Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 11 (6): 1049-1053, 2011
ISSN 1812-5654 / DOI: 10.3923/jas.2011.1049.1053

A Novel Stegnosystem Design for Defying Differential Power Analysis Attacks on Smart Cards

[1]Hanan Mahmoud, [2]Khaled Alghathbar and [3]Alaaeldin Hafez
[1]Centre of Excellence in Information Assurance, Department of Computer Science,
College of Computer and Information Sciences, King Saud University, Saudi Arabia
[2]Centre of Excellence in Information Assurance, College of Computer and Information Sciences,
King Saud University, Saudi Arabia
[3]Department of Information System, College of Computer and Information Sciences,
King Saud University, Saudi Arabia

Abstract: Differential Power Analysis (DPA) attacks extract the secret key of cryptographic algorithm, by analyzing the power dissipation of the smart card during the execution of the computation. Cryptosystems such as DES, the AES and public-key cryptosystems are easily perceptive to the DPA attacks. Several techniques can be used to prevent differential power analysis attacks. One method is to design algorithms that have a constant execution path and use operations that have little variation in their power usage. In this paper, we are proposing algorithmic countermeasures for differential power analysis attacks on smart cards. The proposed countermeasure is to induce a new smart card system that is not cryptosystem. The new technique, namely stegnosystem, relies on using stegnography instead of cryptography. The user has to provide his/her password, which is compared to the password hidden in the smart card memory. The hidden password is retrieved by deciphering the stegnography key stored in the smart card. DPA attacks can measure power dissipation that leaks during deciphering the stegnography key, thus gain knowledge of the location where the password is hidden, but it cannot gain any information of the actual password without the actual possession of the smart card.

Key words: Smart cards, stegnography, DPA attacks, countermeasures

INTRODUCTION

Successful DPA attacks on cryptographic implementation were presented (Moore *et al*., 2002). Countermeasures techniques to DPA have been proposed. DPA countermeasures comprise random masking of intermediate variables (Jin *et al*., 2009). These are platform-dependent, which requires a considerable processing time overhead, augmented power consumption and area. While system level techniques comprise adding noise to the device power consumption through additional zlogic (Alioto *et al*., 2010a) which calls for circuit-level alteration, that requires more area. Random precharging countermeasures have been proposed to prevent DPA (Moore *et al*., 2002). These techniques perform by adding noise to the device power expenditure through random pre-charging.

Differential Power Analysis (DPA) attacks attempt to extract the secret key of cryptographic algorithm, by analyzing the power dissipation of the smart card during the execution of the computation (Hasan, 2001). Cryptosystems such as DES, the AES and public-key cryptosystems are easily perceptive to the DPA attacks (Moore *et al*., 2002). Research on Countermeasures has been considerably required in Hasan (2001). The study proposed the insertion of dummy code, power consumption randomization and balancing of data. But these methods are provably insufficient. Investigation on DPA attacks are applied on the AES algorithms to investigate general countermeasure, such as masking all the inputs and outputs for each operations used by the smart card. DPA attacks are possible because of the following:

- Binary encoding of data may result in power consumption proportional to the number of state changes (Azevedo *et al*., 2005)
- Data transmission on a bus dissipates power due to wire capacitance
- Bus activity is measured by the hamming weight of the state changes

Corresponding Author: Hanan Mahmoud, Centre of Excellence in Information Assurance, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Saudi Arabia

One valid method to reduce data dependent power dissipation is to use indirect data encoding scheme (Hasan, 2001). For instance, the data encoding scheme, 1-of-n code, dissipates constant power to transmit data, but it doesn't guarantee a data independent power signature. Another technique is to induce random noise to the power signature, but randomness can often be discovered and filtered out by signal averaging over repeated runs (Moore *et al*., 2002).

Gate level countermeasures based on masking at gatelevel have been perposed. These gate-level cells are achieved through a library of masked standard cells. On the other hand these countermeasures have large area, power dissipation overheads.

A transistor level approach to prevent DPA is based on the adoption of a logic family whose power consumption is independent of the processed data based on logic design at the transistor-level. They posses good security characteristics, but they are expensive in terms of area, performance and power consumption. For some applications combining more than one low cost countermeasure might be better than using an elevated implementation cost countermeasure.

Multibit Differential Power Analysis (DPA) attacks to precharged buses is presented in Alioto *et al.* (2010a) with stress on symmetric-key cryptographic algorithms. Analysis presents a deeper imminent into the dependence of the DPA on the parameters that identify the attack, the algorithm and the processor architecture. The main parameters of practical DPA attacks are analytically derived under appropriate approximations and a novel figure of merit to measure the effectiveness of DPA for multi-bit attacks is presented.

