Masking at Gate Level in the Presence of Glitches

Wieland Fischer and Berndt M. Gammel

Infineon Technologies AG, St.-Martin-Straße 76,
D-81541 Munich, Germany
{Wieland.Fischer, Berndt.Gammel}@infineon.com

Abstract. It has recently been shown that logic circuits in the implementation of cryptographic algorithms, although protected by "secure" random masking schemes, leak side-channel information, which can be exploited in differential power attacks [14]. The leak is due to the fact that the mathematical models describing the gates neglected multiple switching of the outputs of the gates in a single clock cycle. This effect, however, is typical for CMOS circuits and known as *glitching*. Hence several currently known masking schemes are not secure in theory or practice. Solutions for DPA secure circuits based on logic styles which do not show glitches have several disadvantages in practice. In this paper, we refine the model for the power consumption of CMOS gates taking into account the side-channel of glitches. It is shown that for a general class of gate-level masking schemes a universal set of masked gates does not exist. However, there is a family of masked gates which is theoretically secure in the presence of glitches if certain practically controllable implementation constraints are imposed. This set of gates should be suitable for automated CMOS circuit synthesis.

Keywords: Cryptanalysis, side-channel attacks, power analysis, DPA, digital circuits, logic circuits, masking, random masking, masked logic circuits, glitches.

1 Introduction

Cryptanalysis based on side-channel information exploits the information leaked during the computation of an algorithm. Side-channel information can be contained in the characteristic power consumption, the timing, or the electromagnetic emanation of the device during the processing of secret information. Power analysis attacks exploit the fact that, in general, the instantaneous power consumption of a circuit depends on the data being processed by the circuit. The effect is prominent especially in the widely used CMOS design style. *Differential power analysis* (DPA), first introduced in [12], allows the attacker to exploit correlations between the observable instantaneous power consumption and intermediate results involving the secret. During the last years it has become more and more obvious that it is extremely difficult to protect a security device against

J.R. Rao and B. Sunar (Eds.): CHES 2005, LNCS 3659, pp. 187–200, 2005.

DPA [1,2,3,4,5,6,8,9,13,14,15,16,18,21,22,23]. In the spirit of power analysis attacks Electromagnetic Emanation Analysis (EMA) extracts secret information from the electromagnetic radiation emited during the operation of the device [7].

The first class of *ad-hoc approaches* against power analysis attacks tries to reduce the signal-to-noise ratio of the side-channel leakage and finally to hide the usable information in the noise. Suggested methods are detached power supplies [20], the addition of power noise generators, or the application of a probabilistic disarrangement of the times at which the attacked intermediate results are processed. The latter can be achieved by inserting random delays or applying randomizations to the execution path. While such measures certainly increase the experimental and computational working load of the attacker they do not render the attack infeasible. In practice, typically several countermeasures are combined [5,13]. This can reduce the correlation down to a level that makes a DPA practically impossible. However, higher order differential attacks or the possibility of obtaining a spatial resolution of the power consumption and an increased signal-to-noise ratio by observing local electromagnetic emanations may again open a backdoor for professional attackers.

Circuit design approaches, the second class of countermeasures, aim at removing the root cause for side-channel leakage information. In standard CMOS style circuits the power consumption depends strongly on the the processed data. In some dynamic and differential logic styles, like Sense Amplifier Based Logic (SABL) [21], which is based on Differential Cascode Voltage Switching Logic (DCVLS), the power consumption can be made almost independent of the processed data. However, data independent power consumption requires a maximum activity factor and hence maximum power consumption. It is also essential that the load capacitances of the differential outputs are matched. Remaining asymmetries (parasitics, cross-coupling) make a DPA still possible. Disadvantages of this circuit style are the lack of standard cell libraries and tools, which leads to a full-custom design style. Area (power consumption) of a SABL circuit design are approximately 3.5 times (4.5 times) larger than for a corresponding CMOS design. As for all two-cycle schemes the performance is reduced by a factor of two. The Wave Dynamic Differential Logic style (WDDL) adopts the ideas of SABL. It implements the behavior of a dynamic and differential logic, but is based on standard CMOS cells [22]. Area and power consumption are approximately 3.5 times larger than for a CMOS design. The performance is two times smaller.

Masking approaches, the third class of measures, counteract DPA by randomizing intermediate results occurring during the execution of the cryptographic algorithm. The idea behind this approach is that the power consumption of operations on randomized data should not be correlated with the actual plain intermediate data [15]. Algorithmic countermeasures in the context of symmetric ciphers based on secret sharing schemes have been independently proposed by Goubin and Paterin [9] and Chari et al. [4]. A theory of securing a circuit at the gate level against side-channel attacks (focused on probing) was developed in [10].

Masking at algorithm level for asymmetric algorithms [6,17], as well as for symmetric algorithms, e.g., DES and AES [2,3], has been developed. Cryptographic algorithms often combine Boolean functions (like logical XOR or AND operations) and arithmetic functions (operations in fields with characteristic bigger than two). Masking operations for these two types of functions are referred to as *Boolean and arithmetic masking*, respectively. This poses the problem of a secure conversion between the two types of maskings in both directions [2].

