# Attack Tolerant Cryptographic Hardware Design by Combining Error Correction and Uniform Switching Activity

Jimson Mathew[a,*], Saraju P. Mohanty[b], Shibaji Banerjee[a], Dhiraj K. Pradhan[a]

[a]*Department of Computer Science, University of Bristol, UK.*
[b]*Department of Computer Science and Engineering, University of North Texas, Denton, TX 76207, USA.*

**Abstract**

Thwarting severe cryptographic hardware attacks requires new approaches to logic and physical designs. This paper presents a systematic design approach to fault tolerant cryptographic hardware designs by combining the concurrent error detection and correction, and uniform switching activity cells. The effectiveness of the Hamming code based error correction schemes as a fault tolerance method in stream ciphers is investigated. Coding is applied to Linear Feedback Shift Registers (LFSR) based stream cipher implementations. The method was implemented on industrial standard stream ciphers, e.g. A5/1(GSM), E0 (Bluetooth), RC4 (WEP), and W7. The performance of stream cipher algorithms with error detection and correction was studied by synthesising the designs on FPGA and custom Integrated Circuits. The hardware building blocks are investigated to minimise switching activity of a circuit for all possible inputs and their transitions by adding redundant gates and increasing the overall number of signal transitions. The overheads of the proposed approach are also discussed.

*Keywords:* Cryptographic Hardware, Fault Tolerant Cryptography, Side Channel Attack, Uniformly-Switching Circuits, Concurrent Error Detection and Correction

*Corresponding author
*Email addresses:* Jimson.Mathew@bristol.ac.uk (Jimson Mathew), saraju.mohanty@unt.edu (Saraju P. Mohanty), shibaji100@gmail.com (Shibaji Banerjee), pradhan@compsci.bristol.ac.uk (Dhiraj K. Pradhan)

## 1. Introduction

There is a growing demand for tighter security at banks, airports, industrial sites, military installations, large entertainment complexes, and power stations [1]. In these critical applications various forms of security at the software and hardware components is essential to provide maximum level of security [2]. Designing hardware for such systems is particularly challenging because it must withstand tampering, fault attacks, and eavesdropping [2, 3]. It has recently been shown that for many digital signature and identification schemes an attacker can inject faults into the hardware and the resulting incorrect outputs and compromise the security [4]. Hence, as cryptographic hardware becomes increasingly vulnerable to such fault attacks, future cryptographic processors must continue processing computations correctly in the presence of such attacks. The presence of faults in the public parameters of an elliptic curve cryptosystem may expose the secret keys [5].

Electronic cryptographic hardwares process information at significantly higher rates than software implementations; however can inadvertently leak information through side channels. A resourceful attacker may even be able to observe the performance of an electronic device on inputs of their choice, e.g., trying many passwords per second and watching out for an unusual activity pattern on a chip. Physical contact with the chip is not necessary, as demonstrated recently by electromagnetic-emission and acoustic attacks against public-domain implementations of RSA running on common laptops and desktops [6, 7, 8]. Diagnostic equipment used by chip manufacturers for silicon debugging can also be used to undermine cryptographically secure hardware [9]. Thermal imaging with even poor resolution can distinguish inputs that cause unusual patterns and identify large structural components of the chip, such as multipliers, that are indispensable in public-key cryptography. This approach facilitates timing attacks where the attacker may glean useful information, e.g. during a multiply operation. Such attacks have been detailed in a practical setting against the OpenSSL [10, 11]. In the meantime, more sophisticated spectrographic equipment is available and is rapidly becoming inexpensive. Additionally, attackers may compromise hardware systems through social engineering and gain unauthorised physical access to crit-

ical keyboards, monitors, LEDs or wires. Therefore, security analysis often ascribes seemingly unreasonable powers to the attackers, in the hope to err on the side of overestimating attackers rather than underestimating them. Many types of secure hardware, such as wireless base-stations, aerospace communications, and e-cash, must last for over 10 years, and thus designers must account for future technological advances rather than only consider known attacks. This suggests frugal minimization of side-channel information, new mathematical formalisations, and new design algorithms.

The important point is to complicate attacks against cryptographically secure hardware that are based on Fault attacks and Differential Power Analysis (DPA) [12, 13]. In [13], a statistical technique uses measurements of power consumption of a circuit in different circumstances in the hope that energy patterns may correlate with signal patterns. DPA-based methods automatically formulate numerous hypotheses about cryptographic patterns, e.g. digital keys, and correlate them against empirical side-channel information. While typical DPA attacks rely on measuring supply current, statistically significant data about thermal patterns may also weaken cryptographic hardware. Simply increasing the number of sensors, the frequency of readings, or the sensitivity of thermal measurements may automatically decrease expected discovery time for encryption keys.

From the above discussion it is evident that there is a need for research on robust encryption hardware design which this paper addresses. The remainder of the paper is organised as follows. Contributions of this paper is summarized in Section 2. Section 3 presents the preliminaries on stream ciphers and outlines the approach proposed in this paper, along with definitions considered in the rest of the paper. We construct uniformly-switching variants of various building blocks. In Section 4 we investigate error correction in Linear Feedback Shift registers. Section 5 outlines various experimental results, and contrasts our approach with the others. Section 6 presents the conclusions.

## 2. Contributions of this Paper

The proposed novel design approach for physical attack tolerant cryptography hardware follows a two-tier paradigm: (1) A new Hamming code based concurrent error

detection and correction over Galois Field is explored to mitigate fault attacks in cryptographic hardware. (2) A new uniform-switching activity logic-level library is created using which the cryptography architecture components are realized. The overall concept is depicted in Fig. 1. In light of this, firstly, this paper proposes a fault tolerant design of Linear Feedback Shift Registers (LFSR) and Galois-Field Linear Feedback Shift Register (GLFSR). We consider multiple error detection, in standard stream cipher implementation by sub dividing long blocks in small blocks and applying multiple hamming codes. The overhead for the proposed error correction technique is also analysed. We also study uniformly-switching versions of common logic blocks, such as adders and comparators, and cryptographic hardware-specific blocks such as Galois field multipliers. Given the overhead of uniformly-switching logic, we do not expect that complete secure systems will be entirely based on such circuits. For example, some cryptographic algorithms use published look-up tables that do not compromise secure information. Such look-up tables do not necessarily need to be protected from information leakage. The proposed design approach is validated in three different forms: Field-Programmable Gate Array (FPGA), logic-level synthesis, and SPICE simulations.

