Optical Side Channel Attacks on Singlechip

H.S. Wang, D.G. JI, Y Zhang, K.Y Chen, J.G. Chen, Y.Z. Wang
Department of Information Engineering, Ordnance Engineering College, Shijiazhuang 050003, China

L.A Wu
Laboratory of Optical Physics, Beijing National Laboratory for Condensed Matter Physics, Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China

ABSTRACT: Optical side channel attack is a new kind of method against cipher chips, such as singlechips implementing public cryptographic algorithms. Two kind of optical side channel attacks, active and passive attacks, are presented in this paper. First, we implemented optical fault injection attacks against cipher algorithms running on AT89C52 singlechip, and demonstrated how to exploit secret information under attack. Then, we did photonic emission dependency analysis and revealed the correlation between operation/data and the photonic emission from the AT89C52 singlechip at the instruction level. Our experimental results show that optical side channel attacks pose serious threats to Cipher chips.

KEYWORD: Optical side channel attack; Optical Fault Injection Attack; Photonic Emission Analysis; AES; Singlechip; AT89C52

1 INTRODUCTION

Cipher chips such as singlechips running cryptographic algorithms are used to protect both the confidentiality and the integrity of sensitive information. Side channel attacks can get secret information from the devices. One kind of attack is called passive attack [1]. To get sensitive data, side channel information is collected, such as the power consumption[2],the electromagnetic emanation[3-4], the timing information[5-6] and the light emission [7] that is leaked by the running cipher chips. The effective way to implement a passive side channel attack is to measure the leaking signals when the cipher chip is operating cryptographic data, and use statistical way to extract the secret information. Another kind of attack is called active attack[1] which interferes in the device by changing external or internal condition to influence the system working normally. Faults in the computation are emerged because of these abnormal conditions. Therefore, the secret information of cipher chips can be extracted by getting response to faults. A model of side channel attack is showed in Figure 1.

Optical side channel analysis is a kind of semi-invasive and novel attack. The decapsulation of the cipher chip from its package is required for this sort of attacks. Optical fault injection attack is a typical kind of active fault injection attack against cipher chips and was first proposed in 2002[8]. This active optical fault injection attacks threaten security of cipher chips, and can apply in attacking common public cipher algorithms such as AES, RSA. Photon emission analysis is kind of passive attack and was first proposed in 2008[7], it collects emission photons of the running cipher chip for side channel analysis, allows to select specific part of cipher chip to do in-depth analysis, and has a better signal to noise ratio, compared with electromagnetic or power analysis which concentrates on system-wide side channel information leakage of cipher chip.

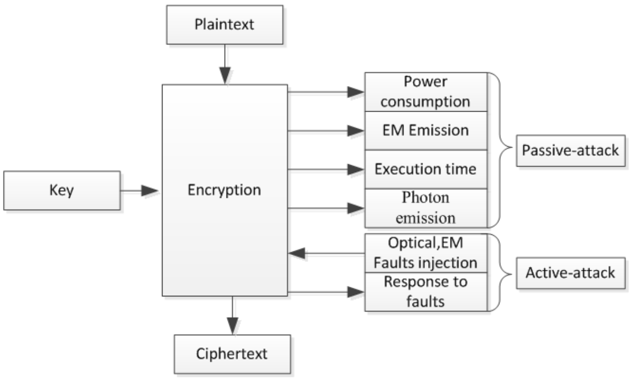


Figure1. Model of side channel attack

A kind of optical fault injection attacks on singlechip AT89C52 is introduced in this paper. The ultraviolet is manipulated to irradiate non-volatile memory of singlechip which was depacked, and the memory of the chip can be erased. Thus an AES software implementation by manipulating the 256 bit S-box table can be attacked.

For photonic emission analysis, this paper aims at AT89C52 singlechip MOV instruction execution, verifies the relationship between photon emission and the singlechip operation and data, to lay the foundation for the subsequent research using photon emission analysis for AES, RSA algorithms.

2 OPTICAL FAULT INJECTION ATTACKS

2.1 *Singlechip and Algorithm*

2.1.1 AT89C52

Singlechip AT89C52 consists of a 8-bit arithmetic-logical unit, 8K bytes in-system reprogrammable Flash program memory and 256 bytes Internal SRAM memory. It is a high-performance and low-power CMOS microprocessor manufactured using Atmel's high-density nonvolatile memory technology. The chip has been depacked. Thus we can use special light to irradiate the chip. The feature of depacked and zoomed AT89C52 area of the die are showed in Figure 2.

