A Lightweight AES Implementation Against Bivariate First-Order DPA Attacks

Weize Yu and Selçuk Köse

Department of Electrical Engineering

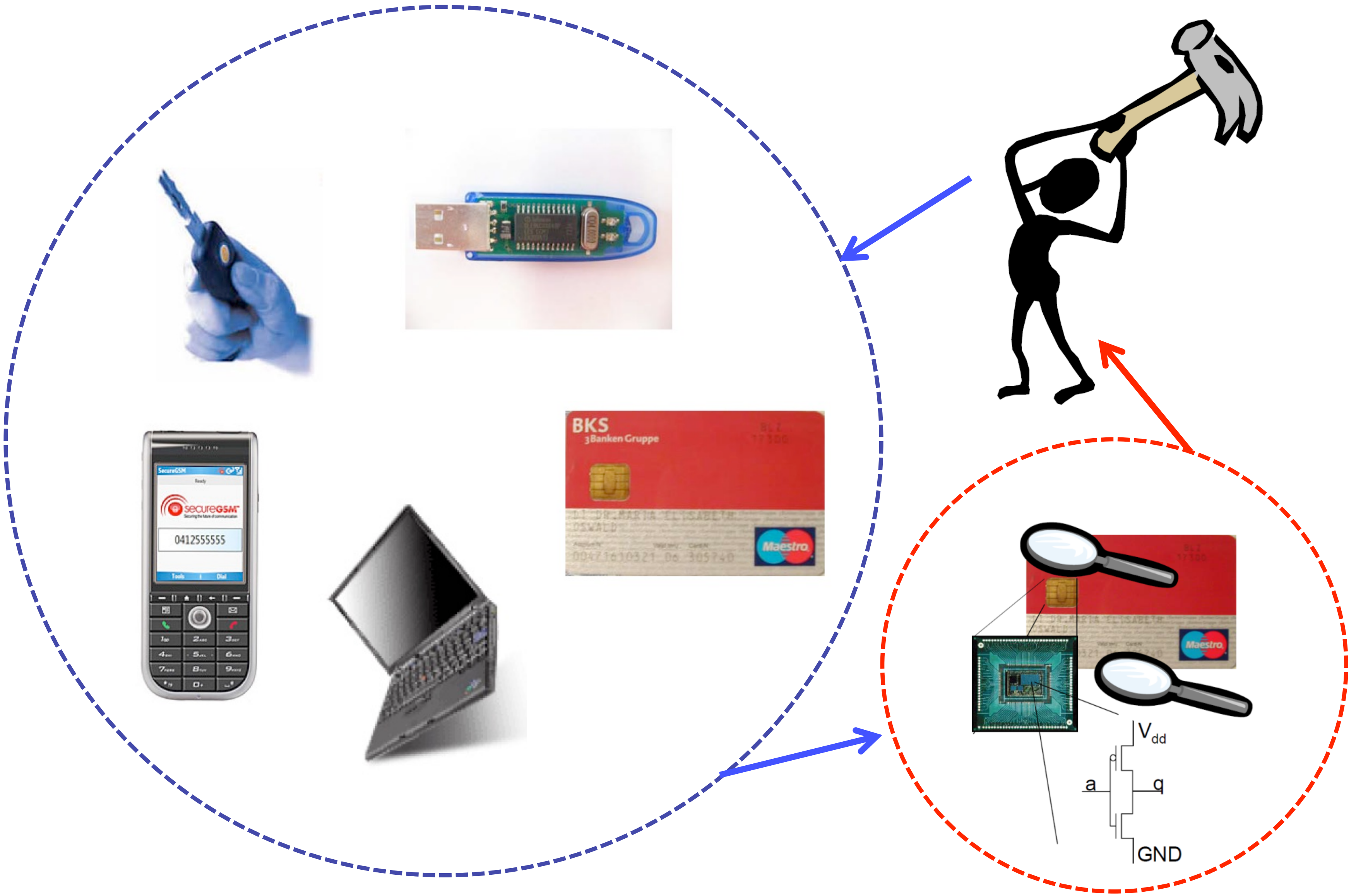
University of South Florida

USF

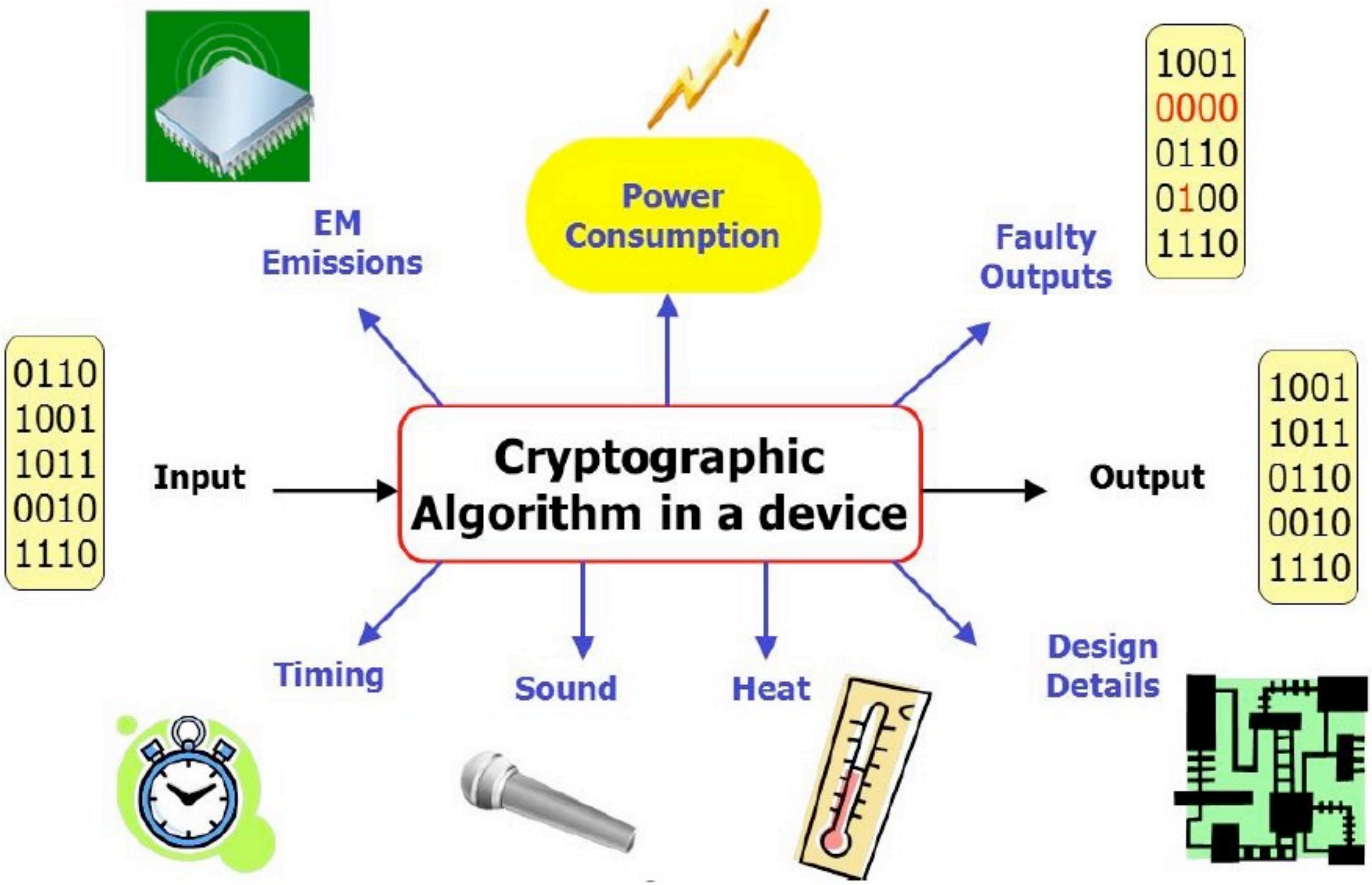
Presentation Flow

- Side-channel attacks
- Power analysis attacks (PAA)
- Previous countermeasures against PAA
- Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks
- Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique
- Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks
- Conclusion

Why Hardware Security is Important?



