Volume: 04 Issue: 06 Pages:1799-1808 (2013) ISSN : 0975-0290

Overview of the Side Channel Attacks

Dr.E.Kesavulu Reddy
Assistant Professor, Department of Computer Science, S.V.University, Tirupati.
Email : ekreddysvu2008@gmail.com

----------**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.

Index Terms: **Side-Channel Attacks, Simple Power Analysis Attacks, Differential Power Analysis Attacks**

Date of Submission: April 07,2013 Date of Acceptance: May 15,2013

1. Introduction

Smart cards are one of the major application fields of cryptographic algorithms, and may contain sensitive data, such as RSA private key. 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 [2], [3]. Side channel attacks can be often much more powerful than mathematical cryptanalysis

In recent years, security has become an important issue in the design of computer systems as more critical services are provided over the Internet and many networked devices communicate through wireless channels. Normally cryptographic algorithms are used to provide basic security functions such as confidentiality, authentication, and digital signature. Therefore their security is vital to any security mechanisms or protocols.

Mobile devices and sensor nodes that work in the field, not protected by physical security mechanisms, are more vulnerable to side-channel attacks. Among all side channel attacks, power analysis, which exploits the power consumption of a cryptographic system, can be carried out easily. It is very effective in breaking cryptographic algorithms [4], [7], [8]. In this type of attacks, adversaries learn what operations are performed and what data are processed by analyzing the power traces of computations. They can then figure out part or all of the bits in the secret key. A lot of work has been done on the countermeasures against power analysis attacks. Many countermeasures studied software implementations, trying to make the power consumption of a crypto system either random or identical for different keys .

The software countermeasures usually only work for specific algorithms and have large performance overhead. Very often, the countermeasures are found vulnerable to more advanced attacks. For example, randomized automata [15] for Elliptic Curve Cryptography operations are found not secure and can be broken by many
new attacks [6], [13], [16], [19]. There are some hardware countermeasures [11], [12], . The use of self-timed dual-rail logics is proposed in [11] to provide protection to power analysis attacks.

Both the two logic styles can make the power consumption of logic gates independent of the data values. One of the drawbacks of these methods is large area and power overhead. The method described in [12] compensates the power consumption of the system with voltage and frequency scaling techniques and an analog current injection circuit. However, besides large power overhead, frequency scaling affects the performance of software and may make the system vulnerable to timing attacks. It should be pointed out that memory security is not the primary focus of these above techniques. Some other hardware countermeasures are at the architectural level [9], [10]. They randomize either the register renaming [9] or the issue of instructions in the instruction window [10] to make the power analysis attacks more difficult. However, these methods may not fit well with the low-end processors, which typically do not have register renaming mechanism or large instruction window to support out-of-order execution.

2. Side-Channel Attacks

An encryption device is perceived as a unit that receives plaintext Input and produces ciphertext output and vice-versa. Attacks were earlier based on either knowing the ciphertext or both or on the ability to define what plaintext

Volume: 04 Issue: 06 Pages:1799-1808 (2013) ISSN : 0975-0290

is to be encrypted and then seeing the results of the encryption. To day, it is known that encryption devices have additional output and often additional inputs which are not the plaintext or the ciphertext. Encryption devices producing timing information that is easily measurable, radiation of various sorts power consumption statistics and more. Often the encryption device also has additional "Unintentional "inputs such as make use of some or all of this information, along with other cryptanalytic techniques, to recover the key the device using.

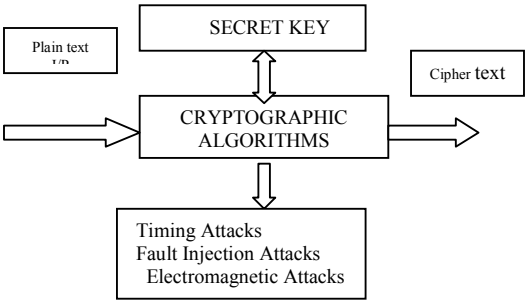

Fig.1. Basic level of Side-Channel Attack

3. Security Problem and Countermeasures

Several countermeasures to power analysis attacks have been suggested that alter the internal operation of the device under attack. So that the secret information content in the power analysis was leaked through the internal changes. Due to this type of changes the value of signature utilization is reduced. While these countermeasures may be effective. They require modification to the internal structure of the processing blocks. The basic information are passed from PC through PT(Power Tracer) to the smartcard(Electronic applications) to trace outs the encryption form of analysis in Power Tracer(PT).Power Tracer send the trigger signal to the digital oscilloscope[2]. The Digital oscilloscopes process these power data and transmit them to PC by network cable .Finally power data will be displayed by tracers in cryptanalysis software which was installed in PC. Data power is displayed in digital oscilloscope(Fig.2.2 shows).

