Exploiting Small Leakages in Masks to Turn a Second-Order Attack into a First-Order Attack

Alexander DeTrano

Sylvain Guilley

Xiaofei Guo

Naghmeh Karimi

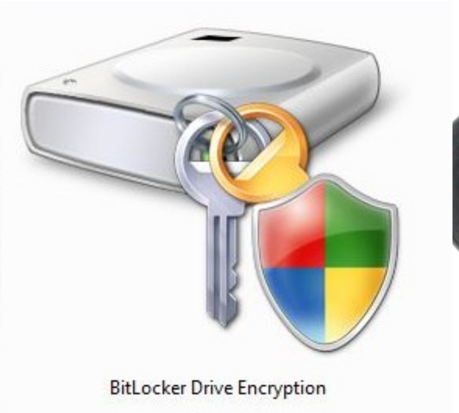
Ramesh Karri

Motivation

MasterCard
paypass

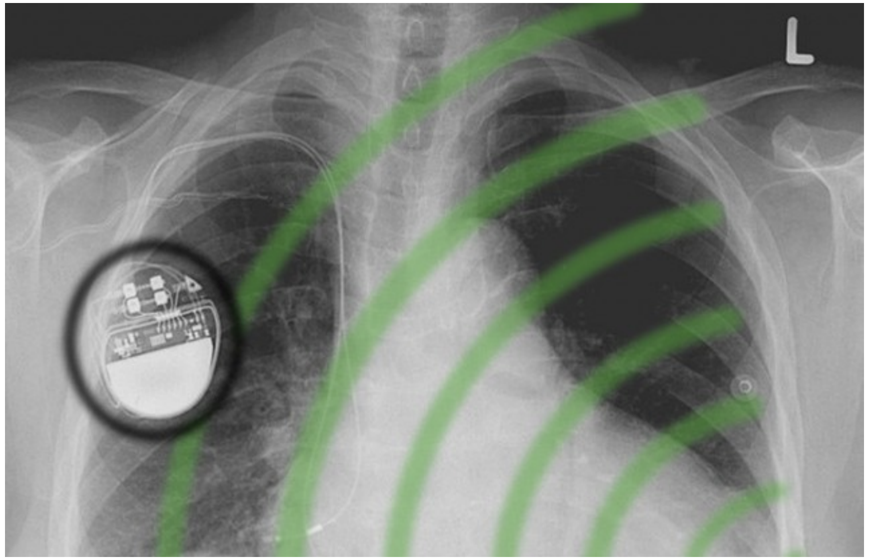
VISA
4000 1234 5678 9010
4000
12/08
B. PARKER
VISA