It is appealing to apply the idea of randomizing intermediate results already on the level of logic gates. *Masking at gate level* leads to circuits where no wire carries a value which is correlated to an intermediate result of the algorithm. Clearly this approach is more generic than the algorithmic approach. Masking at gate level is independent of the specifically implemented algorithm. Once a secure masking scheme has been developed the generation of the masked circuit from the algorithm can be automated, and a computer program can convert the digital circuit of any cryptographic algorithm to a circuit of masked gates. This would also relieve the designers or implementers of cryptographic algorithms from the complex task of elaborating a specific solution against side-channel leakage for each new implementation variant or algorithm. Various generic masking schemes have been proposed. In [16] the multiplexor gate (MUX) used in the implementation of nonlinear operations, like S-boxes, is replaced by a masked MUX gate. In [11] the basic operations of an arithmetic-logic unit (ALU) are protected with one or more random masks at each masked gate. In [23] correction terms for the AND gate in the nonlinear components of the S-box of the AES are introduced. It has been shown that it is possible to break masking schemes that rely on one mask using advanced DPA methods [1].

The security analyses of masking schemes, conducted so far, were based on the implicit assumption that the input signals of any (masked) gate in a combinational CMOS circuit arrive at the same time. Recently it has been shown [14], that this assumption is not sufficient: the output of the gate possibly switches several times during one clock cycle. The transitions at the output of a gate, previous to the stable state right before the next clock edge is attained, are known as *glitches*. Glitches are a typical phenomenon in CMOS circuits and extensively discussed in the literature on VLSI design [19]. Because a glitch can cause a full swing transition at the output of the gate, just like the 'proper' transition to the final value, a glitch is *not* a negligible higher order effect. As made evident in [14] glitches do not just add a background noise due to uncorrelated switching activity – the dissipated energy of nonlinear masked gates is correlated to the processed values whenever the input values do not arrive simultaneously (forcing the output of the gate to toggle several times). Hence glitches can carry side-channel information and their effect must be included in the analysis of any secure masking scheme.

In the next section a model for the power consumption of CMOS gates is developed which takes into account the side-channel of glitches. Based on this model the notion of G-equivariance is introduced and it is shown that in the stated gate and energy models G-equivariance is a necessary condition for ran-

domized gates to prevent a differential power attack. We will show that in a class of gates which is preferred for implementation reasons, there exists no G-equivariant gate that can be used to realize a nonlinear logical function. However, for a model with weakened conditions an explicit construction of a universal set of semi-G-equivariant gates is given. The necessary constraints on gate design and signal routing should be realizable in practice using available design tools.

2 The Glitch Problem

In this section the glitch problem described in [14] is reformulated in a more theoretical and abstract way. First, the abstraction of the energy consumption of a single gate, which is the target of a DPA attack, is recapitulated. The most simple energy model which is commonly used is mentioned and a more general definition is given. Then the basic attack on such a gate with statistical means is described. The definitions of randomized gates (in the classical meaning) is given and it is shown how a DPA may still be successful if the more general energy model is applicable.

2.1 The General Power Consumption Model of a Gate

In a DPA the attacker tries to find a correlation between externally known (and guessed) data and internally processed signals. Since he will not be able to gain these internal signal data directly, he is obliged to use physical effects (the side-channels) which are again somehow correlated to the internal signals/data. One of these side-channels is the current consumption. Since we are interested in a protection of this side channel on gate level, out first step has to be the definition of a power consumption model of a gate: A gate g with n inputs and one output will be interpreted as a function $g\colon \mathbb{F}_2^n \to \mathbb{F}_2$. Our premise is that the power consumption during one clock cycle (in a synchronous design) only depends on the input at the time t_0 shortly before the clock edge (the old input) and after the clock edge (the new input), e.g., at t_1 shortly before the next clock edge. We do not consider dependencies on other signals in the surrounding circuit, like cross-coupling phenomena. The following definition of an energy function of a gate suggests itself:

Definition 1. *Let $g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a gate. Denote the input at time t_0, at or shortly before the rising edge of a clock cycle, as $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$ and the input at time t_1, at or shortly before the next rising edge, as $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. Then the energy consumption of the gate during this transition is given by the real number $E_g(a, x) \in \mathbb{R}$. Hence the* ***Energy function of the gate*** *g is defined to be the map*

$$\begin{aligned} E_g\colon \mathbb{F}_2^n \times \mathbb{F}_2^n &\longrightarrow \mathbb{R} \\ (a, x) &\longmapsto E_g(a, x). \end{aligned}$$

The energy function of a gate may be different for individual gates in a circuit, even if they are functionally equal. The reason is that the energy depends mainly on the individual capacitive load the gate has to drive.

The Simplistic Model: In a simplistic energy consumption model (coined on, e.g., CMOS logic style) one mainly identifies the power consumption of a gate with the energy needed to drive the output capacitance if the output toggles. The energy consumption of a gate is described only by its digital output behavior. Hence it is determined by the output values of g at times t_0 and t_1 and a fixed tuple $(E_{g,0\to0}, E_{g,0\to1}, E_{g,1\to0}, E_{g,1\to1}) \in \mathbb{R}^4$. If for example at time t_0 the output value of g is 1 and at time t_1 it is 0 then the energy for this clock cycle is $E_{g,1\to0}$. Hence, in this model the energy function of the gate g is given by: $E_g(a,x) := E_{g,g(a)\to g(x)}$.

