applied sciences

MDPI

Article

Balancing the Leakage Currents in Nanometer CMOS Logic—A Challenging Goal

Bijan Fadaeinia *, Thorben Moos and Amir Moradi

Horst Görtz Institute for IT-Security, Ruhr University Bochum, 44801 Bochum, Germany; thorben.moos@rub.de (T.M.); amir.moradi@rub.de (A.M.)
* Correspondence: bijan.fadaeinia@rub.de

Abstract: The imbalance of the currents leaked by CMOS standard cells when different logic values are applied to their inputs can be exploited as a side channel to recover the secrets of cryptographic implementations. Traditional side-channel countermeasures, primarily designed to thwart the dynamic leakage behavior, were shown to be much less powerful against this static threat. Thus, a special protection mechanism called Balanced Static Power Logic (BSPL) has been proposed very recently. Essentially, fundamental standard cells are re-designed to balance their drain-source leakage current independent of the given input. In this work, we analyze the BSPL concept in more detail and reveal several design issues that limit its effectiveness as a universal logic library. Although balancing drain-source currents remains a valid approach even in more advanced technology generations, we show that it is conceptually insufficient to achieve a fully data-independent leakage behavior in smaller geometries. Instead, we suggest an alternative approach, so-called improved BSPL (iBSPL). To evaluate the proposed method, we use information theoretic analysis. As an attack strategy, we have chosen Moments-Correlating DPA (MCDPA), since this analysis technique does not depend on a particular leakage model and allows a fair comparison. Through these evaluation methods, we show iBSPL demands fewer resources and delivers better balance in the ideal case as well as in the presence of process variations.

Keywords: side-channel analysis; static power consumption; current leakage; hiding

Citation: Fadaeinia, B.; Moos, T.; Moradi, A. Balancing the Leakage Currents in Nanometer CMOS Logic—A Challenging Goal. *Appl. Sci.* **2021**, *11*, 7143. https://doi.org/10.3390/app11157143

Academic Editors: Guy Gogniat, Vianney Lapotre and Maria Mushtaq

Received: 21 June 2021
Accepted: 30 July 2021
Published: 2 August 2021

1. Introduction

CMOS standard cells in nanometer-scaled technology generations conduct a measurable leakage current whose magnitude depends on the logic values at their respective inputs and outputs [1]. Such an unintended relation between internal values and externally measurable characteristics is often called a side channel and can endanger the secrecy of computation. Over the last two decades, side-channel analysis (SCA) has become a serious threat for security-enabled devices that are supposed to operate in a hostile environment. It is well-known that intermediate values of cryptographic operations can be discovered through SCA attacks to disclose secret data or bypass authentication mechanisms [2]. Although other physical side channels have drawn more attention in the past, especially the dynamic power consumption [3] and electromagnetic radiation [4] of circuits, it can be observed that the static power side channel is progressively catching up. This is primarily due to its emergence in advanced semiconductor technologies. Although the dynamic power consumption per logic operation is reduced when capacitances and supply voltages decrease in newer IC generations, the static leakage per logic unit grows due to lower threshold voltages, shorter channel lengths and thinner gate oxides [5]. Thus, the static power side channel is becoming a more and more relevant security threat in practice.

The first reports describing successful attacks on cryptographic implementations via the static power side channel have been based on simulation results [1,5–9]. It remained uncertain, however, whether the small data-dependent differences in the leakage currents

could be captured in sufficiently high quality to perform such attacks in real world experiments. Hence, several practical evaluations has been conducted on the subject [10–17]. It was not only confirmed that those attacks are indeed feasible, but also that this source of information leakage can become the most informative side channel in certain scenarios. In detail, it was shown that the effectiveness of static power attacks can be increased exponentially by manipulating the operating conditions of devices [14,16]. Previous works also demonstrated that common side-channel countermeasures against dynamic leakage behavior are less effective against its static counterpart [8,10,12,16,17]. For instance, due to a possibility to limit the noise in static power measurements, adversaries can exploit higher-order leakages of masked implementations with a lower data complexity [11,12,16]. The general consensus of all cited works is that static power attacks are indeed a real threat and that dedicated countermeasures must be developed to prevent this side channel from affecting the security of cryptographic circuits in advanced semiconductor technologies.

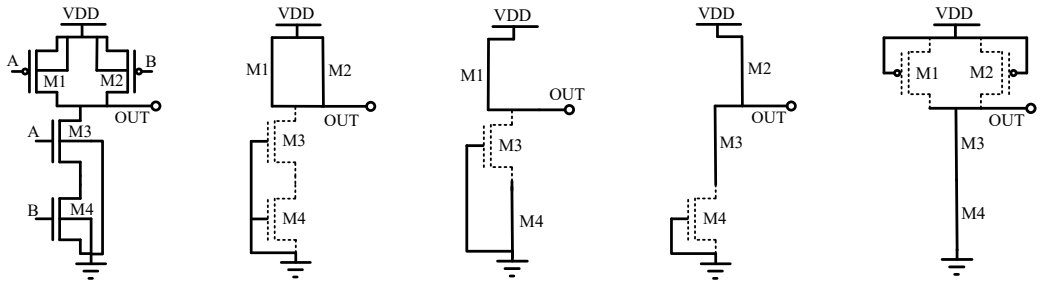
Related Work. In recent years, first potential countermeasures against static power side-channel analysis (SPSCA) have been investigated [18–26]. Similar to the early situation in the field of DPA countermeasures, most of these approaches fall into the hiding category [2] and can be split into two major groups, randomization [18,23–25] and equalization [19–22,26,27]. Randomization approaches aim to reduce the signal-to-noise ratio (SNR) by generating additional noise to bury the signal in (either on-demand or on a constant basis). This is done, for example, by dedicated ring oscillator circuits [18]. Equalization approaches aim to reduce the data dependency of a circuit's dissipation to decrease the exploitable signal. The latter are also known as balancing techniques and come in different flavors. Some are based on conventional standard cells [20]; others require custom cell design [22,26,27]. Some are specifically targeting Hamming weight dependencies [19,21]; others attempt to generally reduce the current variations depending on the input [20,22,26,27]. Although most of the previously listed works only aim at reducing the data dependency to some extent, BSPL [27], or rather *Balanced Static Power Logic* , is the first attempt to fully remove the imbalance by design. Although this succeeds up to a negligible error for a rather outdated technology node, namely 180 nm, we show in this work that the same approach fails to deliver equally promising results in smaller geometries, such as 65 nm and 40 nm. Thus, we develop and introduce an alternative approach that delivers better balance than BSPL in smaller feature sizes at a lower cost.

Our Contribution. As a first step we analyze the BSPL approach presented in [27] and identify several potential issues in its design. Then we use simulations in 65 nm and 40 nm CMOS technology to investigate whether the principles behind BSPL translate to smaller geometries without suffering from a loss of balance due to the different leakage behavior. After concluding negatively in this regard, we determine the cause for such imbalances. Interestingly, we find that primarily leakage currents through the gate insulator of transistors which are switched on by their gate voltage are responsible for this observation. We argue that it is costly, in terms of area and energy, to balance all sources of data-dependent leakage in nanometer CMOS technologies via a generic cell structure. Furthermore, such an approach would suffer from the presence of process variations more severely due to its increased size per gate. Hence, we take a different path and propose an alternative to BSPL that is not generic but technology-specific and thus able to deliver better security at a lower cost. We call our new technique *improved Balanced Static Power Logic (iBSPL)* and compare it to classic CMOS logic as well as BSPL gates. With respect to the comparison metrics we choose the same approach as [27] and present mutual information results between applied inputs and leakage currents of our custom gates. Our results confirm that a lower noise level is required to hide the data dependency exhibited by our iBSPL gates compared to BSPL and classic logic. We also analyze a cryptographic substitution box (PRESENT Sbox) synthesized either with regular CMOS gates, BSPL gates, or our technology-specific cells and demonstrate that in the ideal case as well as in the presence of intra-die process variations of different magnitudes (1%, 3%, 5%, 10%) modeled by Monte Carlo simulations, iBSPL gates are the preferable solution in all analyzed cases. Afterwards, we perform

SPSCA attacks on the different Sbox circuits, which again confirm that the highest effort is required to extract the key for our new logic cells. For completeness we also analyze the success of *dynamic* power analysis attacks on our circuits and demonstrate that unlike the BSPL approach, our new iBSPL logic gates are not any more susceptible to this kind of adversary when compared to classic gates. Although this work focuses on static leakage and introduces a power equalization technique as a countermeasure against side-channel attacks, it is worthwhile to mention that equalization schemes, e.g., iBSPL, are supposed to be combined with algorithmic masking schemes to provide security against dynamic power analysis attacks by masking and harden static power attacks by equalization.

2. Background

CMOS logic is the de-facto standard for integrated circuit design since its introduction in 1963 [28]. It has replaced former logic families such as NMOS logic due to its smaller static power dissipation. This trait is achieved by ensuring that in all CMOS logic gates at least one switched `off` transistor is present in any path between VDD and GND for each combination of input signals. As an example, consider the classical CMOS NAND gate depicted in Figure 1. For any value of its input signals A and B, at least one cut-off transistor, marked by a dotted line, is responsible for breaking the conductive path and preventing uncontrolled current flow between VDD and GND. At the time CMOS logic was invented, this design strategy was sufficient to produce cells with a negligible power consumption in stable states, as leakage currents in individual transistors were almost not present [28]. However, as technology scaling advanced into nanometer dimensions, these leakage currents kept growing and became a serious problem for device applications that require a low standby power.



(**a**) Gate structure (**b**) AB = 00 (**c**) AB = 01 (**d**) AB = 10 (**e**) AB = 11

Figure 1. Classic NAND gate, and the status of the transistors for different input values.

