Improvement of Side-Channel Attacks on Mitaka

Template Attacks with a Power Model

Vladimir Sarde, Nicolas Debande

April 2, 2025

Outline

Introduction

1

The Context
The Mitaka Scheme

Introduction

1

› The Context

The Mitaka Scheme

Introduction

MITAKA: A Simpler, Parallelizable, Maskable Variant of FALCON

Thomas Espitau, Pierre-Alain Fouque, François Gérard, Mélissa Rossi, Akira Takahashi, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu

2021

Introduction

MITAKA: A Simpler, Parallelizable, Maskable Variant of FALCON

Thomas Espitau, Pierre-Alain Fouque, François Gérard, Mélissa Rossi, Akira Takahashi, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu

2021

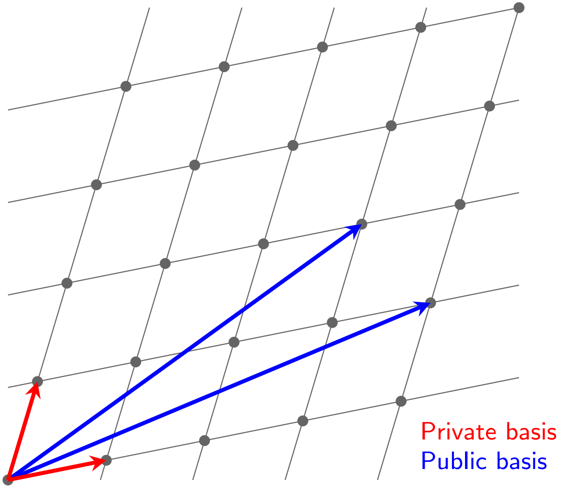
Slightly Improve Performances

Simpler Structure

Introduction

1

Mitaka Parameters



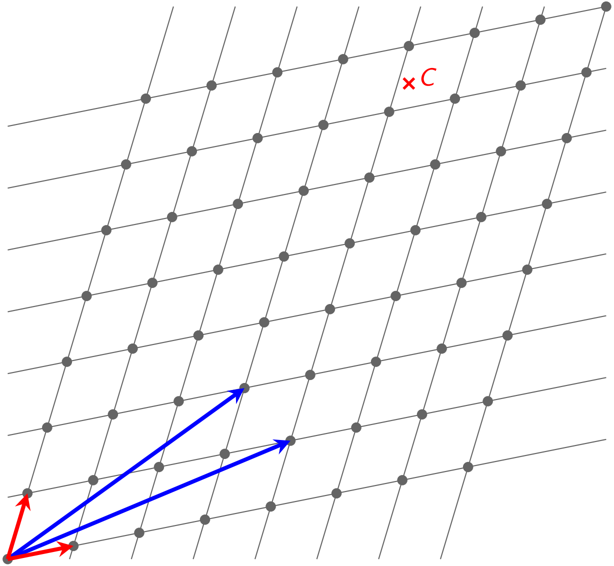
Signature Process

HASH

APPROX-CVP$_\gamma$

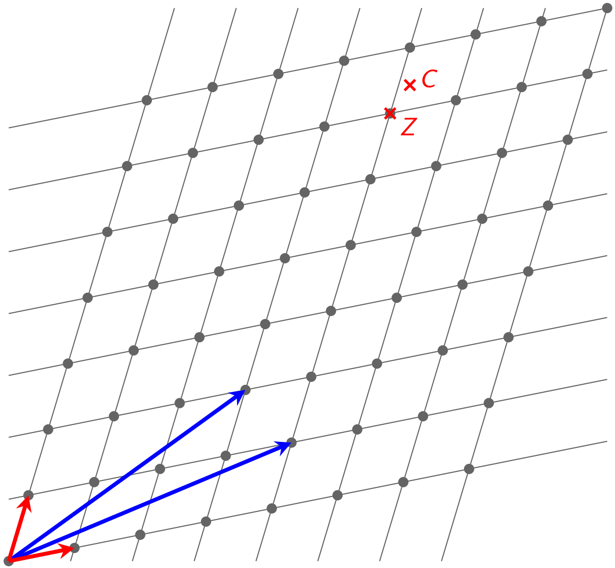
SAMPLING

CENTERED



Signature Process

- HASH
- **APPROX-CVP$_\gamma$**
- SAMPLING
- CENTERED



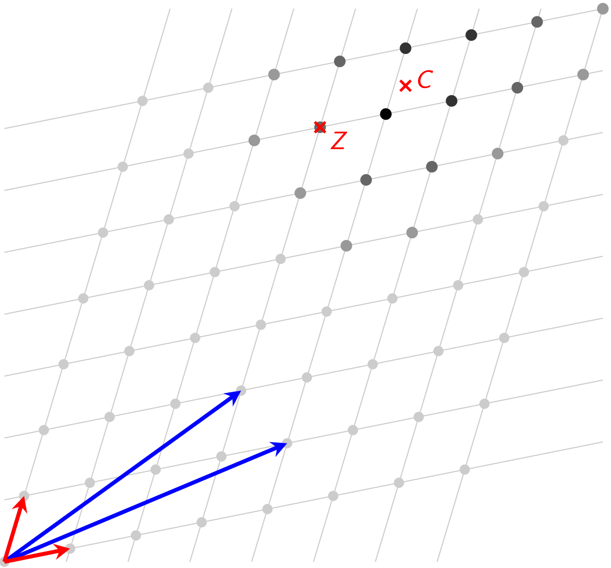
Signature Process

HASH

APPROX-CVP$_\gamma$

SAMPLING

CENTERED



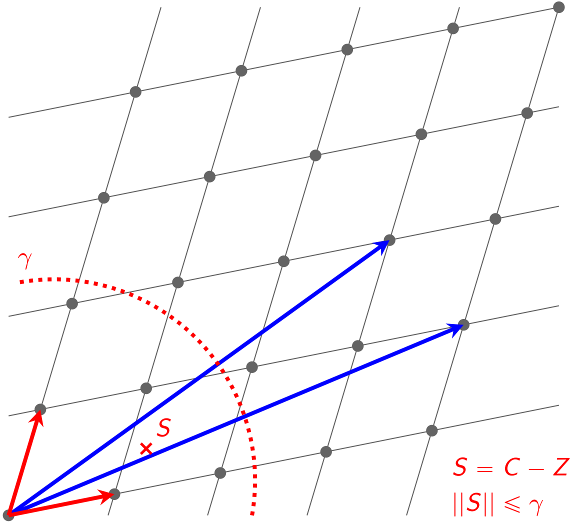
Signature Process

HASH

APPROX-CVP$_\gamma$

SAMPLING

CENTERED



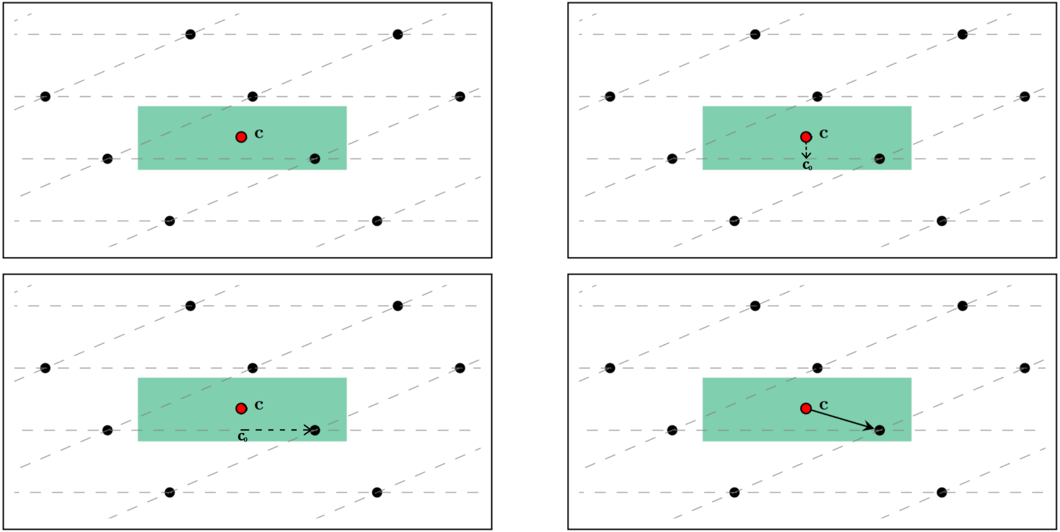
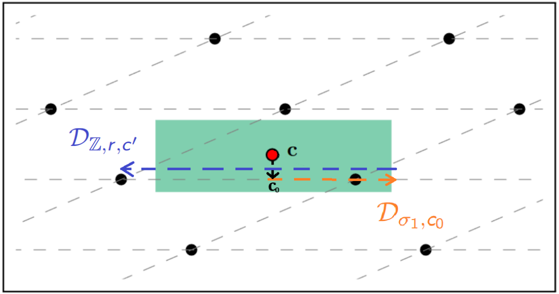
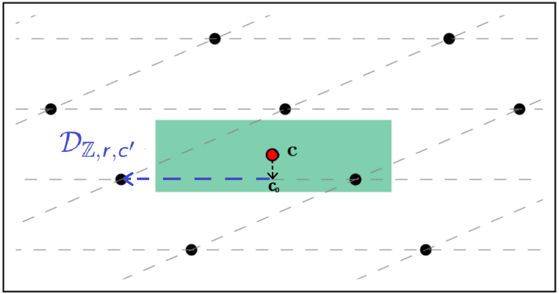


