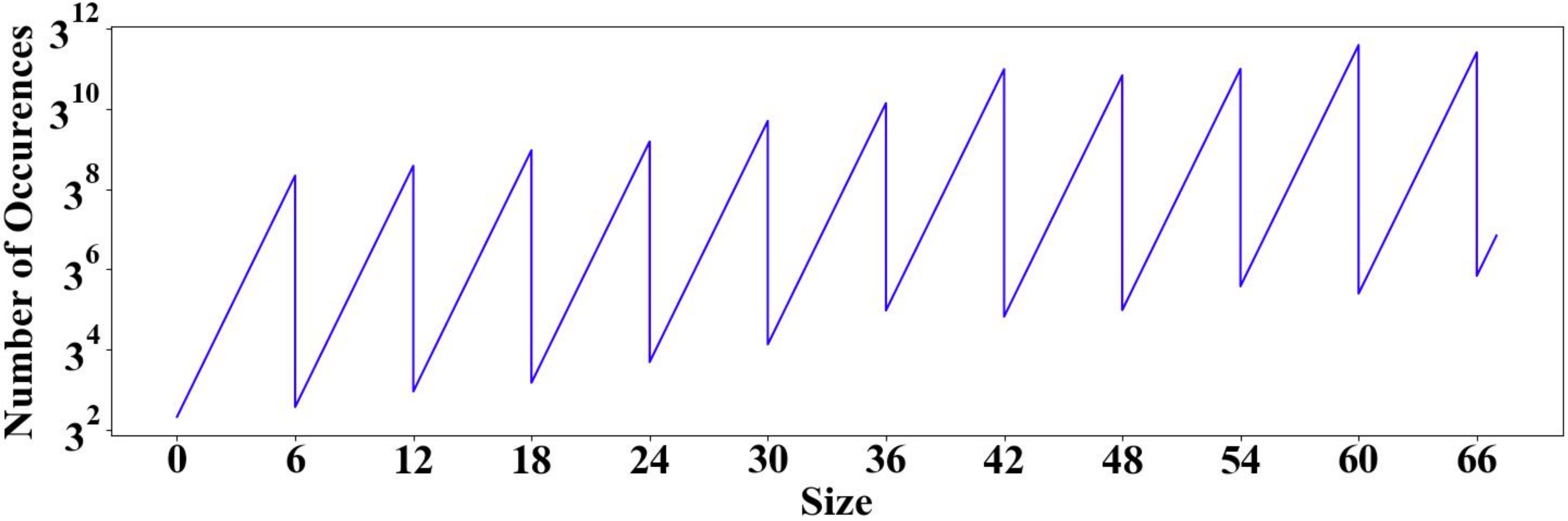
In-Depth CPA

- Vertical CPA: one coefficient at a time with multiple short traces
  - How to squeeze more information from each short trace?

- In-Depth CPA: multiple coefficients at a time with one short trace
  - The intermediate state of e_{p-1} depends on the current (c_j, f_{p-1-j})
  - and all the previous (c_j, f_{p-1-j}). → Extend-and-Prune

Candidate Pruning

❖ Block Size m = 67 + Pruning Period n = 6



Tail-Error Removal

- Tail Errors: at the end of the block
  - In the current block recovery, the correlation still looks great.
  - In the next block recovery, no hypotheses survive.