Another problem is caused by the fact that the magnitude of the current flowing through a CMOS cell with stable inputs is severely data-dependent. One of the dominant sources of static power consumption in transistors is drain-source leakage. With that in mind, we consider again the NAND gate in Figure 1. It is to be expected that two NMOS transistors in series, both in the off-state (AB = 00), conduct a smaller current than a single cut-off NMOS (AB = 01 and AB = 10). Similarly, two off-state PMOS in parallel connection (AB = 11) should conduct more current than the two off-state NMOS in series. This setting leads to a fundamentally data-dependent static power consumption of CMOS cells which can be exploited as a side channel [15].

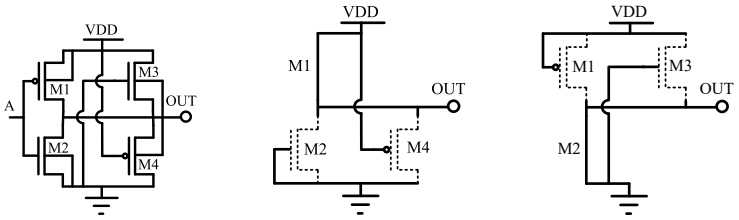
Usually, an adversary requires full control over the clock signal of the device under test (DUT) to perform such attacks. During any desired part of the cryptographic operation the clock is stopped and all I/O signals of the DUT are kept stable [14]. Then, the static power consumption, i.e., the current still flowing through the DUT, is measured for an arbitrary period of time. The length of this period can be adjusted to reduce the noise included in the measurements exponentially until a noise floor, caused by the algorithmic noise, is hit [14]. This is the main reason masking schemes can only provide reasonable resistance to such attacks when it is guaranteed that the algorithmic noise is sufficiently larger than the exploitable signal [11,12,16]. In [16] it is demonstrated that SPSCA attacks can even

be performed without control over the clock signal when the designer of the DUT fails to ensure that all sensitive data are removed from the circuit's state before entering a temporary idle state.

To perform practical SPSCA attacks, a special measurement setup is required. The main differences between measuring the static power and the dynamic power consumption of circuits are the DC nature of the static power, its comparably small magnitude, and its strong dependency on environmental influences [14]. In [14] a setup based on a conventional oscilloscope is described. It is also shown that controlling the voltage and the temperature can make devices orders of magnitude more susceptible to SPSCA [14,16].

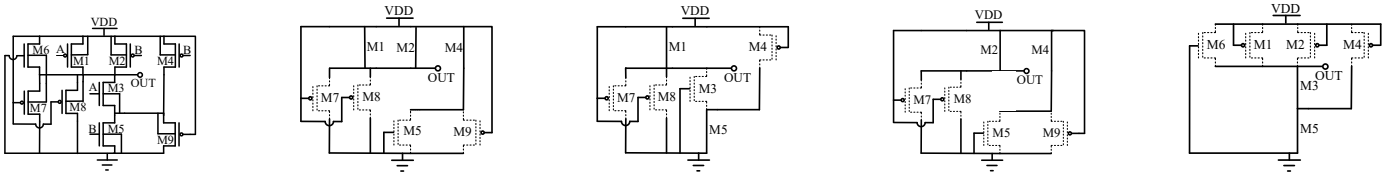
3. BSPL

Here, we briefly review the BSPL concept and point out some shortcomings in its design. The goal of BSPL [27] is to construct circuits with a constant static leakage, independent of the data being processed. As stated in Section 2, one primary origin of data-dependent leakage current is the gate's structure where a different number of cut-off transistors with a different topology are present between VDD and GND. Hence, in BSPL, alternative versions of standard logic cells were developed in such a way that a fixed number of cut-off transistors (from the same type PMOS/NMOS) are placed in the same arrangement between VDD and GND, independent of the given input. This strategy is sufficient to provide optimal data-independence with respect to drain-source leakage. Under the assumption that drain-source leakage is the dominating component in the overall static power consumption, the resulting cells should not show a significant data dependency unless process variations are introduced. The resulting structures of BSPL gates (here NAND, NOR, NOT, and XOR) are shown in Figures 2–4 and 6 respectively.



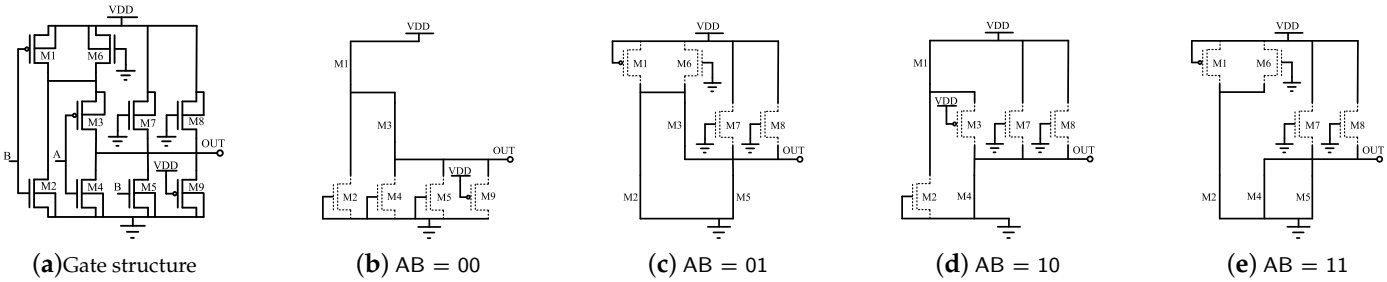
(**a**) Gate structure (**b**) A = 0 (**c**) A = 1

Figure 2. BSPL NOT gate, and the status of the transistors for different inputs.



(**a**) Gate structure (**b**) AB = 00 (**c**) AB = 01 (**d**) AB = 10 (**e**) AB = 11

Figure 3. BSPL NAND gate, and the status of the transistors for different input values.



(**a**)Gate structure (**b**) AB = 00 (**c**) AB = 01 (**d**) AB = 10 (**e**) AB = 11

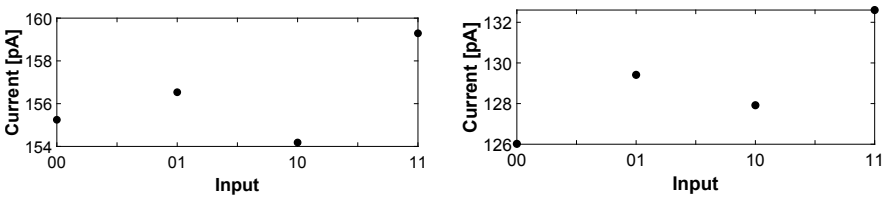
Figure 4. BSPL NOR gate, and the status of the transistors for different input values.

3.1. General Design Issues in BSPL

Although the goal of balancing drain-source currents is indeed achieved in BSPL cells, we point out that these gates suffer from several shortcomings with respect to their usability as universal CMOS standard cells. First, the simulation results reported in [27] have been acquired while sizing both NMOS and PMOS transistors identically. In reality, however, it is required to adapt the size of the transistors in a standard cell to ensure that the rise and fall times of its output signal are balanced. Typically, the width of a PMOS transistor needs to be significantly larger than that of an NMOS transistor in the same cell (typically by a factor of 2.5 or 3). The reason for this disparity is the difference between electron mobility and hole mobility (factor of about $\times 2.7$). Although this deficit is fairly easy to correct in the design of the BSPL cells and should not significantly influence their balancing capability, it certainly impacts the area, latency and energy overhead. Thus, to provide a fair comparison, we have adapted the transistor sizes to achieve balanced rise and fall times in all our simulation results presented in Section 5. A second issue of the BSPL design strategy becomes apparent when noting the bulk connections in Figures 2–4 and 6. Traditional bulk CMOS processes are built on a p-type wafer. Thus, n-type field effect transistors can be built directly in the substrate, so that all NMOS devices share a common bulk voltage. Yet, in the BSPL design it is required to realize NMOS (and PMOS) devices with different bulk voltages in the same gate, which severely complicates the layout process and increases the design area. The third issue originates from the old technology, which BSPL is designed based on it. In larger technologies (old technologies), gate leakage is meaningfully smaller than subthreshold leakage. Hence, the spice simulation using the 180 nm technology file does not show any reasonable leakage through gates and bulks. Meantime, for sub-100 nm technologies, gate leakage increases exponentially with decreasing the oxide thickness [29]. For oxide thickness less than 3 nm due to gate tunneling, the gate leakage current reaches the order of subthreshold leakage [30]. Consequently, by moving to smaller technologies, these leakages are obvious and degrade the balance of the design. Finally, the type of XOR gate that is chosen in BSPL is based on pass-transistor logic which is typically not used in standard cell design due to its lack of drive strength and the large transistor sizes.

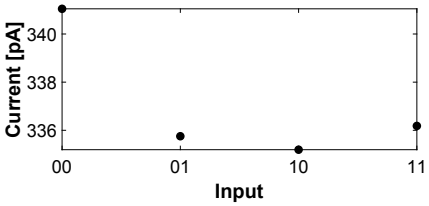
3.2. BSPL in Smaller Geometries

Despite the general design issues pointed out above we want to analyze how effectively BSPL gates balance the leakage currents in smaller geometries, compared to the initially analyzed 180 nm library in [27]. Therefore, we have simulated the leakage currents of BSPL NAND and NOR gates exemplarily in our 65 nm and 40 nm technologies. The results can be seen in Figure 5.

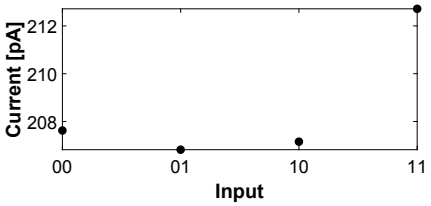


(**a**) BSPL NAND in 65 nm

(**b**) BSPL NOR in 65 nm



(**c**) BSPL NAND in 40 nm



(**d**) BSPL NOR in 40 nm

Figure 5. Input-dependent static leakage currents in BSPL NAND and NOR gates in 65 nm and 40 nm technology.

