Extracting side-channel leakage from round unrolled implementations of lightweight ciphers

Nikhil Chawla, Arvind Singh, Nael Mizanur Rahman,
Monodeep Kar and Saibal Mukhopadhyay

March 1, 2019

Extracting Side-Channel Leakage from Round Unrolled Implementations of Lightweight Ciphers

[1]Nikhil Chawla, [1]Arvind Singh, [1]Nael Mizanur Rahman, [2]Monodeep Kar, [1]Saibal Mukhopadhyay
[1]*Georgia Institute of Technology, Atlanta, GA*
[2]*Intel Corporation, Hillsboro, OR*
{nchawla6, asingh367, naelmr}@gatech.edu, monodeep.kar@intel.com, saibal.mukhopadhyay@ece.gatech.edu

***Abstract*— Energy efficiency and security is a critical requirement for computing at edge nodes. Unrolled architectures for lightweight cryptographic algorithms have been shown to be energy-efficient, providing higher performance while meeting resource constraints. Hardware implementations of unrolled datapaths have also been shown to be resistant to side channel analysis (SCA) attacks due to a reduction in signal-to-noise ratio (SNR) and an increased complexity in the leakage model. This paper demonstrates optimal leakage models and an improved CFA attack which makes it feasible to extract first-order side-channel leakages from combinational logic in the initial rounds of unrolled datapaths. Several leakage models, targeting initial rounds, are explored and 1-bit hamming weight (HW) based leakage model is shown to be an optimal choice. Additionally, multi-band narrow bandpass filtering techniques in conjunction with correlation frequency analysis (CFA) is demonstrated to improve SNR by up to 4×, attributed to the removal of the misalignment effect in combinational logics and signal isolation. The improved CFA attack is performed on side channel signatures acquired for 7-round unrolled SIMON datapaths, implemented on Sakura-G (XILINX spartan 6, 45nm) based FPGA platform and a 24× reduction in minimum-traces-to-disclose (MTD) for revealing 80% of the key bits is demonstrated with respect to conventional time domain correlation power analysis (CPA). Finally, the proposed method is successfully applied to a fully-unrolled datapath for PRINCE and a parallel round-based datapath for Advanced Encryption Standard (AES) algorithm to demonstrate its general applicability.**

Keywords— AES, correlation frequency analysis, energy efficiency, PRINCE, round unrolling, side channel analysis, SIMON, narrow bandpass filtering, leakage models, FPGA, SNR

I. Introduction

Recent shift in the paradigm from mainframe and personal computing to computing at edge nodes has led to an exponential growth in interconnected internet-of-things (IoTs) and internet-of-everything (IoE) devices. In a typical IoT environment, IoT devices sense, process and communicate information to a mobile device or to enterprise/servers over a wireless network. To ensure integrity, confidentiality and security of sensitive information against malicious adversaries, communication is usually encrypted with implementations in software/hardware at the edge node. Due to severe resource constraints for IoT devices, the encryption hardware must be compact, consume small energy/power and be able to meet system performance/throughput requirements. This gave rise to lightweight cryptography with several compact block ciphers, such as Midori [1], PRINCE [2], SIMON and SPECK [3], proposed over the last few years. Although these algorithms are proven secure against cryptanalysis attacks, their hardware implementations tend to leak information in several physical side channels, e.g., timing, power, electromagnetic (EM) emanations, acoustic signatures etc. Differential Power Analysis (DPA) [4] or Correlation Power Analysis (CPA) [5] of these side channel signatures can reveal the secret encryption key used during the encryption process.

To reduce/eliminate leakage through side channels, several hiding and masking-based countermeasures have been proposed [6-9]. Round unrolling was proposed as a simple countermeasure against power-based side channel attacks (PSCA) for data encryption standard (DES) [10], SIMON [11, 12] and PRINCE [13] and are applicable to other lightweight ciphers as well. Although a generic countermeasure, it is highly applicable for lightweight ciphers due to their less complex round functions and large number of rounds. Traditionally, both software and hardware implementations of cryptographic algorithms are pipelined, with intermediate states stored in sequential registers after computation. Since registered values match with the algorithmic values, hypothetical leakage models can be easily derived based on registered intermediate states. However, when cryptographic rounds are fully/partially unrolled, these registered intermediate states can no longer be targeted due to deeper diffusion of the keys through the datapath and key expansion, requiring an adversary to target intermediate states computed at the intermediate nodes of the combinational logic. Extraction of side channel leakage from a combinational logic is difficult due to the reasons described below:

- Inability to find deterministic states to compute a good leakage model as intermediate states computed at the intermediate nodes of a combinational logic do not necessarily match the targeted algorithmic states.
- High glitch activity (a function of logic depth and therefore degree of unrolling) leading to poor SNR.
- Misalignment (in time) of measured power traces as the intermediate states are computed at different instants based on the signal arrival times (a function of logic structure and the input vectors).

Introducing misalignment into the power traces has often been used as a countermeasure to SCA. Data dependent and Random Delay Insertion (RDI) countermeasures have been shown to reduce information leakage by desynchronizing power traces, thereby reducing correlation between current consumption and the computed intermediate state [14, 15]. The misalignment introduced with RDI based countermeasures affect the temporal shift of time-domain signals due to a composition of legitimate and dummy executions. However, they have been shown to be successfully mitigated using alignment techniques both in time and frequency domain [16]. On the other hand, the misalignment inherent in unrolled datapaths is dependent on logic structure organization and is input vector dependent, which results in different delay distributions of targeted bits in a combinational logic as shown in [14]. Success of single and multi-bit CPA attacks in time-domain is dependent on these delay distributions. Therefore, unless an adversary has complete and accurate knowledge of the combinational logic structure, it is very difficult to derive a good leakage model based on targeted algorithmic states. When the deterministic part of the leakage differs from the leakage model used by the adversary, leakage models based on linear regression have been shown to provide a better attack efficiency [17]. However, for SIMON, due to an absence of non-linear functions, 1-bit intermediate states can be targeted with a reduced key complexity without the need for linear regression. Similarly, single-bit leakage models perform much better for highly noisy measurements as demonstrated in [17] with respect to DPA. In this work, we show that single-bit leakage models with reduced complexity is an optimal choice for round unrolled SIMON with respect to the CPA-based distinguisher. However, for PRINCE and AES which have non-linear substitution functions, 1-bit leakage models have the same key complexity as the multi-bit leakage models, and are therefore not an optimal choice[18].

Correlation frequency analysis (CFA) has been previously shown to improve CPA attack efficiency in the presence of RDI or randomized clock-based countermeasures [16, 19]. Due to the presence of noise in the measured signatures, frequency components of leakage signals (expected to have a small amplitude) are isolated from frequency components of noise (expected to have a large amplitude) with bandpass filters in time-domain to eliminate adverse effects of spectral leakage [20]. We show that filtering the measured signatures in time-domain using multiple narrow bandpass filters, each isolating a specific frequency band, followed by windowed FFT, improves the effectiveness of CFA attacks for unrolled datapaths by removing the data dependent misalignment of power samples and improving SNR. The key contributions of this work are described below:

- We demonstrate that single-bit HW-based leakage models on round unrolled datapaths of 128-bit SIMON outperform multi-bit leakage models with respect to CPA.
- We present an improved CFA attack with multi-band narrow bandpass filtering employed in the time-domain followed by windowed FFT to isolate the signal and improve SNR for increased attack efficiency in the frequency domain.
- The proposed leakage models and CFA attack is applied to 7 and 10-round unrolled implementations of SIMON-128 and fully-unrolled implementations of PRINCE-64. All key bits are successfully recovered with a small number of measurements demonstrating that ***unrolled datapaths have very high exploitable leakage***.
- Additionally, the same CFA attack is applied to round-reuse-based 128-bit parallel implementation of AES-128 with HW-based models and leakage from the combinational SBOX output is successfully extracted, demonstrating ***general applicability of the proposed CFA attack to extract side channel leakage from any combinational logic***.