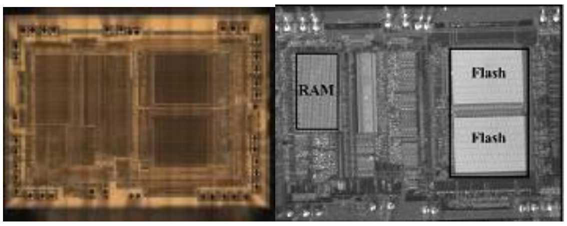


Figure2. Depacked and zoomed AT89C52

2.1.2 CRT-RSA Algorithm

The common RSA encrypting processes is as follows:

1) Choose two large primes p and q, $p \neq q$;

2) Compute $n=pq$;

3) Compute $\varphi(n) = (p-1)(q-1)$;

4) Choose $e:1<e<\varphi(n$，$\gcd(e, \varphi(n))=1$;

5) Compute d: $ed \equiv 1(\bmod \varphi(n))$;

6) Public key: $\{e, n\}$;

7) Private key: $\{d, n\}$;

8) Plaintext: $M \in Z_n = \{0, 1, ... , n-1\}$;

9) Ciphertext: $C= M^e \pmod n$;

For efficiency reasons, Chinese Remaindering Theorem (CRT) is used to speed up the generation of signature M. In CRT model, the signature process is as follows:

1) $e_1 = e \pmod p$;

2) $e_2 = e \pmod q$;

3) $c_p = M^{e_1} \pmod p$;

4)$c_q = M^{e_2} \pmod q$;

5)$C = CRT(c_q, c_p) = [c_p(q^{-1} \bmod p)q+c_q(p^{-1} \bmod q)p](\bmod n)$;

2.1.3 AES Algorithm

AES-128 is implemented by us. AES is operated on a 4 x 4 array of bytes, which is called the state. The AES cipher is specified as a number of repetitions of transformation rounds that is used to convert the plaintext into the ciphertext. Each round is consists of several processing steps, the process of AES encrypt is showed in Figure 3.

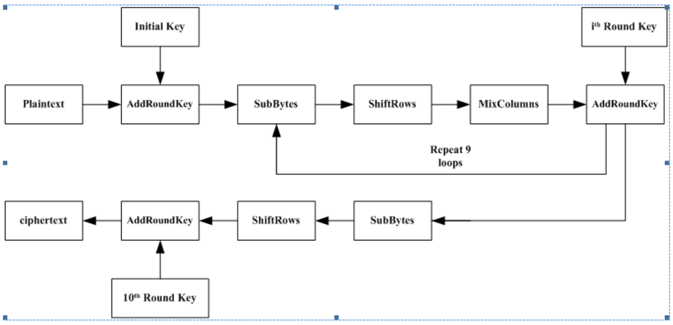


Figure3. AES encrypt process

2.2 *Ultraviolet Fault Injection Attack on AES*

2.2.1 Ultraviolet Irradiation on Flash Memory

FLASH devices can be erased by exposing under UV light. This experiment demonstrates AT89C52 Flash memory can be erased through disinfectant UV light irradiation, and the number of the erased bits is decided by exposing time. Besides, we put a kind of UV protecting ink to cover the Flash memory face, which can prevent the UV light to erase the content of memory. Thus, we can take use of this characteristic to control more accurate attack on Flash memory. At last, our expect faults are gotten. Ultraviolet irradiation on Non-volatile Memory of the AT89C52 cipher chip is showed in Figure 4. Percentage of Flash memory byte changed on condition of ultraviolet irradiation is showed in Figure 5.

