A Novel Hardware Security Mechanism Using Hybrid Cryptography Algorithms

P.BoseBabu[1], Ch.Thanmai[2], J.Rupa Devi[3], A.Yashoda Rani[4]
[1]Asst. Prof, Dept. of ECE, [234]Students of ECE, Vijayawada, A.P.
Andhra Loyola Institute Of Engineering And Technology

Abstract- Data security is a primary concern for every communication system.The security techniques, today the most wide spread,and based on coding algorithms.Communication becomes an essential tool for any business,education,defence services etc.It is essential to transfer data safe and secure. At present various cryptography algorithms have been proposed and implemented. Those algorithms are classified into symmetric and asymmetric algorithms based on number of keys used. Even though several algorithms are used for data security,they compromise the security at the certain period Now the idea is to combine the several secure algorithms to provide a highly secure environment for data transmission.The algorithms that are going to be combined are SHA1 hashing algorithm and AES symmetric cryptographic algorithm.In which SHA1 is used for authentication of the trojan presence and AES is used for the diagnosis .With these two algorithms we ensure the security for the mobile communication while receiving a call.

Keywords- Hardware Trojan, AES, SHA-1, Message digest, cyper text.

I. INTRODUCTION

As today is the era of wireless communication which gives rise to mobile communication. Internet and network usage are increasing rapidly .Everyday a lot of digital data have been exchanging among users. Some of the data is sensitive that need to be protected from intruders.

Smart phones are valuable targets for hackers – more so than laptops or personal computers. This is because they can be used as a “pivot point” to attack heavily protected environments such as banks or critical national infrastructure. Hackers can redirect their malicious traffic through your phone and store collected data on it. This means that all forensics traces would point to you as the hacker rather than the real culprit.

Encryption algorithms play vital role to protect original data from unauthorized access. Since semiconductor manufacturing demands a large capital investment, the role of contract foundries has dramatically grown, increasing exposure to theft of masks, attacks by insertion of malicious circuitry, and unauthorized excess fabrication .

II. LITERATURE REVIEW

Komal Rege et.al [4] proposed a hybrid encryption scheme for Bluetooth communication security, using AES and RSA. The key of 128-bit is encrypted using RSA algorithm, similarly the message of sender is encrypted using AES cipher. Both encrypted AES-key and cipher text of message is used to generate a complex message, which is transmitted over the network. The decryption is exactly the reverse process of encryption algorithm. Palanisamy et.al [5] proposes a hybrid cryptography technique using RSA and AES algorithms. RSA algorithm uses a key size of 128-bytes. It uses two pairs of keys: public key and private key. One pair is used at sender site for encryption/decryption and the other one at receiver’s site. Ali E. TakiEl_Deen [3] has proposed a hybrid encryption algorithm using AES and Blowfish. Plaintext of 64-bit is encrypted using Blowfish algorithm generating 64-bit cipher text which is again encrypted using same algorithm, thus generating a new 64-bit cipher text. The two outputs 64+64=128-bit cipher text is now given as an input to AES algorithm, generating the final 128-bit cipher text. Blowfish and AES algorithms make use of 32-bit and 128-bit key size respectively for their rounds. A statistical comparison of AES, DES, RSA, and Blowfish algorithms has been also provided. RituPahal et.al [6] proposes an efficient implementation of AES. Instead of conventional 128-bit input, 200-bit input is copied into an array of 5*5 matrixes. The first nine rounds are same consisting of four transformations: Substitute Bytes, Shift Rows, Mix Columns, and Add Round Key, but in the final (10th) round transformation Mix Columns is not used. The results of proposed scheme are compared with 128-bit, 192-bit, and 256-bit AES techniques at the end.

III. HTH ATTACK MODEL

A Hardware Trojan Horse (HTH) is an intentional hardware alteration of the design specification or of the corresponding implementation. These alterations only affect the circuit’s functionality in a few specific circumstances and are hidden otherwise. HTHs are more difficult to detect, diagnose, and mask than design bugs or manufacturing faults since they are intentionally implanted to be unperceivable by the current debugging and testing methodologies and tools. The vast number of possibilities for implementing HTHs further complicates their detection. Diagnosis of HTHs can be especially intricate since a large number of Trojans may be present simultaneously in an IC. In addition, HTHs are not necessarily present in all ICs coming from a design. Since HTHs are embedded within the circuit and are active only under certain, very rare conditions, detection methods must be complex.