Side-Channel Attacks

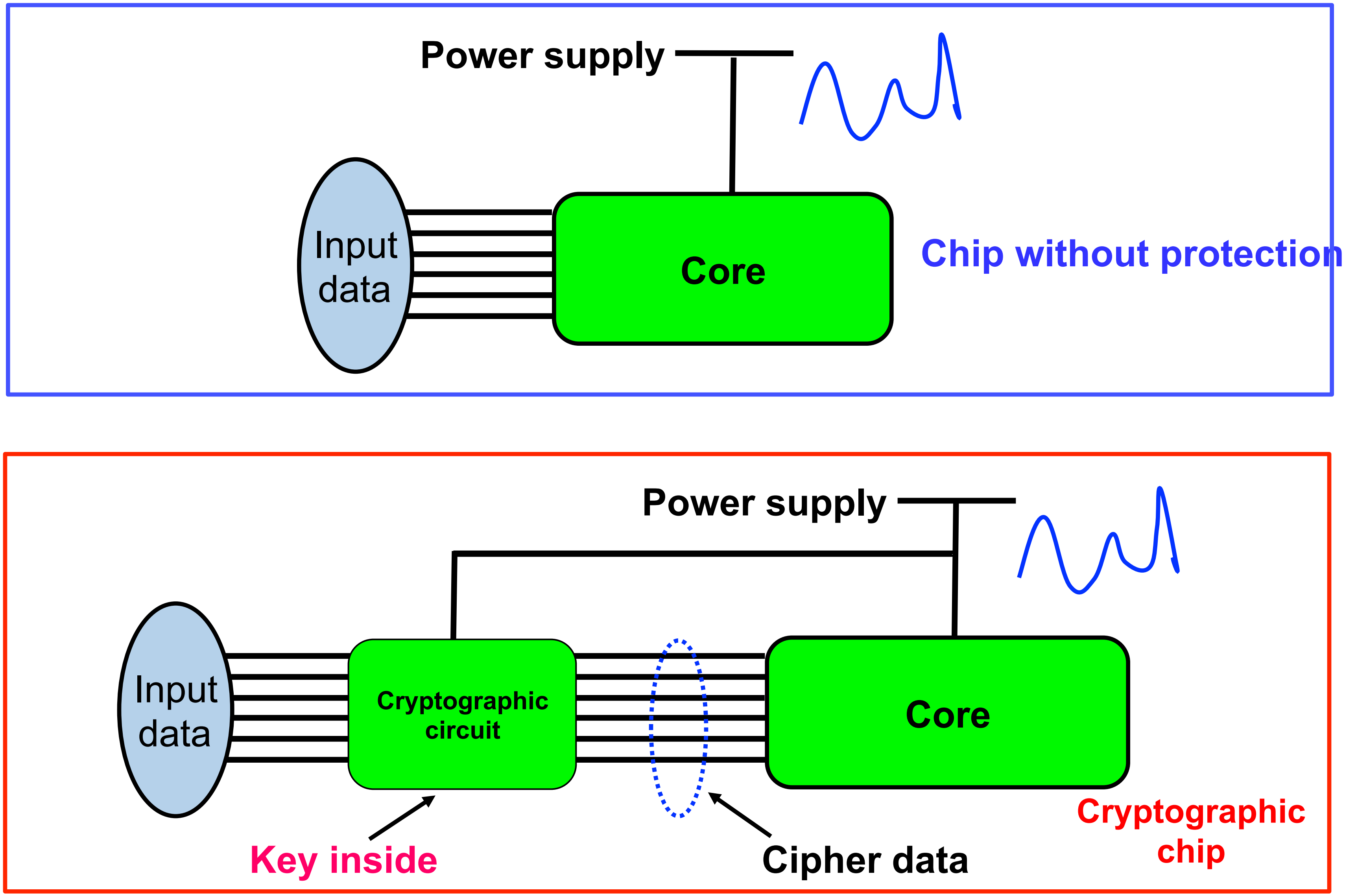


Possible side-channel attacks

Presentation Flow

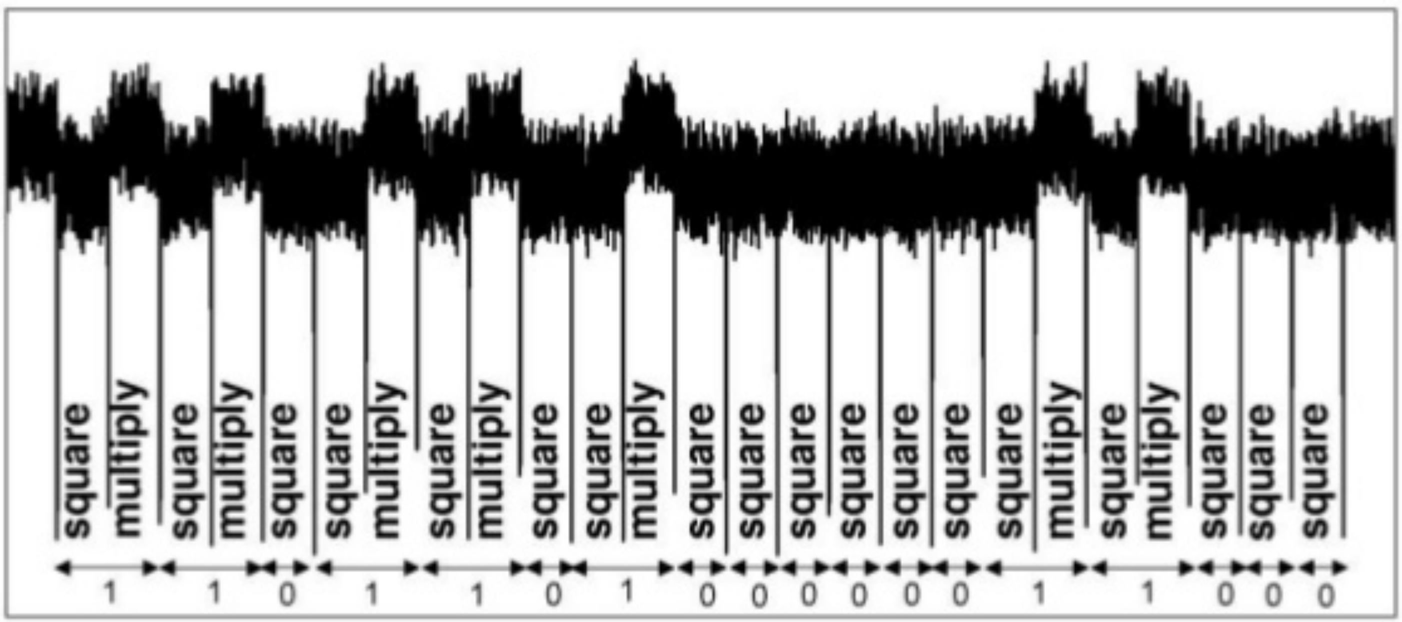
- Side-channel attacks
- Power analysis attacks (PAA)
- Previous countermeasures against PAA
- Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks
- Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique
- Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks
- Conclusion

Power Analysis Attacks



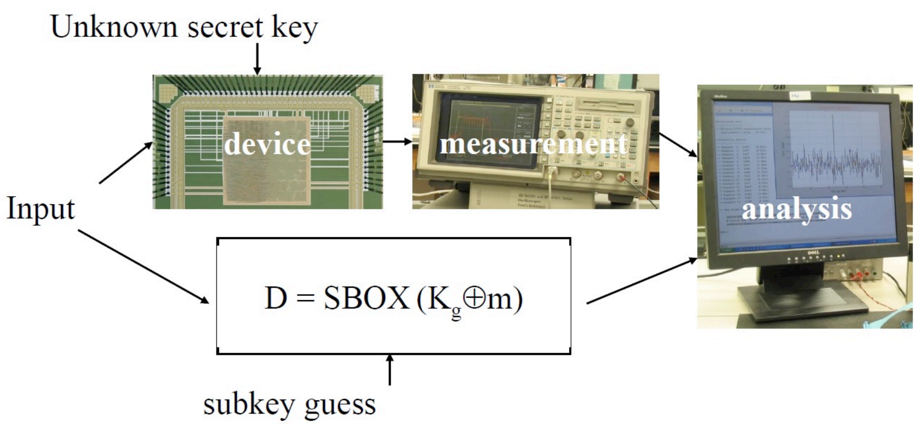
Simple Power Analysis (SPA) Attacks

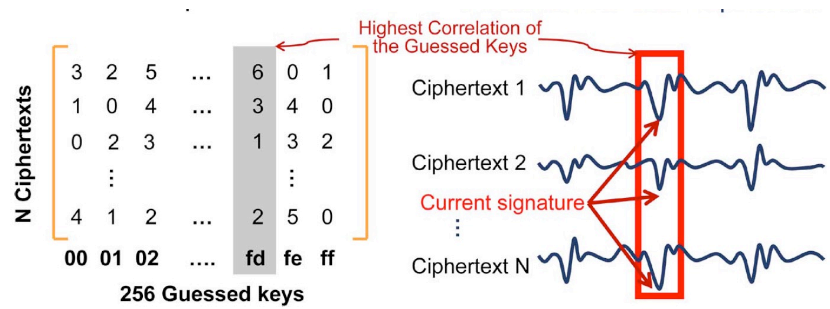
Simple **P**ower **A**nalysis: Directly analyze (few) traces, for example RSA:

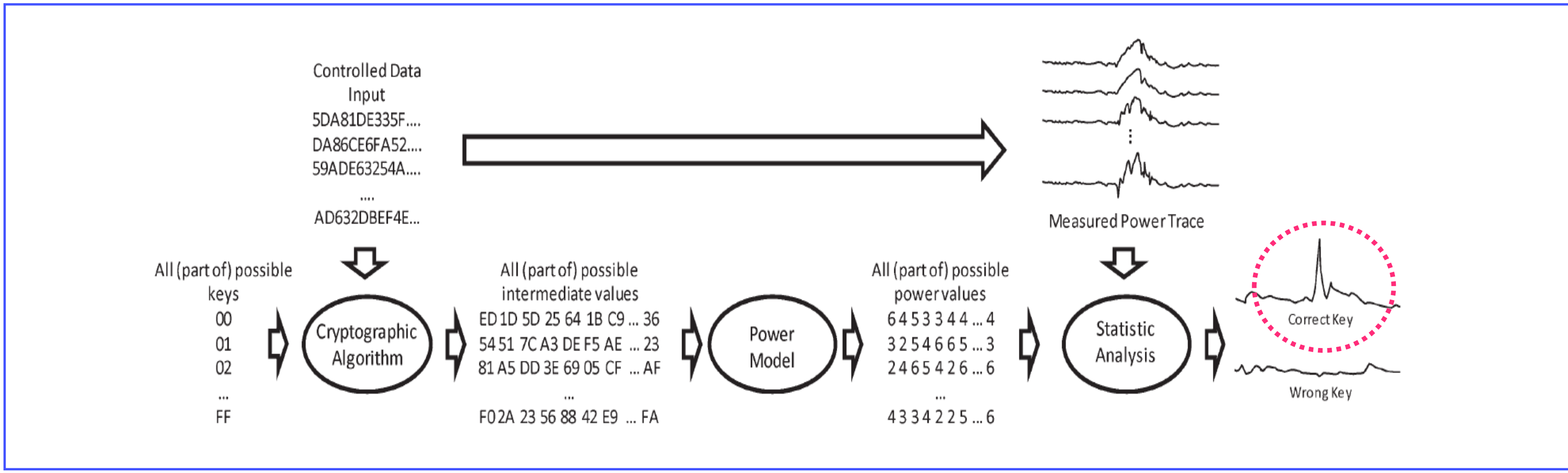


D. Oswald and R.-U. Bochum, “ID and IP theft with Side-Channel Attacks,” EMSEC, 2014

Conventional First-Order (CFO) Differential Power Analysis (DPA) Attacks

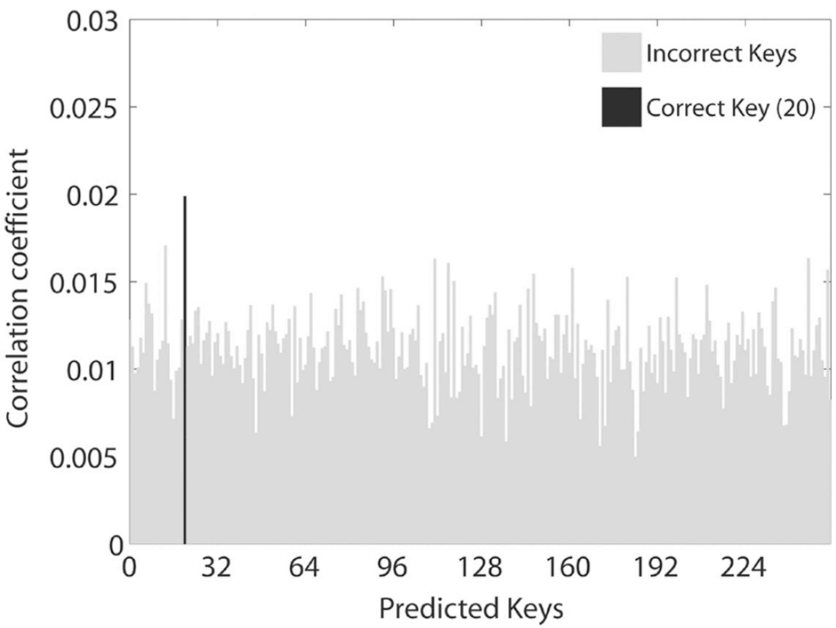




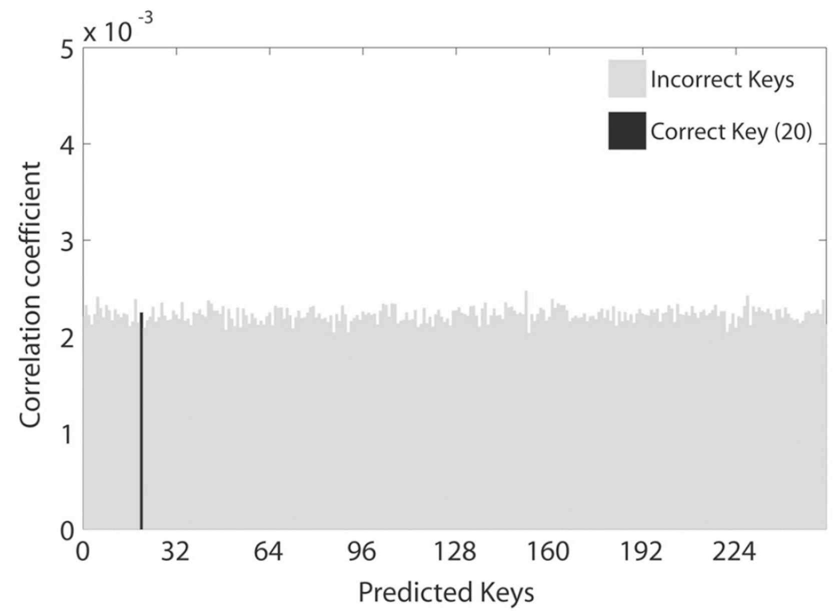


C. Tokunaga and D. Blaauw, “Securing Encryption Systems With a Switched Capacitor Current Equalizer,” IEEE J. Solid-State Cir., Jan. 2010
P.-C. Liu, H.-C. Chang, and C.-Y. Lee, “A Low Overhead DPA Countermeasure Circuit Based on Ring Oscillators,” *IEEE Trans. Cir. and Sys. 2: Express Briefs*, Jul. 2010

Results of CFO DPA Attacks



Successful CFO DPA attacks



Unsuccessful CFO DPA attacks

Correlation coefficient between the correct key and monitored power consumption is important

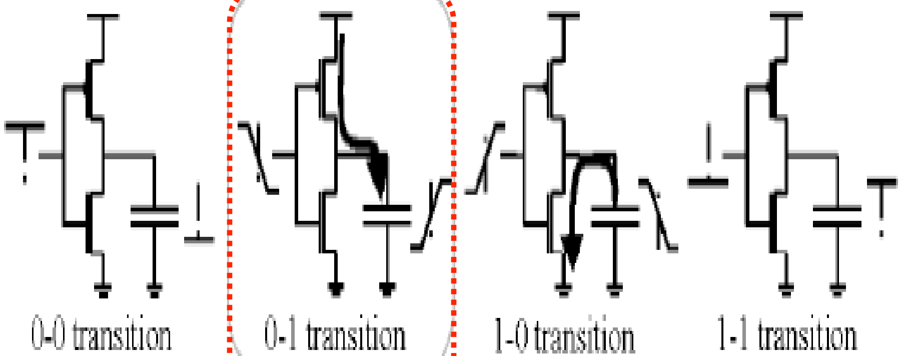
C. Tokunaga and D. Blaauw, "Securing Encryption Systems With a Switched Capacitor Current Equalizer," IEEE J. Solid-State Cir., Jan. 2010