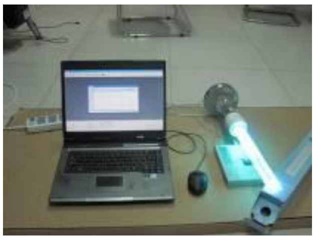


Figure4. UV light fault injection system

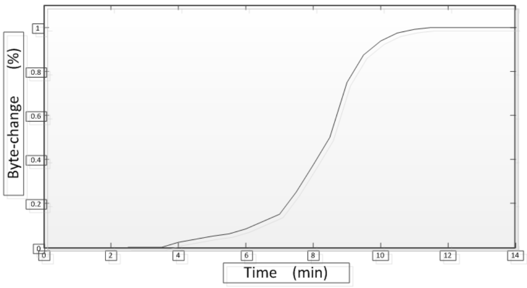


Figure5. Percentage of Flash memory byte changed

2.2.2 Practical Attack

An AES implementation using a fixed S-box table is programmed in AT89C52 Flash memory and it is the target of the experiment. Special strategy is presented to make the S-box only one byte state flip. AT89C52 is connected through a serial port to the PC to implement AES. After 3500 AES encryptions, 16 pairs of ciphertext are gotten, and only one byte is different, and the initial key is exploited too. Different pair of ciphertext $C_{i,j}$ and $\tilde{C}_{i,j}$ are denoted. $K_{i,j}$ is the 10th round key. Supposing the value of the S-box fault byte is Fault value, before fault occurred the byte value is Right value. The attack process is as follows:

```
Initialize $D_{i,j} = -1$ ,  $i, j \in \{0,...,3\}$
    while $D_{i,j} == -1$ do
    if (ciphertext only one byte different )
        $D_{i,j} = C_{i,j}$
    end if
end while
C=AES(random(plaintext))
For $Rightvalue = 0; Rightvalue < 256; Rightvalue++$
    $K_{i,j} = D_{i,j} \oplus Rightvalue$
    $K_{i,j}^{initial}$ =Invert ( $K_{i,j}$ )
    $C^{compare} = AES(M, K_{i,j}^{initial})$
If ( $\mathrm{C}^{\mathrm{r}} == C^{compare}$ )  $Key = K_{i,j}^{initial}$
return Key
```

2.3 *Summarization*

Practical attack and result for ultraviolet light attack on AES and laser light attack on CRT-RSA implemented in AT89C52 singlechip is presented in this paper. Actually, these attacks setup easily and cost very low. Security of these cipher chips is threatened by the optical fault injection attacks, which is brought unprecedented challenges.

3 PHOTONIC EMISSION DEPENDENCY ANALYSIS

3.1 *Photon Emission, Detection and Processing*

3.1.1 *CMOS circuit photon emission mechanism*

Most of the semiconductor integrated circuit is constructed on the basis of COMS structure，it uses complementary transistor as its fundamental element. When the transistor state is switched, the current generated by the electronic transition caused a thermal effects, and thus photons are emitted[9]. The standard COMS inverter circuit is composed by a pair of n-MOS and p-MOS transistors, When its output changes from high state to low, the n-channel transistors emit photons, whereas the p-channel transistors emit photons.

As the different energy obtained by electrons causes a different photonic radiating spectra, the emission photons in the spectral range 500nm to 1200nm, the maximum emission in the range 900nm to 1100nm[9]. Photon emission from switching transistor of CMOS circuit is a probability event, it means that not each switching must emit photons. The probability formula of photon emission for each transistor flip [10] follows below:

$$N_e=S_eBL_HI_d/(qv_s)T_s$$

Where S_e is the spectral emission density, B is the bandwidth of the emission, L_H is the length of the hot carrier region, I_d is the drain current, v_s is the saturated carrier velocity, Ts is the switching frequency, q is the electric charge. Normally, the probability of the transistor photon emission is about 10^{-2} to 10^{-4} per switching[11].

3.1.2 *Single Photon Detection and Processing*

The suitable detector for photonic emission of cipher chip relates to single photon detection domain. Device for single photon detection probably includes a special CCD camera, a photomultiplier tube (PMT) or an avalanche photodiode (APD). Photonic emission spectra of cipher chip covers two wave band: 500-850 nm and 850-1200 nm, Si-based detector is proper for the visible light, and InGaAs-based detector is proper for the near infrared. In order to improve thce efficiency of photonic emission collection, cipher chip should be depacked.

In our experiment, we use an Si-based APD as single-photon detector[12]. An experimental system based on single-photon counting for the detection, transmission, processing and analysis of photonic emission from singlechip has been designed and constructed, using time-correlated single-photon counting (TCSPC) technology[13,14] for processing of photonic radiation signal.

3.1.3 *Principle of TCSPC*

The radiation source under test has low photon intensity, the probability of detecting a photon in a signal acquisition cycle is much less than 1, that is, at most only one photon signal reaches the SPAD photon detector within a period, each photon reaching the detector at different times; after repeated synchronous sampling in high repetition frequency, we can establish the statistical distribution histogram for photons and arriving time.