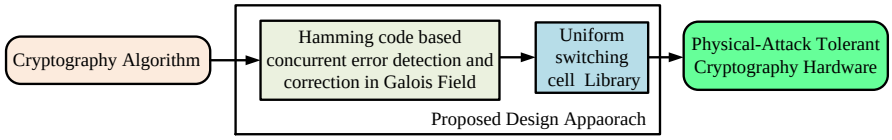



Figure 1: The Proposed Novel Two-Tier Approach for Robust Cryptography Hardware.

## 3. The Concept of Uniform Switching Activity in Galois LFSR

Linear Feedback Shift Registers (LFSR) are used in key-stream and Built-in Self Test (BIST) generators due to their simple hardware structures. They can produce sequences of large period, with good statistical properties. An LFSR of length $n$ consists of $n$ elements capable of storing one bit each. The Galois Linear Feedback Shift Register (GLFSR) is a solution for improving randomness of the pattern generators. Besides generating random numbers, the GLFSR has fault tolerant properties [14]. The GLFSR

is a generalised LFSR, which is defined over Galois Field GF($2^{\partial}$), $\partial > 1$. The GLFSR has three components: adders, multiplier, and memory elements. A general representation of GLFSR is shown in Fig. 2. The feedback polynomial of an $n$-stage GLFSR can be represented as follows:

$$\Phi(y) \; = \; y^n \; + \; \Phi_{n-1} y^{n-1} \; + \; \cdots \; + \; \Phi_1 y \; + \; \Phi_0 \tag{1}$$

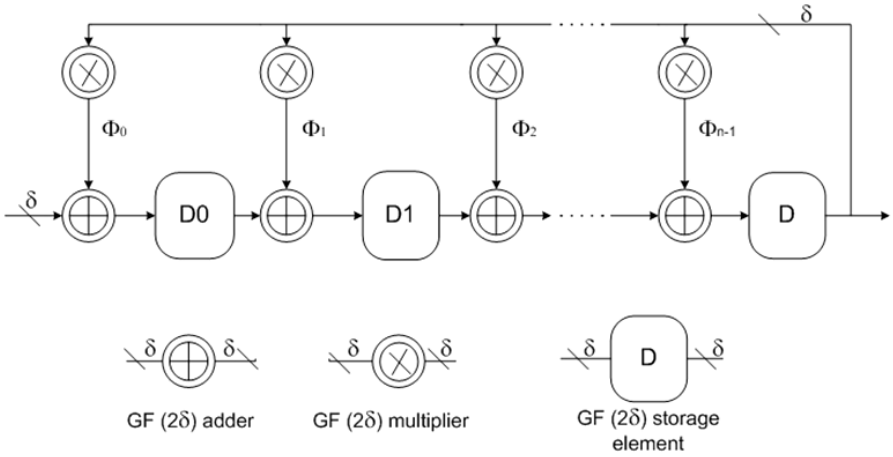



Figure 2: Galois Linear Feedback Shift Register.

There are several stream cipher algorithms presented in the existing literature [15]. In a binary additive stream cipher, the cipher text is produced by bit-wise addition of the plain text with a key-stream; all in binary. The key-stream generator is initialised using a secret key. The most common key-stream generator is a combination of several GLFSRs or LFSRs which are combined together through a non-linear Boolean function. In this paper, we consider four standard stream ciphers and implement two versions (fault tolerant and non-fault tolerant) for comparing their performances. The A5/1, E0, RC4, and W7 are well-known stream ciphers, and they have been specified in popular standards and protocols. The A5/1 is a stream cipher used for encrypting over the air transmissions in the GSM standard [16]. A GSM conversation is transmitted as a sequence of 228-bit frames (114 bits in each direction) every 4.6 milliseconds. Each frame is XORed with a 228-bit sequence produced by the A5/1 key-stream generator. The initial state of this generator depends on a 64-bit secret key, $K_c$, which is fixed dur-

ing the call duration, and on a 22-bit frame number. The encryption of packet payloads in Bluetooth is performed by the E0 stream cipher. The W7 algorithm is a symmetric key stream-cipher that supports key lengths of 128 bits. The W7 cipher contains eight similar models, C1, C2, ..., C8. Each model consists of three LFSRs and one majority function. The RC4 is a variable key-size stream cipher for the RSA Data Security. The RC4 stream cipher has two phases: the key set-up, and the key-stream generation. Both phases must be performed for every new key. During an $n$-bit key set-up the encryption key is used to generate an encrypting variable using two arrays (the state and the key array) and $n$-number of mixing operations [17].

