Radboud University

Intrinsic Side-Channel Analysis Resistance and Efficient Masking

A case study of the use of SCA-related metrics and of design strategies leading to low-cost masking for CAESAR candidates

Ko Stoffelen

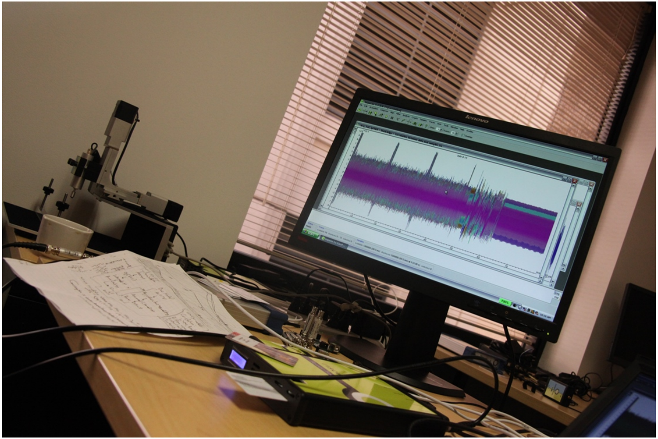
Master thesis presentation
August 27, 2015

Acknowledgements

- Supervisor: Lejla Batina
- And Kostas Papagiannopoulos
- Second reader: Joan Daemen

Outline

Side-Channel Analysis



Masking

- Countermeasure against SCA
- Arithmetic vs. Boolean
- Costs quadratic for nonlinear gates, e.g.:

$$z = x \wedge y \quad \rightarrow \quad \begin{aligned} &(x' = x \oplus x_m) \\ &(y' = y \oplus y_m) \\ &z' = x' \wedge y' \\ &z_m = (x_m \wedge y') \oplus (y_m \wedge x') \oplus (x_m \wedge y_m) \end{aligned}$$

Goals

- How can known metrics be used at the design stage to assess the intrinsic resistance of ciphers to implementation- and device-dependent attacks?

Radboud University

Goals

- How can known metrics be used at the design stage to assess the intrinsic resistance of ciphers to implementation- and device-dependent attacks?
- How can the costs of applying masking countermeasures to ciphers be reduced?

Context – CAESAR competition

ACORN	++AE	AEGIS	AES-CMCC	AES-COBRA
AES-COPA	AES-CPFB	AES-JAMBU	AES-OTR	AEZ
Artemia	Ascon	AVALANCHE	Calico	CBA
CBEAM	CLOC	Deoxys	ELmD	Enchilada
FASER	HKC	HS1-SIV	ICEPOLE	iFeed[AES]
Joltik	Julius	Ketje	Keyak	KIASU
LAC	Marble	McMambo	Minalpher	MORUS
NORX	OCB	OMD	PAEQ	PAES
PANDA	π-Cipher	POET	POLAWIS	PRIMATEs
Prøst	Raviyoyla	Sablier	SCREAM	SHELL
SILC	Silver	STRIBOB	Tiaoxin	TriviA-ck
Wheesht	YAES			

Context – CAESAR competition

ACORN	++AE	AEGIS	AES-CMCC	AES-COBRA
AES-COPA	AES-CPFB	AES-JAMBU	AES-OTR	AEZ
Artemia	Ascon	AVALANCHE	Calico	CBA
CBEAM	CLOC	Deoxys	ELmD	Enchilada
FASER	HKC	HS1-SIV	ICEPOLE	iFeed[AES]
Joltik	Julius	Ketje	Keyak	KIASU
LAC	Marble	McMambo	Minalpher	MORUS
NORX	OCB	OMD	PAEQ	PAES
PANDA	π-Cipher	POET	POLAWIS	PRIMATEs
Prøst	Raviyoyla	Sablier	SCREAM	SHELL
SILC	Silver	STRIBOB	Tiaoxin	TriviA-ck
Wheesht	YAES			

