Purdue University

Quantifying Misalignment Effects in ECC Non-Timing Side-Channel Attacks

Chia-Chien Li / Amyneth Arceo

Elliptic Curve Cryptography (ECC)

Context: Due to its high efficiency, ECC is the standard for modern security (e.g., Bitcoin, FaceID, HTTPS).

The Threat: Physical implementations leak information via power consumption (Side-Channel Analysis).

The Gap: While constant-time programming fixes timing attacks, **Non-Timing Attacks (SPA/CPA)** remain a threat.

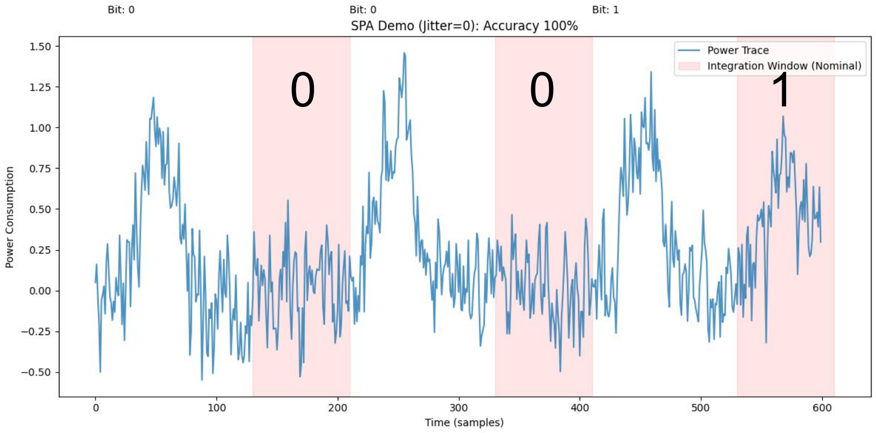
The Real-World Issue: Trace Misalignment (Jitter). Clock jitter and random delays desynchronize leakage points, causing standard attacks to fail.

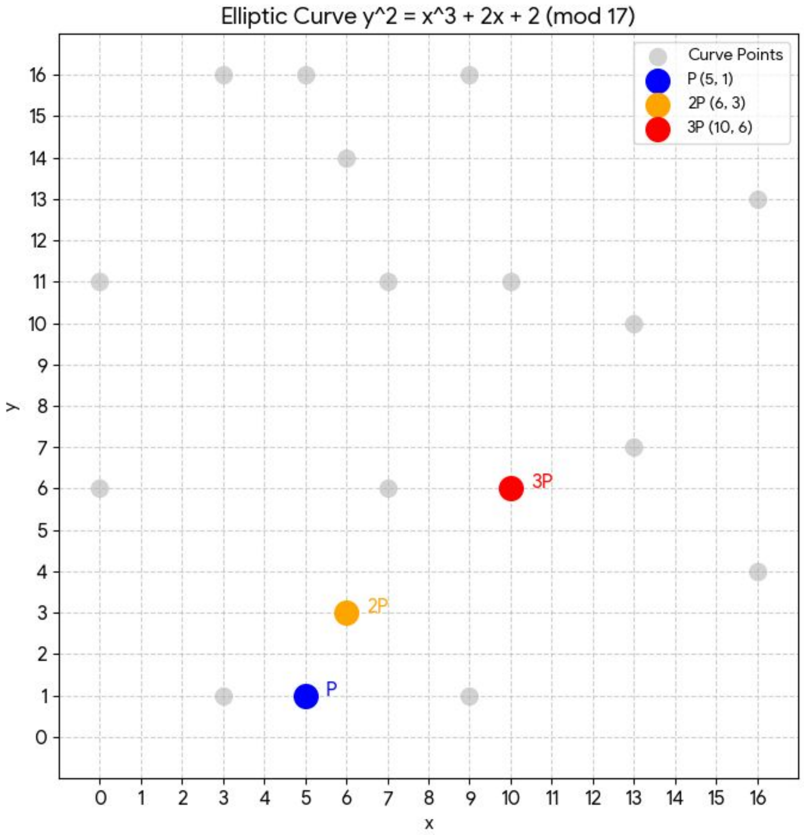
Elliptic Curve Cryptography (ECC)

