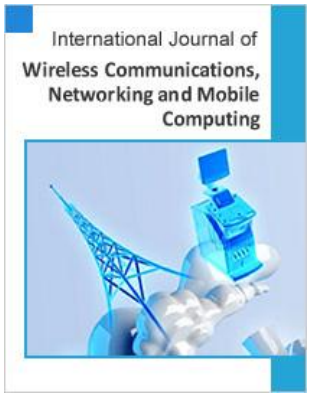
International Journal of Wireless Communications, Networking and Mobile Computing
2016; 3(1): 16-21
Published online February 19 2016 (http://www.aascit.org/journal/wcnmc)
ISSN: 2381-1137 (Print); ISSN: 2381-1145 (Online)

American Association for Science and Technology



Keywords
Elliptic Curve Cryptography,
Simple Power Analysis Attacks,
Differential Analysis Attacks,
Major Collisions,
Minor Collisions

Received: November 22, 2015
Revised: January 25, 2016
Accepted: January 27, 2016

The Role of Major and Minor Collisions in Side Channel Attacks

E. Kesavulu Reddy

Department of Computer Science, Sri Venkateswara University, Tirupati, Andhra Pradesh, India

Email address

ekreddysvu2008@gmail.com, ekreddy2002@yahoo.com

Citation

E. Kesavulu Reddy. The Role of Major and Minor Collisions in Side Channel Attacks. *International Journal of Wireless Communications, Networking and Mobile Computing*. Vol. 3, No. 1, 2016, pp. 16-21.

Abstract

The security of cryptographic algorithms such as block ciphers and public-key algorithms relies on the secrecy of the key. Traditionally, when cryptanalysists examine the security of a cryptographic algorithm, they try to recover the secret key by observing the inputs and outputs of the algorithm. Assuming this type of attack models, cryptologists have made commonly-used cryptographic algorithms secure against such attacks. However, a real computing device not only generates the outputs specified in algorithms but also inevitably produces some other information such as timing and power. These types of information, called side-channel information, can be exploited in side-channel attacks to retrieve secret keys. Side channel attacks have successfully broken many algorithms. The attacker obtains the value of secret key at single instance some iteration is called Major Collisions. The attacker gains two values of random integer at some iteration are called Minor Collisions. We have provided a brief background on Simple (SPA) and Differential (DPA) power and electromagnetic analysis attacks on the classical ECSM algorithms. We study on minor collisions and to provide an analytic result for their probability of occurrence as well as effect of the fixed sequence window method. We prove that mathematically the minor collisions are reduced up to 50% of major collisions. We analysis the role of Major and Minor collisions in side channel attacks.

1. Introduction

Some implementations of cryptographic algorithms often leak "*side channel information*." Side channel information includes power consumption, electromagnetic fields and timing to process. Side channel attacks, which use side channel information leaked from real implementation of cryptographic algorithms, were first introduced by Kocher [16]. Side channel attacks can be often much more powerful than mathematical cryptanalysis.

Power analysis attacks use the fact that the instantaneous power consumption of a hardware device is related to the instantaneous computed instructions and the manipulated data. The attacker could measure the power consumption during the execution of a cryptographic algorithm, store the waveform using a digital oscilloscope and process the information to learn the secret key. Kocher et al., in [16], first introduced this type of at-tack on smart cards performing the DES operation. Then Messerges et al. [12] augmented Kocher's work by providing further analysis and detailed examples of actual attacks they mounted on smart cards.

These attacks are broadly divided into two categories; simple and differential analysis attacks. We will refer to the former category as SPA attacks and the latter as DPA attacks. Though SPA and DPA are the acronyms for simple power analysis and differential power

Analysis. SPA attacks are those based on retrieving valuable information about the secret key from single leaked information from power consumption or electromagnetic emanation trace. On the other hand, DPA attacks generally include all attacks that require more than one such trace along with some statistical analysis tools to extract the implicit information from those traces.