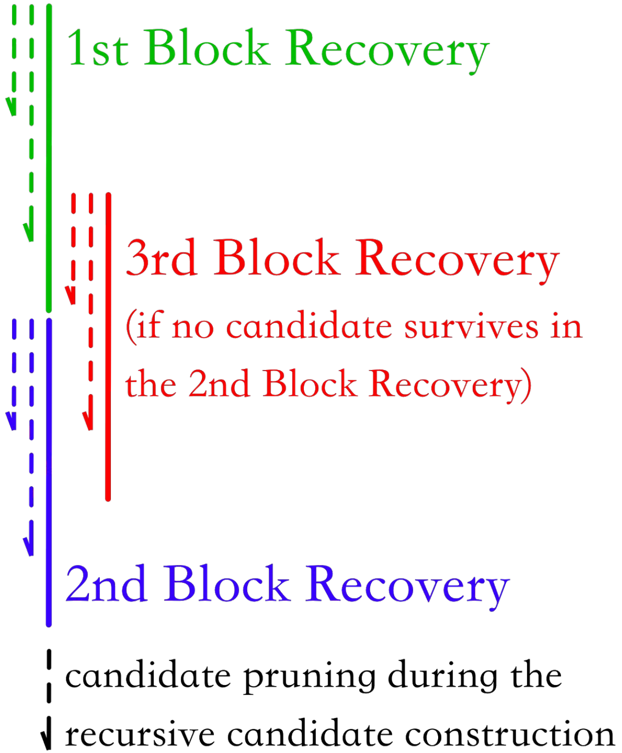
Tail-Error Removal

- ❖ Tail Errors: at the end of the block
  - ➢ In the current block recovery, the correlation still looks great.
  - ➢ In the next block recovery, no hypotheses survive.

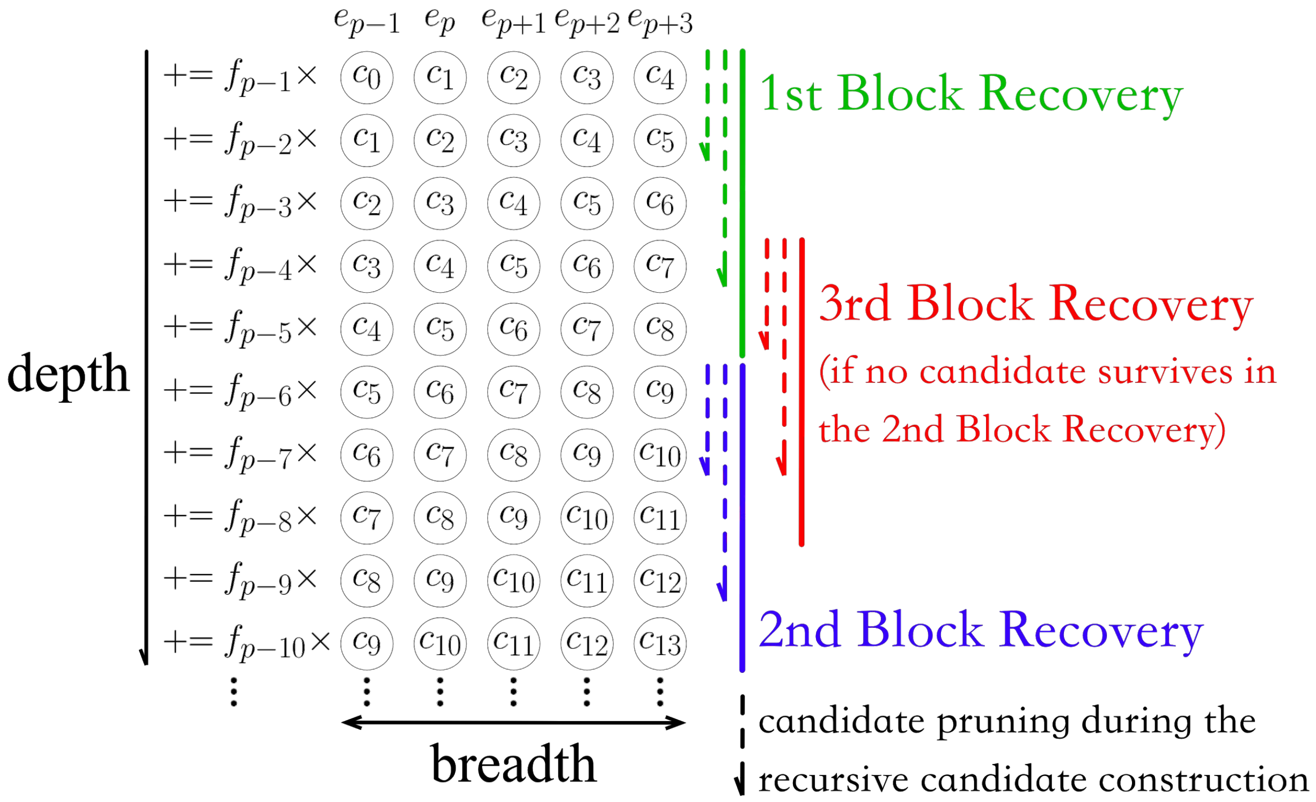
- ❖ Roll Back: by half a block
  - ➢ once no hypotheses survive in the current block recovery.
  - ➢ tail errors in the final block → exhaustive search