Attacks against cryptographically secure hardware that are based on Differential Power Analysis has been addressed in [18]. This presents a statistical technique that uses measurements of power consumption of a circuit in different circumstances in the hope that energy patterns may correlate with signal patterns. DPA-based methods automatically formulate numerous hypotheses about cryptographic patterns, e.g., digital keys, and correlate them against empirical side-channel information. While typical DPA attacks rely on measuring supply current, statistically significant data about thermal patterns may also weaken cryptographic hardware. Simply increasing the number of sensors, the frequency of readings, or the sensitivity of thermal measurements may automatically decrease expected discovery time for encryption keys. In this paper, we use the following definitions to design equally switching logic which are adopted from [18]:

**Definition 1.** *A logic-gate or a Boolean function* $f(x_1, x_2, ..., x_n) = (y_1, y_2, ..., y_k)$ *with* $n$ *inputs and* $k$ *outputs "switches uniformly" iff there is a constant* $0 < M_f \leq k$ *with the following property: For any input combination* $(x_1, x_2, ..., x_n)$*, changing the value of any single bit in it leads to the changing of exactly* $M_f$ *output bits.*

**Definition 2.** *A circuit is called "weak uniformly-switching" if for each input wire* $x_i$ *there exists a constant* $d_i$ *such that for any one-bit input transition on* $x_i$*, the circuit experiences* $d_i$ *logic-gate switches. The vector* $(d_1, d_2, ..., d_n)$ *is called the characteristic vector of the weak uniformly-switching circuit.*

**Definition 3.** *A circuit is called "strong uniformly-switching" with a fixed parameter $C$ if for any one-bit input transition it experiences $C$ gate switches.*

One of the counter measures to mitigate DPA is to equalize power dissipation based on the effective principles. In [18] authors did not preform any power analysis. In this paper we have designed various gate libraries and during synthesis we could use this library for designing uniformly switching logic. When selecting gate libraries, we will require that every gate has the same number of switching outputs for every possible single-output transition. Therefore, when a multiple-input transition is decomposed into a shortest sequence of single-bit transitions, the overall result (in terms of power) does not depend on the specific sequence chosen.

## 4. Proposed Approach for Error Correctable and Uniform Switching-Activity LFSR

In this section, we present the proposed design of the error correctable and uniform switching-activity LFSR. This LFSR when used in encryption chip instead of traditional LFSR provided side-channel attack resilient hardware.

### *4.1. Proposed Error Detecting and Correcting LFSR*

The basic principle is explained using a 4 bit example. The basic structure of a 4 bit block is shown in Fig. 3. The classical LFSR based on a typical primitive polynomial is first designed. In this approach the check bits for each cycle for error detection and correction is first computed based on the Hamming's principles. The Hamming codes are the simplest of a group of codes known as the linear block codes [19]. We divide large chunk of sequential elements into a number of small blocks and encode each of them separately. Next, we present the algorithm for designing the proposed scheme with an example.

Let $\overrightarrow{d} = [d_0, d_1, d_2, \ldots, d_{n-1}]$ be the input of the sequential elements in an LFSR and $\overrightarrow{q} = [q_0, q_1, q_2, \ldots, q_{n-1}]$ the output. Also let $r$ be the number of parity bits, and $\overrightarrow{p} = [p_0, p_1, \ldots, p_{r-1}]^T$ and $\overrightarrow{pc} = [pc_0, pc_1, \ldots, p_{r-1}]$, respectively be the predicted and the parity bits generated from the output bits. Let $\mathbf{H}$ be the parity check matrix associated with the proposed single error correction scheme.

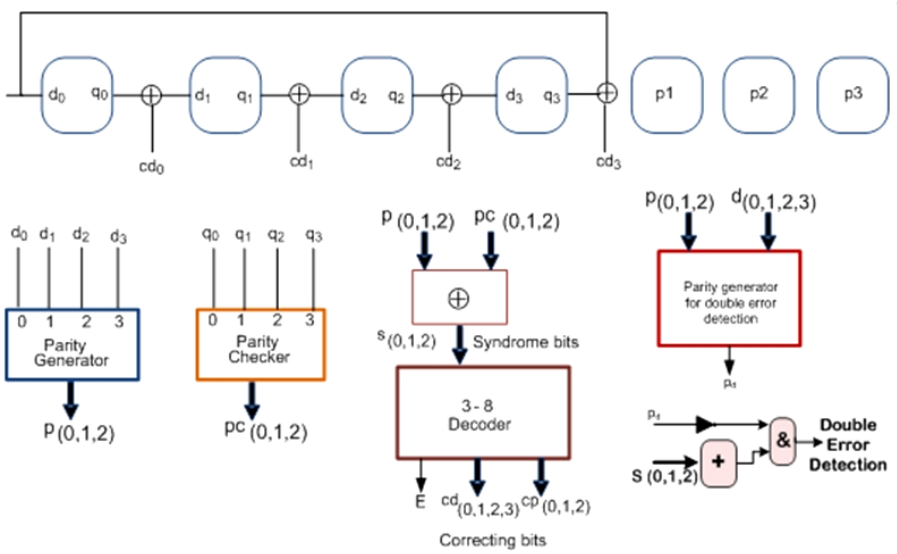



Figure 3: Error correction in a 4-bit block.

*The Steps for the Proposed Design Procedure* are the following:

(1) Determine the number of block checkers ($ms$) required to satisfy the equation $m = \lfloor n/k \rfloor$, where $k$ is number of error corrections.

(2) Determine the number of parity bits ($r$) required to satisfy the equation $m+r+1 \leq 2^r$.

(3) Construct the $\mathbf{H}$ matrix, with $(m + r)$ non-zero $r$-bit column vectors. The dimension of the resulting matrix is $r \times (m + r)$.

(4) A column vector with a single 1 is assigned to parity $P_i$.

(5) The column vector with all 1s is assigned to output bit $c_{m-1}$.

(6) The remaining $m$ columns are assigned the output bits $c_i$, without any constraints.

(7) Generate the parity expressions in terms of $d_i$s.

(8) For Double Error Detection (DED) per block, choose the parity check matrix such that the output bits are assigned to the columns with odd number of ones. In this case additional parity bits maybe required.

(9) Finally, combine the block register, check bit register, output encoder, decoder, and the correction logic as shown in 3.

The following example illustrates the above proposed design procedure.