Side Channel Analysis techniques are of based on the amount of time required for the attack and the analysis depends upon the type of attack. The most common types of attacks of Side Channel Information are

1. Timing Attacks.
2. Simple Power Analysis Attacks
3. Differential Power Analysis Attacks

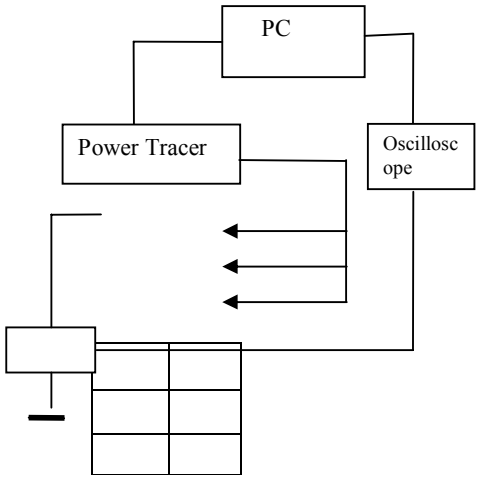

Fig: 2. Nature of Power Analysis

3. Timing Attacks

Timing attacks are based on measuring the time it takes for a unit to perform operations. This information can lead to information about the secret keys. For example, by carefully measuring the amount of time required to perform private key operations, an attacker might find fixed Diffe-Hellman exponents, factor RSA keys and break other cryptosystems[42]. If a unit is vulnerable, the attack is computationally simple and often requires only known ciphertext.

3.1. Countermeasures against Timing Attacks

3.1.1. Adding Delays

The most obvious way to prevent timing attacks is to make all operations take exactly the same amount of time. Unfortunately this often difficult. If a time is used to delay returning results until a pre-specified time factors such as the system responsiveness or power consumption may still change when the operation finishes in a way that can be detected [43].

According to [43] fixed time implementations are likely to be slow. Many performance optimizations can not be used since all operations must take as long as slowest operations. The number of samples required increases roughly as the sequence of the timing noise [43]. So random delays can make the attack a bit more difficult, but still possible.

3.1.2. Timing Equalization of Multiplication and Squaring

The time taken by the unit for the performance of multiplication and the performance of exponentiation actions should be set to be similar. Due to this quality an attacker will not be able to learn if, when and how many multiplications are made and how many exponentiations. This technique prevents timing attacks against the exponentiation operations. Those are performed as part of

Volume: 04 Issue: 06 Pages:1799-1808 (2013) ISSN : 0975-0290

symmetric encryption and which are subject to the most common attacks.

Cryptosystems often take slightly different amount of time to process different outputs. Performance characteristics typically depend on both the encryption key and the input data plaintext or cipher text. However as shown in[42] attacks exist which can exploit timing measurements from vulnerable systems, to find the entire Secret key.

Timing measurements are fed into a statistical model that can provide the guessed key bit with some degree of certainty. Computing the variances is easy and provides a good way to identify correct exponent bit guesses. The numbers of samples needed to gain enough information to allow the recovery of the key are determined by the properties of the signal and noise. More samples are required for more noise generally, error correction techniques increase the memory and processing requirements for the attack, but can greatly reduce the number of samples required.

3.1.3. Remote Timing Attacks

For over two decades, timing attacks have been an active area of research within applied cryptography. These attacks exploit cryptosystem or protocol implementations that do not run in constant time. When implementing an elliptic curve cryptosystem with a goal to provide side-channel resistance, the scalar multiplication routine is a critical component. In such instances, one attractive method often suggested in the literature is Montgomery's ladder that performs a fixed sequence of curve and field operations. Billy Bob Brumley and Nicola Tuveri [4] describe timing attack vulnerability in Open SSL's ladder implementation for curves over binary fields. We use this vulnerability to steal the private key of a TLS server where the server authenticates with ECDSA signatures. Using the timing of the exchanged messages, the messages themselves, and the signatures, we mount a lattice attack that recovers the private key.

4. Simple Power Analysis (SPA) Attacks

Simple Power Analysis is generally based on looking at the visual representation of the power consumption of a unit performs an encryption operation. Simple Power Analysis is a technique that involves direct interpretation of power consumption measurements collected during cryptographic operations. SPA can yield information about device's operation as well as key material.

The attacker directly observes a system's power consumption. The amount of power consumed varies depending on the microprocessor instruction performed. Large features such as DES rounds, RSA operations etc may be identified, since the operations performed by the microprocessor vary significantly during different part of these operations. Similarly many DES implementation have visible differences within permutations and shifts and can thus be broken using SPA.

Because SPA can reveal the sequence of instructions executed. It can be used to break cryptographic implementations in which the execution path depends on the data being processed such as DES key schedule, DES permutations, comparisons, multipliers and exponentiations. Most cryptographic units are tested and found to be vulnerable to SPA attacks, though according to [43] it is not difficult to design a system that should not be vulnerable to such attacks.

4.1.Countermeasures against Simple power Analysis Attacks

4.1.1. Power Consumption Balancing

Power consumption balancing techniques should be applied when possible dummy registers and gates should be added on which is useless. When ever an operation is performed in hardware, a complementary operation should be performed on a dummy element to assure that the total power consumption of the unit remains balanced according to some high value. such techniques by which the power consumption is constant and independent on input and key bits, presents all sorts of power consumption attacks such as SPA..

4.1.2.Hessian Elliptic Curves

In [2], Liardet and Smart suggest to represent elliptic curves as the intersection of two quadrics in P3 as a means to protect against side-channel attacks. Considering the special case of an elliptic curve whose order is divisible by 4 [2] they observe that the same algorithm can be used for adding and doubling points with 16 multiplications (see also [4] . Using [1] the proposed Hessian parameterization, only 12 multiplications are necessary for adding or doubling points. The Hessian parameterization gives thus a 33% improvement over the Jacobi parameterization. Another advantage of the Hessian parameterization is that points are represented with fewer coordinates, which results in substantial memory savings.