Here we present specific HTH, in an attempt to describe the nature of HTH attacks in general. A simple, yet powerful HTH attack is presented in Figure 1, which shows how ghost circuitry can be activated in a cell phone when specific inputs or data are detected at specific memory locations. The unshaded portion of the circuit represents the HTH circuitry when it is activated by a HTH caller ID number. Upon activation, the attacker bitstream (ABS) is activated and the initial cell phone design is corrupted. In this example, HTHs will either cause the cell phones to malfunction or cause confidential information to be leaked. Important information can be disclosed after activation of the HTH. The exploited phone can automatically dial a hidden spy third party when certain numbers are dialed.

Even though the number and types of potential hardware attacks are essentially unlimited, we currently classify HTH attacks into the seven following categories: (i) damage objectives; (ii) components and mechanisms of the attack; (iii) components of the IC under attack; (iv) duration and initiation mechanisms; (v) design phase implantation and usage phase; (vi) optimization level; and (vii) customization level. The HTH attackers desiderata may include alteration of the computed results, slowing the IC, increasing the power consumption, releasing confidential data, and facilitating sidechannel attacks by making the gates' power consumptions observable at output. Attackers can employ various techniques including excessive switching, interconnect resizing, and substrate noise addition. Components, such as gates, clocks, and memory are vulnerable to physical attacks. Attacks may be randomly or actively initiated, e.g., event triggered.

IV. PROPOSED METHODOLOGY

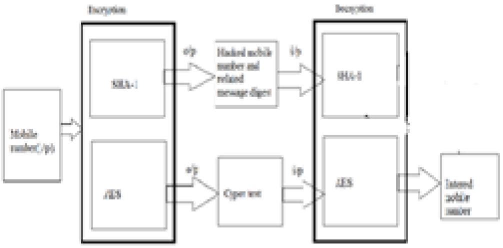

Fig.1: BLOCK DIAGRAM

i. Encryption Process

Mobile number is given as an input to both SHA-1 and AES.SHA generates the message digest to the dialled mobile number and on the other hand AES generates the cyper text to the mobile number.And these outputs are given to the SHA and AES decoders respectively.

ii. Decryption Process

At the decryption side SHA-1 again generates the message digest based on the received mobile number ,then a comparision circuit is used at the decoderto compare the newly generated message digest and the received message digest.

- If both the message digests are same then using the single SHA algorithm call gets forwarded to the original user.
- If both the message digests are not same then SHA receives the input from AES decoder and call gets forwaded.Here AES is used as a synchronizing signal.

SHA-1:

Secure Hash Algorithm (SHA-1) is a major message digest function developed by NSA. SHA-1 processes the data blocks of 512-bit and generates a message digest of 160-bit.The message digest is produced on similar principles used in MD4 and MD5, but SHA-1 has more conservative design. SHA-1 is used in several widely used protocols and security applications like TLS, SSL, PGP, SSH, S/MIME, and IPSEC. Secure Hash Algorithms comes in various flavors like SHA224, SHA256, SHA384, and SHA512.

AES :

AES Advanced Encryption Standard (AES) is a symmetric-key cryptographic technique. Unlike its predecessor DES, the structure of AES does not resemble to that of Feistel Structure. AES has a fixed block size of 128-bit and the key length must be 128, 192, or 256 bits. A 128-bit key thus gives a key space of 2128 keys. Number of rounds in AES is determined by the key size used in the process. Number of rounds will be 10, 12, 14 for key sizes of 128, 192, 256 bits respectively. First n-1 rounds contain four distinct transformations: Substitute Bytes, Shift Rows, Mix Columns, and Add Round Key. The final round contains only three transformations: Substitute Bytes, Shift Rows, and Add Round Key. AES offers a very high security and performance.The proposed scheme consists of two processes, encryption process and decryption process. Both processes make use of AES and SHA1. The reason we have selected these particular algorithms is discussed as:

AES is not only a secure cipher but it offers a very high performance and makes better use of resources. It is strong enough to be certified for use by the US government for top secret information Encryption Process .. SHA-1 a message digest function with a block size of 512- bit generates 160-bit message digest.So all the essential features of these algorithms are made available in our proposed hybrid algorithm. Better encryption of AES, along with the digital signature by making use of SHA-1 are included in a single hybrid system.

