CNN Based Electromagnetic Side Channel Attacks on SoC

Yong Xiao¹, a, Jin Xin¹, b, Yanhua Shen², c
¹Electric Power Research Institute CSG, Guangzhou, China
²School of Materials Science and Engineering South China University of Technology, Guangzhou, China
²xiaoyong@csg.cn, bJinxin1@csg.cn, cshenyh@scut.edu.cn

Abstract. Side channel attacks are well-known threat to ciphers in real world. In this paper, we give a CNN based profiled side channel attacks on AES cipher implemented on HI Silicon Kirin 620 SoC, which is a 1.2GHz multi-core platform. With 100,000 acquired side channel traces to train, the CNN have ability to recover real key byte under 1,000 traces, even though the traces are misaligned.

1. Introduction

Side channel attacks are well-known threat to ciphers in real world. The most famous example is Differential Power Analysis introduced by Kocher et al. in 1999 [1]. Since then, many different leakage channels have been studied. For example, leakages from electromagnetic emission [2] [3] [4], sounds [5] and even photon [6]. Meanwhile, improved analysis methods have also been proposed. Correlation power analysis (CPA) was proposed by Brier et al. [7] in 2004 where the correlation between leakage traces and modeled values (e.g. Hamming weight model) of handled data was taken into account. Subsequently, several works applied this idea to practical environments and achieved good results [8] [9]. Other attack models such as partitioning power analysis (PPA) [10], collision attack [11] and mutual information analysis [12] have also been studied.

Among these analysis methods, template attack (TA) supposes that the attacker has access to one configurable sample to perform the profiling phase, thus produced the idea of profiled SCA. Traditional TA use statistics to perform profiling and matching phases. In recent years, machine learning methods are applied to profile SCA. Methods like support vector machine (SVM) [13] [14] [15] [16] [17] [18] random forest (RF) [19] [18] are extensive researched. As a kind of special machine learning method, deep learning with neural network architecture, especially convolutional neural network (CNN), achieve great success in image classification, speech recognition and other similar scenarios. Martinasek et al. proposed the first study of neural network in profiled SCA [20]. Then Cagli et al. showed that CNN has the ability to defeat jitter-based countermeasure [21]. Benadjila et al. gave a systematic study on CNN in the SCA and introduce ASCAD benchmark [22], which provided reference database to subsequent researches [23] [24].

A system on a chip (SoC) combines the required electronic circuits of various computer components onto a single, integrated chip. Its components usually include a graphical processing unit (GPU), a central processing unit (CPU) that may be multi-core, and system memory (RAM). With improved performance and reduced power consumption, SoC is used in millions of devices. For example, most smartphones and tablets house multicore SoC components. Different from smart cards, SoC is much more complex.
Performing SCA on SoC with gigahertz clock frequencies requires lots of tricks. Longo et al. propose non-profiled side channel attack on ARM processors [25] with electromagnetic leakage.

2. Our Contributions
In this paper, we give a CNN based profiled SCA attack on AES cipher implemented on a SoC. In the setup phase, instead of collecting electromagnetic emission of chip surface, we target at emission from a small capacitor connected to the core power supply line which gives a clear signal. Then we use CNN in profiling and matching phases. As there are no leakage found at the last round of AES, a novel algorithm to recover keys of the first round is proposed. With observations on AES algorithm, we build differential equation of chosen plaintext and intermediate value, which finally turn to probability advantage of correct key.

3. Background

3.1. AES block cipher
The advanced encryption standard (AES) [26] is a block cipher that supports key sizes of 128, 192, and 256 bits. The plaintext is first treated as byte matrix of size 4 × 4. Then round functions are applied to this state matrix. An AES round consists of four operations:
- SubBytes (SB) — applying the same 8-bit to 8-bit invertible S-box 16 times in parallel on each byte of the state
- ShiftRows (SR) - cyclically shifting the i’th row by I bytes to the left
- MixColumns (MC) multiplication of each column by a constant 4x4 matrix over the field GF(2^8)
- AddRoundKey (AK) — XORing the state with a 128-bit round key
The number of rounds depends on the key length: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. In this paper, our target is AES-128 from LibTomCrypt [27], which is an open source cryptographic toolkit.

3.2. Convolutional Neural Networks
Convolutional Neural Network (CNN) is a specific kind of neural network which achieve great success in image classification, speech recognition and other similar scenarios. Usually, a CNN consists of multiple convolutional layers, pooling layers, as well as fully connected layers [28]. Convolutional Neural Networks are linear layers that share weight across space, which have the ability to detect pattern in different positions. Pooling layers are non-linear layers that reduce the spatial size in order to limit the number of parameters. The most common pooling functions are the max-pooling which outputs the maximum value of the certain area and the average pooling which outputs the average value within the certain area. Fully connected layers output results which depends on the entire input. It usually comes at the end of the neural network.

