A Secure D Flip-Flop against Side Channel Attacks

Bruno Vaquie, Sébastien Tiran, Philippe Maurine

To cite this version:

Bruno Vaquie, Sébastien Tiran, Philippe Maurine. A Secure D Flip-Flop against Side Channel Attacks. PATMOS: Power And Timing Modeling, Optimization and Simulation, Sep 2011, Madrid, Spain. pp.331-340, 10.1007/978-3-642-24154-3_33 . lirmm-00762027

HAL Id: lirmm-00762027

https://hal-lirmm.ccsd.cnrs.fr/lirmm-00762027v1

Submitted on 14 Sep 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A Secure D Flip-Flop against Side Channel Attacks

Bruno Vaquie, Sebastien Tiran, and Philippe Maurine

LIRMM UMR 5506-CNRS
161, Rue Ada, 34085 Montpellier, France
firstname.lastname@lirmm.fr

Abstract. Side Channel Attacks (SCA) are a serious threat against security of cryptographic algorithms. Most of the countermeasures proposed to protect cryptosystems against these attacks, are efficient but present a significant area and power consumption overhead. The registers being the main weakness of cryptosystems, the source of leaks the more easily exploitable, we proposed a secure DFF which reduces leaks. In this paper, we present this countermeasure which considerably increases the robustness of cryptographic algorithms against side channel attacks. Moreover, the area and power overhead of our secure DFF in a cryptosystem is attractive.

Keywords: Side-Channel Attacks, hardware countermeasure, Secure D Flip-Flop, Data Encryption Standard (DES).

1 Introduction

Since Differential Power Analysis (DPA) [1], a lot of hardware countermeasures have been proposed to protect cryptographic devices against Side Channel Attacks (SCA). SCA are efficient because they allow the attackers to find secret keys of cryptographic algorithms by correlating processed data and side channel informations such as computing time, electric consumption or electromagnetic emissions. For example, Differential Power Analysis is based on the analysis of dependencies between intermediate data computed by an algorithm and the current consumption. By knowing the algorithm, DPA allows linking the current measured in the device to a theoretical model of power consumption in order to find the secret key. This kind of attack is very powerful because it requires few resources and little technical knowledge.

To protect the cryptographic devices against the SCA, designers have developped coutermeasures. The goal of a countermeasure is to remove this correlation by masking or hiding the internal data activity of cryptographic devices. We can sort the countermeasures into three categories:

- **redundant logics**
  Such secure logics aim at normalizing the power consumption by rendering the activity rate of all nets in the design constant and independent of the

J.L. Ayala et al. (Eds.): PATMOS 2011, LNCS 6951, pp. 331–340, 2011.
© Springer-Verlag Berlin Heidelberg 2011

processed data. This is typically acheived by adopting dual or triple rail encoding of data [2–4].

- **randomisation**
  The masking countermeasure aims at rendering all intermediate values of the algorithm processed by the secure integrated circuit (IC) unpredictable by an attacker. This is typically achieved by mixing the input data with random data that are unknown for the attackers. There are two types of masking:
  - boolean masking : it is mainly used in symmetric algorithms. It consists in applying a XOR between the data and a random number generated on chip at each computations [5].
  - arithmetic masking : this type of masking is mainly used in asymmetric algorithms. This countermeasure uses the algebraic structure of the algorithm by adding random values to sensitive data [6].
- **desynchronisation**
  An underlying assumption to all SCA is that all attackable intermediate values processed by a secure IC are always computed at the same time. The goal of desynchronisation based countermeasures is to break this assumption by ramdomly spreading the critical computations in time. Ending so, Random Process Interrupts (RPI) [7] or random clock frequency [8] have been proposed as efficient countermeasures.

Despite their efficiency, the main drawback of these countermeasures is their area and power consumption overheads (Table 1). Such overheads forbid the use of such countermeasures in several applications like secure RFID tags or other low cost or low power products. It is thus mandatory to develop low power and low area overhead countemeasures.

Table 1. Area overhead of several hardware countermeasures applied to cryptosystems

Countermeasure	Area
Sense Amplifier Based Logic (SABL) [2]	73%
Wave Dynamic Differential Logic (WDDL) [3]	240%
Secure Triple Track Logic (STTL) [4]	455%
Boolean Masking [5]	$\geq$ 100%

In this paper, we propose the use of secure D Flip-Flop (DFF). The D Flip-Flop, as explained in section 2, constitutes the main source of leakage.