The rest of the paper is organized as follows: Section II reviews encryption algorithms employed in this work and related literature; section III presents the experimental setup and side channel analysis methodology; section IV presents SNR and CFA attack results for SIMON-128, section V applies the same methodology and demonstrates successful CFA attacks for fully-unrolled PRINCE-64 and AES-128; and section VI concludes the paper.

II. BACKGROUND

A. SIMON, PRINCE and AES Algorithms

1) Lightweight Ciphers - SIMON and PRINCE: SIMON and SPECK were two ciphers proposed by NSA, which can be optimized for hardware and software implementations. SIMON is a block cipher with a fiestal network with different configurations, each with a different level of mathematical security provided [3]. Encryption and decryption operations are based on a round function. A typical round function for SIMON-128 with a block size of 64-bits is depicted in Fig. 1(a). It consists of 1-AND gate and 3-XOR gates. Encryption in the ith round can be expressed using the Eq. 1:

$$L_{i+1}, R_{i+1} = LS^1(L_i)\ \&\ LS^8(L_i) \oplus LS^2(L_i) \oplus R_i \oplus K_i\ , L_i \quad (1)$$

PRINCE was proposed at ASIACRYPT 2012 by Borghoff et. al. [2] as a lightweight block cipher optimized for low latency operation. It possesses reflectivity features where encryption and decryption can be performed using the same hardware resources. A 64-bit plaintext and 128-bit key is used for encryption. The overall architecture of the cipher is shown in

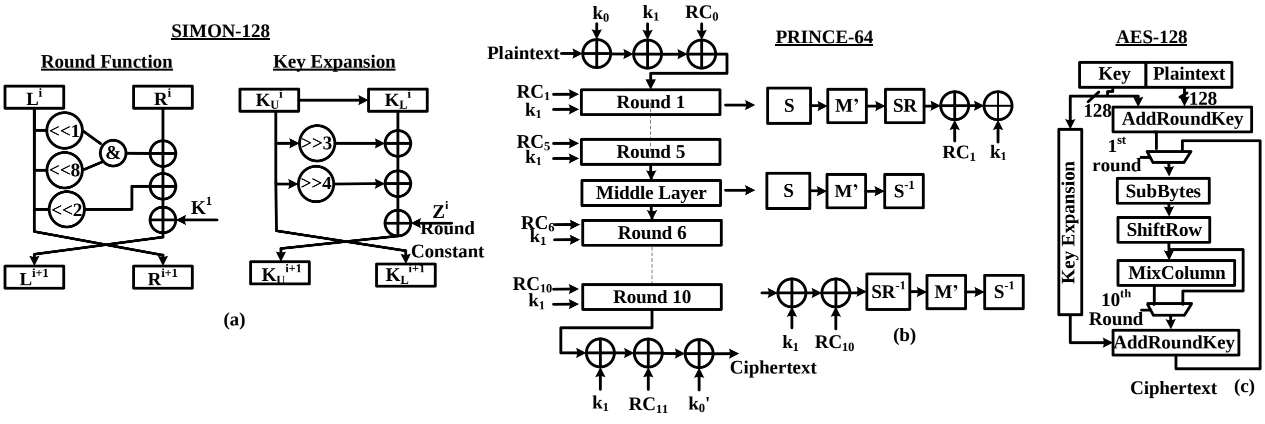

Fig.1 (a) SIMON-128 Round Function and Key Expansion (b) PRINCE-64 datapath (c) AES-128b datapath

Fig. 1 (b). The entire key is split into 2 parts, k_0 and k_1 (64 bits each):

$$k = k_0 \,||\, k_1 \tag{2}$$

k_0' is derived from *k_0* by a transformation as shown below:

$$(k0 \,||k1) \rightarrow (k0 \,||k0' \,||k1) \\ \rightarrow (k0 \,||\, (k0 \ggg 1) \oplus (k0 \gg 63)||\, k1) \tag{3}$$

k_0 and *k_0'* are used as pre-whitening and post-whitening keys respectively. Encryption is completed in 10 fully unrolled rounds. The first 5 rounds perform SBOX, linear operation (M'), and ShiftRow operations. The last 5 rounds perform inverse SBOX, linear and inverse ShiftRow operations. Each round has a unique round constant except the middle layer which has only SBOX, inverse SBOX and linear operations.

2) Advanced Encryption Standard (AES) Algorithm: AES is a National Institute of Standards and Technology (NIST) approved cryptographic algorithm and is the most widely used encryption scheme in modern devices. AES has a block size of 128 bits and a key size of 128, 192 and 256 bits. It consists of 10 rounds of operations and an initial round. Each round consists of 4 operations : 1) SubstituteByte or SBOX, 2) ShiftRow, 3) MixColumn and 4) AddRoundKey. Initial round performs just an AddRoundKey operation and the last round skips the MixColumn operation [Fig. 1(c)].

B. Related Work

Lightweight ciphers are designed for specific applications but may sometimes fail to meet all target requirements due to inherent trade-offs in security, flexibility, side-channel and fault-attack resistance. Serial and parallel datapath implementations of SIMON on FPGA have been shown to be susceptible to CPA attacks [21, 22]. Round unrolling was first proposed as a simple architectural countermeasure on hardware implementations of Data Encryption Standard (DES) algorithm [10] where a fully-unrolled implementation was shown to be resistant to CPA and Mutual Information Analysis (MIA) attacks. More recently, A. Singh et. al. have shown that unrolled implementations of 128-bit SIMON (to 6th degree) improves power side-channel attack resistance. Their CPA attack targeted round 3 output (combinational) with a 1b hamming weight (HW) leakage model but failed to show an attack even with 500K traces, showing inability to extract leakage in time-domain [23]. Author in [12] demonstrated a general Degenerate Grouping Power Attack (DGPA) on different configurations of SIMON and SPECK and showed a successful attack with up to 4th degree of unrolling (r=4). However, they showed that with sufficient degree of unrolling (r>=9), DGPA attack is computationally infeasible to carry out even with state-of-the-art computational resources.

Since its introduction, a significant amount of work has been done on the side channel leakage characteristics of PRINCE. CPA attacks have shown a successful recovery of the correct key in a round-based implementation of PRINCE on a SASEBO-G FPGA where the same hardware was re-used iteratively in a loop to compute each round of the encryption operation [24]. A similar analysis was shown for a DPA attack as well. Both these works were based on the hamming distance (HD) leakage model targeting the first-round output of the encryption block. A fully unrolled architecture of PRINCE has also been analyzed by [13] where a point-of-interest (POI) selection using a Welch's t-test was performed on the measured power traces prior to HD (with respect to back-to-back plaintext) based CPA analysis. The results showed an improved number of key nibbles recovered with up to 250K traces.

The success of CPA attacks improves with pre-processing of acquired power traces, especially filtering. Filters such as matched filters [25], comb filters [26], band pass frequency-domain filtering (near-clock frequency) have shown improved SNR of power traces. In [27], the impact of linear FIR filters with optimized filter coefficients on time and frequency domain CPA is demonstrated. I. Levi et. al. have demonstrated the impact of filters of different widths on a pseudo-asynchronous design style (a countermeasure that reduces information leakage by using data dependencies to generate dynamic clock sampling) [28].

III. PROPOSED LEAKAGE MODELS AND IMPRVOED CFA METHODLOGY

This section describes leakage models, improved CFA methodology and experimental setup to measure side channel activity to validate the hypotheses.

