Power Side Channel Analysis and Anomaly Detection of Modular Exponentiation Method in Digital Signature Algorithm Based Fpga

Burcu Sönmez[1]*Ahmet Bedri* Özer[2]

[1] Department of Computer Engineering, University of Agri Ibrahim Cecen, Agri, Turkey

[2]Department of Computer Engineering, University of Firat, Elazig, Turkey

Abstract. In this study, digital signature application was performed on FPGA with classical RSA and Chinese Remainder Theorem (CRT). The power consumption of the system was observed when the digital signature process was performed on the FPGA. In order to distinguish the modular exponentiation methods as the classical RSA and the Chinese Remainder Theorem (CRT), the anomaly detection method was applied to the digital signature application using the power side channel analysis of the system. According to the obtained result, it is proved that information about the structure of the algorithm executing in the system can be obtained by using the power information consumed by a cryptographic device.

1 Introduction

RSA-based digital signature applications are one of the most used signature applicationsin today. In a public key cryptosystem such as RSA [1] and ElGamal [2], the legitimate user can use the recipient's public key to encrypt a document. A particular recipient uses the secret key to decrypt the encrypted document. On the other hand, a user can sign a document with his private key and any recipient verify the signature using the public key of signer.Therefore, the digital signature can be used to prove the identity of the sender, to protect the privacy of the transmitted document, and to verify the integrity of the received document. The RSA algorithm is the most popular algorithm to secure the public key cryptosystem. It was proposed by Riyest, Shamir and Adleman in 1977 [1]. RSA algorithm is used as a public key cryptosystem in implemented digital signature application.In the classical RSA algorithm, modular exponentiation, left-to-right squared and multiplication algorithm are used. Modular exponentiation is a costly step in creating digital signatures. Especially when very large prime numbers are used in terms of security, modular exponentiation and modular multiplication operations are very costly. There are many commonly used rapid exponentiation and fast multiplication methods to increase efficiency. These methods are referred to in the literature as the Montgomery Multiplication Method and the Chinese Remainder Theorem [3,4]. The method used for the fast modular exponentiation is the Chinese Remainder Theorem. With this theorem, modular exponentiation process is performed as two separate modules. Then, the modules which are divided into two in the signature creation phase are combined [4]. In this case, the classical RSA-based digital signature application is performed in two separate modules instead of the one-step exponentiation in the Chinese Remainder Theorem and faster results are obtained in terms of performance. In this study, Digital Signature was implemented on FPGA using RSA open key cryptosystem with China Remainder Theorem. The power consumption of the digital signature application using a device is measured. The power consumption of the Chinese Remainder Theory and the classical RSA-based digital signature applications are compared.

2 Rsa Digital Signature Algorithm

To sign an M message with the RSA, an N value is obtained, where p and q are two large prime numbers, and the M message is transformed using a hash function representing the $m \epsilon Z_N$ and a padding operation.Then the $m^d \ modN$ is calculated using the secret key of the signer. Thus, a digital signature is obtained for the M message. Here d represents a secret key [5,6]. RSA is based on the modular exponentiation process which can be performed by algorithms of base, square, multiplication and modular exponentiation of digital signature generation calculations. The implemented classical RSA based digital signature algorithm is given in Algorithm 1.In algorithm 1, two prime numbers are chosen as p and q for the calculation of the N module to be used to generate the public (e) and private (d) keys. In step 4, if gcd (e, (n)) = 1 is true, it is certain that e is an inverse of the N module. Thus the secret key d is always present. In the given algorithm, public and private keys are calculated in steps 4 and 5.

Corresponding Author: bsonmez@agri.edu.tr

The power differences in the Chinese Theorem-based and classical RSA-based digital signature application arise in the 5th step, ie the modular exponential phase. As a result of detecting the obtained abnormality, modular exponentiation method can be easily distinguished for both methods.

Algorithm 1:

1. Two prime numbers p and q close to each other are selected.
2. N=p*q and ϕ (N) =(p-1)(q-1) are calculated.
3. An integer e is selected between 1 <e <(N).
4. An integer d is selected such that e*d = 1 (mod (N)).
5. $\mathrm{S} = \mathrm{M}^{\mathrm{d}}$ modNis computed. (S: digital signature)

3 Chinese Remainder Theorem (CRT)

RSA application with China Remainder Theorem (CRT) is a widely used algorithm that requires high performance of the RSA digital signature algorithm [7].Firstly, the signer first computes each prime factor p and q in the signing modüle, separately. Then, signature S modN is calculated using China Remainder Theorem. Since the size of p and q is approximately half that of N, exponentiation with CRT is four times faster than direct exponentiation. The implemented CRT based RSA digital signature algorithm is given in Algorithm 2.Important examples of side-channel attacks on CRT-based RSA digital signature implementation are given in [8] and [9].