It is obvious that the leakage currents of the gates are not constant and depend on the given input signals. This is contrary to the results reported for BSPL gates in 180 nm technology in [27]. Although the BSPL concept sufficiently balances drain-source currents such as the subthreshold leakage, it does not account for leakages through the gate insulator. In the following we detail why and how gate leakages prevent a balanced static power consumption in BSPL gates (Figure 6).

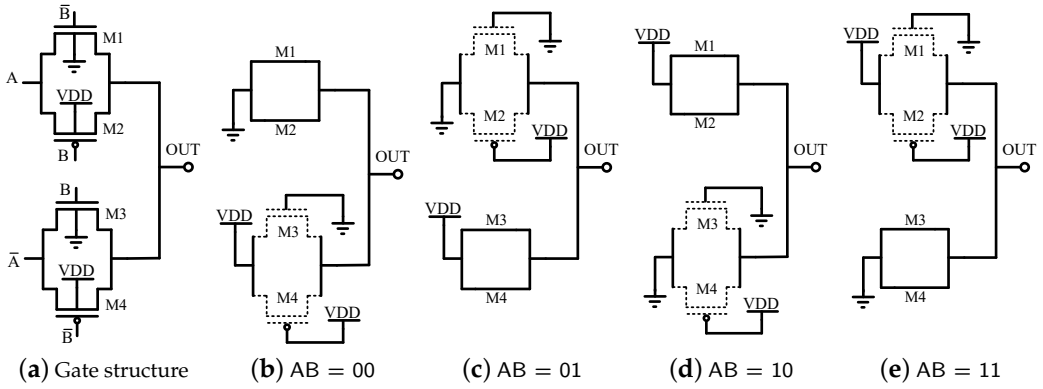


Figure 6. BSPL XOR gate, and the status of the transistors for different input values (inverters to generate $\overline{A}$ and $\overline{B}$ are not shown).

3.3. Imbalance through Gate Leakage

As an example, consider the BSPL NAND gate depicted in Figure 3. For any combination of inputs, there is a parallel connection of 3 × PMOS and 1 × NMOS which are switched `off` and not bridged (Bridged means that its source and drain terminal are connected by a low resistance path (e.g., by another transistor which is conducting) and therefore no significant potential exists between them). All remaining transistors are either switched `on`, or they are bridged. BSPL considers only the four transistors which are `off` and not bridged for its balancing concept, since neither `on`-transistors nor bridged ones are relevant contributors to drain-source leakage (Transistors which are `on` are supposed to conduct current between drain and source and therefore do not *leak* current between these terminals. Transistors which are bridged have no significant potential between drain and source and therefore do not leak a significant current between these terminals). However, gate leakage also occurs in transistors which are switched `on` or bridged, due to the potential between the gate terminal and the source (or drain) terminal. To illustrate the fact that BSPL neglects the gate leakage in its balancing strategy we consider the BSPL NAND gate in Figure 3 again. For inputs AB = 00 (Figure 3b) it can be seen that in addition to the 3 × PMOS (M7, M8, M9) and 1 × NMOS (M5) which are switched `off` and not bridged, there are 3 × PMOS which are `on` (M1, M2, M4) and 2 × NMOS (M3, M6) which are switched `off`, but bridged. In contrast, when considering the same gate for inputs AB = 11 (Figure 3e), it can be seen that again 3 × PMOS (M1, M2, M4) and 1 × NMOS (M6) are switched `off` and not bridged, while 2 × NMOS are `on` (M3, M5) and 3 × PMOS (M7, M8, M9) are switched `off`, but bridged. Clearly, only one of the three groups, namely switched `off` but not bridged, is properly balanced for all input combinations. Although the other two groups do not need to be considered when analyzing drain-source currents exclusively, they certainly play a role in determining the total gate leakage of the cell. We have determined the different transistor states for all possible inputs to the BSPL NAND gate and listed them in Table 1.

Table 1. Transistor states in a BSPL NAND gate for different inputs.

Transistor State	AB = 00	AB = 01	AB = 10	AB = 11
off + not bridged	3 × PMOS 1 × NMOS	3 × PMOS 1 × NMOS	3 × PMOS 1 × NMOS	3 × PMOS 1 × NMOS
off + bridged	2 × NMOS	1 × NMOS 2 × PMOS	2 × NMOS 1 × PMOS	3 × PMOS
on	3 × PMOS	1 × NMOS 1 × PMOS	2 × PMOS	2 × NMOS

Interestingly, we noticed that primarily leakage currents through the gate insulator of switched `on` transistors are responsible for the remaining data-dependent leakage of BSPL gates in 40 nm and 65 nm technology. We analyzed the situation for all BSPL gates (NOT, NAND, NOR, XOR) in both technologies and found that the group of `on` transistors is responsible for 85–92% of the remaining data dependency of the leakage currents, while the group of bridged transistors is responsible for only 8–15%. Hence, we conclude that it is not a viable balancing strategy in sub-100 nm technologies to only consider drain-source currents. Leakage currents through the gate insulator, particularly in switched `on` transistors, need to be considered in balancing approaches as well. This observation also shows that it is a misconception, although a common one, to consider leakage currents only for those transistors in a circuit which are switched `off`.

3.4. Repairing BSPL?

We have asked ourselves whether it is possible to repair BSPL in such a way that gate leakages are considered and balanced as well. However, we have come to the conclusion that any generic BSPL-like cell structure which balances all 3 discussed groups of transistor states properly would be very expensive. In particular, we believe that for common two-input logic functions (like NAND, NOR, XOR) the balanced gate would require at least 4 times the area of the original logic gate. Such a large structure would suffer from imbalances through process variations more severely due to the larger number of transistors. Additionally, there would be no significant advantage of a custom standard cell design, since a similar kind of balancing could also be achieved by implementing the regular CMOS standard cells 4 times and feeding each of them with one possible input combination. Hence, we believe that it is not a promising approach to extend BSPL in such a way that it accounts for all leakage sources. Instead, we introduce a different approach in the following which enables protection against SPSCA at a much lower cost.

4. Our New Strategy

In this section, we introduce our new approach, called *improved Balanced Static Power Logic (iBSPL)*. We made sure to avoid the design issues of BSPL which we have pointed out in the previous section. In particular, we have taken care that all our developed cells produce balanced rise and fall times and ensured that all transistors follow the typical bulk connections (PMOS to VDD, NMOS to GND). Furthermore, instead of using the pass-transistor XOR logic from [27] we have based our new XOR cell on a complementary gate that is commonly used in standard cells (The 12-transistor design is used for example by TSMC and ON Semiconductor (formerly AMI) as shown here: https://vlsiarch.ecen.okstate.edu/flows/MOSIS_SCMOS/latest/cadence/lib/, accessed date 25 July 2021).

Our approach essentially works like this. To convert a standard CMOS logic cell to its leakage-balanced iBSPL version we first identify which combinations of input signals cause a larger and which cause a smaller static power consumption. Then, by systematically adding always-off transistors to carefully chosen input, output or intermediate signals, we raise the static leakage caused by the input combinations which originally resulted in a smaller leakage current to the higher levels. We can exploit the HSPICE optimization feature to determine the optimal width of the added transistors so that the manual effort is comparably low. By following this procedure, we achieve logic gates whose static power

consumption is very close to constant. Of course, the approach increases the average static power consumption of the gates. However, we believe that this is the best option to keep the original logic function and the performance of the gate intact (as much as possible) while providing additional security against SPSCA attacks.

Figure 7 shows all four possible biasing states of PMOS and NMOS transistors which ensure that they are always off, but also cause a leakage current and have the standard bulk connections necessary to be included in a common standard cell (PMOS to VDD, NMOS to GND). We call these transistors *Tiny Consuming Blocks (TCBs)* in the following and use them to balance the static power consumption of CMOS logic gates. We have listed the leakage currents caused by each of the TCBs in Table 2. Those static currents are consumed when the TCBs are instantiated as shown in Figure 7 with minimum width and height in 40 nm and 65 nm CMOS technology respectively. By increasing their width, we can adapt the leakage current of each of those building blocks liberally.

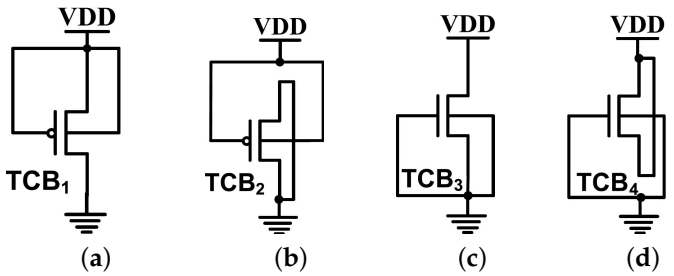


Figure 7. Tiny consuming blocks.

Table 2. Minimum currents consumed by the tiny consuming blocks.

	TCB_1	TCB_2	TCB_3	TCB_4
40 nm	22.41 pA	3.36 pA	32.77 pA	4.22 pA
65 nm	12.49 pA	2.58 pA	27.34 pA	2.56 pA

In the following we explain the procedure to convert a standard CMOS logic gate to its leakage-balanced iBSPL version step by step using the NAND gate as an example. Please note that during the explanation of the design procedure we denote the leakage current of a logic gate for a certain input combination AB by $I_{L_{AB}}$. For example, if input $AB = 00$ is given, the corresponding leakage current is denoted by $I_{L_{00}}$.