**Example 1.** *Consider a four bit LFSR structure over constructed in Fig. 3. Here we have $m = 4$. Therefore, we need 3 parity bits to correct single errors. We have the following parity-check matrix:*

$$\mathbf{H} = \begin{array}{ccccccc} p_0 & p_1 & p_2 & d_0 & d_1 & d_2 & d_3 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array} . \tag{2}$$

*Therefore, the parity check equations are the following:*

$$p_0 = d_0 + d_1 + d_3; \tag{3}$$

$$p_1 = d_0 + d_2 + d_3; \tag{4}$$

$$p_2 = d_1 + d_2 + d_3. \tag{5}$$

The *error correction procedure* involves three steps: (1) compute the output parities, (2) compute syndrome by comparing with stored parity bits, and (3) decode the syndrome and apply corrections. We analyse the various error scenarios on the proposed architecture and their effects. First, a malicious attack and/or error on one of the registers is considered. Consider Fig. 3 with the first register bit in error. Here, we refer to Example 1 with the single error correcting **H** matrix. Let the input of the LFSR be $d = (d_0, d_1, d_2, d_3) = (1, 0, 0, 0)$ . The check bits stored are $p = (p_0, p_1, p_2) = (110)$. Let us assume that , an error in the first bit causes an erroneous output $q = (q_0, q_1, q_2, q_3) = (0, 0, 0, 0)$. At the output the output parity bits $pc = (pc_0, pc_1, pc_2) = (0, 0, 0)$. Comparing the output parity bits with the stored parity bits gives the syndrome $(1, 1, 0)$ and the bit corresponding to this syndrome is $d_0$ (see the **H** matrix). Therefore, the first bit gets automatically corrected as shown. In Fig. 3 $(cd_0,\ cd_1,\ cd_2,\ and\ cd_3$ are the correcting signals. In this example $(cd_0$ set high by the decoding logic to correct $d_0$. Second, a malicious attack/error on the parity check bit is considered. In this case an attack/error on the parity would not cause an error in the functional output and the syndrome generated will be one of the following: $\{(0, 0, 1), (0, 1, 0), (1, 0, 0)\}$. Since these syndromes are not decoded, no correction is applied. With a similar argument, any error in the functional registers that causes single

bit error in the output can be corrected by the above technique, whereas for the errors in the parity circuit that causes single error in the predicted parities are not corrected. Therefore, by introducing the parity check bits will not compromise reliability.

The hardware and performance analysis of the proposed technique is now discussed to study its usefulness. For this purpose, the original algorithm of the four stream ciphers A5/1, E0, W7, and RC4 were implemented in VHDL. The designs were simulated in Modelsim to verify the functionality. Further, the hardware variation with the usage of different optimal register blocks for parity generation is investigated. For example, Fig. 4 shows the possible different groupings for an 128-bit LFSR. The degrees of the LFSRs in each cipher were varied from 64 to 128. The GLFSRs were considered as registers and divided into groups of optimal register sets. The parity bits required in each case and the errors corrected were compared with the area consumed. The comparison with various combination of parity check bits is shown in Fig. 5.

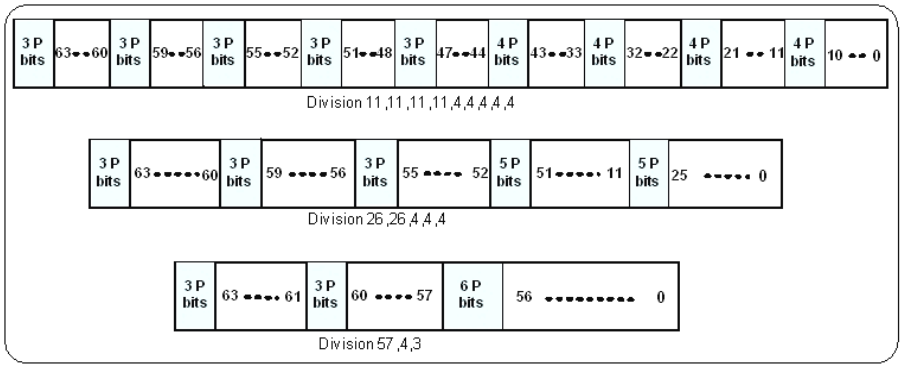
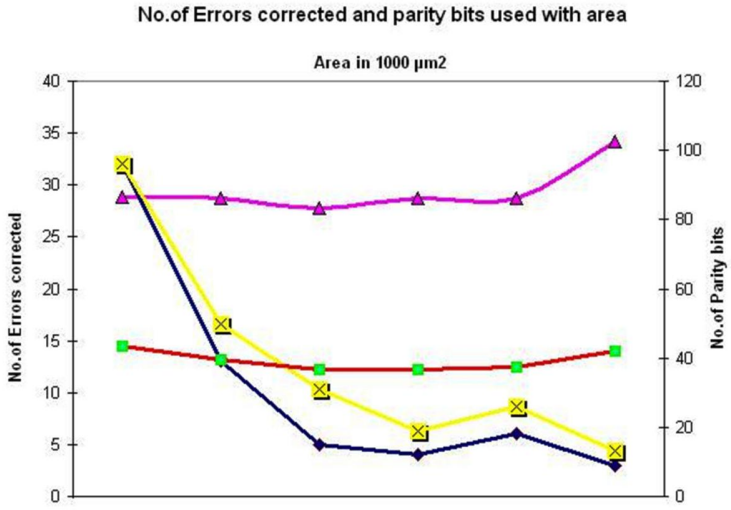



Figure 4: Register grouping for multiple Hamming codes.