Differential Power Analysis of This Model: Assume we have a cryptographic algorithm with some secret (key) implemented as a CMOS circuit. Further assume that there is a gate $g\colon \mathbb{F}_2^2 \to \mathbb{F}_2$ within this circuit. The input values of g at time t_0 are $(a,b) \in \mathbb{F}_2^2$ and later at t_1 are $(x,y) \in \mathbb{F}_2^2$. Since an attacker will survey the energy consumption of this gate during several runs of the algorithm with different messages, these values may be seen as random variables $a,b,x,y\colon \Omega \longrightarrow \mathbb{F}_2$ on some probability space (Ω, Σ, P). This gives rise to the following concatenation

$$\mathcal{E}_g := E_g \circ (a,b,x,y)\colon \Omega \longrightarrow \mathbb{F}_2^2 \times \mathbb{F}_2^2 \longrightarrow \mathbb{R}$$

With the knowledge of the secret key (or parts of it), which is called the *hypothesis*, one may construct a partition of Ω into two disjoint measurable[1] subsets A and B such that $\Omega = A \cup B$, with the property:

$$\mathbb{E}(\mathcal{E}_g|A) \neq \mathbb{E}(\mathcal{E}_g|B),$$

while this construction done with a wrong hypothesis yields: $\mathbb{E}(\mathcal{E}_g|A) = \mathbb{E}(\mathcal{E}_g|B)$. One classical example, cf. [12], is the partition of Ω into

$$A = \{\omega \in \Omega : g(x(\omega), y(\omega)) = 1\} \quad \text{and} \quad B = \{\omega \in \Omega : g(x(\omega), y(\omega)) = 0\}$$

With the simplistic energy model we obtain

$$\mathbb{E}(\mathcal{E}_g|A) = \alpha E_{g,0\to1} + \bar{\alpha} E_{g,1\to1} \quad \text{and} \quad \mathbb{E}(\mathcal{E}_g|B) = \beta E_{g,0\to0} + \bar{\beta} E_{g,1\to0}$$

for $\alpha := P(\{\omega \in \Omega : g(a(\omega), b(\omega)) = 0\}|A)$, $\bar{\alpha} := 1 - \alpha$ as well as $\beta := P(\{\omega \in \Omega : g(a(\omega), b(\omega)) = 0\}|B)$, $\bar{\beta} := 1 - \beta$. In general these two expectation values are not equal (if the hypothesis was correct). This gives rise to the classical DPA.

Remark 1. It is clear that, if $E_{g,0\to0} = E_{g,0\to1} = E_{g,1\to0} = E_{g,1\to1}$, then indeed the two expectation values are always equal, independent of whether the hypothesis was right or wrong. Hence no DPA is possible. In general terms, if the energy function

$$E_g\colon \mathbb{F}_2^2 \times \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2 \text{ is constant,} \qquad (*)$$

[1] Although very important, we are not going to specify the measurability any further.

then the gate does not leak information and a DPA on the gate is not possible. In practice these conditions are only met if a logic style is chosen for the implementation which guarantees the constancy of the energy function itself. This corresponds to the second class of countermeasures (see discussion in the introduction). If this is not desirable, one still may be able to use the additional conditions given by a, b, x, y: We only have to fulfill the condition

$$\mathcal{E}_g \colon \Omega \longrightarrow \mathbb{R} \text{ is constant,} \qquad (**)$$

which is weaker than the former one. However, if we want to find gates for general purposes we have to fulfill this condition (**) for any a, b, x, y. Unfortunately, this is equivalent to condition (*).

Randomized Logic as Countermeasure: In fact, there still may be the possibility that $\mathcal{E}_g$ is constant in some conditional sense, even if E_g is not. This can be in the class of randomized (masked) gates: Randomizing a signal (in our context) means substituting one digital signal $a \in \mathbb{F}_2$ by a number of signals $a_1, \ldots, a_n \in \mathbb{F}_2$ with $a = a_1 + \cdots + a_n$ so that there exists no correlation between a and each summand a_i. For practical reasons, we will be restricted ourselves to the case $n = 2$.

One philosophy is to interpret the randomized signal (a_1, a_2) as the pair of the masked signal $a_m = a_1$ and its mask $m_a = a_2$ (cf. notation in e.g. [14]). But this is just terminology and we will only follow it in our discussion for presenting the randomized gates as in [14]. However this point of view has an impact on the philosophy of randomized (or masked) gates: Since the signals a, b are now split up in two portions, one has to substitute the old gate $g \colon \mathbb{F}_2^2 \to \mathbb{F}_2$ by a new gate.

The first choice would be $g' \colon \mathbb{F}_2^2 \times \mathbb{F}_2^2 \to \mathbb{F}_2$, such that $g(a, b) = g'(a_1, a_2, b_1, b_2)$, with $a = a_1 + a_2$ and $b = b_1 + b_2$. But since the output should also be randomized, one possibility would be $g' \colon \mathbb{F}_2^2 \times \mathbb{F}_2^2 \times \mathbb{F}_2 \to \mathbb{F}_2$, with the property $g(a, b) = g'(a_m, m_a, b_m, m_b, m_c) + m_c$ and $a = a_m + m_a$, $b = b_m + m_b$. This property defines g' uniquely. In the following g' is called **the masked lifting** of g, since the output of g' is the output of $c := g(a, b)$ masked with m_c. Fig. 1 shows an example for a circuit using masked liftings of gates (left hand sketch) and a realization of a lifting of an AND gate [8,23] (right hand sketch).