A Toy Example: m = 5, n = 2, l = 5

$$
\text{depth} \downarrow \quad
\begin{array}{ll}
 & e_{p-1} \\
\mathrel{+}= f_{p-1} \times & c_0 \\
\mathrel{+}= f_{p-2} \times & c_1 \\
\mathrel{+}= f_{p-3} \times & c_2 \\
\mathrel{+}= f_{p-4} \times & c_3 \\
\mathrel{+}= f_{p-5} \times & c_4 \\
\mathrel{+}= f_{p-6} \times & c_5 \\
\mathrel{+}= f_{p-7} \times & c_6 \\
\mathrel{+}= f_{p-8} \times & c_7 \\
\mathrel{+}= f_{p-9} \times & c_8 \\
\mathrel{+}= f_{p-10} \times & c_9 \\
\vdots & \vdots
\end{array}
$$



A Toy Example: m = 5, n = 2, l = 5



Horizontal In-Depth CPA (HIDCPA)

- ❖ In-Depth CPA: inefficient and inaccurate
  - ➢ every *m* coefficients mapped to only *m* samples
  - ➢ the lack of data → ineffective candidate pruning

Horizontal In-Depth CPA (HIDCPA)

- In-Depth CPA: inefficient and inaccurate
  - every *m* coefficients mapped to only *m* samples
  - the lack of data → ineffective candidate pruning

- Learn from horizontal attacks!
  - Observe the calculation of $e_{p-1}, e_p, \ldots, e_{p-2+l}$.
  - For $l \ll p$, we have nearly *l* times as many data.

A Real-World Example: m = 67, n = 6, l = 5

The

Top

```
Candidate 25 -> bestCorr = -0.976936
f_559 ~ f_493: [0, 0, 1, -1, 0, 0, -1, 1, 1, 0, 0, 0, 1, -1, 0, 0, -1, 0, 1,
 0, -1, 0, -1, -1, -1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0,
 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, -1, 0, -1, 0, -1, 0, 0, 0, 0, 0, 0, 1, -1]
Candidate 26 -> bestCorr = -0.983238
f_559 ~ f_493: [0, 0, 1, -1, 0, 0, -1, 1, 1, 0, 0, 0, 1, -1, 0, 0, -1, 0, 1,
 0, -1, 0, -1, -1, -1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0,
 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, -1, 0, -1, 0, -1, 0, 0, 0, 0, 0, 0, 1, 0]
42 candidates reach the final comparison.

- - - - - - - - - - - -
Now start with f_492
- - - - - - - - - - - -
0 candidates reach the final comparison.

- - - - - - - - - - - -
Now start with f_525
- - - - - - - - - - - -
Candidate 1 -> bestCorr = -0.946477
f_525 ~ f_459: [0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0,
-1, 0, -1, 0, -1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, -1, 0, 0, -1, 0, 0, 1,
 0, -1, 1, 0, 0, 0, 0, 0, -1, 0, 0, 0, -1, 0, 0, -1, 1, -1, 1, 0, 1, 1, -1]
```

Tail Error

A Real-World Example: m = 67, n = 6, l = 5

The Middle

```
Candidate 25 -> bestCorr = -0.976936
f_559 ~ f_493: [0, 0, 1, -1, 0, 0, -1, 1, 1, 0, 0, 0, 1, -1, 0, 0, -1, 0, 1,
 0, -1, 0, -1, -1, -1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0,
 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, -1, 0, -1, 0, -1, 0, 0, 0, 0, 0, 0, 1, -1]
Candidate 26 -> bestCorr = -0.983238
f_559 ~ f_493: [0, 0, 1, -1, 0, 0, -1, 1, 1, 0, 0, 0, 1, -1, 0, 0, -1, 0, 1,
 0, -1, 0, -1, -1, -1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0,
 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, -1, 0, -1, 0, -1, 0, 0, 0, 0, 0, 0, 1, 0]
42 candidates reach the final comparison.

- - - - - - - - - - - - - - -
Now start with f_492
- - - - - - - - - - - - - - -
0 candidates reach the final comparison.

- - - - - - - - - - - - - - -
Now start with f_525
- - - - - - - - - - - - - - -
Candidate 1 -> bestCorr = -0.946477
f_525 ~ f_459: [0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0,
-1, 0, -1, 0, -1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, -1, 0, 0, -1, 0, 0, 1,
 0, -1, 1, 0, 0, 0, 0, 0, -1, 0, 0, 0, -1, 0, 0, -1, 1, -1, 1, 0, 1, 1, -1]
```