When the relation between the instructions executed by a cryptographic algorithm and the key bits is not directly observable from the power signal, an attacker can apply differential power analysis (DPA). DPA attacks are in general more threatening and more powerful than SPA attacks because the attacker does not need to know as many details about how the algorithm was implemented. The technique also gains strength by using statistical analysis and digital signal processing techniques on a large num- ber of power consumption signals to reduce noise and to amplify the differential signal. The latter is indicated by a peak, if any, in the plot of the processed data. This peak appears only if the attacker's guess of a bit or a digit of the secret key is correct. The attacker's goal is to retrieve partial or full information about a long-term key that is employed in several ECSM executions. Coron [5] has transferred the power analysis attacks to ECCs and has shown that an unaware implementation of EC operations can easily be exploited to mount an SPA attack. Window methods process the key on a digit (window) level.

2. Relative Work

Kocher et al., in [12], first introduced this type of attack on smart cards performing the DES operation. Then Messerges et al. [12] augmented Kocher's work by providing further analysis and detailed examples of actual attacks they mounted on smart cards. Coron [5] has transferred the power analysis attacks to ECCs and has shown that an unaware implementation of EC operations can easily be exploited to mount an SPA attack. Window methods process the key on a digit (window) level. Fixed-sequence window methods were proposed [9, 14, and 15] in order to recode the digits of the key such that the digit set does not include 0.

As for the SPA attack, Kocher et al. were the first to introduce the DPA attack on a smart card implementation of DES [12]. Techniques to strengthen the attack and a theoretical basis for it were presented by Messerges et al. in [9; 12]. Coron applied the DPA attack to ECCs [2]. A potential DPA countermeasure is known as key splitting [11].

3. Research Problem

In the existing system, [7] experiments are conducted it-relatively for n collisions and find out the length of bits according to n. When we taken the window length = 4, excluding the significant bits of w and the values of kj the collisions average is 63%. The maximum number of collisions t are varied from higher towards the mid- dle iterations, then first and last iterations from 12 for 40 bit integers and 23 for 50 bit integers. According to [7], it is not mathematically proved that when the probability was reduced or increased according to the major collisions depends upon the value of the least significant jw bits of length.

4. Research Work

4.1. Elliptic Curve Scalar Multiplication (ECSM)

Scalar multiplication in the group of points of an elliptic curve is analogous to exponentiation in the multiplicative group of integers modulo a fixed integer. Thus, it isthe fundamental operation in EC-based cryptographic systems. The scalar multiplication, denoted kP, is the result of adding the point P to itself k times, where k is a positive integer, that is kP = P + P + · · · + P | {z} k copies and −kP = k (−P). u is said to be the order of P if u is the smallest integer.

Let $(K_{n-1}, K_{n-2}, ..., K_1, K_0)_2$ 2 be the binary representation of k, i.e., $K_i \in \{0, 1\}$ for $0 \leq i < n - 1$. Thus,

$$kP = \left(\sum_{i=0}^{n-1} K^i 2^i\right) P = 2(2(\cdots 2(2(K_{n-1} P) + K_{n-2} P) + \cdots) + K_1 P) + K_0 P = (K_{n-1} 2^{n-1} P) + \cdots (K_1 2P) + (K_0 P) \quad (1)$$

Hence, kP can be computed using the straightforward double-and-add approach in n iterations.

4.2. Key Splitting Methods

It is based on randomly splitting the key into two parts such that each part is different in every ECSM execution. An additive splitting using subtraction is attributed to [4].

$$\text{It is based on computing} = (k - r) P + rP \quad (2)$$

The authors mention that the idea of splitting the data was abstracted in [3]. where r is a n-bit random integer, that is, of the same bit length as k. Alternatively, [5] suggest the following additive splitting using division, that is, k is written as

$$k = \lfloor k / r \rfloor + (k \bmod r) \quad (3)$$

Hence, if we let $K_1 = (k \bmod r)$, $K_2 2 = \lfloor k / r \rfloor$ and S = rP, we can compute

$$KP = K_1 p + K_2 P \quad (4)$$

Where the bit length of r is n/2. They also suggest that (4) should be evaluated with Shamir-Strauss method as in Algorithm. However, they did not mention whether the same algorithm should be used to evaluate (2).

The following multiplicative splitting was proposed by Trichina and Bellezza [7] where r is a random integer invertible modulo u, the order of P. The scalar multiplication kP is then evaluated as

$$kP = [kr^{-1} \pmod u](rp) \quad (5)$$

To evaluate (5), two scalar multiplications are needed; first R = rP is computed, and then kr^{-1} R is computed.