- **Step 1:** First we simulate the leakage current of a classic NAND gate for all input combinations and calculate the difference between $I_{L_{00}}$ and $I_{L_{10}}$.

$$\Delta_0 = I_{L_{00}} - I_{L_{10}} \tag{1}$$

- **Step 2:** If $\Delta_0 < 0$, we need to increase the static leakage current for $A = 0$, otherwise the current for $A = 1$. In the former case we add either TCB_1 or TCB_2, depending on the magnitude of $|\Delta_0|$, and in the latter case either TCB_3 or TCB_4 are added, again depending on the magnitude of $|\Delta_0|$. In more detail, if $|\Delta_0| < I_{TCB_1}$ or $|\Delta_0| < I_{TCB_3}$ choose TCB_2 or TCB_4 respectively, otherwise choose TCB_1 or TCB_3. It may be necessary or beneficial to add a combination of TCBs to model the complemented static power Δ_0 as accurately as possible. The optimal width and combination of the additional transistors is determined by HSPICE's optimization feature. The additional transistors are incorporated into the gate by connecting signal A to their drain terminal (and source terminal in the case of TCB_2 or TCB_4). At the end of this step, we expect $I_{L_{00}} \approxeq I_{L_{10}}$.
- **Step 3:** Next we calculate the average of the new values for $I_{L_{00}}$ and $I_{L_{10}}$.

$$Avg_{|_{B=0}} = (I_{L_{00}} + I_{L_{10}})/2 \tag{2}$$

Then we calculate difference Δ_1 as follows.

$$\Delta_1 = Avg_{|_{B=0}} - I_{L_{01}} \tag{3}$$

- **Step 4:** If $\Delta_1 < 0$, we need to increase the static leakage current for $B = 0$, otherwise the current for $B = 1$. In the former case we add either TCB_1 or TCB_2, depending on the magnitude of $|\Delta_1|$, and in the latter case either TCB_3 or TCB_4 are added, again depending on the magnitude of $|\Delta_1|$. In more detail, if $|\Delta_1| < I_{TCB_1}$ or $|\Delta_1| < I_{TCB_3}$ choose TCB_2 or TCB_4 respectively, otherwise choose TCB_1 or TCB_3. It may be necessary or beneficial to add a combination of TCBs to model the complemented static power Δ_1 as accurately as possible. The optimal width and combination of the additional transistors is determined by HSPICE's optimization feature. The additional transistors are incorporated into the gate by connecting signal B to their drain terminal (and source terminal in the case of TCB_2 or TCB_4). At the end of this step, we expect $I_{L_{00}} \approxeq I_{L_{10}} \approxeq I_{L_{01}}$, which means that the leakage current is close to constant for $OUT = 1$.
- **Step 5:** Next we calculate the average of the three input states that lead to $OUT = 1$.

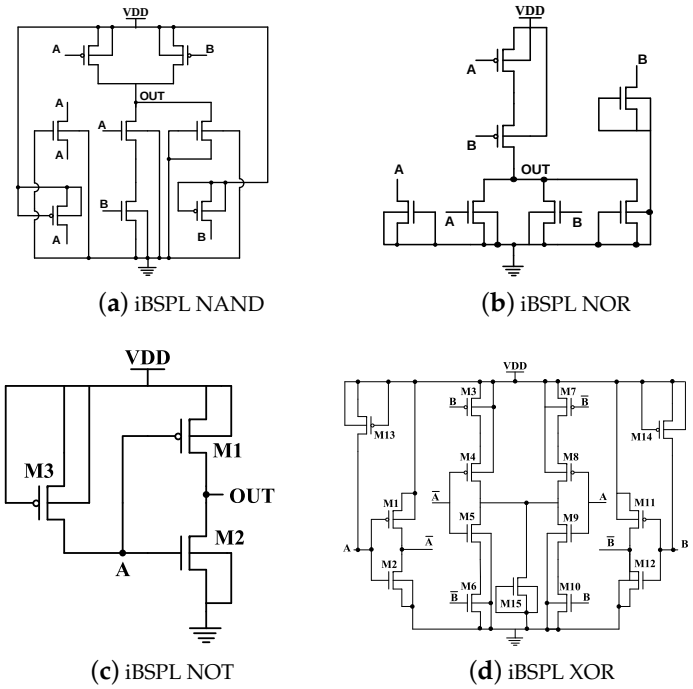
$$Avg_{|_{OUT=1}} = (I_{L_{00}} + I_{L_{10}} + I_{L01})/3 \tag{4}$$

Then we calculate the last difference Δ_2 as follows.

$$\Delta_2 = I_{L_{11}} - Avg_{|_{OUT=1}} \tag{5}$$

- **Step 6:** If $\Delta_2 < 0$, we need to increase the static leakage current for $OUT = 0$, otherwise the current for $OUT = 1$. In the former case we add either TCB_1 or TCB_2, depending on the magnitude of $|\Delta_2|$, and in the latter case either TCB_3 or TCB_4 are added, again depending on the magnitude of $|\Delta_2|$. In more detail, if $|\Delta_2| < I_{TCB_1}$ or $|\Delta_2| < I_{TCB_3}$ choose TCB_2 or TCB_4 respectively, otherwise choose TCB_1 or TCB_3. It may be necessary or beneficial to add a combination of TCBs to model the complemented static power Δ_2 as accurately as possible. The optimal width and combination of the additional transistors is determined by HSPICE's optimization feature. The additional transistors are incorporated into the gate by connecting signal OUT to their drain terminal (and source terminal in the case of TCB_2 or TCB_4). At the end of this step, we expect $I_{L_{00}} \approxeq I_{L_{10}} \approxeq I_{L_{01}} \approxeq I_{L_{11}}$, which means that the leakage current is balanced and should be almost data-independent.

The design procedure for the NOR gate is almost the same as for the NAND gate, except that $I_{L_{01}}$ and $I_{L_{11}}$ are compared in step 1, $Avg_{|_{B=1}}$ and $I_{L_{10}}$ in step 2, and $I_{L_{00}}$ and $Avg_{|_{OUT=0}}$ in step 3. Similar procedures can be applied to balance the currents leaked by NOT and XOR gates. The resulting cells are shown exemplarily for our 40 nm technology in Figure 8a–d. It is clear that when applying this approach to different process technologies, the number of transistors required for the balancing as well as their size and type, are not necessarily constant. Thus, the concrete overhead associated with iBSPL depends on the underlying process technology. We have listed the required transistor numbers, types and widths for both of our technology generations and all four different logic gates in Table 3.



(**a**) iBSPL NAND (**b**) iBSPL NOR

(**c**) iBSPL NOT (**d**) iBSPL XOR

Figure 8. iBSPL gates in 40 nm.

Table 3. Number and size of TCBs added to each gate to achieve a balanced static power consumption.

Gate	Technology	TCB_1	TCB_2	TCB_3	TCB_4
NAND	40 nm	w = 120.00	-	w = 397.15	w = 160.63
		w = 140.39	-		
	65 nm	w = 181.57	-	w= 172.99	-
		w = 228.96	-		-
NOR	40 nm	-	-	w = 172.70	-
		-	-	w = 291.94	-
	65 nm	-	-	w = 155.99	w = 3 × 360.00
		-	-	w = 127.11	w = 1209.16
XOR	40 nm	w = 2 × 271.72	-	w = 314.88	-
	65 nm	w = 3 × 152.51	w = 3 × 509.44	-	-
NOT	40 nm	w = 271.72	-	-	-
	65 nm	w = 152.51	-		-

5. Analysis Results

In this section, we analyze our newly developed iBSPL logic cells and compare them to classic CMOS logic gates as well as the BSPL cells originally proposed in [27]. Our simulations are performed by HSPICE using transistor models from two commercial nanometer process technologies, 40 nm and 65 nm. To achieve balanced rise and fall times for all analyzed logic cells we have set the width of (functional) PMOS transistors significantly larger than the width of NMOS transistors, especially when stacked, to account for the difference between electron and hole mobility, while keeping the lengths identical. As a first step we analyze the area overhead associated with balancing the leakage currents in nanometer process technologies. In that regard, we put the required transistor-only area of BSPL and iBSPL cells in relation to classic CMOS logic gates. Those results can be found in Table 4. It is obvious that the overhead associated with our new iBSPL cells is consistently lower than that of BSPL cells, with the only exception being the XOR gate. We have also measured the average power consumption for a PRESENT SBox for one clock cycle. Table 5 shows that the iBSPL circuit consumes less power in comparison to BSPL. As

previously stated, the BSPL concept neglects the fact that the pass-transistor-based XOR is not suitable for standard cell design; in iBSPL we have used a complementary XOR gate. Hence, comparing their area overheads is not much meaningful.

Table 4. Area overhead (transistor-only) of BSPL and iBSPL logic gates compared to regular CMOS standard cells.

Gate	Technology	BSPL	iBSPL
NAND	40 nm	+162%	+85%
	65 nm	+160%	+60%
NOR	40 nm	+87%	+76%
	65 nm	+87%	+66%
XOR	40 nm	±0%	+21%
	65 nm	±0%	+85%
NOT	40 nm	+100%	+56%
	65 nm	+100%	+31%

Table 5. Average power consumption for one clock cycle.