A Real-World Example: m = 67, n = 6, l = 5

```
Candidate 25 -> bestCorr = -0.976936
f_559 ~ f_493: [0, 0, 1, -1, 0, 0, -1, 1, 1, 0, 0, 0, 1, -1, 0, 0, -1, 0, 1,
 0, -1, 0, -1, -1, -1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0,
 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, -1, 0, -1, 0, -1, 0, 0, 0, 0, 0, 0, 1, -1]
Candidate 26 -> bestCorr = -0.983238
f_559 ~ f_493: [0, 0, 1, -1, 0, 0, -1, 1, 1, 0, 0, 0, 1, -1, 0, 0, -1, 0, 1,
 0, -1, 0, -1, -1, -1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0,
 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, -1, 0, -1, 0, -1, 0, 0, 0, 0, 0, 0, 1, 0]
42 candidates reach the final comparison.

- - - - - - - - - - - -
Now start with f_492
- - - - - - - - - - - -
0 candidates reach the final comparison.

- - - - - - - - - - - -
Now start with f_525
- - - - - - - - - - - -
Candidate 1 -> bestCorr = -0.946477
f_525 ~ f_459: [0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0,
-1, 0, -1, 0, -1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, -1, 0, 0, -1, 0, 0, 1,
 0, -1, 1, 0, 0, 0, 0, 0, -1, 0, 0, 0, -1, 0, 0, -1, 1, -1, 1, 0, 1, 1, -1]
```

Corrected

The Bottom

Topics

- ❖ NTRU Prime
- ❖ A Brief Preview
- ❖ Correlation Power Analysis: vertical vs. horizontal in-depth
- ❖ Online Template Attacks
- ❖ Chosen-Input Simple Power Analysis
- ❖ Finale

- Lejla Batina, Lukasz Chmielewski, Louiza Papachristodoulou, Peter Schwabe, and Michael Tunstall. Online Template Attacks.

Template Attacks

- What if the assumption of simple power models fails?
  - Classical Correlation Attacks: the Hamming weight/distance models
  - Classical Template Attacks: multivariate normal distribution