4.3. Major Collisions

A Major collisions is defined as the occurrence of $K^j = K_{2z-1} \rightarrow$ j at some iteration j ∈ [1, z-1]. The intermediate point computed of this value of k^j is the same value that would be computed when no counter measure is in place.

Lemma: For some j ∈ [1, z-1], $K^j = K_{2z-1} \rightarrow$ j iff $G_{j-1\rightarrow 0} = 0$

Proof: We know that K = g * r +h

$$g = G_{z\rightarrow j} * 2^{jw} + G_{j-1\rightarrow 0}$$

$$h = H_{z\rightarrow j} * 2^{jw} + H_{j-1\rightarrow 0}$$

Now $K = (G_{z\rightarrow j} * 2^{jw} + G_{j-1\rightarrow 0}) * r + (H_{z\rightarrow j} * 2^{jw} + H_{j-1\rightarrow 0}) = (G_{z\rightarrow j} * 2^{jw}) * r + G_{j-1\rightarrow 0} * r + H_{z\rightarrow j} * 2^{jw} + H_{j-1\rightarrow 0}$

$$K = (G_{z\rightarrow j} * r + H_{z\rightarrow j}) * 2^{jw} + G_{j-1\rightarrow 0} * r + H_{j-1\rightarrow 0}$$

Let $K^j = G_{z\rightarrow j} * r + H_{z\rightarrow j}$

$$K = K^j * 2^{jw} + G_{j-1\rightarrow 0} * r + H_{j-1\rightarrow 0} \quad (6)$$

Case (i):

Let us assume that $G_{j-1\rightarrow 0} = 0$

$$(1) \Rightarrow K = K^j * 2^{jw} + H_{j-1\rightarrow 0} \quad (7)$$

But we know that

$$K^j = K_{2z-1} \rightarrow j * 2^{jw} + K_{j-1\rightarrow 0} \quad (8)$$

From (2) & (3) $K^j = K_{2z-1} \rightarrow$ jand

$$H_{j-1\rightarrow 0} = K_{j-1\rightarrow 0}$$

Case (ii):

Let us assume that $K^j = K_{2z-1} \rightarrow$ j

$$1) \Rightarrow K = K_{2z-1} \rightarrow j * 2^{jw} + G_{j-1\rightarrow 0} * r + H_{j-1\rightarrow 0} \quad (9)$$

But we know that

$$K = K_{2z-1} \rightarrow j * 2^{jw} + K_{j-1\rightarrow 0}$$

From (4) & (5)

$$G_{j-1\rightarrow 0} * r + H_{j-1\rightarrow 0} = K_{j-1\rightarrow 0} \quad \frac{G_{j-1\rightarrow 0} * r}{2^{jw}} + \frac{H_{j-1\rightarrow 0}}{2^{jw}} = \frac{k_{j-1\rightarrow 0}}{2^{jw}}$$

$$\left\lfloor \frac{G_{j-1\rightarrow 0} * r}{2^{jw}} \right\rfloor + \left\lfloor \frac{H_{j-1\rightarrow 0}}{2^{jw}} \right\rfloor = \left\lfloor \frac{k_{j-1\rightarrow 0}}{2^{jw}} \right\rfloor \left\lfloor \frac{G_{j-1\rightarrow 0} * r}{2^{jw}} \right\rfloor + 0 = 0$$

$$\therefore \left\lfloor \frac{G_{j-1\rightarrow 0} * r}{2^{jw}} \right\rfloor = 0$$

$$r \geq 2^{l-1} \Rightarrow r \geq 2^{(z-1)w}$$

$$z\text{-}1 = \left\lfloor \frac{l}{w} \right\rfloor \frac{r}{2^{jw}} \geq \frac{2^{(z-1)w}}{2^{jw}}$$

$$z\text{-}1 \leq \frac{l-1}{w} \frac{r}{2^{jw}}$$

$$w(z\text{-}1) \leq l\text{-}1 \therefore G_{j-1\rightarrow 0} = 0$$

The Probability of major collisions= $\frac{2^{(z-1)w} / 2^{jw}}{2^{(z-1)w}} = \frac{1}{2^{jw}} = 2^{-jw}$

