IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 28, 2017, accepted October 21, 2017, date of publication November 2, 2017,
date of current version November 28, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2766243

A Survey of the Sensitivities of Security Oriented Flip-Flop Circuits

ITAMAR LEVI, NETANEL MILLER, ELAD AVNI, (Student Member, IEEE), OSNAT KEREN, AND ALEXANDER FISH, (Member, IEEE)
Faculty of Engineering, Bar-Ilan University, Ramat Gan 5290002, Israel

Corresponding author: Itamar Levi (itamarlevi@gmail.com)

The work of O. Keren was supported by the Israel Science Foundation under Grant 923/16. The work of A. Fish was supported by the Israel Science Foundation under Grant 1868/16.

ABSTRACT Side channel attacks have become a major threat to hardware systems. Most modern digital IC designs utilize sequential elements which dominate the information leakage. This paper reports the first unified analysis and comprehensive comparison of known secure flip-flop circuits. We present a device level analysis of the information leakage from these FFs and propose several evaluation metrics to quantify their security. We show that simulated PA attacks that utilize the information evaluated by these metrics at the gate-level extract more information at the module-level.

INDEX TERMS Cryptography, countermeasures, CPA, DPA, flip-flops, power analysis, sequential-circuits, synchronous.

I. INTRODUCTION

Digital systems that process or store personal information are liable to Side Channel Analysis attacks (SCA) [1], [2]. SCA attacks utilize information that is associated with the physical implementation of the hardware to extract private information. One of the most powerful side channel attacks is known as Power Analysis (PA) [2], [3]. PA attacks exploit the correlation between the processed data and the device's dissipated current, which they use to extract the cryptographic key employed for encryption. In model-based PA attacks, the attacker computes a hypothesized dissipated current, which reflects the current induced by expected logical transitions of signals in the circuit, and then correlates it with the measured power supply current. Correlation-based attack-methodologies must rely on statistics since the current samples are very noisy. A successful attack depends on the attacker's ability to correlate multiple hypotheses with the corresponding current samples from the times they are processed.

Correlation-based [4] PA attack procedures can be divided into several stages as detailed in [2] and [3]. Prior to these stages, the attacker implements the necessary preprocessing step of segmenting the large amount of power measurements that have been collected and synchronizes the segments with the hypothesized currents. The efficiency of the PA attack depends almost exclusively on this synchronization.

Most modern digital IC designs nowadays are implemented in the synchronous design style which have become very popular mainly because of their design simplicity. In conventional synchronous designs, a single clock is utilized for many design modules such that many vectors in the design are sampled simultaneously. This makes synchronous designs very vulnerable to PAs. The Globally Asynchronous Locally Synchronous (GALS) design style [5]–[7] is considered to be attractive from the hardware security perspective. In GALS designs each local module is synchronized by a local clock signal but communication between different local modules takes place asynchronously. In this case, only local module signals are sampled by the same clock, so their level of security is thought to be higher than synchronous designs.

Both synchronous and GALS designs utilize sequential elements. Therefore, groups of signals are sampled with synchronization to a clock using these sequential elements. This makes the design of secured sequential elements a key challenge [3], [8]. The sequential elements are typically constructed from a large number of transistors, as compared to basic combinational elements. Thus, their operation draws large currents leaving a substantial power profile signature.

The hardware security problem is considered as a multidisciplinary problem. Flip-Flops are a key component in any hardware system- thus their contribution to the system's immunity to side channel attacks (such as power attacks) should be taken into account across levels and disciplines, starting from the circuit designers through cryptographers up to the system engineers.

Many sequential elements have been proposed over the years to optimize electrical properties such as [9]–[11] energy, area, performance and reliability. The increased interest in the security characteristics of sequential elements (mainly their sensitivity to Power Analysis attacks) has resulted in proposals for several topologies of these elements. These solutions aim to weaken the correlation between input transitions (or input states) and the current dissipated by these elements. Flip-flop (FF) circuits are used almost exclusively by digital system designers and are supported by digital-automation tools. As such and as expected, FFs have been the most highly researched sequential elements in terms of PA immunity and are the focus of this paper. For example, the Sense Amplifier Based Logic (SABL) [12] and the Improved SABL [13]–[15] flip-flops have a symmetric transistor-level scheme and operation targeted to consume equal energy/current for all transitions (similarly concepts to that of the dynamic current mode logic based flip-flop, DyCML [30]). The Secured Detect D-FF [16] is designed to identify states in which the output does not switch, by triggering a dummy flip-flop that consumes the "switching" energy in these states. The delayed detection mechanism based FF (denoted by DelayedFB DFF) [17] and the Three Phase Dual Rail Logic based (TDPL) FF [18], [19] are implemented using the concepts of dynamic logic and utilize a unique timing scheme to *precharge* and/or discharge the stored energy to provide constant energy for each computation.

Although a variety of secured sequential elements have been proposed in the literature, their security properties have not been thoroughly evaluated and compared using the same evaluation environment and metrics. This manuscript aims to provide a solid evaluation environment for the PA security characteristics of sequential elements. In addition, we evaluate previously reported security metrics at the gate level and propose improved metrics.

The contributions of this work are as follows:

- A unified comparison of known secured-FFs.
- A circuit level analysis of the secured-FFs weaknesses.
- Presentation of several evaluation metrics which are shown to better quantify the security of the secured- FFs.
- Soft-spots of various security oriented FFs are associated with security metrics so as to identify them.
- Simulated PA attacks that utilize the information evaluated by the proposed metrics at the gate-level are shown to extract more information at the module-level.

The remainder of this manuscript is organized as follows: Section 2 provides a short background on related work. The evaluation setup used to examine and compare information leakage is detailed in Section 3. In Section 4 we discuss several known metrics to evaluate the information leakage of these devices. In addition, several new evaluation metrics are proposed. Section 5 analyzes the device-level information leakage mechanisms of the sequential elements under consideration. A discussion and examination of these metrics based on the device level examination follows in Section 6. Section 7 proves that PA attacks on the module level that utilize the information evaluated through the proposed gate-level metrics are more efficient and Section 8 concludes and summarizes this manuscript.

II. A SECURITY PERSPECTIVE ON KNOWN SECURED FLIP-FLOPS

Flip-Flops (FF) are typically (and almost exclusively in standard libraries) constructed from Master-Slave [9] latches. A conventional *static* latch is comprised of a back-to-back inverter pair [20] (cross-coupled structure) and additional control signals (e.g. clock) and circuitry. The back-to-back pair, which is the main reason for the robust operation of a static latch, is responsible for its "*differential*" nature. In other words, each latch stores both a data bit and its complement. In conventional FFs the "no-change" and "change" states can be differentiated, thus making them vulnerable to power attacks.

Due to the resistive or capacitive *imbalance* between the nodes in the non-ideal (physical) world, each of the two "change" states (0→1 and 1→0) can be distinguished by a PA attack. This imbalance can be caused by different sizes of the devices, imbalanced routing, physical mismatch or variations.

In this section, we present a short security-oriented review on related work and previously proposed solutions for secured FFs implementations.[1]

A. SECURED DETECT FLIP FLOP (DETECT-FF)

The *Detect*-FF structure[16], shown in Fig. 1(a), aims to achieve a data-independent current by duplicating the main flip-flop (which results in FF1 and FF2) and by adding a *detector-generator* unit. The role of the detector-generator is to identify whether switching of FF1 has occurred or not, and trigger the switching operation of FF2, if needed. This scheme assures that only one FF (FF1 or FF2) will switch in each cycle. This functionality makes the *detect*-FF *dynamic*[2] and *differential*[3]; however, the main pitfall of this architecture is that the detector-generator unit responds differently to various inputs. When doing so, the detector-generator unit draws current that leaks information on the manipulated input data. Later in this manuscript we analyze and show in which circumstances this information-leak is substantial and discuss the reasons for this information leakage.

B. SENSE AMPLIFIER BASED LOGIC FLIP FLOP (SABL-FF)

SABL-logic gates [12] are based on a sense amplifier circuit, as shown in Fig. 1(b). A basic sense amplifier circuit is sensitive to the voltage-difference between its inputs and amplifies this difference (positive and negative differences result in '0'

[1] For a detailed review of a specific scheme or for other orientations than security the reader is referred to the relevant papers.

[2] *Dynamic* refers to a node that first *charges* (or *discharges*) its voltage to a known deterministic value and then *evaluates* (or computes) its voltage to a logical value which corresponds to the inputs and the functionality.

