# 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, U.S.A.
e-mail: {wdiehl, kgaj}@gmu.edu

*Abstract*— **Masking is a proven countermeasure to protect physical cryptographic implementations against power analysis side-channel attacks, such as differential power analysis (DPA). Boolean masking is one of several types of masking schemes that can be added to a cipher to increase its security. However, implementing a secure and efficient Boolean masking scheme across all components of a cipher, including non-linear transformations, can be challenging. In this research, a 1st order Boolean masking scheme is applied to the SCREAM authenticated cipher, a CAESAR Round Two candidate. The non-masked and masked versions of the full authenticated cipher are implemented in the Virtex-6 FPGA and compared in terms of throughput, area, and throughput-to-area (T/A) ratio. The SCREAM block cipher is then compared to a masked version of AES to determine the relative costs of masking among the two ciphers. The results show that the T/A ratio of the masked SCREAM full authenticated cipher is only 50% of the T/A ratio of the non-masked version, and that the masking cost of the SCREAM block cipher is roughly equal to that of an equivalently-masked version of the AES block cipher.**

*Keywords*- **Authentication, cryptography, encryption, field programmable gate array, side channel attack, masking, AES**

## I. Introduction and Background

AUTHENTICATED ciphers combine the functions of confidentiality, integrity, and authentication. In July 2015, CAESAR, the Competition for Authenticated Encryption: Security, Applicability, and Robustness, selected 29 authenticated cipher candidates for Round Two of the competition, including SCREAM (Side-Channel Resistant Authenticated Encryption with Masking). [1].

CAESAR candidates are evaluated in terms of security, size, robustness, flexibility, and performance. Although the addition of masking schemes is not required for candidate submissions, the ability to include a masking scheme provides an additional measure of security against side-channel attacks (SCA). SCA, such as power analysis, seek to bypass the cryptographic security of algorithms by exploiting phenomena that are inevitably present in physical implementations of ciphers such as variable power, variable timing, and electromagnetic leakage [2]. Masking is a scheme of performing operations on random bits of a sensitive variable, in such a way that none of the individual bits of the variable can be subsequently analyzed to recover sensitive information, and in such a way that the original data can be reconstructed at the end of the computation in a computationally-efficient manner [3, 4].

Unfortunately, masking schemes which are both secure and efficient are difficult to realize in practice. However, the SCREAM authors claim to introduce certain properties into the construction of their cipher to facilitate the addition of a Boolean masking scheme [5, 6].

In this research, we construct a 1st order Boolean masking scheme for the SCREAM cipher. We then implement the SCREAM full authenticated cipher with and without masking schemes in the Xilinx Virtex-6 FPGA, and compare the implementations in terms of throughput, area, and throughput-to-area (T/A) ratio. Finally, we compare the relative masking cost of the SCREAM Tweakable Block Cipher (TBC) against a comparably-masked version of Advanced Encryption Standard (AES).

The contributions of this research are to provide the first documented masked version of the SCREAM Version 3 full authenticated cipher, and introduce comparisons of masking cost of CAESAR candidates relative to more mature ciphers (such as AES) which could provide an additional method of evaluating the CAESAR candidates for selection to future rounds.

## II. Comparison of non-masked and masked version of the SCREAM full authenticated cipher

### A. *Boolean masking scheme*

Details of the SCREAM cipher are available at [5]. In this research we adapt the scheme described in [7] to apply a 1st order Boolean masking scheme to the SCREAM cipher. The sensitive variables are the 128-bit state variable $x$ and the 128-bit secret key *key*. Each sensitive variable is separated as $a = a' \oplus r_a$, where $a$ is the sensitive variable, $a'$ is the masked variable, and $r_a$ is the mask (i.e., a random 128-bit variable). Once $a$ is separated into $a'$ and $r_a$, it is important that separate calculations be performed on these variables throughout the cryptographic transformation and only recombined when the resulting state is needed for output.

The secret key is separated into *key'* and $r_{key}$ at the beginning of each block so that uncorrelated Boolean additions are performed on the state variable during initial tweak key addition. Likewise, *key'* and $r_{key}$ are computed separately across the final tweak key-to-state variable addition which occurs at the end of each step. The tweak and round constants themselves are not sensitive variables because they are derived neither from the state variable nor secret key, are deterministic (i.e., specified in the SCREAM algorithm), and are assumed to be known by the attacker.

The L-Box is trivially applied to the separated state variable, since the L-Box is a linear transformation on $x$, and $L[a] = L[a' \oplus r_a] = L[a'] \oplus L[r_a]$. Thus, one unaltered L-Box is applied to each variable chain $a'$ and $r_a$ in the masked version.