Presentation Flow

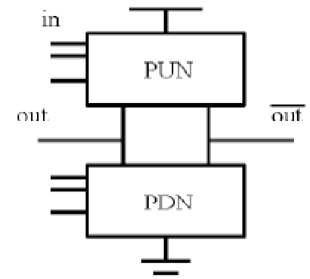
- Side-channel attacks
- Power analysis attacks (PAA)
- Previous countermeasures against PAA
- Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks
- Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique
- Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks
- Conclusion

Encryption Logic Circuit Modification

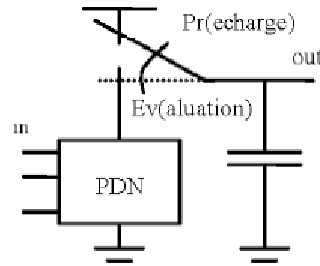
Power information leakage



0-1



in_i	in_{i+1}	out_i	out_{i+1}	$\overline{out}_i$	$\overline{out}_{i+1}$
0	1	1	0	0	1
1	0	0	1	1	0
0	0	1	1	0	0
1	1	0	0	1	1



in_i	in_{i+1}	out_{Ev}	out_{Pr}
0	1	0	1
1	0	1	1
0	0	1	1
1	1	0	1

differential logic
0-1 and 1-0 are the same
0-0 and 1-1 are the same

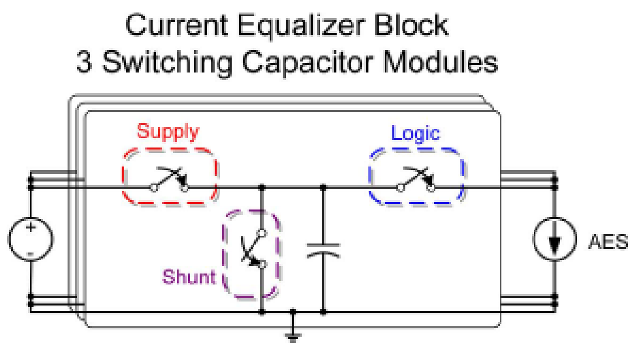
differential logic
0-1 and 1-1 are the same
0-0 and 1-0 are the same

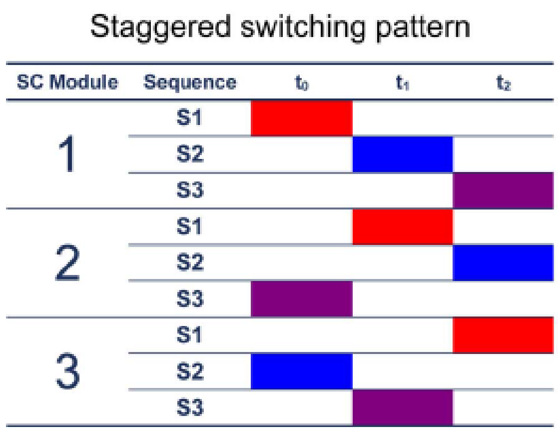
Combine them together

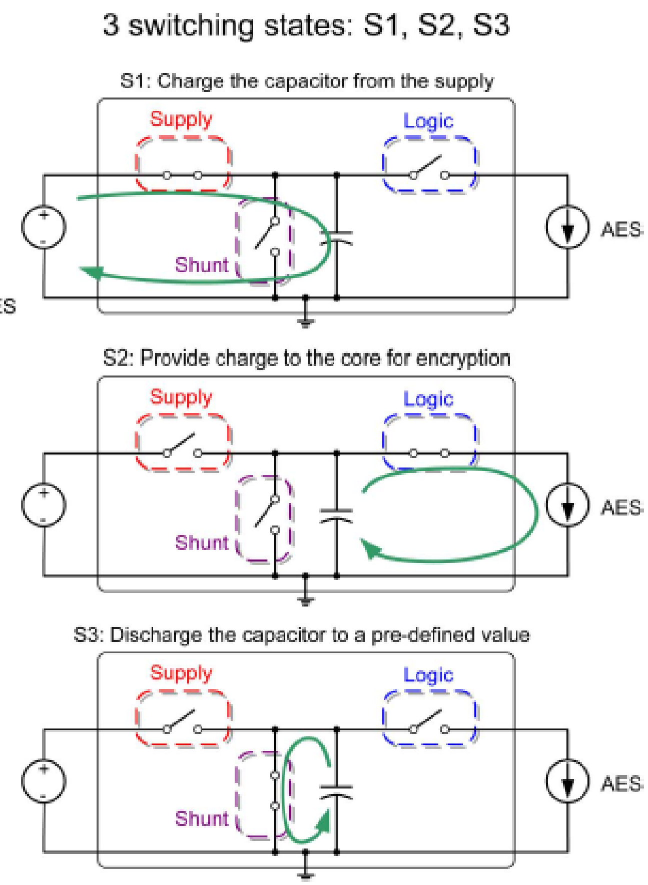
Drawback: High power/area/ performance overhead

K. Tiri, M. Akmal, and I. Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards," in *Proc. 28th European Solid-State Circuits*, Sep. 2002

Power Supply Scrambling







stage 1

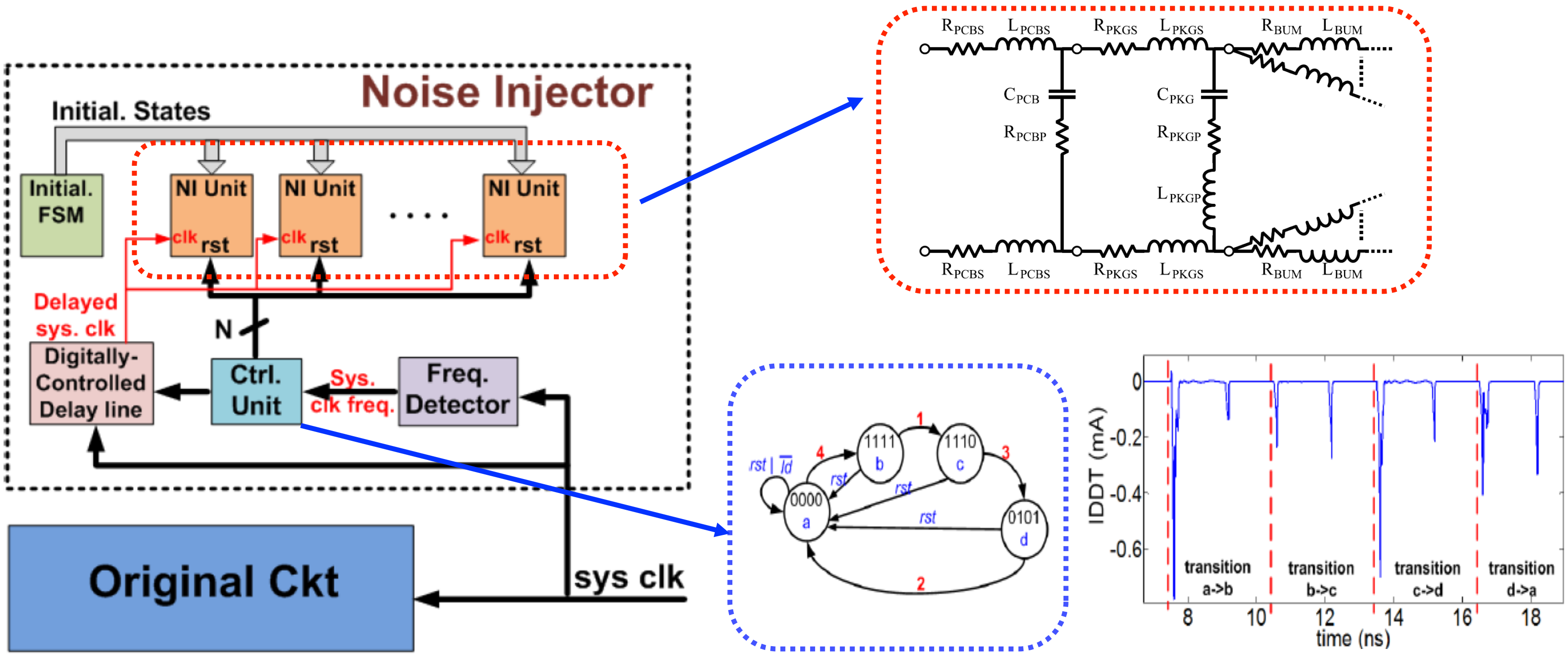
stage 2

stage 3

Drawback: High power/area/performance overhead

C. Tokunaga and D. Blaauw, "Securing Encryption Systems With a Switched Capacitor Current Equalizer," *IEEE J. Solid-State Circuits*, Jan. 2010