4.1.3. Lightweight SSL Implementation Resistant to Side-Channel Attacks

Ever-growing mobility and ubiquitous wireless Internet access raise the need for secure `communication with devices that may be severely constrained in terms of processing power, memory capacity and network speed. We [17] describe a lightweight implementation of the Secure Sockets Layer (SSL) protocol with a focus on small code size and low memory usage.

We [17] integrated a generic public-key crypto library into this SSL stack to support elliptic curve cryptography over arbitrary prime and binary fields. Furthermore, we aimed to secure the SSL handshake against side-channel attacks (in particular simple power analysis) by eliminating all data-dependent or key-dependent branches and memory accesses from the arithmetic operations and compare the resulting performance with an unprotected implementation.

Our lightweight SSL stack has only 6% of the code size and RAM requirements of Open SSL, but outperforms it

Volume: 04 Issue: 06 Pages:1799-1808 (2013) ISSN : 0975-0290

in point multiplication over prime fields when no appropriate countermeasures against side-channel attacks are implemented. With such countermeasures, however, the execution time of a typical SSL handshake increases by roughly 50%, but still completes in less than 160 msec on a 200 MHz PDA when using an elliptic curve over a 192-bit prime field.

4.1.4. A Simple Power Analysis Attack on the Serpent Key Schedule

Serpent was designed and submitted as an AES candidate proposal by Ross Anderson, EliBiham, and Lars Knudsen [7]. We describe an SPA attack on an 8-bit smart card implementation of the Serpent block cipher. Our attack uses measurements taken during an on-they key expansion together with linearity in the cipher's key schedule algorithm to drastically reduce the search time for an initial key. The results here show that Hamming weight measurements from 8-bit smart card implementations of Serpent's key schedule reveal enough side channel information to uniquely determine a 256-bit initial key in a few milliseconds.

More generally, we have shown that LFSRs may be very susceptible to SPA attacks and those algorithm designs can greatly accelerate side channel attacks. Kevin J. Compton¤ Brian Timmy Joel VanLavenz [6] suspect that the attack presented here can be made error-robust, as well, since we use only the first 200 rows of the reduced row echelon matrix [A "/e"]. The remaining 328 rows could be used for error correction. Also, pre-shift Hamming weights could be used.

4.1..5. Exponent Recodings for the Exponentiation against Side Channel Attacks

SAKAI & SAKURAI [8] propose a new side channel attack, where exponent recodings for public key cryptosystems such as RSA and ECDSA are considered. The known side channel attacks and countermeasures for public key cryptosystems were against the main stage (square and multiply stage) of the modular exponentiation (or the point multiplication on an elliptic curve).

AKAI and SAKURAI are [8] compute the exponent recoding has to be carried out before the main stage. There are some exponent recoding algorithms including conditional branches, in which instructions depend on the given exponent value. Consequently exponent recoding can constitute an information channel, providing the attacker with valuable information on the secret exponent. The width-w NAF and the unsigned/signed fractional window representation are used to recover the secret exponent on attack for exponent recoding in proposed algorithms

4.1.6. Countermeasures On ηT *pairing* Over Binary Fields

Since many efficient algorithms for implementing pairings have been proposed such as ηT pairing and the Ate pairing, pairings could be used in constraint devices such as smart cards. They are [9] investigated the security of the ηT pairing on supersingular curves over characteristic two against timing attack, SPA and DPA. To avoid such attacks we proposed explicit algorithms of the ηT pairing using randomized projective coordinates. We demonstrated that the proposed method is the most efficient countermeasure compared with previous techniques. We further demonstrated that the proposed algorithms are secure against SPA, DPA, and RPA. However, the proposed algorithms could be susceptible to higher-order DPA attacks. Thus, a direction for further research would be to investigate security against higher-order DPA.

4.1.7. Register File Resistant to Power Analysis Attacks

We [10] propose RFRF, a register file that is resistant to power analysis attacks. By storing a flipped copy of data and adding a pre charge phase for write operations, RFRF has the same number of transitions on bit lines for all read or write operations. We also validate our method with simulations. The results show that the power trace of RFRF is independent of data values. When combined with similar solutions for other processor components, it is expected that the proposed method can strongly protect the system from power analysis attacks.

The overhead of RFRF mainly comes from the redundant register bank and additional circuitry for the pre charge phase in writes and for the data bypassing during back-to back write and read. However, the overhead is considered worthwhile as chip security is becoming a top priority in most embedded systems. Future efforts will also be spent on improving the cost-efficiency of the solution. To reduce the power overhead, the RFRF has two working modes where only security applications incur energy overhead for the security enhancement. It should also be pointed out that due to variations in process, voltages, and temperature, as well as differences in routing of the two register banks, the power consumption may not always be absolutely independent on data values.

However, this effect is considered difficult to exploit for the power analysis attacks. RFRF will also be studied for other purposes such as thwarting fault analysis attacks and improving the reliability of devices.

4.1.8. Sommer's SPA attack

In, Sommer has provided experimental evidence that the Hamming weight of secret data can be found from a single power trace of a smart card. She studied an algorithm written in the assembly language of the 8-bit processor. The algorithm consisted of a loop, where in each iteration only the data value was changed and was then moved from the accumulator to an internal register or written to output ports. She collected traces of the power consumption of the card where the sampling rate was 50 samples per card clock cycle.

