ABSTRACT

Side Channel Attacks (SCAs) have been employed to reveal the secret key of cryptographic algorithms implemented in hardware devices (crypto-devices) by analyzing the processed-data and their Physical Leakage Information (PLI). The processed-data can either be the plaintext or the ciphertext. The PLI includes power dissipation, electromagnetic interference, acoustic, temperature, and timing information. The Correlation based Attack (CbA) is the most commonly used SCAs. The CbA can be used to intercept the encryption process where the PLI can be correlated to the processed-data to reveal the secret key. On the other hand, in order to secure the secret key against the CbA, countermeasure techniques can be applied to reduce the correlation between the processed-data and the PLI. This thesis pertains to the investigation and implementation of highly efficient SCA as well as highly secured countermeasure techniques for crypto-devices such as smartphone, smartcards, wearable devices, and Internet of Things (IoT) applications. The countermeasure techniques are implemented with emphases on highly secure against power and electromagnetic based CbA with low overheads. Four main research works have been completed as follows:

First, we propose a Profiling through Relevance-Learning (PRL) technique on PLI to extract highly correlated PLI with processed-data, as to achieve a highly efficient yet robust SCAs. The nearest-neighbor *k*-NN variance clustering is used to reduce the sampling points of PLI by clustering the high variance sampling points and discarding the low variance sampling points of PLI measurements (traces). Subsequently, the relevance learning algorithm is adopted to learn the relevance factor for each clustered sampling point to quantify the degree of leakage associated with the secret key. Our proposed PRL technique successfully reduces 94.53%-to-98.19% of traces

when performing with different noise levels. By comparing with reported techniques which require >10^6 traces, our proposed PRL is ~2,000× more efficient in performing SCAs.

Second, we propose a highly-secured State-shift Local Clock (SsLC) countermeasure technique to hide the PLI against CbA SCAs. It embodies a finite state machine which can be employed to regularly shift the timing operation of cryptographic algorithm implementations. The power dissipation overhead is negligible and hence it is highly applicable for low power applications. Our proposed SsLC countermeasure technique features wide distribution of PLI in time domain, dissipates 2.77mW of power and emits 12.2mV/m of EM signal @ 2.4MHz. In comparison with the reported counterparts, the resistance of our proposed SsLC against SCAs is significantly improved as the number of power dissipation and EM traces to reveal the secret key has increased by >18× and >25× respectively.

Third, we propose an Authentication based Matrix-transformation cum Parallel-encryption implemented on an asynchronous Multicore Processor (AMP-MP) to achieve a high throughput and yet secure Advanced Encryption Standard based on Counter with Chaining Mode (AES-CCM). We employ the matrix multiplication in GF(2^8) computation to transform each message of 16 plaintexts into 1 plaintext, hence improving the authentication speed by 32× collectively at the transmitter and receiver. We further propose a key adjusting technique based on S-Box byte-key transformation to protect the key against pattern-based attack. Our proposed AMP-MP is realized on an 8-bit asynchronous 9-core processor fabricated based on 65nm CMOS process. The experimental results show that the throughput of authentication is 13.54Gbps while the throughput of the authentication and encryption collectively is 8.32Gbps, which are 17× and 70× faster than the reported counterparts. Based on the power dissipation and EM SCAs on our proposed AMP-MP, the secret key is unrevealed at 5×10^5 traces, which is ~17× more secured than the standard

ASIC AES-CCM implementation. With additional security feature of our key adjusting technique on 256 randomly generated secret keys, the 4 patterns within the keys are completely removed.

Fourth, we propose ultra-low power Nano-AES-128 encryption to secure Bio-Implant device applications with smallest gate counts of 1,745 gate counts which is 80.78% of reduction from 9,080 gate counts of conventional AES implementation. The encryption is performed based on byte based encryption which requires 21 clock cycles for each round operation. This implies our proposed Nano-AES-128 is 21× slower than conventional AES, requires only one clock cycle for each round. However, the power dissipation of our proposed Nano-AES-128 is reduced 8× and the SCAs resistance is increased by 9× when compared with conventional AES. Based on experimental results on FPGA implementation, the secret key is unrevealed with $> 10^6$ PLI measurements on advanced leakage power model to emulate data encryption of our proposed Nano-AES-128.

List of Publications

Journal

1. **A. A. Pammu**, K.-S. Chong, B.-H. Gwee, "A Highly-Secured Arithmetic Hiding cum Look-Up Table (AHLUT) based S-Box for AES-128 Implementation", *Advances in Science, Technology and Engineering Systems Journal*, vol. 2, no. 3, pp. 420-426, 2017.
2. **A. A. Pammu**, K. S. Chong, Yi Wang and B. H. Gwee, "A Highly Efficient Side Channel Attack with Profiling through Relevance Learning on Physical Leakage Information," *IEEE trans. On Dependable Secure Computing*, 2018, major revision, May 2018.
3. **A. A. Pammu**, W. G. Ho, K. Z. L. Ne, K. S. Chong and B. H. Gwee, "A High Throughput and Secure Authentication-Encryption AES-CCM Algorithm on Asynchronous Multicore Processor," *IEEE trans. on Information Forensics & Security*, 2018, major revision, May 2018.

Conference

1. **A. A. Pammu**, K. S. Chong, K. Z. L. Ne and B. H. Gwee, "High Secured Low Power Multiplexer-LUT Based AES S-Box Implementation," *2016 International Conference on Information Systems Engineering (ICISE)*, Los Angeles, CA, 2016, pp. 3-7. **(Best Presenter Award, California, Los Angeles, USA)**
2. **A. A. Pammu**, K. S. Chong and B. H. Gwee, "Secured Low Power Overhead Compensator Look-Up-Table (LUT) Substitution Box (S-Box) Architecture," *2016 IEEE International Conference on Networking, Architecture and Storage (NAS)*, Long Beach, CA, 2016, pp. 1-7.
3. **A. A. Pammu**, K. S. Chong, W. G. Ho and B. H. Gwee, "Interceptive side channel attack on AES-128 wireless communications for IoT applications," *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, Jeju, 2016, pp. 650-653.
4. **A. A. Pammu**, K. S. Chong, N. K. Z. Lwin, W. G. Ho, N. Liu and B. H. Gwee, "Success rate model for fully AES-128 in correlation power analysis," *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, Jeju, 2016, pp. 115-118.
5. **A. A. Pammu**, K. S. Chong and B. H. Gwee, "Highly secured arithmetic hiding based S-Box on AES-128 implementation," *2016 International Symposium on Integrated Circuits (ISIC)*, Singapore, 2016, pp. 1-4. **(Best Student Paper Award, Singapore)**
6. W. G. Ho, **A. A. Pammu**, N. Liu, K. Z. L. Ne, K. S. Chong and B. H. Gwee, "Security analysis of asynchronous-logic QDI cell approach for differential power analysis attack," *2016 International Symposium on Integrated Circuits (ISIC)*, Singapore, 2016, pp. 1-4.
7. **A. A. Pammu**, K. S. Chong and B. H. Gwee, "Highly secured state-shift local clock circuit to countermeasure against side channel attack," *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*, Baltimore, MD-USA, 2017, pp. 1-4.