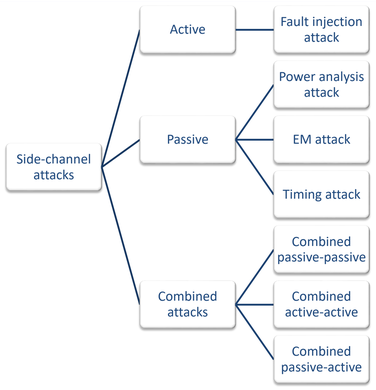
The Strength of Combined Distinguishers and Combined Side-channel Attacks

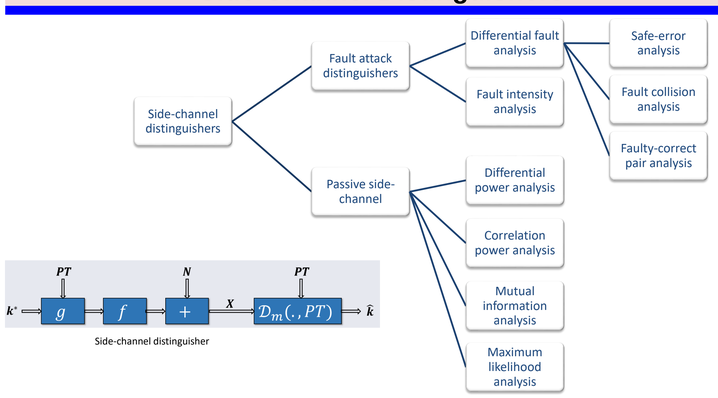
Selçuk Köse, University of Rochester, Rochester, NY

http://hajim.rochester.edu/ece/sites/kose/

Side-Channel Attacks – a taxonomy



Side-Channel Distinguishers



Definition of a "Combined Attack"

We explicitly use *"combined attack"* for either one of the following

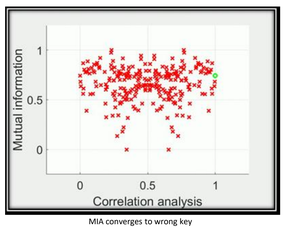
1. Using more than one distinguisher used for a particular attack
   - Different statistical tools to analyze a given data
     - ❑ i.e., using both Pearson correlation and Mutual information analysis for power side-channel attack
2. Performing two different attacks to obtain the same information
   - Different types/forms of (correlated or uncorrelated) data providing information about the stored secrets
     - ❑ i.e., using both power side-channel and fault injection attacks to obtain the secret key

Combined Distinguishers: CPA + MIA

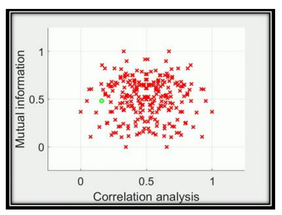
Combination of distinguishers

1. Improve confidence in achieving correct guess
2. Reduce number of measurements to disclose

1. Distinguisher may converge to wrong key
   - There is no prior information about leakage
     - Leakage model is not known
     - No prior information about noise/parasitic
       - Can leak to a non-Gaussian noise + parasitic + spikes



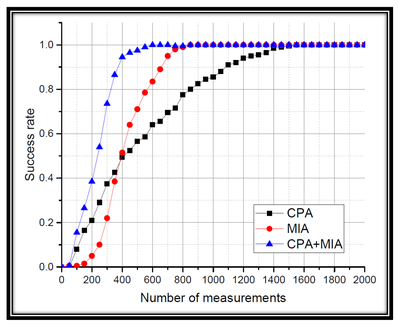
MIA converges to wrong key



CPA converges to wrong key

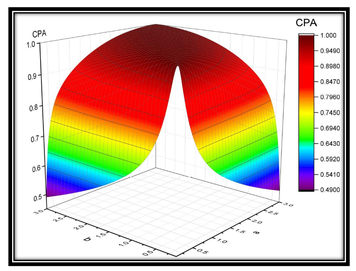
2. CPA and MIA are not equivalent
   - Additive information
   - Combination can be used to decrease uncertainty

Favor	MTD
CPA	$MTD_{MIA} \gg MTD_{CPA}$
?	$MTD_{MIA} > MTD_{CPA}$
?	$MTD_{MIA} \approx MTD_{CPA}$
?	$MTD_{MIA} < MTD_{CPA}$
MIA	$MTD_{MIA} \ll MTD_{CPA}$

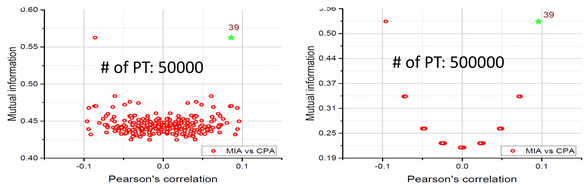


CPA vs MIA

- CPA is optimal for known model and Gaussian N
  - Converges faster to correct hypothesis
  - Robust to additive Gaussian noise variations
- MIA is better when
  - Noise is non-Gaussian
  - Model is partially known



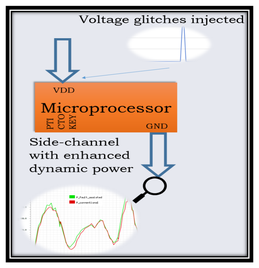
Uniform N + Known model

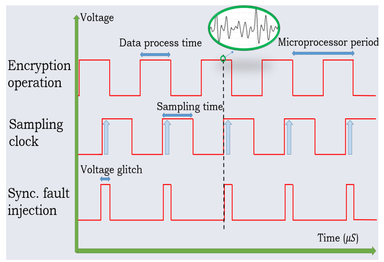


Combined Attacks: Passive + Active

Fault assisted side-channel attack

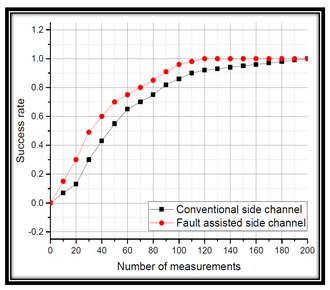
- Voltage glitch assisted side-channel
  - Dynamic power increases → improve detection



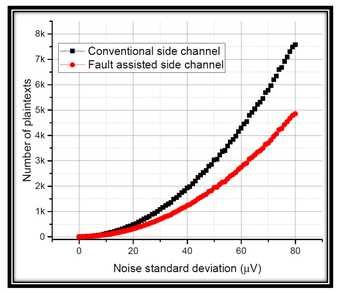


Fault Assisted Side-Channel Attack

SNR increases → MTD decreases



Improvement in success rate with proposed fault assisted side-channel. MTD for SR=0.9 reduced by 18.2%.



Reduction in MTD with proposed fault assisted side-channel. Average reduction of MTD for SR=9 is 34.36%.

- Combined distinguishers and combined attacks significantly increase the strength of physical side-channel attacks
- Mathematical foundations and practical considerations are investigated

Impact on Society

- Proposed solutions will pave the way to protect our digital data more effectively
- Results of this research will enable more effective countermeasures against various side-channel attacks

Impact on Education

- Course modules will be developed to be integrated into any hardware security related course
- Software modules are being developed to implement practical attacks on FPGA dev boards

- Optimal distinguisher depends on the design of the cryptographic engine implementation
  - No universal distinguisher
  - Can be combined to form a stronger attack under certain noise/model conditions
- Multiple attacks can be combined either
  - To reduce the solution space of an attack or
  - To increase the SNR of the signal obtained by an attack

CNS-1929774
SaTC: STARSS: Small: Combined Side-channel Attacks and Mathematical Foundations of Combined Countermeasures