4.4. Minor Collisions

A Minor collision occurs when at some iteration j ∈ [1, z] for two values ofr: r_1 and r_2, such that $r_1 \neq r_2$ we have $k_1^j = k_2^j \neq K_{2z-1} \rightarrow$ j

Lemma: Probability of the occurrence of the minor collision is around $\frac{2^{-jw}}{2}$

Proof: We know that k = g * r + hand

$$K^j = G_{z\rightarrow j} * r + H_{z\rightarrow j}$$

Now $K_1^j = G_{1z\rightarrow j} * r_1 + H_{1z\rightarrow j}$

$$K_2^j = G_{2z\rightarrow j} * r_2 + H_{2z\rightarrow j}$$

Case (i):

$$\text{Let } h_1 = h_2 \Rightarrow H_{1z\rightarrow j} = H_{2z\rightarrow j} \quad (10)$$

For $k_1^j = k_2^j$ we have

$$G_{1z} * r_1 + H_{1z\rightarrow j} = G_{2z\rightarrow j} * r_2 + H_{2z\rightarrow j}$$

$G_{1z\rightarrow j} * r_1 = G_{2z\rightarrow j} * r_2$ from (1)

$$\left|\frac{G_{1z\to j} * r_1}{2^{1+jw}}\right| = \left|\frac{G_{2z\to j} * r}{2^{1+jw}}\right| \quad (11)$$

Since z = $\left|\frac{l}{w}\right|$

$$z \le \frac{l-1}{w}$$

$$1 + zw \le l$$

$$r_1 \ge 2^l \text{ and } r_2 \ge 2^l$$

$$r_1 \ge 2^{l+jw} \text{ and } r_2 \ge 2^{l+jw}$$

$$\frac{r_1}{2^{1+jw}} \ge \frac{2^{1+zw}}{2^{1+jw}} \text{ and } \frac{r_2}{2^{1+jw}} \ge \frac{2^{1+zw}}{2^{1+jw}}$$

Therefore $\frac{r_1}{2^{1+jw}}$

And $\frac{r_2}{2^{1+jw}}$

Eq (2) possible only when $G_{1z\to j} = 0$ and

$$G_{2z\to j} = 0$$

Therefore the probability of occurrence of minor collision:

$$\frac{2^{1+zw} \diagup 2^{1+jw}}{2^{1+zw}} = \frac{1}{2^{1+jw}} = \frac{2^{-jw}}{2}$$

The above probability is the half of that of major collisions

Case (ii): Let $g_1 \ne g_2$ and $h_1 \ne h_2$

For $k_1^j = k_2^j$

$$G_{1z} * r_1 + H_{1z\to j} = G_{2z\to j} * r_2 + H_{2z\to j} + \left|\frac{H_{1z\to j}}{2^{1+jw}}\right| = \left|\frac{G_{2z\to j} * r}{2^{1+jw}}\right| \quad (12)$$

Since z = $\left|\frac{l}{w}\right|$

$$z \le \frac{l-1}{w}$$

$$1 + zw \le l$$

Now $r_1 \ge 2^l$, $r_2 \ge 2^l$

$$r_1 \ge 2^{l+jw}, r_2 \ge 2^{l+jw}$$

$$\frac{r_1}{2^{1+jw}} \ge \frac{2^{1+zw}}{2^{1+jw}} \text{ and } \frac{r_2}{2^{1+jw}} \ge \frac{2^{1+zw}}{2^{1+jw}}$$

$\frac{r_1}{2^{1+jw}}$ and $\frac{r_2}{2^{1+jw}}$

Eq (3) possible only when $G_{1z\to j} = 0$ and $G_{2z\to j} = 0$

Therefore the probability of occurrence of minor collision:

$$\frac{2^{1+zw} \diagup 2^{1+jw}}{2^{1+zw}} = \frac{1}{2^{1+jw}} = \frac{2^{-jw}}{2}$$

4.4.1. Algorithm: Fixed-Sequence Window Method

Window Methods

This method is sometimes referred to as m-ary method. What is common among them is that, if the window width is w, some multiples of the point P up to ($2^w - 1$) P are precomputed and stored and k is processed w bits at a time. k is recoded to the radix 2^w. k can be recoded in a way so that the average density of the nonzero digits in the recoding is 1/(w + ξ), where$0 \le \xi \le 2$ depends on the algorithm. This ECSM method is suitable for unknown or fixed point P. The cost is Storage: t points, where $2^{w-2} \le t \le 2^{w-1}$ depending on the algorithm. This ECSM method is suitable for unknown or fixed point P. The cost is Storage: t points, where $2^{w-2} \le t \le 2^{w-1}$ depending on the algorithm.

