ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Review on Various Classification of Cryptographic Attack and The Countermeasures.

Elavarasi V[1]*, and Saravanan S[2].

[1]M.Tech VLSI Design, SASTRA UNIVERSITY, Thanjavur, Tamil Nadu, India-613401.
[2]Assistant Professor, School of Computing, SASTRA UNIVERSITY, Thanjavur, Tamil Nadu, India-613401.

ABSTRACT

It presents an analysis of bit stream reverse engineering and also the side-channel attacks which are able to modify the elements in cryptographic primitives. It broadly discuss about the devices which are under attacks like Xilinx Virtex II-Pro, V-4 and V-5, Xilinx Virtex-II and Altera stratix-II. These attacks are based on the power analysis, timing issues, correlated power analysis, Ring Oscillator (RO) based Trojan insertion and temperature based analysis etc. This provides an overview of attacks that can change the bit streams. DRAM is used as a storage element and in some cases it should be avoided. Cold-boot attacks can extract the bit streams even when the system is in off condition. This also includes the look-up table around the bit streams for security purposes. This design uses some algorithms such as AES, DES and 3DES which helps in providing security for the cryptographic primitives.

Keywords: Advanced Encryption Standard (AES), Data Encryption Standard (DES), Side-Channel Attack (SCA), FPGA.

Corresponding author

ISSN: 0975-8585

INTRODUCTION

Nowadays most of the digital systems and the advanced computer technology facing the same problems. The major problem is theft of the intellectual property and insertion of some of the hardware Trojans in to the cryptographic elements of the FPGA. By implementing these Trojans are made helpful in extracting the encryption or decryption keys from the bit streams of FPGA. In this review we are going to discuss about the details on various types of cryptanalysis attacks which causes major effects in the cryptographic primitives. The first attack is called side-channel attacks, here the attack is performed by the measurement of single power-up. The power analysis is executed for extracting the keys from the bit Strems. The next is bit stream reverse engineering, by doing reverse process of the bit streams the attackers can extract the bit streams from the FPGA. Using side channel analysis one can regain all the 128 bits of AES in 30,000 measurements. The insertion of hardware Trojans in to the bitstreams causes damage to the FPGA. This reveals the insufficient information about the location of the bit streams and it shows how they attack the internal functionality. Along with the bitstreams of FPGA there is also some advanced algorithm provided by the federal organization named AES, DES and Triple DES encryption and decryption algorithms which provides some sort of security related to the threat. They includes the look-up table around the bitstreams for security purposes. Some countermeasures are discussed against the cryptanalysis attacks and their positive and negative effects.

Side-channel attacks are the most realistic attack so that one can regain all the cryptographic elements during its single power-up analysis. This analysis can trace almost all the bit streams in 30,000 measurements within 3 hours. This can move all the physical information which can leak the cryptographic elements during the implementation process**.** Divide and conquer method is the basic principle behind this attack.

Hardware Trojans causes serious impact on the military applications and other security designs. Trojans are inserted into a system to extract the physical information and some may leads to the malfunctions. This results in lowering the reliability and leakage of the elements in the cryptographic primitives. These Trojans has different detection methods such as side-channel analysis method and full Trojan activation method.

RELATED WORKS

In paper [1] it describes about the FPGA configurations and the implementations. FPGA security Foundations, principles, design and flow manufacturer, usage of the software, and model attacks such as reverse-engineering, side-channel analysis, counterfeit, and invasive and semi-invasive attacks. It provides a secure remote configuration which includes updated logics, updates server routines, authenticity and confidentiality.It specifies the encryption algorithm AES 32 modules, AES 128 and AES 128U modules.It gives a brief illustration about the encryption and decryption algorithm. Finally they discuss about the applications and their source code, optimization goal and the disadvantages.

Many digital system have been used FPGA as the major component for the design.To avoid the attacks and to protect the IP we need to provide bitstream encryption feature which is a hardwired and it allows the user to protect their designs from the attacks. In side-channel attacks, the power analysis attack [2] is done to extract the secret keys that is used for the decryption in the FPGA during configuration.

Besides the other attacks such as reverse engineering, hardware Trojans,side-channel attack is the basic attack to be considerwhich affects the bit stream encryption.It can easily extract the secret keys in 3 minutes. Xilinx also include a lithium battery which provides security for the key but it cannot be abolished during attacks. Even though Xilinx design an unclear bit streamswe cannot experience an action against the side-channel attacks.As the result of the attacks the bit streams becomes uncomplicated. This makes an undesirable damage to the reliability of the products.

It is similar to the paper [2], it describes about the need of countermeasure for the side-channel analysis. It includes the consequences of analysing the Virtex-4 and Virtex-5 family shows that the bitstream encryption are entirely smashed with modest effort. The key extraction is made possible by using single

power-up analysis so we should target in changing the locality of the key and also in handling the design to protect the IP from theft. Most of the corporate companies and also the government companies also facing these problems. Fabricators of highly securedconfection and safety interpretation labs are known about the side-channel analysis.

