

# Fault Attack on PLL-TRNG: Randomness Degradation through Clock Glitch-Induced PLL Perturbation

**Hikaru Nishiyama**<sup>\*</sup>, Daisuke Fujimoto<sup>†</sup>  
Shinichi Kawamura<sup>\*</sup>, Yuichi Hayashi<sup>†</sup>

<sup>\*</sup> National Institute of Advanced Industrial Science and Technology (AIST), Japan

<sup>†</sup> Nara Institute of Science and Technology (NAIST), Japan

NATIONAL INSTITUTE OF  
ADVANCED  
INDUSTRIAL  
SCIENCE &  
TECHNOLOGY

## 1: CW-based Fault Attack on PLL-TRNG

- CW(Continuous Wave) injection into the external PLL input clock degrades PLL-TRNG randomness without timing synchronization.

## 2: PLL Bandwidth-dependent Robustness

- PLL bandwidth affects both nominal randomness and susceptibility to CW injection.

## 3: Differential PLL Responses

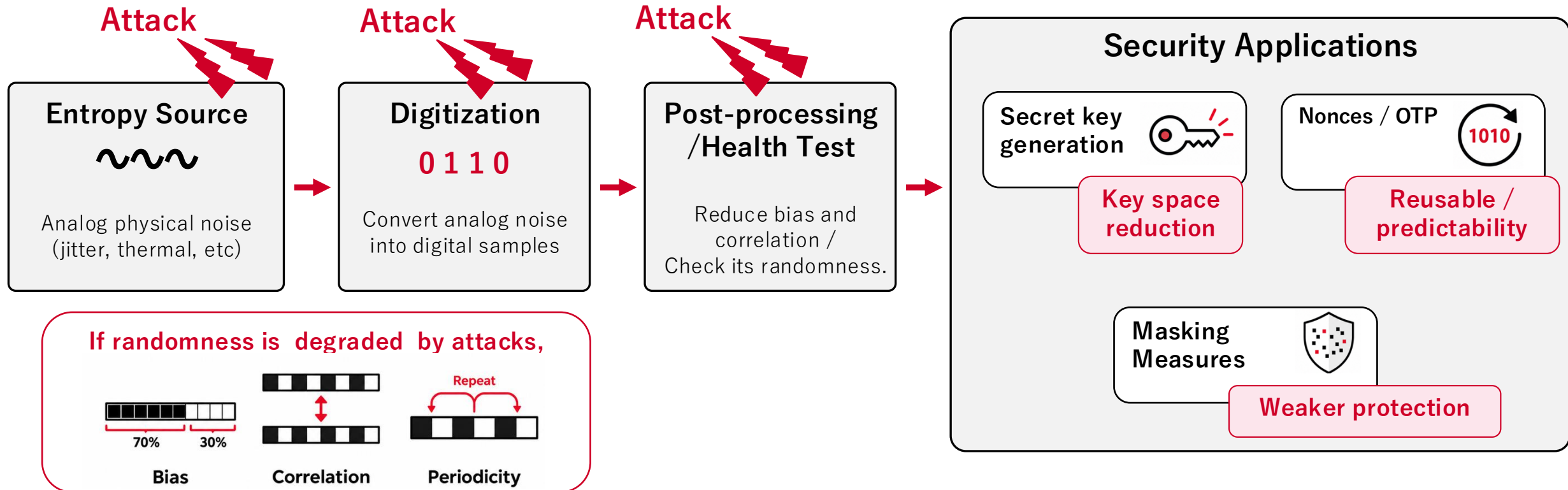
- The two PLLs respond differently to the same input-clock disturbance.

## 4: Experimental Validation and Quantitative Characterization

- Large output-frequency shifts are strongly associated with entropy degradation, but frequency shift alone is not a complete indicator.

.

# True Random Number Generators (TRNGs) and Physical Attacks



TRNGs provide unpredictable values for:

- Secret key generation
- Nonces and initialization vectors
- Masking against side-channel attacks etc.



Degraded randomness can directly weaken cryptographic security.

- introduce **bias**, increase **correlation**,
- generate **periodic patterns**
- reduce the effective entropy of the output.

# Why PLL-TRNGs?

## PLL-TRNG features:

- Low implementation cost
- High Throughput
- Compatibility with **stochastic models**
- Flexible optimization through PLL parameters etc.

## Commercial relevance:

- **Thales Aquarius PTRNG**  
Two PLL outputs used as a physical entropy source  
*NIST SP 800-90B E144*
- **AMD Versal TRNG**  
PLL random sources  
*AMD Versal TRM, AM011*

## PLL-TRNG Research:

:Design  :Optimization  
 :Attacks  :Physical Model

[4] Fischer et al.  
**CHES 2002**  
First Proposal of  
PLL-TRNG

[16] Simka et al.,  
**Radioeng. 2011**  
Evaluate the effect  
of temperature

[10] Allini et al.  
**DATE 2018**  
Improving  
Optimization of  
PLL Parameters

[11] Colombier et al.  
**DATE 2020**  
Backtracking Search  
of PLL Parameters

[12] Ma et al.,  
**TCHES 2025**  
Improved  
Stochastic  
models

### Design, optimization, physical modeling of PLL-TRNGs and Attacks

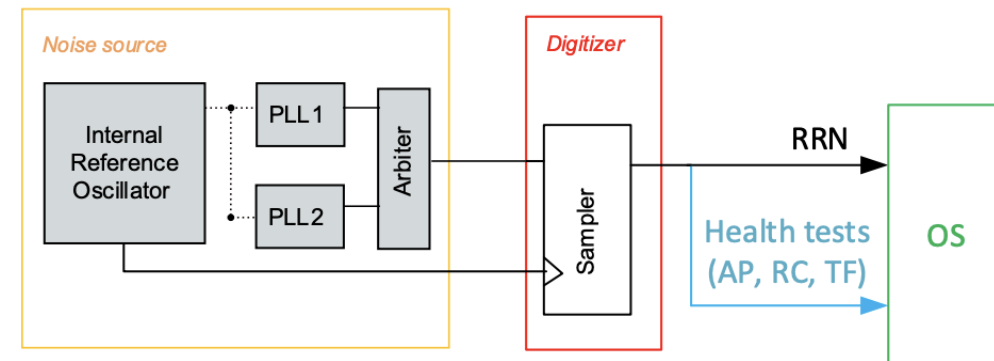
[5] Fischer et al.  
**CHES 2004**  
High-speed  
FPGA design