2 Cryptographic Devices Leakages

In this paper, we focus on symmetrical cryptosystems. During a cryptographic computation, sources of leaks are multiple, and occur at specific times. However, we may highlight the two most important ones.

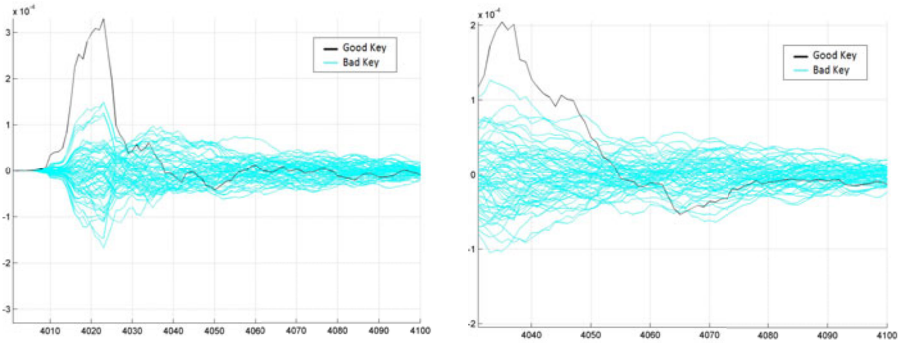
The main one is undoubtly the DFF banks or registers. Several reasons explain this fact. First, they usually sample, at each clock edge (thus in a perfectly synchronised way), either in a slave or master stage, the intermediate values targetted by the attackers.

Second, their power consumption significantly differs depending on if the data to be sampled is the opposite to that sampled during the previous rising edge of the clock or not. Indeed, if D has changed during the last clock cycle, then both master and slave have to switch, while none switch if D has been keep constant during the last clock cycle.

As a result, the amplitude of the current to be supplied to the secure IC, during an edge of the clock, is proportional to the number of DFF that have updated their content. This gives rise to the so called Hamming Distance Model [1].

The second main source of leakage is the first logic layers of standard cells after the DFF. Indeed, the switching activity of these gates is highly correlated to that of DFF and also remains quite synchronous [9]. Note however that this second source is less significant than the other.

Figure 1 gives evidences of this. It represents the difference of means (DoM) [1] after a simulated DPA, considering (a) a time windows embedding the switching of both DFF and the first layers of cells, and (b) a time windows that embed only the switching of the first layers of gates. As shown, it is necessary to process respectively 100 and 1500 power traces to disclose the key when considering or not the DFF activity.



(a) Switching of DFF and gates

(b) Switching of gates

Fig. 1. Difference of Means (a) after 100 traces - (b) after 1500 traces

So DFF are the critical security issue in a CMOS cryptoprocessor. In order to provide low power and low area countermeasures, we introduce below a secure DFF.

3 Secure D Flip-Flop

3.1 Secure DFF Implementation

To normalize the power consumption, we propose to double the master-slave stage (DFF1 and DFF2) and to add a detector-generator of switching. This latter block detects switches in the DFF1, and provokes a switch in DFF2, when DFF1 does not switch.

As shown Figure 2, the detector-generator of switching is built so that at the clock's rising edge:

- when $Q1 \neq D1$, the DFF 1 switches.
- when $Q1 = D1$, the DFF 2 switches.

As a result, independently of the data processed by the secure DFF, there is always one and only one switching. Such a behaviour results in normalizing the power consumption of sequential elements as dual rail logic does for combinational elements.