Context – CAESAR competition

ACORN	++AE	AEGIS	AES-CMCC	AES-COBRA
AES-COPA	AES-CPFB	AES-JAMBU	AES-OTR	AEZ
Artemia	Ascon	AVALANCHE	Calico	CBA
CBEAM	CLOC	Deoxys	ELmD	Enchilada
FASER	HKC	HS1-SIV	ICEPOLE	iFeed[AES]
Joltik	Julius	Ketje	Keyak	KIASU
LAC	Marble	McMambo	Minalpher	MORUS
NORX	OCB	OMD	PAEQ	PAES
PANDA	π-Cipher	POET	POLAWIS	PRIMATEs
Prøst	Raviyoyla	Sablier	SCREAM	SHELL
SILC	Silver	STRIBOB	Tiaoxin	TriviA-ck
Wheesht	YAES			

Context – CAESAR competition

(S-boxes of)

8x8	5x5	4x4
AES	Ascon	Joltik
AES^{-1}	ICEPOLE	Joltik^{-1}
iSCREAM	Ketje/Keyak	LAC
SCREAM	PRIMATE	Minalpher
SCREAM^{-1}	PRIMATE^{-1}	Prøst
		RECTANGLE
		RECTANGLE^{-1}

Traditional S-box design criteria

S-box	Width	Nonlinearity	Degree	δ
AES	8	112	7	4
iSCREAM	8	96	6	16
SCREAM	8	96	5/6	16
Ascon	5	8	2	8
ICEPOLE	5	8	4	8
Ketje/Keyak	5	8	2	8
PRIMATE	5	12	2/3	2
Joltik	4	4	3	4
LAC	4	4	3	4
Minalpher	4	4	3	4
Prøst	4	4	3	4
RECTANGLE	4	4	3	4

SCA metrics

Why additional SCA-related criteria?

- SCA highly effective
- Countermeasures only applied to implementations
- Countermeasures expensive (area, speed)
- Perfect countermeasure does not exist
- A lot to gain with an intrinsically more resistant S-box

Existing metrics

- Number of measurements
- Signal-to-noise ratio
- Transparency order
- Success rate
- New signal-to-noise ratio
- Guessing entropy
- Confusion coefficient
- Modified transparency order
- Second minimum distance

But. . .

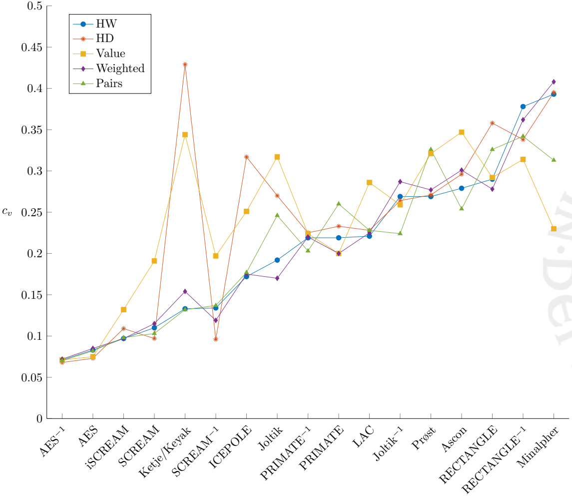
- Metrics take different approaches
- Metrics work under different assumptions (power model, Gaussian noise, . . .)
- Some only applicable in certain cases
- Not all meaningful in design stage

Radboud University

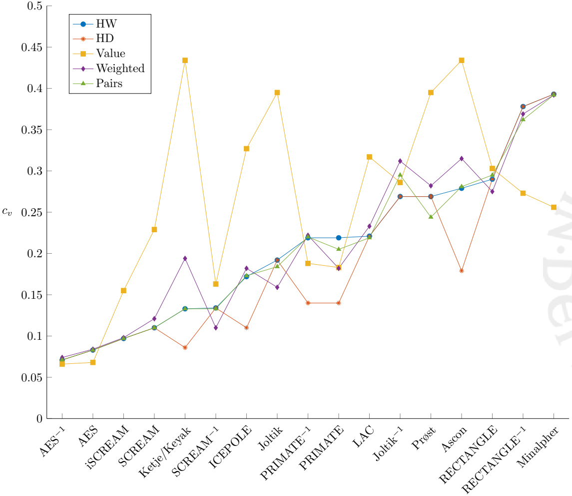
Confusion coefficient

- Intuitively: probability that power analysis attack succeeds
- Result is frequency distribution
- Lower mean $\Rightarrow$ higher resistance
- Mean only depends on size of S-box
- Higher variance $\Rightarrow$ higher resistance