Example: Calculate Q=5P

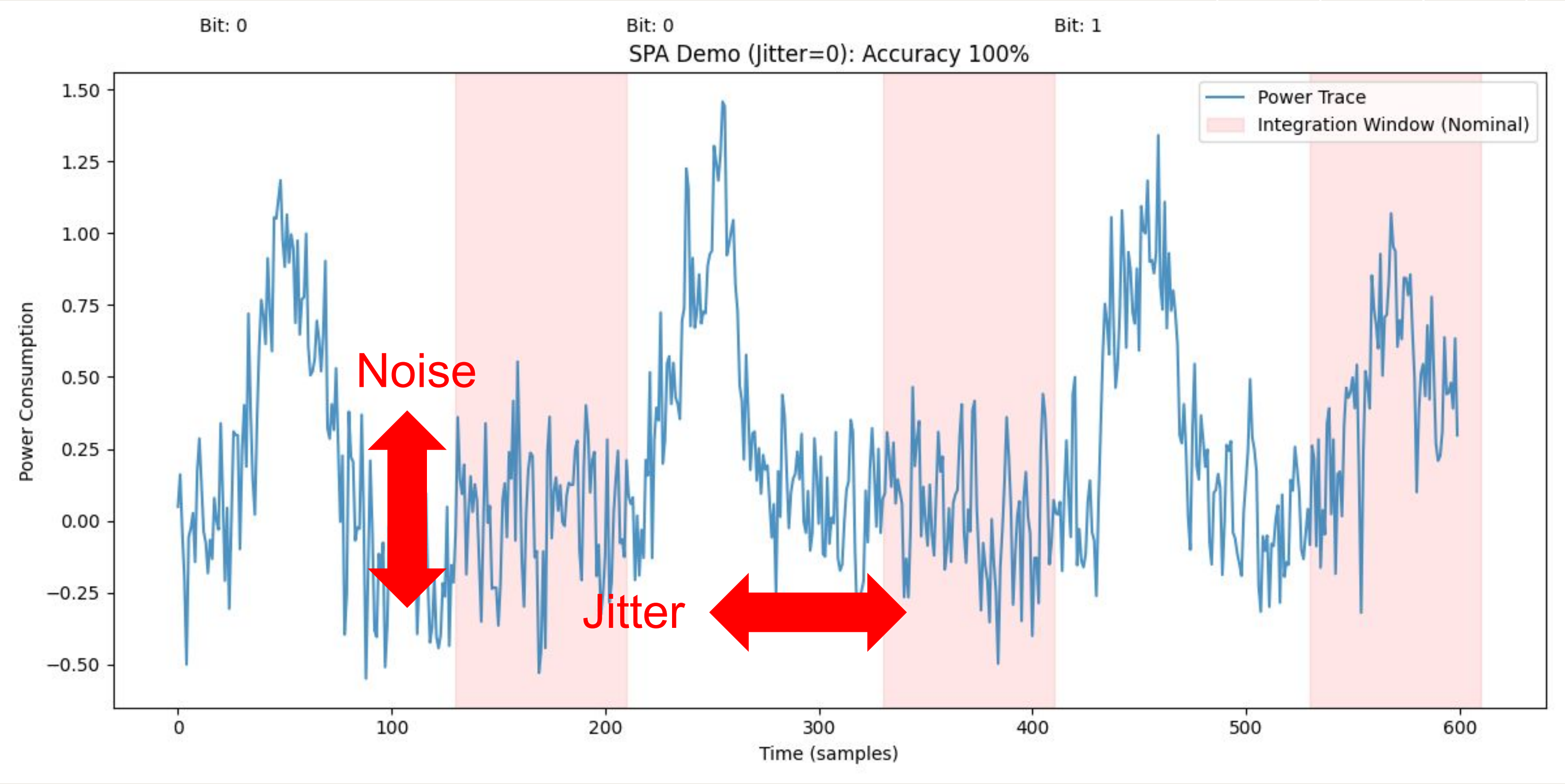
- **Secret Key (k):** 5
- **Binary:** 1 0 1
- **Start:** Current Value = 0

