



Method to Estimate Transfer Characteristics of Side-Channel Waveform in Correlation Power Analysis

Hideaki Sone⁽¹⁾, and Yuichi Hayashi⁽²⁾

(1) Tohoku University, Sendai, Japan; ORCID: 0000-0002-9395-9987

(2) Nara Institute of Science and Technology, Ikoma, Nara, Japan; ORCID: 0000-0002-1160-8156

Correlation Power Analysis (CPA) [1] against cryptographic chip analyzes side-channel waveform which is caused from transient current of switching logic gate transistors (Figure 1). Generated transient waveform depends on number of inverting gates, and may differ according to characteristics of the transistors and surrounding circuit. The observed waveform after travel along power/ ground circuits is affected by the transfer characteristics within the chip or board, and resulting correlation decreases from calculated one [2].

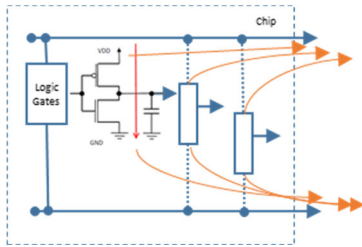


Figure 1. Transient Current and Propagation.

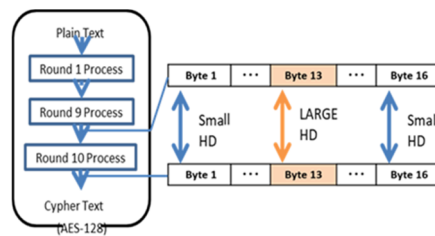


Figure 2. Controlled Transient in Encryption Processing.

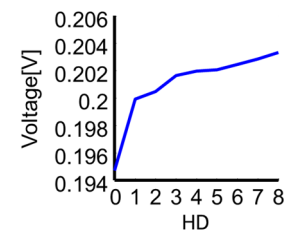


Figure 3. Relationship of voltage change and HD.

This report proposes a method to consider the transfer characteristics of the waveform from each switching gate as an approach to have precise correlation. Output and operation of each logic gate are determined by cipher algorithm, secret key, and processed plain text. From stand point to evaluate safety of the hardware, we know the cryptographic algorithm and can select the secret key and plain text. By selecting the text we change transient waveforms caused by the cipher process.

The side channel waveform reflects the number of transients, or Hamming Distance (HD) of previous/ current status, in operation of logic gates of corresponding byte register at a specified processing cycle. Figure 2 illustrates concept of schematic operation of AES encryption. When a suitable plain text is selected for a key of AES-128, 15 bytes among 16 bytes (128 bit) can be controlled to have minimized HD and only one byte has a large HD, thus we can observe the transient of gates for the targeted single byte at an intended process cycle. By analyzing observed waveform and calculated HD, we can estimate the characteristics of generation and propagation of transient waveform.

Figure 3 shows an example of the relationship of waveform changes and HD for the case that Byte 13 in Round 10 Process is observed. We should notice that the relationship is not linear in this figure.

By applying this method to select a single byte register to have large HD, we can estimate generation characteristics of transient waveform at gate transistors and transfer characteristics of the circuit, and the method may improve the correlation analysis of observed side channel waveform.

This work is supported by JSPS Kakenhi Grant JP21K03995.

Figures in this report are results by Mr. Takumi Sasaki as a part of his Master's Thesis in Tohoku University [3].

References

- [1] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," CHES 2004, Lecture Notes in Computer Science, 3156, pp. 16-29, Aug. 2004.
- [2] H. Sone, Y. Hayashi, "A Fundamental Study on Effect of Transfer Characteristics of Side-Channel Waveform in Correlation Power Analysis," 2023 URSI GASS, Th-P2E-PM3-16, August, 2023. doi: 10.46620/URSIGASS.2023.3608.JLPT6242
- [3] T. Sasaki, Y. Hayashi, T. Mizuki, H. Sone, "Efficient Analysis Method of EM Information Leakage from Cryptographic Devices Using Selecting Plaintexts," (in Japanese) SICE Tohoku Branch 50th Anniversary Seminar, C304, December 2014.