Image credits: Thomas Prest

Mitaka



Falcon



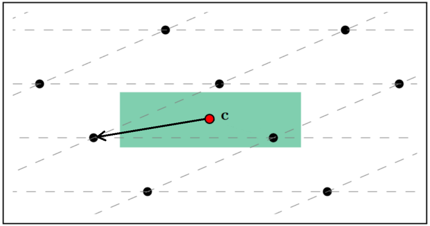
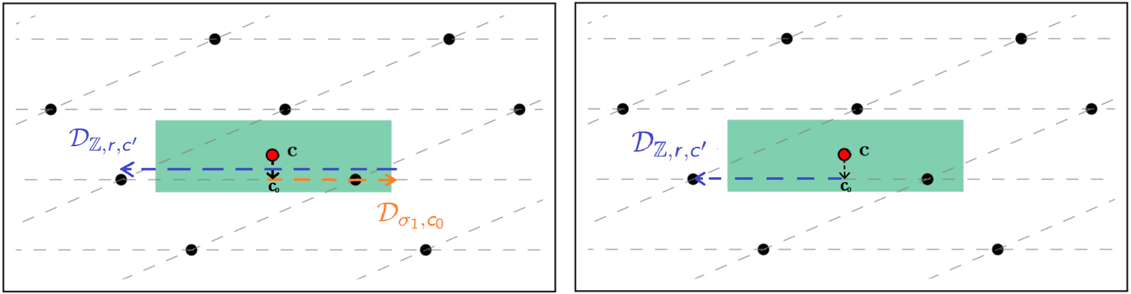
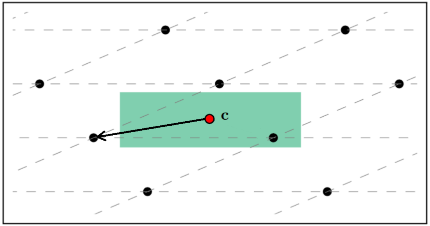


Image credits: Thomas Prest

Mitaka

Falcon





Works well but $\mathcal{D}_{\mathbb{Z},r,c}$ represents a major leak in side-channel.

Image credits: Thomas Prest

Previous Known Attacks

2

Side Channel Attack

Theoretical Attack on the Masking Scheme

Previous Known Attacks

2

› Side Channel Attack

Theoretical Attack on the Masking Scheme

Half Gaussian Leakage

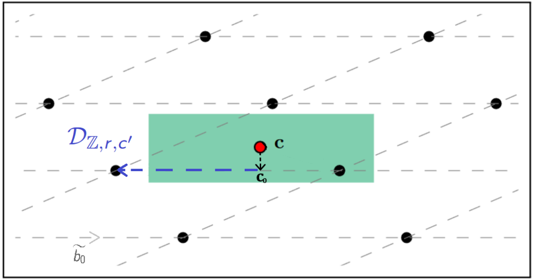
The attack targets the sampling in the direction of $\widetilde{b_0} = b_0 = \begin{pmatrix} f \\ g \end{pmatrix}$.

Half Gaussian Leakage

The attack targets the sampling in the direction of $\widetilde{b_0} = b_0 = \begin{pmatrix} f \\ g \end{pmatrix}$.

$$\left[\begin{array}{cccc|cccc} f_0 & -f_{n-1} & \dots & -f_1 & F_0 & -F_{n-1} & \dots & -F_1 \\ f_1 & f_0 & \dots & -f_2 & F_1 & F_0 & \dots & F_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ f_{n-1} & f_{n-2} & \dots & f_0 & F_{n-1} & F_{n-2} & \dots & F_0 \\ \hline g_0 & -g_{n-1} & \dots & -g_1 & G_0 & -G_{n-1} & \dots & -G_1 \\ g_1 & g_0 & \dots & -g_2 & G_1 & G_0 & \dots & -G_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{n-1} & g_{n-2} & \dots & g_0 & G_{n-1} & G_{n-2} & \dots & G_0 \end{array}\right]$$