1. **Bit 1:** Double (0) → Add P ⇒ **Current: 1P** *(High Power)*
2. **Bit 0:** Double (2P) → (No Add) ⇒ **Current: 2P** *(Low Power)*
3. **Bit 1:** Double (4P) → Add P ⇒ **Current: 5P** *(High Power)*



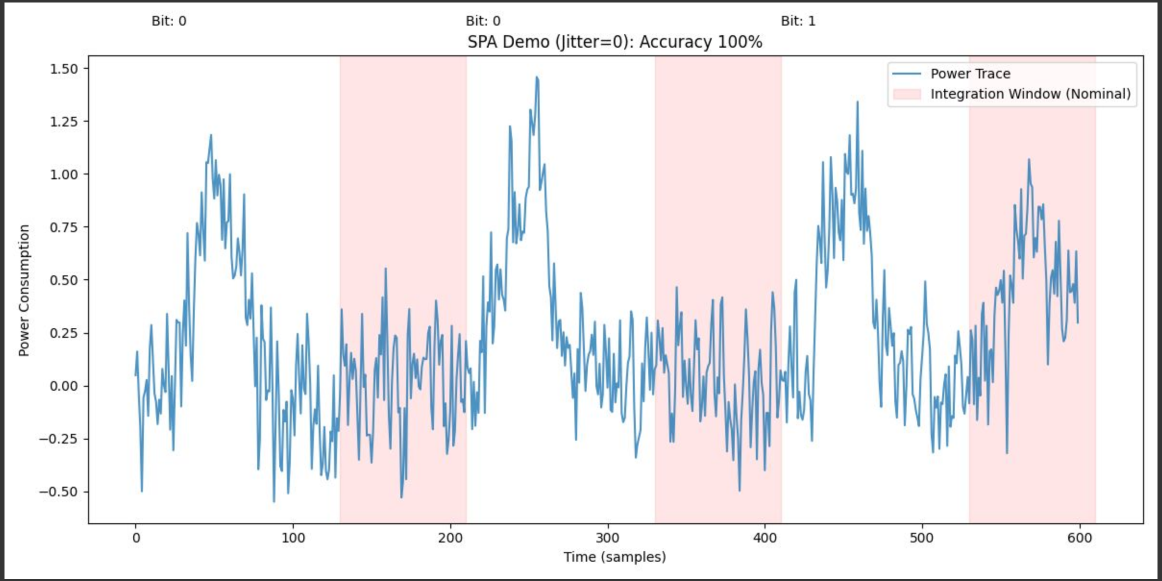


Jitter and Noise



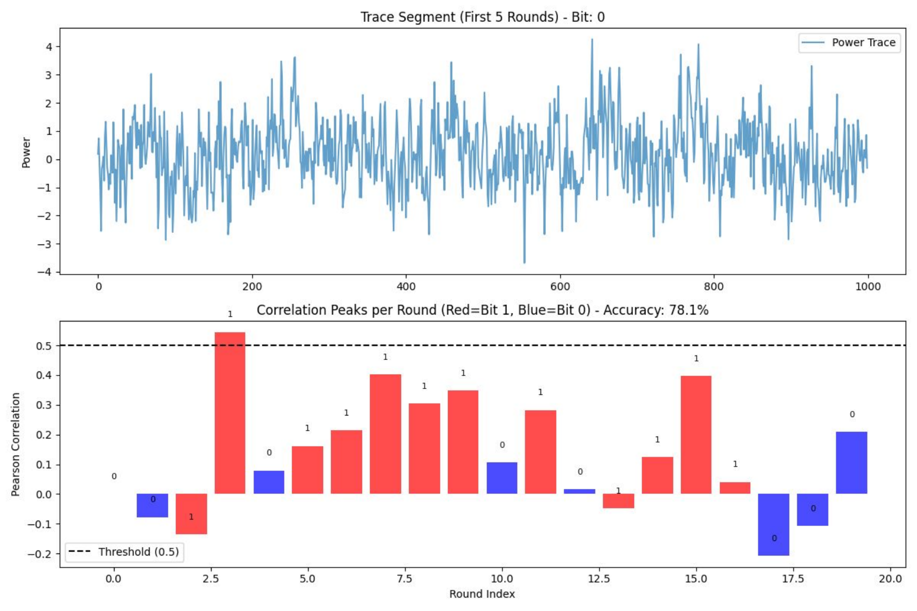
Simple Power Analysis (SPA)

The Leak: 'Add' operations (Bit 1) consume significantly more energy than 'Double' operations (Bit 0).
The Method: We calculate the **total energy** inside each operation window (the pink boxes).
The Automation: We use **Otsu's Method** to automatically find the perfect threshold that separates the "High Energy" peaks from the "Low Energy" noise.