PASSPORT
United States of America


BitLocker Drive Encryption

HOLD

RSA
SecurID®
159 759
Secured by RSA

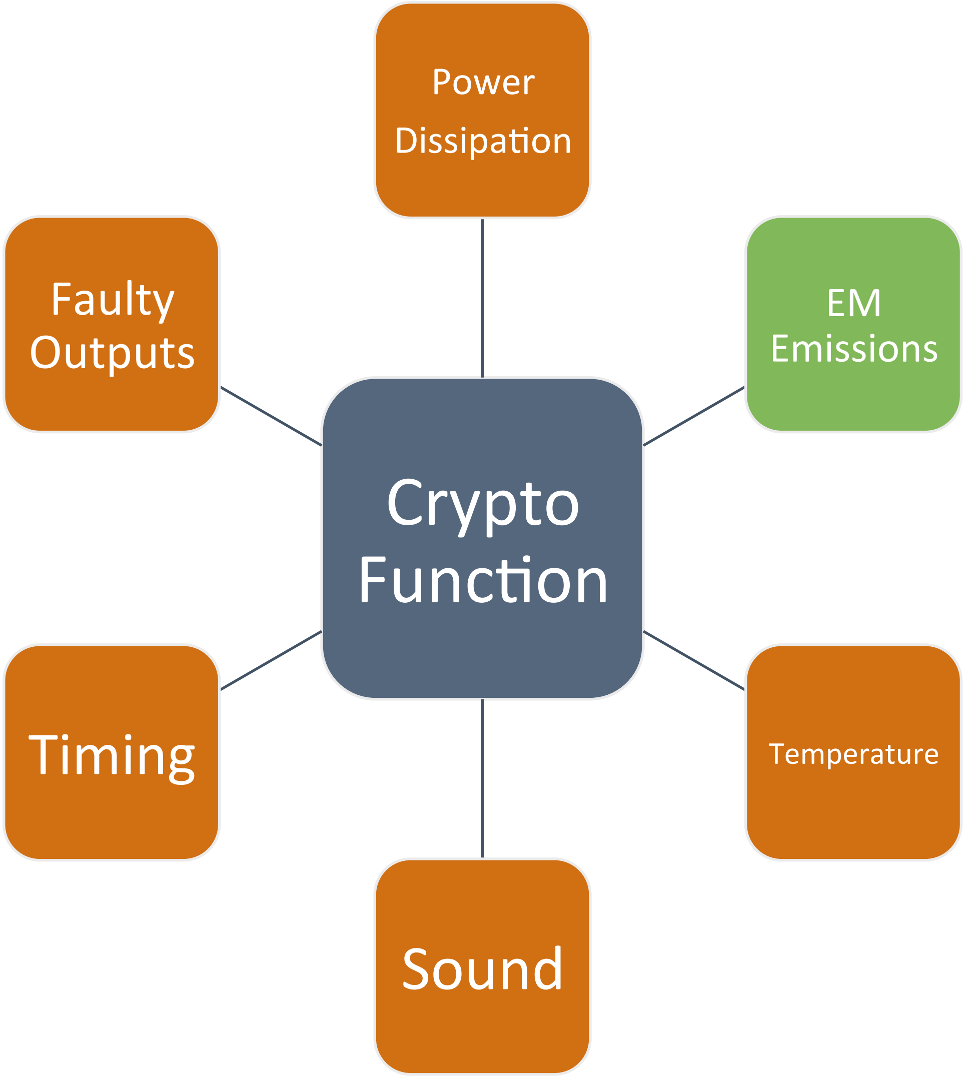

L

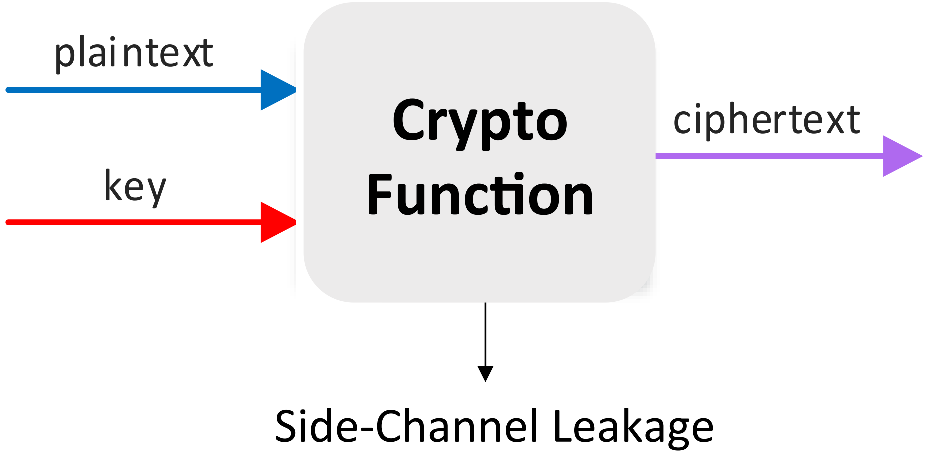
ATM
WELCOME

CABLEVISION
SCM

Side-Channel Attacks

- Algorithm implementations may inadvertently leak information through different sources
- These sources are called “side-channels”
- A side-channel attack exploits one or more of these to learn secret information





Masking Countermeasure

- Countermeasures such as masking have been developed to thwart side-channel attacks
- Masking tries to remove the correlation between the power consumption and the data that is being handled

Boolean Masking

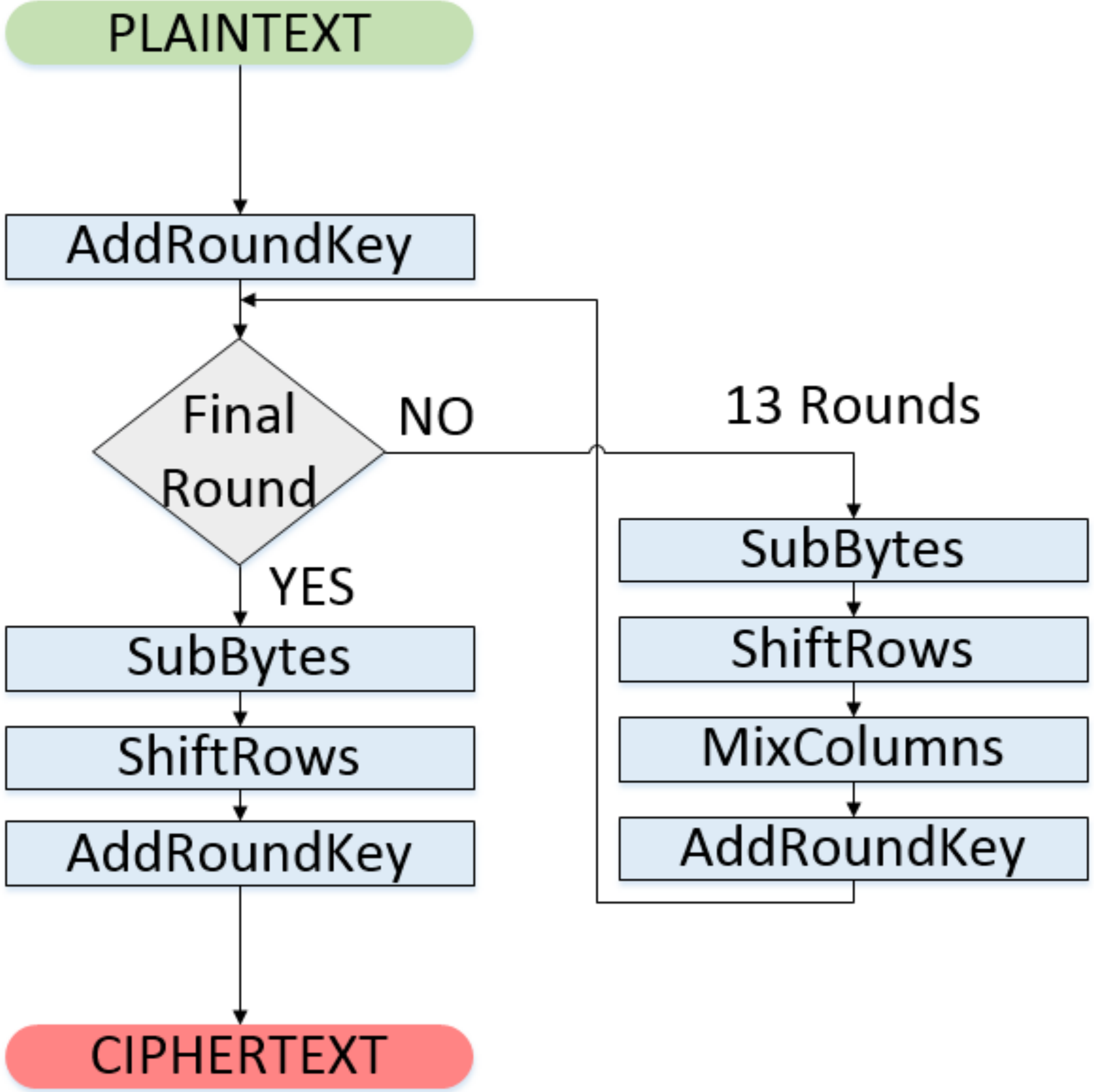
Unmasked	Masked
$x = d \oplus k$	$x \downarrow m = d \oplus k \oplus m$