[9] Petura et al.  
**ISCAS 2017**  
Genetic  
Optimization of  
PLL Parameters

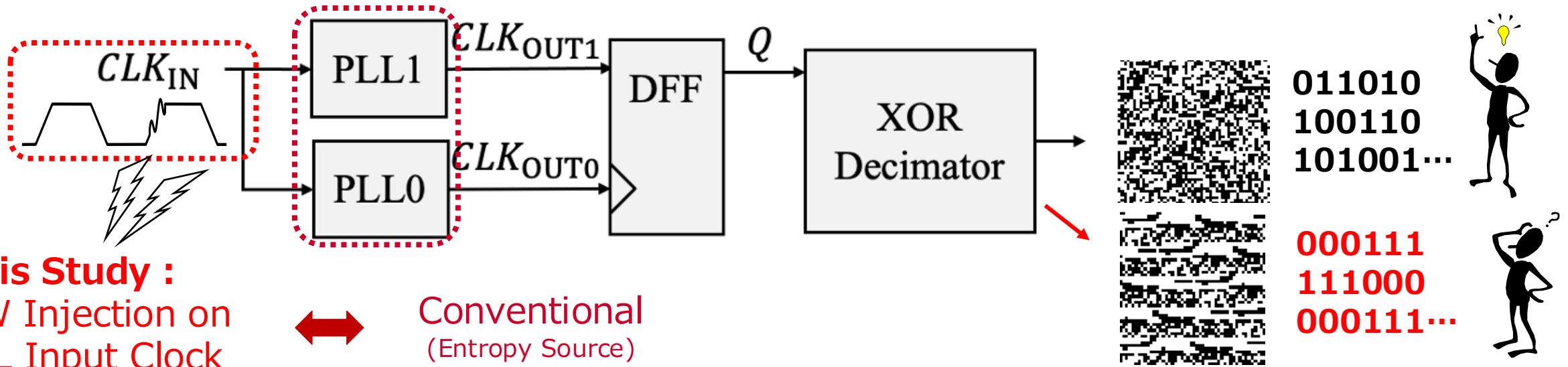
[7] Fischer et al.  
**Inf. Tech. 2019**  
Case study of  
Implementations

[8] Fischer et al.  
**TCHES 2023**  
Proposal of  
Stochastic models

**This work**  
**FDTC 2026**  
Fault attack using  
CW Injection on  
PLL-TRNG.



# PLL is hardwired, but the input clock path is exposed.



## PLLs are considered robust :

- ✓ Dedicated hardwired blocks
- ✓ Physical separation from configurable logic
- ✓ Reduced direct coupling from surrounding circuitry



## Research Question

How do external clock perturbations degrade PLL-TRNG randomness?

## Research Objective

To investigate whether perturbations injected through the external PLL input clock can degrade the randomness of a PLL-TRNG.

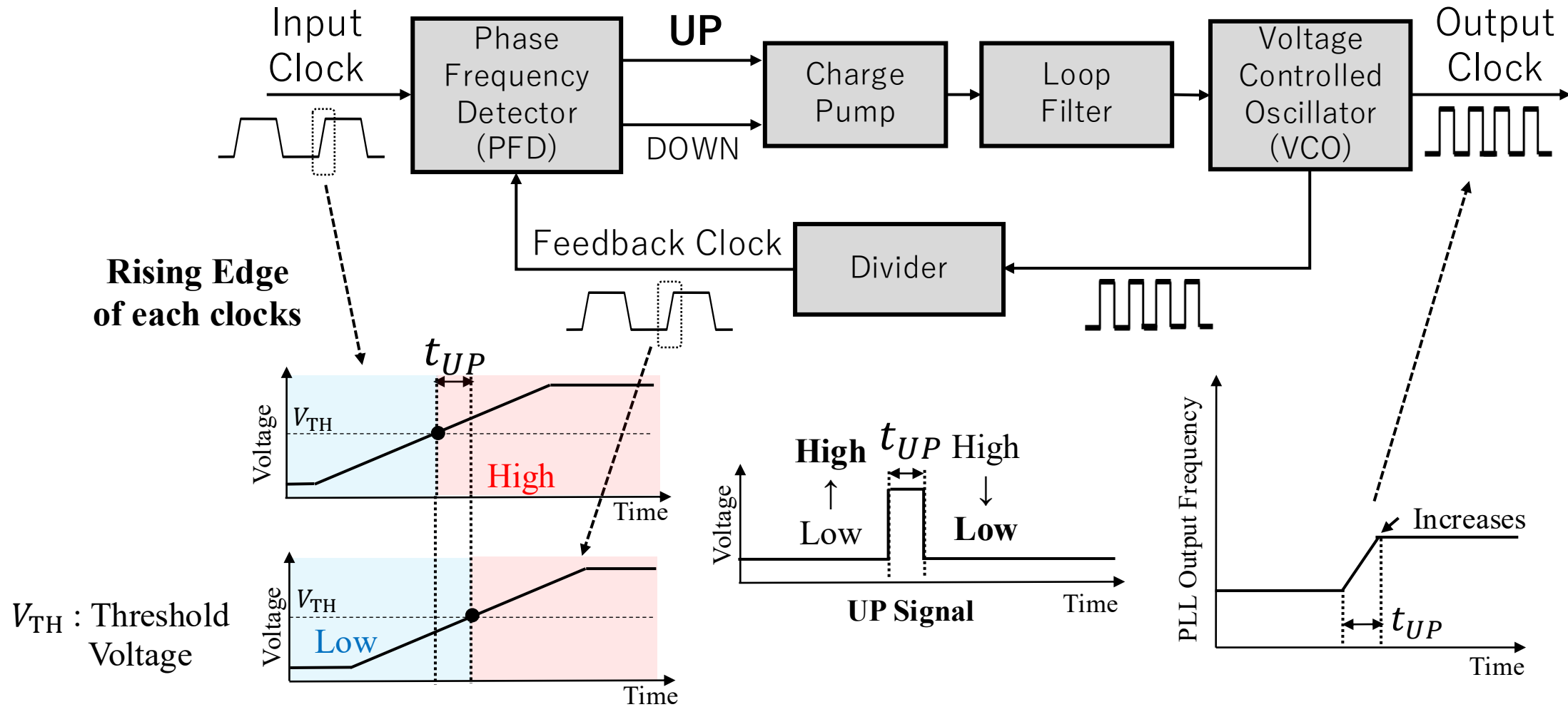
## Contributions

We identify the externally supplied PLL input-clock path as a potential attack surface of PLL-TRNGs.

