Implementation of a Boolean Masking Scheme for the SCREAM Cipher

William Diehl and Kris Gaj

Department of Electrical and Computer Engineering, George Mason University, Fairfax, Virginia, USA, http://cryptography.gmu.edu

Introduction

- Physical cryptographic implementations subject to side-channel attack (SCA)
- Boolean masking is one countermeasure applied against power-analysis SCA
- CAESAR, the Competition for Authenticated Encryption: Security, Applicability, and Robustness, evaluates cipher candidates to select a final portfolio
- SCREAM is a Round Two CAESAR candidate with bitslice S-Box designed to be easily masked using Boolean masking scheme
- This research implements 1st order Boolean masking scheme in the full SCREAM cipher, and compares masking cost with equivalent-masked version of AES

Previous Work

- Studies of Simple Power Analysis (SPA) and Differential Power Analysis (DPA) side-channel attacks (SCA) [Kocher et al, 1999]
- Duplication method; early Boolean masking [Goubin & Patarin, 1999]
- Security against probing attacks along *d* wires [Ishai, Sahai, Wagner, 2003]
- Masking schemes for DES, AES, SHA-3 candidates [Pramstaller et al, 2004; Oswald et al, 2004; Standaert et al, 2006; Francq et al, 2012]
- Boolean masking applied to $GF(2^8)$ inversion of AES [Prouff & Rivain, 2010]
- Securing bitslice ciphers against power analysis attacks and "easy-to-mask" bitslices [Daemen et al, 2001; Grosso et al, 2014]
- AES implementations using subfields of $GF(2^8)$ [Satoh et al, 2001; Canright, 2005]
- Masked AES Implementations using AES S-Box using subfields of $GF(2^8)$ [Oswald et al, 2005; Zakeri et al, 2007; Canright & Batina, 2008; Kim et al, 2007]
- Masking of AES in FPGA [Yuan et al, 2011; Regazzoni & Standaert, 2011]

Application of Boolean masking to Sensitive Variable

Apply Boolean masking to sensitive variable as follows:

- Mask sensitive variable *a* as *a'* = $a \oplus r_a$, where r_a is source of random masking
- Sensitive variables are *x* (separated into *x'* and r_x) and *key* (separated into *key'* and r_{key})
- Masking trivial for linear transformations (like L-Box) since $L[a] = L[a' \oplus r_a] = L[a'] \oplus L[r_a]$
- Masking difficult for non-linear transformations (like S-Box); Apply Alg. 1 to all expressions

ALGORITHM 1 – EXPANSION TO BOOLEAN MASKING

1. Variables a, b, and c are separated as $a = a' \oplus r_a$, $b = b' \oplus r_b$, $c = c' \oplus r_c$, where r_a, r_b, and r_c are random variables
2. Expand expressions of type $x = a \oplus b$ to
   $x' = a' \oplus b'$
   $r_x = r_a \oplus r_b$
3. Expand expressions of type $x = a \oplus (b \wedge c)$ to
   $x' = a' \oplus (b' \wedge c') \oplus (b' \wedge r_c)$
   $r_x = r_a \oplus (r_b \wedge c') \oplus (r_b \wedge r_c)$
4. Expand expressions of type $x = a \oplus (b \vee c)$ to
   $x' = a' \oplus (b' \wedge c') \oplus (b' \vee r_c)$
   $r_x = r_a \oplus (r_b \vee c') \oplus (r_b \wedge r_c)$

Figure 1 - Algorithm to apply Boolean Masking to logic expressions

Estimated Overhead resulting from Boolean Masking

- In d^{th} order masking, sensitive variable separated into d + 1 shares
- The gate count increases as $\sim(d+1)^2$ for non-linear operations

Operation	Required XOR gates	Required AND/OR gates
$a \oplus b$	(d+1) × #(XOR gates)	0
$a \oplus b \wedge c$	$(d+1)^2$ × #(XOR gates)	$(d+1)^2$ × #(AND gates)
$a \oplus b \vee c$	$(d+1)^2$ × #(XOR gates)	$(d+1)^2$ × #(OR gates)

Table 1 - Masking cost in gate count for dth order Boolean masking

Boolean Masking applied to SCREAM Block Cipher

- Boolean masking scheme applied on SCREAM step function using "Unrolled x2" (i.e., two rounds per clock cycle) architecture.
- Masked step function (Fig. 3) shares invertible S-Boxes to save resources

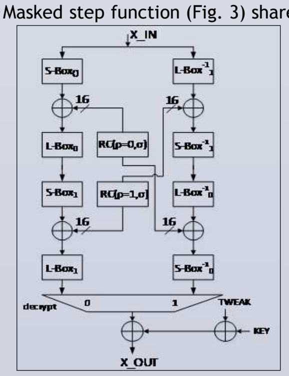

Figure 2 - Non-masked SCREAM Step Function with two rounds per step and no sharing of S-Boxes. Bus widths are 128 bits unless indicated.