Conditions under which a cryptographic chip should be tested to assess its robustness is discussed in Alioto *et al.* (2010a). Several properties of DPA attacks are derived and suggestions to design algorithms and circuits with higher robustness against DPA are given. Their model is validated in the case of DES and AES algorithms.

Smartcard leaks power during encryption or signature (Jin *et al*., 2009). Differential power analysis (DPA) attackers can analysis encryption key from power data; RSA is a widely used public key algorithms. Nevertheless, when it is implemented in embedded devices, it is threatened by power analysis. DPA methods based on algorithmic level of RSA and methods against DPA are studied and a countermeasure of triple masking method against DPA roundly have been implemented in Jin *et al.* (2009).

POWER ANALYSIS ATTACKS

Smart cards microprocessors dissipate different amounts of power according to the instructions being executed. Switching current drawn by the transistors varies along the logic path for different instruction. Therefore, It is possible to gain great knowledge of the internal algorithms being used in smartcards by simply examining power traces. This is known as simple power analysis. On the other hand, differential power analysis is a better, more sophisticated statistical techniques that can detect small power variations such that individual bits can be identified, resulting in secret key extracted from smartcards (Hasan, 2001; Daemen and Rijmen, 2002).

The differential power analysis has the ability to extract important information during the execution of the computation, power dissipation of the microcontroller or the electromagnetic radiations of the circuit can be measured and analyzed (McEvoy *et al*., 2009). DPA is defined as an attack against the smart card security and is executed to extract information about the secret key contained in the smartcard This is achieved by performing a statistical analysis of the electric consumption measured for a large number of computations performed with the same key (Amiel *et al*., 2009).

The effectiveness of the DPA attacks depends on the attackers ability to successfully generate the differential signal for the correct guess of the key symbols. The attacker attempts to maximize this signal in an effort to simplify the analysis on the monitored power signals. Number of techniques, including noise reduction using digital filtering and signal magnification by multiple bit DPA, have been investigated which can maximize the differential signal

SMARTCARD KEY CRYPTOGRAPHY

There are many smartcard key cryptography techniques in literature. In this section we are going to summarize symmetric and asymmetric key authentication techniques used in smart card.

Symmetric key authentication: The Digital Encryption Standard (DES) algorithm is a symmetric key cryptography method commonly used smart card systems. This method uses a stored, secret cryptographic key and the public DES algorithm in each smart card and card acceptor device (Hasan, 2001; Alioto *et al*., 2010b)

The technique in symmetric key authentication is as follows:

- The smart card gives the microprocessor serial number to the card acceptor device, which then combines the number with the master key to form the smart card key (K), which is loaded in the each smart card during card initialization
- The card acceptor device produces a random number (R) and encrypts it to form Y
- The smart card decrypts Y into X , returning X to the card acceptor device
- The card acceptor device compares R and X, accepting the card if the two values match

Asymmetric key authentication: Authentication using the asymmetric key algorithm such as RSA is presented in the following steps:

- The card acceptor device sends a random number (X) to the smart card
- The smart card sends its identification word (I) and the random number encrypted into Y with the secret key (k) in the smart card. It also provides its public key (n), in such a way a certificate formed with n and I. The certificate helps to validate the public key by the card acceptor device
- The card acceptor device checks the cards response by deciphering Y (X') and comparing it to the random number

RSA requires an exponentiation module for computing the electronic signature, a relatively large random access memory for storing intermediate values, program memory for storing the additional instructions.

COUNTERMEASURES

Several techniques can be used to prevent differential power analysis attacks. One method is to design algorithms that have a constant execution path and use operations that have little variation in their power usage. Unfortunately this variation cannot be reduced to zero and so power analysis is still possible (but would require a larger number of traces to detect the variations). Another approach is to provide aggressive shielding on the device, but this adds to the device's cost and size (Alioto *et al*., 2010b).

A third option is to introduce random noise into power consumption measurements. This will increase the number of samples required to detect variations, but cannot eliminate them completely. Key randomization can be used before each scalar multiplication. This is done by adding a number of redundant symbols and insert them at random locations in the secret key sequence. At the other end, for the technique to generate the shared secret in a righteous fashion, these redundant symbols, must nullify their own effects. The last approach is that to build up new design algorithms with the underlying hardware in mind. Thus, even though the underlying hardware may leak information, the algorithm will not be affected. For example, non-linear key update techniques could be used so that power traces cannot be correlated between transactions (Moore *et al*., 2002; Amiel *et al*., 2009; Jin *et al*., 2009).