Algorithm: Fixed-sequence window method

Input: Window width w, d = $\left\lceil n / w \right\rceil$ an n-bit odd integer e and P $\in$ E(Fp).

Output: eP

1. Precomputation.

1.1 T [2^{w-1} w−1]← P.

1.2 T [2^{w-1} -1] ←2P.

1.3 For i from 2^{w-1} to $2^w - 2$ do

T [i + 1] ←T[i] + T[$2^w - 1$].

1.4 fori from $2^{w-1} - 1$ down to 0 do

T[i] ←−T[$2^w - 1 - i$].

2. e' = SHR(e) = (E'_{d-1}...E'_0) 2^w.

3. Q ←T[$E'_{d-1} + 2^{w-1}$].

4. For i from d − 2 down to 0 do

4.1 Q ← 2^w Q.

4.2 Q ←Q + T [E'_1].

5. Return (Q).

The Effect of Probability of Minor Collisions on Fixed Sequence Window

The Probability of major collisions = 2^{-jw+1}, j $\in [1, z-2]$

Mathematically we find the probability of occurrence of minor collision: = $\frac{2^{-jw}}{2}$ j$\in [1, z]$

4.4.2. Performance Comparisons

In the existing system according to major collisions the condition of major collision depends on the least significant jw +1 bits of g the probability of occurrence of this collision

is around 2^{-jw+1} for both values of which are expected to be equally likely. The condition of minor collision depends on the value of the least significant bits of length. The probability of the occurrence of these collisions is around $2^{-jw/2}$ for the both values of h_{jw} which are expected to be equally likely.

Experiments are conducted iteratively for n collisions and find out the length of bits according to n. When we taken the window length = 4, excluding the significant bits of w and the values of K^j the collisions average is 63%. The maximum number of collisions t are varied from higher towards the middle iterations, then first and last iterations from 12 for 40 bit integers and 23 for 50 bit integers. According to [7], it is not mathematically proved when the probability was reduced or increased according to the major collisions depends upon the value of the least significant jw bits of length. The probability of minor collisions is reduced up to 50% compared with that of major collisions. It is proved that when z ∈ [1, n] the minor collisions are reduced 50% of major collisions.

4.4.3. Role of Major and Minor Collisions in Side Channel Attacks

In the splitting process the key is split into k1 and k2 is performed before every elliptic curve scalar multiplication executions. If the key splitting process is subtraction, processing the key every time then the attacker can obtain the less information about the key words such as their hamming weights by averaging the side channel trace obtained.

J is a some end of iteration in different key splitting schemes. If the j is increases or decreases depending upon the key splitting schemes. It is difficult for the attacker to locate the instances to manipulate the key. Based on the value of iteration of j we can define the Major or Minor Collisions. But the probability increases with the iteration of ECSM algorithm the collisions are same in major collisions or minor collisions then the attacker locate the instances to trace the key processes the data. If the collisions are not same in major collisions or minor collisions, the attacker unable to locate the instances on the processing key either SPA attacks or DPA attacks.

5. Conclusion

We have presented a background on side-channel attack s along with the different methods used to against side-channel attacks. We provide the basic nature of the power analysis attacks and power consumption of cryptographic devices in side-channel analysis. SPA attacks can be prevented by making the ECSM execution uniform over all iterations, preferably with no dummy operations. The first order DPA attacks are based on the fact that intermediate points computed by the algorithm can be guessed by the attacker. Hence, to prevent them these intermediate points should be randomized. To resist those attacks, the key value should be randomized before the ECSM execution.