[3] *Differential* is a property associated with two nodes that compute/hold both a logical value and its complement.

and '1' values at the output, respectively). In the context of the *SABL* gates, the inputs are *differential* (D and $\bar{D}$) and its architecture is symmetric in layout and operation. In the *ideal* case, this symmetry leads to current data-independence between "switching" transitions. *SABL* gates also utilize two clocked transistors which *precharge* the *differential* outputs in every clock cycle. Therefore, the circuit is *differential* and *dynamic* (circuits having both properties are typically referred to as *Dual-Rail Precharge, DRP* [17]).

In fact, the *SABL*-FF architecture employs an SR-latch which is connected to the sense amplifier outputs (highlighted in grey in the figure). The SR latch stores the FF state on a *cross-coupled NANDs* structure (N_1 and N_2 in Fig. 1(b)). The clocked *precharge* transistors trigger an update in the SR state when *clock*='0'. The sense amplifier then reacts on a clock transition to a logical '1'. It is important to note that even though the SR-latch implementation is symmetric (*differential*) and its inputs are dynamically *precharged*, the concatenation of the sense-amplifier and the SR-latch is not *dynamic*. It reacts differently to an input change or no-change.

This is a significant drawback in the context of security, as will be detailed in Section IV.

C. IMPROVED SABL-FF

The *Improved SABL*-FF is based on the *SABL*-FF with two additions:

- An additional transistor is superimposed between the *differential* pair outputs as shown in Fig. 1(c), similarly to the *Strong Arm*-FF [13], [14] circuit. This transistor is added to *discharge* both int_1 and int_2 internal nodes during the *evaluation*[4] (clock = '1'). That is, when the *n-MOS* footer transistor (*ft*) is open, both internal nodes are discharged (one to '0' and one to the *n-MOS* threshold voltage, V_{th}). This mechanism initiates the *discharge* and *precharge* of the pair of the differential internal nodes, which means that no information from a capacitive imbalance of these nodes can be utilized. However, as one of the nodes will only discharge to V_{th} *and not to 0V*, the efficiency of this mechanism is undermined.
- The *SR*-Latch is replaced by an *improved SR*-Latch which is designed (by changing device sizing) to provide smaller data-dependent currents for the latch than the *SABL* as discussed in the next section.

Up to this point all these FFs have been compatible with a standard synchronous system operating by a single clock signal. Below we discuss FFs that are only compatible with dynamic-logic flavors (e.g. np-Domino [20], NORA [21], Domino [22], DML [23], [24]) that employ signals with unique timing control. In these FFs the data signals (*D* and its complement) are bound to specific *precharge* and/or *discharge* periods within the clock cycle. Note that the construction of the systems which follows these strict timing diagrams is more complex.

As discussed above, the design of an ideal *dynamic* and *differential* circuit is complex since the *SABL*-FF's *SR*-latch operation reveals information about the data. However, the *Improved SABL*-FF's SR-latch and the added internal transistor operation induce currents which are still data dependent. The asymmetry of the *Detect-FF's detector-generator* unit leaks information on all possible output transitions.

D. DELAYEDFB-DFF

The *DelayedFB-DFF* [17] is based on the *SABL*-FF structure with two main differences:

- Two delay elements (buffers) are added in the feedback-loops of the differential pair (as shown in Fig. 1(e)). These elements tolerate imbalanced differential-input transitions (variations in transition-*slopes*, *arrival-delays etc.*). The principle of operation is based on the fact that an input change triggers the operation of the *cross-coupled pair* with an additional delay. This means that if the input-change duration is smaller than the added delay, the internal nodes affected by the inputs will already be stable when the *cross-couple* pair reacts. Thus, the same current will be drawn from the power supply in case of *imbalance*.
- The outputs of the *DelayedFB-DFF* FFs are *discharged* to '0' (or *precharged* to '1', if an output inverter is added) during the *precharge* phase. During the *evaluation* phase, only one of the outputs will be *charged* (or *discharged*). This contrast with the *SABL*-FF; though the internal nodes of the *SABL*-FF are *precharged* in each cycle, its outputs are not.

E. THREE PHASE DUAL RAIL FLIP FLOP (TDPL-FF)

The *TDPL* logic family [18], [19] operation is somewhat more complex than the two-phased *dynamic* logic (i.e. *precharge* and *evaluation* phases). The *TDPL* circuits utilize *dynamic* logic gates; however, they operate in three phases: *precharge*, followed by *evaluation,* followed by *discharge*. The *TDPL*-FF architecture uses two *TDPL* inverters, at its input and output, connected through a slightly modified *SR*-latch to store the data, as shown in Fig. 1(d).

The main difference with the two-phase methodologies discussed above is the ability to tolerate differential output imbalances. In the physical (non-ideal) world, differential outputs can be affected by the imbalance between resistive and/or capacitive networks. In two-phase timing-schemes, this implies that the *instantaneous* current and/or *total* energy differ for different transitions. The special three-phase *TDPL* timing diagram ensures that both differential output nodes are *precharged* and *discharged* in each clock cycle. Therefore, the *total energy* consumed per clock cycle is not affected by variations in capacitance. However, it is important to note that the *instantaneous current* will show data-dependency due to the imbalance in resistance.

[4] *Evaluation* is the phase of settling on a desired logical value after a charge or *discharge* phase (denoted typically by *precharge or discharge*).

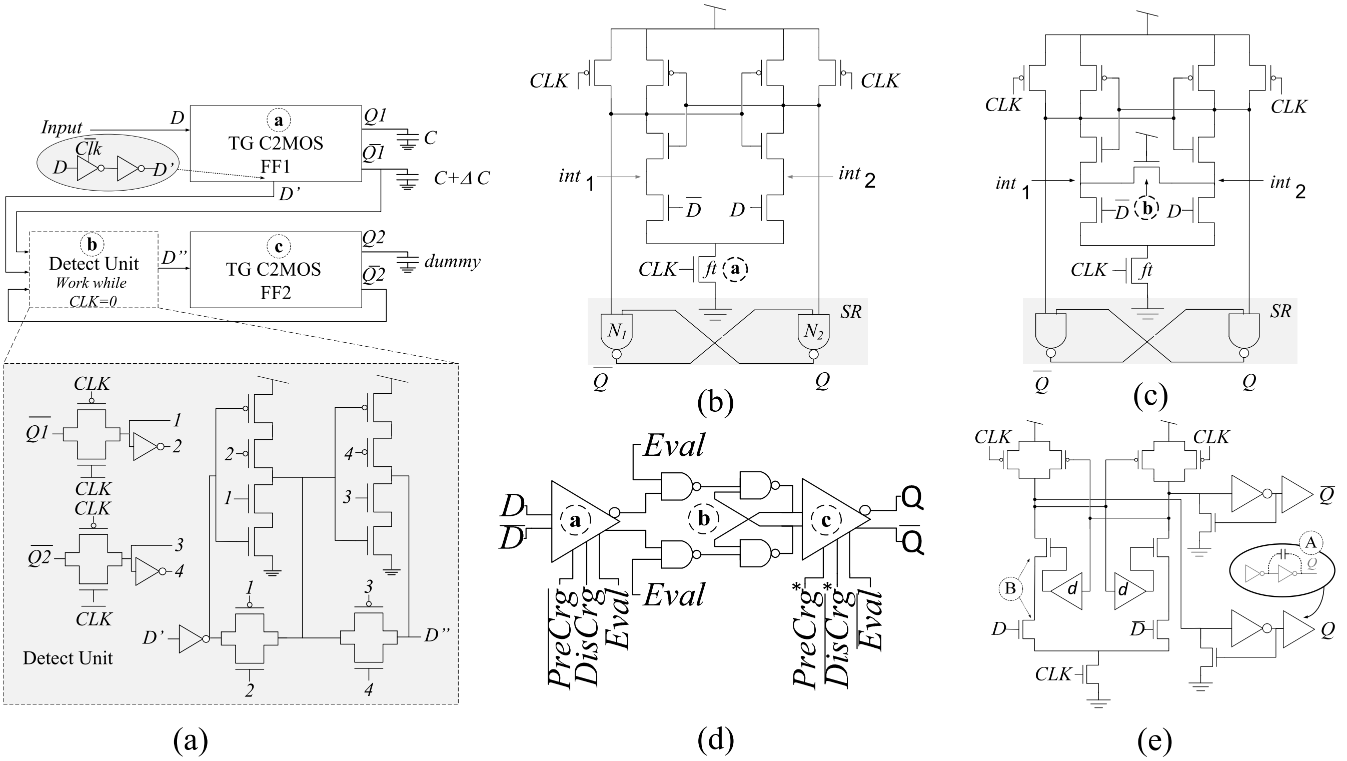


FIGURE 1. FF designs: (a) ***Detect-FF*** (b) ***SABL*-FF** (c) ***Improved SABL*-FF** (d) ***TDPL*-FF** (e) ***DelayedFB-D*FF.**

Note that the two *TDPL* inverters (Fig. 1(d)) are controlled by different control signals; namely, the *evaluation* phases of the two inverters are complementary and the corresponding *precharge* and *discharge* phases precede and follow (respectively) the evaluation phases of one of the gates (in Fig. 1(d) the output *TDPL*-inverter control signals are marked by an '∗' to denote the difference).