Confusion coefficient – first-order



Confusion coefficient – second-order



Confusion coefficient conclusions

- Confusion coefficient can deal with low-entropy masking schemes

Confusion coefficient conclusions

- Confusion coefficient can deal with low-entropy masking schemes
- The ranking of the S-boxes according to the confusion coefficient is mostly preserved by various power consumption models

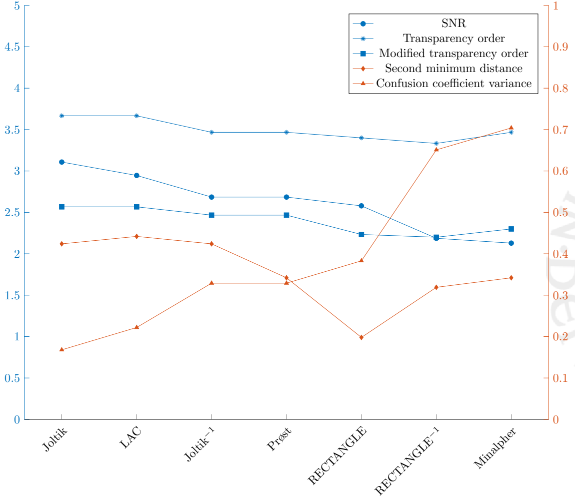
Confusion coefficient conclusions

- Confusion coefficient can deal with low-entropy masking schemes
- The ranking of the S-boxes according to the confusion coefficient is mostly preserved by various power consumption models
- The ranking of the S-boxes according to the confusion coefficient is mostly preserved by higher-order attacks

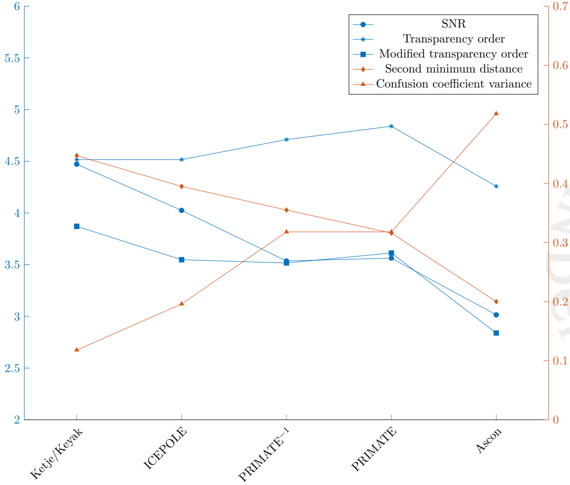
Confusion coefficient conclusions

- Confusion coefficient can deal with low-entropy masking schemes
- The ranking of the S-boxes according to the confusion coefficient is mostly preserved by various power consumption models
- The ranking of the S-boxes according to the confusion coefficient is mostly preserved by higher-order attacks
- Assumption: mean and variance are of similar importance

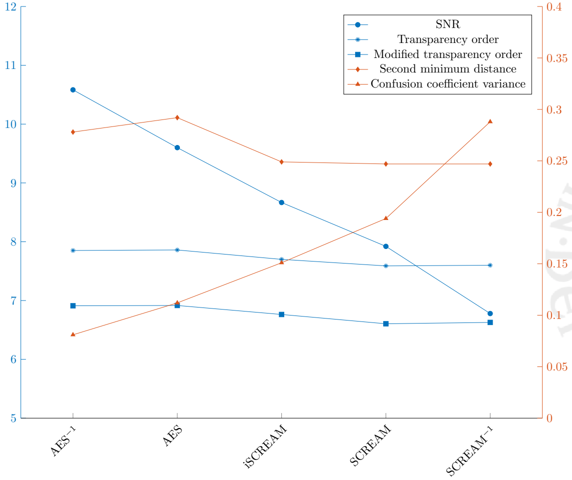
SCA metrics comparison



SCA metrics comparison



SCA metrics comparison



SCA metrics verdict

- SNR, modified transparency order, and confusion coefficient are consistent in their predictions

SCA metrics verdict

- SNR, modified transparency order, and confusion coefficient are consistent in their predictions
- Second minimum distance a bit less, requires further research