According to the existing system it is not proved the probability of minor collisions increased or reduced of that major collision depends on the value of the least significant bits of jw length. We proved that mathematically the minor collisions are reduced up to 50% of major collisions. We analysis the role of major and minor collisions in side channel attacks

Acknowledgements

I thankful to my son E. Digvijaykumar Reddy and my daughter E. Spandhana to encourage my research work when I was delayed at home. I was most thankful to my wife Smt. E. Gouri Sree to encourage my research work when I was disappointed with the review processes.

References

[1] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, “Towards sound approaches to counteract power-analysis attacks,” Advances in Cryptology - Crypto’ 99, LNCS 1666, pp. 398-412, Springer-Verlag, 1999.

[2] M. Ciet, Aspects of Fast and Secure Arithmetics for Elliptic Curve Cryptography, Ph.D .thesis, Universit ́e Catholique deLouvain, 2003.

[3] M. Ciet, J. J. Quisquater, and F. Sica, “Prevent-ing differential analysis in GLV elliptic curve scala rmultiplication,” Cryptographic Hardware and Embedded Systems - CHES’ 02, LNCS2523, pp. 540-550, Springer- Verlag, 2003.

[4] C. Clavier, and M. Joye, “Universal exponentiation algorithm a first step towards provable SPA resistance,” Cryptographic Hardware and Embedded Systems - CHES’ 01, LNCS 2162, pp. 300-308, Springer-Verlag, 2001.

[5] C. Clavier, and M. Joye, “Universal exponentiation algorithm a first step towards provable SPA-resistance,” Cryptographic Hardware and Embedded Systems - CHES’ 01, LNCS 2162, pp. 300-308, Springer-Verlag, 2001.

[6] J. S. Coron, “Resistance against differential powera nalysis for elliptic curve cryptosystems,” Crypto-graphic Hardware and Embedded Systems - CHES’99, LNCS 1717, pp. 292-302, Springer-Verlag, 1999.

[7] N. M. Ebied, Key Randomization Counter Measures To Power Analysis Attacks on EllipticCurve Cryptosystems, Ph.D thesis, University of Waterloo, On-tario, Canada, 2007

[8] C. Heuberger, and H. Prodinger, Personal commu-nication, Aug. 2003.

[9] M. Joye, and K. Villegas, “A protected division algorithm,” Smart Card Research and Advanced Applications - CARDIS’ 02, pp. 59-68, Usenix Association, 2002.

[10] M. Joy, DefenesAgainst Side Channel Analysis, Ad-vances in Elliptic Curve Cryptography, Chap5, Cam-bridge University Press, 2005.

[11] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” Advances in Cryptology –CRYPTO’ 99, LNCS 1666, pp.388-397, Springer-Verlag, 1999.

[12] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Investigations of power analysis attacks on smartcards," USENIX Workshop on Smart- card Technology, pp. 151-161. May 1999.

[13] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart card security under the threat of power analysis attacks," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541-552, May 2002.

[14] B. Moller, "Securing elliptic curve point multiplica-tion against side channel attacks, International Security Conference- ISC' 01, LNCS 2200, pp. 324-334, Springer-Verlag, 2001.

[15] K. Okeya, and T. Takagi, "The width-w NAF method provides small memory and fast elliptic scalar multiplications secure against side channel at-tacks," Topics in Cryptology –CT-RSA' 03, LNCS2612, pp. 328- 343, Springer-Verlag, 2003.

[16] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," Advances in Cryptology - CRYPTO' 99, LNCS 1666, pp.388-397, Springer-Verlag, 1999.

Biography

E. Kesavulu Reddy

Dr. E. Kesavulu Reddy, an Assistant Professor in Dept. of Computer Science, Sri Venkateswara University College of Commerce Management and Computer Science, Tirupati (AP)-India, he received Master of Computer Applications and Doctorate in Computer Science from S. V. University, Tirupati, Andhra Pradesh India. Also he received Master of Philosophy in Computer Science from M.K. University, Madurai, and Tamilnadu, India. He presented a paper in WCECS2010, U.S.A and two papers published in WCE 2011 & 2012, London, U.K. He published various papers in International Journals, also attending in International and National conferences. His research areas of interest in the field of Computer Science are Elliptic Curve Cryptography-Network Security, Data Mining, and Neural Networks.