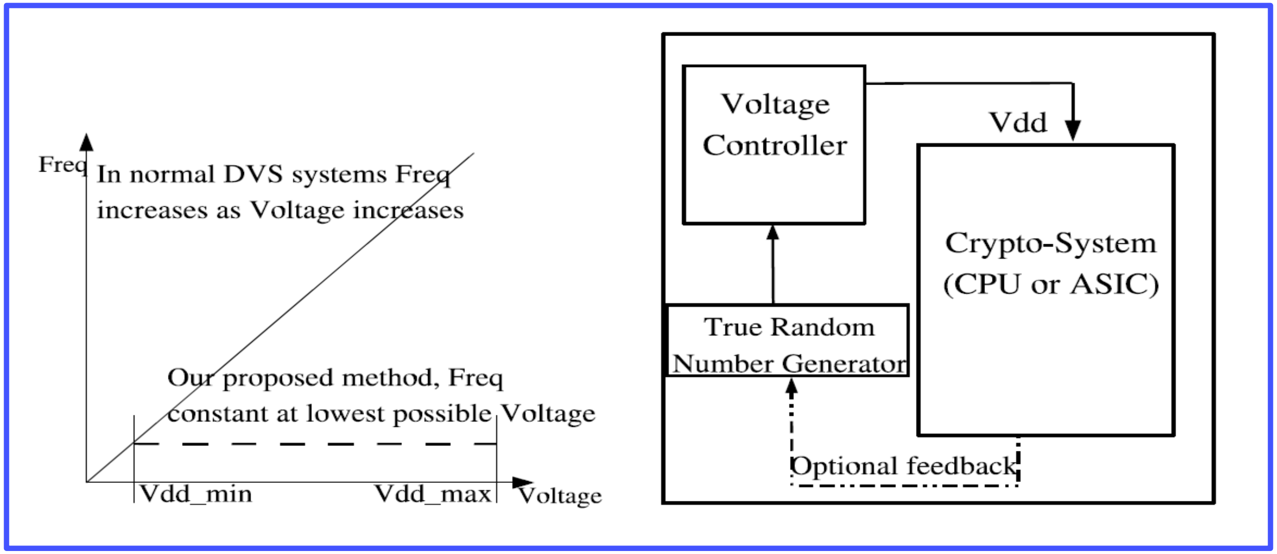
Power Delivery Network (PDN) Modification



Drawback: High PDN impedence hurts the circuit's energy efficiency and robustness

X. Wang, W. Yueh, D. B. Roy, S. Narasimhan, Y. Zheng, S. Mukhopadhyay, D. Mukhopadhyay and S. Bhunia, "Role of Power Grid in Side Channel Attack and Power-Grid-Aware Secure Design," in *Proc. Design Automation Conference (DAC)*, 2013

Random Dynamic Voltage Scaling (RDVS)



Input data dependent

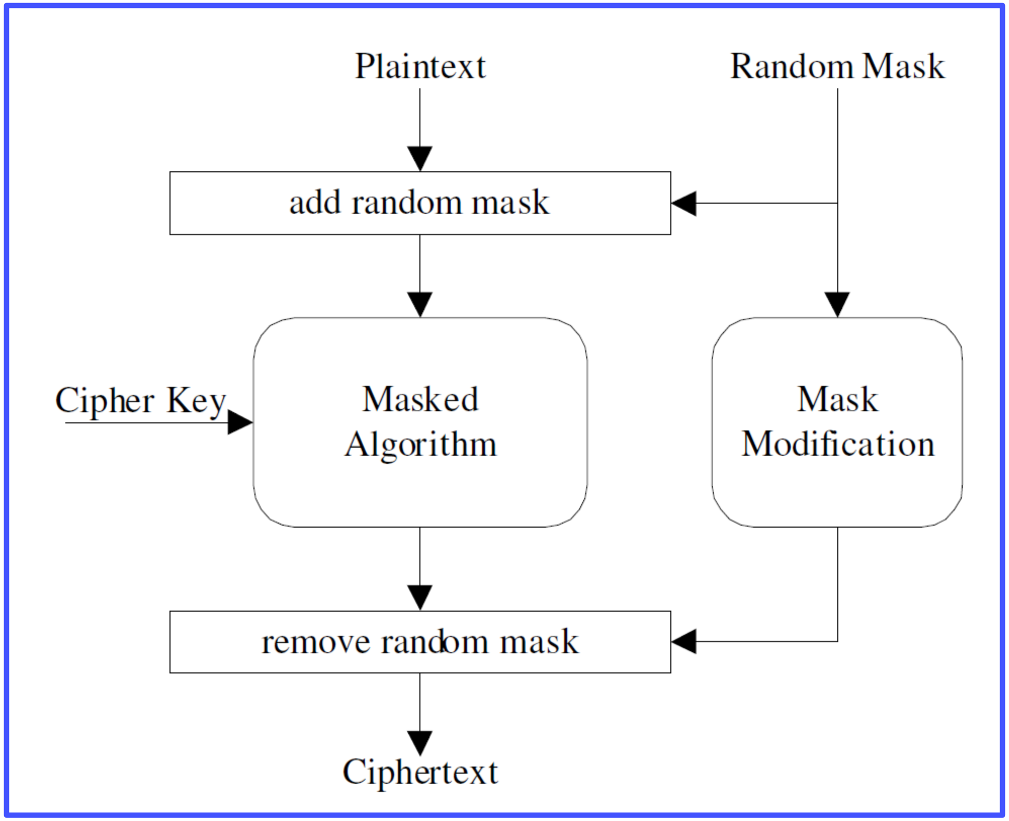
$$P_{dyn} = \alpha C V_{dd}^{2} f_c$$

Randomly alter V_{dd}

Drawback: High power overhead

K. Baddam and M. Zwolinski, "Evaluation of Dynamic Voltage and Frequency Scaling as a Differential Power Analysis Countermeasure," in *Proc. VLSI design*, Jan. 2007

Plaintexts Masking



Input data dependent

$$P_{dyn} = \alpha C V_{dd}^2 f_c$$

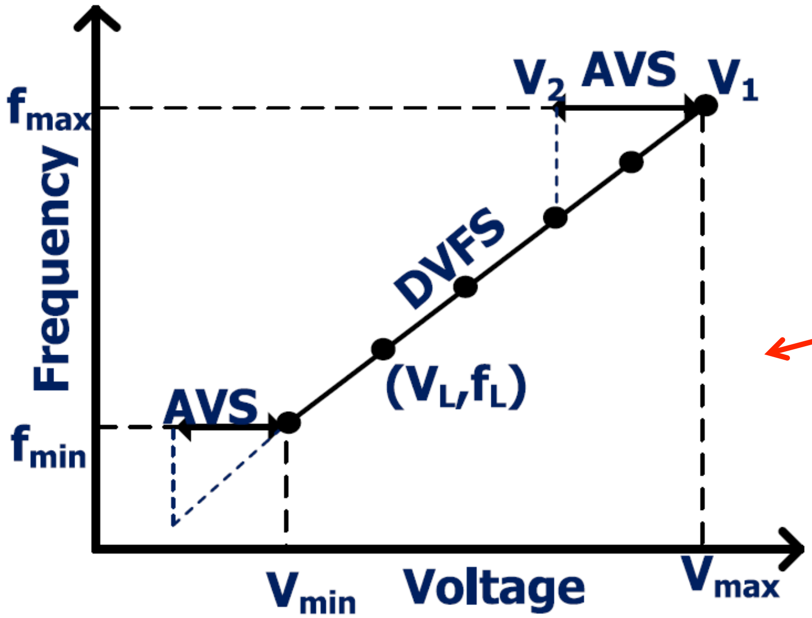
Drawback: High area/performance overhead due to a large amount of mask data