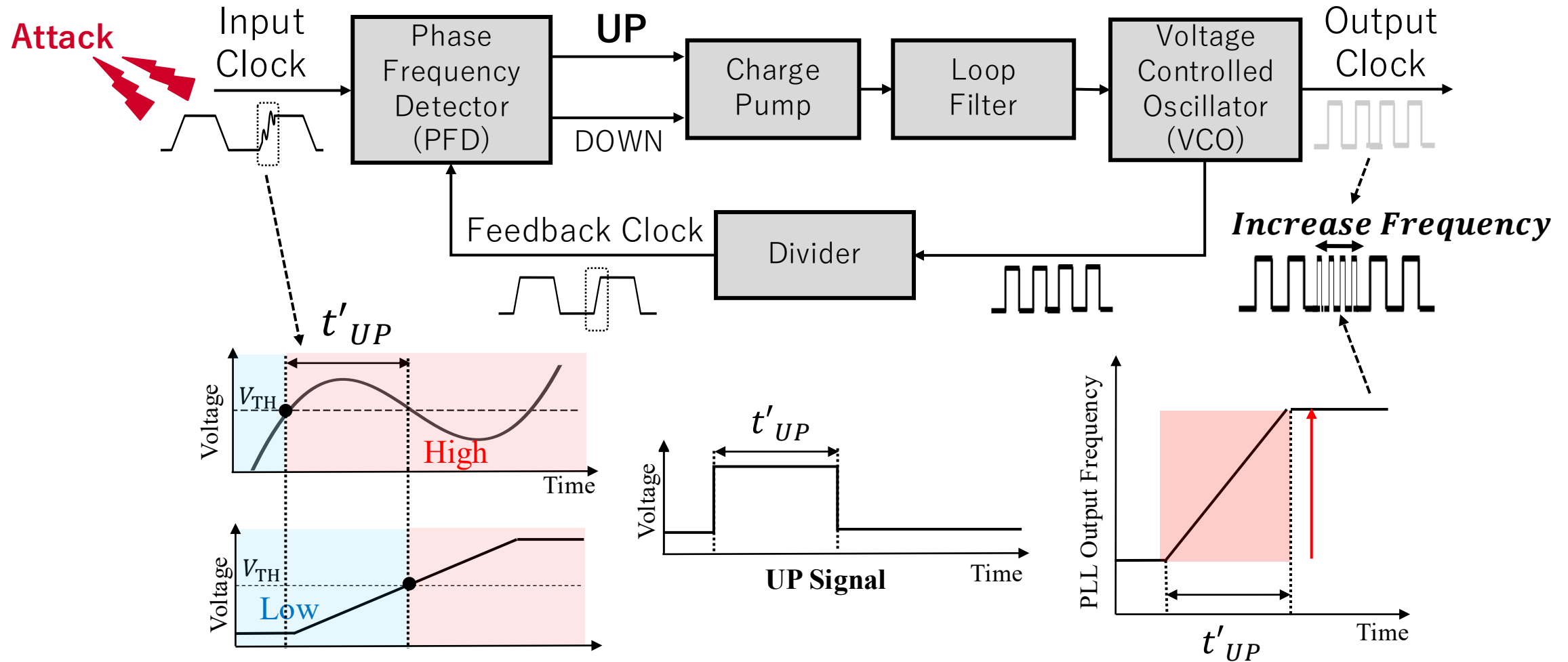
We propose a method to superimpose a CW signal to induce timing perturbations at the PLL input without synchronization to random-number generation.

We experimentally demonstrate randomness degradation and investigate the relationship between measured PLL output-frequency and estimated min-entropy.