Another choice is using two gates $(g_1, g_2) \colon \mathbb{F}_2^2 \times \mathbb{F}_2^2 \to \mathbb{F}_2^2$ with the property $g(a, b) = g_1(a_1, a_2, b_1, b_2) + g_2(a_1, a_2, b_1, b_2)$. Here g_1 and g_2 are not uniquely defined by this equation. But, of course, if g_1 is given then g_2 will be fixed. The pair (g_1, g_2) is called **a randomized lifting** of g.

Using the simplistic energy consumption model from above

$$E_{g'}((\tilde{a}, \tilde{b}, m_c), (\tilde{x}, \tilde{y}, m_z)) = E_{g', g'(\tilde{a}, \tilde{b}, m_c) \to g'(\tilde{x}, \tilde{y}, m_z)},$$

where $(\tilde{a}, \tilde{b}, m_c) \in \mathbb{F}_2^2 \times \mathbb{F}_2^2 \times \mathbb{F}_2$ is the input at time t_0, $(\tilde{x}, \tilde{y}, m_z) \in \mathbb{F}_2^2 \times \mathbb{F}_2^2 \times \mathbb{F}_2$ the input at time t_1 with the abbreviations $\tilde{a} = (a_m, m_a)$, etc., the energy consumption $E_g((a, b), (x, y))$ has to be substituted by the (conditional resp. a, b, x, y) expectation value

$$\mathbb{E}(E_{g'}((\tilde{a}, \tilde{b}, m_c), (\tilde{x}, \tilde{y}, m_z))),$$

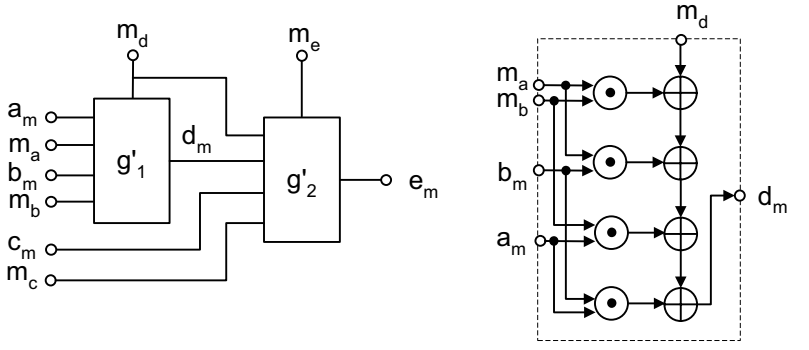

Fig. 1. Example for a combinational circuit consisting of two masked liftings of gates. The figure to the right shows a masked AND gate as given in [23,8]. The $\odot$ and $\oplus$ symbols denote a logical AND and XOR gate, respectively.

where $\tilde{a} = (a_m, m_a)$, $\tilde{b} = (b_m, m_b)$, m_c, $\tilde{x} = (x_m, m_x)$, $\tilde{y} = (y_m, m_y)$, m_z are interpreted as random variables with $a = a_m + m_a$, etc. An attacker will not be able to know the exact (microscopic) signals $(\tilde{a}, \tilde{b}, m_c), (\tilde{x}, \tilde{y}, m_z)$, but rather only the (macroscopic) signals a, b, x, y.

Indeed, if $m_c, m_z \colon \Omega \to \mathbb{F}_2$ are uniformly distributed random variables, independent to the random variables $g(a, b), g(x, y)$ then the masked lifting g' of a gate g does not leak information: $\mathbb{E}(E_{g'}((\tilde{a}, \tilde{b}, m_c), (\tilde{x}, \tilde{y}, m_z)))$ is independent of a, b, x, y. This was stated in [23,8].

2.2 Power Consumption of a Gate in the Presence of Glitches

As realized in [14], in realistic CMOS implementations the different signals x_m, m_x, y_m, m_y, m_z may not arrive at the gate g' the same time. In the example circuit of Fig. 1 signal d_m may arrive with a delay at the input of gate g'_2 compared to signals m_d, c_m, m_c due to the gate delay imposed by g'_1. Furthermore, all input signals of gate g'_2 have in general different additional delay contributions due to the propagation delay caused by wire capacitances. These delays depend on the route of the signal and are fixed when the circuit is laid out.

Consider the example that the signals arrive in the distinct order $y_m \longrightarrow m_y \longrightarrow m_z \longrightarrow x_m \longrightarrow m_x$. In this case the output value of the gate changes not only once during the clock cycle but five times leading to the consecutive output transitions $c_1 := g(a_m, m_a, b_m, m_b, m_c) \longrightarrow c_2 := g(a_m, m_a, y_m, m_b, m_c) \longrightarrow c_3 := g(a_m, m_a, y_m, m_y, m_c) \longrightarrow c_4 := g(a_m, m_a, y_m, m_y, m_z) \longrightarrow c_5 := g(x_m, m_a, y_m, m_y, m_z) \longrightarrow c_6 := g(x_m, m_x, y_m, m_y, m_z)$. Therefore the energy consumption will be given by the sum $E_{g',c_1 \to c_2} + E_{g',c_2 \to c_3} + E_{g',c_3 \to c_4} + E_{g',c_4 \to c_5} + E_{g',c_5 \to c_6}$.

Hence a new power model is required such that $E_{g'}((\tilde{a}, \tilde{b}, m_c), (\tilde{x}, \tilde{y}, m_z))$ is given by the sum from above. Unfortunately, with this model, it was shown in [14] that $\mathbb{E}(E_{g'}((\tilde{a}, \tilde{b}, m_c), (\tilde{x}, \tilde{y}, m_z)))$ is not independent of a, b, x, y any more, opening a door for DPA.