### *4.2. Approach for Uniformly-Switching Gates and Circuits of the LFSR*

For synthesis of uniformly-switching circuits we propose to use a complete gate library consisting of uniformly-switching gates [18]. The idea is depicted in Fig. 6. One-input one-output buffer and inverter gates are uniformly-switching, but we also need more powerful gates. Adding two-input one-output uniformly-switching gates is not sufficient either. Such a gate library only allows to compute all Boolean functions that are with respect to the bitwise XOR operation. In general, any negation




| | | | | | | |
|---|---|---|---|---|---|---|
| Area for single error correction | 28.798528 | 28.779008 | 27.724252 | 28.666058 | 28.701584 | 34.22063 |
| No. of Errors corrected | 32 | 13 | 5 | 4 | 6 | 3 |
| No. of Parity bits used | 96 | 50 | 31 | 19 | 26 | 13 |
| Area for double error detection | 43.352576 | 39.517114 | 36.84309 | 36.807532 | 37.41722 | 41.881488 |

Figure 5: Comparison of multiple error correction.

and/or permutation of the outputs of a uniformly-switching function produces another uniformly-switching function.

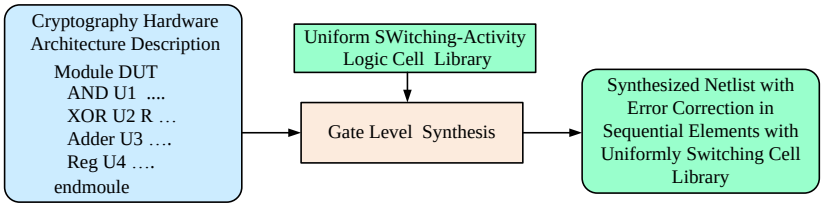



Figure 6: Uniform Switching Activity Circuit based Cryptography Module Realization.

The technique most related to ours includes the Sense-Amplifier Based Logic (SABL) family [20] and the Wave Dynamic Differential Logic (WDDL) [21]. A major advantage of WDDL is that it can be handled by a traditional EDA tool flow. Our approach goes further in the sense that we show how to reuse existing tools for synthesis and layout. However, we pursue a different task: equalising energy dissipation, and not total power consumption. Indeed, in CMOS power is consumed mostly during the 0-1 tran-

sitions, but both the 0-1 and 1-0 transitions dissipate energy. We observe that empirical results in [21] require careful interpretation. For example, the path delay overhead does not account for the use of every second cycle in the WDDL circuits for "pre-charging waves", which halves data rate for the same cycle time.

## 5. Experimental Results

### *5.1. Area, Timing and Power Analysis*

The two versions (classical and weak uniformly-switching) of typical combinational logic blocks have been designed and coded in VHDL. The test circuits were divided into two groups: (1) AND/OR functions and basic arithmetic circuits, and (2) AND-XOR intensive, such as Galois multiplier circuits. This was done to validate our basic constructs and demonstrate that our technique extends to larger circuits. For comparison, the doubling construction version of the Galois multiplier circuits were also designed. The arithmetic circuits designed over the Galois fields are crucial to the implementation of certain cryptographic algorithms, such as the elliptic curve cryptography. The designs were simulated using ModelSim$^{TM}$ and were tested for functionality by giving various inputs. The designs were synthesized using the Synopsys tools in the UMC technology library, using the 0.18$\mu$m CMOS technology. The Synopsys Power Compiler$^{TM}$ was used to estimate the power consumptions. The area, delay, and power estimates for the basic circuits are shown in Table 2. The overhead varies depending on the type of circuit and logic elements used. For instance, AND/OR dominated circuits are expensive, requiring up to 144% extra area to make them weak uniformly-switching. As mentioned earlier, since the proposed design is for cryptographic applications, we have also analysed various Galois field circuits. For Galois multipliers, which are widely used in cryptographic processor designs, there is approximately 90% area and power overhead to make them weak uniformly-switching. The area, delay, and power analysis for the various Galois field multiplier designed with the various approaches (original, weak uniformly switching, and using the doubling construction) are shown in Figs. 7, 8, and 9 respectively. First the designs were made weak uniformly switching and then the doubling construction was applied. The actual values are normalised with respect to the original design. The overhead is on an average about

300% after doubling construction. There is a slight delay overhead in transition from the original design to the doubled variant due to the extra XOR gates used in the doubling construction, whereas there is no delay difference between the original and weak uniformly switching versions. Since the analysis presented here is based on standard-cell CMOS layouts, we have focused mostly on validating the key concepts proposed and estimating the power, area, and delay overhead. However, further optimizations are possible at the transistor and silicon level.

Table 1: Synthesis results of various designs

| Prim Design | ASIC ($area\ in\ um^2$) | | FPGA (LUTs) | |
|---|---|---|---|---|
| | Original | with EC | Original | with EC |
| A5/1 | 33420.3 | 46558.2 | 365 | 445 |
| E0 | 70315.0 | 111354.3 | 607 | 936 |
| RC4 | 244687.1 | 401162.1 | 3627 | 5803 |
| W7 | 36924.5 | 59505.5 | 373 | 622 |

Table 2: Uniformly-switching variants of various circuits.

| $circuit$ | $area$ $(um^2)$ | $delay$ $(ns)$ | $power(uw)$ $(uw)$ | $area$ $(um^2)$ | $delay$ $(ns)$ | $power$ $(uw)$ |
|---|---|---|---|---|---|---|
| Full adder | 90.1 | 0.43 | 13.5 | 197.1 | 0.43 | 29.4 |
| Mux-2-1 | 51.6 | 0.28 | 5.6 | 139.90 | 0.28 | 24.4 |
| Decoder-2-4 | 64.5 | 0.16 | 9.1 | 116.9 | 0.16 | 16.8 |
| Multiplier (2bit) | 132.6 | 0.45 | 13.6 | 222.6 | 0.45 | 31.76 |
| 4bit adder/ subtractor | 787.04 | 1.34 | 140 | 1593 | 1.34 | 226.3 |

### *5.2. SPICE Simulation Results*

Both the proposed architecture and the classical designs have been implemented in CMOS transistor level using the HSPICE tool in the 0.18$\mu$m technology. The simulated power trace and its histogram of a GF(64) multiplier circuit for traditional CMOS is shown in Fig. 10. The designs have been simulated with a 20 ns clock period for all the 4096 input transitions. The weakly switched variant design version simulation results are shown in Fig. 11. It may be noted that the proposed design has more uniform power consumption irrespective of the switching activity. We also considered 10% process variation in the design parameters. The process variation study conducted relies on