The principle of TCSPC is showed in Figure6 [14]. TCSPC technique is with high sensitivity, based on the amount of time channels it can reach picosecond time resolution.

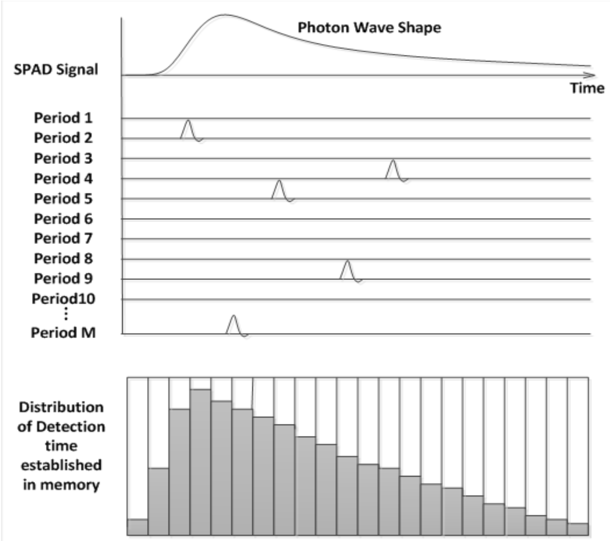


Figure6. Principle of TCSPC

3.1.4 *Photon Emission Dependency of cipher chip*

Photonic emission analysis attacks can obtain secret information by gathering and analyzing photon radiation track features from cipher chip at runtime. This mainly uses two types of photon emission dependency: operation dependency and data dependency. That is to say, transient photon emission depends on the operation and the processing performed by the cipher chip data.

3.2 *Experimental Setup*

3.2.1 *Photoelectric Experimental System based on TCSPC*

We use a Si-based Single Photon APD(SPAD) as single-photon detector to detection photon emission of cipher chip. The Si-based SPAD can capture 400nm to 1060nm wavelength photons, which have a high collect efficiency for the visible parts. The photoelectric experimental system is shown in Figure 7.

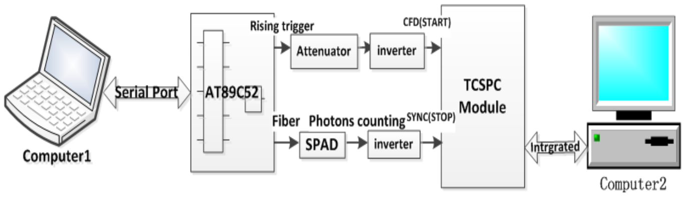


Figure7. Photoelectric experimental system

The TCSPC module for data acquisition and processing receives the SPAD's output signals, records them on the 4096 channels according to the arriving time. Computer1 sends different messages to AT89C52 through the serial port, controlls AT89C52 to execute the relevant tested procedures and to process the related data. The TCSPC module is installed in Computer2, which stores data and performs photonic signal processing and photonic emission analysis based on and TCSPC techniques.

3.2.2 *Singlechip under Test*

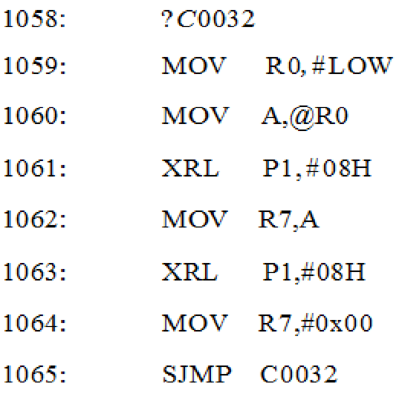
As the chip under test in the experiment, AT89C52's working clock frequency is 12 MHz, its Machine Cycle is 1 μs, its instructions and data performed is customized. External computer communicates with AT89C52 via RS232 interface, controls which instruction and data to be performed by AT89C52. AT89C52 receives the plaintext data via RS232 interface, and sends the encrypted ciphertext back to the external computer. Main area of the observation and analysis is in the SRAM memory area.

AT89C52 should be depacked and Figure 2 shows the chip surface image of the depacked AT89C52 by using an optical microscope camera with high resolution. In our experiment, we use single-photon detectors to detection the register in the chip SRAM area, Figure 8 shows the zoomed SRAM.