Family	Technology	Power (µW)
Classic	40 nm	2.00
	65 nm	2.92
BSPL	40 nm	2.80
	65 nm	3.26
iBSPL	40 nm	2.40
	65 nm	2.96

As a next step we analyze how much information can be extracted from the leakage of each of the balanced and unbalanced gates. In the simulation environment, the (static) power measurements are free of noise. Hence, even extremely small differences between the power consumption associated with the processing of different data values lead to successful key recovery. Therefore, the goal of a proper security evaluation in the simulation domain is to put the feasibility of attacks on the underlying circuit in relation to the noise level. In reality, the power measurements are always affected by noise originating from the measurement setup and environmental parameters. To this end, an evaluation metric based on the concept of Information Theory has been developed in [31]. It considers Gaussian-distributed noise centered to the simulated power values, and estimates the mutual information between the simulated leakage and the processed data. For a given noise standard deviation, the technique evaluates the amount of available information which can be exploited by the *worst-case* adversary, independent of the type of relationship between leakage and processed data (e.g., specific leakage models, linear/non-linear dependency, ...). Therefore, the purpose of IT analysis is to extract a curve of the mutual information over the noise standard deviation, therefore identifying the necessary noise level to fully hide the information leakage. The lower the required noise, the higher is the robustness, since the leakage can more easily (with lower noise) be hidden. Such a security evaluation has been used to assess the robustness of DPA-resistant logic styles in [32]. We have conducted this type of analysis on our new logic gates and compare them to BSPL and classic logic. The result is shown in Figures 9 and 10 for all gates in both 40 nm and 65 nm technology. To compare the results, it is important to observe which mutual information curve drops at a lower amount of noise, identifying the more robust countermeasure [31,32]. It is obvious that the iBSPL gates require the least amount of noise to hide the data dependency which indicates the highest protection against attacks.

Although in the dynamic area, load capacitances dominate the current consumption and consequently information leakage, in the case of static leakage, the leakage current is dominated by subthreshold, and gate leakages, which are also a function of various parameters such as threshold voltage, oxide thickness, transistors dimensions, supply voltage [33–35]. Naturally, process variations and layout imbalances affect any equalization countermeasures. Furthermore, layout and RC-extraction through the post-layout analysis improve the accuracy of simulations [36,37]. Ignoring such post-layout and post-production can mitigate the leakages. However, the mitigation level is undoubtedly reduced in reality (post-production), and the benefit of the countermeasure will not entirely vanish. Hence, here we just consider the impact of process variations on the ability of a worst-case (i.e., strongest possible) adversary to extract information. In this regard we have used Monte Carlo simulations to model intra-die process variations of severity levels of 1%, 3%, 5% and 10%. For every SBox circuit and every possible input value, we carried out 500 Monte Carlo simulations, performed the information theoretic analysis for a noise standard deviation σ, and took the maximum mutual information value as the representative value for the given noise level. Although the margin between iBSPL and BSPL/Classic is clearly reduced when process variations are considered, our newly developed logic cells still provide the highest level of protection against information extraction across all levels of process variations. Table 6 compares the energy (static and dynamic) and latency overhead associated with the BSPL and iBSPL versions of the PRESENT SBox. Clearly, iBSPL does not only provide the better protection, it also comes at a lower overhead in terms of energy and latency.

Table 6. Energy and latency overhead of the PRESENT SBox synthesized in BSPL and iBSPL cells compared to regular CMOS logic.

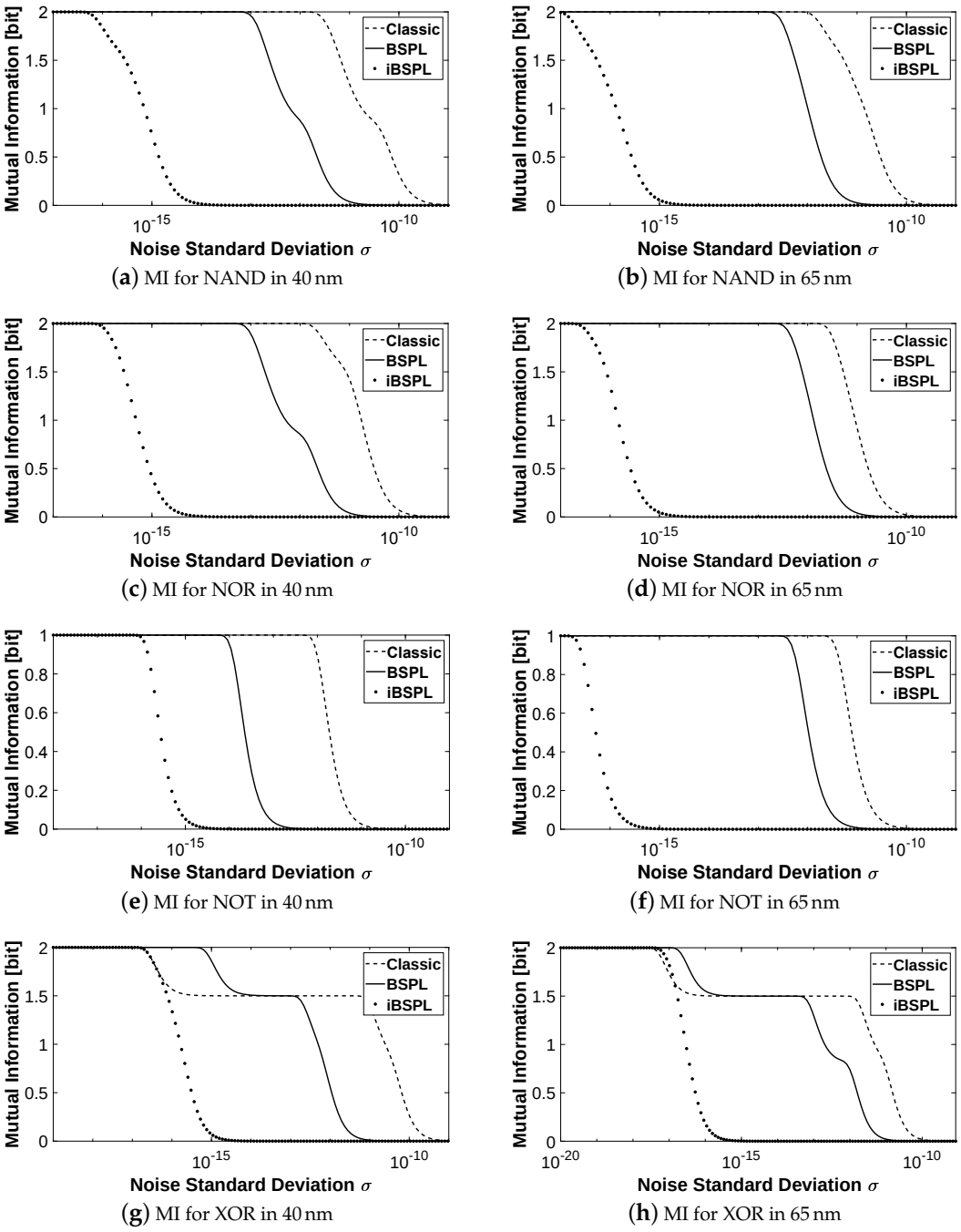
Cells	Technology	Dynamic Energy (Average)	Static Energy (Average)	Latency (Average)	Latency (Average)
BSPL	40 nm	+21.57%	+195.46%	+42.20%	+6.13%
	65 nm	+35.04%	+192.09%	+69.98%	+10.89%
iBSPL	40 nm	+10.87%	+109.65%	+13.56%	+1.65%
	65 nm	+3.86%	+88.10%	+12.92%	+0.34%

As a final comparison between classic logic, BSPL and iBSPL we consider static power and dynamic power analysis attacks on the synthesized SBox circuits. For that purpose, we have simulated the leakage current of each SBox circuit 5000 times for random inputs while adding Gaussian-distributed noise. In fact, we have repeated that process 500 times to model the influence of process variations corresponding to the given severity level. As an attack strategy we have chosen Moments-Correlating DPA (MCDPA) [38], since this analysis technique does not depend on the choice of a particular leakage model and therefore allows a fair comparison. Please note that the same attack has also been successfully applied to experimental static power side-channel measurements in [12]. Our results are shown in Figure 11 for 40 nm technology and Figure 12 for 65 nm technology. To exclude any influences of the probabilistic nature of additional noise to the traces we have used exactly the same noise distribution for classic logic, BSPL and iBSPL. Although it is clearly more difficult to recover the key difference in the case of the BSPL circuit compared to regular logic cells, the SBoxes synthesized with iBSPL cells again provide the highest level of protection in this analysis. In fact, most of the attacks are not able to isolate the correct key difference (black) from the incorrect ones (grey) using the available number of traces.

As a matter of fact, both gate leakage and subthreshold leakage are sensitive to the supply voltage and temperature. Hence, an iBSPL-based circuit should be powered through a built-in voltage regulator to prevent the attacker from exploiting the information by supply voltage manipulation. Furthermore, an internal temperature sensor should monitor the circuit temperature and put the chip in an idle mode, if its temperature exceeds

the tolerable temperature. This is essential to avoid the adversary to operate the chip at a high temperature to better exploit the information leakage.

Finally, to assess whether balancing the static power consumption in BSPL and iBSPL cells has any impact on the exploitability of their dynamic power consumption, we have performed MCDPA attacks on simulated dynamic power curves as well. The results are shown in Figure 13. Although BSPL seems to be more susceptible to such attacks, which makes sense due to the increased number of transistors switching for every input change, iBSPL seems to be not any more vulnerable than regular CMOS logic. As already discussed in [27] it makes sense to combine the static power balanced circuits with a masking scheme to provide protection against both types of power analysis adversaries, static and dynamic.