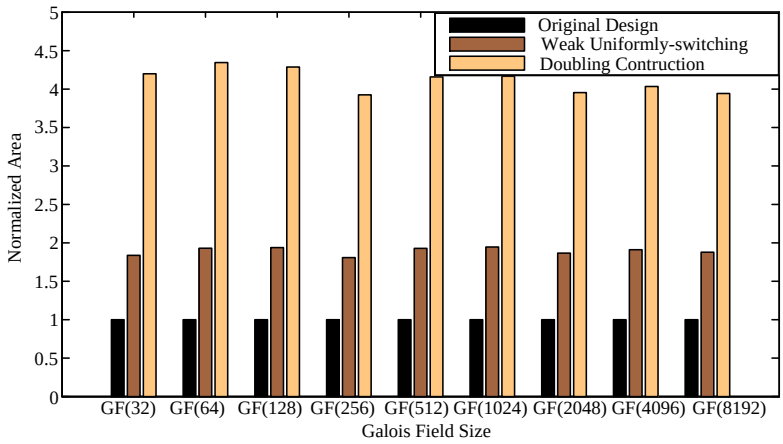



Figure 7: Area analysis of various Galois field multipliers and their uniformly-switching variants.

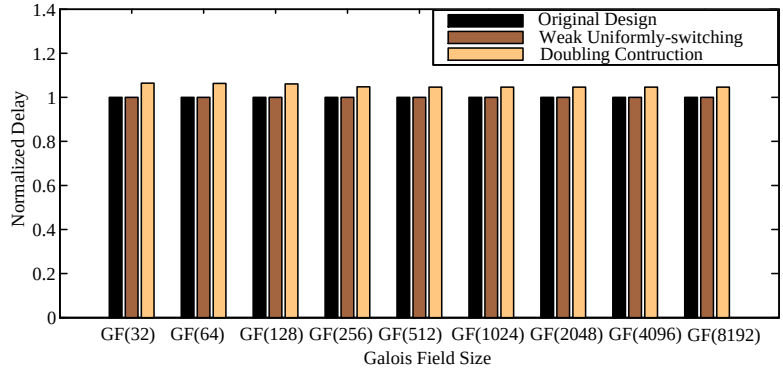



Figure 8: Delay analysis of various Galois field multipliers and their uniformly-switching variants.

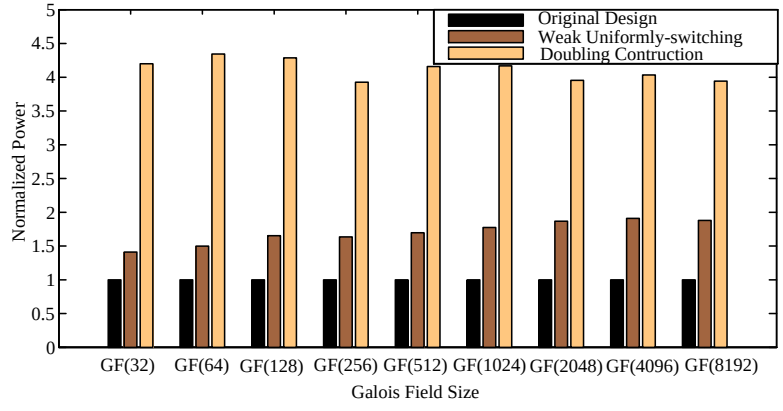



Figure 9: Power analysis of various Galois field multipliers and their uniformly-switching variants.

the well known Monte Carlo method that could be done in a reasonable amount of time. The power consumptions for 100 Monte Carlo simulations is shown in Fig. 12. We noticed more or less random changes in the power consumptions as we varied the process parameters.

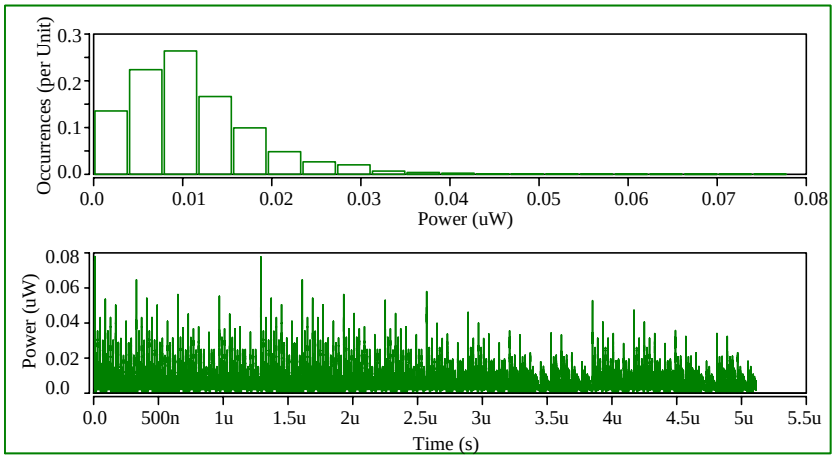



Figure 10: Histogram and simulated power trace of classical designs.