The difficulty arises in implementing a masking scheme for the S-Box, since the S-Box is a non-linear substitution, and $S[a] = S[a' \oplus r_a] \neq S[a'] \oplus S[r_a]$. This means that the S-Box must be redesigned to maintain linearity across the complete transformation. The SCREAM S-Box consists of three types of expressions: the linear $x = a \oplus b$, and the non-linear $x = a \oplus (b \land c)$ and $x = a \oplus (b \lor c)$. The following algorithm, depicted in Algorithm 1 and adapted from [7], is applied to each equation in the S-Box:

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 $x = a \oplus (b \land c)$ to
      $x' = a' \oplus (b' \land c') \oplus (b' \land r_c)$
      $r_x = r_a \oplus (r_b \land c') \oplus (r_b \land r_c)$
4. Expand expressions of type $x = a \oplus (b \lor c)$ to
      $x' = a' \oplus (b' \land c') \oplus (b' \lor r_c)$
      $r_x = r_a \oplus (r_b \lor c') \oplus (r_b \land r_c)$
```

The modified combined step and round functions are shown in Figure 1.

## B. Additional overhead

One of the primary drawbacks of Boolean masking schemes is increased area and reduced performance. In this implementation, the required growth in the number of logic gates is shown in Table 1. In Table 1, $d^{th}$ order Boolean masking is defined as the separation of a sensitive variable $x$ into $d+1$ shares, on which computations take place independently.

TABLE I
REQUIRED ADDITIONAL GATES USING DTH ORDER BOOLEAN MASKING

| Operation | Required XOR gates | Required AND/OR gates |
|---|---|---|
| $a \oplus b$ | $(d+1) \times$ #(XOR gates) | 0 |
| $a \oplus b \land c$ | $(d+1)^2 \times$ #(XOR gates) | $(d+1)^2 \times$ #(AND gates) |
| $a \oplus b \lor c$ | $(d+1)^2 \times$ #(XOR gates) | $(d+1)^2 \times$ #(OR gates) |

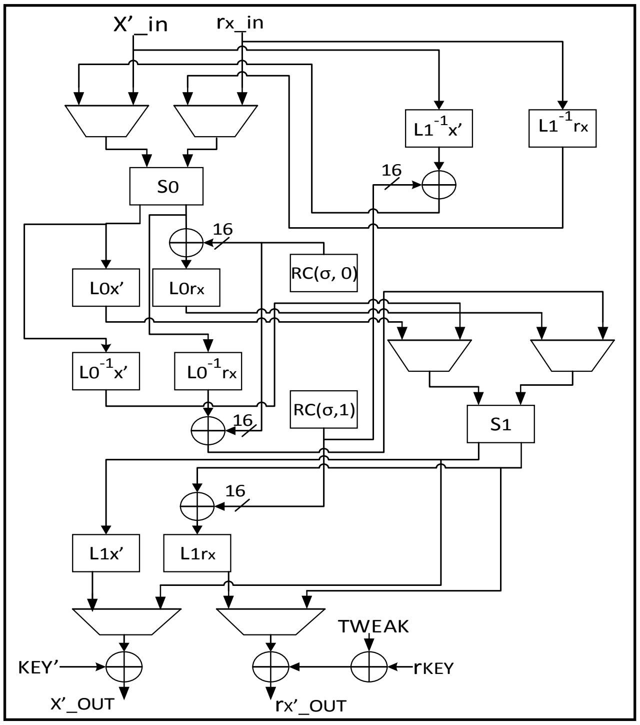

Fig. 1. SCREAM Masked Step with two rounds per step, and shared S-Boxes and round constants. Li is "L-Box i" and Sj is "S-Box j," where i, j ∈ {0, 1}. All bus widths are 128 bits unless indicated.

## C. Hardware design

The non-masked and masked SCREAM full authenticated ciphers are implemented in the Virtex-6 FPGA. Design is accomplished in VHDL using the Xilinx 14.7 WebPack ISE; simulation and functional verification are performed in Xilinx iSim; and synthesis and implementation are performed in Xilinx XST. Both implementations conform to the George Mason University (GMU) Hardware API for Authenticated Ciphers, are computed around AEAD_Core (with wrapper), and are optimized for the best throughput-to-area (T/A) ratio using the balanced strategy of the ATHENa optimization tool [8, 9].

# III. COMPARISON OF NON-MASKED AND MASKED VERSION OF THE SCREAM FULL AUTHENTICATED CIPHER

The results for the hardware implementation in VHDL on the Virtex-6 FPGA are shown in Table 2. In the non-masked versions, the version without shared S-Boxes (i.e., separate S-Boxes and inverse S-Boxes for encryption and decryption, respectively) has the highest T/A ratio, as the reduction in critical path dominates over the increase in size from two non-masked S-Boxes. However, the version with shared S-Boxes (i.e., reuse of "nearly involute" S-Boxes for both encryption and decryption) has the highest T/A ratio of the masked versions, since the addition of masked S-Boxes is especially costly. In the best case, the T/A ratio of the masked version suffers a 50% reduction from that of the non-masked version.

TABLE II
RESULTS OF MASKED AND NON-MASKED SCREAM FULL AUTHENTICATED CIPHER IMPLEMENTED IN VIRTEX-6 FPGA

| | LUTs | Slices | Clock Freq (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 |

## IV. COMPARISON WITH AES

SCREAM was designed using a combinational logic structure which the cipher's authors claim is especially conducive to masking. We have implemented a 1st order Boolean masking scheme in SCREAM, and seen that (in the best case) the masking scheme imposes about a 50% reduction in T/A ratio across the full authenticated cipher. But how does SCREAM compare with more mature ciphers in terms of relative masking cost? In this section, we investigate the relative masking cost of SCREAM in comparison to AES, for which there has been more than a decade of masking research.