One can conceive an even worse situation: if a well-equipped attacker is able to measure the different partial energies of the five transitions the constraints for a gate to be resistant against DPA are even more difficult to fulfill.

3 Abstraction and Analysis of the Glitch Problem

The last section has motivated the following strategy and definitions. First the abstract model of the gates together with their energy model will be defined. Then conditions imposed on the gates will be formulated, which ensure that a differential power attack cannot be mounted.

3.1 The Power Consumption Model in the Presence of Glitches

Because of glitches the gate $g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ can switch up to n times within one clock period and because every transition of the output consumes an amount of power $E_{g,0\to0}, E_{g,0\to1}, E_{g,1\to0}$, or $E_{g,1\to1}$, the notion of the energy function has to be generalized. Also, since the four values from above may strongly depend on the individual gate and its position in a circuit, it makes sense to treat these values as indeterminates. Therefore, it is natural to value the energy function not in $\mathbb{R}$ but rather in the 4-dimensional vector space $V := \mathbb{R}\cdot e_{00} \oplus \mathbb{R}\cdot e_{01} \oplus \mathbb{R}\cdot e_{10} \oplus \mathbb{R}\cdot e_{11}$. For a certain implementation one may concatenate the energy function with the evaluation function $ev\colon V \to \mathbb{R}, (x_{00}, x_{01}, x_{10}, x_{11}) \mapsto \sum_{i,j} x_{ij} E_{g,i\to j}$. We first give the formal definition of our power consumption model:

Definition 2. *Let $g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a gate with n inputs and one output. The **(partial) energy functions** of the gate g are given by:*

$$E_{g,i}\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathrm{Map}(\{1,\dots,n\},\{1,\dots,n,\}) \longrightarrow V$$
$$(\tilde{a}, \tilde{x}, \varphi) \longmapsto e_{g(\tilde{b}_i), g(\tilde{b}_{i+1})},$$

for $i = 1,\dots,n$. Here $\tilde{b}_i = (b_{i1},\dots,b_{in}) \in \mathbb{F}_2^n$ is defined by $\tilde{b}_1 := \tilde{a}$ and

$$b_{(i+1)j} := \begin{cases} x_j, & \text{if} \quad \varphi(j) = i, \\ b_{ij}, & \text{else}, \end{cases}$$

in particular we have $\tilde{x} = \tilde{b}_{n+1}$.

The map φ describes the order of the incoming (changing) input signals. If $\varphi(j) = 1$ then signal j changes first and the signal to change next is the one with $\varphi(j) = 2$, and so on. Since two or more signals may arrive at the same time the map φ does not need to be a permutation. The old energy description of a gate can be obtained by fixing $\varphi \equiv 1$ (or any constant between 1 and n).

The n+1 tuples $\tilde{b}_i$ are the different input value during the clock cycle at $n+1$ possible different moments in time: $\tilde{b}_0 = \tilde{a}$ is the input value at t_0 and $\tilde{b}_{n+1} = \tilde{x}$ is the final input value at t_1. $\tilde{b}_1, \dots, \tilde{b}_n$ are the consecutive input signals in between.

We see the order of the signals φ as a constant associated for each single gate within a circuit. This order is fixed at the design time of the circuit and is given by parameters such as the depth of logic tree at each input of the gate and the precise route of the signals.

Remark 2. This definition of the energy consumption of a gate reflects the assumption (idealization) that the implementation of a gate does not have any usable internal side-channels. This means, for instance, that the gate itself is inherently glitch free and there is only one signal change at the output if one input signal changes. Also the output delay must not depend on the input value. It can safely be assumed that these prerequisites can be realized in practice with relatively high accuracy if a masked logic cell is crafted for use in a library.

3.2 Randomized Signal Pairs

Randomization in our context means splitting up a signal a into a pair (a_1, a_2) of signals such that $a = a_1 + a_2$ and the individual bits a_1 and a_2 are unknown, i.e., random and uniformly distributed. Since we are, first of all, interested in the randomized realization of (macroscopic) 2-1 gates like AND, OR, etc. we will restrict ourselves to gates with two (macroscopic) inputs, a, b, which means four actual inputs a_1, a_2, b_1, b_2 for a randomized lifting of the gate. Fig. 2 depicts a combinational circuit where two normal gates $g_1(a, b)$ and $g_2(d, c)$ have been replaced by two randomized liftings of gates $(g_{11}(a_1, a_2, b_1, b_2), g_{12}(a_1, a_2, b_1, b_2))$ and $(g_{21}(d_1, d_2, c_1, c_2),\ g_{22}(d_1, d_2, c_1, c_2))$, which have been selected to sustain the old functionality of the circuit. The following two definitions describe this situation.

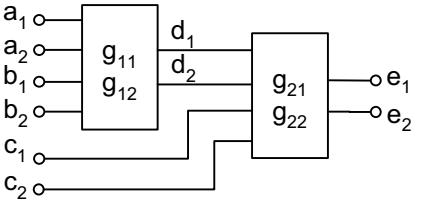

Fig. 2. Example of a combinational circuit using randomized liftings of gates

Definition 3. *A **randomized signal pair** is a 4-tuple (a_1, a_2, b_1, b_2) of random variables $a_1, a_2, b_1, b_2 \colon \Omega \longrightarrow \mathbb{F}_2$ such that the following properties are fulfilled:*

1. *a_1, a_2, b_1, b_2 are uniformly distributed, i.e., $P(a_1 = 0) = P(a_2 = 0) = P(b_1 = 0) = P(b_2 = 0) = 1/2$.*
2. *The random variables a_i and b_j are independent for $1 \leq i, j \leq 2$.*

Remark 3. The pairs a_1, a_2 and b_1, b_2 are in general not independent!

