On selected issues of Boolean function application in symmetric key cryptography against side channel attacks

Kamaruzzaman Seman¹, Muhammad Fahim Roslan¹, Azni Haslizan Ab Halim², M Nor Azizi Syam Mohd Sayuti¹

¹Fakulti Kejuruteraan dan Alam Bina, Universiti Sains Islam Malaysia
²Fakulti Sains dan Teknologi, Universiti Sains Islam Malaysia
¹drkzaman@usim.edu.my

Abstract. Boolean function plays a prominent role in building strong cryptography algorithm especially in symmetric block cipher. However, there may be some issues and conflicting criteria which prevent such a Boolean function to resist the algorithm to all known attacks. Within this work, the nonlinearity and correlation immunity issues of Boolean function is discussed followed by complementary counter measure against side channel attack especially differential power attack (DPA)

1. Introduction
Within the last few decades, cryptography has become one of the important elements as a secure measure for our confidential data in the digital world. One of its main components is Boolean function in which its application is to provide a better complexity to the algorithm, so it will not trivially breakable. Due to that, a large body of work have been dedicated to Boolean function alone. The most prominent one is the construction of Boolean function with specific properties such as high nonlinearity, high correlation immunity, high algebraic degree and balancedness. These characteristics are not in the same page in which some of them are contradicting each other. Hence most of the works are trying to optimize the construction so that the constructed Boolean function would have an optimum level in every property. Besides, the construction also need to match with the need of cryptography application.

A new type of attacks called as side channel attacks have been invented in recent years is believed to be far more efficient compared to classical attacks such as linear and differential attacks. This kind of attack depend on the leakage of hardware in which the adversary does not necessarily know the internal algorithm. Instead, they just record and analyze the leakage during the execution of the algorithm. Within this paper context, we would like to emphasize some of these issues regarding the implementation of Boolean function in symmetric key cryptography against side channel attacks. Several counter measures are also listed out. The next section is all about preliminaries concept relating Boolean function. In Section 3, the selected issues are listed out with the respective countermeasures. Last section will conclude the paper.

2. Preliminaries Concept
A Boolean function $f$ is a mapping of $n$-input variables of the field $\mathbb{F}_2^n$ to the base field $\mathbb{F}_2 = \{0,1\}$ which can be defined as $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$. There are $2^n$ different input form $\mathbb{F}_2^n$ which lead to the array of $2^n$ output known as the truth table of function $f$. The set of Boolean function $f$ of $n$ variables is denoted as $\mathcal{B}_n$ with the cardinality of $2^{2^n}$. Each Boolean function $f$ can be represented by two ways which are the truth table and algebraic normal form (ANF). The truth table as mentioned before is the
array of output corresponding to the input arrange in lexicographically order. While the ANF is a polynomial representation of $f$ of the form

$$f = a_0 + a_1 x_1 + a_2 x_2 + \cdots + a_n x_n + a_{1,2} x_1 x_2 + \cdots + a_{i,j} x_i x_j + \cdots + a_{1,2,\ldots,n} x_1 x_2 \cdots x_n$$  \hspace{1cm} (1)$$

There are several terms associate with the Boolean function $f$ such as support of $f$ which is defined as $\text{supp} = \{x \in \mathbb{F}_2^n | f(x) = 1\}$. The size of support is denoted as the Hamming weight, $w_h(f)$. Given any two function $f,g \in \mathbb{F}_2^n$, the distance is quantify as the size of set $d(f,g) = |\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\}|$. Another representation of Boolean function is in term of Walsh spectrum that can be derived from the Walsh-Hadamard transform of the form,

$$W_f(y) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)\overline{y}(x,y)}, y \in \mathbb{F}_2^n$$  \hspace{1cm} (2)$$

In evaluating function $f$, a group of parameters called as cryptography properties are often use. The most essential are nonlinearity, balancedness, algebraic degree and correlation immunity. The nonlinearity is defined as the distance between any function $f$ to the set of all affine function $\ell$. The evaluation can be expressed in term of Walsh-Hadamard transform as follows,

$$N_f = 2^{n-1} - \frac{1}{2} \max |W_f(y)|$$  \hspace{1cm} (3)$$

The range of $N_f$ start from value 0 which indicate affine function and bounded by $N_f = 2^{n-1} - 2^{n-1}$. Any function $f$ achieve this maximum value is called as Bent function, the function with maximum nonlinearity. Balancedness indicates the function $f$ has balance number of 0 and 1 in its truth table. However, using Walsh-Hadamard transform, the balanced function can be trace if $W_f(\overline{0}) = 0$. The algebraic degree is defined by using ANF. The largest product term in ANF with non-zero coefficient is defined as the algebraic degree of function $f$. The last one, function $f$ is correlation immunity or order $k$, $CI_k$ if the output of the function is statistically independent of the combination of any $k$ of its output. It also related to Walsh-Hadamard transform as follows,