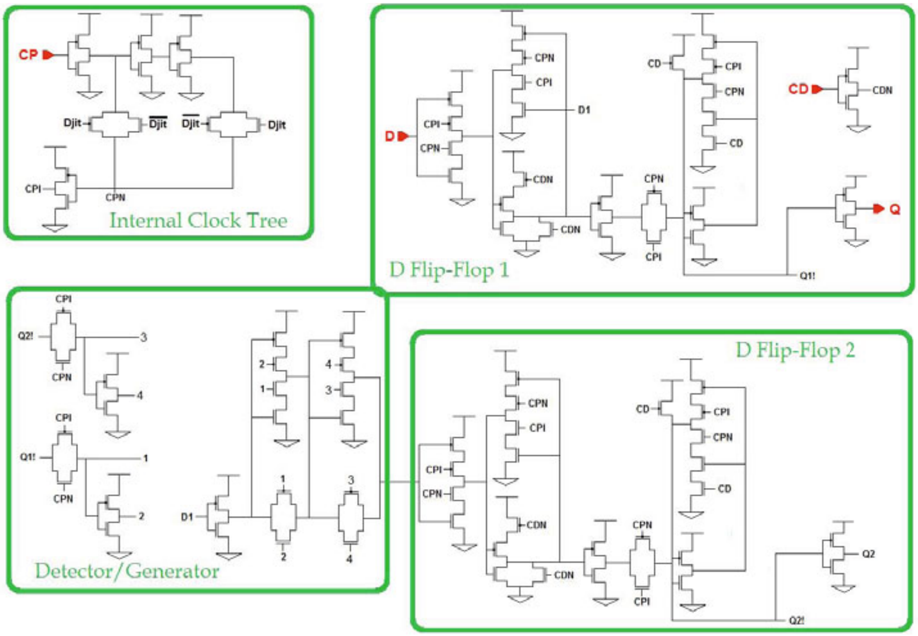


Fig. 2. Implementation of the secure D Flip-Flop

To go further, we also propose to add a jitter in the internal clock tree of our D Flip-Flop to improve its robustness. The figure 3 shows our internal clock tree with a jitter. The figure in full line is a standard internal clock tree while the dotted line shows our modifications.

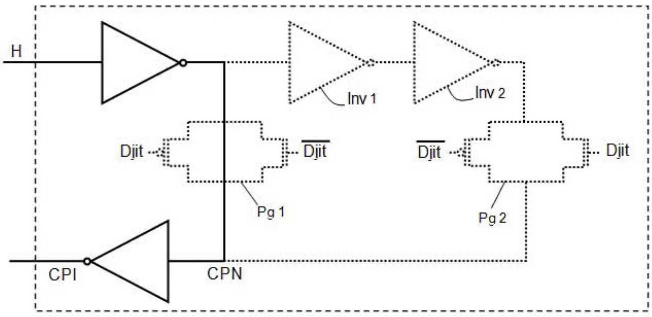


Fig. 3. clocktree with jitter of the D Flip-Flop

The jitter is composed of two inverters (Inv1 and Inv2) and two path gates (Pg1 and Pg2). The two path gates are controlled in phase opposition by $Djit$ and $\overline{Djit}$ by complementary. This signal is provided by a True Random Number Generator (TRNG).

When the signal Djit is low, the path gate Pg1 is closed and the path gate Pg2 is opened. The jitter is desactivated and the clock tree works like a standard clock tree (full line). When the signal Djit is high, the path gate Pg1 is opened and the path gate Pg2 is closed. The jitter is activated and the signal H goes through the two inverters Inv1 and Inv2 (dotted line).

Therefore, thanks to the signal Djit, we can modulate the time delay of the clock tree. This delay can take two distinct values, depending on the number and the size of inverters used to generate the signal CPI; which is two or four in our clock tree. The delay is well below the clock period. In our secure DFF, it is about half the propagation delay between input signal H and the Q output of a standard D Flip-Flop, that is to say between 50 ps and 100 ps for the 130 nm technology under consideration.

The jitter has two effects on the security.

- While the attacker captures the traces of power consumption, the jitter spreads in time and wreathes the traces.
- Because of the variation in the response time of the output of the DFF, the consumption of first layers of gates is desynchronized.

The jitter can therefore improve the robustness of cryptosystems by reducing leakages both in the DFF and in the first layers of gates.

3.2 Standard Characterisation

We wish to know the cost in area, consumption and timing of our secure D Flip-Flop, compared to a D Flip-Flop without countermeasures.

Area and power consumption considerations. We estimated that the surface of our secure DFF is four times bigger than that of a standard DFF. The power consumption has been simulated. Results show it is six time bigger than that of a standard DFF. That can be explained by the addition of a second master-slave stage, of the logic circuit detector/generator and of the jitter. the latter considerably increases the power consumption. In comparison, the same secure DFF without the jitter ability consumes three times more than a standard DFF, due to high switching activity.

Timing Considerations. Tables 2, 3, and 4 give timing metric comparisons between our secure DFF and a standard DFF for the 130 nm technology.