Sign Leakage

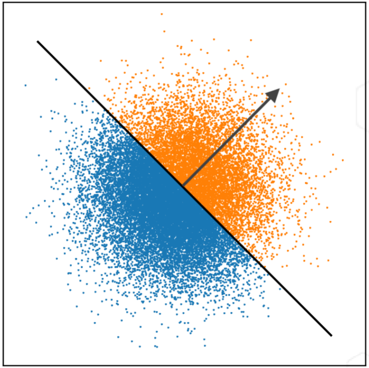


$$S = C - Z$$

Image credits: Thomas Prest

Sign Leakage

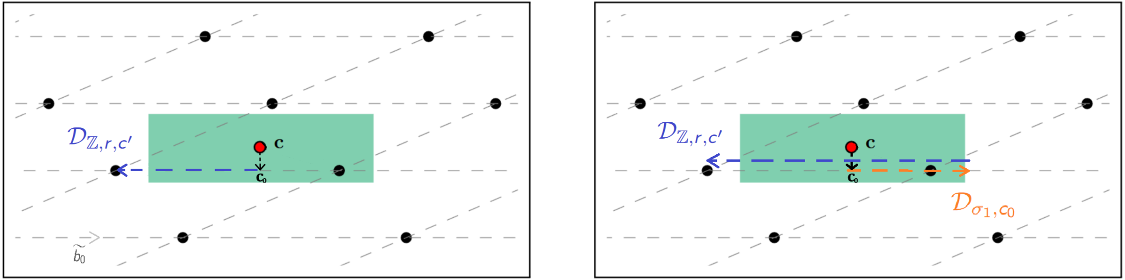
According to the sign the authors can split a set of signatures in two.



Falcon

Image credits: [ZLYW23]

Sign Leakage

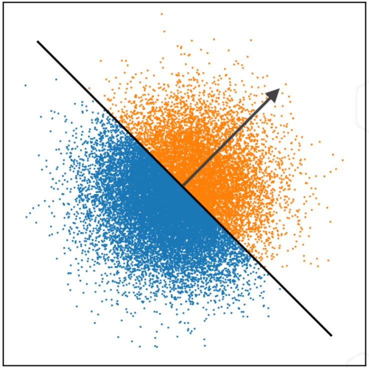


$$S = C - Z$$

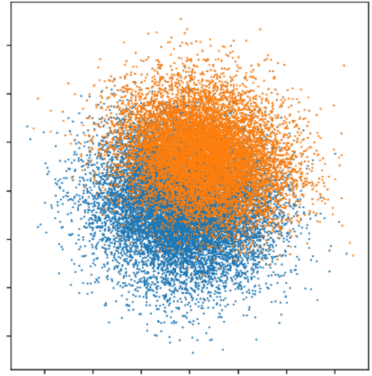
Image credits: Thomas Prest

Sign Leakage

According to the sign, the authors can split a set of signatures in two.



Falcon



Mitaka

Image credits: [ZLYW23]

Previous Known Attacks

2

Side Channel Attack

› Theoretical Attack on the Masking Scheme

The Generation

Secure Mitaka uses an arithmetically masked gaussian generation.

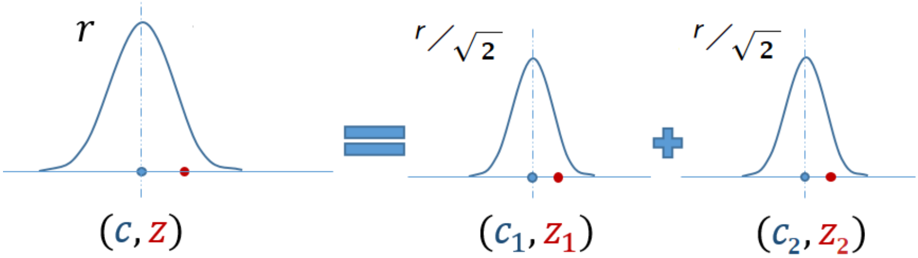


Image credits: Quyen Nguyen

The Generation

However, Prest [Pre23] broke the security proof for masking order $t \geqslant 3$.

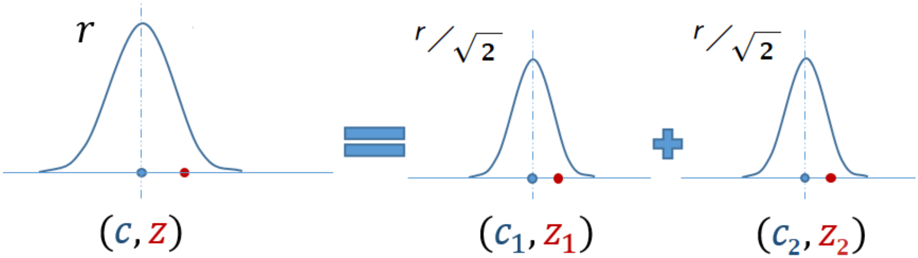


Image credits: Quyen Nguyen

Our Attack and Improvements

3

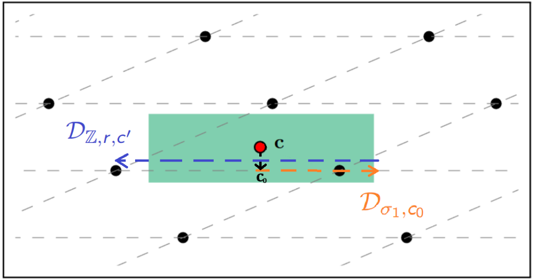
Our Practical Attack on the Masking Scheme
Reducing the Number of Traces
Countermeasures