Correlation Power Analysis (CPA)

The Math: Uses **Pearson Correlation** to find a linear relationship between our "Guessed Key" and the actual power consumption.
The Upgrade: We applied **Matched Filters** (template matching) to maximize the Signal-to-Noise Ratio (SNR) before attacking.
The Weakness: Unlike SPA, CPA is **Phase Sensitive**. If the trace shifts by even 1 sample (Jitter), the correlation breaks.

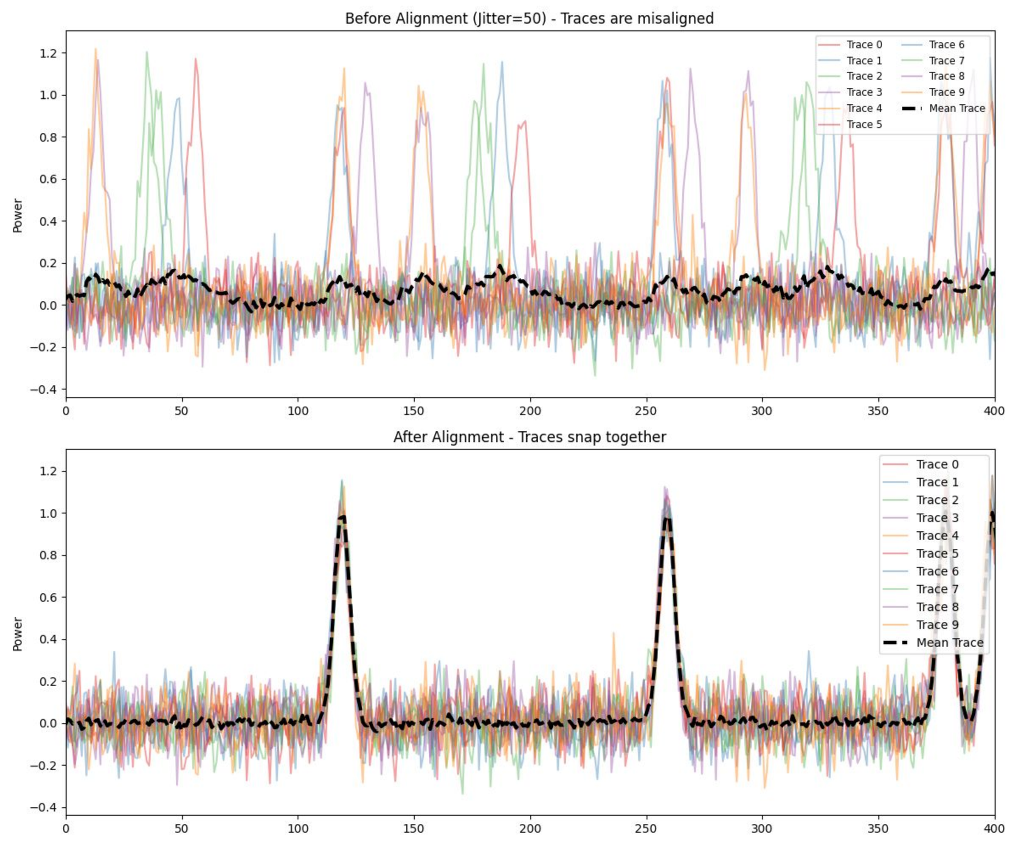


Alignment Preprocessing

The Fix: We implemented **Cross-Correlation** to mathematically calculate the time shift (Δ) between each trace and a "Reference Trace".

The Result: As shown in the graph, alignment "snaps" the traces back together. The "flat line" (top) caused by jitter is restored to sharp, distinct peaks (bottom).