Figure8. Zoomed SRAM area

3.2.3 *Experimental procedure*

In order to verify the instruction-level operation dependency and data dependency of cipher chip photon emission, the assembly procedure performed by the AT89C52 is shown in Figure 9, mainly concentrated on the analysis of MOV instruction and its operand. Each of the XOR instruction (XRL) and the conditional branch instruction (SJMP) requires two machine cycles to execute, and each instruction of the rest requires one machine cycle, each machine cycle is 1us, the test program cycle totals 10us.



```
1058:        ?C0032
1059:        MOV    R0,#LOW
1060:        MOV    A,@R0
1061:        XRL    P1,#08H
1062:        MOV    R7,A
1063:        XRL    P1,#08H
1064:        MOV    R7,#0x00
1065:        SJMP   C0032
```

Figure 9. Tested assembly procedure

3.3 *Practical Experiments and Analysis*

3.3.1 *Analysis on Operation Dependency*

The AT89C52 controlled by computer1 performs the experimental procedure shown in Figure 9, The photoelectric experimental system based on TCSPC illustrated in Figure 10 is used for the acquisition of photonic radiation signal. During the experiments, a Si-based SPAD collects the photons radiation emitted from the AT89C52, and the AT89C52 provide trigger signals for TCSPC processing module. Because the SPAD outputs standard TTL signal, and the TCSPC module card requires a negative pulse input, the inverter is used. The photons distribute in the 4,096 channels of the TCSPC module according to arrival time at SPAD. The SPAD is aimed at the area of AT89C52's SRAM via fiber, collecting photons for 10 minutes, the collected data is processed in the instruction sequence shown in Figure 9, and the result is shown in Figure 10. It is found that the number of emitting photons of different instruction execution cycles is not the same, and it indicates that the photonic emission intensity of cipher chip relates to instruction operation.

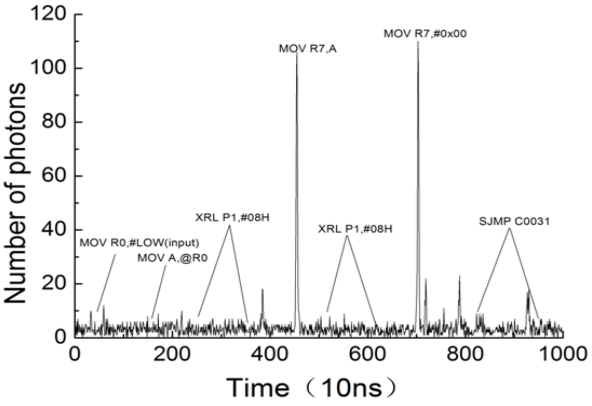


Figure10. Time distribution of photonic emission for different instructions

3.3.2 *Analysis on Data Dependency*

The photonic emission of cipher chip within a certain time interval is not only dependent on the instructions, but also on the data to be processed. To get the photonic emission characteristics for cipher chip to perform the same instruction and process different data, SPAD is aimed at R7 register in SRAM area via fiber, we probe for AT89C52 R7 register, and let AT89C52 execute the instruction MOV R7, A. During the experiment we refer to the Hamming distance model[15], R7 is set to 00 (hex, the same below) before the value of register R7 is changed every time, to ensure that each transformation of R7 is flipped from 00 to a value. Then the value of R7 is changed respectively to 00, 01, 03, 07, 0F, 1F, 3F, 7F, FF, the corresponding register R7 is flipped 0-8 bit (binary) in sequence. The data analysis of photonic emission for instruction MOV R7, A is shown in Figure 11, the acquisition time is 10 minutes. The experimental results show that the register flips more bits, the more number of photons emission. Changes in the data (changes for each bit in binary data) correlate with the photonic emission intensity.

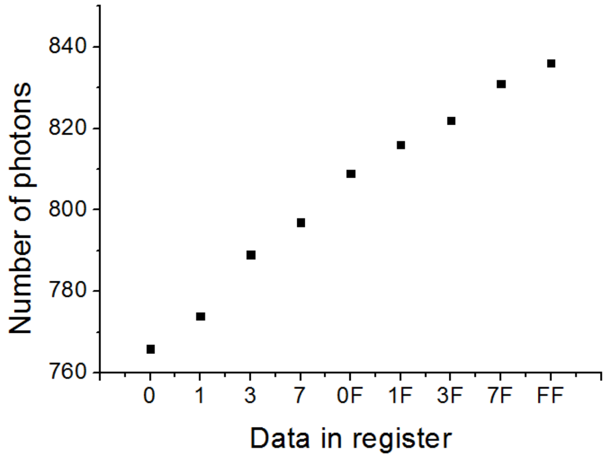


Figure11. Photonic emission dependency relationship with the register data changes