A common CNN is expressed by the following formula:

\[ S = [\gamma]^{n1} \circ [\delta \circ \gamma^{n2}]^{n3} \]  

Where \( \gamma \) is a convolutional layer, \( \delta \) is a pooling layer and \( \lambda \) is a fully connected layer. S is softmax function outputs a probability distribution.

3.3. An overview of HiKey board
The HiKey platform was the first board to be certified 96Boards Consumer Edition compatible from LeMaker. The board is based around the HiSilicon Kirin 620 SoC. Figure 1 illustrate a block diagram of this SoC, where ACPU subsystem contains the central 64-bit ARM Cortex-A53 core which is clocked up to 1.2 GHz.
Figure 1. A block diagram of the HiSilicon Kirin 620 SoC [28]

From the schematics [28], we know that the core is worked under voltage of 1.05 volt. Several capacitors are connected to core power supply line to stabilize voltage.

3.4. Experimental environment
The measurement equipment to acquire traces is listed below:
- Lecroy 8104 1 GHz oscilloscope
- Langer MFA-K 01-12 near-field probe (100MHz-6GHz).

Figure 2. Schematics of HiKey platform [28]
The experiment setup is shown in Figure 3. Instead of collecting electromagnetic emission of chip surface, we target at emission from a 10 NF capacitor (C1356 in schematics) connected to the core power supply line which gives a clear signal as illustrated in Figure 4.

4. Analysis of Leakage
We acquire 200 thousand of traces under sample rate of 2.5 GHz, where 100 thousand is used for profiling and the left is used for matching. The original trace is shown in Figure 5. It can be easily recognized 9 similar patterns in the trace, which should be the first 9 rounds of AES encryption. The first round is around 20000 samples. After zooming in, we find that the traces are slightly misaligned, as shown in Figure 6. Luckily, CNN has ability to overcome clock jitter and misalignment [21]. We do not execute any synchronization here.
With fast Fourier transform (FFT), we plot the spectrum of acquired traces in Figure 7, where there is a clear leakage around 1.2 GHz.

![Figure 7. Spectrum of an acquired trace](image)

5. Key byte recovery with CNN

5.1. Network structure

The structure of CNN network is shown in Figure 8. The network has three convolutional and polling layers. The kernel size of every convolutional layer is all 3. The filters are 64, 128 and 256 respectively. For the pooling layer, we use set all the pooling size and the stride to 2. The first fully connected layer has 1024 neurons while the second has 256 neurons.

5.2. Target Operation

Regarding the targeted operation, we consider one byte of AES S-Box outputs during the first round: \( L = \text{S-box} [X \oplus k^*] \) where \( X \) and \( k^* \) are the plaintext and key respectively. Outputs of S-Box are common targets in side channel analysis which have high level of confusion.

5.3. Experiment result

During the profiling phase, the CNN is first trained under only 10 epochs with batch size of 128. The label is set as target operation above. During the matching phase, one byte the output of S-box is predicted with trained CNN. For every prediction, we can deduce key byte with \( k = \text{Sbox}^{-1} (L) \oplus X \), which gives a distribution of key bytes. For different traces, the distributions are accumulated. The accumulated distribution is a distinguisher of real key byte. The result of the fifth byte is shown in Figure 9. The real key is recovered under 1000 traces.

6. Conclusion

We claimed that CNN based side channel attack is a threat to embed devices with gigahertz clock frequencies. In this paper, we give the first example recovering key of AES cipher implemented on Hi Silicon Kirin 620 SoC, which is a 1.2 GHz multi-core platform. The acquiring set up is explained in detail. With only 1000 acquired traces, the real key byte is recovered.

References

[1] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Advances in Cryptology-CRYPTO99, pages 388 - 397. Springer, 1999.

[2] Karine Gandolfi, Christophe Mouretel, and Francis Olivier. Electromagnetic analysis: Concrete results. In International workshop on cryptographic hardware and embedded systems, pages 251-261. Springer, 2001.

[3] Jean-Jacques Quisquater and David Samyde. Electromagnetic analysis (ema): Measures and counter-measures for smart cards. In International Conference on Research in Smart Cards, pages 200-210. Springer, 2001.
[4] Jake Longo, Elke De Mulder, Dan Page, and Michael Tunstall. Soc it to em: electromagnetic side-channel attacks on a complex system-on-chip. In International Workshop on Cryptographic Hardware and Embedded Systems, pages 620-640. Springer, 2015.

[5] Daniel Genkin, Adi Shamir, and Eran Tromer. Rsa key extraction via low-bandwidth acoustic cryptanalysis. In Annual Cryptology Conference, pages 444-461. Springer, 2014.