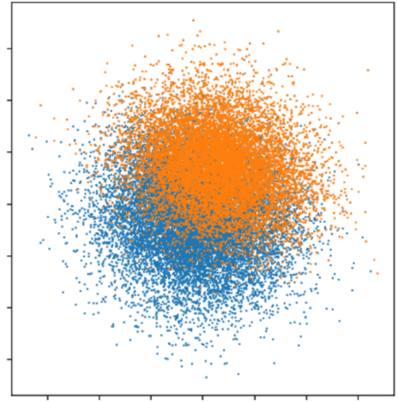
Our Attack and Improvements

3

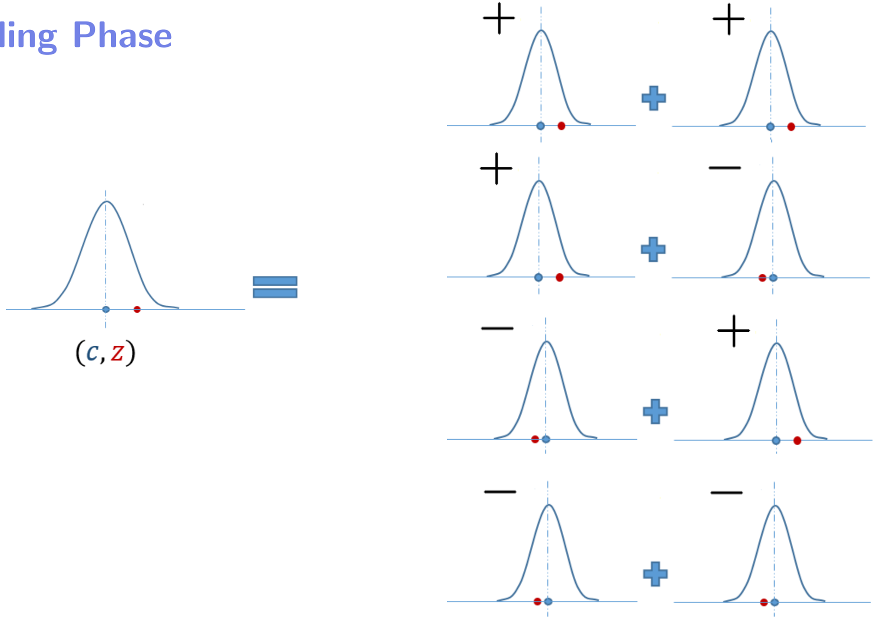
- Our Practical Attack on the Masking Scheme
- Reducing the Number of Traces
- Countermeasures