FPGA manufacturers are responsible forproviding a secure IP protection system. But in the case of microcontroller the designer can manipulate the customised bootloaders. For e.g., adding encryption function to the coding. Some of the designers using the same security designs which will lowered the reliability of the newer product. Use of same security design should be avoided.Today computing power analysis can produce 60000 power breath using 32-bit key can be done in 4.5 hours. Here the side-channel attacks doesn't have any knowledge about the architecture. From our view an important problem in security technology is that both the purchasers and constructorare not concerned about the security affects that come with unguarded employment of cryptographic elements in embedded systems. We should take some measurements against the attackers to overwhelm the security problems.

In order to protect the intellectual property [4], FPGA has design the encryption algorithm such as AES and DES. Here it represent the advantageousattack on the bitstreams of the Altera Stratix II FPGA. Reverse engineering attack is made to extract the bitsteams from the FPGA. Using side channel analysis one can regain all the 128 bits of AES in 30,000 calibration. Moreover to the lost IP, the attacker again reprograming the FPGA with different code for locating the hardware Trojan confidentially which is danger for many security applications.

The side-channel analysis can regain all the encryption bitstreams after the reverse engineering function of the Quartus II. As an output of the effects offers replication of the products provide Altera Stratix II FPGA for which thecharacteristics of bit streams encryption develop into uncomplicated. This influences the military application. The Stratix II is a former generations of Altera FPGAs and due to the reality that SCA countermeasures have been eradicated at the time of development stage. However the latest families such as Stratix V or Arria II probably works on different pattern for bitstream encryption. Therefore analysing the recent stratix II family for high security protection is required for future process.

In paper [5] it describes about the other attack called Hardware Trojans. It reveals the information about how the hardware Trojans are inserted in to the encryption bitstreams in the FPGA. This attack proves the insufficient of the information about the bitstreams and the internal functionality. It shows how the Trojans are inserted and how they are moved to other internal systems.In this paper, there are some of the techniques to prevent those attacks. It generate the state of being aware about the consequences of the attacks and about the FPGA.

Previously we discussed about the AES algorithm, after the existence of AES algorithm the need of the block ciphers become less. The algorithm has more advantages than the block ciphers. But in some of the situations the block ciphers are used. For example sensor networks and in Radio frequency identification tags. So they introduced a new block ciphers called ultra-light weight block cipher.Here [7] both the performance of hardware and security responses are important at the time of the design. They offer high security block sizewhen compared to other block cipher.

In opposite to the widespread assumption, DRAM is the memory storage element which stores the memory even though the power is lost. Because of this nature there is a restriction in an operating system to protect the cryptographic keys from the attacks. We practically signalize broaden and foreseeability of memory continuously and reporting the permanence times increased rapidly by cooling effect. They provide amodern method for detectingcryptographic keys in memory appearance and for editingerrors due to bit decay.

However the DRAM stores the data. It has some data even when the power is lost. Here we describes about the cold-rebooting [8] the system which can boot the computer while running condition and the information's are stored and the system can work as it is. By doing cold-reboot the data or the cryptographic keys extracted from the memory storage element and also the lock screen passwords, antivirus, software etc.

so that the DRAM is the untrusted storage element. We should avoid storing data in DRAM but it is not possible during architecture.

This paper [9] is published by federal organisation. It states two important cryptographic algorithms such as DES and triple DES to secure the data. At the time of data transmission or even storing the data it should be maintain confidentially. Transformation of original data into a ciphers and vice-verse needs a mathematical model.

It provides information about the physical security procedures, management practices, and computer or network admittance controls.

It discuss about the easiest method to climb up from the attacks without checking for the delusion in the present encryption algorithm such as AES and DES and also other cipher blocks. A simple attacks become more vulnerable even for a stronger algorithm due to weak implementation [10].It discuss about the feasibility of entire key recovery function and the uses of those design and also some of the countermeasures against the attacks.It picturize that the cryptographic primitives are implemented only inside the modules where they design. Most of the block ciphers and other algorithms are working in the same environment. This condition should be changed and it is the time to think correctly to recover from the attacks.

Federal Information Processing Standards Publications (FIPS PUBS) produces encipher algorithm called AES [11] which is approved by issued by the National Institute of Standards and Technology (NIST) which was approved by the Secretary of Commerce. It discuss about the input/output functions,Mathematical preliminaries, algorithm specification such as sub-bytes transformation, shift rows transformation, mix-columns transformation, add round key transformations and implementation issues.

Installing the new software in the cryptographic primitives was entirely of without any secure where some of the stranger can control the condition. They discuss in paper [12] about the encrypted-composed-functionwhich helps to protect the cryptography primitives from the white-box attacks experimentally. For an illustration it shows how the keys are hidden by a sequence of look-up tables which are key dependent feature. It partly given the statement about the AES implementation and their applications.