A. Proposed Leakage Models

The success of any side channel attack not only depends on the chosen distinguisher (CPA, DPA, mutual information analysis – MIA, etc), but also on the leakage model. For unrolled datapaths with deeper key diffusion, leakage from sequential registers cannot be targeted, thus requiring modeling of intermediate states within the combinational logic, which is not deterministic. The success of attacks, thus, depends on how well the modeled intermediate variable (modeled leakage) matches the true intermediate variable (true leakage). Single-/multi-bit intermediate variables can be targeted to create single-/multi-bit leakage models based on the corresponding key dependencies of the target. For encryption algorithms with a non-linear substitution operation, the key dependency generally remains unchanged, irrespective of the number of target bits chosen. For example, the key dependencies at any SBOX output for PRINCE and AES is the same regardless of the number of bits chosen for the target intermediate variable. It has been demonstrated that for such cases, all bits in the intermediate variable that correspond to the respective key-dependencies need to be chosen for better attack efficiency. In contrast, SIMON does not contain non-linear functions, which leads to a reduced key complexity (2-bit key dependency for 1-bit of the output at round 2). Additionally, when there is a mismatch between modeled leakage and true leakage, multi-bit HW/HD leakage models can be improved with linear regression (linear combination of weighted bits). In such a case, single-bit leakage model (DPA) is also demonstrated to perform better than multi-bit (but not as good as linear regression) [17].

Considering the reduced key-dependency, CPA (equivalent to normalized DPA) with 1-bit leakage models in SIMON are expected to provide better results without the need for linear regression (only 1-bit targeted; different weights don't affect

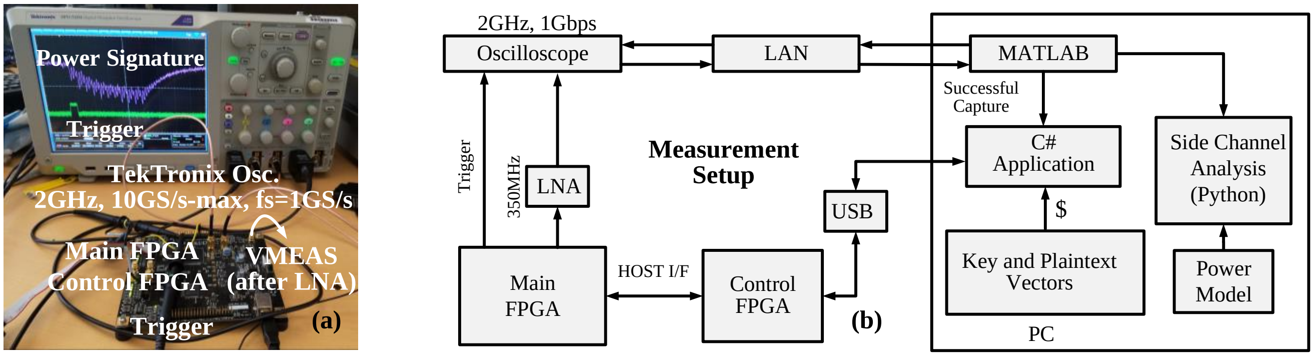

Fig. 2. (a) Sakura-G side channel characterization platform (b) Measurement setup details (c) Post Processing of raw captured traces to remove out-of-band noise for different frequency bands from 5M-105MHz in the interval of 5MHz.

the output of CPA). HW based models are preferred, compared to HD, because the previous state in a combinational node is unknown due to high glitching activities and large number of transitions prior to reaching the final state.

B. *Improved CFA attack*

CFA attacks are usually employed to break time domain misalignment-based countermeasures (random delay insertion, clock randomization, globally asynchronous locally synchronous – GALS designs etc). In the case of unrolled datapaths, the arrival times of signals at different nodes of combinational logic is input-vector-dependent as opposed to registered sequential circuits. Large noise and high glitch activity reduce the efficiency of CFA attacks on combinational logic. In this regard, we attempt to improve CFA by employing multiple time-domain narrow bandpass (5 MHz) filters. In contrast to conventional techniques, we filter the entire power trace (5MHz to 105MHz) into 5MHz bands to isolate signal from noise in the time domain, eliminate the effect of spectral leakage (side lobes of noise frequency leaking into nearby signal frequency with small amplitude), while also improving SNR. Then, windowing in frequency domain of each of these 5MHz bands further enhances leakage extraction. This overall methodology improves the attack, minimizing MTD and recovers all bytes.

C. *Experimental Setup for Validation*

The unrolled architectures for SIMON-128, PRINCE-64 and round-based parallel datapath architecture for AES-128 were synthesized and mapped on Sakura-G FPGA platform [Fig.2 (a)]. Randomly generated plaintext vectors and a fixed secret key are loaded from C# application running on PC to the control FPGA through USB interface. Target design is mapped onto the main FPGA (spartan-6, 45nm technology) which performs encryption. An on-board LNA (350MHz bandwidth, 10× gain) amplifies the power signatures which are measured during the encryption. An internal trigger signal, generated by the main FPGA, triggers Tektronix DSO5204 oscilloscope (2GHz BW, 10Gbps sampling rate, sampled at 1Gbps) to read samples from the scope using a MATLAB script [Fig. 2(b)].

Traces were captured with a channel bandwidth of 250MHz. The frequency of operation for all the designs was 24MHz. All the acquired signatures were filtered using a wide band pass filter (15-35MHz) and several narrow bandpass filters (5MHz band, ranging from 5MHz to 105MHz) [Fig. 3]. Fig. 4(a) plots the raw measured power signatures for 7-round unrolled SIMON-128, fully-unrolled PRINCE-64 and parallel AES-128. FFT of the measured power shows a high peak at the design clock frequency (24MHz) and its harmonics [Fig. 4(b)]. Several low frequency peaks are also observed. Fig. 4(c) plots the filtered (with a 15-35MHz bandpass filter) waveforms for the measured power signatures.

Metrics used to characterize and compare leakage models and the proposed improved CFA attack are described below:

1) Signal to Noise Ratio (SNR): Signal to noise ratio of captured traces is represented using the leakage model

$$L(x) = \varepsilon \times |\phi(x)| + L_0 + N(0, \sigma^2) \qquad (4)$$

where ε is the leakage conveyed by one-bit toggle and is the signal, $\phi(x)$ is the leakage model related to the plaintext and the key, L_0 is average circuit power due to activity of other parts of the design, $N(0,\ \sigma 2)$ is an additive white Gaussian noise (AWGN). Signal (ε) can be modeled as covariance between power traces and leakage model [29], which is given by:

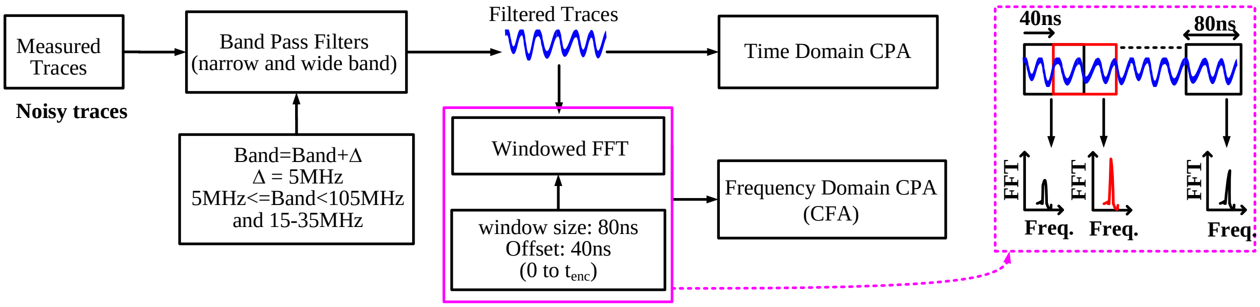

Fig. 3. CPA attack methodology performed on power traces for multiple bands in 5MHz interval followed by windowed FFT. Best attack shows minimum traces to disclosure (MTD) with smallest value and corresponding band as highest leaking band.