III. GENERIC EVALUATION ENVIRONMENT FOR FFS

To state that solution A provides more security than solution B a generic testing environment needs to be defined in which their effectiveness in concealing information is tested and compared under the same setup, equivalent conditions and the same metrics. In what follows we describe this type of testing environment and provide a rationale.

As mentioned above, there is a difference between an ideal FF and a fabricated one caused by variations in driving strengths, physical delays, local and global variations, noise etc. This leads to mismatches between the differential signals and their associated devices and the security the FF provides. The following generic environment mimics realistic operation conditions and supports the following factors:

1) IMBALANCE IN LOAD CAPACITANCES OF THE FF'S DIFFERENTIAL OUTPUTS

Many secured FFs contain complementary outputs which must be assigned equal loads. In practice, given different load gates, Fan-Outs and routing imbalance, the load on each output can be different. Hence the sensitivity of the FF to this imbalance must be evaluated.

2) DELAY MISMATCH BETWEEN THE TWO COMPLEMENTARY INPUTS (DENOTED BY INVERTED INPUT DELAY)

In general, in circuits with more than one input, the arrival time of each input can be different due to process-voltage-temperature (PVT), glitches, paths delays (gates and routing) etc. The same also applies to differential inputs.

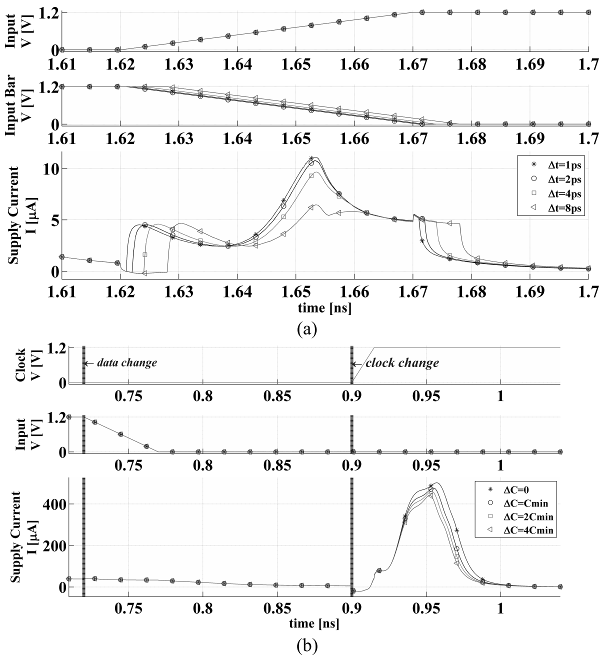
3) IMBALANCE IN INPUT SLOPES

The voltage transition slope of each node in a design depends on many factors. This includes the logical gates in the path leading to the node, the physical parameters of the wires and loads, different Fan-Outs, etc. The generic evaluation environment allows for a characterization with a set of slopes, S, per technology.

4) DATA CHANGE AT INPUTS DURING DIFFERENT CLOCK STATES

The behavior of a FF depends on the clock state. Clearly this results in a different current signature if the input data changes while the clock is at '0' or at '1'.

To illustrate the impact of these *imbalance* factors, Fig. 2 shows current measurements of two *SABL*-FF designs



(a)

(b)

FIGURE 2. Illustrative supply current dependence on (a) *Inverted Input Delay* and (b) *Different Load Capacitance.*

TABLE 1. Examples of simulation parameters.

Symbol	Quantity	Simulated Values
ΔC	capacitance imbalance	0,*C$_{out}$, 2 C$_{out}$, 4 C$_{out}$
Δt_{inv}	Inverted input delay	1, 2, 4, 8 [ps]
S	Input slope	50, 60, 70 ,80 [ps]

*C$_{out}$ reflects a Fan-Out of one input load.

using this environment. Fig. 2(a) presents the influence of the *delay* between two complementary *inputs* (denoted by Δt) on the measured current. Fig. 2(b) shows the impact of imbalance on the *differential load-capacitance (denoted by* ΔC_{out}).

Illustrative sets of imbalance factors for 65*nm* bulk technology with a supply voltage of 1.2V are listed in Table. I. It is clear that the sets depend on the technology under evaluation. All simulations were conducted using an analog simulation tool (Cadence Virtuoso) over the post-layout parasitic extracted designs and were further post processed in Matlab.

A generic setup that allows for FF evaluation as a function of these imbalances is illustrated in Fig. 3. Three emulation units were connected to the units-under-test (UUTs). The *input generator* is responsible for generating all the differential input transitions, each is repeatedly generated with all specified *slopes* (set S) and *Inverted Input Delays* set (Δt_{inv}). The *differential capacitance generator* unit provides a set of *differential load capacitances* (ΔC). For all experiments the power supply current was measured on a dedicated resistor and stored for further processing in Matlab.

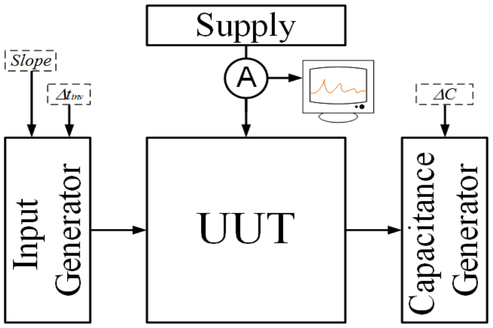


FIGURE 3. Parametric evaluation setup.

IV. EVALUATION METRICS

This section reviews known metrics for gate-level security evaluation and presents two new metrics. In particular, we address the Instantaneous Variance, NED_1, NSD_1, NV_1 used and discussed in [12], [14], [18], [19], and [25].

A. KNOWN METRICS

The gate-level security of FF's is usually evaluated by the variance of the dissipated current over different data transitions or by simplified versions of this matric, for example: Normalized Variance (NV$_1$), Normal Standard Deviation (NSD_1), Normalized Energy Deviation (NED_1) as evaluated in [12], [14], [18], [19], and [25]. In all metrics, high values correspond with high information leakage.

The NED_1 and NSD_1 metrics utilize information from the consumed current during the whole clock period; that is, the instantaneous current has to be integrated over the whole clock cycle period prior to the analysis. These metrics reduce the amount of information to be stored and processed; nevertheless, the integration filters out valuable instantaneous information.

These matrices are defined as follows:

- The NED_1 metric is a function of the *max* and *min energy* (E_{max}, E_{min}) over all possible data transitions. It reflects the normalized difference between the two. Thus, it disregards the probabilities distribution of these values. Formally,

$$NED_1 = \frac{E_{\max} - E_{\min}}{E_{\max}}$$

where, the random variable E stands for the computation energy:

$$E = V_{DD} * \int_0^T I_{V_{DD}}(t)dt.$$

- The NSD_1 is the *standard deviation* of the energy normalized by the *mean* value of the energy:

$$NSD_1 = \frac{\sigma_E}{\mu_E}$$

Where σ_E and μ_E are the standard deviation and mean of the energy (E) respectively.

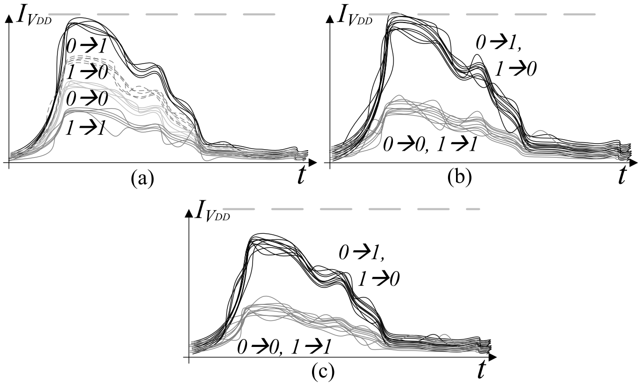


FIGURE 4. Schematic current waveform of three different ***abstract***-FFs.