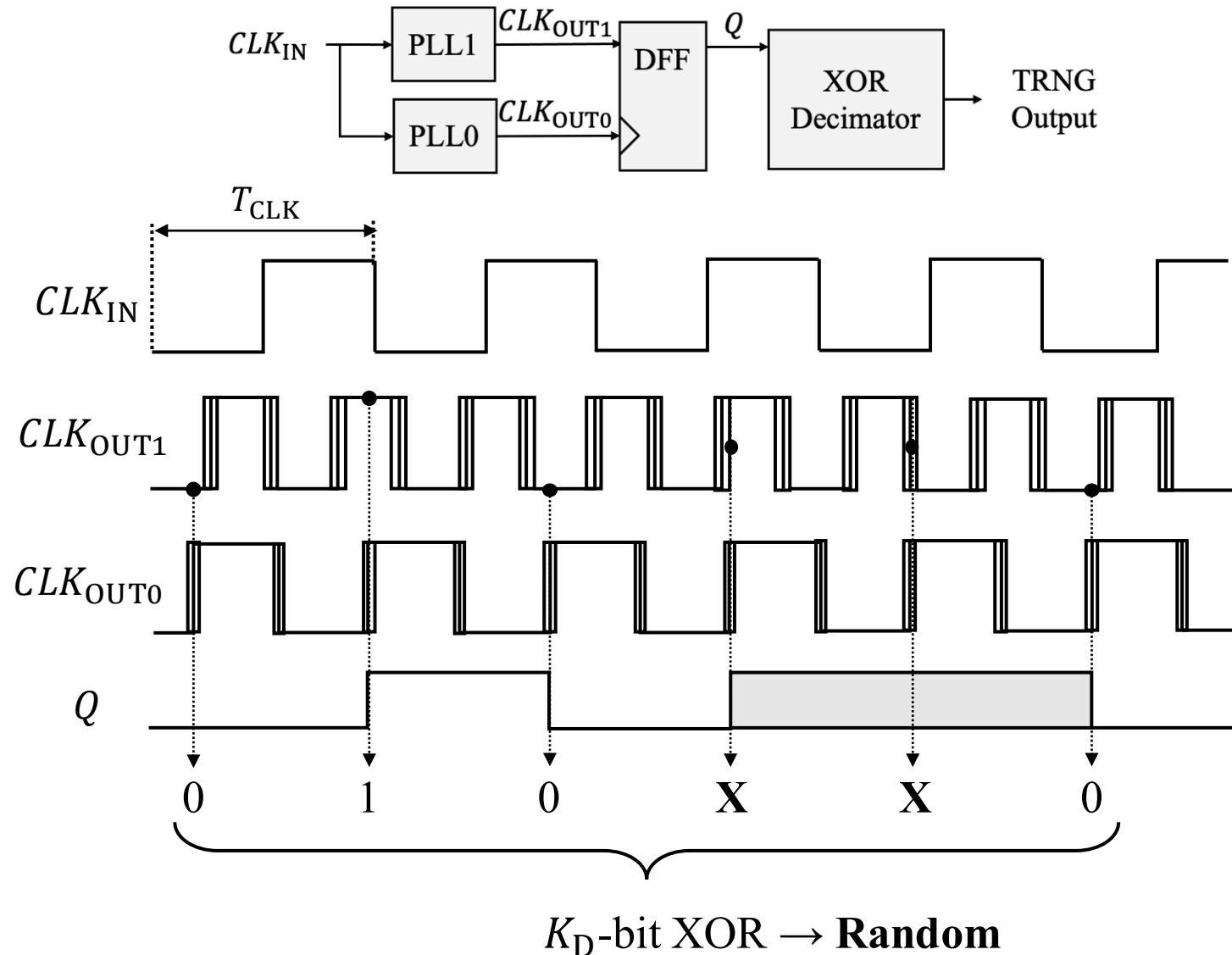
# Basics of PLL Operation



# Input-Clock Timing Perturbation Can Disturb PLL Control

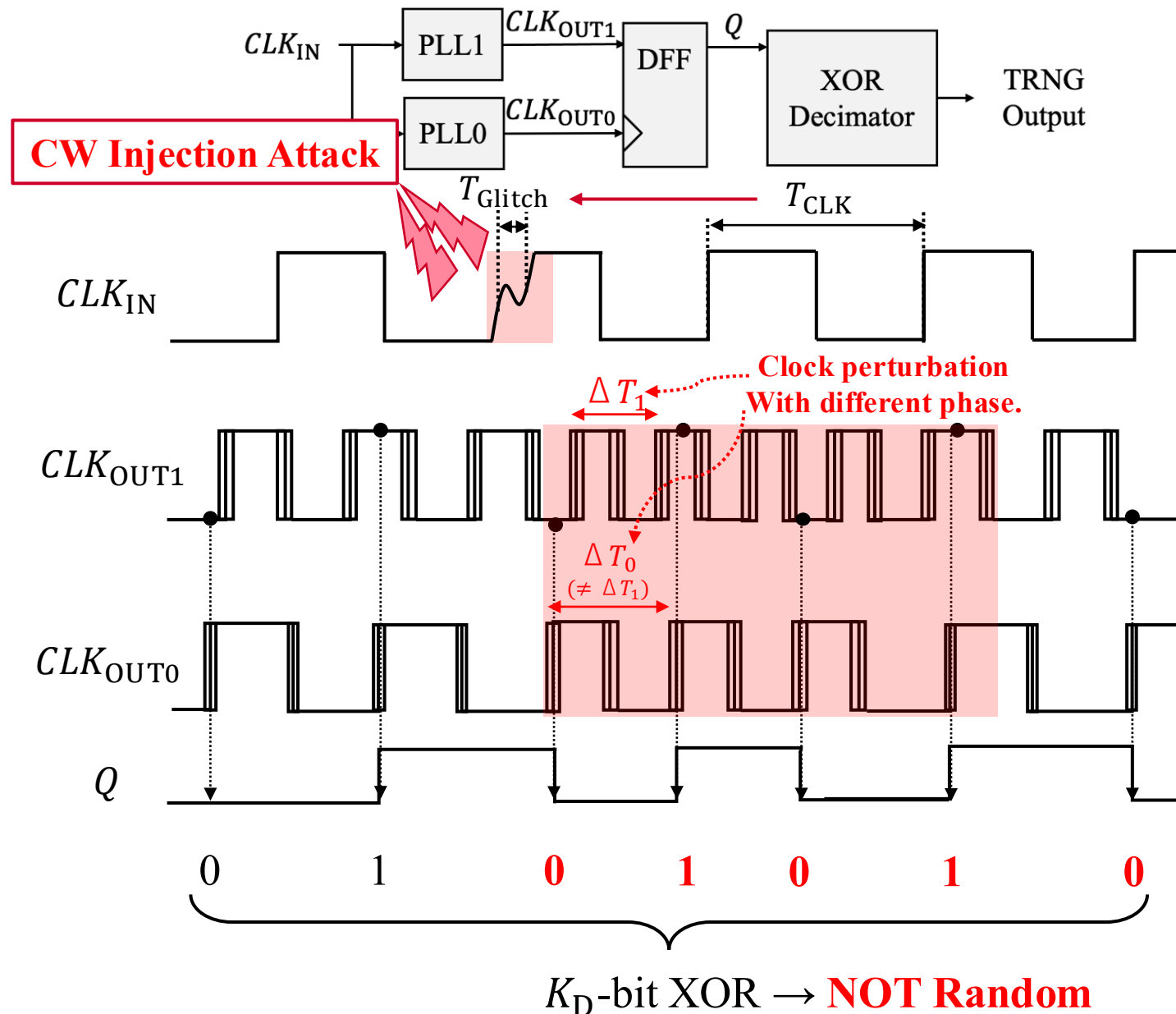


# Basics of Random Number Generation by PLL-TRNG



- The two PLL output frequencies are designed to satisfy a rational frequency relationship.
- Most sampling points are deterministic, while samples close to  $CLK_{OUT1}$  transitions become probabilistic due to PLL jitter.
- These probabilistic samples are called **contributors (X)**.  
(Entropy of the PLL-TRNG)

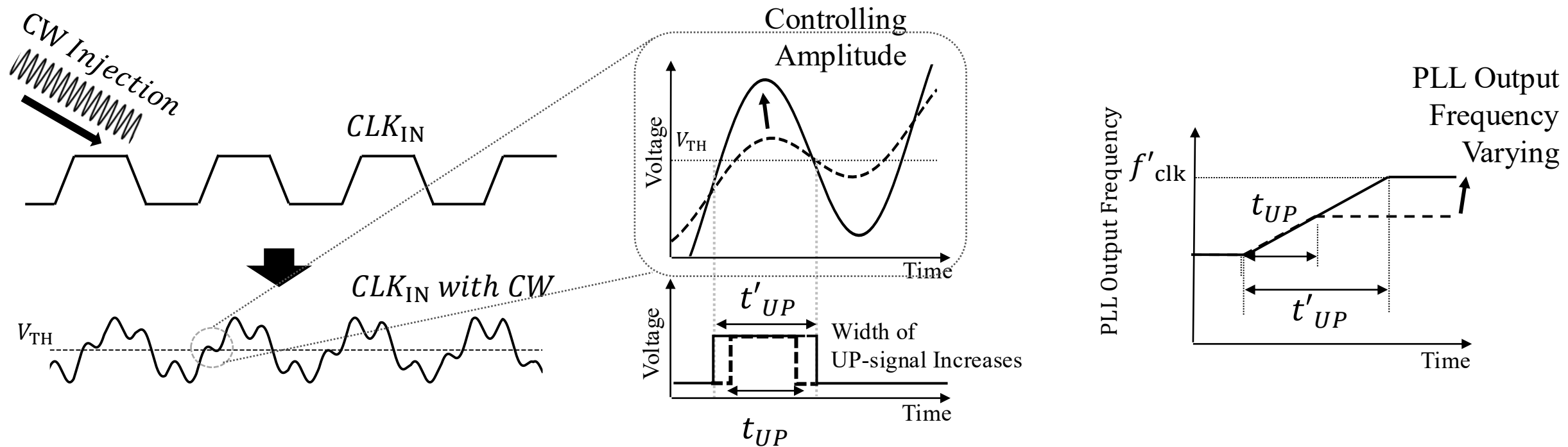
# How Does CW Injection Create a PLL Output Clock Perturbation?



## Proposed attack mechanism:

1. A CW-induced timing perturbation is applied to the **common PLL input clock**.
2. PLL0 and PLL1 have **different multiplication/division parameters** and loop dynamics.  
→ Common input disturbance  
**Different output perturbations**
3. The number of effective contributors (X) may be reduced.  
→ **Randomness Degradation**