Table 2. Clock to Output Time

Standard DFF	→	85 to 97 ps
Secure DFF with inactive jitter	→	180 to 205 ps
Secure DFF with active jitter	→	296 to 317 ps

Table 3. Setup Time

τ_H τ_D	50 ps	100 ps	150 ps	200 ps
50 ps	46 365 245	40 360 230	46 350 225	41 350 160
100 ps	51 370 250	55 360 238	51 356 230	45 354 225
150 ps	65 375 250	61 370 240	56 3365 235	61 360 231
200 ps	71 385 201	66 376 195	61 367 180	67 360 176

Table 4. Hold Time

τ_H τ_D	50 ps	100 ps	150 ps	200 ps
50 ps	-25 36 155	-20 50 171	-16 56 175	-11 61 180
100 ps	-31 31 150	-26 46 155	-21 51 170	-16 55 175
150 ps	-46 25 135	-31 31 150	-36 46 155	-31 50 160
200 ps	-40 21 130	-36 26 136	-41 41 150	-36 44 155

Table 2 shows the clock to output (Ck to Q) time for a DFF without countermeasures and our secure DFF with jitter active or not. Compared to a standard DFF, the Ck to Q time for our secure DFF is two time bigger when the jitter is inactive and three times when it is active.

Tables 3 and 4 display respectively the setup and the hold times versus the rise time of the clock and the input D of the DFF. In each box of the tables, the first line represents the setup or the hold time for a standard DFF, the second represents our secure DFF with inactive jitter, and the third represents our secure DFF with active jitter.

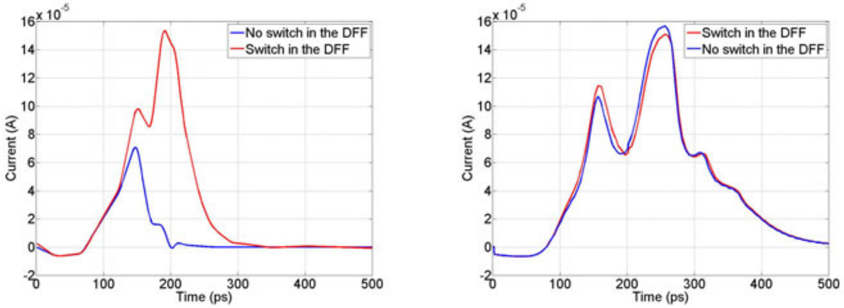
As a result of this comparison, we may conclud that our secure DFF prevents some acceptable timing metrics but exhibits a significant power overhead at cell. However, this overhead remains small compared to that reported on Table 1 for a whole cryptosystem.

3.3 Secure Characterisation

To evaluate the robustness of our DFF, we designed a Data Encryption Standard (DES) [10] with our secure DFF using a 130nm technology.

Area and Power Consumption Considerations. We want to know the area and power consumption overhead of our secure DFF in an algorithm like the DES. We estimated that the surface of a DES with our secure DFF is 30% bigger considering that of a DES with standard DFF. Results show that the power consumption is also 22% bigger compared to a DES with standard DFF. Once again, these values have to be compared to that of Table 1.

Power Consumption Model. Figures 4 and 5 show the impact of our countermeasure.



(a) Standard DFF

(b) Secure DFF without jitter

Fig. 4. Power consumption model

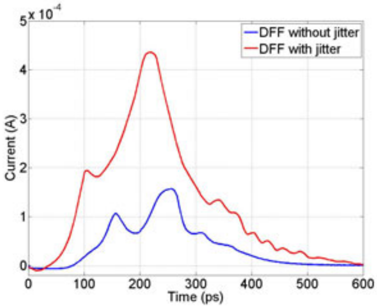


Fig. 5. Power consumption model of our DFF with jitter or not

Figure 4 shows the differences in power consumption model between a standard DFF (a) and our secure DFF (b). In (a), there are two distinct power consumption models: the red line is when the DFF switches and the blue continues dash is when the DFF does not switch. In (b), both red and blue lines are the same; the power consumption models are identical. As shown, the addition of a second master slave stage quasi normalise power consumption of our secure DFF.

Figure 5 shows the power consumption model of our secure DFF with jitter. It represents the mean of several hundred power consumption traces. Compared to Figure 4, we notice that the power consumption is spreaded in time due to the effect of the jitter.

Evaluation Against Side Channel Attacks. In order to estimate the robustness of our countermeasure, we attacked a DES with our secure DFF with three different side channel attacks. We applied a Differential Power Analysis (DPA) [1], a Correlation Power Analysis (CPA) [11], and a Mutual Information Analysis (MIA) [12] with a Hamming Distance (HD) model.

We designed three different DES in technologie 130 nm:

- a standard DES without any countermeasure.
- a DES with our secure DFF
- a DES with three versions of our secure DFF, each one is characterized by a specific jitter value.