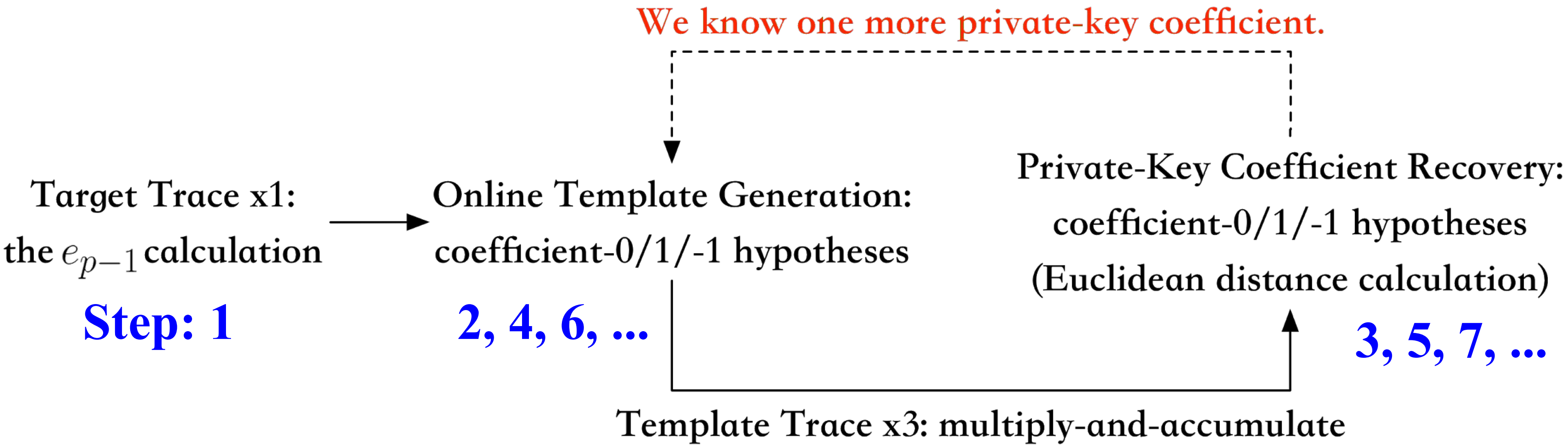
Template Attacks

- ❖ What if the assumption of simple power models fails?
  - ➢ Classical Correlation Attacks: the Hamming weight/distance models
  - ➢ Classical Template Attacks: multivariate normal distribution

- ❖ The Profiling Stage
  - ➢ numerous template traces + heavy computational power

Can we mount template attacks with few template traces?

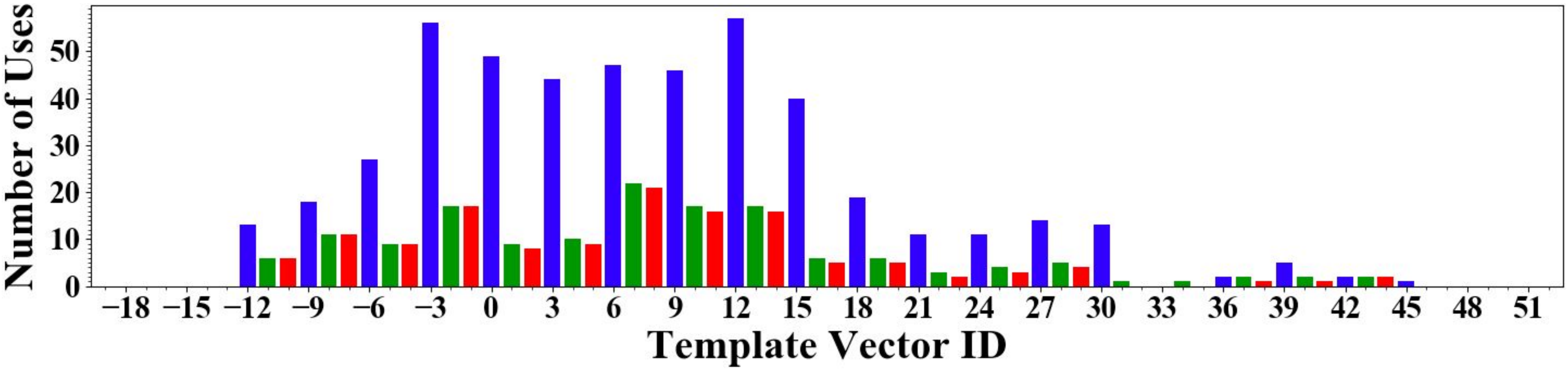
Online Template Attacks (OTA)



Can we mount template attacks with fewer executions?

The Chosen-Input Offline Variant

- Chosen-Input: $c_0 = c_1 = \ldots = c_{p-1}, 3 \mid c_0$
  - enhancing the reusability of template traces



The Chosen-Input Offline Variant

- Illegitimate Private Key: *f** on the template generator
  - generating all the required template traces within four executions
  - $c^* = c + (c_1^* - c_0)x$ and e_{p-1} expressed as $c_0 \times t \bmod q$

c_1^* \ f^*	$x + x^3 + x^5 + \cdots + x^{p-2}$	$-x - x^3 - x^5 - \cdots - x^{p-2}$
$c_0 \times (-w) \bmod q$	$[+]$ for $t = -w, \cdots, -1, 0$ $[\times]$ for $t = -w, \cdots, -1, 0$	$[\times]$ for $t = 0, 1, \cdots, w$ $[-]$ for $t = 0, 1, \cdots, w$
c_0	$[+]$ for $t = 1, 2, \cdots, w$ $[\times]$ for $t = 1, 2, \cdots, w$	$[\times]$ for $t = -w, \cdots, -2, -1$ $[-]$ for $t = -w, \cdots, -2, -1$

Topics

- ❖ NTRU Prime
- ❖ A Brief Preview
- ❖ Correlation Power Analysis: vertical vs. horizontal in-depth
- ❖ Online Template Attacks
- ❖ Chosen-Input Simple Power Analysis
- ❖ Finale

- Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis.