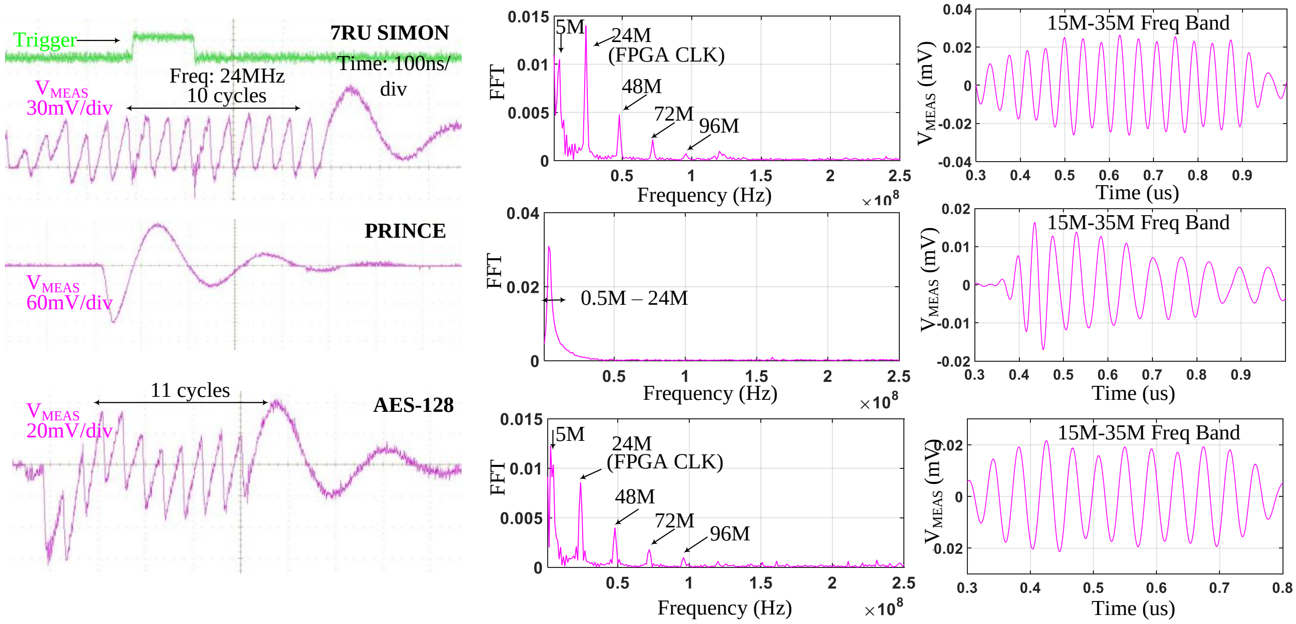

Fig. 4. (a) Captured raw power trace for duration of 1us (b) FFT of Power Trace sampled at Fs=1GS/s, (c) Band pass filtered waveforms with corner frequencies of Fp1=15MHz, Fp2=35MHz, Fs=1GHz, for 7RU SIMON, PRINCE, AES

$$\varepsilon = \frac{cov(L,M)}{4n} \qquad (5)$$

where *M* is leakage model and *n* is the number of bits in the intermediate variable. The SNR with this leakage model is then given as:

$$SNR = \frac{\varepsilon}{\sigma} \qquad (6)$$

2) Success Rate (SR) for CPA/CFA: All 64 bits of the lower key for SIMON-128 were analyzed with respect to CPA/CFA attack. The attack efficiency for the time/freq. domain attacks with different leakage models was compared with respect to number of bits recovered with increasing number of measurements, namely success rate (SR) [17]. Additionally, minimum-traces-to-disclose (MTD) is also used to show a successful attack for the chosen bits.

$$success\ rate\ (SR) = \frac{\#\ of\ recovered\ bits}{\#\ of\ all\ bits} \qquad (7)$$

IV. Extracting Leakage from Unrolled SIMON-128

This section explores different leakage models targeting the initial few rounds, presents SNR and applies the improved CFA attack on 7- and 10-round unrolled datapaths for SIMON-128 to extract side channel information leakages.

A. Comparison of Leakage Models with respect to SNR

For CPA/CFA attacks, an adversary must model leakage generated due to switching of intermediate nodes. Switching activity and therefore power consumption is generally modeled with hamming weight (HW) or hamming distance (HD) based models. Although, HD models dynamic power consumption more closely, it requires the knowledge of underlying hardware implementations to observe state transitions. On the other hand, HW can be generated based only on the algorithmic understanding of block cipher operation, which benefits an adversary without knowledge of the underlying hardware architecture.

To understand the impact of leakage models, several HW-based leakage models are evaluated including the 1b HW leakage model described in the previous section for 7-round unrolled SIMON. We have evaluated 1-bit (1b), 2-bit (2b), 3-bit (3b) and 4-bit (4b) HW leakage models at round 2 output, and 1-bit (1b) HW model at round 3 output. Increasing bit-width further or targeting round 4 output significantly increases

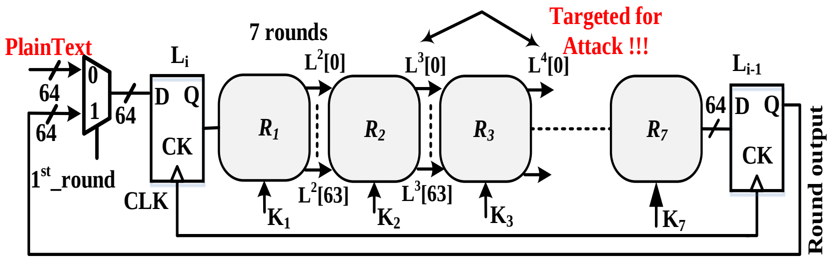

Fig 5. A 7-round unrolled SIMON architecture with attack location at the output of round 2 and round 3. [Note: Round 2 output is not stored but it is at output state at logic gate node]

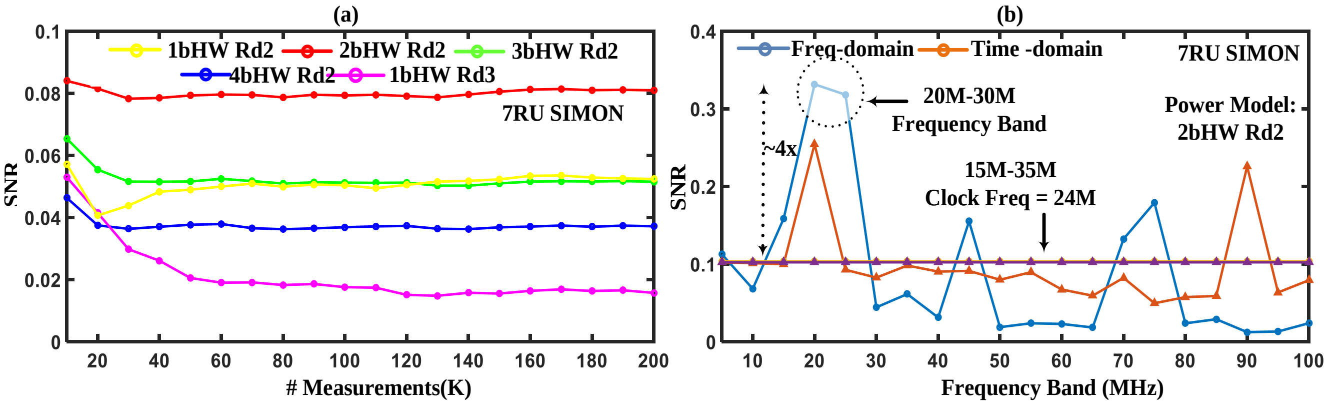

Fig. 6. (a) Signal to Noise Ratio (SNR) vs number of measurements for different HW based power models (b) SNR in different frequency bands for 2b-HW model compared to SNR in 15MHz to 35MHz band.