3.4 *Summarization*

Experiments on operation dependency and data dependency analysis of AT89C52 singlechip show that cipher chip photonic emission analysis based on TCSPC technology is a relatively low cost but effective method for optical side-channel attacks, it can obtain direct or indirect correlation between the photonic emission and the information inside the cipher chip, and it poses a serious practical threat to cipher chip security. Meanwhile, the above research has laid a good foundation to further develop for AES or RSA cipher chips, such as Simple Photonic Emission Analysis and Differential Photonic Emission Analysis.

4 CONCLUSIONS

Active and passive optical side channel attacks are presented in this paper. Optical fault injection attacks exploit secret information by inducting faults to the implemention of cryptographic algorithms through optical irradiation in running cipher chip. Photonic emission analysis reveals secret information through the correlation between operation/data and the photonic emission of the cipher chip. Experimental results show that both of the active and passive optical side channel attacks cost low or relatively low, and are effective for cracking cipher chips.

5 ACKNOWLEDGMENT

The authors would like to thank Song Kai and Gao

Yan-lei for their useful comments on the preliminary version of this article. We would also like to thank Institute of Physics Chinese Academy of Sciences to provide important experimental equipment.

This paper is supported by the National Natural Science Foundation of China (Grant Nos. 51377170, 61271152), the National High Technology Research and Development Program of China (Grant No.2011AA120102), and the Natural Science Foundation of Hebei, China (Grant No. F2012506008).

REFERENCES

[1] Korobogatov S. 2005. Semi-invasive attacks -a new approach to hardware security analysis. London: University of Cambridge, Computer Laboratory

[2] PAUL K, JOSHUA J, and BENJAMIN J. 1999. Differential Power Analysis: 19th Annual International Cryptology Conference. California: Advances in Cryptology. 388–397.

[3] Quisquater. J.J.Samyde.D.2001. Electromagnetic analysis (EMA): Measures and counter-measures for smart cards. In: E-smart. pp.200-210

[4] Karine G, Christophe M, and Francis O. 2001. Electromagnetic Analysis: Concrete Results. In Cryptographic Hardware and Embedded Systems-CHES2001. Third International Workshop, pages.251-261,

[5] Paul K, 1996.Timing Attack on Implementation of Diffe-Hellman, RSA, DSS and other Systems. Advances in Cryptology; proceedings of Crypto '96. New York, Springer-Verlag,

[6] CHEN C.S, WANG T, ZHENG Y.Y. 2009. Timing Attacks and Defenses on RSA Public-key Algorithms, Computer engineering, 35(2): 123-125

[7] Ferrigno, J. Hlavac, M.: 2008. When AES blinks: introducing optical side channel. Information Security, IET 2(3), 94 -98

[8] Skorobogatov S., Anderson R.2002.Optical fault induction attacks.Cryptographic Hardware and Embedded Systems Workshop (CHES-2002), LNCS 2523, pp. 2–12.

[9] Villa S., Lacaita A.L., Pacelli A., 1995 .Photon emission from hot electrons in silicon. Physical Review B, Vol. 52, pp. 10993–10999

[10] Stellari F., Zappa F., Ghioni,M. Cova S., 1999 Non-invasive optical characterisation technique for fast switching CMOS circuits, Solid-State Device Research Conference, Leuvem, Belgium pp. 172–175

[11] Skorobogatov S.. 2009. Using Optical Emission Analysis for Estimating Contribution to Power Analysis, computer society, 39, pp. 111

[12] Excelitas Technologies.2012 www.excelitas.com

[13] Becker W 2005 *Advanced Time-Correlated Single-Photon Counting Techniques* (Berlin:Springer) pp19-22

[14] Becker W 2012 *The bh TCSPC Handbook* 5th Edition (Berlin: Becker & Hickl GmbH) pp51-57

[15] Mangard S, Oswald E, Popp T (translated by Feng D G, Zhou Y B, Liu J Y) 2010 *Power Analysis Attacks* (Beijing: Science Press) pp1-129 (in Chinese)