N. Pramstaller, E. Oswald, S. Mangard, F. K. Gurkaynak, and S. Hane, “A Masked AES ASIC Implementation,” in *Proc. Austrochip*, 2004

Presentation Flow

- Side-channel attacks
- Power analysis attacks (PAA)
- Previous countermeasures against PAA
- Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks
- Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique
- Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks
- Conclusion

Aggressive Voltage Scaling (AVS) Technique



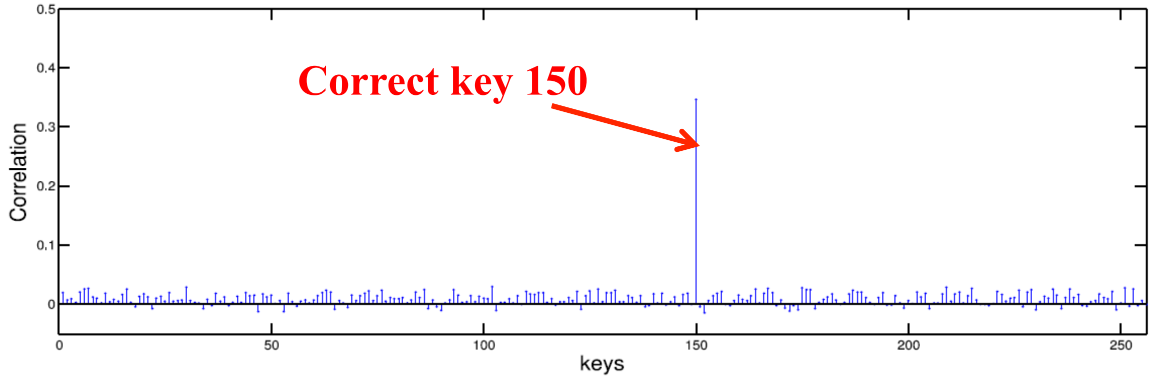
AVS technique

Scheme	Area	Power	Performance	PVT Tolerance
Logic Style (WDDL)	3X	4X	.25X	×
Masking	3X	-	0.5X	×
RDVFS	-	0.73X	0.85X	×
AFS	1.03X	1.05X	1.57X	√
AVS	1.03X	0.5X	0.95X	√

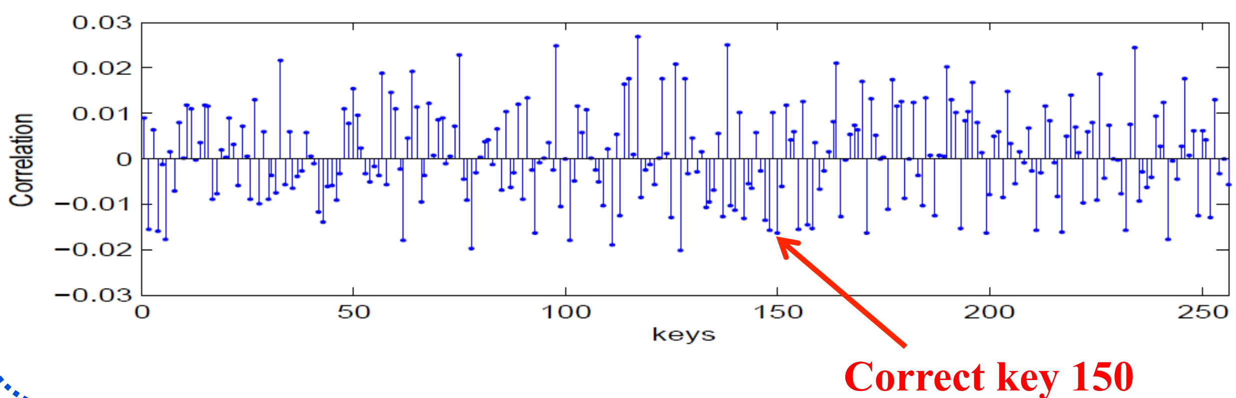
Low overhead

N. D. P. Avirneni and A. K. Somani, "Countering power analysis attacks using reliable and aggressive designs," IEEE Transactions on Computers, Jun. 2014.

AVS Technique Against CFO DPA Attacks



Successful CFO DPA attacks on an S-box without countermeasure after inputting 10 thousand plaintexts



Unsuccessful CFO DPA attacks on an S-box with AVS technique after inputting 1 million plaintexts

N. D. P. Avirneni and A. K. Somani, “Countering power analysis attacks using reliable and aggressive designs,” IEEE Transactions on Computers, Jun. 2014.

Presentation Flow

- Side-channel attacks
- Power analysis attacks (PAA)
- Previous countermeasures against PAA
- Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks
- Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique
- Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks
- Conclusion

BFO DPA Attacks on a Cryptographic Circuit with AVS Technique

Two adjacent power consumptions of a cryptographic circuit with AVS technique

$$P_{dyn,j} = \beta_{0\rightarrow 1,j} f_c V^2_{dd,[\frac{j}{h}]} C_L \xrightarrow{\text{CFO DPA attacks}} X_j$$

$$P_{dyn,j+1} = \beta_{0\rightarrow 1,j+1} f_c V^2_{dd,[\frac{j+1}{h}]} C_L \xrightarrow{\text{CFO DPA attacks}} X_{j+1}$$

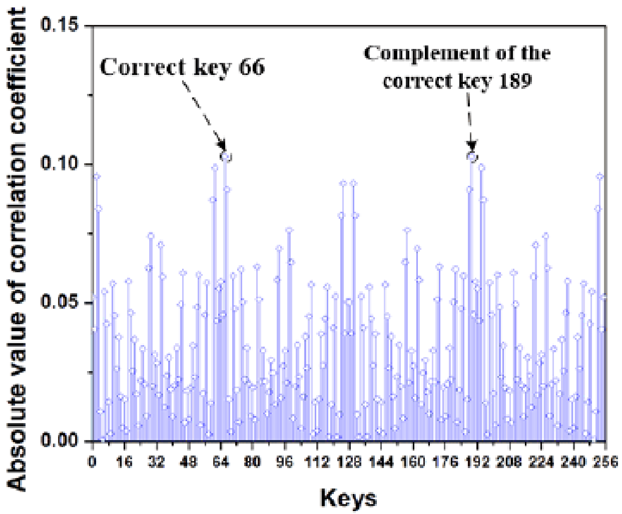
Two adjacent input data

V_{dd} changes slowly

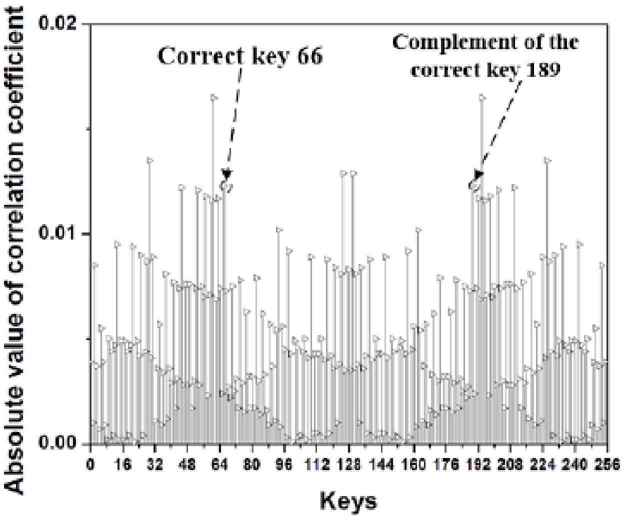
$$\frac{P_{dyn,j+1}}{P_{dyn,j}} = \frac{\beta_{0\rightarrow 1,j+1}}{\beta_{0\rightarrow 1,j}} \xrightarrow{\text{BFO DPA attacks}} X_{j+1}/X_j$$

The power noise induced by randomly reshuffling Supply voltage V_{dd} is eliminated by executing BFO DPA attacks!