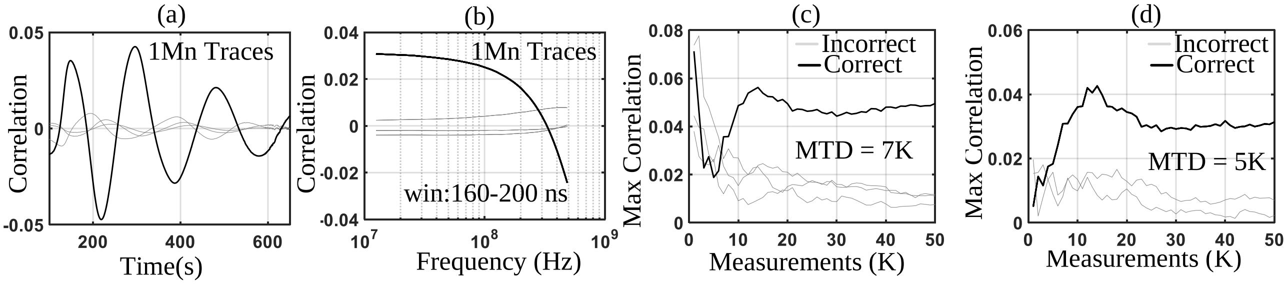

Fig. 7. A successful (a) CPA attack and (b) CFA attack is shown on 7 rounds unrolled (RU) SIMON architecture targeting round 2 output (Rd2) with 1bHW power model. Maximum correlation vs. Number of Measurements in (c) Time-domain with MTD of 7K and (d) frequency domain with MTD of 5K.

the key dependencies and complexity of the leakage model. SNR is computed for each leakage model against number of measurements and is shown in Fig. 6(a). Signal strength is evaluated using correlation between the actual power trace and the leakage model for the correct key guess. Noise is modeled as a gaussian random variable. SNR also depends on the number of bits used to compute HW. A reduction in SNR is observed as bit-width is increased in HW-based leakage models. Also, SNR degrades for 1b HW leakage model at round 3 output. This is attributed to an increase in depth of the combinational logic leading to a higher glitch activity. We see that 2b HW leakage model gives the highest SNR.

SNR is also evaluated in multiple filter bands for the 1b HW leakage model as shown in Fig. 6(b). It is observed that narrow band pass filtering in frequency domain improves SNR by atleast 4× compared to wide-band (15MHz to 35MHz) around the clock frequency. It also shows that frequency domain analysis improves SNR over time-domain in most bands. Moreover, leakage is present not only in the clock band region, but in its harmonics as well as some low-frequency bands.

B. *Successful Key Recovery with Proposed Leakage Models and Improved CFA attack*

1) 7-round Unrolled SIMON-128: A. Singh et. al. have shown 6-round unrolled SIMON-128 implementation being resistant to power-side channel attacks with no key recovery possible even with 500K traces [23]. The authors have targeted flop output and shown the infeasibility of modeling power due to increased key dependencies. However, 6-round unrolled SIMON can be easily attacked with respect to known-ciphertext attacks as the last clock cycle only performs 2 rounds of operation (SIMON-128 has 68 rounds and each cycle in a 6-round unrolled datapath executes 6 rounds with the last cycle executing only 2 rounds). Therefore, we attack a 7-round unrolled SIMON to demonstrate leakage extraction in combinational circuits of unrolled datapaths, as it is advantageous over 6-round unrolled datapath presented in [23] with respect to both known plaintext and ciphertext attacks.

We have performed CPA and CFA using several HW based leakage models, considering different number of bits at round 2 and round 3 output. For 1-bit HW leakage model, 1 bit of the intermediate state at the output of round 2 (R2) is considered to generate key dependencies and the leakage model. We have evaluated all possible 1-bit leakage models for revelation of all 64 bits of the lower key. Altogether, 64 leakage models were generated which could recover 64 bits of the lower key. Each leakage model had a 2-bit key dependency (total of 4 key guesses). Fig. 5 shows the attack location, which is the output of round 2 and round 3. Key dependencies for the highest leaking bit are described in the equations below.

$$L^3[60] = (L^2[59] \,\&\, L^2[52]) \oplus L^2[58] \oplus R^2[60] \oplus K^2[60]$$
$$L^2[59] = (L^1[58] \,\&\, L^1[51]) \oplus L^1[57] \oplus R^1[59] \oplus \mathbf{K^1[59]}$$
$$L^2[52] = (L^1[51] \,\&\, L^1[44]) \oplus L^1[50] \oplus R^1[52] \oplus \mathbf{K^1[52]}$$
$$L^3[60] = \text{fn}\,(\mathbf{K^1[59], K^1[52]})$$
$$\text{HW}\,\{L^3[60]\} \tag{8}$$

The plots for time-domain CPA and freq. domain CFA are shown in Fig. 7 (a, b) where the correct key guess shows a distinct peak compared to other key guesses. MTD plot against the number of measurements is shown in Fig. 7(c, d). We observe a revelation of keys, $K^1[59]$ and $K^1[52]$. 7K and 5K is

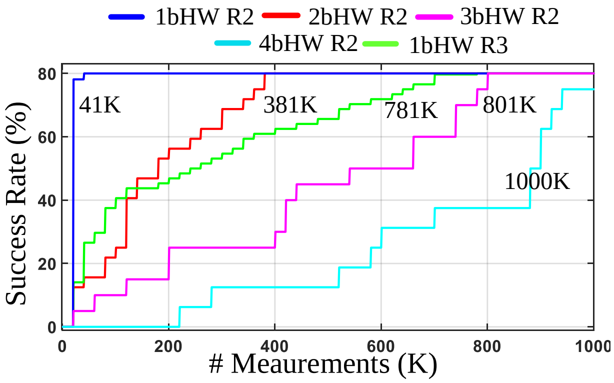

Fig. 8 Success Rate (%) vs Number of Measurements for comparison of different HW power models at the output of round 2 and round 3

the MTD in both time and frequency domain for the highest leaking band (5-10MHz). These results show 1-bit leakage models to be optimal in revealing the correct key.

To demonstrate the effectiveness of the proposed improved CFA attack, we have evaluated the SR against number of measurements targeting all 64-bits of the lower key, using up to 1 million measurements. Fig. 8 summarizes the SR with different leakage models against number of measurements. MTD for 80% SR is used as a metric to compare different leakage models and post-processing methods. 1bHW R2 based leakage model reveals 80% bits with only 41K measurements while 2bHW R2, 3bHW R2 based leakage models at round 2 output require 381K and 801K measurements respectively. 1bHW based leakage model at round 3 output reveals 80% bits with 781K traces. 4bHW leakage model at round 2 output could not recover 80% bits with 1 million measurements. Therefore, 1bHW leakage model at round 2 output is the optimal choice for leakage models. However, when we look at SNR results, 2bHW leakage model at round 2 output shows the highest SNR but a slightly poorer MTD for 80% SR. This could be attributed to the modeling of intermediate states. In unrolled datapaths, the states that are computed at intermediate nodes of the combinational logic is difficult to predict (with only the final state of the combinational logic at the end of the unrolled rounds known) and depends on the logic structure. Therefore, multi-bit leakage models may not be a good choice as these bits may not be getting computed together. 1-bit leakage models, thus, act as a better distinguisher [30]. Multi-bit leakage models may provide a better result when linear regression-based analysis is used with different contributions from each bit [31].