d : plaintext, k : secret key, m : uniformly distributed random mask

Advanced Encryption Standard (AES)

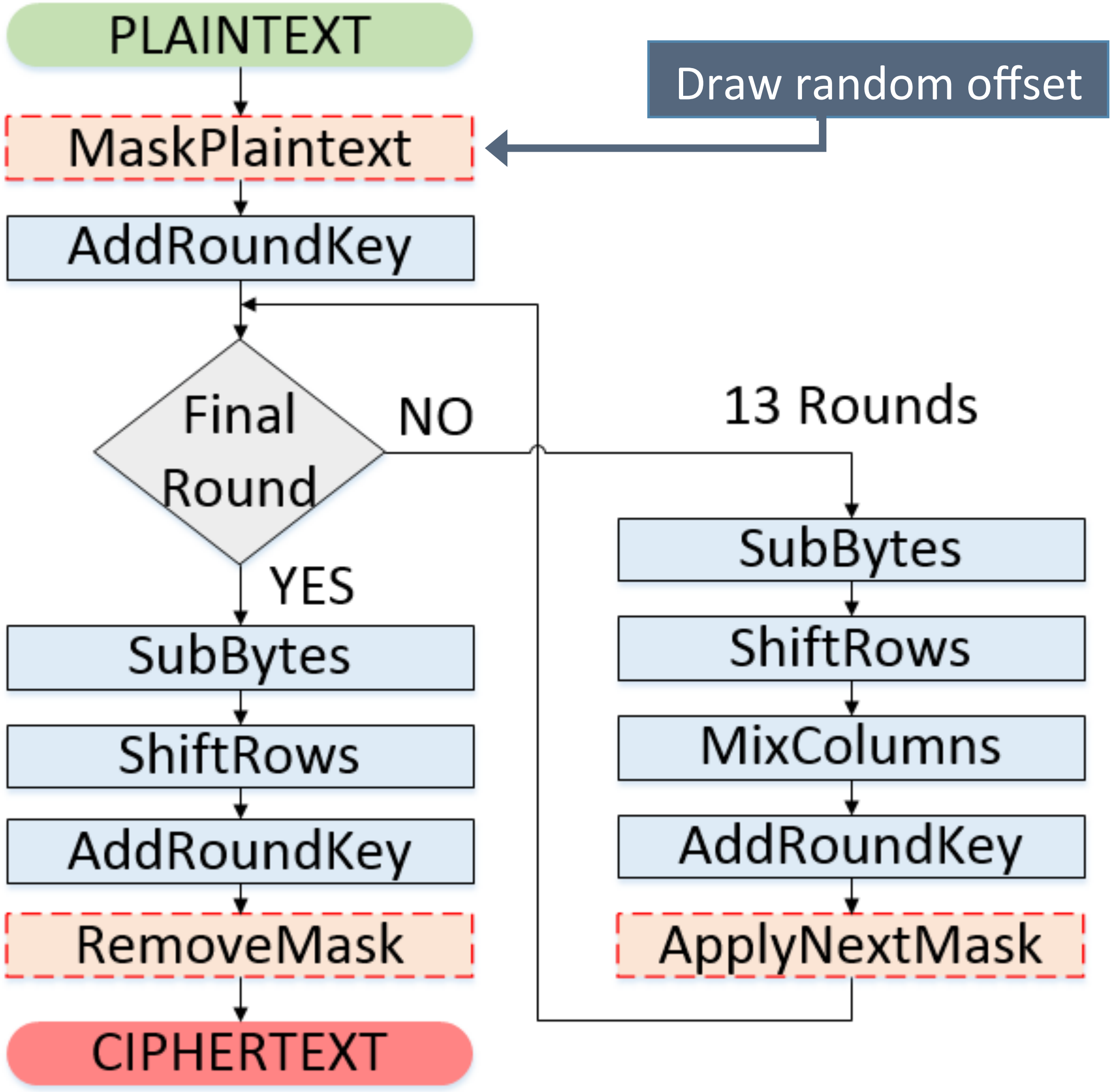
- Plaintext/ciphertext: 128 bits
- Key: 128/192/**256** bits
- 13 rounds + 1 pre-round

AddRoundKey	XOR operation
SubBytes	Look-up table
ShiftRows	Byte-wise permutation
MixColumns	Matrix multiplication



Rotating S-Box Masking (RSM)

- Carefully chosen masks reduces storage requirements
  - RSM uses 16 masks
- HW : 2nd-order zero-offset resistance
- EM traces publicly from DPA Contest v4
  - AES256-RSM implemented on a smartcard with 8-bit microcontroller Atmel ATMega-163