- The instantaneous NV_1: Unlike the NED_1 and NSD_1, the current normalized variance (NV_1) metric relates to the points in time where the instantaneous current is maximized. It utilizes information from the instantaneous current trace and finds the point in time where the variance is maximal (for this reason the matric is denoted by *instantaneous*). Formally

$$NV_1(t) = \frac{\sigma^2_{I(t)}}{\mu^2_{I(t)}}$$
$$\overline{NV}_1 = \max_{t\in(0..T)} (NV(_t))$$

where $\sigma_{I(t)}$ and $\mu_{I(t)}$ are the standard deviation and mean of the instantaneous current in time sample t, respectively. Although the NV_1 metric better reflects the information leakage it has a drawback; it does not distinguish between leakage of different transitions. Fig. 4 demonstrates this point: The schematic current waveform of three different FFs are illustrated. FF-a is an abstraction and simplification of a Single-Rail logic in which each data-transition induce different current profile. FF-b and FF-c are a schematic abstraction of a Dual-Rail logic where the current's shape reflects only two current profiles (depending on the *Hamming Distance*). Notice that FF-a and FF-b have the same Max and Min Energy therefore the NED_1 will indicate that in terms of security they are equivalent. Whereas FF-a and FF-c have the same average energy, thus, the NSD_1 and NV_1 cannot indicate that FF-a leaks much more information than FF-c. In what follows we introduce two alternative metrics to evaluate the information leakage more accurately.

B. NEW METRICS

Below we introduce two alternative flavors to the metrics described above.

To better highlight differences between the methods we attach a subscript to the name of the metric (e.g. NED_1, NED_{state}, NV_{HD}). Index *1* indicates that the metric computation was done on the whole set of current trace vectors.

Here we suggest dividing the currents into four groups, where each group is associated with a specific data transition *state*. The set of states' S is $S = \{0 \rightarrow 1, 0 \rightarrow 0, 1 \rightarrow 0, 1 \rightarrow 1\}$. For each $s \in S$ the average trace $\overline{I}_s$is computed over all the current traces corresponding to this transition. Then, the three metrics are computed with respect to the four average traces; for example

$$NED_{State} = NED_1\left(\overline{I_s}, s \in S\right),$$

The second metric is based on *Hamming Distance* model. It divides the currents into two disjoint groups according to the *HD* ('0' or a '1'), and computes two average currents, $\overline{I}_{HD_0}$ and $\overline{I}_{HD_1}$. Then the metrics are computed, for example

$$NED_{HD} = NED_1\left(\overline{I}_{HD_0}, \overline{I}_{HD_1}\right).$$

The grouping prior to the metric computations emphasizes cases where each input transition derives a unique current pattern or when groups of transitions leak different information. This is quite similar to DPA-grouping [3] or templating different groups [3], [26]; however, this is done at the gate-level to quantify leakage sensitivities. In Section VI these metrics are evaluated and their efficiency is examined for different FF circuit topologies.

V. SECURITY ANALYSIS – TRANSISTOR LEVEL

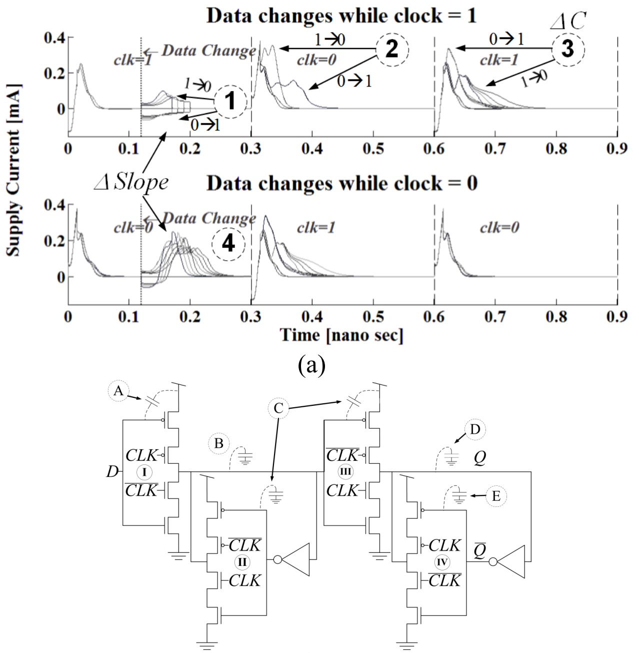
Next, we analyze the mechanisms of information leakage at the transistor-level of the FFs described in Section II. For each of these FFs, we provide a waveform showing where in time the information leak takes place and explain the transistor level mechanisms that trigger them. Clearly, understanding the soft-spots of the FFs enables a more robust evaluation of their information leakage and provides opportunities for designing secured circuits.

A. C^2MOS FF

The C^2MOS-FF [see Fig. 5(b)] has never been used for security applications, since its current dissipation is highly data-dependent. That is, each input transition is associated with a distinct current pattern. As will be discussed below, C^2MOS -FF is an important building block for some secured FFs. In addition, the C^2MOS *FF* based architecture is widely used in standard cell libraries and therefore can serve as a reference point for non-secured-FFs [9]. For these reasons, it is briefly discussed in this sub-section.

Fig. 5(a) shows the current waveforms of all possible data transitions[5] over all ***imbalance*** factors, as discussed in Section III. The upper figure shows the case where the data change occurs while the clock is at '1'. The clock toggles every 0.3 *ns*, starting from a logical '1'. The change in data occurs in $t \in \{0, 0.3\}$ [*ns*]. The figure indicates the points-of-interest (POIs) in time where large current variance is captured (denoted by numbered circles, 1:3). The C^2MOS -FF scheme is shown in Fig. 5(b). This figure will be used

[5] Note that the term *Data change* in the figures relates to all possible data transitions; that is, the set $\{D_{old}, D_{new}\} = \{i, j\}$; $i, j \in \{0, 1\}$.



(a)

(b)

FIGURE 5. ***C^2MOS -FF:*** **(a) current trace for *data-change* while *clock='1'* (upper) and *clock='0'* (lower) and (b) *scheme*.**

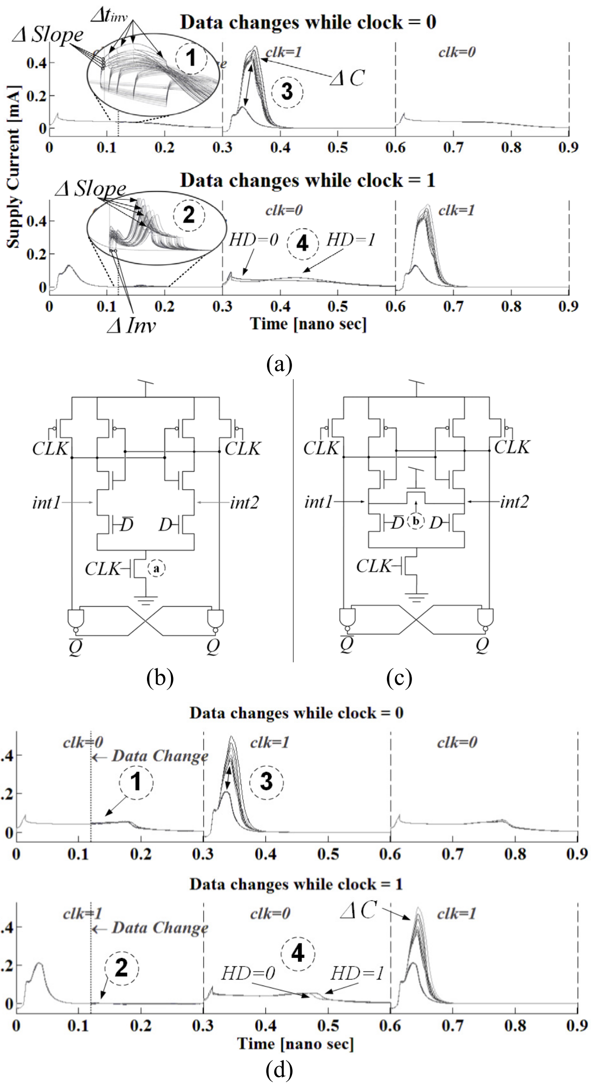
to examine transistor-level mechanisms associated with the high variance POIs. In order to simplify the presentation, the devices are denoted by circled capital letters in Fig. 5(b).