# How Do CW Frequency and Amplitude Affect PLL Perturbation?



**CW Frequency** : Determines when and how often effective threshold crossings occur [23].

**CW Amplitude** : Sufficient amplitude is required to create effective threshold crossings.

**Control both CW injection frequency and amplitude to identify the conditions that maximize randomness degradation.**

## Target

- PLL-TRNG driven by an externally supplied clock

## Attack Goal

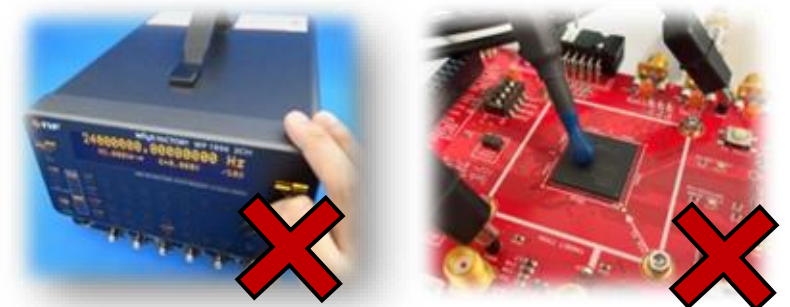
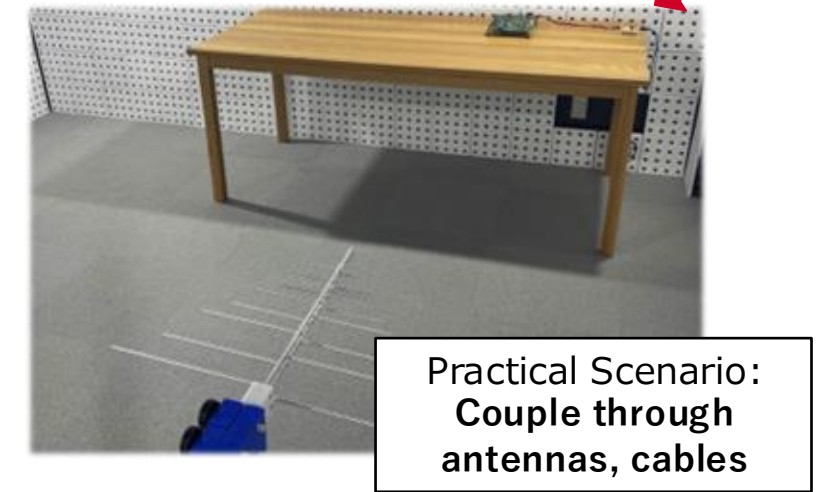
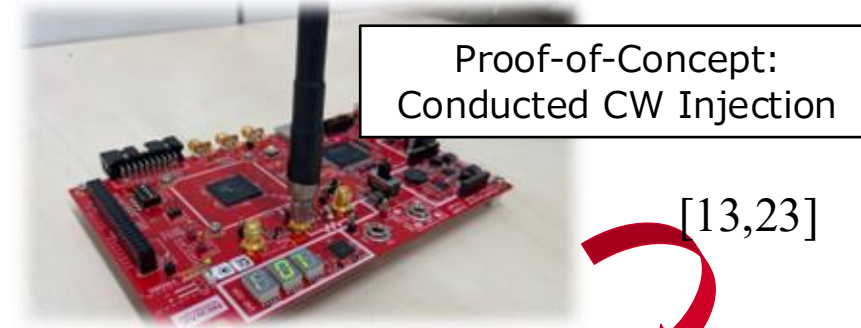
- Degrade randomness of output bits
  - Bias, correlation or periodical patterns.

## Attacker Capability

- Couple CW disturbance into the external clock path  
( e.g. power cables [13] or antenna [23] )
- Sweep CW frequency and amplitude

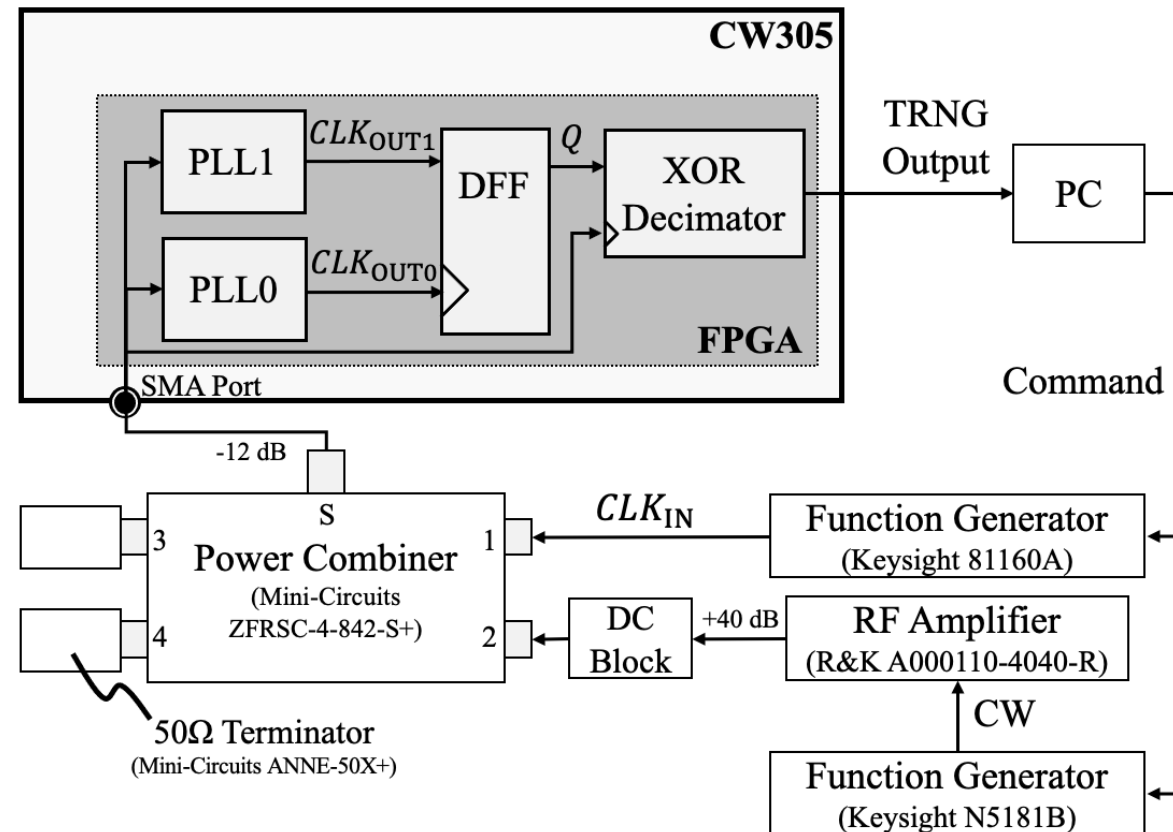
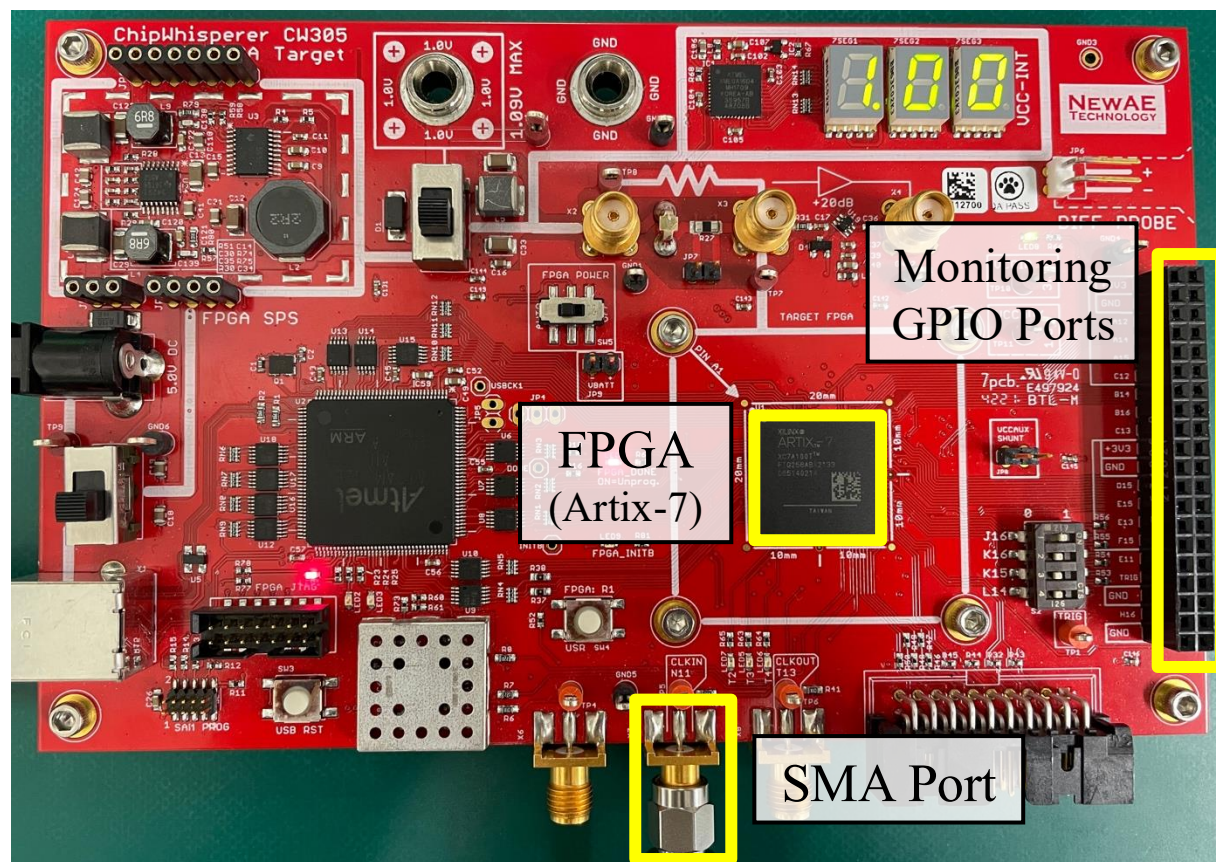
## Not Required for Attack