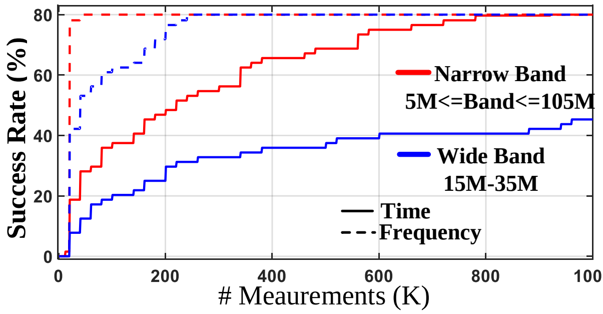

Fig. 10 Success Rate vs Number of Measurements to compare Narrow-band vs Wide-band Filtering

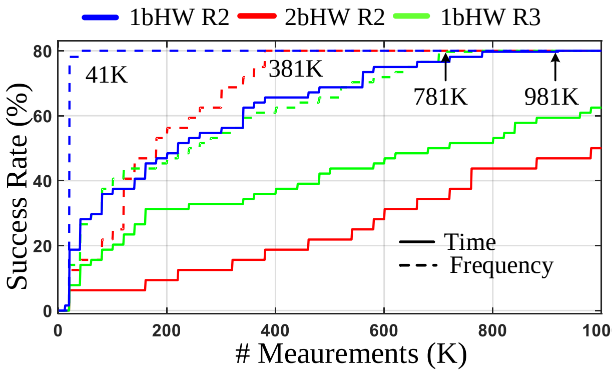

Fig. 9 Success Rate (%) vs Number of Measurements for comparison of time vs frequency domain leakage behavior

SR for SCA in the time domain and frequency domain for 3 different leakage models is shown in Fig 9. Clearly, SR for time-domain CPA attacks for all 3 considered leakage models is lower than CFA attacks. CPA also fails to reveal 80% of bits with 1000K traces, except for 1bHW R2 leakage model, where the MTD is quite high (781K). On the other hand, CFA reveals 80% of the bits with all the 3 leakage models.

The advantage of narrow bandpass filtering techniques is demonstrated with respect to MTD for 80% SR plotted in Fig. 10. The highest leaking band (5MHz-10MHz) for narrow bandpass filtering is compared with wide band (15MHz-35MHz). MTD in the wide-band for CFA attack reveals 80% bits with 241K traces, but time-domain has a poor SR (45%) even with 1000K traces. It also, indicates that some bytes show leakage in bands outside wide band around clock frequency, which cannot be exploited with 15M-35M wide band filters.

2) 10-round Unrolled SIMON-128: S. Cavanaugh has demonstrated a Degenerate Grouping Power Attack, (DGPA), a kind of partition power analysis, on SIMON 64/128 and have shown infeasibility of targeting attack on architectures with >9 degree of unrolling [10]. The proposed methodology in this paper targets leakage from initial few rounds and it should show attack on 10 round unrolled architecture. We have evaluated side-channel resistance of round unrolled implementation to 10th degree, and successfully demonstrated CFA attack revealing 80% bits with 40K traces. The plot shown in Fig. 11,

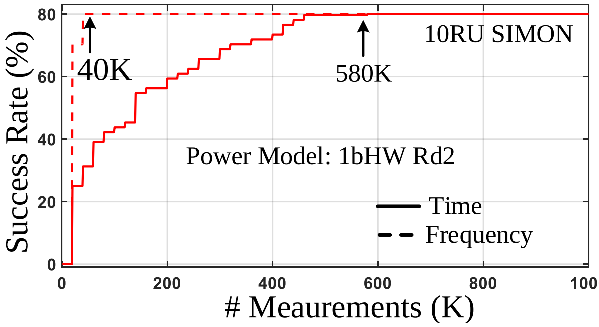

Fig. 11 Success Rate vs Number of Measurements for time-domain and frequency domain correlation attack on 10 rounds unrolled (RU) SIMON

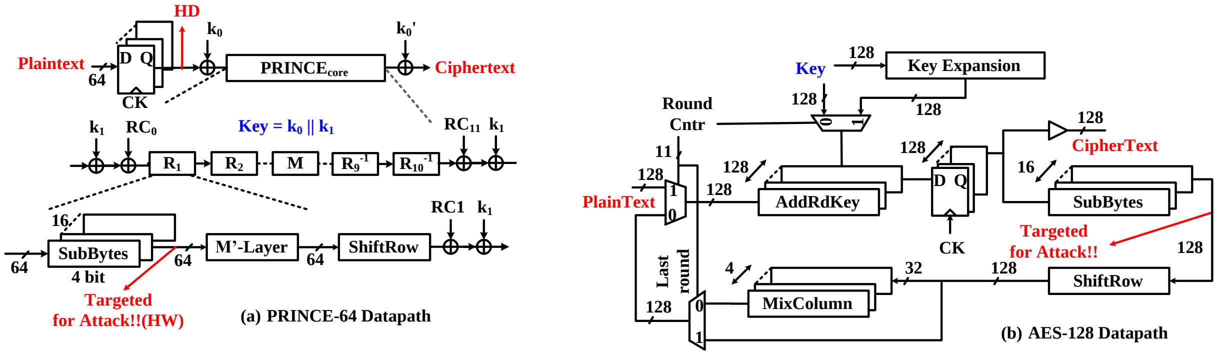

Fig. 12. (a) PRINCE-64 datapath, attack location is the SBOX output of round 1 and (b) AES-128 datapath, implemented as round – reuse logic, attack location is the SBOX output of round 1.

is based on a 1bHW leakage model in round 2. In comparison, time-domain plot could also reveal 80% of bits but has a higher MTD of 580K.

V. Extracting Leakage from Unrolled PRINCE-64 and Parallel AES-128

To demonstrate the general applicability of the improved CFA attack, we have evaluated the power side channel attack (PSCA) resistance of fully unrolled PRINCE block cipher and round-based parallel datapath for AES.

For the fully unrolled architecture of PRINCE, both HW/HD based leakage models were analyzed. The absence of a pipeline makes the encryption engine a purely combinational logic block. The attack location for HD model is the output of first round SBOX and the HD is between the output of the first round SBOX and the input register. For AES, the 128-bit parallel datapath implementation uses round-based logic and reuses the same hardware for 11 rounds to complete the encryption. Since each round output is registered, switching activity can be easily modeled using HD based leakage models. PSCA evaluation of parallel AES has been demonstrated in many prior works. The leakage model is generated using HD between the output at the last round and 2nd to last round. The methodology of targeting non-registered intermediate states as described in Section III, is used to demonstrate PSCA attack with HW based leakage model, demonstrating general exploitability of leakage from combinational circuits.

A. *Fully-unrolled PRINCE-64*

The PRINCE architecture with the target location for mounting CFA, is shown in Fig. 12(a). The output of the SBOX in round 1, R_1, was targeted to generate the required leakage model. Prior to the first round, the plaintext is XOR-ed with k0 followed by k_1 (RC_0=0 and can be ignored in the power-model). Therefore, a hypothesis can be made for a 64-bit key, K, where $K = k_1 \oplus k_0$. This K is subsequently XOR-ed with the 64-bit plaintext before being input into the SBOX of R_1. The SBOX being a 4-bit non-linear operation, creates a 4-bit key dependency for every nibble of its output. We targeted each nibble of the output and generated the HD based leakage model utilizing the key dependencies represented by the following sets of equations:

$$\begin{aligned} \beta i &= Sbox(Plaintext_i \oplus K) \\ \beta_{i-1} &= Sbox(Plaintext_{i-1} \oplus K) \\ HD_i &= (\beta_{i-1} \oplus \beta_i) \end{aligned} \tag{9}$$

where β_i and β_{i-1} are Sbox outputs in the current and previous states respectively, corresponding to successive plaintexts inputs. The HW is calculated simply based on the number of 1 bits in the current state of the output and is represented by:

$$HW = HW(\beta i) \tag{10}$$

For our analysis, we only focus on the extraction of the key K. However, once K is determined, k_1 can be easily targeted by keeping K constant, making a hypothesis for k_1 and targeting the output of the SBOX of round 2. Here we have shown the successful recovery of all the nibbles of K within 1000k measurements. MTD required to recover 80% of bits is expressed as a percentage of the total number of nibbles. Success rate against number of measurements, for HW and HD leakage models for CPA and CFA is depicted in Fig. 13(b). The 80% SR data shows the overall best case MTD to be 280K with HD based leakage models. In contrast, only 13 out of 16 nibbles were recovered using traditional time-domain CPA even after 1000K measurements.