Next, we elaborate on the POIs and their associated information leakage mechanisms.

POI-(1) At this POI the input changes while the clock='1' (the first clocked inverter, *I*, is "closed"). The input change induces a power bounce on V_{DD} due to the upper *p-MOS* gate-source coupling-capacitance (denoted by *A*). A rising 0→1 (falling 1→0) input induces a negative (positive) supply current (as shown in the figure). POI-(1) also exhibits many curves surrounding a central lobe, which are due to the set of different input slopes (*S*). A faster input transition results in a higher current amplitude.

POI-(2) At 0.3 *ns,* the clock changes to '0' and the master-latch becomes transparent (the clocked inverter, *I*, becomes transparent) and the data propagate. A rising data change induces falling voltage on node *B*. This triggers a positive supply current due to the clocked inverter's (*III*) coupling-capacitance and a charging of the slow feedback-inverter output (both are denoted by *C*). On the other hand, a falling data change induces charging of node *B*. It is clear that the current signature is different in these two cases, and results in a substantial data dependency.

POI-(3) When the clock rises (t=0.6ns), the data propagate through the second latch to the outputs *Q* and $\overline{Q}$. Rising data induce a fast charge of node *D* and falling data results in charging of node *E*, but only after a delay due to the feedback. Clearly, the current varies for different values of the load capacitances set, ΔC, provided by the evaluation setup.



(a)

(b)

(c)

(d)

FIGURE 6. ***SABL-* and*Strong-SABL FFs:*** **(a) current traces for *SABL*, (b) *SABL-FF scheme*, (c) *Strong-SABL-FF scheme*, (d) current traces for *Strong-SABL*.**

POI-(4) In POI-(4) the data change during the low phase of the clock (the first master latch is transparent). In this case, this involves a combination of mechanisms of POI-(1) and POI-(2) which are associated with the specific data change.

As expected, the C^2MOS –FF leaks substantial information on the processed data during all phases of operation.

B. SABL-FF

Fig. 6(a-b) shows the current traces and the scheme of the *SABL*-FF circuit. In what follows, we elaborate on the POIs of this circuit and emphasize their security weaknesses.

POI-(1) The first POI is associated with the case of input data change during the *precharge* state (*clock*='0') of the FF. During the *precharge* state the input transistor's drain capacitances (int_1 and int_2) are charged to '1'. A rise in the input signal leads to the injection of current to the power supply because of the gate-drain coupling-capacitances of the input n-MOSs. Falling input has the opposite effect of drawing current from the power supply. In the ideal case, the total current from the power supply sums to zero. However, in the case of imbalanced slopes (S) and arrival times of the inputs (Δt_{inv}), the total current is data dependent, as can be seen clearly in the figure.

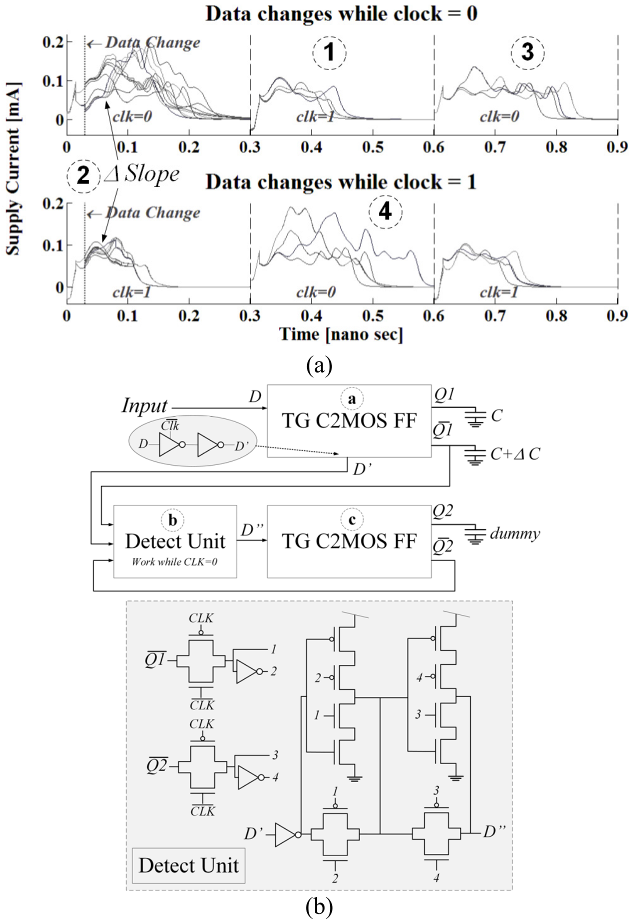
POI-(2) The second POI refers to input changes during the evaluation state (clock='1'). In this case, int_1 and int_2, which were *precharged* during the preceding *precharge* state, are already stable in one of the states ({0,1} or {1,0}). If the inputs change, the final-state of int_1 and int_2 will be similar to the current state. Note that the cross-coupled pair does not switch in this case. Ideally, the voltage changes across the input transistor's drain coupling-capacitances do not lead to current draw. However, like POI-(1), in the case of imbalanced slopes (S) and arrival times of the inputs (Δt_{inv}), the total current is data dependent.

POI-(3) Immediately after the rising edge of the clock, one of the *precharged feedback-inverters* will switch (depending on the data). If the final state is different from the final state of the previous clock cycle, the SR-latch will react (i.e. data-dependently). A very substantial current peak emerges when a switch occurs, as compared to the small current peak in the no-change case. Note that in the no-change case all curves are superimposed on each other. However, switching of the outputs will lead to a distribution of the set of curves (due to the output capacitance ***imbalance***, ΔC, which is triggered by the *SR*-latch).

POI-(4) The fourth POI relates to the case of input data change before the *precharge* state of the FF, i.e. before evaluation ends. The voltage change over the drain capacitance of transistor (a) in Fig. 6(b) causes the data dependent current. In the case where D='1' during the evaluation, the input transistors associated with D and the transistor above int_2 are open. During the *precharge,* the drain capacitance of (a) will charge through the right branch associated with D. On the other hand, when D changes from '1' to '0', the transistor associated with D will close and the transistor associated with $\overline{D}$ will open. In this case, the current will flow through the left branch. The left branch is triggered by the *precharge* of the right branch by opening the int_1 transistor. This time-consuming mechanism results in a slower response, as shown in the figure (denoted by HD=1). This causesa significant difference between the change and no-change states.

C. STRONG SABL-FF

The *Strong SABL*-FF circuit has many similarities to the *SABL*-FF circuit. Although the *Strong SABL*-FF presents a significant improvement at POI-(3),[6] where the *non-dynamic* activity is less damaging thanks to the improved *SR*-Latch design, its current signatures at POI-(1), POI-(2) and POI-(4) behave very similarly to the "classic" SABL. An additional bridging transistor of the Strong SABL-FF, denoted by (b) in Fig. 6(c), results in reduced information leakage at all POIs, as discussed in Section II(c).