Sign Leakage

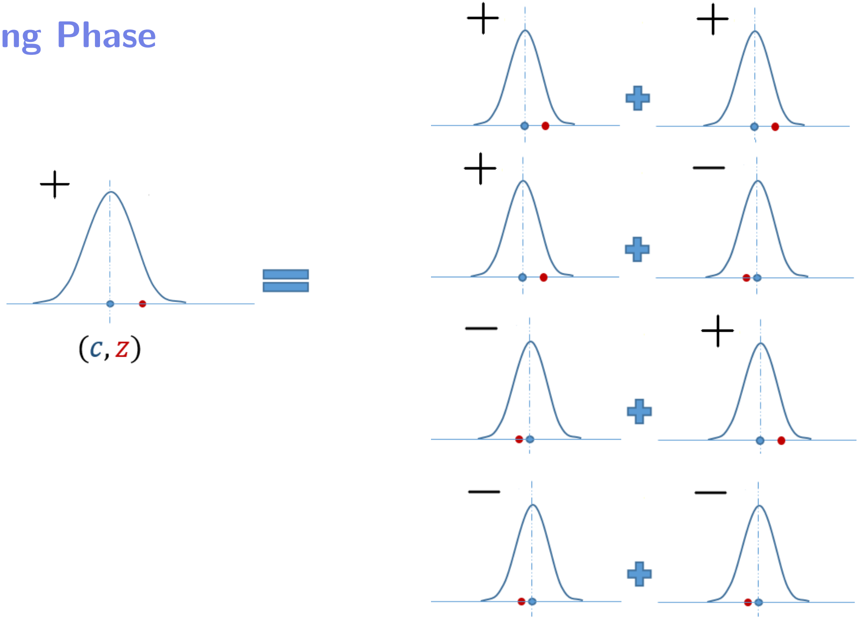




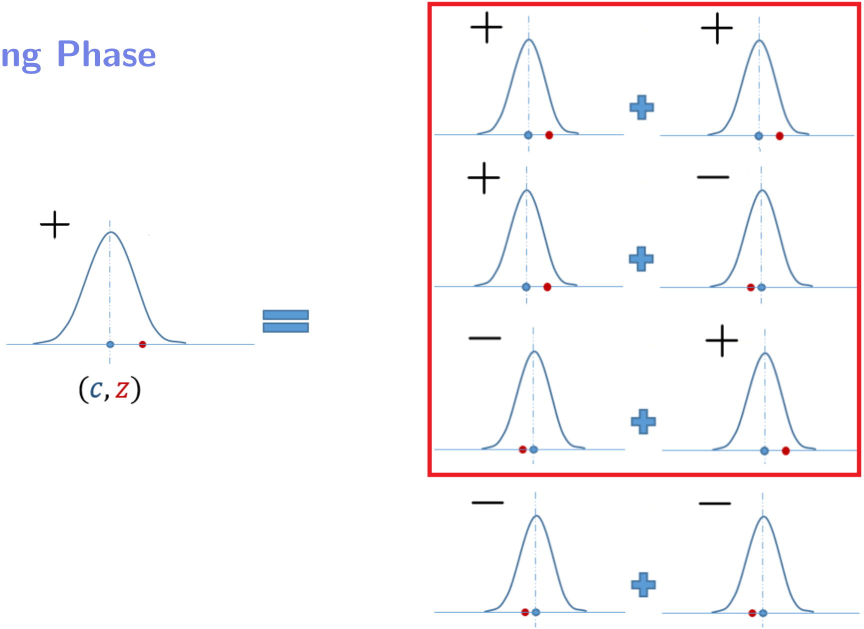
Building Phase



Building Phase



Building Phase



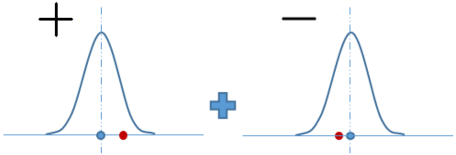
Building Phase

Leveraging this bias and other optimization, we construct a first order template.

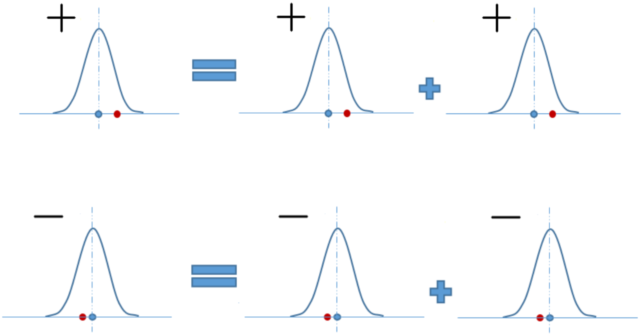
Building Phase

Leveraging this bias and other optimization, we construct a first order template.

We can use this template for every shares.



Matching Phase



We recover the sign of roughly half of the signature.

Our Attack and Improvements

3

- Our Practical Attack on the Masking Scheme
- › Reducing the Number of Traces
- Countermeasures

Structure of $\tilde{B}$

The orthogonal basis used for the projections in Mitaka.

$$
\widetilde{B} = \left[\begin{array}{cccc|cccc}
f_0 & -f_{n-1} & \dots & -f_1 & \widetilde{b}_{1,0} & -\widetilde{b}_{1,n-1} & \dots & -\widetilde{b}_{1,1} \\
f_1 & f_0 & \dots & -f_2 & \widetilde{b}_{1,1} & \widetilde{b}_{1,0} & \dots & -\widetilde{b}_{1,2} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
f_{n-1} & f_{n-2} & \dots & f_0 & \widetilde{b}_{1,n-1} & \widetilde{b}_{1,n-1} & \dots & \widetilde{b}_{1,0} \\
\hline
g_0 & -g_{n-1} & \dots & -g_1 & \widetilde{b}_{1,n} & -\widetilde{b}_{1,2n-1} & \dots & -\widetilde{b}_{1,n+1} \\
g_1 & g_0 & \dots & -g_2 & \widetilde{b}_{1,n+1} & \widetilde{b}_{1,n} & \dots & -\widetilde{b}_{1,n+2} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
g_{n-1} & g_{n-2} & \dots & g_0 & \widetilde{b}_{1,2n-1} & \widetilde{b}_{1,2n-2} & \dots & \widetilde{b}_{1,n}
\end{array}\right]
$$