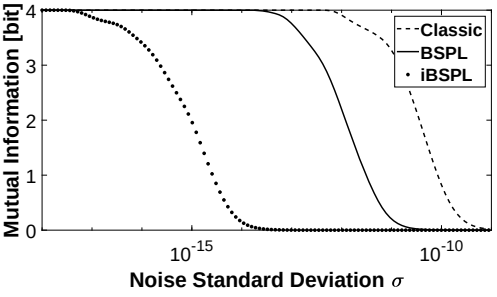
(**a**) MI for NAND in 40 nm (**b**) MI for NAND in 65 nm

(**c**) MI for NOR in 40 nm (**d**) MI for NOR in 65 nm

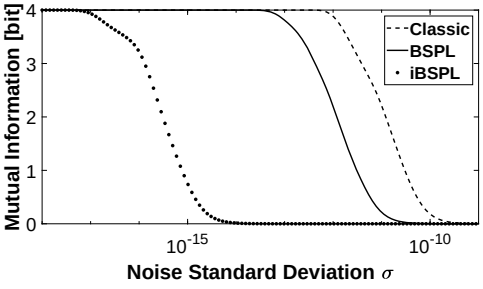
(**e**) MI for NOT in 40 nm (**f**) MI for NOT in 65 nm

(**g**) MI for XOR in 40 nm (**h**) MI for XOR in 65 nm

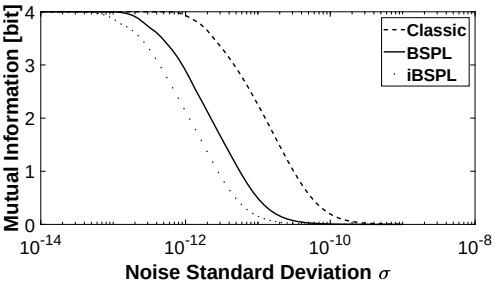
Figure 9. Information theoretic analysis of Classic, BSPL and iBSPL logic gates.



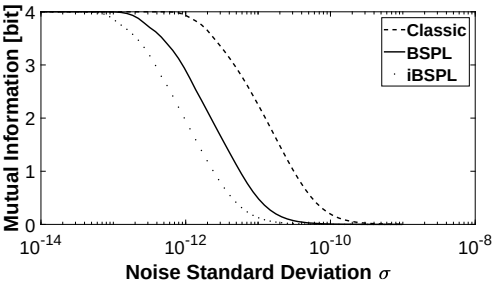
(**a**) SBox 40 nm 0%



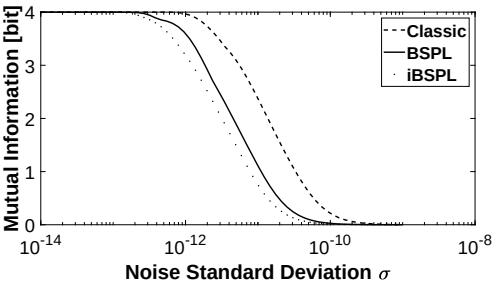
(**b**) SBox 65 nm 0%



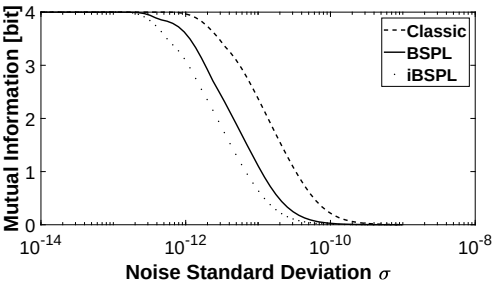
(**c**) SBox 40 nm 1%



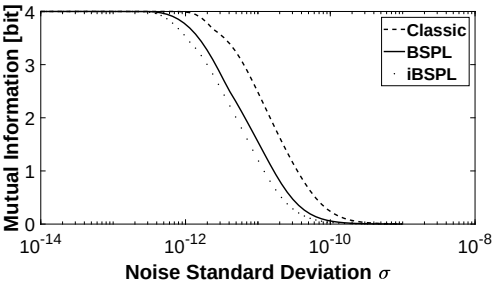
(**d**) SBox 65 nm 1%



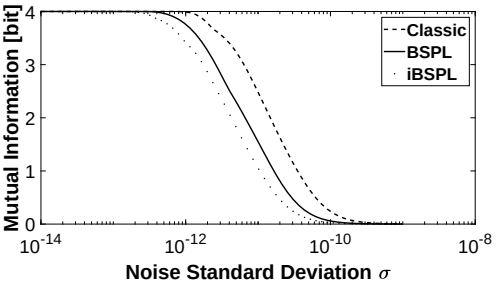
(**e**) SBox 40 nm 3%



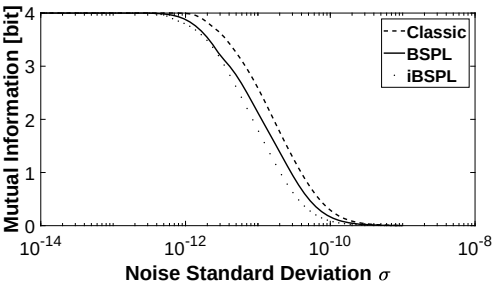
(**f**) SBox 65 nm 3%



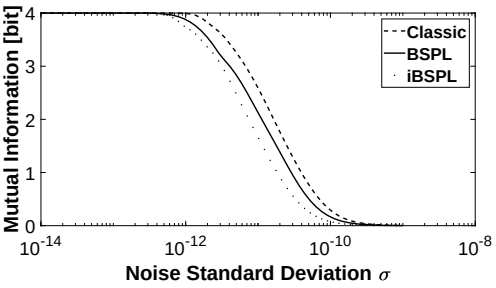
(**g**) SBox 40 nm 5%



(**h**) SBox 65 nm 5%

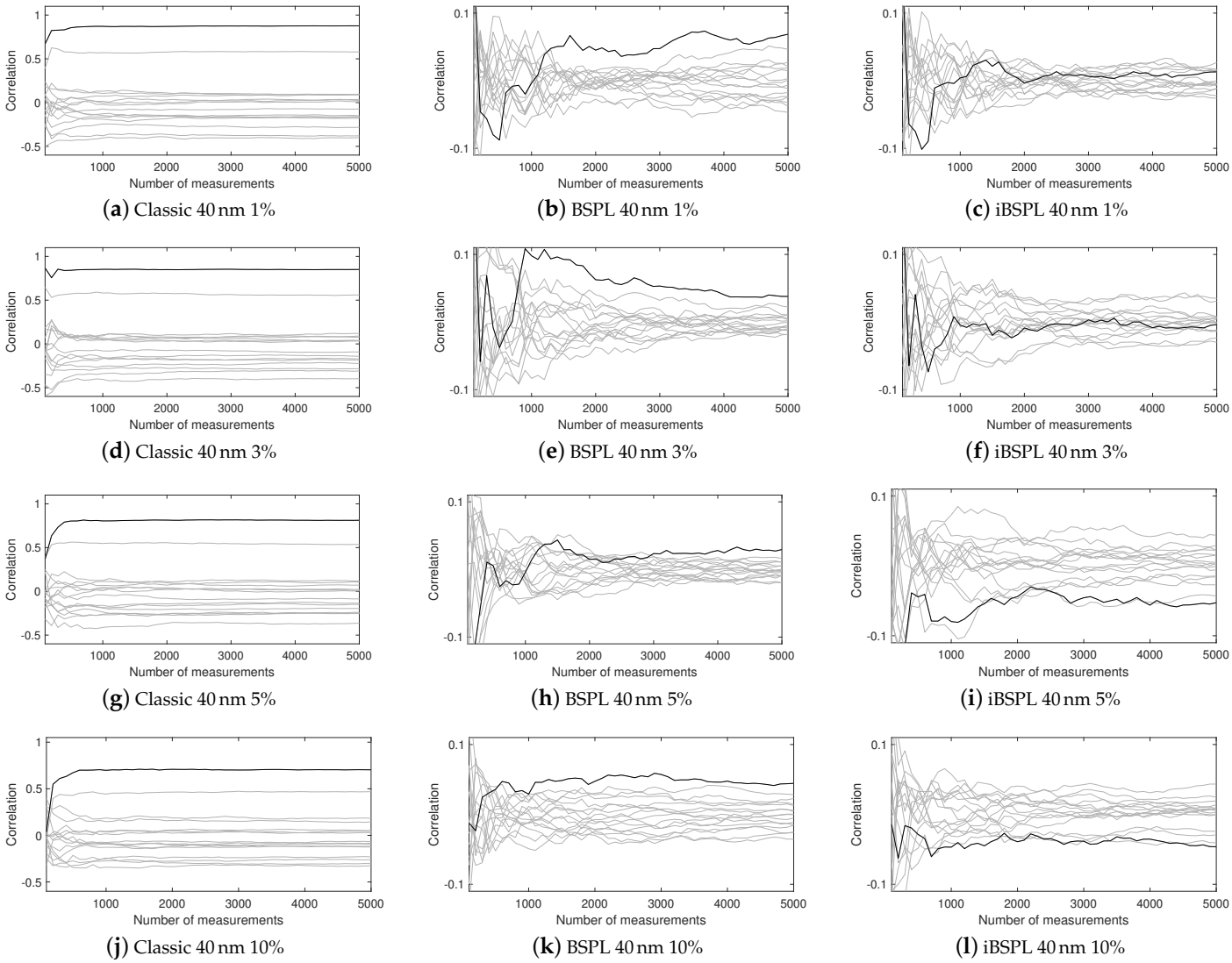


(**i**) SBox 40 nm 10%



(**j**) SBox 65 nm 10%

Figure 10. Information theoretic analysis of the PRESENT SBox synthesized in Classic, BSPL or iBSPL logic gates for different levels of process variations considered.