(a)

(b)

FIGURE 7. ***Detect-DFF:*** **(a) current trace for *data change* while *clock=1* (upper) and*clock=0* (lower) and (b) *scheme.***

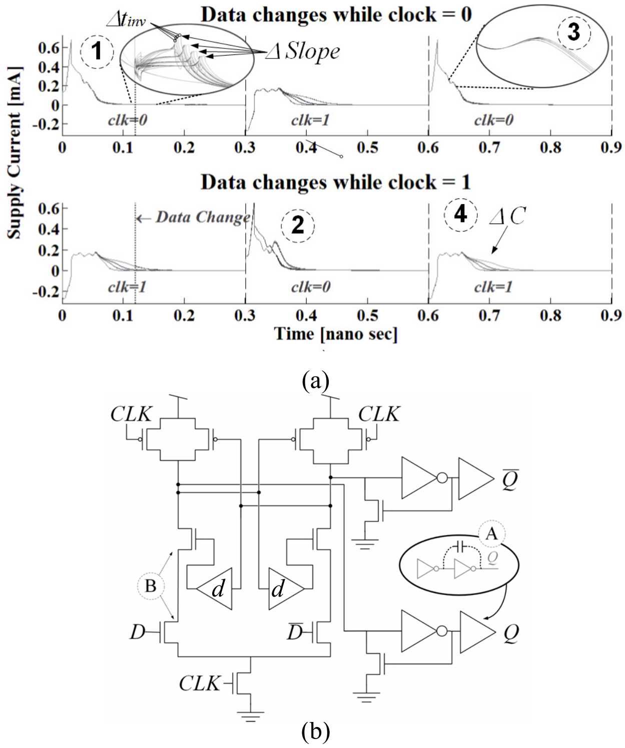
D. DETECT-DFF

In contrast to the protected FFs discussed above, the *Detect-DFF* architecture is asymmetric in structure (see Section II(a)). This asymmetry induces four different current patterns for each data transition. As shown in Fig. 7, POIs of the *Detect-DFF*:

POI-(1) In the Detect FF circuit while the clock is at '1', the second latch of the complementary TG C^2MOS FF is transparent. On one hand when HD=1 the FF denoted by (a) will switch its outputs $Q1$ and $\overline{Q1}$. In case of a load capacitance mismatch (C and $C + \Delta C$), it induces two different current patterns (for '0'→'0' and '1'→'0' switch). On the other hand, when HD=0 the FF denoted by (c) will switch its outputs, $Q2$ and $\overline{Q2}$, which are prone to additional load-capacitance mismatches. In turn, this yields two additional current patterns.

POI-(2) The *Detect-DFF* is not *dual rail* in the traditional sense since it does not incorporate *differential* inputs;

[6] The ***imbalance*** in the output capacitance, ΔC, still provides a data-dependent current



(a)

(b)

FIGURE 8. ***DelayedFB-DFF:*** **(a) current trace for *data-change* while *clock=1* (upper) and *clock=0* (lower) and (b) *scheme*.**

therefore, Δt_{inv} sensitivity does not exist. However, different input *slopes* (S) do impact the current signature. When the clock= '0' all the data changes propagate through the *Detect-Unit* differently, which induces different data dependent currents. Each of these currents exhibits slightly different variations because of the different *slopes*. When the clock='1' the *Detect-Unit* is disabled; however, the data flow through the Master-FF (denoted by (a)) and the standard C^2MOS sensitivities are visible. It is important to note that the data-dependent currents in this case (when the clock='1') are more distinct than the C^2MOS design because the data (D) signal has more transistors connected to it and one of the outputs of the Master-FF (a) is connected in a capacitance ***imbalanced*** fashion to the *Detect-Unit*.

POI-(3) While the clock = '0' the *Detect-Unit* operates. This unit is affected by the current and the previous input data because both the inputs and outputs of the FFs are connected to it. In terms of the *Detect-Unit* scheme, there are four different paths from D' to D'', each of which is triggered by different data changes. The difference between POI-(3) and POI-(4) is that in the case that D changes (or not), addition current is drawn (or not) by the path from D through D' to the *Detect-Unit*.

E. DELAYEDFB-D-FF

Fig. 8 shows the current traces and the scheme of the *DelayedFB-DFF* circuit. In this subsection, the POIs of this circuit are described.

POI-(1-2) Similar to the case of the *SABL* FF, POI-(1) and POI-(2) describe the effect of ΔS and Δt_{inv} on the *DelayedFB-DFFcurrent* during the *precharge* phase (clock='0'). These effects are due to the *coupling-capacitances* of the differential input transistors. During the *precharge* phase (POI-(2)), the capacitance between the two transistors, denoted by (B), is charged. Two distinct current waveforms can clearly be seen in POI-(2). The first relates to the case where D = '0' at the beginning of the *evaluation* phase (which implies that (B) was charged), and changes to '1' while the circuit is still in *evaluation*. In this case node (B) is discharged without affecting the output. When entering the *precharge* phase (clock change to '0'), node (B) is charged only after the added delay-buffer (denoted by d) switches to '1' (connected to the gate of the upper transistor (of B)).

The second waveform is associated with the case where D = '1' at the beginning of the evaluation phase and does not change during the entire *evaluation*. In this case, the upper transistor (of B) is already open and the node (B) charges immediately without stalling by the delay-buffer. Therefore, POI-(2) shows two distinct current patterns differentiated by whether the data were changed or not during the evaluation.

POI-(3) During *precharge* both outputs discharge. Although the internal-nodes coupling capacitances are symmetric because of the circuit symmetric structure, the differential output capacitance is asymmetric. Therefore, it induces different currents depending on which of the output nodes is discharged.

POI-(4) This POI is associated with the ΔC impact during *evaluation* while one of the outputs rises.

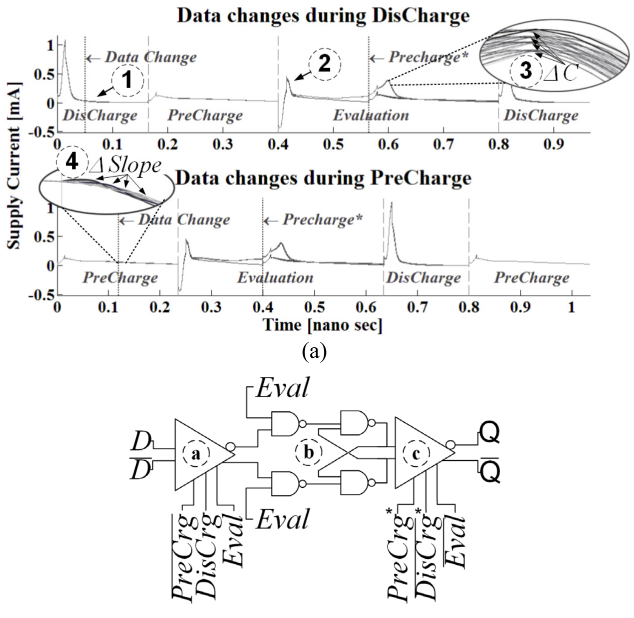
F. TDPL-FF

As discussed in Section II(e), each element of the *TDPL* FF operates in three phases which are unique to this element. The *TDPL* FF scheme is shown in Fig. 9(b). The input *TDPL* inverter (a) operates with *precharge-evaluation-discharge* phases. The output inverter, (c), operates with a complementary *evaluation* phase and its corresponding *precharge*∗ and *discharge*∗ phases [18]–[19].

The main POIs of the *TDPL*-FF are listed below:

POI-(1) The data inputs change during the *discharge* phase. In this case the supply voltage is disconnected from the *TDPL* inverter (a). This means that the current is independent of the input *slopes* and Δt_{inv}. This feature solves the issues of coupling effects caused by changes of input data that were visible at this point in all the other FFs presented above. However, as can be seen at PIO-(4), information leakage associated with the input data change still exists: if the data change during the *precharge* phase, the supply voltage is connected and the set of slopes, S, and Δt_{inv} affect the dissipated current.

POI-(2) Similar to the *SABL* FF, the *TDPL* FF utilizes an *SR*-latch, (b), to store the data. As discussed above, the *SR*-latch reveals information through its current between the case with data change and the case without change in the data.



(a)

(b)

FIGURE 9. ***TDPL-FF:*** **(a) current trace for *data-change* while *Discharge* (upper) and *Precharge* (lower) and (b) *scheme*.**

POI-(3) During the *precharge*∗ of the inverter (c), the output are charged and affected by ΔC, leading to information leakage.

VI. SECURITY ANALYSIS - METRICS EVALUATION

In this section, the secured-FFs are compared using the metrics described in Section IV. The *NED*, *NSD* and *NV* were calculated for all three grouping methodologies. For example, in Fig. 6(a) that shows the POI-(3) of the SABL architecture, the *HD* grouping corresponds to cases where the difference between data change and no change was significant. The *State* grouping indicates that for the *detect DFF* (example POI-(4) in Fig. 7(a)) the current is unique for each input transition.

Fig. 10 depicts three equipotential radar-plots for each metric. Each axis (corner) represents one of the three groupings. The smaller the values become (are closer to the origin) the more the security increases and the less information is captured. Table II summarizes the results where for each metric for all groupings (one triangle curve in the plots) the worst case (*Max*) *Max* value is listed. The grouping that has the maximal value is indeed the best tactic for an attacker.