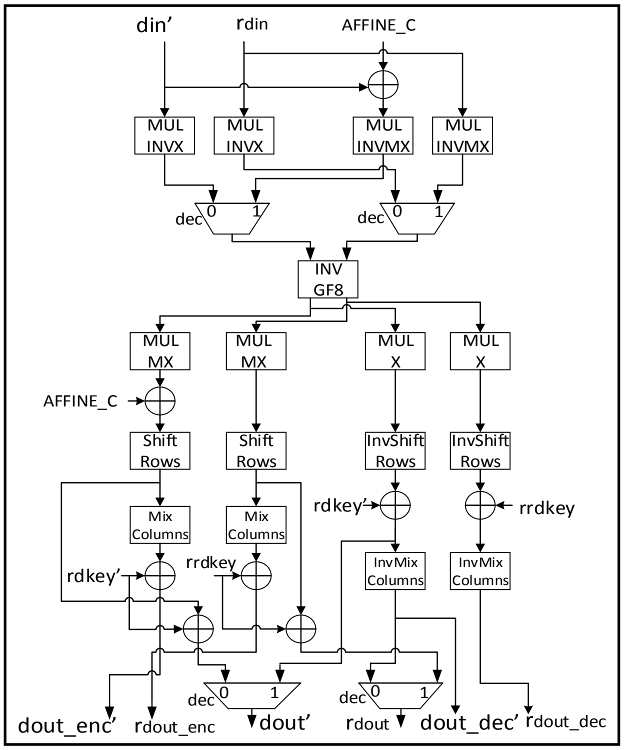

Fig. 2. Masked AES Combined Round, based on [10, 11]

### A. *Construction of masked AES*

We compare the masked version of SCREAM with a masked version of AES, based on the design outlined in [10], which is in turn based on a normal basis representation of the subfields of GF($2^8$) [11]. Boolean masking is then applied to the non-linear components of this inverter in accordance with Algorithm 1. The masked AES combined round is shown in Figure 2. Further background and detail are available at [10, 11].

### B. *Methodology for comparison of SCREAM to AES*

In order to perform as fair and direct a comparison as possible, only block ciphers themselves are compared, not full authenticated ciphers. Both ciphers are capable of encryption and decryption, use 128-bit status words and 128-bit keys, and require ten clock cycles for execution. There are certain irreconcilable differences, however. AES executes in ten rounds, where each round consists of four transformations (SubBytes, ShiftRows, MixColumns, and AddRoundConstant), while SCREAM Tweakable Block Cipher (TBC) executes in ten steps, each of which consist of two rounds of three transformations each (S-Box, Round Constant, and L-Box). SCREAM TBC includes a 128-bit tweak, which must be updated each step, requiring two 128-bit XORs. Finally, AES is required to include hardware to compute its own round keys, which requires one additional forward S-Box equivalent, or a complex set of multiplexers and control signals which will also increase area and increase critical path. Both ciphers are implemented with the same interface; both include organic controllers which provide for the cipher's operation (and nothing else), and both are packaged in a top-level "wrapper" which minimizes the number of I/O ports and allows for full implementation on most FPGAs.

### C. *Results of comparison of SCREAM to AES*

The results of implementation on the Virtex-6 FPGA of the SCREAM Tweakable Block Cipher (TBC) and AES in the top-level wrapper are shown in Table 3. Based on T/A ratio, AES has a statistically equal masking cost with SCREAM TBC. Specifically, the T/A ratio of masked AES is 38.4% of the non-masked version, which is a 61.8% reduction. In comparison, the T/A ratio of lowest-cost masked version of the SCREAM TBC is 37.7% of the non-masked version, which is a 62.3% reduction. Strictly based on area cost, the SCREAM TBC using shared S-Boxes has the lowest growth ratio at 2.00. However, the T/A ratio takes into account that we are forced to pay for the convenience of lower area by additional multiplexers which add critical path and routing delays.

TABLE III

COMPARISON OF RESULTS OF NON-MASKED AND MASKED VERSIONS OF SCREAM AND AES BLOCK CIPHERS IN THE VIRTEX-6 FPGA

| | LUTs | Slices | Clock Freq (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 |

## V. CONCLUSION

Both non-masked and masked versions of the SCREAM Version 3 full authenticated cipher were implemented in the Virtex-6 FPGA. The masked versions use a 1st order Boolean masking scheme capitalizing on the special circumstances of the SCREAM bitslice S-Box, and additional modifications as described above. The masked versions show significant degradation in throughput, area, and throughput-to-area (T/A) ratio compared to the non-masked versions, which conforms to expected theory. The magnitude of the degradation accentuates the need for continued research into efficient masking schemes, or other countermeasures against side-channel attack.

In terms of comparison to a cipher for which more masking research has been conducted, the observed best masking cost of the SCREAM block cipher, in terms of T/A ratio, is roughly equal to an equivalently-masked efficient version of AES.