$$W_f(y) = 0, \text{ for } 1 \leq w_a(y) \leq k$$  \hspace{1cm} (4)$$

3. Some Selected Issues

Side channel attacks includes several types of attack which are depend on the type of leakages. Type of attack that have been given a spotlight are differential power attack due to easy hardware setup and implementation. Other attacks are acoustics attack and electromagnetics attack. The successful of the attack somehow depend on the implemented Boolean function inside the algorithm. Within this section, three issue are presented which follows by its countermeasure. The first one related to nonlinearity of Boolean function $f$ implemented in substitution box. A dedicated parameter has been developed in order to quantify the strength of S-Box against DPA. The second one is related on how the S-Box is implemented and the effect of its on power leakages. An alternative method make the algorithm to less dependent on the action of predefined table store in the hardware. The last one is specific to variation of input and its corresponding output result.

3.1. Nonlinearity of Substitution Box

Substitution Box or called as S-Box are the composition of several function $f_i$. In formal, it received $n$-input and produced $m$-output. It also can be represented as function $S: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ where the composition can be represent as $S = \{f_i | i = 1, 2, \ldots, m\}$. Some literatures are consider the function $f_i$ as the coordinate function of $S$. The measure of nonlinearity are taken on all coordinate function in which the minimum one is consider the nonlinearity $N_f$ of the S-Box. The AES S-Box that received 8-bit input and produced 8-bit output have the nonlinearity of 112. Other construction found in the
literature constructed an AES class S-Box with lower value of nonlinearity [1]–[5]. The main issue with nonlinearity of S-Box against DPA was first introduced by [6] in which the authors claimed the higher the nonlinearity, or the better shielded against linear cryptanalysis, the more vulnerable the algorithm against DPA. Besides that, in the same paper the author point out the Bent function which achieve maximum nonlinearity $N_f$ cannot by definition resist DPA. On the opposite side, the affine function would be the better choice in preventing DPA though it highly risk the algorithm against linear cryptanalysis. In order to quantify the S-Box whether it is better shielded against DPA, the notion of transparency order (TO) was introduced in the same work. TO would have lower value if the S-Box are better shielded while higher value for less secure S-Box against DPA. Due to this conflicting issue, a large amount of work has been published in which the objective is to find the best optimization between nonlinearity $N_f$ and the TO. Some of these works can be found in [7], [8], [9] and [10]. However, a decade after the first work on TO, another author claimed they may be some redundancy in TO definition. Hence, the author presented in [11] the modified TO.

Even though TO may redefined the criteria of secure S-Box implementation, it cannot be avoided to say lower nonlinearity S-Box would open to risk to linear cryptanalysis. An alternative way to implement high nonlinearity S-Box with better DPA security is by modifying the flow of the algorithm. In other word, we manipulate the output leakages so that the secret key is untraceable. In [12], an alternative of predefined table is presented in implementing S-Box. This method called as composite field arithmetic which make the algorithm less dependent on the large table. In addition, it somehow transform the nonlinear of the S-Box into the set of linear operation while maintaining the nonlinear relationship between input and output. In AES, the methods simply transfer the heavy operation in large field $F_2^{2^8}$ or can be noted as $GF(2^8)$ to the composite field $GF((2^4)^2)$. Some work extend the composition to the lowest base field $GF((2^2)^5)$ which can be found in [13]. As the objective is to optimize the power usage, it also can be applied to counter the risk of DPA. This has been done in [14] in which the authors implementing composite field arithmetic for S-Box in AES and also the MixColumn operation. Another work found in [15] combine the method of composite field arithmetic with masking method.

3.2. Correlation Immunity of Boolean function
Correlation immunity of degree $k$ denoted as $CI_k$ is one of the important properties in constructing good linear combiner in stream cipher. This type of function has the property of maintaining the same output distribution even though some of the input variables are fixed. Several works have reported that correlation immune function has the ability to thwart side channel attacks by becoming the alternative of masking methods which has huge drawbacks in term of implementation cost [16]. However, high correlation function are reported to have low algebraic degree which is susceptible to Berlekamp-Messy Attack [17]. The bound of any $CI_k$ function is known as Siegenthaler’s bound that state that any $k$-resilient function ($0 \leq k < n - 1$) has algebraic degree smaller than or equal to $n - k - 1$. In addition, any $(n-1)$-resilient function is actually an affine function. This also lead to another problem which is low algebraic immunity. Any correlation immune function can help reduce the threat of side channel attacks especially DPA in two ways, 1) by applying leakage squeezing method [18] and 2) uses rotating S-Box masking for block cipher. Several works have been dedicated to search for any Boolean function that can optimize the correlation immunity and other properties such as algebraic degree. Some of them can be found in [19] and [7].