The C^2MOS FF emerged as more sensitive than all the other candidates for almost all metrics (Fig. 10). The *Detect-DFF,* which was shown above to be highly sensitive to the *State* analysis, exhibited relatively high *State* sensitivity in the *NV* metric, almost reaching the level of C^2MOS FF sensitivity. As expected, FFs that utilize an SR-Latch (*i.e.* non-*differential*) showed high *HD* and *State* metric sensitivities compared to their fully-differential counterparts (*e.g. DelayedFB-DFF*).

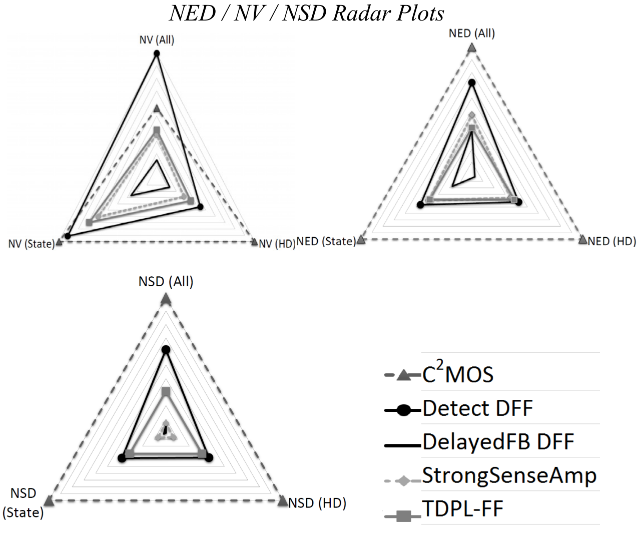


FIGURE 10. **Radar plots.**

TABLE 2. **Metric comparisons among FF's.**

FF Architecture	NED	NSD	NV
	MAX	MAX	MAX
C²MOS	1 (*state, HD, all*)	1 (*state, HD, all*)	1 (*state, HD*)
Detect DFF	0.723 (all)	0.616 (all)	1 (all)
TDPL	0.381 (state)	0.31 (state)	0.691 (state)
Strong SABL	0. 471(all)	0.073 (state)	0.310 (state)
DelayedFB DFF	0.349 (state)	0.05 (*state, HD, all*)	0.264 (state)

Max represent the value of the most sensitive metric.

For asymmetric transistor-level architectures such as the *Detect-DFF* and C^2MOS, each input change concludes in a unique current pattern. Therefore, these stand out in the *NV State* analysis shown in Fig. 10. Crucially, the *Detect-DFF* is designed to consume the same amount of energy regardless of the data processed. The *NED* and *NSD* metrics thus distinguish *Detect-DFF* much more poorly than the *NV* metric as shown in Fig. 10.

Note that the *State* results only exceed the *HD* results in cases where the current leaks state dependent information, as shown for the *Detect-DFF*, *Strong-SABL* and *TDPL-FF*s.

Generally, the *TDPL* emerged as less secure than the *Strong-SABL*. This can be attributed to the use of a non-secured (non-dynamic) *SR-Latch* (as discussed in section IV(3)).

Although the *Detect-DFF* leaks more information than the other designs, it is the only FF that is standard CMOS design-compatible and does not require a dual rail I/O (or dual rail coding).

VII. SECURITY ANALYSIS – IMMUNITY TO POWER ATTACKS

To validate the first-order information leakage observations (Section IV) and the proposed evaluation metric results (Section VI) in this section, the model-based CPA

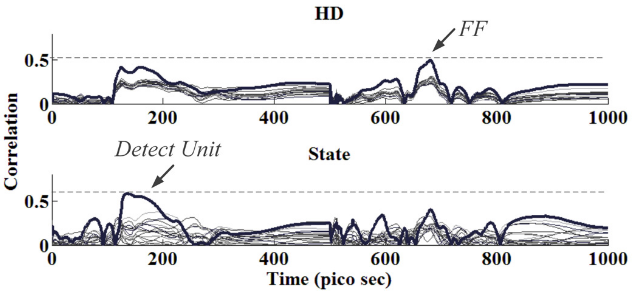


FIGURE 11. ***DelayedFB-DFF Correlation versus Time.***

attacks results are shown. Each of these attacks was run with a different current model that used information from the gate-level characterization (and grouping). This was done to show that correct use of the *State* and *HD* dependent information obtained from a gate level examination can increase the module level attack success ratio. In some ways CPA attacks that are updated with different *State* weights are similar to template attack scenarios where the current of each state of a module is templated [3]. However, unlike *template-attacks* these templates do not require special knowledge or an already cracked device, but merely a characterization of the standard cell library primitives (FFs).

To perform these attacks, a simplified module of a 4-bit *Add_Key_SBOX* DUT was constructed based on the 4-bit SBOX discussed in [27] and [28]. Four-bit input plaintext (d) was XORed with a 4-bit key, followed by an SBOX. The output was sampled by a group of four Flip-Flops which was attacked.

All possible 16×16 input transitions were injected into the design. The currents were divided into groups. The standard-*CPA* attack procedure was adjusted to maximize the attack success rate by taking into account the characteristics of the FFs according to the theoretical analysis in the previous section. That is, we used the radar-plots from the previous section to allocate the type of grouping which would provide information about the secret key better.

The three radar plot analysis of the instantaneous current provides more information than an averaging analysis. Therefore, the attacks were based on the maximal correlation over the whole clock period (intra-cycle *instantaneous* attack).

The correlation values computed for the CPA attacks are shown in Fig. 11. For the Detect-DFF there were 16 curves in the plot, each corresponding to a different key. The correlation values indicate the *instantaneous* correlation between the hypothesized current and the measured current. The correct hypothesis appears as the bold black curve and all other hypotheses are in light gray. The upper plot was derived from a CPA conducted with an *HD*-based current hypothesis model and the lower plot was derived with the modeled *State*-based current hypothesis. It shows that an attack with the *HD* model provides substantial information around 650 *ps* which is associated with the C^2MOS embedded FFs. An attack with the *State*-based model provides substantial information around 150 *ps* which is associated with the *State*-sensitive *Detect* unit. Similar temporal sensitivities emerged for the other designs.

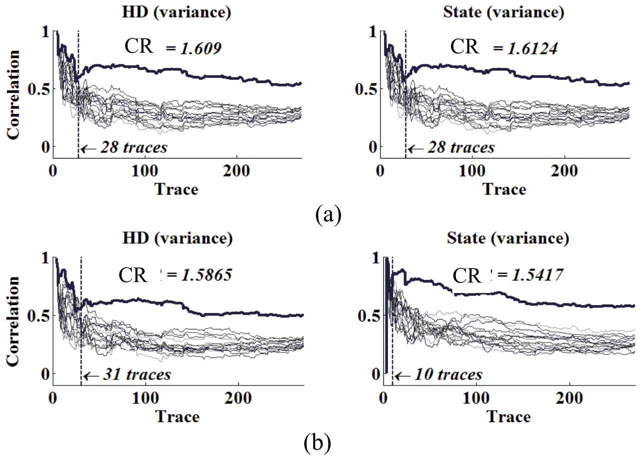


FIGURE 12. **Correlation vs. # of Traces: (a)** ***Strong SABL*** **and (b)** ***DelayedFB-DFF.***

TABLE 3. **DPA attack results.**

FF Architecture	HD CR	HD @#TRACES	STATE CR	STATE @#TRACES
C^2MOS	1.6489	4	1.9169	4
Detect DFF	1.5865	31	1.5417	10
DelayedFB-DFF	< 1	270	1.433	12
Strong SABL	1.609	28	1.6124	28
TDPL	1.6853	6	1.6853	6

After the examination of correlation *vs.* time, the *relative correlation ratio, CR*,[7] was derived as a function of the number of traces (samples) collected, as shown in Fig. 12. Clearly, a *CR* larger than 1 implies a successful attack. The figure shows two examples: a circuit embedded with *Strong-SABL* FFs and with a *Detect-DFF* (Fig 12(a) and (b), respectively). In Fig. 12(a) the *CR* is plotted for *HD* and *State* based models (left and right). It shows that the *CR*s crosses the $CR=1$ points with as few as 28 current traces and the maximum *CR* values are quite close. This is reasonable since the *Strong-SABL* devices show *HD* dominated leakage and the *State* analysis does not provide substantial additional information. In contrast, the *Detect-FF* (Fig. 12(b)) shows more *State* dependent information which is manifested in the fact that the *CR* crosses 1 with as few as 10 traces compared to 31 with the *HD* model.