Maxime Nassar, Youssef Souissi, Sylvain Guilley, Jean-Luc Danger. RSM: a Small and Fast Countermeasure for AES, Secure against 1st and 2nd-order Zero-Offset SCAs, DATE’12

Mask Recovery Attack

- A 1st order CPA attack fails to recover the key after 100,000 traces
- Prior work: non-uniform distribution of the masks after an XOR (174), collision attacks (1100), 2nd-order CPA (300),
- Our attack : 10 traces

Observation

- Masks are deployed in a predictable sequence
- The device leaks the Hamming Weight of the masks each time they are handled

Idea

- Launch a 1st order *horizontal* CPA attack to recover the masks
- Recover the masks, then recover the key

Moradi, A., Guilley, S., Heuser, A., “Detecting Hidden Leakages”, ACNS’14

Kutzner, S., Poschmann, A., “On the Security of RSM — Presenting 5 First and Second-order Attacks”, COSADE’14

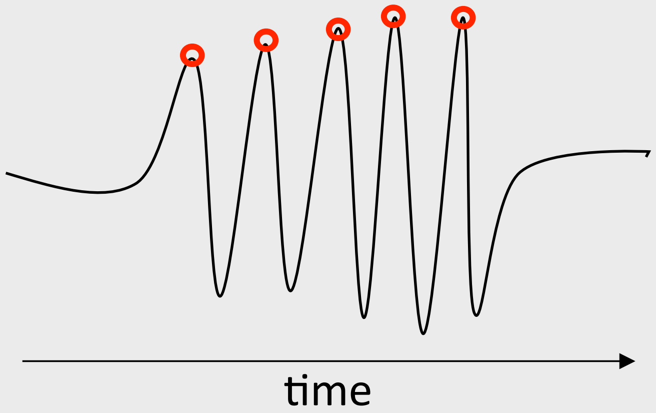
Belgarric, P., Bhasin, S., Bruneau, N., Danger, J.L., Debande, N., Guilley, S., Heuser, A., Najm, Z., Rioul, O., “Time-Frequency Analysis for Second-Order Attacks”, CARDIS’14

1st order CPA Attack

Hypothetical Power Model

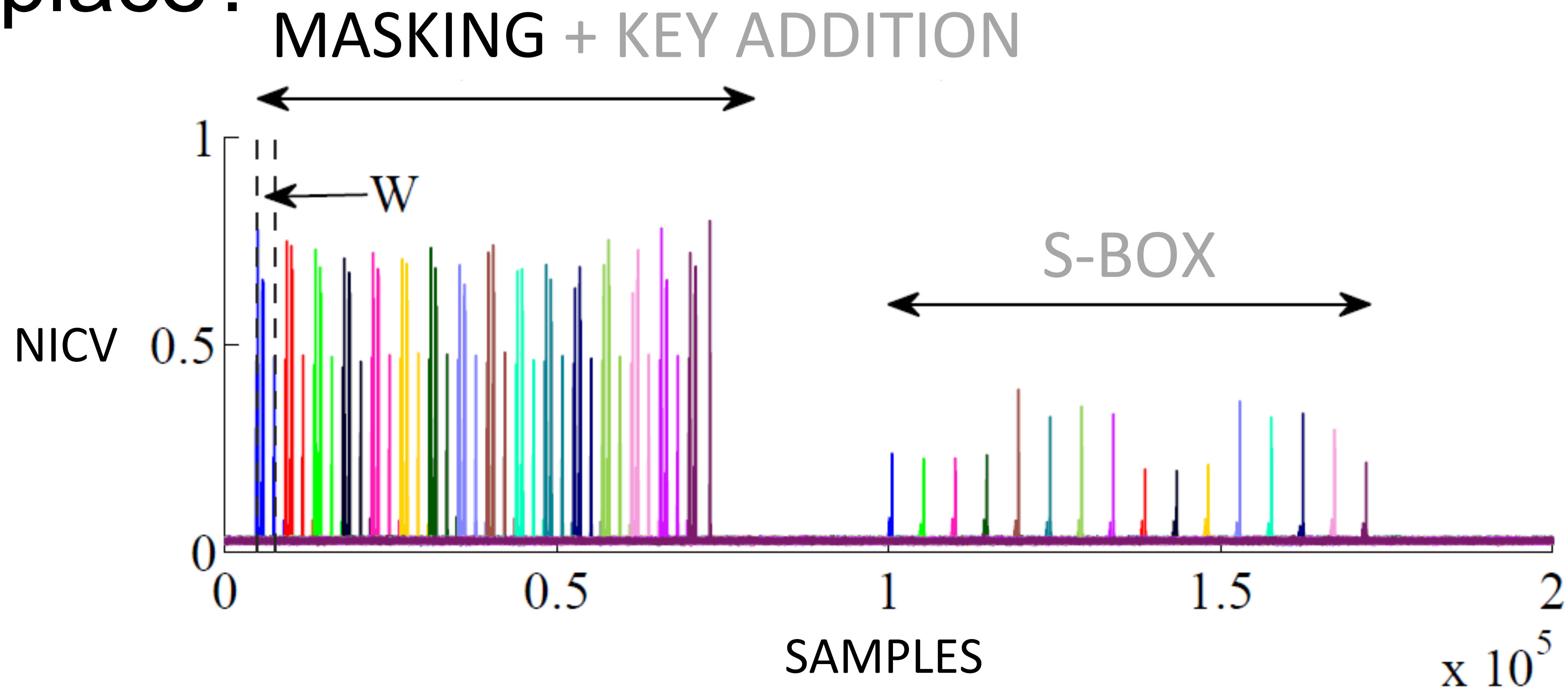
HW(■■[■■■*m*0 *m*11⋮ &■*m*1*m*2 ⋮ &■■*m*2*m*3 ⋮ &■■⋯⋯⋮ & &*m*15&*m*0&·

Measured Power Traces



Correlation

Mask Recovery – When does masking take place?