Algorithm 2:

1. Two prime numbers p and q close to each other are selected.
2. N=p*q and ϕ (N) =(p-1)(q-1) are calculated.
3. An integer e is selected between 1 <e <(N).
4. An integer d is selected such that e*d = 1 (mod (N)).
5. $m_{p=}$ m (modp) and m_q= m (modq) are calculated.
6. d_p= d(mod (p-1)) and d_q=d(mod (q-1)) are calculated.
7. $\mathrm{xp} = \mathrm{m}_{\mathrm{p}}^{\mathrm{dp}}$ modpvexq = $\mathrm{m}_{\mathrm{q}}^{\mathrm{dq}}$ modq are calculated separately.

4 Power Side Channel Analysis and Anomaly Detection of ModularExponentiation

Power analysis attacks use dependency between the power consumption on a cryptographic device and the data being processed or performed [10]. With power analysis, the power consumption of the device is monitored by taking advantage of the system's current differences. In this way, there is a relationship between the power consumption of the device and the confidential information. Firstly, the power consumption of the device must be measured. For this purpose, a small-valued resistor is placed on the line between the circuit and the source, and current information is obtained by taking advantage of the voltage differences at both ends of the resistor [11]. The measurement setup is shown in Fig 1.

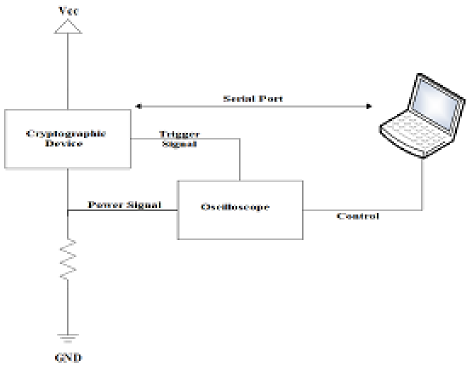

Fig 1 Measurement system for monitoring power consumption

In order to determine the modular exponentiation method of the digital signatures, the power side channel of the system is observed using the system in Fig 1.In [12], the necessary hardware information for power attacks is given in detail.One of the methods developed in recent years to prevent side channel attacks is the detection of the attack process using anomaly detection [13,14]. Anomaly detection is a method of machine learning techniques based on the problem of finding unexpected behaviors in data. These unsuitable templates are generally expressed in terms of anomalies, outliers, anomalous observations, exceptions, deviations [15].

In the performed power analysis attack, the power consumption of the digital signatures using the classical RSA algorithm and Chinese Remainder Theorem was used as an attribute. Information about the modular exponentiation method of the system according to the power side channel analysis has been obtained. The results obtained are given in the next section.

5 Experimental Results

In this study, Digital Signature was implemented on FPGA using RSA open key cryptosystem with China Remainder Theory. The Chinese Remainder Theorem compares the power consumption of classical RSA based digital signatures. As a result of the implemented digital signature application, it is observed that the Chinese Remainder Theorem consumes less power. In the implemented application, the message to be signed is processed as two separate sections as Mp and Mq. The digital signature is obtained by combining the separately performed modular exponentiation operations. Altera EP4CE115F29C7 set was used in the application. The ZXCT1021 low offset high-side current monitor integrated is used to detect the power consumed. A 0.1 ohm resistor is used in the application circuit for precisely measurement. Fig 2 shows the application circuit.

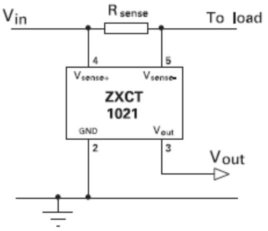

Fig 2 ZXCT1021 integrated circuit

Fig 3 shows the power consumption signal measured from the Vout pin of the ZXCT1021 integrated circuit shown in fig 3 as a result of the implementation of digital signature application with the Chinese Remainder Theory and the classical RSA on the experimental set. As a result of the obtained tension differences, it is observed that the digital signing application of Chinese Remainder Theorem in the modular exponential phase reduces the workload.

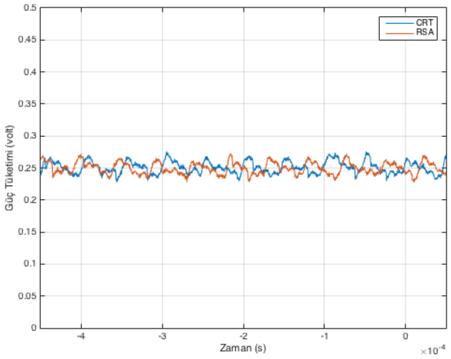

Fig 3 Chinese Remainder Theorem and RSA power traces

Especially when very large prime numbers are used, Chinese Remainder Theorem will be more advantageous than the classical RSA-based digital signature implementation of the Theorem.In order to distinguish the method used in a digital signature application from the values in this chart, an anomaly detection method is applied by using power consumption as information leak of the system. In this method, the k-average clustering algorithm is applied to the power consumption values of the system. The values outside the cluster were determined as anomaly values belonging to the Chinese Remainder Theorem, as shown in Fig 4.