NOVEL ALGORITHMIC COUNTERMEASURES FOR DIFFERENTIAL POWER ANALYSIS ATTACKS ON SMART CARDS

In this study, we are introducing a new technique for hiding the secret key in smart cards. The new technique is an algorithmic extension that does not need any new hardware design or alteration of smart cards.

Smart card design: The block diagram of original design of a cryptosystem smart card is presented in Fig. 1 (Hasan, 2001). The block diagram of the novel design of a Stegnosystem is depicted in Fig. 2. A more detailed block diagram of the novel design is presented in Fig. 3.

Algorithms: Algorithm to add a password (Account-Id A, password P, BitArray Steg, address Addr).

- Input the password P
- Call stegenograph (Steg, P, address)

Fig. 1: Block diagram of a cryptosystem smart card which has its secret key stored and relies on an external power source (Hasan, 2001)

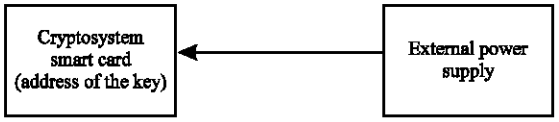

Fig. 2: Block diagram of a stegnosystem smart card which has its secret key stegnographed and relies on an external power source

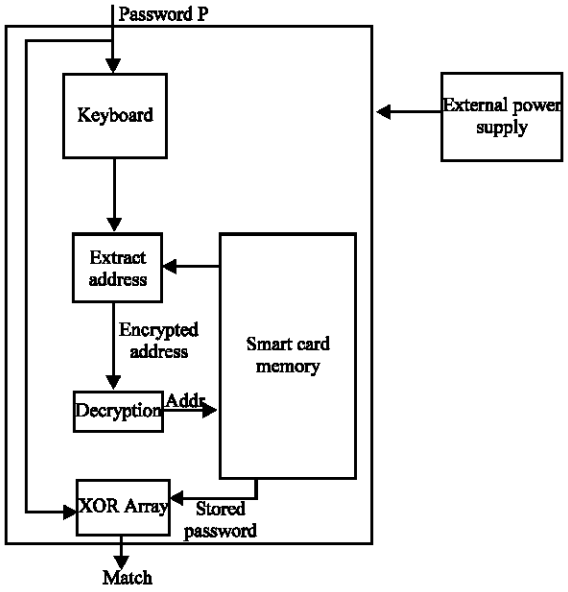

Fig. 3: The Detailed proposed stegnosystem for smart card

- Encrypt address into key
- Save the key in place Addr

Algorithm stegenograph (Steg, P, address)

- Hide P in steg
- Get the address where P is hidden (It can be the key to resolve the stegnography algorithm)

Algorithm authenticate (password P)

- User input the password P
- Decrypt (address)
- Extract the hidden password P
- X= Compare (P,P1)//using XOR
- If X=0 then P=P1 and authenticate the user

Stegnosystem key authentications: Authentication using the stegnosystem key algorithm is presented in the following steps.

- The card acceptor device accepts a value R from the owner of the smart card
- The smart card sends the encrypted location of the key from its memory to the card acceptor device
- The card acceptor device decrypt the number with the master key to form the smart card key (K), which is loaded in the each smart card during card initialization