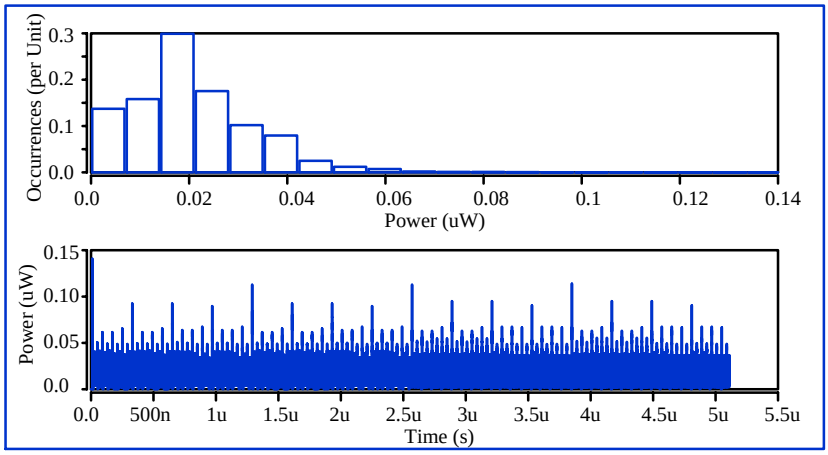



Figure 11: Histogram and simulated power trace of weakly uniformly-switched variants.

### *5.3. Comparative Discussions*

Our techniques affect data rate due to the gate sizing, and, as experiments in Section 5.1 show, the overhead is marginal. Area and delay overhead may strongly depend

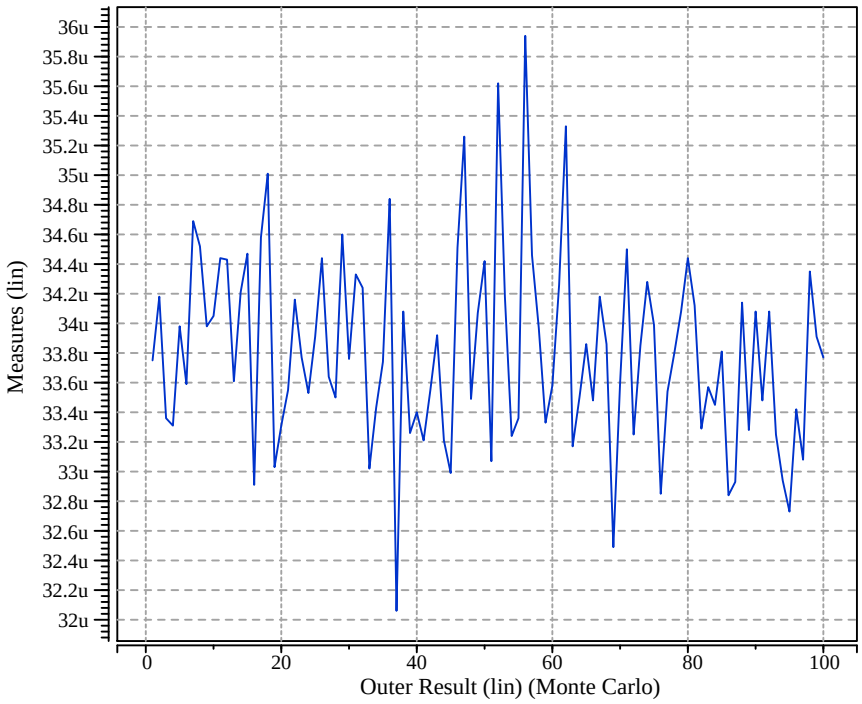



Figure 12: Power consumptions under 10 percent process variation.

on the logic functions. Indeed, the WDDL logic requires re-expressing each Boolean function using AND/OR/NOT gates, while the uniformly-switching logic extends existing circuits. The former results in a large overhead when many XOR operations are required, e.g. in the Kasumi algorithm [21]. Our techniques adapt existing circuits and do not impose significant restrictions on the gates used. They incur the smallest overhead on circuits consisting entirely of the XOR, XNOR, and NOT gates. In particular [22] reported a 3 times ($\approx \frac{2.45}{0.79}$) area increase for the implementation of AES, while using our construction the area increase is at most 2 times (in the worst case, using the doubling construction on top of the AES implementation which is linear). In addition, in our algorithm the data rate is not slowed down by the design to such extend as it is for WDDL.

Since in WDDL all the inputs are pre-charged to zero, the use of AND/OR gates instead of NAND/NOR seems unavoidable, implying additional 50% area overhead in

CMOS (however, a convenient LUT-based implementation is proposed in [21]). This and the pairing of AND/OR gates in WDDL implies a lower bound of $3\times$ on the area overhead, which agrees with the empirical data in [21] and sharpens the lower bound of $2\times$ as presented in [21]. The use of WDDL seems to require complete re-synthesis, whereas we adapt existing circuits and preserve the structure of critical paths.

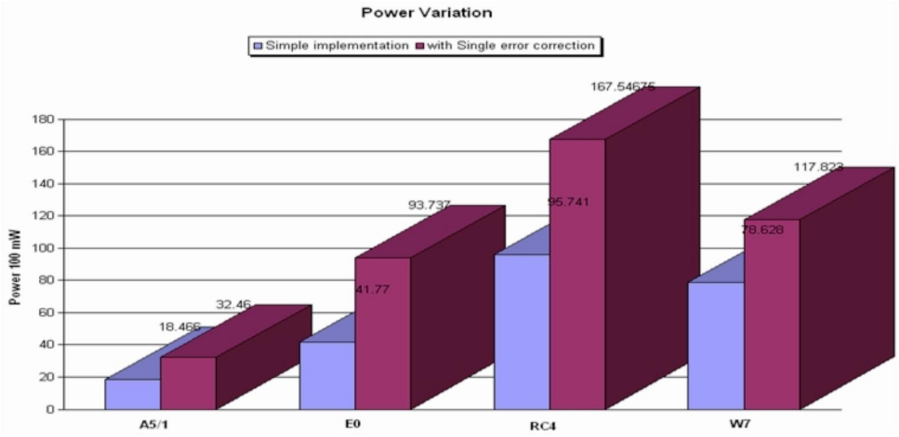



Figure 13: Power Consumption: original vs. fault tolerant

## 6. Conclusions

In this paper we proposed a systematic design approach for fault tolerant cryptography hardware. Firstly, we analysed the effectiveness of Hamming code based fault tolerance in stream ciphers. The method was implemented on industrial standard stream ciphers, e.g. A5/1(GSM), E0 (Bluetooth), RC4 (WEP), and W7. The performance variation of stream cipher algorithms with error detection and correction was studied by synthesising the designs on FPGAs and ASICs. Further, we explored the uniformly-switching logic for cryptographic applications to mitigate side-channel attacks based on dissipated energy. The cumulative area overhead is less than two times the area occupied without the redundancies. It is still affordable when DPA-resistance is a bottleneck but circuit size is not. The uniformly-switching logic incur particularly small overhead for deeply pipelined circuits and many arithmetic circuits. Further reducing the area and delay overhead of uniformly-switching logic is a major direction for future

research. Additionally, ASICs may be bottlenecks for some low-power applications. Developing low-power cryptography along with attack resilience and fault-tolerance is another research direction.