Volume: 04 Issue: 06 Pages:1799-1808 (2013) ISSN : 0975-0290

4.1.9. Single-Exponent, Multiple-Data Attack (SEMD)

In this attack, it is assumed that the attacker can make the card exponentiate several random inputs with the secret key and with another known key. The attacker collects the power consumption traces of the exponentiations that use the secret key and computes their average. He repeats this procedure again but with the known key (111 . . . 1)2 in his attack. He then subtracts the two averaged signals. The resulting signal will show spikes in the iterations where the bits of the two keys differ. The portions of the averaged signals that are data dependent or where the bits of the exponents agree will approach 0. Messerges' countermeasure to this attack is to blind the exponent before every exponentiation.

4.1.10. Multiple-Exponent, Single-Data Attack (MESD)

In this attack it is assumed that the cards will exponentiate the same input, not necessarily known to the attacker, with several keys of the attacker's choice. The attacker first collects the average power trace of the exponentiation of the input with the secret key. Now, assuming that the attacker knows the first j − 1most significant or least significant, depending on the algorithm—bits of the key, he wants to attack the jth bit. He guesses that this bit is 1 and sets a new key equal to the bits that he knows concatenated with the guessed bit and arbitrary value for the remaining bits. He asks the card to exponentiate several times the constant input with that key and collects the average power trace. He repeats this step with the guessed bit reset to 0. He subtracts each of the collected averaged traces from the original one. For the correct guess, the resulting trace will approach zero through all iterations including iteration j, but for the wrong guess, the resulting trace will depict differences in iteration j.

5. Differential Power Analysis (DPA) Attacks.

Differential Power Analysis attacks are harder to prevent. These attacks are not visible. The keys information obtained from statistical analysis and Error-correction techniques. DPA usually consists of data collection and data-analysis stages that make extensive statistical functions for noise filtering. It is also used for gaining additional information about the processes that the unit is performing.

In addition to large – scale power variations due to the instruction sequence, these effects correlated to the data values being manipulated. These variations tend to be smaller and are something overshadowed by measurement errors and other noise. In such cases it is still possible to break the systems using statistical functions tailored to the target algorithms. Because DPA automatically locality correlated regions in a device's power consumption. The attacker can target the implementation can be automated and little or no information.

To implement a DPA attack, an attacker first observes M encryption operation and captures power traces T[1 :: M] [1::K] containing k samples each. In addition the attacker records the cipher texts C [1::M]. Not necessary to known the plaintext. DPA analysis uses power consumption measurements and statistical methods to determine whether a key block guess k is correct. Analyzing the outer DES operation first , using the resulting key to decrypt the cipher texts , and attacking the next DES sub key can be find Triple – DES keys . DPA can use known plaintext or known cipher text and find encryption or decryption keys .

Several improvements can be applied to the data collection and DPA analysis process to reduce the number of samples required or to circumvent countermeasures. For example it is helpful to apply correctness for the measurement variance, yielding the significance of the variations instead of their magnitude. One variant of this approach, automated template DPA, can find DES keys using fewer than 15 traces from most smart cards .

High-order DPA involves looking at power consumptions between several sub-operations of the encryption operation. The DPA techniques described above analyze information across a simple event between multiple cryptographic sub-operations. It mentioned that there is no known unit that vulnerable to Higher-order DPA techniques and is not vulnerable to DPA as well. In other words the precautions that are taken to prevent DPA should be ones against that work against High-order DPA as well. According to [43] no systems are currently known that are resistant to DPA and are not resistant to high-Order DPA.

5.1. Countermeasures against differential power analysis attacks

5.1.1. Reduction of Signal Size

One approach to prevented DPA attacks is by reducing the signal sizes, such as by using constant execution path code, choosing operations that leak less information in this power consumption balancing Hamming weights and state transitions or by physically shielding the device. The signal size can not be reduce to zero when the attacker able to perform an infinite number of samples on DPA on the signal .

5.1.2. Addition of Noise

Another approach against DPA involves introducing noise into power consumption measurements. Like signal size reduction adding noise increase the number of samples required for an attack, possible to an unfeasibly large number.

5.1.3. DPA Resistant To Hardware Implementation of the RSA Cryptosystems

Volume: 04 Issue: 06 Pages:1799-1808 (2013) ISSN : 0975-0290

RSA [25] cryptosystem was implemented on hardware, and then modified to be resistant against Differential Power Analysis attacks by using the Randomized Table Window method. This is the first FPG realization of an algorithmic countermeasure which makes RSA resistant to power analysis attacks. Modular exponentiation is realized with Montgomery Modular Multiplication.

The Montgomery modular multiplier has been realized with Carry-Save Adders. Carry-Save representation has been used throughout the RSA encryption algorithm. The primarily implemented RSA architecture prevents the extraction of the secret key using Simple Power Analysis attacks. When comparing the protected implementation with the unprotected, it can be seen that the total time has increased by 24.2%, while the throughput has decreased by 19.5%. first hardware implementation of a RSA cryptosystem which is resistant to power analysis attacks.