MASKING + KEY ADDITION

S-BOX

$NICV = Var(\mathbb{E}[T|X])/Var(T)$

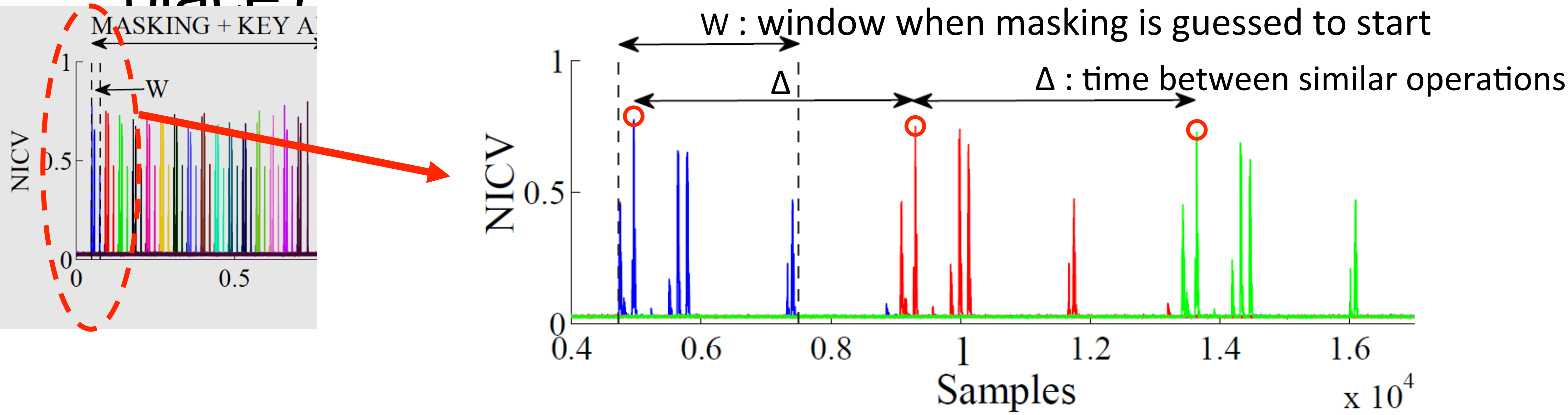
W : window when masking is suspected to occur

NICV : Normalized Inter-class Variance

T : power traces

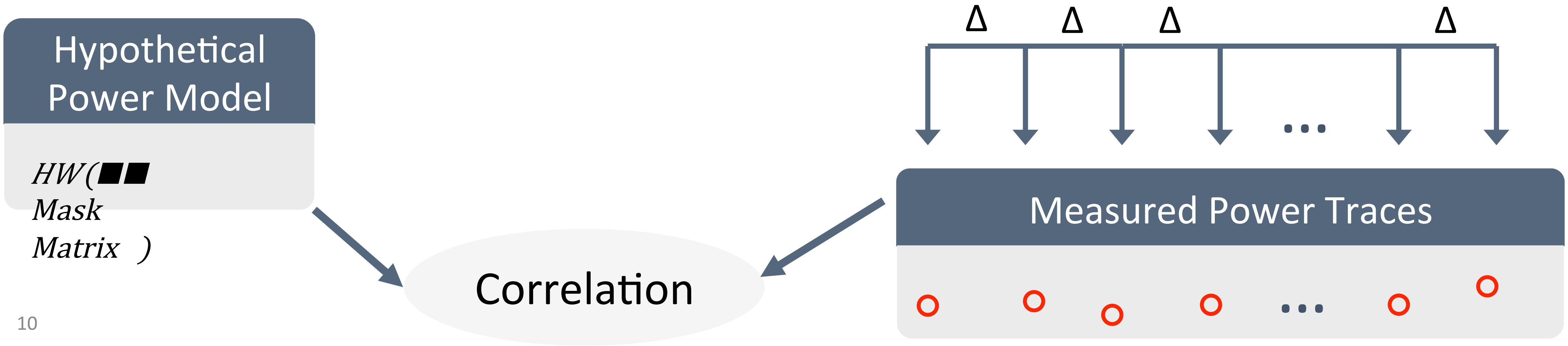
X : plaintext byte

Mask Recovery – When does masking take place?



W : window when masking is guessed to start

Δ : time between similar operations



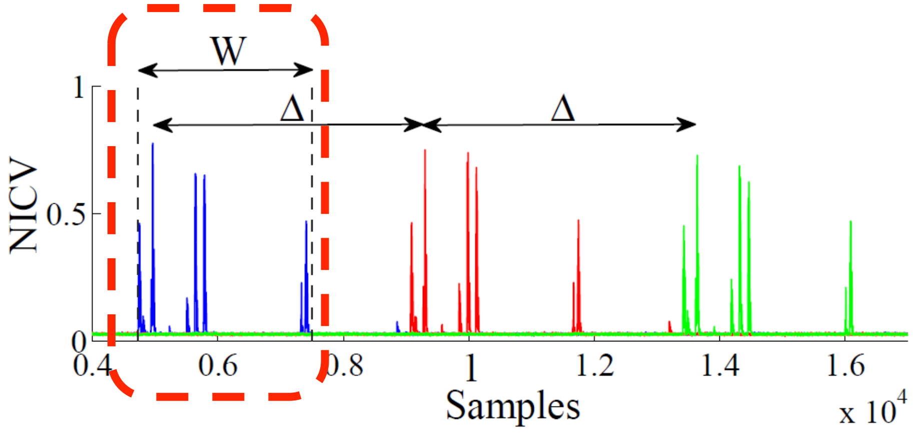
Hypothetical Power Model

HW(■■ Mask Matrix)