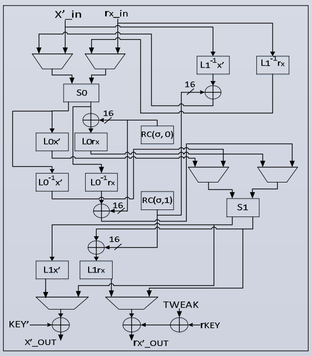

Figure 3 - Masked SCREAM Step Function with two rounds per step and sharing of S-Boxes. Bus widths are 128 bits unless indicated

Results of 1st order Boolean Masking of Full SCREAM Cipher

- Implementation in Virtex-6 FPGA includes GMU API for Authenticated Ciphers
- Masking and implementation with and without shared S-Boxes. Shared S-Boxes more efficiently masked, since majority of growth of Boolean masking is in S-Box.
- In best case, TP/A ratio of masked cipher is 50% of non-masked cipher.

	LUTs	Slices	Frequency (MHz)	Throughput (Mbps)	Throughput/ Area(Mbps/LUT)
SCREAM without shared S-Boxes					
Non-masked	3140	1043	99.8	1161	0.370
Masked	5605	1750	73.1	850	0.152
Ratio	1.79	1.68	0.73	0.73	0.411
SCREAM with shared S-Boxes					
Non-masked	2912	1003	89.2	1038	0.356
Masked	4691	1480	72.0	838	0.179
Ratio	1.61	1.48	0.81	0.81	0.502

Table 2 - Comparison of non-masked to masked versions of Full SCREAM Cipher in terms of Area (LUTs), Performance (MHz), Throughput (Mbps) and Throughput-to-area (TP/A) ratio (Mbps/LUT)

Compare cost of masking SCREAM against AES

- Compare SCREAM block cipher against AES using equivalent Boolean masking scheme on both ciphers to determine relative masking cost
- AES version uses S-Box with "Tower Fields," i.e., field inversions in subfields of $GF(2^4)$ and $GF(2^2)$ using Boolean masking described in Algorithm 1.

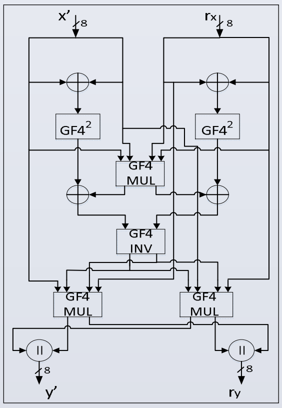

Figure 4 - Masked Inversion of AES in $GF(2^4)$ in Tower Fields implementation of AES. Bus widths are 4 bits unless indicated.

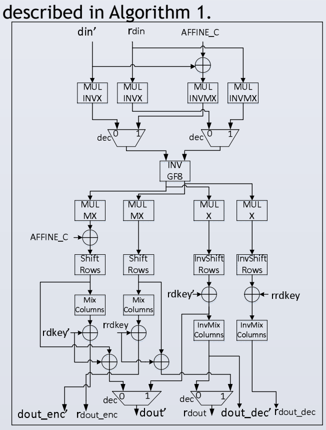

Figure 5 - Masked Combined AES Round in Masked AES, adapted from [Gaj & Chodowiec, 2009]. Bus widths are 128 bits.

Results of Comparison of Masked AES and SCREAM Block Ciphers

- 1st-order Boolean Masking of Block Ciphers only in Virtex-6 FPGA using "wrapper"
- Masked AES TP/A ratio equal (within 2%) to SCREAM TBC with shared S-Box

	LUTs	Slices	Frequency (MHz)	Throughput (Mbps)	Throughput/ Area(Mbps/LUT)
SCREAM Tweakable Block Cipher without shared S-Boxes					
Non-masked	2002	662	111.4	1426	0.712
Masked	4532	1474	87.3	1117	0.246
Ratio	2.26	2.23	0.783	0.783	0.345
SCREAM Tweakable Block Cipher with shared S-Boxes					
Non-masked	1766	570	101.8	1303	0.738
Masked	3533	1094	77.0	986	0.278
Ratio	2.00	1.92	0.756	0.757	0.377
AES					
Non-masked	2312	776	133.6	1710	0.740
Masked	4933	1425	109.4	1400	0.283
Ratio	2.13	1.84	0.819	0.819	0.384

Table 3 - Comparison of non-masked to masked versions of SCREAM Block Cipher and AES in terms of Area (LUTs), Performance (MHz), Throughput (Mbps) and Throughput-to-area (TP/A) ratio (Mbps/LUT)

Conclusion

- SCREAM cipher easily masked using Boolean masking scheme, but costly in terms of area and performance; lowers TP/A ratio by 50% in best case.
- SCREAM block cipher has roughly equal masking cost with equivalently masked AES; TP/A decreases by 62% in masked version compared to non-masked version.
- Introduces method of comparison to determine practical masking cost of CAESAR authenticated cipher candidates versus known standard (i.e., AES) and versus each other; supports Round Three and Final Round of CAESAR competition.