4. Conclusion
This paper explore some of the issue or limiting condition of implementing Boolean function in resisting the algorithm from side channel attacks especially DPA. Two properties have been discussed which are nonlinearity and correlation immunity. Nonlinearity of Boolean function $f$ is conflicting with the parameter transparency order (TO). Bent function which has maximum nonlinearity is reported to have worst TO which in definition not good implementation against DPA. Besides that, high correlation immunity is said not to have good algebraic degree which susceptible to Berlekamp-Messy Attack.
References

[1] H. Isa, N. Jamil, and M. R. Z. Z’aba, “Construction of Cryptographically Strong S-Boxes Inspired by Bee Waggle Dance,” New Gener. Comput., vol. 34, pp. 221–238, 2016.

[2] M. F. Roslan, K. Seman, A. H. Ab Halim, and M. N. S. Mohd Sayuti, “Current Implementation of Advance Encryption Standard (AES) S-Box,” J. Fundemental Appl. Sci., vol. 9, no. 4S, pp. 518–542, 2017.

[3] T. Farah, R. Rhouma, and S. Belghith, “A novel method for designing S-box based on chaotic map and Teaching–Learning-Based Optimization,” Nonlinear Dyn., vol. 88, no. 2, pp. 1059–1074, 2017.

[4] T. Zhang, C. L. P. Chen, L. Chen, X. Xu, and B. Hu, “Design of Highly Nonlinear Substitution Boxes Based on I-Ching Operators,” IEEE Trans. Cybern., vol. PP, pp. 1–10, 2018.

[5] M. Ahmad, D. Bhatia, and Y. Hassan, “A Novel Ant Colony Optimization Based Scheme for Substitution Box Design,” Procedia - Procedia Comput. Sci., vol. 57, pp. 572–580, 2015.

[6] E. Prouff, “DPA Attacks and S-Boxes,” in 12th International Workshop, FSE 2005, 2005, pp. 424–441.

[7] S. Picek, B. Ege, L. Batina, D. Jakobovic, L. Chmielewski, and M. Golub, “On using genetic algorithms for intrinsic side-channel resistance: The case of AES S-box,” Proc. First Work. Cryptogr. Secur. Comput. Syst. ACM, pp. 13–18, 2014.

[8] L. Fan, Y. Zhou, and D. Feng, “A fast implementation of computing the transparency order of S-boxes,” Proc. 9th Int. Conf. Young Comput. Sci. ICYCS 2008, pp. 206–211, 2008.

[9] B. Mazumdar, D. Mukhopadhyay, and I. Sengupta, “Constrained search for a class of good bijective S-boxes with improved DPA resistivity,” IEEE Trans. Inf. Forensics Secur., vol. 8, no. 12, pp. 2154–2163, 2013.

[10] B. Mazumdar, D. Mukhopadhyay, and I. Sengupta, “Design and implementation of rotation symmetric S-boxes with high nonlinearity and high DPA resilience,” Proc. 2013 IEEE Int. Symp. Hardware-Oriented Secur. Trust. HOST 2013, pp. 87–92, 2013.

[11] K. Chakraborty, S. Sarkar, S. Maitra, B. Mazumdar, D. Mukhopadhyay, and E. Prouff, “Redefining the transparency order,” Des. Codes, Cryptogr., vol. 82, no. 1–2, pp. 95–115, 2017.

[12] D. Canright, “A Very Compact S-Box for AES,” Ches 2005, pp. 441–455, 2005.

[13] C. Carlet and S. Guilley, “Correlation-Immune Boolean functions for easing counter measures to side-channel attacks,” Algebr. Curves Finite Fields Cryptogr. Other Appl., vol. 16, pp. 41–70, 2014.

[14] C. Carlet, “Boolean functions for cryptography and error correcting codes,” Boolean Model. methods Math. Comput. Sci. Eng., vol. 2, pp. 257–397, 2010.

[15] C. Carlet, J.-L. Danger, S. Guilley, and H. Maghrebi, “Leakage Squeezing of Order Two,” in International Conference on Cryptology in India, 2012, pp. 120–139.

[16] S. Picek, C. Carlet, D. Jakobovic, J. F. Miller, and L. Batina, “Correlation Immunity of Boolean Functions: An Evolutionary Algorithms Perspective,” GECCO ’15 Proc. 2015 Annu. Conf. Genet. Evol. Comput., pp. 1095–1102, 2015.