**Acknowledgments**

This current archival journal paper is based on our conference publication [23]. Authors would like to acknowledge the editors and unknown reviewers for their constructive feedbacks.

**References**

[1] S. Gorman, Electricity Grid in U.S. Penetrated By Spies, Wall Street Journal, Accesed on 29th July 2012, http://online.wsj.com/article/SB123914805204099085.html (April 8 2009).

[2] S. P. Mohanty, A Secure Digital Camera Architecture For Integrated Real-Time Digital Rights Management, Journal of Systems Architecture - Embedded Systems Design 55 (10-12) (2009) 468–480.

[3] E. Kougianos, S. P. Mohanty, R. N. Mahapatra, Hardware Assisted Watermarking For Multimedia, Computers & Electrical Engineering 35 (2) (2009) 339–358.

[4] D. Boneh, R. A. DeMillo, R. J. Lipton, On the Importance of Eliminating Errors in Cryptographic Computations, Journal of Cryptology 14 (2) (2001) 101–119.

[5] M. Ciet, M. Joye, Elliptic Curve Cryptosystems in the Presence of Permanent and Transient Faults, Designs, Codes and Cryptography 36 (1) (2005) 33–43.

[6] S. Ravi, A. Raghunathan, P. Kocher, S. Hattangady, Security in Embedded Systems: Design Challenges, ACM Transactions on Embedded Computing Systems 3 (3) (2004) 461–491.

[7] A. S. and E. Tromer, Acoustic Cryptanalysis, http://cs.tau.ac.il/~tromer/acoustic/, Accessed on 22 June 2012 (2004).

[8] W. Knight, Computer Chip Noise May Betray Code, New Scientist, http://www.newscientist.com/news/news.jsp?id=ns99994979, Accessed on 22 June 2012 (May 2004).

[9] J. Markoff, Intel Technicians Use Delicate Silicon Surgery to Fine-Tune Microchips, New York Times, accessed on 22 June 2012 (08/09/2004).

[10] D. Brumley, D. Boneh, Remote Timing Attacks Are Practical, Computer Networks 48 (5) (2005) 701–716.

[11] P. C. Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, in: Proceedings of the 16th Annual International Cryptology Conference, 1996, pp. 104–113.

[12] L. Benini, E. Omerbegovic, A. Macii, M. Poncino, E. Macii, F. Pro, Energy-Aware Design Techniques For Differential Power Analysis Protection, in: Proceedings of the Design Automation Conference, 2003, pp. 36–41.

[13] P. C. Kocher, J. Jaffe, B. Jun, Differential Power Analysis, in: Proceedings of the 19th Annual International Cryptology Conference, 1999, pp. 388–397.

[14] M. Chatterjee, D. Pradhan, A BIST Pattern Generator Design For Near-Perfect Fault Coverage, IEEE Transactions on Computers 52 (12) (2003) 1543–1558.

[15] H. C. A. van Tilborg, S. Jajodia (Eds.), Encyclopedia of Cryptography and Security, 2nd Ed, Springer, 2011.

[16] Digital Cellular Telecommunications System (Phase 2+); Security Aspects, Tech. rep., European Telecommunications Standards Institute (ETSI), http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_11_Mainz/Docs/PDF/S3-000142.pdf, Accessed on 22 June 2012 (2000).

[17] M. D. Galanis, P. Kitsos, G. Kostopoulos, N. Sklavos, C. E. Goutis, Comparison of the Hardware Implementation of Stream Ciphers, International Arab Journal of Information Technology 2 (4) (2005) 267–274.

[18] I. L. Markov, D. Maslov, Uniformly-Switching Logic for Cryptographic Hardware, in: Proceedings of the Design, Automation and Test in Europe Conference and Exposition, 2005, pp. 432–433.

[19] R. W. Hamming, Error Detecting And Error Correcting Codes, Bell System Technical Journal 29 (2) (1950) 147–160.

[20] K. Tiri, M. Akmal, I. Verbauwhede, A Dynamic and Differential CMOS Logic With Signal Independent Power Consumption to Withstand Differential Power Analysis On Smart Cards, in: Proceedings of the 28th European Solid-State Circuits Conference, 2002, pp. 403–406.

[21] K. Tiri, I. Verbauwhede, A logic level design methodology for a secure dpa resistant asic or fpga implementation, in: Proceedings of the Design, Automation and Test in Europe Conference and Exhibition, 2004, pp. 246–251.

[22] K. Tiri, D. Hwang, A. Hodjat, B. Lai, S. Yang, P. Schaumont, I. Verbauwhede, A Side-Channel Leakage Free Coprocessor IC in 0.18 $\mu$m CMOS For Embedded AES-based Cryptographic and Biometric Processing, in: Proceedings of the 42nd Design Automation Conference, 2005, pp. 222–227.

[23] J. Mathew, S. Banerjee, H. Rahaman, D. K. Pradhan, S. P. Mohanty, A. M. Jabir, On the Synthesis of Attack Tolerant Cryptographic Hardware, in: Proceedings of the International Conference on Very Large Scale Integration of System-on-Chip, 2010, pp. 286–291.