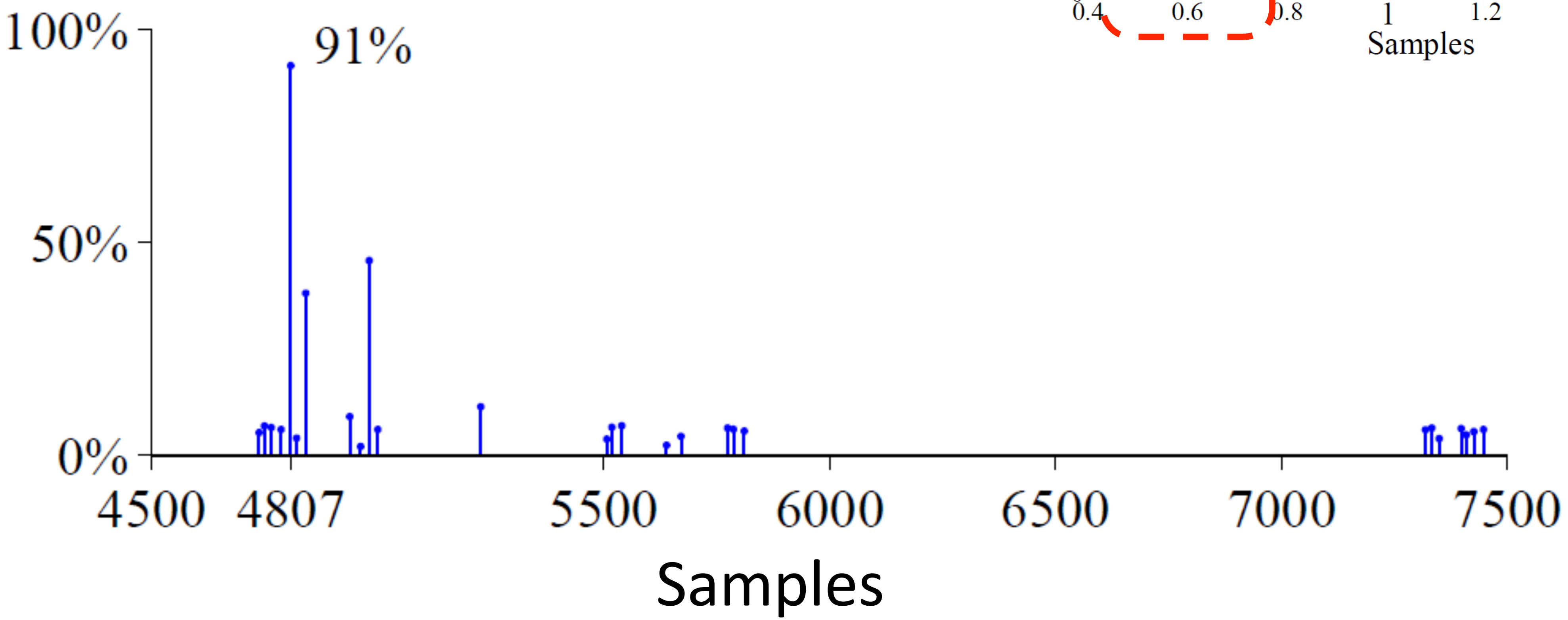
Correlation

Measured Power Traces

Mask Recovery Results

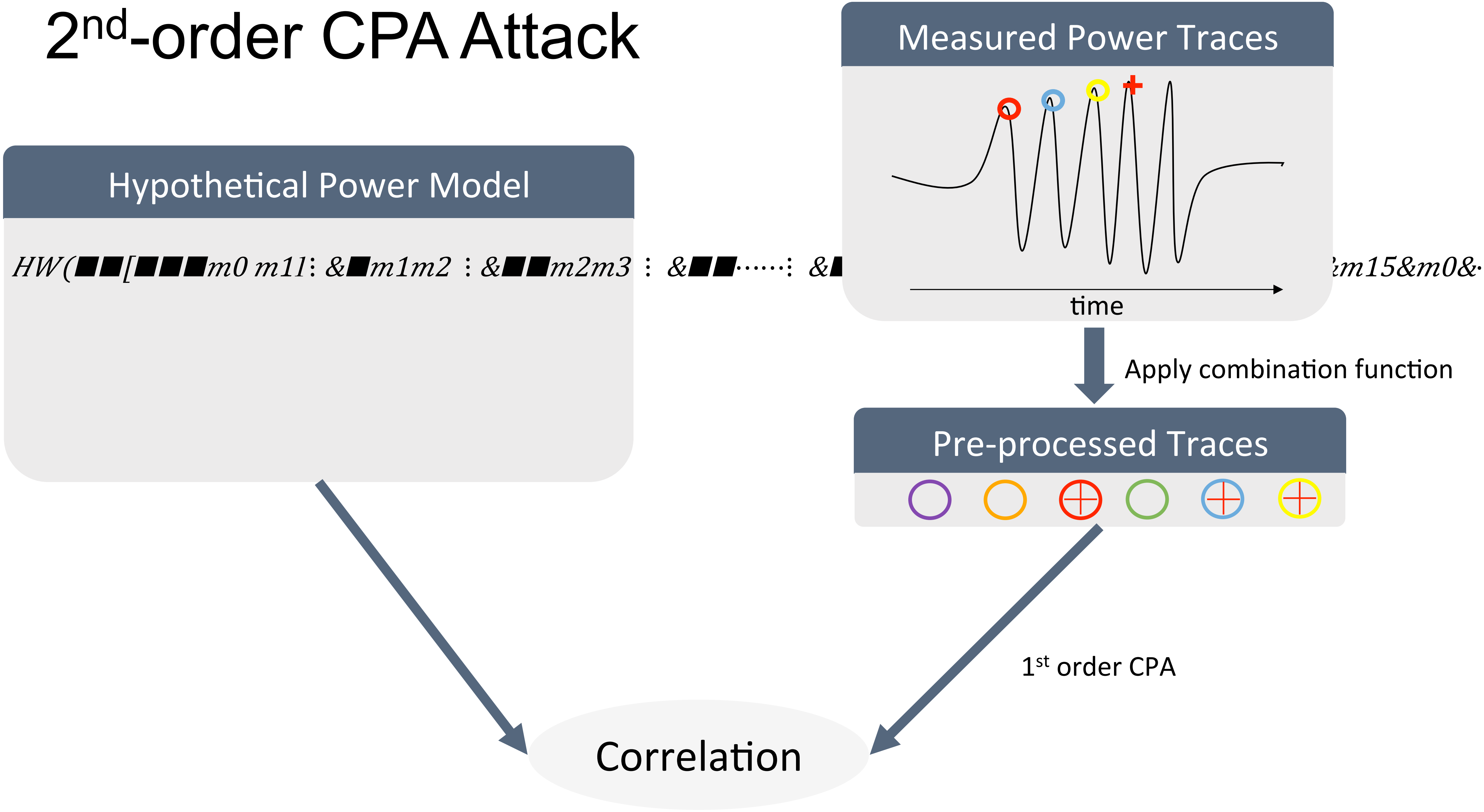


Mask Recovery Success Rate



Taken over 10,000 power traces

2nd-order CPA Attack



Measured Power Traces

Apply combination function

Pre-processed Traces

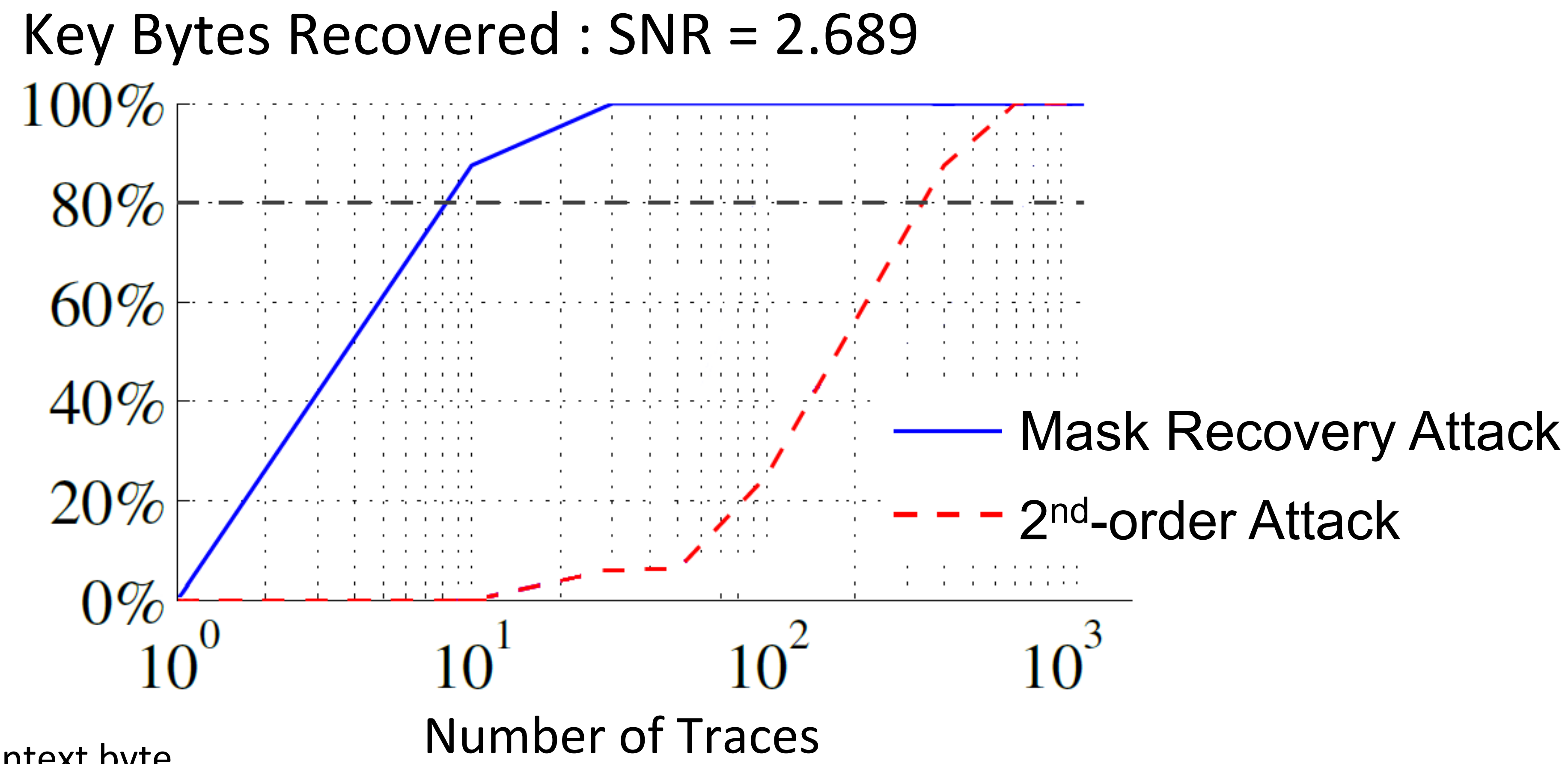
1st order CPA

Hypothetical Power Model

HW(■■[■■■*m*0 *m*11⋮ &■*m*1*m*2 ⋮ &■■*m*2*m*3 ⋮ &■■⋯⋯⋮ &■ … &*m*15&*m*0&·

Correlation

Comparison with 2nd-Order Attack^



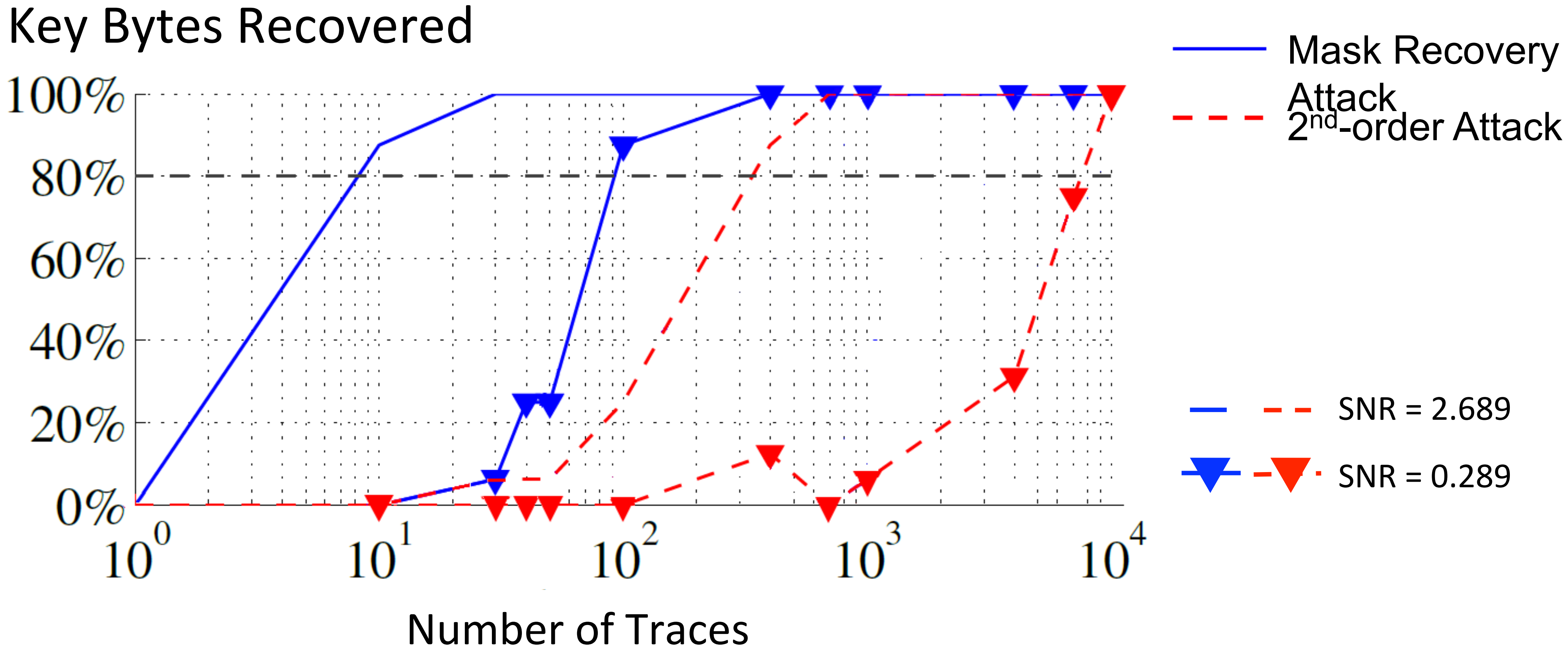
T : power traces, X : plaintext byte