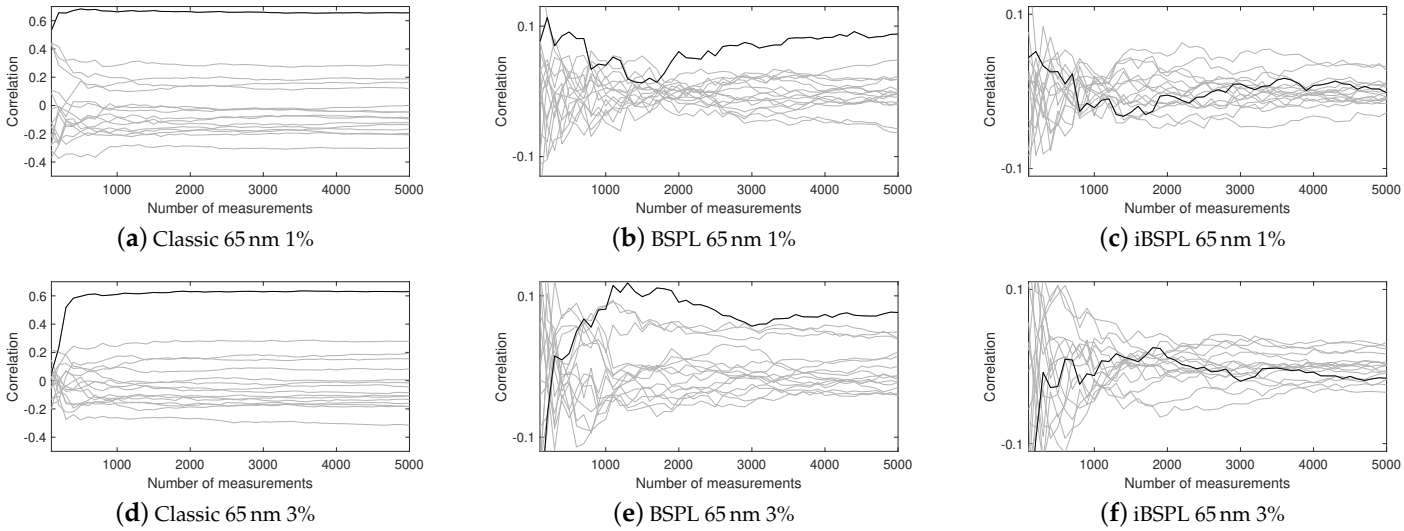
(**a**) Classic 40 nm 1% (**b**) BSPL 40 nm 1% (**c**) iBSPL 40 nm 1%

(**d**) Classic 40 nm 3% (**e**) BSPL 40 nm 3% (**f**) iBSPL 40 nm 3%

(**g**) Classic 40 nm 5% (**h**) BSPL 40 nm 5% (**i**) iBSPL 40 nm 5%

(**j**) Classic 40 nm 10% (**k**) BSPL 40 nm 10% (**l**) iBSPL 40 nm 10%

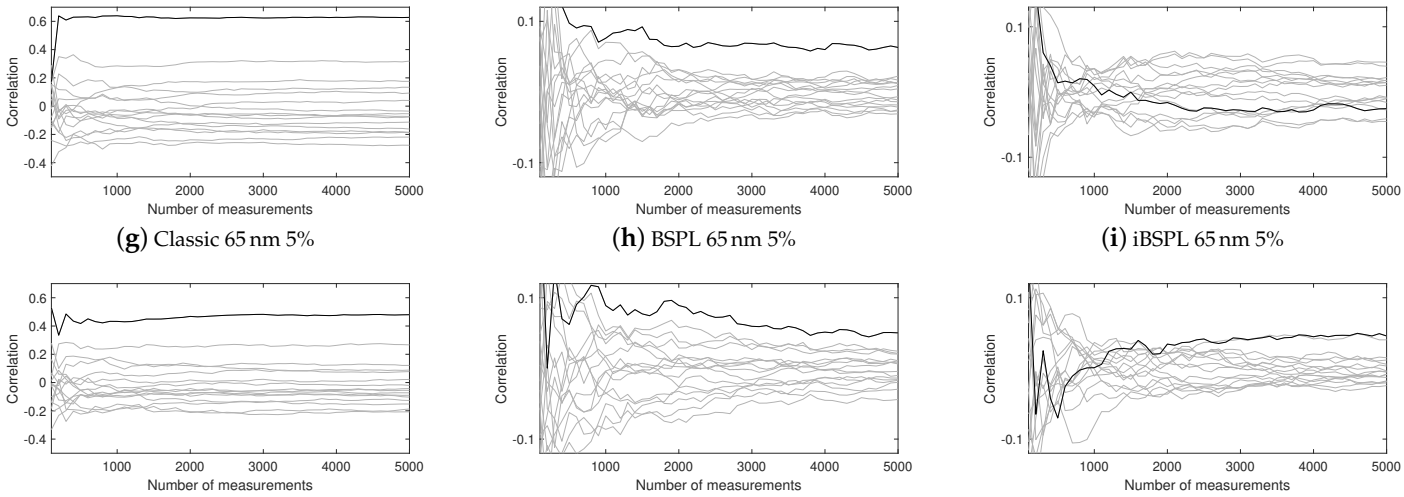
Figure 11. Average of 500 MCDPA attacks using 5000 simulations of noisy SBox leakage currents for random inputs modeling different levels of intra-die process variations (40 nm).



(**a**) Classic 65 nm 1% (**b**) BSPL 65 nm 1% (**c**) iBSPL 65 nm 1%

(**d**) Classic 65 nm 3% (**e**) BSPL 65 nm 3% (**f**) iBSPL 65 nm 3%

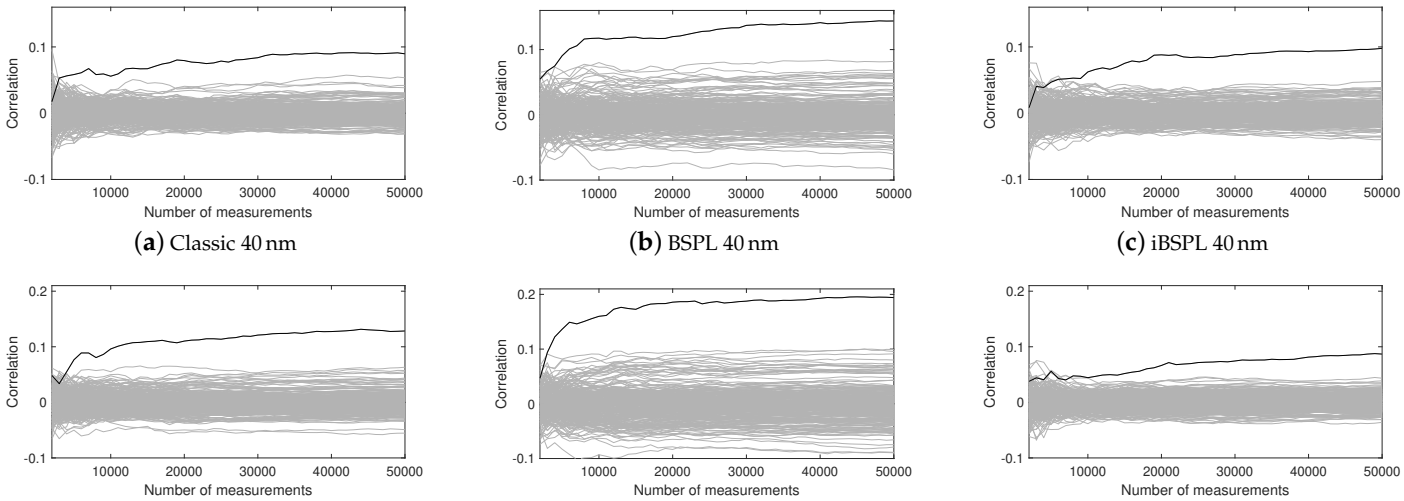
Figure 12. *Cont*.



(**g**) Classic 65 nm 5% (**h**) BSPL 65 nm 5% (**i**) iBSPL 65 nm 5%

(**j**) Classic 65 nm 10% (**k**) BSPL 65 nm 10% (**l**) iBSPL 65 nm 10%

Figure 12. Average of 500 MCDPA attacks using 5000 simulations of noisy SBox leakage currents for random inputs modeling different levels of intra-die process variations (65 nm).



(**a**) Classic 40 nm (**b**) BSPL 40 nm (**c**) iBSPL 40 nm

(**d**) Classic 65 nm (**e**) BSPL 65 nm (**f**) iBSPL 65 nm

Figure 13. MCDPA attack on 50,000 simulated dynamic power traces for random input transitions.

6. Conclusions

In this work we have discussed several shortcomings of the Balanced Static Power Logic (BSPL) approach introduced in [27]. Most notably, we have found that balancing drain-source currents is not sufficient anymore in nanometer process technologies due to the significant impact of the gate leakage on the data dependency of the leakage currents. In fact, it is also insufficient to consider only the switched `off` transistors when analyzing the leakage currents of a gate. In our experiments 85–92% of the remaining data dependency of BSPL gates in 40 nm and 65 nm technologies originated from leakages through the gate insulator of switched `on` transistors. We argue that generic cell structures which balance both drain-source currents *and* gate leakages, would be highly cost-inefficient. Therefore, we propose an alternative strategy based on systematically adding always-`off` transistors to determined signal lines of classic CMOS logic gates in a step-by-step process to balance out any input dependency. We showed that our designed *improved Balanced Static Power Logic (iBSPL)* cells require less area and energy, while at the same time being faster and more secure in both of our analyzed commercial process technologies 40 nm and 65 nm.

As future work on this topic we plan to construct full cell layouts including drive strength tuning, and perform characterization of the iBSPL logic gates to create a usable and manufacturable standard cell library. Afterwards we want to tape-out a test chip using our iBSPL library to perform an experimental validation of its merits on a fabricated silicon chip.

Author Contributions: Methodology, B.F.; investigation, A.M.; writing—original draft preparation, B.F.; writing—review and editing, T.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Deutsche Forschungsgemeinschaft (DFG) through the Germany's Excellence Strategy under Grant EXC 2092 CASA-390781972, and in part by the Project "Aged but Fit: Long Lasting Security for Trusted Platforms" under Grant 418658052.