Definition 4. *If we define* $a := a_1 + a_2 \colon \Omega \to \mathbb{F}_2$ *and* $b := b_1 + b_2 \colon \Omega \to \mathbb{F}_2$ *then* $(a, b) \colon \Omega \to \mathbb{F}_2^2$ *is a pair of random variables and we say* $(\tilde{a}, \tilde{b})$ ***is a lifting of the pair*** (a, b)*, where* $\tilde{a} := (a_1, a_2)$ *and* $\tilde{b} := (b_1, b_2)$*.*

In the following we do *not* try to find a single gate g' which exactly lifts the functionality of a specific gate g. Instead we follow the general strategy to search for a *universal set* of lifted gates. That is a family of gates, which have the property that the energy of the macroscopic transition $(a, b) \to (x, y)$ does not leak information and which can be combined to realize any logical function.

In the next section we give a precise formulation of the necessary conditions for lifted gates which do not leak information also in the presence of glitches.

3.3 The Criterion of Glitch-Equivariance of Gates

The notion of glitch-equivariant gates will be introduced. Gates satisfying this criterion do not leak information about the macroscopic transition $(a, b) \to (x, y)$, because they have no flaw in the side-channel of glitches.

Based on the model for the energy function of a masked CMOS gate, Definition 2, and the notion of a randomized signal pair, Definition 3, the following definition describes necessary conditions for the resistance of masked gates in a DPA attack in the presence of gitches.

Definition 5. *A gate* $g \colon \mathbb{F}_2^2 \times \mathbb{F}_2^2 \to \mathbb{F}_2$ *is called* ***G-equivariant*** *if for any* $\varphi \in \mathrm{Map}(\{1, \ldots, 4\}, \{1, \ldots, 4\})$ *and* $i = 1, 2, 3, 4$*, the expectation values of the partial energies* $\mathbb{E}(E_{g,i}((\tilde{a}, \tilde{b}), (\tilde{x}, \tilde{y}), \varphi)) \in V$ *are independent of any choice of randomized signal pairs* $(\tilde{a}, \tilde{b}), (\tilde{x}, \tilde{y})$*.*

Since the family of the randomized signal pairs can be very large we need a simpler criterion in order to decide if a gate is G-equivariant.

Lemma 1. *1) A gate* $g \colon \mathbb{F}_2^2 \times \mathbb{F}_2^2 \to \mathbb{F}_2$ *is G-equivariant if and only if for any* φ *and* i *the expectation value* $\mathbb{E}(E_{g,i}((\tilde{a}, \tilde{b}), (\tilde{x}, \tilde{y}), \varphi)) \in V$ *is independent of any choice of randomized signal pairs* $(\tilde{a}, \tilde{b}), (\tilde{x}, \tilde{y})$ *which are liftings of any* constant *pairs* $(a, b), (x, y)$*.*
2) A gate $g \colon \mathbb{F}_2^2 \times \mathbb{F}_2^2 \to \mathbb{F}_2$ *is G-equivariant if and only if for any* φ *and* $i = 1, 2, 3, 4$*, the* 2^4 *values are equal:*

$$\sum_{\substack{a_1+a_2=a \\ b_1+b_2=b \\ x_1+x_2=x \\ y_1+y_2=y}} E_{g,i}((a_1, a_2, b_1, b_2), (x_1, x_2, y_1, y_2), \varphi), \quad \text{with } a, b, x, y \in \mathbb{F}_2,$$

From the definition of G-equivariance it is immediately obvious that gates satisfying this criterion overcome the problem of side-channel leakage in the presence of glitches (the dominant effect captured by the stated model). It is a simple task to perform an exhaustive search on all 2^{16} possible gates $g \colon \mathbb{F}_2^2 \times \mathbb{F}_2^2 \to \mathbb{F}_2$ using Lemma 1 to obtain a complete list of all G-equivariant gates.

Table 1. The Boolean functions of the 50 G-equivariant gates

$c, c+a_i, c+b_i, c+a_i+b_j, c+a_ib_j, c+a_i+a_ib_j, c+b_i+a_jb_i, c+a_i+b_j+a_ib_j$

There are 50 G-equivariant gates. In the algebraic normal forms, given in Tab. 1, the indices i, j can take on the values 1 or 2 and the constant c is either 0 or 1.

Unfortunately, in the set of G-equivariant gates there are no two gates which can be paired to a lifting of any nonlinear gate (like AND or OR). Thus we have shown that:

Theorem 1. *There is no universal set of masked gates of the form* (g_1, g_2) *with* $g_1, g_2 \colon \mathbb{F}_2^2 \times \mathbb{F}_2^2 \to \mathbb{F}_2$ *satisfying the G-equivariance criterion.*

4 The Logic Family of Semi-G-equivariant Gates

The negative result from the last section leads to the question, whether the strong condition of G-equivariance can be mediated for the realization of a masked CMOS circuit in practice.

