Stochastic Bitstream Computation for Enhanced Resistance to Against Power Analysis Attack

Jun Wu\textsuperscript{1a)}, Hengsi Qin\textsuperscript{1}, Yiyu Shi\textsuperscript{1}, Ho Joon Lee\textsuperscript{2}, Yong-Bin Kim\textsuperscript{2} and Minsu Choi\textsuperscript{1}

\textsuperscript{1} Department of Electrical and Computer Engineering
Missouri University of Science and Technology
Rolla, MO, USA
\textsuperscript{2} Department of Electrical and Computer Engineering
Northeastern University
Boston, MA, USA
\textsuperscript{a)} jw6t6@mst.edu

Abstract: Power analysis attacks explore the encrypted information by monitoring the power traces of physical crypto-systems. Among all published power analysis attacks, correlation power analysis (CPA) is the most effective attack that has been reviewed by many researchers recently. Meanwhile, various countermeasures have been proposed to against CPA attacks. In this work, a novel approach based on stochastic logics is proposed to enhance the resistance against CPA attacks. The probabilistic bitstreams, generated by encoders with random numbers, are used to represent binary logic states. The output bitstreams are converted back into the binary logics using decoders, ensuring the capability with other conventional logic functions. An 8-bit AES S-Box has been implemented using the proposed structure in VHDL and verified in ModelSim. Experimental result shows that three factors affect the accuracy of stochastic logic devices: the length of bitstreams for a given logic state, the decision weight of the encoders, and the repeat times of an input. A specified side-channel attack (SCA) standard evaluation FPGA board (SASEBO-GII) has been used for power measurement. Experimental results also demonstrate that the proposed design could effectively randomize the power consumption so that CPA attacks are not able to reveal the correct secret key.

Keywords: correlation power analysis (CPA), power analysis attacks, security, stochastic bitstream.

Classification: Integrated circuits.

References

1 Introduction

Securing cryptographic devices against various side channel attacks (SCA) has become a very attractive research topic in recent years along with the developments of information technologies. SCAs explore the security information (i.e., secret key) by monitoring the emitted outputs from physical crypto-systems. These outputs include execution timing, power consumptions, electromagnetic emissions, and even thermal/acoustic emanations [1].

Among many SCA approaches, differential power analysis (DPA) and correlation power analysis (CPA) are the most popular and effective attacks. Meanwhile, many SCA countermeasures were proposed, including Masked Dual-Rail Pre-charged Logic (MDPL) [3], Wave Dynamic Differential Logic (WDDL) [2], and Null Conventional Logic (NCL) [4, 5]. The CPA focuses on the dynamic power consumption that is dissipated during the transistors switching rather than static leakage power consumption. Therefore, this work presents a CPA countermeasure method based on cryptographic devices using stochastic bitstreams. Stochastic logic device was proposed in [6]. It has the advantages of simplifying the complex logic operations, great fault tolerance, and high security due to its high redundant and probabilistic encoding.

This work proposes a stochastic bitstream based implementation of the AES S-box, which is the key component of an AES cryptographic device. It validates the possibility of using stochastic bitstream logic in cryptographic devices by experimental results. It also shows that the resistance against CPA can be enhanced by using the proposed stochastic S-box design.
2 Stochastic Bitstream based Cryptographic Devices

Stochastic logic operates on probabilistic bitstreams, where the signal is encoded by the probability of obtaining a one or a zero from a given input signal [6]. The highly randomness property of bitstreams is helpful for cryptographic devices to avoid power analysis attacks and thus, to enhance security. Our proposed structure has good compatibility that could be used in different combinational logic core of encryption standards. In this work, an 8-bit AES S-box has been used for demonstration. The system diagram of the proposed structure is shown in Figure 1. In the following, we define HIGH and LOW to represent the states of binary logics in the input and output, while 1s and 0s to represent the states of the stochastic bitstreams. In Figure 1, the solid lines represent the conventional logic states, while the dash lines represent the stochastic bitstreams.

![System diagram](image)

Fig. 1: System diagram

To ensure the backwards compatibility, the input (i.e., plaintext) and output (i.e., ciphertext) of the proposed structure are in standard boolean logic. As Figure 1 shows, there are eight encoders, which generates stochastic bitstreams for each of the input data. The inputs of encoders are one bit from the input data and a 32-bit fixed-point random number (RN), which is ranging from 0 to 1. The random numbers are generated by combining the design of linear feedback shift register (LFSR) and cellular automata shift register (CASR) based pseudo-random number generators. This combined random number generator (RNG) has better bit independence, longer cycle length, and more unpredictable randomness [8]. The equation of encoders is

\[
E_o(i) = \begin{cases} 
1, & x = HIGH \text{ and } P_1 \geq RN, \\
1, & x = LOW \text{ and } P_0 \geq RN, \\
0, & x = HIGH \text{ and } P_1 < RN, \\
0, & x = LOW \text{ and } P_0 < RN, 
\end{cases} 
\]  

(1)

where \(x\) represents the input, \(P_1\) and \(P_0\) are the decision weight of the encoders, which are the probability of 1s and 0s in the bitstreams, respectively.
Note that $P_1 + P_0 = 1$ ($P_1 > 0, P_0 > 0$). The distribution of $P_1$ and $P_0$ defines the decision weight of encoders, which affects the performance of the proposed structure. The outputs of each encoder ($E_o$) are stochastic bitstreams that have the probability of $P_1$ to be '1' when its input is HIGH and the probability of $P_0$ to be '0' when its input is LOW. $RN$ represents the random number that is generated by the random number generators.