Modular exponentiation is realized with Montgomery Modular Multiplication. The Montgomery modular multiplier has been realized with Carry-Save Adders. The primarily implemented RSA circuit's architecture prevents the extraction of the secret key using Simple Power Analysis attacks. In the second implementation of this work, the changes within the Randomized Table-Window Method (RT-WM) have been applied over the first implementation in order to have a DPA resistant implementation. This is the first hardware realization of RT-WM.

5.1.4. High-Level Simulation for Side Channel Attacks

In particular, differential power analysis (DPA) [20][21] is very risky, because it cracks security codes by statistically processing the difference in electricity consumption and can be easily attacked. Therefore, it is important to verify DPA in the early stage of designing an algorithm. This study proposes a new simulator that can evaluate the resistance of DPA at the algorithm design level. Moreover, experiments proved the validity of the proposed simulator. Paper [22] noticed that the hamming weight of the medium value in a round of data encryption standard (DES) cryptogram reflected a bias of the transition probability due to nonlinearity of substitution-box (S-BOX). This result indicated that DPA simulation at the algorithm level could be performed using the hamming weight as a power consumption model.

However, this simulation can not distinguish between hardware architectures. Next, regarding the logic design phase, a paper [23] extracted the logic toggle information from the results of delay simulation. Then the paper simulated a CPA attack using the logic toggle information as power consumption model. Regarding studies on tamper-resistance verification of actual devices, such as field-programmable gate array (FPGA) and application-specific ICs (ASICs), papers [24[25] reported a CPA evaluation according to the advanced encryption standard (AES) embedding method by using a side-channel attack standard evaluation board-R (SASEBO-R).

A tamper-resistance simulation method using a tamper-resistance simulation method using a High-accuracy power consumption model at the algorithm level developed in the present study has not been reported to our knowledge. This study proposed a new simulation method by which tamper resistance to an encryption device could be verified at the algorithm level. In the proposed simulation method, a sophisticated power consumption model was only introduced into a circuit block with nonlinearity, and it is a target of side-channel attack.

The verification environment defined by programming language was used in the other parts. Using this simulation method with mixed-level, high-accuracy and high-speed simulation could be realized. Using the encryption algorithm of AES, three device configuration methods of truth table, PPRM3, and composite field methods were evaluated. In the future, we will compare the results obtained in this study with those obtained by power analysis attacks such as DPA and CPA by using ASIC. Moreover, we will investigate interconnection delays at algorithm level.

5.1.5. Messerges DPA Attacks

Messerges et al. have mounted the following DPA-like attacks on smart cards running RSA exponentiation algorithms. Their attacks have been based on monitoring the power consumption leakage. They are mounted on left-to-right or right-to-left exponentiation algorithms that processed the key one bit at a time.

5.1.6. Zero-Exponent, Multiple-Data Attack (ZEMD)
This attack is the same DPA attack as explained in Section A.3. Hence, unlike the SEMD and the MESD attacks, it assumes that the attacker knows how the exponentiation algorithm is performed and can simulate it to compute intermediate points. The intermediate point computed by Messerges is the result of the multiplication in the iteration processing the guessed bit rather than the result of the squaring of the next iteration as was done by Coron. This is because his attack was on a square-and-multiply algorithm where the multiplication was performed only when the current bit of the key is 1. But Coron's attack was on a double-and-add-always algorithm where the addition was performed regardless of the value of the current bit and its result collected if that bit was 1. Hence, the result of the doubling of the next iteration can reveal the validity of the guess. Also Messerges used as a partitioning function the Hamming weight of some byte in the intermediate result being 8 or 0 Messerges' countermeasure to the MESD and the ZEMD attacks is to blind the input before every exponentiation and unbind it at the end

5.1.7. Second-Order DPA Attack

Volume: 04 Issue: 06 Pages:1799-1808 (2013) ISSN : 0975-0290

The definition of a high-order DPA attack was first presented by Kocher et al. [43] as a DPA attack that combines multiple samples from within a trace. The following is the definition according to Messerges [47]:An nth-order DPA attack makes use of n different samples in the power Consumption signal that correspond to n different intermediate values calculated during the execution of an algorithm. The power leakage model which is proposed, and experimentally verified, by Messerges assumes that the power consumption of an instruction, C (t), varies linearly with the Hamming weight H(w) of the data w processed by this instruction at time t. i.e. $C(t) = \in H(w) + l$.
Where $\in$ and l are some hardware-dependent constants.
Messerges presented a second-order DPA attack on a typical algorithm of a public key cryptosystem. He chose two instructions of the algorithm that are not necessarily consecutive to monitor their power consumption every time the algorithm is executed. The first instruction processes random data and the second one processes a part of the secret key XOR ed with input data XOR ed with the random data of the first instruction. To reveal bit j of the secret key, the attacker sets bit j of the input data to 0 and the other ones to random values and gathers the power consumption traces of both instructions with different input data. The attacker repeats the same procedure but with setting bit j of the input data to 1. By averaging the difference in power consumption between these two instructions for the 0 and 1 set of traces, the attacker could reveal the value of the key bits.

6. Preventing Side Channel Attacks.

6.1. General Data-Independent Calculations
All operations are performed by the module shall be data-independent in their time consumption. In other words, the time that operations take totally must be independent of input data or key data. The different sub operations are performed according to input or key bits, and these sub operations should take same number of clock cycles. The general feature of making the time needed for operation execution fixed for every piece of data prevents all timing attacks. This is because these attacks are based on variations in the computation time according to input and key bits.