Consider the replacement of all simple gates g_i with input a_i, b_i and output c_i by gates $\tilde{g}_i$ with input $\tilde{a}_i = (a_{i1}, a_{i2}), \tilde{b}_i = (b_{i1}, b_{i2})$ and output $\tilde{c}_i = (c_{i1}, c_{i2})$. It is obvious that the pair of correlated signals (say a_{i1}, a_{i2}) of a macroscopic signal (a_i) have always the same gate depth, since they always pass through the same gates. The requirement for the implementation of a masked gate g_i, that the gate delay for both outputs, (c_{i1}, c_{i2}), should be identical, can be fulfilled in practice. Under this condition the cumulative gate delay for each signal of a pair of correlated signal would be equal. The remaining source for different propagation times of the two correlated signals are different routes leading to different capacitances at the outputs of the gate. With contemporary routing technology, however, it is possible to control routing in a way that both signals paths have the same capacitances (with high accuracy). If these design and routing constraints are met the signals of each pair of correlated signals arrive simultaneously at the inputs gate of the next gates. This practically realizable setup for a CMOS circuit implementation rules out certain combinations of the arrival times of signals. Specifically, the conditions in Definition 2 can be reduced to all maps φ with $\varphi(1) = \varphi(2)$ (for a_1, a_2) and $\varphi(3) = \varphi(4)$ (for b_1, b_2).

Definition 6. *A gate* $g \colon \mathbb{F}_2^2 \times \mathbb{F}_2^2 \to \mathbb{F}_2$ *is called* ***semi-G-equivariant*** *if for any* $\varphi \in \mathrm{Map}(\{1, \ldots, 4\}, \{1, \ldots, 4\})$ *with* $\varphi(1) = \varphi(2)$ *and* $\varphi(3) = \varphi(4)$ *the expectation value of the partial energies* $\mathbb{E}(E_{g,i}((\tilde{a}, \tilde{b}), (\tilde{x}, \tilde{y}), \varphi)) \in V$ *is independent of any choice of randomized signal pairs* $(\tilde{a}, \tilde{b}), (\tilde{x}, \tilde{y})$.

An exhaustive search on all 2^{16} gates yields 58 semi-G-equivariant gates. The list of 58 semi-G-equivariant gates comprises the 50 gates from Tab. 1 and additionally the 8 gates given in Tab. 2 below.

Table 2. Boolean function of the additional 8 semi-G-equivariant gates

$$\boxed{c + a_i + b_j + a_1b_1 + a_1b_2 + a_2b_1 + a_2b_2}$$

The 8 additional semi-G-equivariant gates now allow pairings to liftings of non-linear gates. A semi-G-equivariant AND gate can be realized, for instance, by the lifting

$$AND'(a_1, a_2, b_1, b_2) = (a_1 + b_1, a_1 + b_1 + a_1b_1 + a_1b_2 + a_2b_1 + a_2b_2)$$

using entries of Tab. 1 and Tab. 2. One immediately finds 8 realizations for an AND gate. Correspondingly, one possible realization of an OR gate is given by

$$OR'(a_1, a_2, b_1, b_2) = (a_2 + b_2, a_1 + b_1 + a_1b_1 + a_1b_2 + a_2b_1 + a_2b_2).$$

Thus there is a universal set of masked semi-G-equivariant gates. The described gates could be used to craft a set of library cells suited for an automated masked CMOS design. Any implementation of a masked semi-G-equivariant gate of course must avoid unmasked intermediate values on internal cell structures.

5 Conclusions

It has been shown that within the defined gate and energy models G-equivariance is a necessary condition on randomized gates to withstand a differential power attack (in an otherwise unconstrained CMOS circuit). However, there exists no universal set of G-equivariant gates in the considered general class of randomized gates. If practically controllable implementation constraints are imposed a set of masked gates, which are theoretically secure in the presence of glitches, can be constructed. The power model developed in this paper is inevitably a coarse abstraction of the complicated physical processes of the energy dissipation in an active CMOS circuit. Next-higher order effects may be related to the transient behavior of a switching event of a CMOS gate. Such effects may include partial swings of the outputs of gates (overlapping glitches) or cross-couplings between neighboring wires which lead to mutual information leakage. Such higher-order effects, however, are not specific to CMOS circuits, but affect also other circuit styles, such as dynamic and differential logic styles. Further experimental investigations will be necessary to quantify the side-channel leakage signal-to-noise ratio of circuits built with semi-G-equivariant gates, as well as to determine the factor for the design size increase.

References

1. M.-L. Akkar, R. Bevan, and L. Goubin: Two Power Analysis Attacks against One-Mask Methods, *11th International Workshop on Fast Software Encryption – FSE 2004,* (B. K. Roy and W. Meier, eds.), Lecture Notes in Computer Science, vol. 3017, pp. 332–347, Springer-Verlag, 2004.