The outputs of all encoders, an 8-bit bitstream (i.e., $E_o(0)$ to $E_o(7)$), contain information of the plaintext and are fed into a combinational logic S-box. The outputs of the S-box are the encrypted information, which is also in bitstreams. Therefore, decoders are needed to obtain the ciphertext, which count the number of 1s to determine whether the present bitstream represents HIGH or LOW logic. The equation of decoder is

$$D_o(i) = \begin{cases} \text{HIGH}, & \frac{N_{a=1}}{N_{clk}} \geq 0.5, \\ \text{LOW}, & \frac{N_{a=1}}{N_{clk}} < 0.5, \end{cases}$$

where $N_{a=1}$ is the number of 1s in the input bitstreams of a decoder and $N_{clk}$ is the number of bitstream bits for an input logic state. $D_o$ is the output of decoder.

The present work analyzes two aspects of the proposed stochastic logic S-box: (1) functionality and (2) resistance to power analysis attacks, which will be discussed in the following sections.

3 Logic Validation

Stochastic logic introduces randomness and uncertainty into the data flow by its nature, which helps to avoid power analysis attacks. However, on the other hand, the accuracy of the implemented combinational logic has not been analyzed. For cryptographic devices, 100% accuracy is important. Three factors affect the accuracy of stochastic logic devices: the length of bitstreams for a given logic state, the decision weight of the encoders, and the repeat times of an input.

The proposed structure is implemented in VHDL and simulated using ModelSim. The output data are exported to a text file using VHDL textio package, and then, compared with the correct answers using a script. Using this method, errors can be located and the error rate can be analyzed as well. Figure 2 shows the error rate of the stochastic S-box for a number of decision weight at three different bitstream lengths with three different repeat times of an input. For each bitstream length, the error rate increases as $P_0$ increases. Increase in the difference between $P_0$ and $P_1$ means the bitstreams contains more randomness. $P_0 = P_1 = 0.5$ means complete randomness (the bitstreams contain no information), while $P_0 = 0, P_1 = 1$ means no randomness (same as the conventional binary logic). In Figure 2, more randomness results in a higher error rate. On the other hand, it is trivial to use no randomness in this work. The longer the bitstream for an input state is, the lower the error rate is. The more repeat times for an input, the lower the error rate is. However, this is a minor effect, as shown in Figure 2.
Based on the simulation results, there are several patterns lead the proposed structure to achieve nearly 100% accuracy. 1) Decision weight of \( P_0 = 0.1, \ P_1 = 0.9 \) with bitstream length of 512 or more clock cycles, and 2) \( P_0 = 0.05, \ P_1 = 0.95 \) with bitstream length of 256 or more clock cycles.

**Fig. 2: Error rate of stochastic bitstream S-box**

4 CPA Results

Besides ModelSim simulation, the proposed stochastic bitstream S-Box has been also verified using a specified SCA standard evaluation FPGA board (SASEBO-GII). It includes two FPGA cores to implement cryptographic logic and configuration logic separately. So the power traces from cryptographic core would not be affected by configuration circuit, increasing the effectiveness of power analysis attacks. CPA is more effective in revealing a secret key than DPA. CPA calculates the correlation coefficients between an estimated power model and the real measured power consumption. Since the power consumption of an integrated circuit can be estimated by the Hamming Distance (HD) between the current state and its consequential state[3]. The estimated power model is the Hamming Weight (HW) matrix of all outputs for all possible hypothesis keys. Once the correlation coefficients between the HW matrix and the measured power consumption matrix are calculated. The trace with the highest correlation coefficient is supposed to be correct secret key. We have described the detailed procedure of carrying a CPA attack in [7].

Figure 3 shows the result of the attempted CPA attack. The X-axis represents the length of a data window and Y-axis represents the correlation value for each key hypothesis. There would be total 256 possibilities for a 8-bit key. The correct key (63d) is plotted in black, while other hypothesis keys are plotted in grey. The correct key is buried by the other keys. There is no correlation coefficient trace that is significantly higher than the others. Therefore, it is difficult to know the correct secret key. This indicates that the stochastic bitstream S-box design is resistant to the CPA attacks. The same
CPA has conducted to a regular Boolean S-box design in [7], the attack is successful. The proposed stochastic bitstream method can enhance security against power analysis attacks without the need to completely re-design the core logic functional blocks. Therefore, the method in this work can be applied to many other devices when they require enhanced security.

![Fig. 3: CPA results of stochastic bitstream S-box](image)

5 Conclusions
This work presents a novel approach to enhance the security of cryptographic devices against the power analysis attacks. The proposed approach uses stochastic logics, which utilizes probabilistic bitstreams, to represent the binary logic states. The stochastic bitstream is generated by encoders with combination of CASR and LFSR based random number generators. The input and output signals of the core cryptographic component are the stochastic bitstreams, whose randomness makes it difficult to carry power analysis attacks. The output bitstreams are converted back to the conventional binary logic signals by decoders, to ensure compatibility with other logic functions. The functionality of the proposed design has been verified using an 8-bit AES S-box. The effects of decision weight, bitstream length, and input repeat times on error rates have been studied. Utilizing the two FPGAs included in the SASEBO-GII board, the configuration and cryptographic functions are able to be performed separately to ensure that the power trace measurements for CPA do not interfere with each other. The CPA result shows that the proposed approach enhances the resistance to against the CPA attack.