SCA metrics verdict

- SNR, modified transparency order, and confusion coefficient are consistent in their predictions
- Second minimum distance a bit less, requires further research
- Metrics behave as they should under various circumstances

SCA metrics verdict

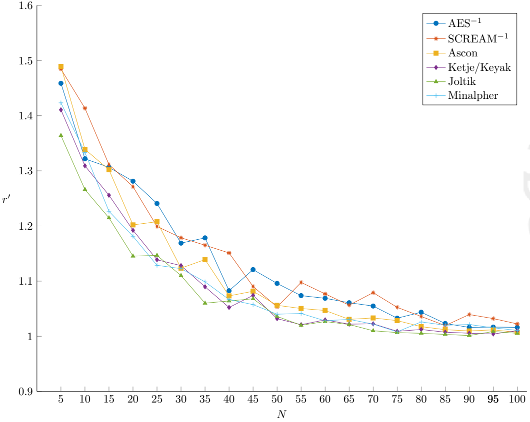
- SNR, modified transparency order, and confusion coefficient are consistent in their predictions
- Second minimum distance a bit less, requires further research
- Metrics behave as they should under various circumstances
- Minalpher, Ascon, SCREAM^{-1} are suggested to have the most DPA-resistant S-boxes

SCA metrics verdict

- SNR, modified transparency order, and confusion coefficient are consistent in their predictions
- Second minimum distance a bit less, requires further research
- Metrics behave as they should under various circumstances
- Minalpher, Ascon, SCREAM^{-1} are suggested to have the most DPA-resistant S-boxes
- However. . .

SCA metrics verdict

- SCA simulation results do not agree
- Usefulness of metrics still unclear



Optimizing masking costs

Nonlinear operations

Multiplicative complexity (MC)

- Recall that the cost of masking nonlinear operations is quadratic in the number of inputs

Multiplicative complexity (MC)

- Recall that the cost of masking nonlinear operations is quadratic in the number of inputs
- Most nonlinear operations in the nonlinear part of the primitive: the S-box

Multiplicative complexity (MC)

- Recall that the cost of masking nonlinear operations is quadratic in the number of inputs
- Most nonlinear operations in the nonlinear part of the primitive: the S-box
- MC: minimal number of `AND`/`OR` gates required to implement function

Multiplicative complexity (MC)

- Recall that the cost of masking nonlinear operations is quadratic in the number of inputs
- Most nonlinear operations in the nonlinear part of the primitive: the S-box
- MC: minimal number of `AND`/`OR` gates required to implement function
- Goal is to compute the MC of CAESAR S-boxes

Minimizing AND/OR gates

- Existing logic synthesis tools not very helpful
  - E.g. Espresso, SIS, misII, Logic Friday, ABC, ...
- Instead: convert to SAT and let SAT solvers do the work
- Converting problem to SAT nontrivial, but feasible

Reducing decisional MC to SAT

$$
\begin{aligned}
q_0 &= a_0 + a_1 \cdot x_0 + a_2 \cdot x_1 + a_3 \cdot x_2 + a_4 \cdot x_3 \\
q_1 &= a_5 + a_6 \cdot x_0 + a_7 \cdot x_1 + a_8 \cdot x_2 + a_9 \cdot x_3 \\
t_0 &= q_0 \cdot q_1 \\
q_2 &= a_{10} + a_{11} \cdot x_0 + a_{12} \cdot x_1 + a_{13} \cdot x_2 + a_{14} \cdot x_3 + a_{15} \cdot t_0 \\
q_3 &= a_{16} + a_{17} \cdot x_0 + a_{18} \cdot x_1 + a_{19} \cdot x_2 + a_{20} \cdot x_3 + a_{21} \cdot t_0 \\
t_1 &= q_2 \cdot q_3 \\
q_4 &= a_{22} + a_{23} \cdot x_0 + a_{24} \cdot x_1 + a_{25} \cdot x_2 + a_{26} \cdot x_3 + a_{27} \cdot t_0 + a_{28} \cdot t_1 \\
q_5 &= a_{29} + a_{30} \cdot x_0 + a_{31} \cdot x_1 + a_{32} \cdot x_2 + a_{33} \cdot x_3 + a_{34} \cdot t_0 + a_{35} \cdot t_1 \\
t_2 &= q_4 \cdot q_5 \\
y_0 &= a_{36} x_0 + a_{37} \cdot x_1 + a_{38} \cdot x_2 + a_{39} \cdot x_3 + a_{40} \cdot t_0 + a_{41} \cdot t_1 + a_{42} \cdot t_2 \\
y_1 &= a_{43} x_0 + a_{44} \cdot x_1 + a_{45} \cdot x_2 + a_{46} \cdot x_3 + a_{47} \cdot t_0 + a_{48} \cdot t_1 + a_{49} \cdot t_2 \\
y_2 &= a_{50} x_0 + a_{51} \cdot x_1 + a_{52} \cdot x_2 + a_{53} \cdot x_3 + a_{54} \cdot t_0 + a_{55} \cdot t_1 + a_{56} \cdot t_2 \\
y_3 &= a_{57} x_0 + a_{58} \cdot x_1 + a_{59} \cdot x_2 + a_{60} \cdot x_3 + a_{61} \cdot t_0 + a_{62} \cdot t_1 + a_{63} \cdot t_2
\end{aligned}
$$