Structure of $\tilde{B}$

Unlike Falcon, in Mitaka 512 passages leak information.

$$
\widetilde{B} = \left[\begin{array}{cccc|cccc}
f_0 & -f_{n-1} & \dots & -f_1 & \widetilde{b}_{1,0} & -\widetilde{b}_{1,n-1} & \dots & -\widetilde{b}_{1,1} \\
f_1 & f_0 & \dots & -f_2 & \widetilde{b}_{1,1} & \widetilde{b}_{1,0} & \dots & -\widetilde{b}_{1,2} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
f_{n-1} & f_{n-2} & \dots & f_0 & \widetilde{b}_{1,n-1} & \widetilde{b}_{1,n-1} & \dots & \widetilde{b}_{1,0} \\
\hline
g_0 & -g_{n-1} & \dots & -g_1 & \widetilde{b}_{1,n} & -\widetilde{b}_{1,2n-1} & \dots & -\widetilde{b}_{1,n+1} \\
g_1 & g_0 & \dots & -g_2 & \widetilde{b}_{1,n+1} & \widetilde{b}_{1,n} & \dots & -\widetilde{b}_{1,n+2} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
g_{n-1} & g_{n-2} & \dots & g_0 & \widetilde{b}_{1,2n-1} & \widetilde{b}_{1,2n-2} & \dots & \widetilde{b}_{1,n}
\end{array}\right]
$$

Structure of $\tilde{B}$

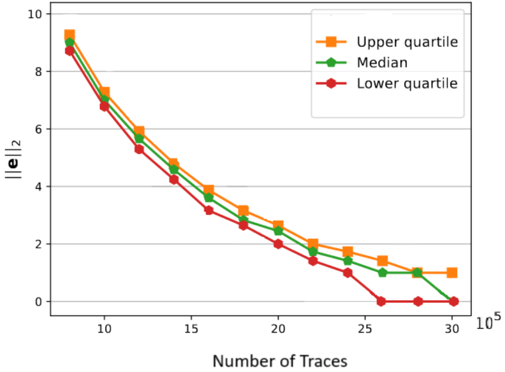
Unlike Falcon, in Mitaka 512 passages leak information.

$$\widetilde{B} = \left[\begin{array}{cccc|cccc}
f_0 & -f_{n-1} & \cdots & -f_1 & \widetilde{b}_{1,0} & -\widetilde{b}_{1,n-1} & \cdots & -\widetilde{b}_{1,1} \\
f_1 & f_0 & \cdots & -f_2 & \widetilde{b}_{1,1} & \widetilde{b}_{1,0} & \cdots & -\widetilde{b}_{1,2} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
f_{n-1} & f_{n-2} & \cdots & f_0 & \widetilde{b}_{1,n-1} & \widetilde{b}_{1,n-1} & \cdots & \widetilde{b}_{1,0} \\
\hline
g_0 & -g_{n-1} & \cdots & -g_1 & \widetilde{b}_{1,n} & -\widetilde{b}_{1,2n-1} & \cdots & -\widetilde{b}_{1,n+1} \\
g_1 & g_0 & \cdots & -g_2 & \widetilde{b}_{1,n+1} & \widetilde{b}_{1,n} & \cdots & -\widetilde{b}_{1,n+2} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
g_{n-1} & g_{n-2} & \cdots & g_0 & \widetilde{b}_{1,2n-1} & \widetilde{b}_{1,2n-2} & \cdots & \widetilde{b}_{1,n}
\end{array}\right]$$

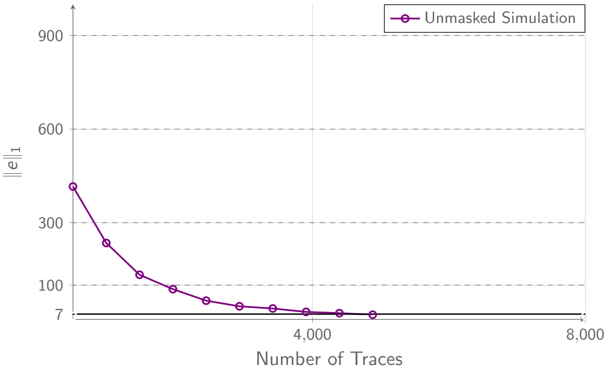
$\Rightarrow$ Divided by 512 the number of traces.