6.2. Blinding

Techniques used for blinding signatures can be adapted to prevent attacks from knowing the input to the modular exponentiation function [17].

6.3.Avoiding Conditional Branching and Secret Intermediates

According to [4], avoiding procedures that can use secret intermediates of keys for conditional branching operations will mask many SPA characteristics. Software implementations of critical code shall not contain branching statement computations should be performed using functions that utilize elementary operations such as AND, OR and XOR and not using any branching and conditional of portions of the code.

6.4. Licensing Modified Algorithms

The most effective general solution is to design and implement cryptosystems with the assumption that information leak. A few companies develop approaches for securing existing cryptographic algorithms to make systems remain secure for ever though the underlying circuits may leak information.

7. Power Consumption Of Cryptographic Devices

7.1. Power Models

A requirement of a deferential power analysis attack which utilizes correlation as it's primary method of determining the key is that there be a model which can approximate the power consumption of a circuit during the encryption process. There are several different methods for constructing this power model. An accurate method for describing the power consumption of a device is to simulate the device in a software environment designed to show power consumption.

If the target cryptographic device has an architecture that is known, then such a simulation may provide a precise prediction of the power consumption of the circuit during encryption. In instances where the target device's architecture is not entirely known or it is infeasible to simulate it, a more general power model must be used. The power models currently used in these instances are the Hamming weight and the Hamming distance models.

7.2. Hamming Weight Power Model
The Hamming weight model is the most basic power consumption model. It is most applicable to approximate the power consumption of a circuit utilizing a data or address bus, and relies on the basic premise that a bus will consume an amount of power that is proportional to the numbers of bits that are switched on within that bus. If no bits are switched on, the bus will consume very little power compared to a data bus with all bits switched on.

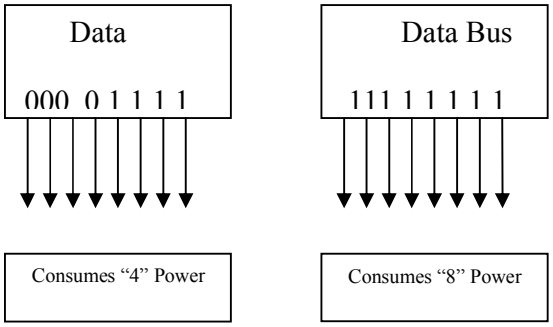

Fig..3.An example showing the Hamming weight model

Volume: 04 Issue: 06 Pages:1799-1808 (2013) ISSN : 0975-0290

The Hamming weight of the value on the data bus is taken to be proportional to the power consumption of the bus. This model can be used when very little information is known about the circuit that the attack is being performed on. It also carries an advantage over the Hamming distance model in that it does not require any information about the data on the bus during the encryption routine. However, the model only weakly describes power consumption within a circuit. While deferential power analysis attacks are possible using the HW model, they are not as efficient compared to the Hamming distance model. In general, whenever some information is known about the target circuit's implementation the HD model should be used [31].

7.3. Hamming Distance Power Model

The Hamming distance model is an extension of the Hamming weight model which uses changes in logic values in a certain time interval to determine power usage. The change can occur in many different circuit components such as a data or address bus, register, memory, or some other component. Using this model, you can determine the approximate power consumption of a circuit as being proportional to the number of 0,1 and 1,0 transitions made within the circuit. The number of bit transitions is simply the Hamming weight of the exclusive or of the two values. For example, the Hamming distance between two register values (R0 and R1) is given as: HD (R0; R1) = HW (R0 ` R1)

Several basic assumptions are made when this power model is used. It is assumed that bits which do not change (0,0, 1,1) do not contribute to the power consumption of a circuit. It is also assumed that a 0, 1 and 1, 0 transition consume an equal amount of power. In most circuits this may be found to not be the case. If more information is known about the specific power consumption of the device, minor enhancements can be made to the model by weighting transitions differently. An example showing how a register updating its value on a clock edge is shown in Figure.2.4

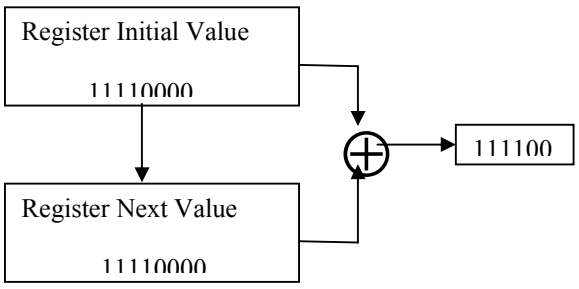

Fig. 4. An example showing the Hamming Distance model.

As the register updates from one state to the next, it consumes a certain amount of power. In this example, the Hamming distance shows that the power consumed when the register updates is proportional to 6. Regardless of the weaknesses, the Hamming distance model provides a very convenient method for determining the expected power consumption of a circuit during a certain time frame. In any case where a change in data can be observed, the Hamming distance model should be used over the Hamming weight model.

8. Scalar Multiplication

The operation consisting in calculating the multiple of a point $k \cdot P = P + P + \cdots + P$ (k times) is called scalar multiplication and the integer k is thus referred to as the scalar.