- Internal TRNG process / state
- Synchronization with random-number generation
- FPGA modification/destruction



[13] H. Nishiyama et al., IEEE TEMC 2024. [23] H. Nishiyama et al., JCEN, 2025.

# PLL-TRNG Implementation & Experimental Setup



**Platform:** ChipWhisperer CW305 (AMD Artix-7 FPGA) , Two PLLE2 primitives

**BANDWIDTH settings:** PLLE2 settings (OPTIMIZED/LOW/HIGH)

**PLL Parameters [10]:**

[10] Allini et al. DATE 2018

| $(M_0, N_0, C_0)$ | $(M_1, N_1, C_1)$ | $K_M$ | $K_D$ | Valid $f_{\text{ref}}$ [MHz] |
|-------------------|-------------------|-------|-------|------------------------------|
| (33, 2, 4)        | (62, 3, 5)        | 496   | 495   | 57.00–90.29                  |

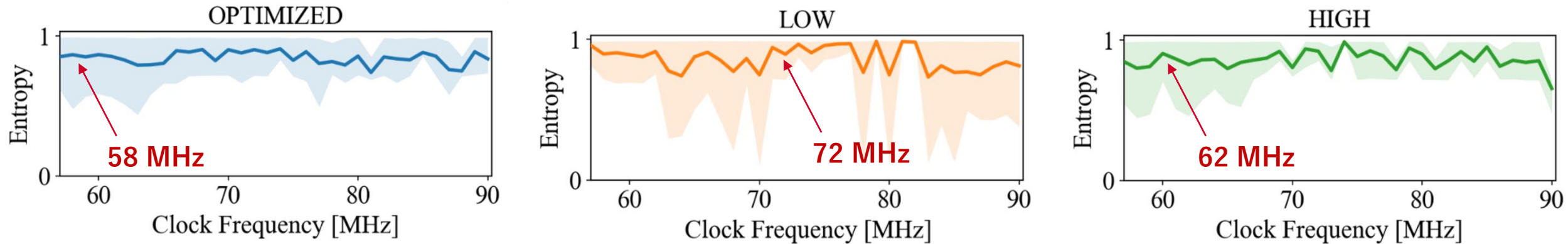
**Injected CW Parameters:**

Frequency : 10–250 MHz, 1-MHz step

Power : 21.0 / 13.0 dBm at combiner output

# Randomness Evaluation under Normal Operation

- Acquire 5,000,000 bits per repetitions(10 repetitions per setting)
- NIST SP 800-90B non-IID entropy estimators are used as relative indicators



< Min-Entropy with different PLL Input Clock Frequency and BANDWIDTH settings.>

| BW   | $f_0^{\text{nom}}$ [MHz] | $f_1^{\text{nom}}$ [MHz] | $H_{\text{normal,mean}}$ | $H_{\text{attack,grid}}$ | $R$ [Mbit/s] | $S$ [ $\text{ps}^{-1}$ ] |
|------|--------------------------|--------------------------|--------------------------|--------------------------|--------------|--------------------------|
| OPT  | 239.25                   | 239.73                   | 0.863                    | 0.435                    | 0.483        | 0.1187                   |
| LOW  | 297.00                   | 297.60                   | <b>0.898</b>             | <b>0.692</b>             | <b>0.600</b> | <b>0.1473</b>            |
| HIGH | 255.75                   | 256.27                   | 0.831                    | 0.661                    | 0.517        | 0.1269                   |

Bold values indicate the largest values in the entropy, bit-rate, and jitter-sensitivity columns.

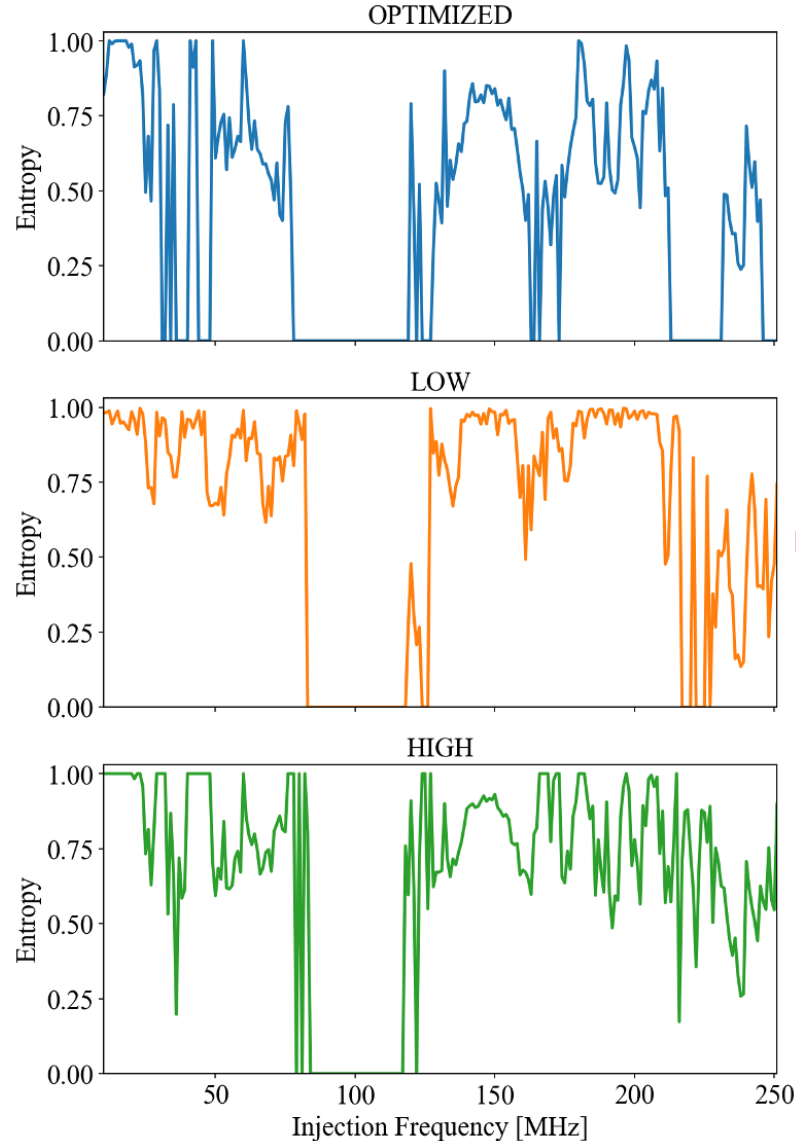
< Min-Entropy with different PLL Input Clock Frequency and BANDWIDTH settings.>