The above masked implementations separate all computations across both shares of the sensitive variables and are theoretically secure against 1st order DPA, assuming an adequate source of randomness is employed to generate the two shares. While this Boolean masking scheme can be extended to provide protection against High Order Differential Power Analysis (HODPA), the cost in terms of area and performance quickly becomes excessive. Additionally, intelligent synthesis tools and compilers for hardware and high-level language software implementations may introduce optimizations that undo the intended masking schemes. Therefore, no implementation should be considered secure until verified on actual hardware in a laboratory environment.

## VI. RECOMMENDATIONS FOR FUTURE STUDY

Follow-on research should verify the increased resistance to DPA of the masked versions versus the non-masked versions of this cipher in a laboratory environment. Additionally, this research did not consider masked implementations that are secure in the presence of CMOS-circuit glitches, as discussed in [12]. Future masking schemes for SCREAM and other CAESAR candidate authenticated ciphers will be constructed to provide "glitch-free" masking. Finally, the comparison of relative masking cost among CAESAR candidates is an open field of research which can contribute to the fair evaluation and selection of candidates to higher rounds of the competition.

## REFERENCES

[1] "CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness." Internet: http://competitions.cr.yp.to/caesar.html, Jun. 16, 2014 [Jun. 23, 2016].

[2] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *Proceedings of CRYPTO '99 - 19th International Conference on Cryptology*, Aug. 15-19, Santa Barbara, CA., 1999.

[3] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in CRYPTO '99, 1999, pp. 398-412.

[4] M. L. Akkar and C. Giraud. "An Implementation of DES and AES, Secure against some attacks." In *CHES '01: Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, London, U.K., 2001. Springer-Verlag, pp. 309-318.

[5] V. Grosso, G. Leurent, F. Standaert, K. Varici, A. Journault, F. Durvaux, L. Gaspar, S. Kerckhof, "SCREAM, Side-Channel Resistant Authenticated Encryption with Masking," Version 3 (Second Round Specifications), Internet: http://competitions.cr.yp.to/round2/screamv3.pdf Aug. 2015 [Jun. 23, 2016].

[6] V. Grosso, G. Leurent, F.-X. Standaert, and K. Varici, LS-designs: "Bitslice encryption for efficient masked software implementations." *Proceedings, 21st International Workshop on Fast Software Encryption (FSE 2014)*, London, U.K., Mar. 3 – 5, 2014.

[7] J. Daemen, M. Peeters, G. Van Assche, "Bitslice Ciphers and Power Analysis Attacks," In G. Goos, J. Hartmanis, J. van Leeuwen, and B. Schneier (eds.) Fast Software Encryption Vol. 1978, Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2001, pp. 134-149.

[8] E. Homsirikamol, W. Diehl, A. Ferozpuri, F. Farahmand, M. Sharif and K. Gaj, "GMU Hardware API for Authenticated Ciphers," Cryptology ePrint Archive, Report 2015/669

[9] Cryptographic Engineering Research Group (CERG), "Automated Tool for Hardware Evaluation," George Mason University, Fairfax, VA, USA. https://cryptography.gmu.edu/athena/ [Jun. 23, 2016]

[10] K. Gaj, P. Chodowiec, "FPGA and ASIC Implementations of AES," In Ç. K. Koç (ed.) *Cryptographic Engineering*, Springer Science & Business Media, 2009, pp. 235-294.

[11] D. Canright, "A very compact S-box for AES," In J.R. Rao and B. Sunar (eds.), International Workshop on Cryptographic Hardware and Embedded Systems (CHES 05), Proceedings, LNCS, vol. 3659, pp. 441-455, Springer-Verlag, 2005.

[12] S. Mangard, N. Pramstaller, E. Oswald, "Successfully attacking masked AES hardware implementations." In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 157–171. Springer, Heidelberg (2005)