Scalar multiplication is used in ECDSA signature [1] and ECDH key agreement [2] protocols. Implementing such protocols on embedded devices requires particular care from both the efficiency and the security points of view. Indeed scalar multiplication turns out to be the most time consuming part of the aforementioned protocols, and since it uses secret values as scalars, side-channel analysis endangers the security of those protocols

8.1. Atomicity Improvement for ECSM

We [11] address the problem of protecting elliptic curve scalar multiplication implementations against side-channel analysis by using the atomicity principle. First of all we reexamine classical assumptions made by scalar multiplication designers and we point out that some of them are not relevant in the context of embedded devices. They describe the state-of the-art of atomic scalar multiplication and propose an atomic pattern improvement method. Compared to the most efficient atomic scalar multiplication published so far, our technique shows an average improvement of up to 10.6%.

We [11] propose a new atomic pattern for scalar multiplication on elliptic curves over Fp and detail our method for atomic pattern improvement. Firstly we maximize the use of squarings to replace multiplications since the latter are slower. Secondly we minimize the use of field additions and negations since they induce a non-negligible penalty.

In particular, they point out that the classical hypothesis taken by scalar multiplication designers to neglect the cost of additions/subtractions in Fp is not valid when focusing on embedded devices such as smart cards. In this cntext our method provides an average 18.3% improvement for the right-to-left mixed scalar multiplication from [12] protected with the atomic pattern from [13]. They recommend that algorithm designers, addressing the scope of embedded devices, take into account additions and subtractions cost when these operations are heavily used in an algorithm. Moreover the issue of designing efficient atomic patterns should be considered when proposing non regular sensitive algorithms.

8.2. Securing ECSM against Side-Channel Attacks

Volume: 04 Issue: 06 Pages:1799-1808 (2013) ISSN : 0975-0290

A common disadvantage is that each of them requires specially selected elliptic curves: All curves suitable for [27] group order divisible by 4; curves suitable for [1] group order divisible by 3; and curves suitable for [28] (curves with Montgomery form) again have group order divisible by 4. None of these methods is applicable to the NIST and SECG recommended curves given in [30] and [29], whose use is often encouraged in order to ease interoperability.

We [26] have presented a method for elliptic curve point multiplication that can be shown to provide security against side-channel attacks. The algorithm uses a special signed-digit encoding to ensure that point doublings and point additions occur in a uniform pattern. No dummy additions are required; implementing the method using randomized projective coordinates and storing precomputed points in extended point representation limits information leakage to a minimum.

9. Conclusion

We have presented a background on side-channel attacks along with the different methods used to countermeasures 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 (excluding Sommer's attack) 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.

AUTHOR INFORMATION

I am Dr.E.Kesavulu Reddy working as an Assistant Professor in Dept. of. Computer Science, Sri Venkateswara University College of Commerce Management and Computer Science, Tirupati (AP)-India. I received Master of Computer Applications and Doctorate in Computer Science from S.V.University, Tirupati, Andhra Pradesh India. Also I received Master of Philosophy in Computer Science from M.K. University, Madurai, and Tamilnadu, India. I am one paper presented in WCECS2010, U.S.A and two papers published in WCE 2011 & 2012, London, U.K. I published eight papers in International and five in National Journals, also attending in Five International and six National conferences. My research interest in the field of Computer Science in the area of Elliptic Curve Cryptography-Network Security, Data Mining, and Software Engineering.

REFERENCES

[1]. Agrawal D., B. Archambeault, J. R. Rao & P. Rohatgi. The EM Side- Channel(s) Attacks and Assessment Methodologies. Internet Security Group,IBM Watson search Center.

[2] . Anderson R Eli Biham, and Lars Knudsen. Serpent: A proposal for the Advanced Encryption Standard. In First Advanced Encryption Standard (AES) Candidate Conference, National Institute of Standards and Technology (NIST), 1998.

[3]. Awasthi A. K. and S. Lal, \ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings," International Journal of Network Security, vol. 4, no. 2, pp. 187-192, Sept. 2007.

[4]. Alexandridis. Georgios C. Artemios G. Voyiatzis, and Dimitrios N. Sopranos Crypto Palm: A Cryptographic Library for Palm OS "Pp 1-10 University of Patras, GR-26504, Patras Greece.

[5]. BAYAM. Keklik ALPTEKIN, Berna ORS " Differential Power Analysis Resistant Hardware Implementation of the RSA Cryptosystem ", Turk J Elec Eng & Computer Science, Vol.18, No.1, 2010, TUBITAK.

[6]. Billet. Ollivier and Marc Joye The Jacobi Model of an Elliptic Curve and Side Channel Analysis, Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Vol 2643 of Lecture Notes in Computer Science, pp 43-42, Springer Verlag, 2003.

[7]. Blake. I. F. G. Seroussi, and N. P. Smart, "Elliptic Curves in Cryptography," London Mathematical Society Lecture Note Series, 265, Cambridge Univ. Press, 2000.

[8]. Brumley and. Billy Bob, Nicola Tuveri Remote Timing Attacks are Still Practical? Aalto University School of Science, Finland.

[9]. Boneh, D. and Daswani, N. "Experimenting with electronic commerce on the PalmPilot". In proceedings of Financial Cryptography '99. Lecture Notes in Computer Science, vol. 1648. p 1 – 16 Springer-Verlag Heidelberg, 1999.

[10]. Boneh, D. ,R. A. DeMillo & R. J. Lipton. "On the importance of eliminating errors in cryptographic computations". Journal of Cryptology, pp 14:101–119, 2001 EUROCRYPT '97.