Table 5. Robustness Comparisons on SCA

	DPA		CPA		MIA	
	MTD	Stability	MTD	Stability	MTD	Stability
Standard DES	96	593	98	606	970	1680
DES with secure DFF	832	10502	490	2472	3512	15230
DES with 3 different secure DFF	504	39150	492	27350	2309	13223

Table 5 shows the comparison of results obtained for the three DES, respectively against simulated DPA, CPA, and MIA. The traces used in these attacks are without noise and are obtained thanks to the simulation tool NanoSim. The Minimum Trace to Disclosure (MTD) is defined as the minimal number of traces needed to correctly find the secret key. The stability is the number of traces required to recover the full key at least 100 consecutive times. The latter metric suggests that the secret key is definitely broken.

According to Table 5, we can observe that the DES with our secure DFF offers a better resistance against DPA, CPA, and MIA than the DES with standard DFFs. Furthermore, the addition of two more DFF with different jitter considerably increases the robustness on the DES against DPA and CPA. These results highlight the importance of using DFF with different jitters in DES.

To go further, we wanted to estimate the impact of noise on the SCA results. We added a Gaussian noise of mean zero and Variance V equal to a percentage of the maximum peak current of the DES. We reapplied simulated DPA and CPA. Table 6 and Table 7 show the results of the attacks versus the percentage of noise added in the traces.

Table 6. Stability on traces with noise on DPA

% noise, V=	0,15%	1,5%	15%	30%	50%
Standard DES	605	602	1203	2032	3032
DES with secure DFF	10510	11000	15000	-	-
DES with 3 different secure DFF	40000	41000	-	-	-

Table 7. Stability on traces with noise on CPA

% noise, V=	0,15%	1,5%	15%	30%	50%
Standard DES	637	673	853	1873	4324
DES with secure DFF	2500	3000	13000	-	-
DES with 3 different secure DFF	27000	29000	-	-	-

According to Table 6 and Table 7, we can see that the addition of noise complicates the attacks. The attacks become ineffective on the DES with our secure DFF when the noise reaches a certain level, 30% for the DES with our secure DFF and 15% for the DES with 3 different secure DFF.

In completing, the element which breaks in first in the DES despite our countermeasure is the first layers of gates after our secure DFF.

4 Conclusion

Security is a major concern in many applications. To offer a high level of security, many countermeasures have been proposed and proven efficient. However, most of them are impacted by extremely large area and power consumption overheads. As a result, they cannot be used in low power applications such as RF tags. Within this contrast, we proposed a secure DFF to indrease significantly the level of security of low power and secure products. Its use implies a power overhead of 22% only.

References

1. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
2. Tiri, K., Akmal, M., Verbauwhede, I.: A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards. In: Proceedings of 28th European Solid-State Circuits Conf. ESSCIRC 2002 (2002)
3. Tiri, K., Verbauwhede, I.: A Logic Level design methodology for a secure DPA resistant ASIC or FPGA implementation. In: Proceedings of DATE 2004, pp. 246–251 (February 2004)
4. Lomne, V., Maurine, P., Torres, L., Robert, M.: Evaluation on FPGA of Triple Rail Logic Robustness against DPA and DEMA. In: DATE, pp. 634–639 (2009)

5. Standaert, F.-X., Rouvroy, G., Quisquater, J.-J.: FPGA Implementations of the DES and Triple-DES Masked Against Power Analysis Attacks. In: Proceedings of FPL 2006 (2006)
6. Coron, J.-S., Goubin, L.: On Boolean and Arithmetic Masking against Differential Power Analysis. In: Paar, C., Koç, Ç.K. (eds.) CHES 2000. LNCS, vol. 1965, pp. 231–237. Springer, Heidelberg (2000)
7. Clavier, C., Coron, J.-S., Dabbous, N.: Differential Power Analysis in the Presence of Hardware Countermeasures. In: Paar, C., Koç, Ç.K. (eds.) CHES 2000. LNCS, vol. 1965, pp. 252–263. Springer, Heidelberg (2000)
8. Akkar, M.-L., Bévan, R., Dischamp, P., Moyart, D.: Power analysis, what is now possible... In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 489–502. Springer, Heidelberg (2000)
9. Suzuki, D., Saeki, M., Ichikawa, T.: DPA Leakage Models for CMOS Logic Circuits. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 366–382. Springer, Heidelberg (2005)
10. National Bureau of Standards, Data Encryption Standard. Federal Information Processing Standards Publication 46 (January 1977)
11. Brier, E., Clavier, C., Olivier, F.: Correlation Power Analysis with a Leakage Model. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg (2004)
12. Gierlichs, B., Batina, L., Tuyls, P., Preneel, B.: Mutual information analysis. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 426–442. Springer, Heidelberg (2008)