[6] Elad Carmon, Jean-Pierre Seifert, and Avishai Wool. Photonic side channel attacks against rsa. In 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pages 74-78. IEEE, 2017.

[7] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. In Cryptographic Hardware and Embedded Systems-CHES 2004, pages 16-29. Springer, 2004.

[8] Christophe Clavier, Benoit Feix, Georges Gagnerot, Mylene Roussellet, and Vincent Verneuil. Improved collision-correlation power analysis on first order protected aes. In Cryptographic Hardware and Embedded Systems-CHES 2011, pages 49-62. Springer, 2011.

[9] Amir Moradi, Oliver Mischke and Thomas Eisenbarth. Correlation-enhanced power analysis collision attack. In Cryptographic Hardware and Embedded Systems, CHES 2010, pages 125-139. Springer, 2010.

[10] Thanh-Ha Le, Jessy Clediere, Cecile Canovas, Bruno Robisson, Christine Serviere, and Jean-Louis Lacoume. A proposition for correlation power analysis enhancement. In Cryptographic Hardware and Embedded Systems-CHES 2006, pages 174-186. Springer, 2006.

[11] Andrey Bogdanov. Improved side-channel collision attacks on aes. In Selected Areas in Cryptography, pages 84-95. Springer, 2007.

[12] Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel. Mutual information analysis. In Cryptographic Hardware and Embedded Systems-CHES 2008, pages 426-442. Springer, 2008.

[13] Liran Lerman, Romain Poussier, Gianluca Bontempi, Olivier Markowitch, and Francois-Xavier Standaert. Template attacks vs. machine learning revisited (and the curse of dimensionality in side-channel analysis). In International Workshop on Constructive Side-Channel Analysis and Secure Design, pages 20-33. Springer, 2015.

[14] Stjepan Picek, Annelie Heuser, Alan Jovic, Simone A Ludwig, Sylvain Guilley, Domagoj Jakobovic, and Nele Mentens. Side channel analysis and machine learning: A practical perspective. In 2017 International Joint Conference on Neural Networks (IJCNN), pages 4095-4102. IEEE, 2017.

[15] Hera He, Josh Jaffe, and Long Zou. Side channel cryptanalysis using machine learning. CS229 Project, pages 1-392, 2012.

[16] Stjepan Picek, Annelie Heuser, Alan Jovic, Shivam Bhasin, and Francesco Regazzoni. The curse of class imbalance and conflicting metrics with machine learning for side-channel evaluations. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018.

[17] Liran Lerman, Gianluca Bontempi, and Olivier Markowitch. A machine learning approach against a masked aes. Journal of Cryptographic Engineering, 5(2):123-139, 2015.

[18] Liran Lerman and Olivier Markowitch. Efficient profiled attacks on masking schemes. IEEE Transactions on Information Forensics and Security, 14(6):1445-1454, 2019.

[19] Stjepan Picek, Annelie Heuser, Alan Jovic, Simone A Ludwig, Sylvain Guilley, Domagoj Jakobovic, and Nele Mentens. Side channel analysis and machine learning: A practical perspective. In 2017 International Joint Conference on Neural Networks (IJCNN), pages 4095-4102. IEEE, 2017.

[20] Zdenek Martinasek and Vaclav Zeman. Innovative method of the power analysis. Radioengineering, 22(2):586-594, 2013.

[21] Eleonora Cagli, Cecile Dumas, and Emmanuel Prouff. Convolutional neural networks with data augmentation against jitter-based countermeasures. In International Conference on Cryptographic Hardware and Embedded Systems, pages 45-68. Springer, 2017.

[22] Rmi Strullu Eleonora Cagli Ryad Benadjila, Emmanuel Prouff. Study of deep learning techniques
for side-channel analysis and introduction to ascad database.

[23] Benjamin Timon. Non-profiled deep learning-based side-channel attacks with sensitivity analysis. IACR Transactions on Cryptographic Hardware and Embedded Systems, pages 107-131, 2019.

[24] Guang Yang, Huizhong Li, Jingdian Ming, and Yongbin Zhou. Convolutional neural network based side-channel attacks in time-frequency representations. In International Conference on Smart Card Research and Advanced Applications, pages 1-17. Springer, 2018.

[25] Jake Longo, Elke De Mulder, Dan Page, and Michael Tunstall. Soc it to em: electromagnetic side-channel attacks on a complex system-on-chip. In International Workshop on Cryptographic Hardware and Embedded Systems, pages 620-640. Springer, 2015.

[26] Joan Daemen and Vincent Rijmen. Aes proposal: Rijndael. 1999.

[27] LibTomCrypt. https://www.libtom.net/LibTomCrypt.

[28] HiKey Schematics. https://github.com/96boards/documentation/blob/master/consumer/hikey/hikey620/hardware/docs/HiKey_schematics_LeMaker_version_Rev_A1.pdf.