## DEMO VIDEO

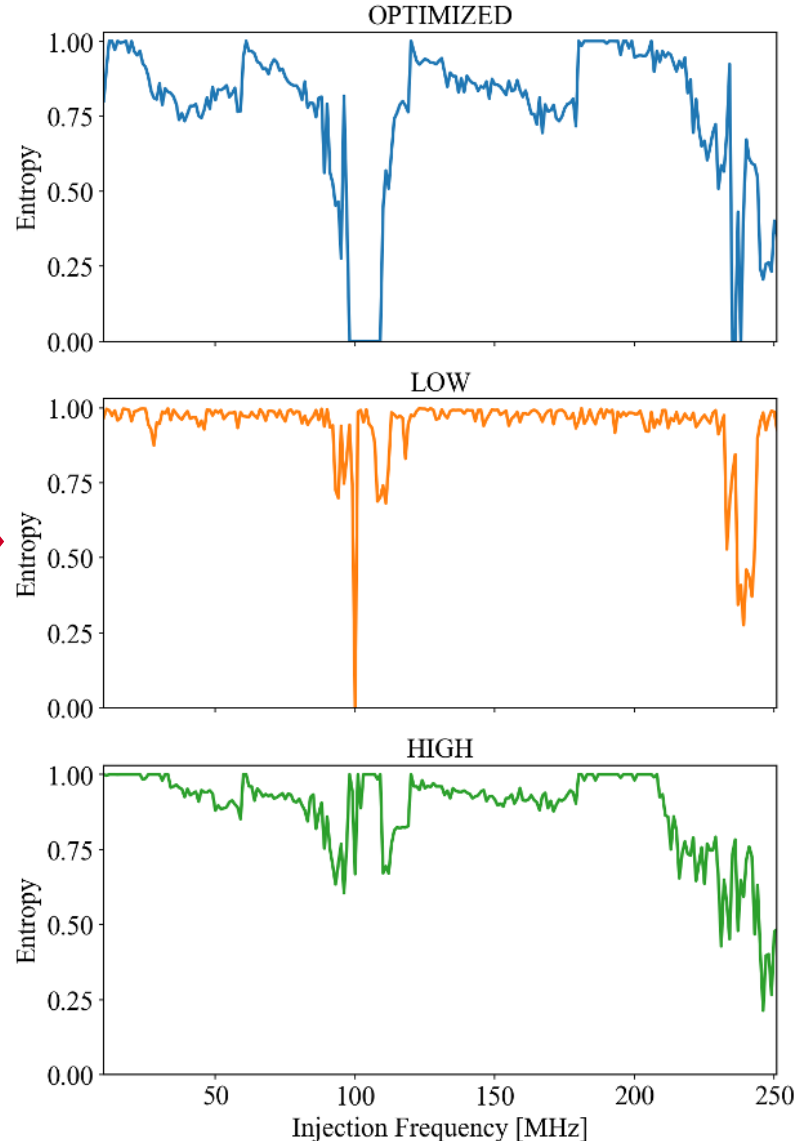
**Fault Attack on PLL-TRNG:  
Randomness Degradation through Clock Glitch-Induced PLL Perturbation**

**FDTC 2026**

# Result of Randomness Degradation caused by CW Injection



Combiner Output Power :  
**21.0 dBm**



Combiner Output Power :  
**13.0 dBm**

## OPTIMIZED

Broadest low-entropy regions.

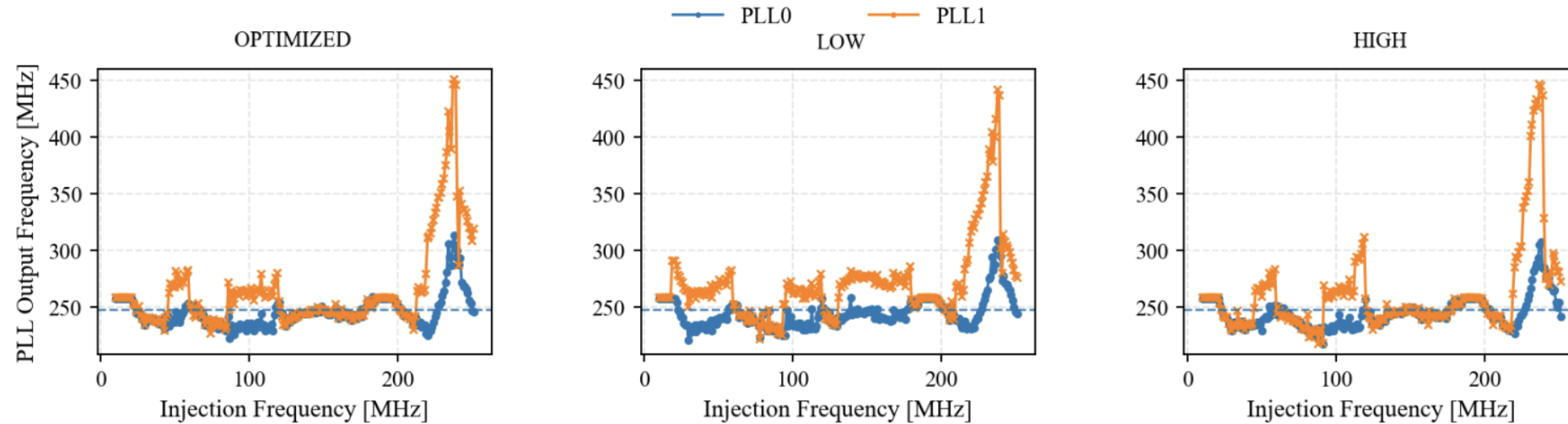
## LOW

Degradation is less, but severe local drops remain.