B. *Parallel AES-128*

The AES-128 datapath highlighting the target location is depicted in Fig. 12(b). We have generated an 8bHW leakage model, which is the output bit-width of the SBOX. To generate a leakage model, the input plaintext is divided into 16 bytes, $Plaintext_i$, while the input key (K) is also divided into 16 bytes, K_i. This is followed by AddRoundKey operation which is essentially an XOR of the input plaintext and the key. This is the output of the targeted 1st round SBOX. HW at the output of the SBOX can be described as:

$$HW = Sbox(Plaintext_i \oplus K_i) \tag{11}$$

CPA and CFA are performed on all 16 SBOX outputs. Therefore, 16 HW leakage models are analyzed which cover all 128 key bits. The side channel analysis methodology is applied, and minimum MTD, corresponding frequency domain window, and the highest leaking band is derived from PSCA analysis. MTD required to reveal 80% bits with CPA and CFA are 60K

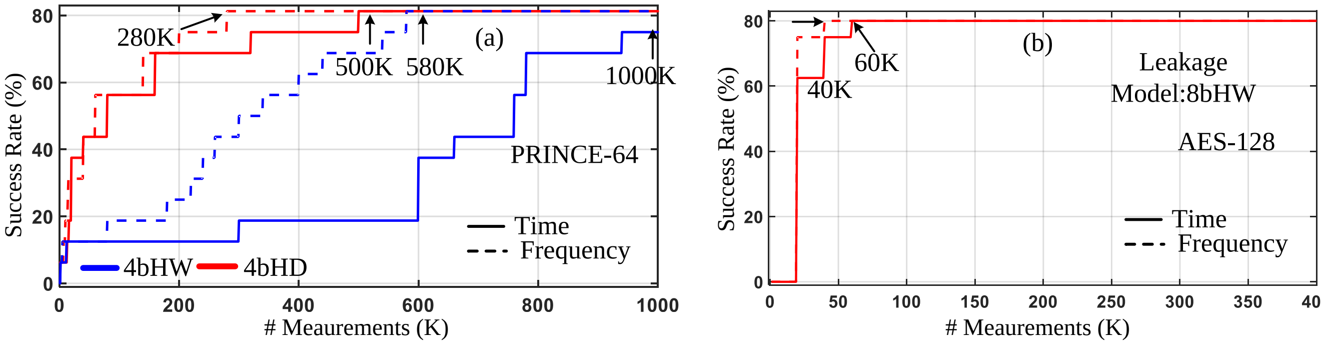

Fig. 13. Success rate vs. number of measurements for time-domain and frequency domain correlation attack for (a) PRINCE-64 for HD and HW power models and (b) AES-128 when combinational SBOX output is targeted instead of sequential registers.

Table 1:Comparison of minimum MTD for 80% Success Rate (SR) for SIMON-128

MTD for 80% Success rate(% bits revealed with 1000K)			
	SIMON		
Filtering	PowerModel	Time	Freq
Narrow Bandpass Filtered	1bHW R2	921K(81.25)	41K(100)
	2bHW R2	1000K(50)	381K(100)
	3bHW R2	1000K(25)	801K(100)
	4bHW R2	1000K(12.5)	1000K(75)
	1bHW R3	1000K(62.5)	781K(100)
Unfiltered	1bHW R2 for SIMON	1000K(45.3)	661K(98.4)
15-35MHz		1000K(45.3)	241K(100)
Narrow bandpass		921K(81.2)	**41K(100)**

Table 2: comparison of minimum MTD for 80% Success Rate (SR) for PRINCE-64 and AES-128

MTD for 80% Success rate(% bits revealed with 1000K)					
		PRINCE		AES	
Filtering	PowerModel	Time	Freq	Time	Freq
Narrow Bandpass Filtered	4bHW R1	1000K(75)	580K(100)	N/A	
	4bHD R1	500K(100)	280K(100)		
	8bHW R1	N/A		60K(100)	40K(100)
Unfiltered	4bHD for PRINCE, 8bHW for AES	500K(87.5)	740K(81.2)	189K(93.7)	44K(100)
15-35MHz		1000K(68.75)	540K(87.5)	58K(100)	58K(100)
Narrow bandpass		500K(100)	**280K(100)**	50K(100)	**40K(100)**

and 40K respectively. SR vs. number of measurements for 8-bit HW leakage model is plotted in Fig. 12(b).

C. Summary and Discussion

Table 1 summarizes the key results obtained for all the leakage models along with their CPA/CFA attacks for 7-round unrolled SIMON-128. It is observed that:

- With the optimal choice of leakage model (1b HW at round 2 output), 80% bits of 7-round unrolled SIMON-128 can be revealed with only 41K measurements. In general, increasing the number of bits considered in the intermediate variable reduces the SNR (2b HW is an exception) and attack efficiency.
- Proposed improved CFA attack with narrow bandpass filtering techniques reduces the MTD for 80% SR by 6× over wide-band filtering and 16× over unfiltered.
- Proposed improved CFA attack when compared to conventional time-domain CPA reduces the MTD for 80% SR by 22× indicating that adverse effects of misalignment are resolved in frequency domain.

The advantage of the improved CFA attack is also reflected in PRINCE-64 where a 2.6× reduction in MTD for 80% SR is observed (Table 2). Even though the improved CFA attack reveals all bits for AES-128, the advantage of using narrow bandpass filtering over unfiltered or wide bandpass is not significant. This could be attributed to a better match between modeled and true leakage possible due to no logic optimization happening between SBOX and Mix-Column operation.

Table 3 compares the proposed leakage models and improved CFA attack with existing works on attack methods on unrolled architectures of lightweight ciphers. Both [10] and [11] could not reveal any key bits with 100K and 500K measurement respectively. Authors in [12] have highlighted that when more than 9 rounds are unrolled for 128-bit SIMON, DGPA attack is computationally infeasible. In comparison, our work shows that all bits of unrolled SIMON-128 can be revealed with a small number of measurements, regardless of the number of rounds unrolled.

We observe that the proposed 1-bit HW leakage models offer the best attack efficiency with a significant reduction in attack efficiency when employing multi-bit leakage models. Linear regression with multi-bit leakage models is expected to improve the attack efficiency because the contribution from all the bits is not expected to be the same for unrolled datapaths based on the mismatch between modeled and true leakage. However, this work only focuses on first-order attacks on unrolled architectures rather than a comparison of different attack methods. Future work will investigate applying linear regression for multi-bit leakage models as well as applying the improved CFA attack for fully-unrolled implementations presented for DES in [10]. Additionally, mutual information analysis (MIA)-based distinguisher, template attacks and higher order DPA could also be explored to see if attack efficiency can be further improved.