$^*SNR = 1/1/NICV - 1 = \ \ Var(\mathbb{E}[T|X])/Var(T) - Var(\mathbb{E}[T|X])$

*S. Bhasin, J-L Danger, S. Guilley, and Z. Najm, “Side-Channel Leakage and Trace Compression using Normalized Inter-Class Variance”, HASP’14

^E. Prouff, M. Rivain, and R. Bevan. Statistical analysis of second order differential power analysis. IEEE Trans. on Computers’09

Adding Noise to the Power Traces



*$SNR = 1/1/NICV - 1 = \quad Var(\mathbb{E}[T|X])/Var(T) - Var(\mathbb{E}[T|X])$

T : power traces, X : plaintext byte

*S. Bhasin, J-L Danger, S. Guilley, and Z. Najm, “Side-Channel Leakage and Trace Compression using Normalized Inter-Class Variance”, HASP’14

Conclusion

- Our attack outperforms a 2nd-order attack by two orders of magnitude w.r.t to number of traces needed to recover the key
- A 2nd-order attack fails to recover the key for SNR < 0.289, while our attack succeeds for SNR ≤ 0.035
- The implementation leaks the Hamming Weight of the masks as they are fetched from memory
- The predictable deployment order of the masks and Hamming Weight variation allow an attacker to recover the mask offset
- We also analyzed the relationship between mask recovery success rate and window width/number of masks attacked

Thank you!

Questions?