Regular methods of implementation of AES is uncomplicated for the white-box cryptography attacks, so for the first time we introduced the AES algorithm along with look-up tables constitute the encoded method. In this paper, they recognise the difficulty of component exhaustion and attack such as Square-like. The problem of attacks on multiple components or on multiple implementations remain to be thoroughly investigated.

Table 1: Comparison on Various Devices, Attacks, Protocols Used and Other Techniques

Ref No	Device Under Attack	Name Of Attacks	Attacks Based On	Configuration& Protocol Used	Other Techniques
2	Xilinx Virtex II-Pro	SCA Reverse Engineering	Power analysis, timing issues	JTAG, Master or Slave Select MAP mode and Master or Slave Serial mode.	Cross correlation, Digital filtering
3	Virtex -4 and virtex- 5	SCA	Correlation power analysis	TCK,JTAG, Slave Serial mode, Select MAP mode.	Shielding and moulding of electric circuits.
4	Altera stratix-II	SCA Reverse engineering	Power analysis, voltage Drop, CPA	Fast passive parallel(FPP), Active serial (AS), Passive Serial(PS)	Digital Pre-Processing.
	Xilinx Virtex-II	Insertion OF hardware	RO-based Trojan		CRC check

5		Trojans	insertion, temperature based.		
6	Block Cipher	SCA, Invasive – Hardware Attack	Power consumption, Timing Issues.		Tiny Encryption algorithm
7	S-BOX	Linear & cryptanalysis attack	Area Requirement		Walsh Co-efficient
8	DRAM memory element	Cold-Boot attack, Warm-Boot Attack	Power-Off, Transplant DRAM	Extensible Firmware Interface(EFI)	Decay Rate, Error Rate

CONCLUSION

This paper concentrates initially on the bit stream reverse engineering process to extract the keys from the FPGA, whereas in 3DES they can extract the entire keys within 3 minutes by the power trace of 25,000 measurements by using a cost effective oscilloscope with a small sample rate of 100MS/s. The content of the FPGA becomes uncomplicated after reverse engineering of the bit streams. The present approach gives the information about the side-channel attacks. Usability of same security design should be prohibited to avoid the theft.

An attacker (or) hacker not only extract the keys and reverse-engineer the bit stream, but also alter it and design an entirely new thing to be approved by the device. The insertion of hardware Trojans reveals the fact that it can change the entire module in the FPGA. Most of the designs have DRAM as the storage element, by using cold-boot attacks we can extract the keys even when the system is in off mode. These make the DRAM as untrusted storage element and restrict the use DRAM to store important data. A detailed discussion about the encryption algorithms such AES, DES and 3DES is carried out. By reviewing these algorithms along with its countermeasures we can provide more security to the key extraction and information available in FPGA.

REFERENCES

[1] Drimer S, April 2008; Vol: 96.
[2] Moradi A, Barenghi A, Kasper T, and Paar C, Extracting keys from Xilinx Virtex-II FPGAs in Proceedings of the 18th ACM Conference on Computer and Communications Security, ser. CCS '11. ACM, 2011; pp: 111–124.
[3] Moradi A, Kasper M, and Paar C, - CT-RSA 2012; Vol: 7178. Springer, 2012; pp: 1–18.
[4] Moradi A, Oswald D, Paar C, and Swierczynski P, 2013; pp: 91–100.
[5] Chakraborty R, Saha I, Palchaudhuri A, and Naik G, IEEE, April 2013; Vol: 30, no. 2, pp: 45–54.
[6] Bogdanov A, Knudsen L, Leander G, Paar C, Poschmann A, Robshaw M, Seurin Y, and Vikkelsoe C, CHES 2007, ser. Lecture Notes in Computer Science, Paillie. P and Verbauwhede. I, Eds. Springer-Verlag, 2007; Vol: 4727, pp: 450–466.
[7] Leander G. and Poschmann A, Carlet C and Sunar B, Eds. Springer-Verlag, 2007; Vol: 4547, pp: 159–176.
[8] Halderman. J A, Schoen. S D, Heninger D, Clarkson W, Paul W, Calandrino. J A, Feldman. A J, Appelbaum J, and Felten. E W, May 2009; Vol: 52, no. 5, pp: 91–98.
[9] NIST, FIPS-46-3: Data Encryption Standard (DES), National Institute of Standards and Technology (NIST) Std. 1999.
[10] Kerins T and Kursawe K, In 1st Benelux Workshop on Information and System Security WISSec, 2006; pp: 12.
[11] NIST, FIPS 197 Advanced Encryption Standard (AES), 2001.
[12] Stanley Chow. H J, Philip Eisen A and van Oorshot. P C, 2002; Vol: 2595, pp: 250–270.