Institutional Review Board Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Giorgetti, J.; Scotti, G.; Simonetti, A.; Trifiletti, A. Analysis of data dependence of leakage current in CMOS cryptographic hardware. In Proceedings of the 17th ACM Great Lakes Symposium on VLSI 2007, Stresa, Italy, 11–13 March 2007; pp. 78–83.
2. Mangard, S.; Oswald, E.; Popp, T. *Power Analysis Attacks—Revealing the Secrets of Smart Cards*; Springer: New York, NY, USA, 2007.
3. Kocher, P.C.; Jaffe, J.; Jun, B. Differential Power Analysis. In Proceedings of the Annual International Cryptology Conference 1999 (CRYPTO'99), Santa Barbara, CA, USA, 15–19 August 1999; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1666, pp. 388–397.
4. Gandolfi, K.; Mourtel, C.; Olivier, F. Electromagnetic Analysis: Concrete Results. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Paris, France, 14–16 May 2001; pp. 251–261.
5. Lin, L.; Burleson, W. Leakage-based differential power analysis (LDPA) on sub-90 nm CMOS cryptosystems. In Proceedings of the 2008 IEEE International Symposium on Circuits and Systems (ISCAS), Seattle, WA, USA, 18–21 May 2008; pp. 252–255.
6. Alioto, M.; Giancane, L.; Scotti, G.; Trifiletti, A. Leakage Power Analysis attacks: Theoretical analysis and impact of variations. In Proceedings of the 2009 16th IEEE International Conference on Electronics, Circuits and Systems (ICECS), Yasmine Hammamet, Tunisia, 13–16 December 2009; pp. 85–88.
7. Alioto, M.; Giancane, L.; Scotti, G.; Trifiletti, A. Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits. *IEEE Trans. Circuits Syst.* **2010**, *57*, 355–367. [CrossRef]
8. Alioto, M.; Bongiovanni, S.; Djukanovic, M.; Scotti, G.; Trifiletti, A. Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations. *IEEE Trans. Circuits Syst.* **2014**, *61*, 429–442. [CrossRef]
9. Alioto, M.; Bongiovanni, S.; Scotti, G.; Trifiletti, A. Leakage Power Analysis attacks against a bit slice implementation of the Serpent block cipher. In Proceedings of the 2014 21st International Conference Mixed Design of Integrated Circuits and Systems (MIXDES), Lublin, Poland, 19–21 June 2014; pp. 241–246.
10. Moradi, A. Side-Channel Leakage through Static Power—Should We Care about in Practice? In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems 2014 (CHES 2014), Busan, Korea, 23–26 September 2014; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8731, pp. 562–579.
11. Pozo, S.M.D.; Standaert, F.; Kamel, D.; Moradi, A. Side-channel attacks from static power: When should we care? In Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France, 9–13 March 2015; pp. 145–150.
12. Moos, T.; Moradi, A.; Richter, B. Static power side-channel analysis of a threshold implementation prototype chip. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), Lausanne, Switzerland, 27–31 March 2017; pp. 1324–1329.
13. Bellizia, D.; Cellucci, D.; Stefano, V.D.; Scotti, G.; Trifiletti, A. Novel measurements setup for attacks exploiting static power using DC pico-ammeter. In Proceedings of the 2017 European Conference on Circuit Theory and Design (ECCTD), Catania, Italy, 4–6 September 2017; pp. 1–4.
14. Moos, T.; Moradi, A.; Richter, B. Static Power Side-Channel Analysis–An Investigation of Measurement Factors. *IEEE Trans. Very Large Scale Integr. Syst.* **2019**, *28*, 376–389. [CrossRef]
15. Karimi, N.; Moos, T.; Moradi, A. Exploring the Effect of Device Aging on Static Power Analysis Attacks. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2019**, *2019*, 233–256. [CrossRef]
16. Moos, T. Static Power SCA of Sub-100 nm CMOS ASICs and the Insecurity of Masking Schemes in Low-Noise Environments. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2019**, *2019*, 202–232. [CrossRef]
17. Moos, T. Unrolled Cryptography on Silicon A Physical Security Analysis. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2020**, *2020*, 416–442. [CrossRef]

18. Zhu, N.; Zhou, Y.; Liu, H. Counteracting leakage power analysis attack using random ring oscillators. In Proceedings of the Conference on Sensor Network Security Technology and Privacy Communication System, Harbin, China, 18–19 May 2013; pp. 74–77.
19. Halak, B.; Murphy, J.P.; Yakovlev, A. Power balanced circuits for leakage-power-attacks resilient design. In Proceedings of the 2015 Science and Information Conference (SAI), London, UK, 28–30 July 2015; pp. 1178–1183.
20. Zhu, N.H.; Zhou, Y.J.; Liu, H.M. A standard cell-based leakage power analysis attack countermeasure using symmetric dual-rail logic. *J. Shanghai Jiaotong Univ. Sci.* **2014**, *19*, 169–172. [CrossRef]
21. Jayasinghe, D.; Ignjatovic, A.; Ambrose, J.A.; Ragel, R.G.; Parameswaran, S. QuadSeal: Quadruple algorithmic symmetrizing countermeasure against power based side-channel attacks. In Proceedings of the 2015 International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES), Amsterdam, The Netherlands, 4–9 October 2015; pp. 21–30.
22. Padmini, C.; Ravindra, J.V.R. CALPAN: Countermeasure against Leakage Power Analysis attack by normalized DDPL. In Proceedings of the 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, India, 18–19 March 2016; pp. 1–7.
23. Yu, W.; Köse, S. Security-Adaptive Voltage Conversion as a Lightweight Countermeasure Against LPA Attacks. *IEEE Trans. Very Large Scale Integr. Syst.* **2017**, *25*, 2183–2187. [CrossRef]
24. Yu, W.; Köse, S. False Key-Controlled Aggressive Voltage Scaling: A Countermeasure Against LPA Attacks. *IEEE Trans. CAD Integr. Circuits Syst.* **2017**, *36*, 2149–2153. [CrossRef]
25. Yu, W.; Wen, Y. Leakage Power Analysis (LPA) Attack in Breakdown Mode and Countermeasure. In Proceedings of the 2018 31st IEEE International System-on-Chip Conference (SOCC), Arlington, VA, USA, 4–7 September 2018; pp. 102–105.
26. Belohoubek, J.; Fiser, P.; Schmidt, J. Standard Cell Tuning Enables Data-IndependentStatic Power Consumption. In Proceedings of the 23rd IEEE International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS), Novi Sad, Serbia, 22–24 April 2020.
27. Fadaeinia, B.; Moos, T.; Moradi, A. BSPL: Balanced Static Power Logic. *IACR Cryptol. ePrint Arch.* **2020**, *2020*, 558.
28. Wanlass, F.; Sah, C. Nanowatt logic using field-effect metal-oxide semiconductor triodes. In *Proceedings of the Solid-State Circuits Conference*; Digest of Technical Papers; IEEE: Piscataway, NJ, USA, 1963; Volume VI, pp. 32–33.
29. Roy, K.; Mukhopadhyay, S.; Mahmoodi-Meimand, H. Leakage current mechanisms and leakage reduction techniques in deep-submicrometer CMOS circuits. *Proc. IEEE* **2003**, *91*, 305–327. [CrossRef]
30. Yang, S.; Wolf, W.; Vijaykrishnan, N.; Xie, Y.; Wang, W. Accurate stacking effect macro-modeling of leakage power in sub-100 nm circuits. In Proceedings of the 18th International Conference on VLSI Design Held Jointly with 4th International Conference on Embedded Systems Design, Kolkata, India, 3–7 January 2005; pp. 165–170. [CrossRef]
31. Standaert, F.; Malkin, T.; Yung, M. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques 2009, Zagreb, Croatia, 10–14 May 2009; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5479, pp. 443–461.
32. Macé, F.; Standaert, F.; Quisquater, J. Information Theoretic Evaluation of Side-Channel Resistant Logic Styles. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems 2007, Vienna, Austria, 10–13 September 2007; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4727, pp. 427–442.
33. Hanchate, N.; Ranganathan, N. LECTOR: A technique for leakage reduction in CMOS circuits. *IEEE Trans. Very Large Scale Integr. Syst.* **2004**, *12*, 196–205. [CrossRef]
34. Helms, D.; Eilers, R.; Metzdorf, M.; Nebel, W. Leakage Models for High-Level Power Estimation. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **2018**, *37*, 1627–1639. [CrossRef]
35. Keerti Kumar, K.; Bheema Rao, N. Variable gate oxide thickness MOSFET: A device level solution for sub-threshold leakage current reduction. In Proceedings of the 2012 International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 15–16 March 2012; pp. 495–498. [CrossRef]
36. Sangameswaran, S.; Yamauchi, S. Post-layout parasitic verification methodology for mixed-signal designs using fast-SPICE simulators. In Proceedings of the 2005 IEEE Dallas/CAS Workshop on Architecture, Circuits and Implementtation of SOCs, Richardson, TX, USA, 10 October 2005; pp. 211–214. [CrossRef]
37. Kamon, M.; McCormick, S.; Shepard, K. Interconnect parasitic extraction in the digital IC design methodology. In Proceedings of the 1999 IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers (Cat. No.99CH37051), San Jose, CA, USA, 7–11 November 1999; pp. 223–230. [CrossRef]
38. Moradi, A.; Standaert, F. Moments-Correlating DPA. In Proceedings of the ACM Workshop on Theory of Implementation Security (TIS@CCS 2016), Vienna, Austria, 24–28 October 2016; Bilgin, B., Nikova, S., Rijmen, V., Eds.; ACM: New York, NY, USA, 2016; pp. 5–15. [CrossRef]