[11]. Boneh, D. and M. Franklin, "Identity-Based Encryption from the Weil Pairing," J. Kilian, Ed., Advances in Cryptology — CRYPTO, 2001, LNCS, vol. 2139, , pp. 213–29, Springer-Verlag, 2001.

[12]. Brown *et al* .M., "Software Implementation of the NIST Elliptic Curves over Prime Fields," D. Naccache, Ed., Topics in Cryptology — CT-RSA 2001, LNCS, vol.2020, pp 250–65 .Springer-Verlag, 2001, pp. 250–65.

[13]. Brown, M., Hankerson, D., Lopez, J., and Menezes, A. "Software Implementation of the NIST Elliptic Curves over Prime Fields" In proceedings of Cryptographer's Track at RSAConference 2001,SanFrancisco,Lecture Notes in Computer Science, vol. 2020, pp 250 – 265, Springer-Verlag Heidelberg, January 2001:

Volume: 04 Issue: 06 Pages:1799-1808 (2013) ISSN : 0975-0290

[14]. Certicom Press Release. "Certicom Announces Elliptic Curve Cryptosystem Challenge Winner". November 6, 2002.

[15]. Certicom Research. Standards for efficient cryptography {SEC 1: Elliptic curve cryptography. Version 1.0, 2000.

[16]. Chari. S, C. S. Jutla, J. R. Rao & P. Rohatgi. "Towards sound approaches to Counteract power-analysis attacks." In Advances in Cryptology – CRYPTO 99, LNCS, vol. 1666, pp. 398–412. Springer-Verlag, 1999. 24.

[17]. Chevallier-Mames, M. Ciet, and M. Joye. Low-cost Solutions for Preventing Side-Channel Analysis, Side-Channel Atomicity. IEEE Transactions on Computers, 53(6):760–768, 2004.

[18]. Chudnovsky D. V, and G. V. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, Advances in *Applied Maths.* 7 (1986/7), 385{434.

[19]. Ciet. M. Aspects of Fast and Secure Arithmetic are for Elliptic Curve Cryp tography. Ph.D. thesis, pp 120, 170, 171, 180, Universities Catholiquede Louvain, 2003.

[20]. Ciet. M. & M. Joye. "(Virtually) free randomization techniques for elliptic curve Cryptography". In Information and Communications Security – ICICS '03, LNCS, vol. 2836, pp. 348–359. Springer-Verlag, 2003.

[21]. Ciet. M., J.-J. Quisquater & F. Sica. "Preventing differential analysis in GLV Elliptic curve scalar multiplication". In Cryptographic Hardware and Embedded Systems – CHES '02, LNCS, vol. 2523, pp. 540–550, 4, 25, 126, 173, 179. Springer- Verlag, 2003.

[22]. Ciet *et al.* M, "Trading Inversions for Multiplications in Elliptic Curve Cryptography," preprint, 2003.

[23]. Clavier. C & M. Joye. "Universal exponentiation algorithm a first step towards provable SPA-resistance". In Cryptographic Hardware and Embedded Systems CHES '01, LNCS, vol. 2162, pp. 300–308, 4, 24, 120, Springer-Verlag, 2001.

[24]. Compton. Kevin J, Brian Timmy. Joel VanLavenz, A Simple Power Analysis Attack on the Serpent Key Schedule, Computer Science and Engineering ***Division***, MI 48109-2212, USA, September 24, 2009.

[25]. Coron. J.-S,"Resistance against differential power analysis for elliptic curve Cryptosystems". In Cryptographic Hardware and Embedded Systems – CHES 99, LNCS, vol. 1717, pp. 292–302., 2, 22, 24, 158, 170, 180, 181, 186, Springer - Verlag, 1999.

[26]. Daniel M. Gordon, "A Survey of Fast Exponentiation Methods,"Algorithms,Vol 27, No. 1, pp . 129–46 , 1998.

[27]. ElGamal.T, "A public key cryptosystems and a signature scheme based on Discrete logarithms" IEEE Transactions on Information Theory, 31(4), pp: 469– 472, 1985.

[28]. Enge, A. Elliptic curves and their applications to cryptography. Kluwer Academic Publishers, 1999

[29]. Elliptic Curve Cryptosystem: Remarks on the Security of the Elliptic Curve Cryptosystem, Certicom 1997.ECC Additional Groups for IKE, Mar. 2001.

[30]. Eisentraeger *et al.* K."Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation," M. Joye, Ed., Topics in Cryptology — CT-RSA 2003, LNCS, vol. 2612, pp. 343–54 Springer-Verlag, 2003.

[31]. Giacomo de Meulenaer and Francos' Xavier Standeart "Stealthy Compromise Wireless sensor Nodes with Power analysis Attacks" Associate Researcher of the Belgian Fund for Research.

[32]. Goos. G. and Hartmanis J., editors., "World Wide Number Field Sieve Factoring Record: on to 512 Bits," "Advances in Cryptology Asia crypt 96", Kyongju, Korea, LNCS, vol. 1163, pp. 382–94, Springer-Verlag, 1996.

[33]. Gupta. V. S. Gupta, and S. Chang, "Performance Analysis of Elliptic Curve Cryptography for SSL,"ACM Workshop Wireless Security, Mobicom 2002, Atlanta, A, Sept. 2002.