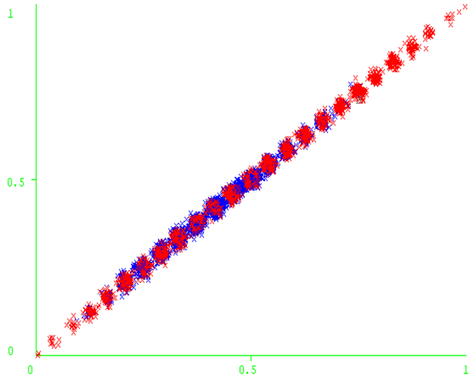

Fig 4 Anomaly detection results

The x and y axis in Fig 4 represent power consumption values. Blue marked values belong to the classical RSA algorithm, red marked value and Chinese Remainder Theorem (CRT) values. As can be seen in this figure, values greater than 0.75 have been found to be anomaly for the Chinese Remainder Theorem. According to the obtained result, it has been proved that information about the structure of the algorithm executing in the system can be obtained by using machine learning techniques by using the power information consumed by a cryptographic device. As a result of this study, it is observed that if the side channel measures are not taken for the systems, confidential information such as transactions, ciphers, keys can be obtained by using side channel information leaking from a system. This study attention to side channel analysis attacks. With the evolving technology, cryptographic devices need to be designed taking into account side channel attacks.

6 Conclusion

As a result of this study, it has been observed that if the side channel measures are not taken for the systems, information such as the processes and methods performed by the system can be obtained by using side channel information leaked from a system. With the evolving technology, cryptographic devices need to be designed to resist side channel attacks. In recent years, however, the use of cryptography in combination with artificial intelligence has become widespread as a support for information security. The study shows that artificial intelligence can be used in security measures such as intrusion detection methods.As a result of the information obtained, it has been proved that machine learning techniques can be used to detect attacks and obtain information about applied methods.

Preferences

1. R.*Rivest,* A.*Shamir*, L.*Adleman,* A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 120-126, 1978.
2. T.Elgamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, pp. 469–472, 1985.
3. P.Lawrence Montgomery, Modular Multiplication Without Trial Division, Mathematics of Computation, 4A 170, 519-521, 1985.
4. P.A.Fouque, N.Guillermin, D.Leresteux, M.*Tibouchi*, J.C.Za- palowicz, Attacking RSA-CRT Signatures with Faults on Montgomery Multiplication, Cryptographic Hardware and Embeded Sysytems CHES 2012.
5. C.Paar, J.Pelzl, Understanding Cryptography, Springer Heidelberg Dordrecht London New York, 2009.
6. C.D. Walter, Ç.K.Koç, Christof Paar, Cryptographic Hardware and Embedded Systems-CHES 2003, 5th International Workshop Cologne, 254-269, 2003.
7. J.J.Quisquater, C. Couvreur, Fast decipherment algorithm for RSA public-key cryptosystem, Electronics letters, 18(21), 905-907, 1982.
8. Kim, C., Ha, J., Kim, S. H., Kim, S., Yen, S. M., & Moon, S. A secure and practical CRT-based RSA to resist side channel attacks. In *International Conference on Computational Science and Its Applications*, pp. 150-158, Springer, Berlin, Heidelberg, May 2004.

9. Fournaris, A. P.,& Koufopavlou, O. CRT RSA Hardware Architecture with Fault and Simple Power Attack Countermeasures. In *Digital System Design (DSD), 2012 15th Euromicro Conference on* ,pp. 661-667, IEEE, September 2012.
10. Le T.H., Canovas C., Clédière J.,An overview of side channel analysis attacks, Proceedings of the 2008 ACM symposium on Information, computer and communications security Pages 33-43, Tokyo, March 18 – 20.
11. J.J.Quisquater, M.Rizk, Side Channel Attacks, Access Date: 24 March 2018,https://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf, October 2002.
12. Gamaarachchi, H.,& Ganegoda, H. Power Analysis Based Side Channel Attack. *arXiv preprint arXiv:1801.00932*, 2018.
13. M.Chiappetta, REAL TIME DETECTION OF CACHE-BASED SIDE-CHANNEL ATTACKS USING HARDWARE PERFORMANCE COUNTERS, Computer Science and Engineering, Master's Thesis, 2016.
14. M.Chiappetta, E.Savas, C.Yilmaz, Real time detection of cache-based side-channel attacks using hardware performance counters, Applied Soft Computing, Volume 49, 1162-1174, December 2016.
15. Chandola, Banerjee and Kumar, Anomaly Detection: A Survey, A modified version of this technical report will appear in ACM Computing Surveys, September 2009.