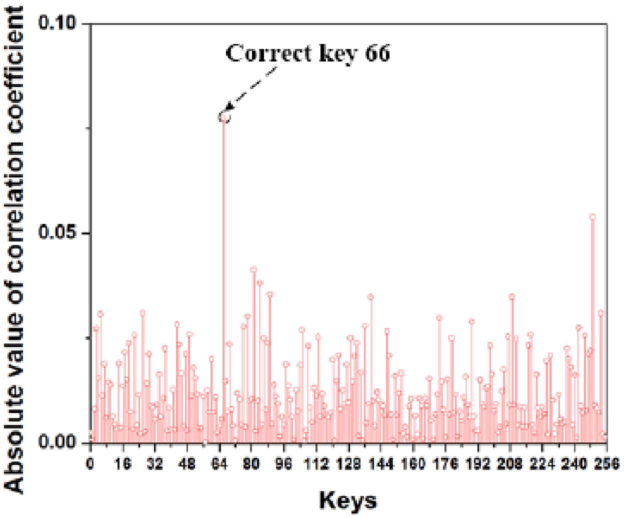
Results of DPA Attacks on S-Boxes with AVS Technique



Successful CFO DPA attacks
on an S-box without countermeasure
after inputting 1 thousand
plaintexts



Unsuccessful CFO DPA attacks
on an S-box with AVS technique
after inputting 100 thousand
plaintexts

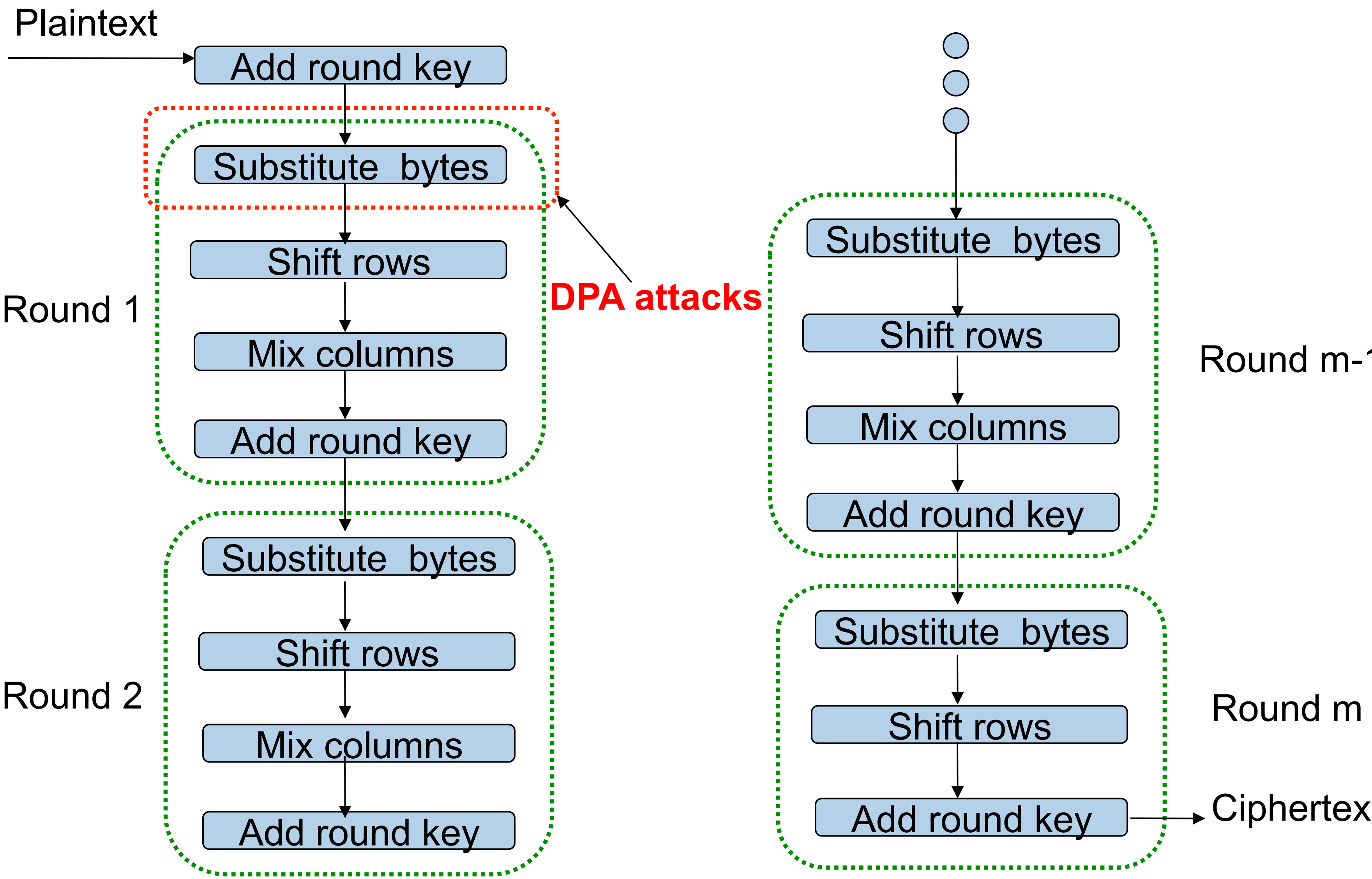


Successful BFO DPA attacks
on an S-box with AVS technique
after inputting 6 thousand
plaintexts

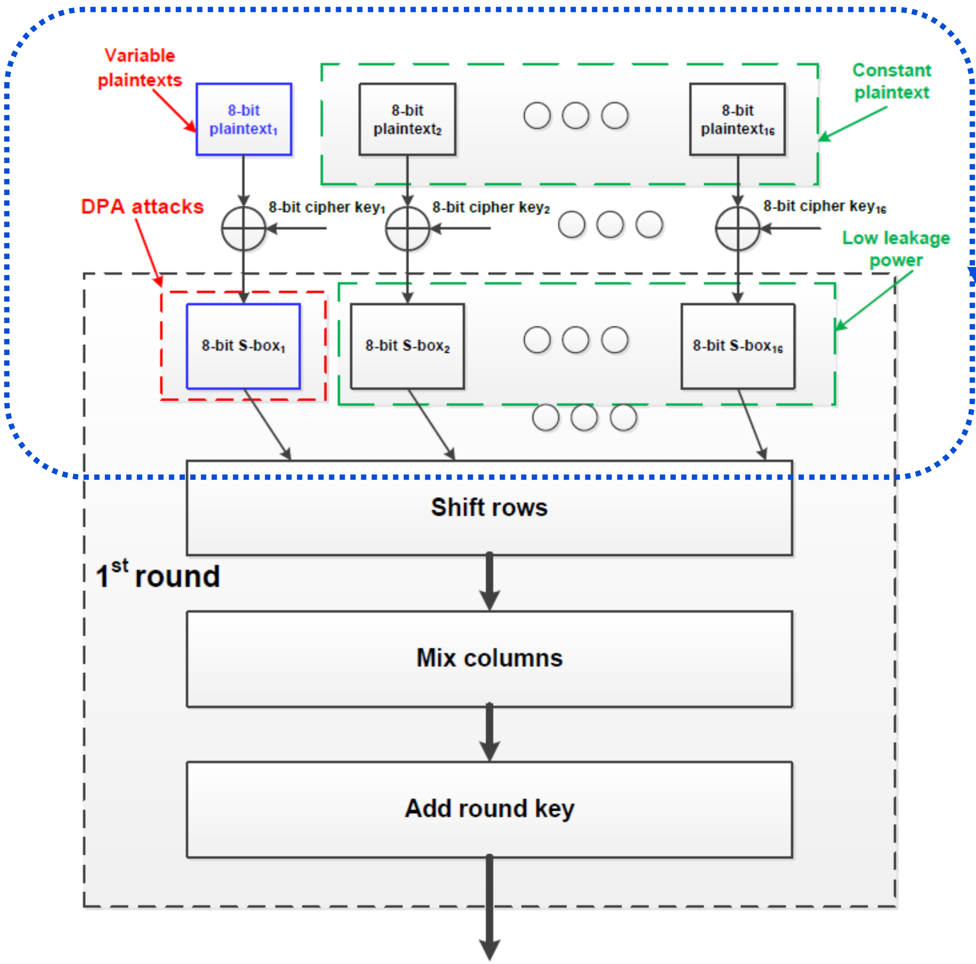
Presentation Flow

- Side-channel attacks
- Power analysis attacks (PAA)
- Previous countermeasures against PAA
- Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks
- Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique
- Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks
- Conclusion