Experimental Results

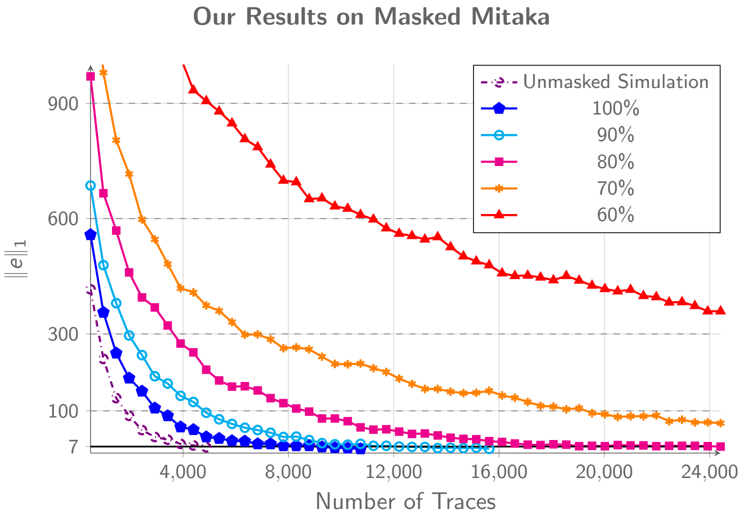
Previous Result [ZLYW23]



Our Results on Unmasked Mitaka



Experimental Results



Our Attack and Improvements

3

- Our Practical Attack on the Masking Scheme
- Reducing the Number of Traces
- › Countermeasures

Countermeasures

Shuffle the calls to the sampler

$$\left[\begin{array}{cccc|cccc}
f_0 & -f_{n-1} & \cdots & -f_1 & \widetilde{b}_{1,0} & -\widetilde{b}_{1,n-1} & \cdots & -\widetilde{b}_{1,1} \\
f_1 & f_0 & \cdots & -f_2 & \widetilde{b}_{1,1} & \widetilde{b}_{1,0} & \cdots & -\widetilde{b}_{1,2} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
f_{n-1} & f_{n-2} & \cdots & f_0 & \widetilde{b}_{1,n-1} & \widetilde{b}_{1,n-2} & \cdots & \widetilde{b}_{1,0} \\
\hline
g_0 & -g_{n-1} & \cdots & -g_1 & \widetilde{b}_{1,n} & -\widetilde{b}_{1,2n-1} & \cdots & -\widetilde{b}_{1,n+1} \\
g_1 & g_0 & \cdots & -g_2 & \widetilde{b}_{1,n+1} & \widetilde{b}_{1,n} & \cdots & -\widetilde{b}_{1,n+2} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
g_{n-1} & g_{n-2} & \cdots & g_0 & \widetilde{b}_{1,2n-1} & \widetilde{b}_{1,2n-2} & \cdots & \widetilde{b}_{1,n}
\end{array}\right]$$

Countermeasures

(1)
Shuffle the calls to the sampler

$$\left[\begin{array}{cccc|cccc}
f_0 & -f_{n-1} & \cdots & -f_1 & \widetilde{b}_{1,0} & -\widetilde{b}_{1,n-1} & \cdots & -\widetilde{b}_{1,1} \\
f_1 & f_0 & \cdots & -f_2 & \widetilde{b}_{1,1} & \widetilde{b}_{1,0} & \cdots & -\widetilde{b}_{1,2} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
f_{n-1} & f_{n-2} & \cdots & f_0 & \widetilde{b}_{1,n-1} & \widetilde{b}_{1,n-2} & \cdots & \widetilde{b}_{1,0} \\
\hline
g_0 & -g_{n-1} & \cdots & -g_1 & \widetilde{b}_{1,n} & -\widetilde{b}_{1,2n-1} & \cdots & -\widetilde{b}_{1,n+1} \\
g_1 & g_0 & \cdots & -g_2 & \widetilde{b}_{1,n+1} & \widetilde{b}_{1,n} & \cdots & -\widetilde{b}_{1,n+2} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
g_{n-1} & g_{n-2} & \cdots & g_0 & \widetilde{b}_{1,2n-1} & \widetilde{b}_{1,2n-2} & \cdots & \widetilde{b}_{1,n}
\end{array}\right]$$

(2)
Constant time implementation for rejection

Conclusion
4

Conclusion

- We adapted the theoretical attack of Prest with $t \geqslant 3$ to a practical attack with $t \geqslant 1$.

Conclusion

- We adapted the theoretical attack of Prest with $t \geqslant 3$ to a practical attack with $t \geqslant 1$.

- We identified a new leakages on a unstudied sampler.

Conclusion

- We adapted the theoretical attack of Prest with $t \geqslant 3$ to a practical attack with $t \geqslant 1$.
- We identified a new leakages on a unstudied sampler.
- We divided by 512 the number of traces required.

Conclusion

- We adapted the theoretical attack of Prest with $t \geqslant 3$ to a practical attack with $t \geqslant 1$.
- We identified a new leakages on a unstudied sampler.
- We divided by 512 the number of traces required.
- We presented new specific countermeasures.