The Cost: While this restores CPA feasibility, it is computationally expensive (O(LlogL)), tripling the total time required for the attack.

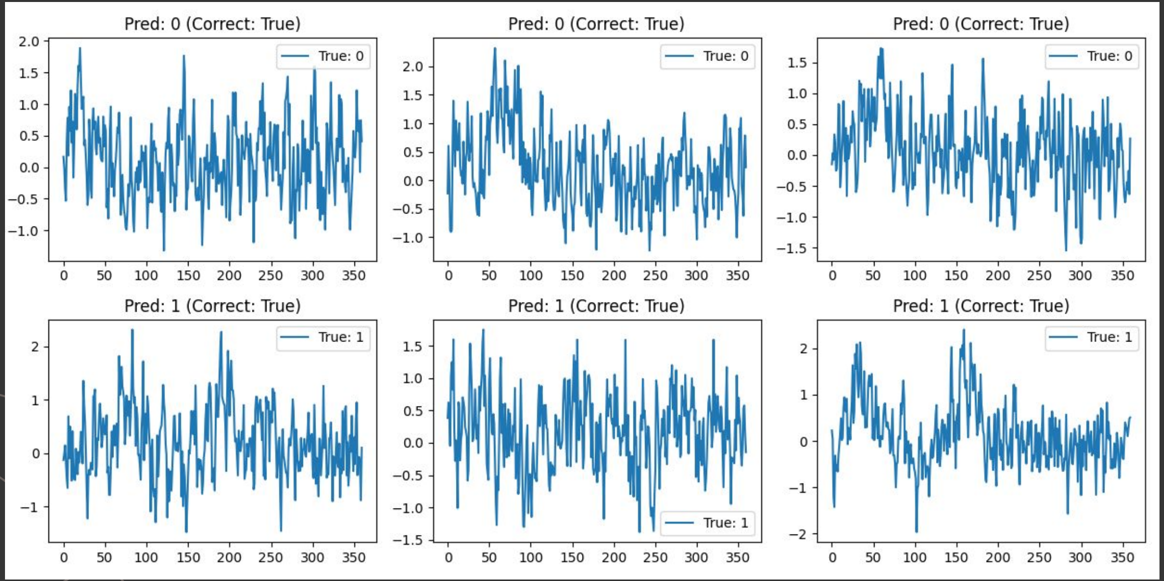


Deep Learning (CNN)

The Approach: We trained a **1D-Convolutional Neural Network (CNN)** to classify traces, rather than using fixed mathematical formulas like average or correlation.

The Secret Weapon: Translation Invariance.
By using large kernel sizes (filters), the network learns to recognize the *shape* of the "Add" operation regardless of *where* it appears in the window.

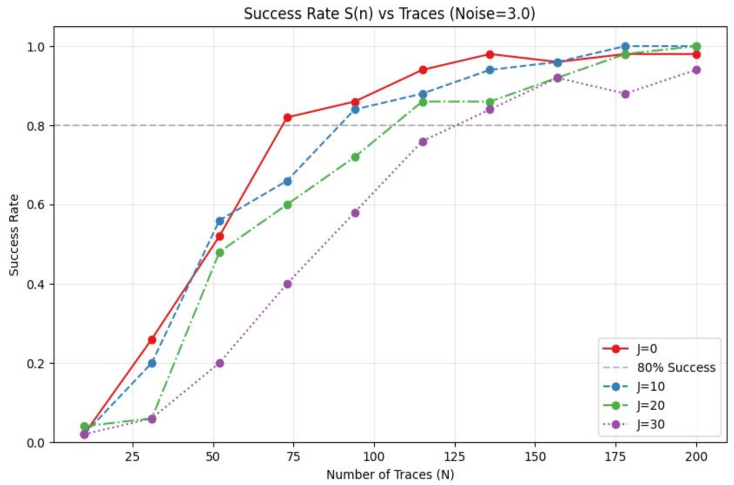
The Result: The CNN is the most robust method. It effectively "learns" to ignore the jitter without needing explicit alignment preprocessing.