Advanced Encryption Standard (AES) Cryptographic Algorithm



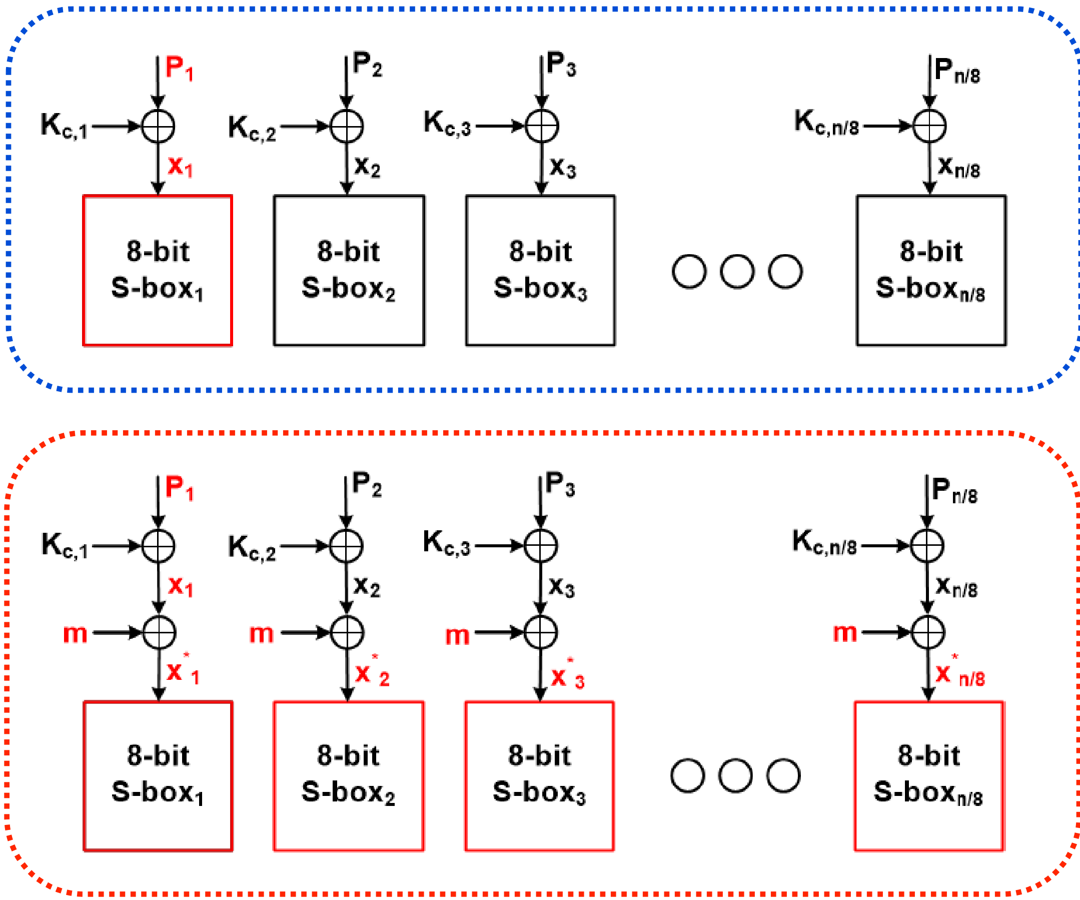
DPA Attacks on AES Engine



1st encryption round of a typical 128-bit AES engine

Select input plaintexts to simplify DPA attacks.

Proposed Lightweight Masked AES Engine



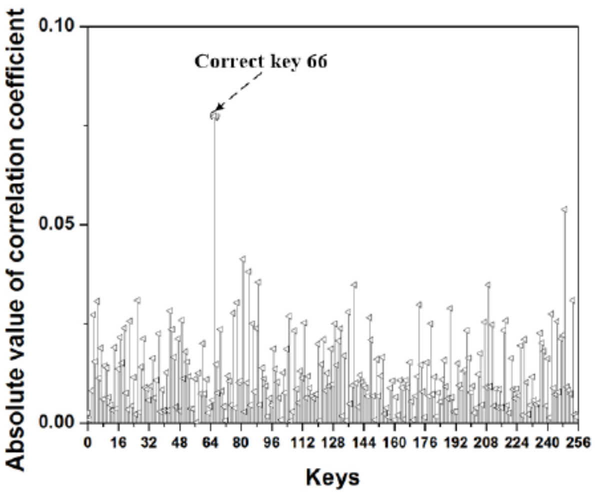
Conventional AES engine (1st encryption round)

Proposed lightweight masked AES engine (1st encryption round)

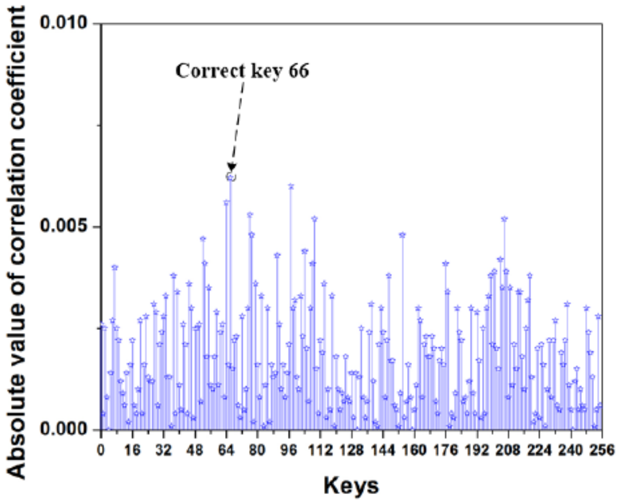
Mask: m=(00000000), (11111111), (00000000), (11111111), ... Constant sequence

or m=(00000000), (00000000), (11111111), (00000000), ... Random sequence

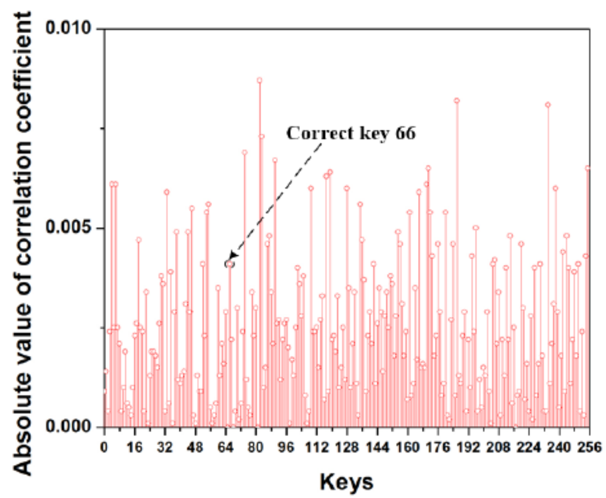
Results of BFO DPA Attacks on AES Engines with AVS Technique



Successful BFO DPA attacks on a conventional AES engine with AVS technique after inputting 6 thousand plaintexts



Successful BFO DPA attacks on a lightweight masked AES engine (constant masking sequence) with AVS technique after inputting 500 thousand plaintexts



Unsuccessful BFO DPA attacks on a lightweight masked AES engine (random masking sequence) with AVS technique after inputting 1 million plaintexts

Presentation Flow

- Side-channel attacks
- Power analysis attacks (PAA)
- Previous countermeasures against PAA
- Aggressive voltage scaling (AVS) against conventional first-order (CFO) DPA attacks
- Bivariate first-order (BFO) DPA attacks on cryptographic circuit with AVS technique
- Proposed countermeasure for securing cryptographic circuit with AVS technique against BFO DPA attacks
- Conclusion

Conclusion

- Cryptographic circuit is vulnerable against power analysis attacks
- Aggressive voltage scaling (AVS) technique is an efficient countermeasure against conventional first-order (CFO) DPA attacks with low overhead
- Conventional AES engine employs AVS technique is vulnerable against bivariate first-order (BFO) DPA attacks
- Lightweight random masked AES engine with AVS technique thwarts DPA attacks efficiently with negligible power/area/ performance overhead

Thanks!