Not Countermeasures

- ❖ Apply a random mask to each output coefficient.
  - ➢ integer offsets added at the beginning and removed at the end

- ❖ Shuffle multiply-and-accumulates for each output coefficient.
  - ➢ input-coefficient pairs accessed in a random order

- Mun-Kyu Lee et al. Countermeasures against Power Analysis Attacks for the NTRU Public Key Cryptosystem.

Not Countermeasures

- ❖ Apply a random mask to each output coefficient.
  - ➢ integer offsets added at the beginning and removed at the end

subject to chosen-input SPA (CISPA)

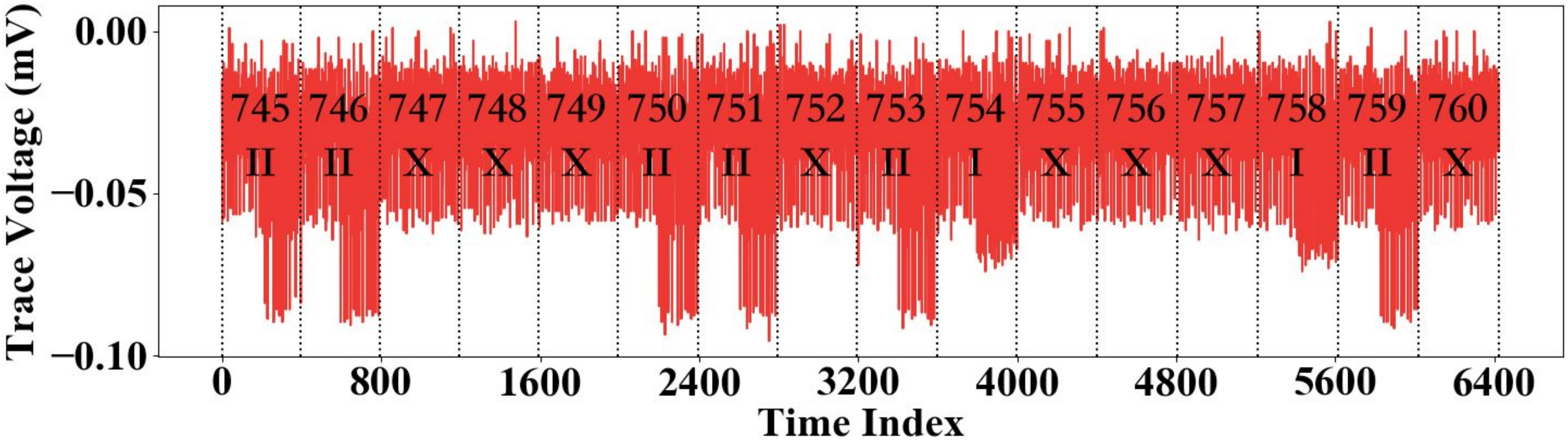
- ❖ Shuffle multiply-and-accumulates for each output coefficient.
  - ➢ input-coefficient pairs accessed in a random order

subject to chosen-input SPA (CISPA)