Table 3: Comparison of minimum MTD of the proposed method with existing works

Power Attack Technique	**Cipher**	**Architecture**	**Time/ Freq.**	**Leakage Model**	**Minimum MTD**
CPA, MIA [13]	DES	Fully Unrolled	Time	6b HD at round 1	100K(No Attack)
CPA [14]	SIMON	6-round Unrolled	Time	1b HW at round 3	500K(No Attack)
DGPA [15]	SIMON	>= 9-round Unrolled	Time	1b, 4b PPA and AON	Not Feasible
This work: Improved CFA	**SIMON**	**7- and 10-round Unrolled**	**Freq.**	**1b HW at round 2**	**5K (7r), 20K (10r)**

VI. Conclusion

This paper demonstrated optimal leakage models and an improved CFA attack to extract leakage from combinational logic of unrolled architectures of lightweight ciphers. Through side-channel analysis, performed on Sakura-G FPGA for SIMON, PRINCE and AES implementations, we showed the applicability of the approach to any degree of unrolling. Exploration of leakage model selection and impact of narrow band pass filtering is studied to reduce the minimum-trace-to-disclosure for key recovery. Through the analysis performed on 7 rounds unrolled SIMON using SNR and SR, we showed 1bHW leakage model to be the optimal choice with respect to improved CFA, with lowest MTD (41K) for 80% SR. Furthermore, 24× improvement is achieved with improved CFA attack when compared with conventional time-domain CPA. General applicability of the proposed methods is also demonstrated by successfully recovering all key bits from fully unrolled implementation of PRINCE-64 and parallel AES-128.

VII. Acknowledgement

This material is based on work supported by Semiconductor Research Corporation through Texas Analog Center of Excellence (#2810.002).

References

[1] B. Subhadeep, “Midori: A Block Cipher for Low Energy.” In: Proceedings, Part II, of the 21st International Conference on Advances in Cryptology --- ASIACRYPT 2015.

[2] J. Borghoff, et. al., “PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications”, In: Wang X., Sako K. (eds) Advances in Cryptology – ASIACRYPT 2012. ASIACRYPT 2012. Lecture Notes in Computer Science, vol 7658. Springer, Berlin, Heidelberg.

[3] R. Beaulieu, et. al., "The SIMON and SPECK lightweight block ciphers," 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, 2015, pp. 1-6.

[4] P. C. Kocher, et. al., “Differential Power Analysis”, In Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '99), Springer-Verlag, London, UK, UK, 388-397.

[5] E. Brier, et. al., “Correlation Power Analysis with a Leakage Model”, In: Joye M., Quisquater JJ. (eds) Cryptographic Hardware and Embedded Systems - CHES 2004. CHES 2004. Lecture Notes in Computer Science, vol 3156. Springer, Berlin, Heidelberg.

[6] S. Mangard, N. Pramstaller, E. Oswald, “Successfully Attacking Masked AES Hardware Implementations. In Cryptographic Hardware and Embedded Systems – CHES 2005. CHES 2005. Lecture Notes in Computer Science, vol 3659. Springer, Berlin, Heidelberg

[7] B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov, V. Rijmen, “Higher-Order Threshold Implementations” In Advances in Cryptology – ASIACRYPT 2014. ASIACRYPT 2014. Lecture Notes in Computer Science, vol 8874. Springer, Berlin, Heidelberg

[8] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De and S. Mukhopadhyay, "8.1 Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator," 2017 IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, CA, 2017, pp. 142-143.

[9] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De and S. Mukhopadhyay, "Improved power side channel attack resistance of a 128-bit AES engine with random fast voltage dithering," ESSCIRC 2017 - 43rd IEEE European Solid State Circuits Conference, Leuven, 2017, pp. 51-54.

[10] S. Bhasin, et. al., “Unrolling Cryptographic Circuits: A Simple Countermeasure Against Side-Channel Attacks” In: Pieprzyk J. (eds) Topics in Cryptology - CT-RSA 2010. CT-RSA 2010. Lecture Notes in Computer Science, vol 5985. Springer, Berlin, Heidelberg

[11] A. Singh, et. al., "Energy Efficient and Side-Channel Secure Cryptographic Hardware for IoT-edge Nodes," in IEEE Internet of Things Journal.

[12] S. Cavanaugh, “A General Degenerate Grouping Power Attack with Specific Application to SIMON and SPECK.” Cryptology ePrint Archive, Report 2017/382.

[13] V. Yli-Mayry, et. al., “Improved power analysis on unrolled architecture and its application to PRINCE block cipher.” In: G¨uneysu, T., Leander, G., Moradi, A. (eds.) LightSec 2015. LNCS, vol. 9542, pp. 148–163. Springer, Heidelberg (2016).

[14] I. Levi, et.al., "Data-Dependent Delays as a Barrier Against Power Attacks," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 62, no. 8, pp. 2069-2078, Aug. 2015

[15] J.-S. Coron et. al., “An efficient method for random delay generation in embedded software,” in Cryptographic Hardware and Embedded Systems-CHES 2009. Springer, 2009, pp. 156–170

[16] O. Schimmel, et. al., “Correlation power analysis in frequency domain”. In: COSADE 2010 - First International Workshop on Constructive Side-Channel Analysis and Secure Design, 2010

[17] F.-X. Standaert, et. al., “A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks.” In proceedings of Eurocrypt 2009, Lecture Notes in Computer Science, 2009, pp 443-461. Retrieved from: the Cryptology ePrint archive

[18] E. Prouff, M. Rivain and R. Bevan, "Statistical Analysis of Second Order Differential Power Analysis," in IEEE Transactions on Computers, vol. 58, no. 6, pp. 799-811, June 2009.

[19] S. Tiran, et. al., “A Frequency Leakage Model and its application to CPA and DPA.” IACR Cryptology ePrint Archive 2013 (2013): 278.

[20] R. Scheffer-Teixeira, et. al., “On High-Frequency Field Oscillations (>100 Hz) and the Spectral Leakage of Spiking Activity”, Journal of Neuroscience, 2013

[21] S. Bhasin, et. al., “A look into SIMON from a side-channel perspective.” In Hardware-Oriented Security and Trust, HOST 2014, pages 56–59. IEEE Computer Society, 2014.

[22] D. Shanmugam, et. al., “Differential Power Analysis Attack on SIMON and LED Block Ciphers”, In: Chakraborty R.S., Matyas V., Schaumont P. (eds) Security, Privacy, and Applied Cryptography Engineering. SPACE 2014. Lecture Notes in Computer Science, vol 8804. Springer, Cham.

[23] A. Singh, et. al., "Energy efficient and side-channel secure hardware architecture for lightweight cipher SIMON," IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, 2018, pp. 159-162.

[24] R. Selvam, et.al., "Side channel attacks: Vulnerability analysis of PRINCE and RECTANGLE using DPA" Proc. IACR Cryptology ePrint Archive pp. 1-15 2014..

[25] T.S. Messerges, et. al., “Investigations of Power Analysis Attacks on Smartcards.” In: USENIXWorkshop on Smartcard Technology, pp. 151–162 (1999)

[26] C. Clavier, et. al., “Differential power analysis in the presence of hardware countermeasures.” In: Ko¸c, C¸.K., Paar, C. (eds.) CHES 2000. LNCS, vol. 1965, pp. 252–263. Springer, Heidelberg (2000)

[27] D. Oswald, et. al., “Improving side-channel analysis with optimal linear transforms.” In: Mangard, S. (ed.) CARDIS 2012. LNCS, vol. 7771, pp. 219–233. Springer, Heidelberg (2013)

[28] I. Levi, et. al., "Low-Cost Pseudoasynchronous Circuit Design Style With Reduced Exploitable Side Information," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 26, no. 1, pp. 82-95, Jan. 2018.

[29] S. Guilley, et. al., “Quantifying the quality of side channel acquisitions,” COSADE’11 - First International Workshop on Constructive Side-Channel Analysis and Secure Design.

[30] F.-X. Standaert, et. al.,“Partition vs. Comparison Side Channel Distinguishers: An Empirical Evaluation of Statistical Tests for Univariate Side-Channel Attacks.” In: Lee, P.J., Cheon, J.H. (eds.) ICISC 2008. LNCS, vol. 5461, pp. 253–267. Springer, Heidelberg (2009)

[31] F.X., Standaert, “Univariate side channel attacks and leakage modeling.” In: Proceedings of Constructive Side-Channel Analysis and Secure Design ,COSADE 2011, pp. 1–15 (2011)