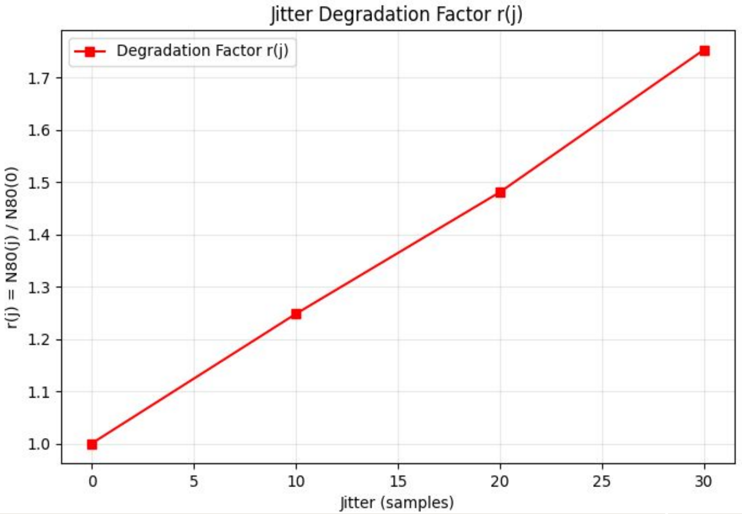


Quantifying Difficulty: The Degradation Factor

SPA Robustness: As shown in the left graph, SPA (Energy Integration) is generally robust. The curves for Jitter=0 and Jitter=10 are nearly identical.
The Shift: However, at **Jitter=30** (Purple line), the curve shifts significantly to the right, meaning we need more traces to succeed.
The Metric r(j): We defined a "Degradation Factor" to measure this shift.

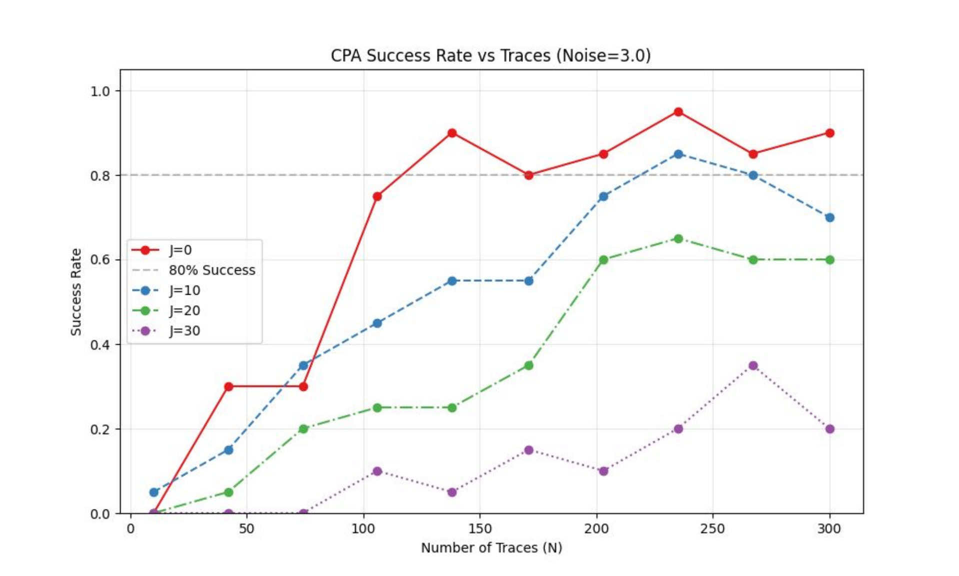
- **Result:** A jitter of 30 samples yields **r(30)≈1.75**.
- **Meaning:** The attacker must collect **75% more data** to achieve the same success rate compared to a jitter-free environment.