CISPA on Countermeasure 2

$$c = c_0, \text{where } c_0 \neq 0 \text{ and } 3 \mid c_0$$

one sample per 64 clock cycles



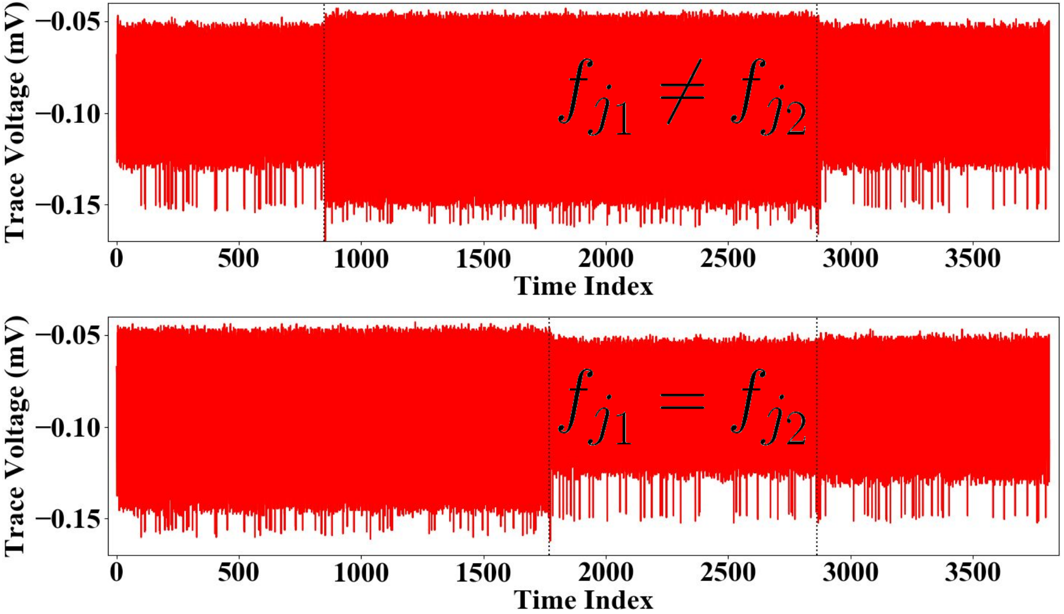
CISPA on Countermeasure 1

- ❖ Two Stages: nonzero f_j identification + clustering

- ❖ The First Stage: continuous? discontinuous?
  - ➢ similar to CISPA on Countermeasure 2
  - ➢ Zero or Nonzero: output coefficient → private-key coefficient

CISPA on Countermeasure 1

- The Second Stage: $c = c_0 x^{p-1-j_1} + c_0 x^{p-1-j_2}$
  - knowing $f_{j_1} \neq 0 \text{ and } f_{j_2} \neq 0$ + observing the e_{p-1} calculation



Topics

- ❖ NTRU Prime
- ❖ A Brief Preview
- ❖ Correlation Power Analysis: vertical vs. horizontal in-depth
- ❖ Online Template Attacks
- ❖ Chosen-Input Simple Power Analysis
- ❖ Finale

Two Optimizations and One Countermeasure

- Optimized Product Scanning
  - Modular Reduction: per multiply-and-accumulate → per e_i calculation
  - $\mathrm{SMLABB} \rightarrow \mathrm{SMLADX}$: two multiply-and-accumulates per instruction
  - 4.4x faster / immune to OTA / still subject to HIDCPA and CISPA

- Cortex-M4 Devices Generic User Guide. http://infocenter.arm.com/help/topic/com.arm.doc.dui0553b/DUI0553.pdf

Two Optimizations and One Countermeasure

- Optimized Product Scanning
  - Modular Reduction: per multiply-and-accumulate → per e_i calculation
  - SMLABB → SMLADX: two multiply-and-accumulates per instruction
  - 4.4x faster / immune to OTA / still subject to HIDCPA and CISPA

- First-Order Masking: both inputs masked
  - If the ciphertext not masked: horizontal CPA
  - If the private key not masked: SPA or profiling attacks (potentially)

- Stefan Mangard, Elisabeth Oswald, and Thomas Popp. Power Analysis Attacks - Revealing the Secrets of Smart Cards.

Conclusion

- Single-Trace Power Analysis on the Product Scanning Method
  - applicable to NTRU Prime Decap/Encap/KeyGen
  - targeting the reference/protected/optimized implementations
  - with short observation span, few template traces, or the naked eye

Conclusion

- Single-Trace Power Analysis on the Product Scanning Method
  - applicable to NTRU Prime Decap/Encap/KeyGen
  - targeting the reference/protected/optimized implementations
  - with short observation span, few template traces, or the naked eye

- Potential Applications
  - other ideal-lattice-based cryptosystems with
  - private/session-key coefficients from a small set of possibilities
  - multi-level Karatsuba ending with the product scanning method

- Anatolii Karatsuba. Multiplication of Multidigit Numbers on Automata.

Q & A