My work

- Wrote scripts to generate logic formulas in ANF from S-box and given MC
- Use tool to convert ANF to CNF
- Let MiniSAT and CryptoMiniSAT do the work on DS cluster node
- Wrote scripts to convert back to S-box implementation

Radboud University

Results

S-box	MC	S-box	MC
AES	≤ 32	PRIMATE^{-1}	$\in \{6, 7, 8, 9, 10\}$*
AES^{-1}	≤ 32	Joltik	4
iSCREAM	≤ 12	Joltik^{-1}	4*
SCREAM	≤ 11	LAC	4*
SCREAM^{-1}	≤ 11	Minalpher	5*
Ascon	5	Prøst	4
ICEPOLE	6*	RECTANGLE	4
Ketje/Keyak	5	RECTANGLE^{-1}	4*
PRIMATE	$\in \{6, 7\}$*		

Optimizing masking costs

Comparing CAESAR candidates

High-level operations

- Table lookups
- Bitwise Boolean functions
- Shifts and rotates
- Modular addition/multiplication
- Modular polynomial multiplication

Results

Operation	Table lookups	Bitwise Boolean	Shifts/ rotates	Mod. add. and mult.	Mod. poly. mult.
AES	256 bytes	XOR	Fixed		✓
iSCREAM	512 bytes	AND,OR,XOR	Fixed	× mod 256	
SCREAM	512 bytes	AND,OR,XOR		× mod 256	
Ascon		AND,OR,XOR	Fixed		
ICEPOLE	96 bytes	AND,XOR	Fixed		
Ketje/Keyak		AND,XOR	Fixed		
PRIMATE	25 bytes	XOR	Fixed		✓
Joltik	64 bytes	XOR	Fixed	+ mod 16	✓
LAC	16 bytes	XOR	Fixed		
Minalpher	16 bytes	XOR			
Prøst		AND,XOR	Fixed		
RECTANGLE		AND,OR,XOR	Fixed		

Results

- Expected masking costs not so high on average
- Ascon, Ketje, Keyak, LAC, Minalpher, Prøst, and RECTANGLE stand out
- Designers should use operations that are cheap to mask using a Boolean scheme

Conclusions

- SNR, modified transparency order, and confusion coefficient credible in theory

Conclusions

- SNR, modified transparency order, and confusion coefficient credible in theory
- However, SCA simulations do not reflect the expectations suggested by metrics

Conclusions

- SNR, modified transparency order, and confusion coefficient credible in theory
- However, SCA simulations do not reflect the expectations suggested by metrics
- For 4- and 5-bit S-boxes, we can find an implementation with a provably minimum number of AND/OR operations

Conclusions

- SNR, modified transparency order, and confusion coefficient credible in theory
- However, SCA simulations do not reflect the expectations suggested by metrics
- For 4- and 5-bit S-boxes, we can find an implementation with a provably minimum number of `AND`/`OR` operations
- Ascon, Ketje, Keyak, LAC, Minalpher, Prøst, and RECTANGLE are expected to have the lowest masking costs

Questions

?