Table III summarizes the maximum *CR* and the crossing point of $CR=1$ for all designs with the *HD* and *State* based hypotheses. Clearly, the C^2MOS was the most sensitive design whereas the *DelayedFB-DFF* design exhibited the most secured characteristics since it was not attackable with the *HD* model and had the smallest *CR* and smaller correlation values with the *State* model.

[7] The *CR* is defined by the maximum correlation (in time) of the correct key divided by the maximum correlation of the second best key [28], [29].

VIII. CONCLUSION

Sequential elements dominate the information leakage of synchronous hardware systems. Governed by a global clock signal they make it feasible to synchronize measurements, which is the required preliminary for statistical side-channel-analysis attacks. This manuscript presented a unified analysis framework and a comprehensive comparison of known secure Flip-Flop circuits. An in-depth investigation on device level information leakage from these FFs was provided, supplemented by important insights. In addition, several evaluation metrics were proposed to quantify these elements' security. Simulated power analysis attacks are discussed, empowered by information evaluated by the proposed metrics at the gate-level and show that more information at the module-level can be exploited.

REFERENCES

[1] Y. Zhou and D. Feng. (2005). "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing." Cryptol. ePrint Arch. Tech. Rep. 2005/388. [Online]. Available: http://eprint.iacr.org/

[2] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[3] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. New York, NY, USA: Springer, 2007.

[4] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems—CHES*, M. Joye and J.-J. Quisquater, Eds. Berlin, Germany: Springer, 2004, pp. 16–29.

[5] D. M. Chapiro, "Globally-asynchronous locally-synchronous systems," Dept. Comput. Sci. Stanford Univ. Stanford, CA, USA, Tech. Rep. STAN-CS-84-1026, Oct. 1984.

[6] J. Muttersbach, T. Villiger, and W. Fichtner, "Practical design of globally-asynchronous locally-synchronous systems," in *Proc. 6th Int. Symp. Adv. Res. Asynchron. Circuits Syst. (ASYNC)*, 2000, pp. 52–59.

[7] M. Krstic, E. Grass, C. Stahl, and M. Piz, "System integration by request-driven GALS design," *IEE Proc.-Comput. Digit. Techn.*, vol. 153, no. 5, pp. 362–372, Sep. 2006.

[8] A. Moradi *et al.* (2008). "Information leakage of flip-flops in DPA-resistant logic styles." IACR Cryptol. EPrint Arch. Tech. Rep. 2008-188. [Online]. Available: http://eprint.iacr.org/

[9] V. Stojanovic and V. G. Oklobdzija, "Comparative analysis of master-slave latches and flip-flops for high-performance and low-power systems," *IEEE J. Solid-State Circuits*, vol. 34, no. 4, pp. 536–548, Apr. 1999.

[10] D. Markovic, B. Nikolic, and R. Brodersen, "Analysis and design of low-energy flip-flops," in *Proc. Int. Symp. Low power Electron. Design*, 2001, pp. 52–55.

[11] M. Alioto, E. Consoli, and G. Palumbo, "Analysis and comparison in the energy-delay-area domain of nanometer CMOS flip-flops: Part I—Methodology and design strategies," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 19, no. 5, pp. 725–736, May 2011.

[12] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. 28th Eur. Solid-State Circuits Conf. (ESSCIRC)*, 2002, pp. 403–406.

[13] B. Nikolic, V. G. Oklobdzija, V. Stojanovic, W. Jia, J. K.-S. Chiu, and M. M.-T. Leung, "Improved sense-amplifier-based flip-flop: Design and measurements," *IEEE J. Solid-State Circuits*, vol. 35, no. 6, pp. 876–884, Jun. 2000.

[14] B. Nikolic, V. Stojanovic, V. G. Oklobdzija, W. Jia, J. Chiu, and M. Leung, "Sense amplifier-based flip-flop," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 1999, pp. 282–283.

[15] A. G. M. Strollo, D. De Caro, E. Napoli, and N. Petra, "A novel high-speed sense-amplifier-based flip-flop," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 11, pp. 1266–1274, Nov. 2005.

[16] B. Vaquie, S. Tiran, and P. Maurine, "Secure D flip-flop against side channel attacks," *IET Circuits Devices Syst.*, vol. 6, no. 5, pp. 347–354, Sep. 2012.

[17] C. Amir and G. S. Yee, "Dual rail dynamic flip-flop with single evaluation path," U.S. Patent 6 265 923 B1, Jul. 24, 2001.

[18] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Proc. Int. Workshop Cryptogr. Hardw. Embedded Syst.*, 2006, pp. 232–241.

[19] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "A flip-flop for the DPA resistant three-phase dual-rail pre-charge logic family," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 11, pp. 2128–2132, Nov. 2012.

[20] J. M. Rabaey, A. P. Chandrakasan, and B. Nikolic, *Digital Integrated Circuits*, vol. 2. Englewood Cliffs, NJ, USA: Prentice-Hall, 2002.

[21] N. F. Goncalves and H. D. Man, "NORA: A racefree dynamic CMOS technique for pipelined logic structures," *IEEE J. Solid-State Circuits*, vol. SSC-18, no. 3, pp. 261–266, Jun. 1983.

[22] D. Harris and M. A. Horowitz, "Skew-tolerant domino circuits," *IEEE J. Solid-State Circuits*, vol. 32, no. 11, pp. 1702–1711, Nov. 1997.

[23] I. Levi and A. Fish, "Dual mode logic-Design for energy efficiency and high performance," *IEEE Access*, vol. 1, pp. 258–265, 2013.

[24] I. Levi, A. Belenky, and A. Fish, "Logical Effort for CMOS-Based Dual Mode Logic Gates," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 22, no. 5, pp. 1042–1053, May 2014.

[25] F. Macé, F.-X. Standaert, and J.-J. Quisquater, "Information theoretic evaluation of side-channel resistant logic styles," in *Proc. Int. Workshop Cryptogr. Hardw. Embedded Syst.*, 2007, pp. 427–442.

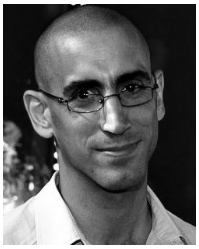
[26] B. Gierlichs, K. Lemke-Rust, and C. Paar, "Templates vs. Stochastic methods," in *Proc. Int. Workshop Cryptogr. Hardw. Embedded Syst.*, 2006, pp. 15–29.

[27] I. Levi, O. Keren, and A. Fish, "Data-dependent delays as a barrier against power attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 8, pp. 2069–2078, Aug. 2015.

[28] I. Levi, A. Fish, and O. Keren, "CPA secured data-dependent delay-assignment methodology," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 25, no. 2, pp. 608–620, Feb. 2016.

[29] M. Alioto, S. Bongiovanni, M. Djukanovic, G. Scotti, and A. Trifiletti, "Effectiveness of leakage power analysis attacks on DPA-resistant logic styles under process variations," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 2, pp. 429–442, Feb. 2014.

[30] J. Shen, L. Geng, and F. Zhang, "Dynamic current mode logic based flip-flop design for robust and low-power security integrated circuits," *Electron. Lett.*, vol. 53, no. 18, pp. 1236–1238, Aug. 2017.



ITAMAR LEVI received the B.Sc. and M.Sc. degrees in electrical and computer engineering from Ben-Gurion University, Israel, in 2012 and 2013, respectively. He is currently pursuing the Ph.D. degree in electrical engineering at Bar-Ilan University.

NETANEL MILLER received the B.Sc degree in electrical engineering from Bar-Ilan University in 2016. He is currently a Design and Verification Engineer with Texas Instruments Israel and specializes in Wi-Fi IOT protocols.

ELAD AVNI received the B.Sc. degree in electrical engineering from Bar-Ilan University in 2016. His current research and interests are in communication systems.

OSNAT KEREN received the M.Sc. degree in electrical engineering from the Technion-Israeli Institute of Technology in 1988 and the Ph.D. degree from Tel-Aviv University in 1999. Since 2004, she has been with the Faculty of Engineering, Bar-Ilan University, Israel.

ALEXANDER FISH received the B.Sc. degree in electrical engineering from the Technion, Israel Institute of Technology, Haifa, Israel, in 1999, and the M.Sc. and Ph.D. *(summa cum laude)* degrees from Ben-Gurion University, Israel, in 2002 and 2006, respectively. He has been with the Faculty of Engineering, Bar-Ilan University, Israel, since 2013.