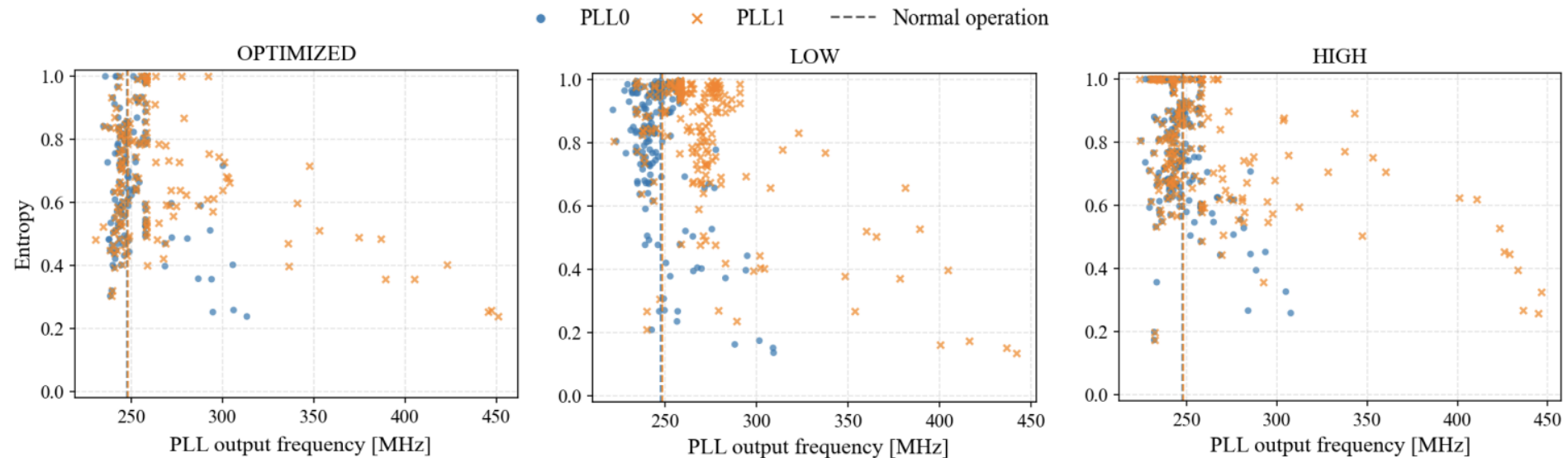
## HIGH

Severe frequency-selective local drops also appear

# Differential Responses of the Two PLLs under CW Injection

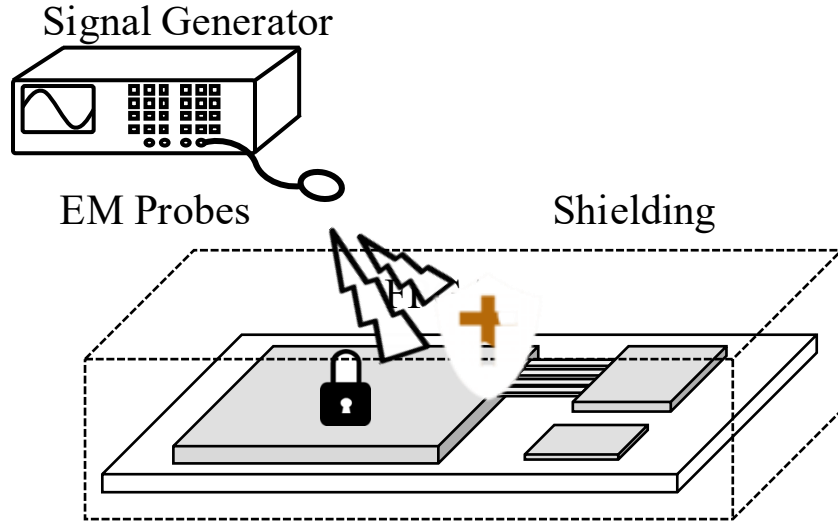


<Measured PLL Output Frequency under 21.0 dBm CW Injection>

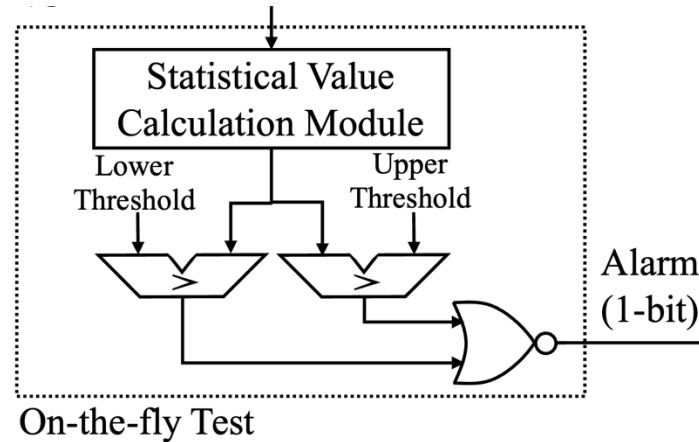


< Estimated Min-Entropy vs. Measured PLL Output Frequency >

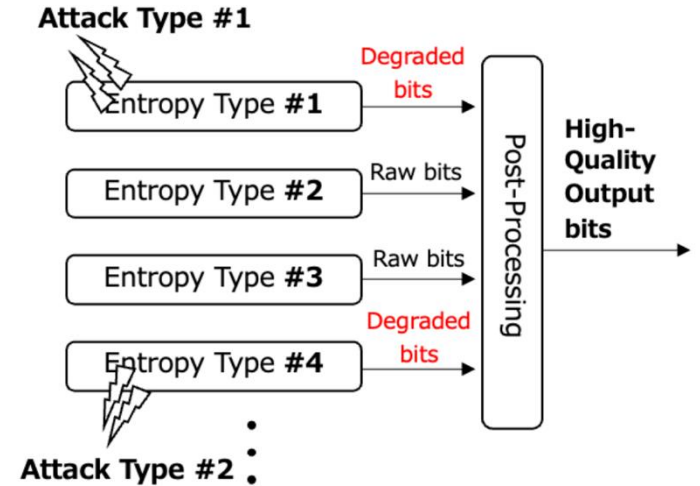
# Three Countermeasure Directions



<Shielding for countering EM Attacks>



<Block Diagram of TRNG Health Test>



<Image of applying Multiple Entropy>

## 1: Suppression

- **Shielding**
- Filtering
- Impedance control
- Proper termination

## 2: Detection

- **Health Tests [8,25]**
- PLL lock monitoring [26]
- Monitoring frequency/phase/Clock Variation

## 3: Improved Robustness

- Multiple independent entropy sources [27,28]
- Cryptographic conditioning
- PLL Configurations [14]

## Research Question

How do external clock perturbations degrade PLL-TRNG randomness?



## Results

### 1. Propose PLL-TRNG Randomness Degradation Mechanisms

- CW injection caused frequency-dependent reductions in estimated min-entropy.

### 2. PLL Bandwidth-dependent Robustness

- PLL bandwidth affected both nominal randomness and attack-induced degradation.

### 3. Demonstration of Randomness Degradation & PLL Perturbation

- Two PLL outputs showed different responses under the same disturbance.

Future work includes:

- Deeper analysis of raw contributors, clock waveforms and lock signals.
- Additional devices and PLL configurations

# Thank you!

Any questions or comments?

Contact: [hikaru.nishiyama@aist.go.jp](mailto:hikaru.nishiyama@aist.go.jp)

NATIONAL INSTITUTE OF  
ADVANCED  
INDUSTRIAL  
SCIENCE &  
TECHNOLOGY