Why CPA Fails: Phase Sensitivity

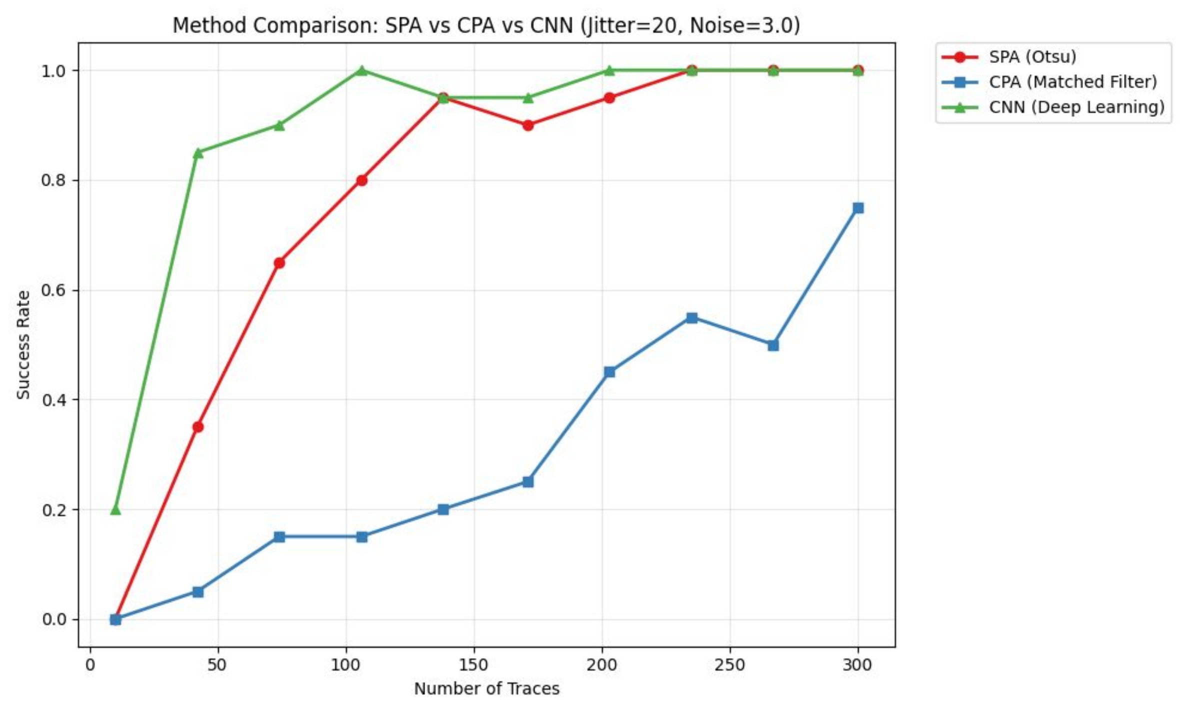
The Expectation: At Jitter=0 (Red line), CPA is powerful, reaching 80% success with just ~100 traces.
The Reality: As soon as we introduce **Jitter=10** (Blue line), the success rate drops precipitously.
The Collapse: At **Jitter=30**, the attack effectively flatlines (Green/Purple lines).
The Reason: CPA relies on sample-wise correlation. Jitter causes "Phase Mismatch," where the leakage point shifts away from the sampling point, destroying the correlation.



CNN vs. CPA vs. SPA

Experimental Setup: We tested all three methods under identical "Hard" conditions: High Noise (σ=3.0) and Moderate Jitter (J=20). **The Hierarchy of Robustness:**

- **CPA (Blue):** Reaches only ~80% success with ~300 traces. Statistical attacks cannot handle raw jitter.
- **SPA (Red):** Reaches ~100% success but requires ~250 traces. Robust due to energy integration.
- **CNN (Green): Dominant.** Reaches 100% success with only ~100 traces.



Conclusion: The 1D-CNN effectively learns **Translation Invariance**, solving the misalignment problem more efficiently than traditional methods.

Conclusion & Engineering Implications

The Hard Metric: We successfully quantified that Jitter is a security parameter, not just noise.

- A jitter of just 30 samples increases the attacker's data cost by **~75%** ($r(30) \approx 1.75$).

The Hierarchy of Attack:

- **CPA:** Fails without expensive alignment.
- **SPA:** Tolerates misalignment effectively due to energy integration.
- **CNN:** The State-of-the-Art. It effectively learns to "see through" the jitter.

Design Recommendation: Clock jitter is a highly effective, low-cost defense. However, it is not a silver bullet.

- **Future Work:** To defeat Deep Learning, jitter must be combined with **Masking** and **Shuffling**.