2. M.-L. Akkar and C. Giraud: An Implementation of DES and AES, Secure against Some Attacks, *Cryptographic Hardware and Embedded Systems – CHES 2001,* (Ç. K. Koç, D. Naccache, and C. Paar, eds.), Lecture Notes in Computer Science, vol. 2162, pp. 309–318, Springer-Verlag, 2001.
3. J. Blömer, J. G. Merchan, and V. Krummel: Provably Secure Masking of AES, *Selected Areas in Cryptography – SAC 2004,* Lecture Notes in Computer Science, vol. 3357, pp. 69–83, Springer-Verlag, 2004.
4. S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi: Towards Sound Approaches to Counteract Power-Analysis Attacks, *Advances in Cryptology – CRYPTO'99,* (M. J. Wiener, ed.), Lecture Notes in Computer Science, vol. 1666, pp. 398–412, Springer-Verlag, 1999.
5. C. Clavier, J.-S. Coron, and N. Dabbous: Differential Power Analysis in the Presence of Hardware Countermeasures, *Cryptographic Hardware and Embedded Systems – CHES 2000,* (Ç. K. Koç and C. Paar, eds.), Lecture Notes in Computer Science, vol. 1965, pp. 252–263, Springer-Verlag, 2000.
6. J.-S. Coron: Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems, *Cryptographic Hardware and Embedded Systems – CHES 1999,* (Ç. K. Koç and C. Paar, eds.), Lecture Notes in Computer Science, vol. 1717, pp. 292–302, Springer-Verlag, 1999.
7. K. Gandolfi, C. Mourtel, and F. Olivier: Electromagnetic Analysis: Concrete Results, *Cryptographic Hardware and Embedded Systems – CHES 2001,* (Ç. K. Koç, D. Naccache, and C. Paar, eds.), Lecture Notes in Computer Science, vol. 2162, pp. 251–261, Springer-Verlag, 2001.
8. J. D. Golić and R. Menicocci: Universal Masking on Logic Gate Level, *Electronics Letters* **40(9)**, pp. 526–527 (2004).
9. L. Goubin and J. Patarin: DES and Differential Power Analysis – The Duplication Method, *Cryptographic Hardware and Embedded Systems – CHES 1999,* (Ç. K. Koç and C. Paar, eds.), Lecture Notes in Computer Science, vol. 1717, pp. 158–172, Springer-Verlag, 1999.
10. Y. Ishai, A. Sahai, and D. Wagner: Private Circuits: Securing Hardware against Probing Attacks, *Advances in Cryptology – CRYPTO 2003,* (D. Boneh, ed.), Lecture Notes in Computer Science, vol. 2729, pp. 463–481, Springer-Verlag, 2003.
11. F. Klug, O. Kniffler, B. M. Gammel: Rechenwerk und Verfahren zum Ausführen einer arithmetischen Operation mit verschlüsselten Operanden, *German Patent DE 10201449 C1*, Jan. 16, 2002.
12. P. C. Kocher, J. Jaffe, and B. Jun: Differential Power Analysis, *Advances in Cryptology – CRYPTO'99,* (M. J. Wiener, ed.), Lecture Notes in Computer Science, vol. 1666, pp. 388–397, Springer-Verlag, 1999.
13. S. Mangard: Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness, *Topics in Cryptology – CT-RSA 2004,* (T. Okamoto, ed.), Lecture Notes in Computer Science, vol. 2964, pp. 222–235, Springer-Verlag, 2004.
14. S. Mangard, T. Popp, and B. M. Gammel: Side-Channel Leakage of Masked CMOS Gates, *Topics in Cryptology – CT-RSA 2005,* (A. Menezes, ed.), Lecture Notes in Computer Science, vol. 3376, pp. 351–365, Springer-Verlag, 2005.
15. T. S. Messerges: Securing the AES Finalists Against Power Analysis Attacks, *7th International Workshop on Fast Software Encryption – FSE 2000,* (B. Schneier, ed.), Lecture Notes in Computer Science, vol. 1978, pp. 150–164, Springer-Verlag, 2001.
16. T. S. Messerges, E. A. Dabbish, and L. Puhl: Method and Apparatus for Preventing Information Leakage Attacks on a Microelectronic Assembly, *US Patent 6,295,606*, Sept. 25, 2001, (available at `http://www.uspto.gov/`).

17. T. S. Messerges, E. A. Dabbish, and R. H. Sloan: Power Analysis Attacks of Modular Exponentiation in Smartcards, *Cryptographic Hardware and Embedded Systems – CHES 1999,* (Ç. K. Koç and C. Paar, eds.), Lecture Notes in Computer Science, vol. 1717, pp. 144–157, Springer-Verlag, 1999.
18. T. S. Messerges, E. A. Dabbish, and R. H. Sloan: Examining Smart-Card Security under the Threat of Power Analysis Attacks, *IEEE Transactions on Computers*, **51(5)**, pp. 541–552, 2002.
19. J. M. Rabaey: *Digital Integrated Circuits,* Prentice Hall, 1996, ISBN 0-13-178609-1.
20. A. Shamir: Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies, *Cryptographic Hardware and Embedded Systems – CHES 2000,* (Ç. K. Koç and C. Paar, eds.), Lecture Notes in Computer Science, vol. 1965, pp. 71–77, Springer-Verlag, 2000.
21. K. Tiri and I. Verbauwhede: Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology, *Cryptographic Hardware and Embedded Systems – CHES 2003,* (C. D. Walter, Ç. K. Koç, and C. Paar, eds.), Lecture Notes in Computer Science, vol. 2779, pp. 137–151, Springer-Verlag, 2003.
22. K. Tiri and I. Verbauwhede: A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation, *Proc. of Design, Automation and Test in Europe Conference – DATE 2004,* IEEE Computer Society, pp. 246–251, 2004.
23. E. Trichina: Combinational Logic Design for AES SubByte Transformation on Masked Data, Cryptology ePrint Archive, Report 2003/236 (available at `http://eprint.iacr.org/`).