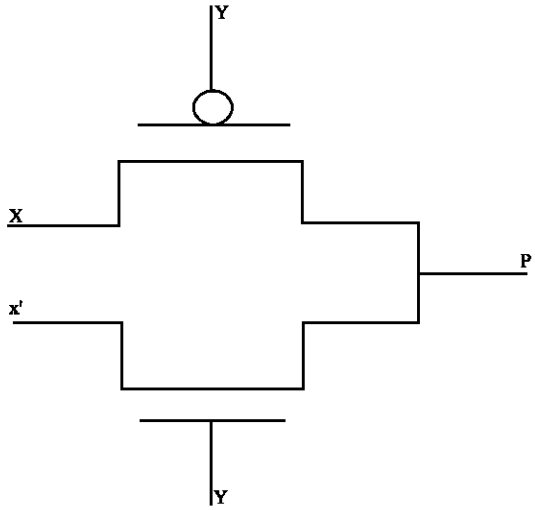

Fig. 4: The design for the XOR

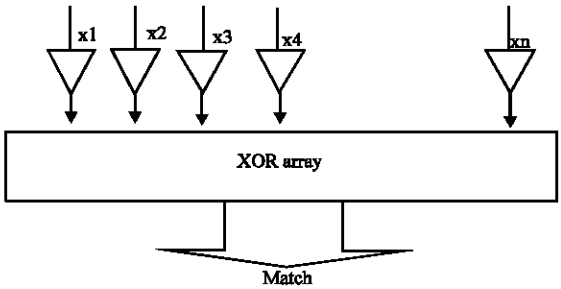

Fig. 5: The design for the match unit using invertors and XORs

- The smart card returns the value (K) into X (value (K) means the value stored at location K), returning X to the card acceptor device
- The card acceptor device compares R and X, accepting the card if the two values match

XOR DESIGN

The power trace from the cryptographic algorithm to decrypt the location of the password (key) can be attacked by a DPA and it can be analysed and the stegnography of the key in the memory can be retrieved. This will be of no use to any invasive attack (no physical possession of the key). The information that can be extracted by the DPA is useless, because the user has to provide the password that then will be xored by the value stegnographed to get a match.

We can use different design for XORs and we can choose the design in Fig. 4, because it gives the same transistor transitions in both cases for inputs 00 and 11.

Other design has to be carefully examined to make sure that the power traces generated is the same for the inputs 00 and 11. The proposed XOR was presented by the principal of Mahmoud and Bayoumi (1999). Same design can be implemented using transmission gates instead of pass transistors. The match unit that takes n bits and exclusive or them is shown in Fig. 5.

CONCLUSIONS

In this study we proposed an algorithmic countermeasure for differential power analysis attacks on smart cards. The proposed countermeasure is done by inducing a new smart card system that is not cryptosystem. The new technique, namely stegnosystem, relies on using stegnography instead of cryptography. The user has to provide her password which is compared to the password hidden in the smart card memory. The hidden password is retrieved by deciphering the stegnography key stored in the smart card. DPA attacks can measure power dissipation that leaks during deciphering the stegnography key, thus gain knowledge of the location where the password is hidden but it can't gain any information of the actual password without the actual possession of the smart card.

REFERENCES

Alioto, M., M. Poli and S. Rocchi, 2010a. A general power model of differential power analysis attacks to static logic circuits. IEEE Trans. VLSI Syst., 18: 711-724.

Alioto, M., M. Poli and S. Rocchi, 2010b. Differential power analysis attacks to precharged buses: A general analysis for symmetric-key cryptographic algorithms. IEEE Trans. Dependable Secure Comput., 7: 226-239.

Amiel, F., B. Feix, M. Tunstall, C. Whelan and W.P. Marnane, 2009. Distinguishing multiplications from squaring operations. Lecture Notes Comput. Sci., 5394: 346-360.

Azevedo, A., A. Kejariwal, A. Veidenbaum and A. Nicolau, 2005. High performance annotation-aware JVM for Java cards. Proceedings of the 5th ACM International Conference on Embedded Software, Sept. 19-22, New Jersey, USA., pp: 52-61.

Daemen, J. and V. Rijmen, 2002. The Design of Rijndael: AES-the Advanced Encryption Standard. Springer-Verlag, Berline.

Hasan, M.A., 2001. Power analysis attacks and algorithmic approaches to their countermeasures for koblitz curve cryptosystems. IEEE Trans. Comput., 50: 1071-1083.

Jin, J.F., E.H. Lu and X.W. Gao, 2009. Resistance DPA of RSA on smartcard. Proceedings of the 5th International Conference on Information Assurance and Security, Aug. 18-20, Xi'An China, pp: 406-409.

Mahmoud, H.A. and M.A. Bayoumi, 1999. A 10-transistor low-power high speed full adder cell. Proceedings of IEEE IEEE International Symposium on Circuits and Systems, July 1999, Orlando, pp: 43-46.

McEvoy, R.P., C.C. Murphy, W.P. Marnane and M. Tunstall, 2009. Isolated WDDL: A hiding countermeasure for differential power analysis on FPGAs. ACM Trans. Reconfigurable Technol. Syst., 2: 1-23.

Moore, S., R. Anderson, P. Cunningham, R. Mullins and G. Taylor, 2002. Improving smart card security using self-timed circuits. Proceedings of the 8th International Symposium on Asynchronous Circuits and Systems, April 8-11, University of Cambridge, pp: 211-218.