The figure below shows the process of the design .Whenever Trojan has been inserted with in the circuitary then it dials to the third party ,if not dials to the original number.And here we propose the detection mechanism through the hybrid algorithm techniques(SHA-1 and AES).

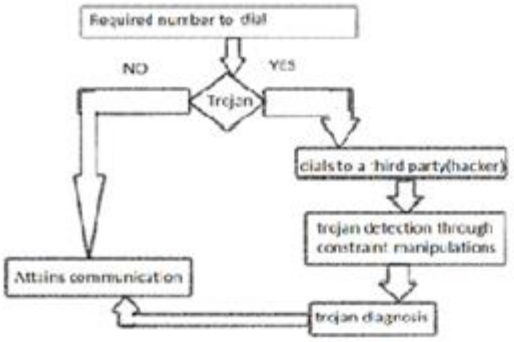
Required number to dial
NO
YES
Trojan
dials to a third party(hacker)
trojan detection through constraint manipulations
trojan diagnosis
Attains communication

Fig.2: Flow chart of the design

V. RESULTS

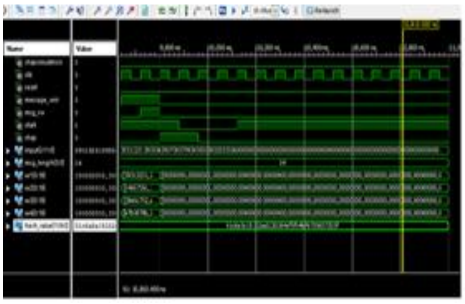

Fig.3:Output for original input

- Message digest for the given mobile number is as follows: **"01c6a3a15152ca0230384af5f64b76735637253f".**

Sha algorithm majorly has five steps and based on the input(mobile number) given it takes around 80 iterations and generates a 160 bit message digest value as shown above.

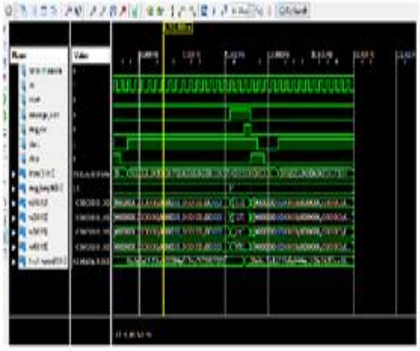

Fig.4: Output for hackedinput

- This represents the output at the decoder (BTS) .Such that in presence of malware it receives two different message digests one from the encoder and other from the received (hacked) mobile number. This case represents malware presence and call gets disconnected.

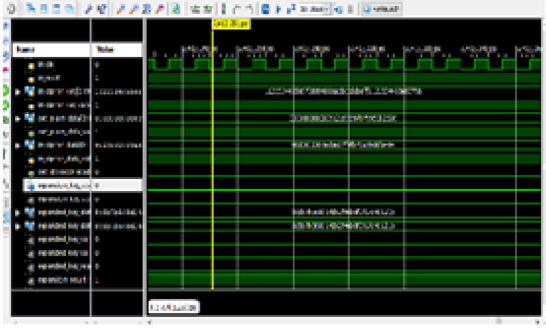

Fig.5:Output after diagnosis(aes decoder output)

- Whenever the message digests are unequal then AES inputs the original mobile number to the SHA decoder inorder to forward the call to the original user.

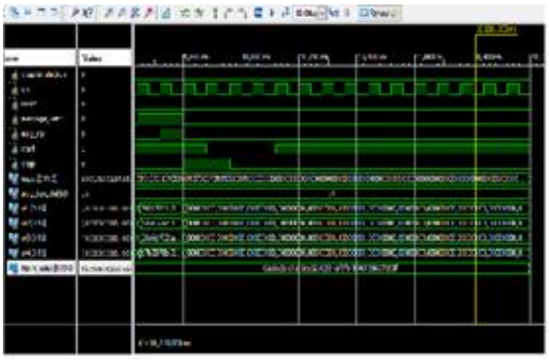

Fig.6:Output after diagnosis(sha decoder output)

- In presence of Trojan SHA decoder receives the output from the AES and forwards call to the original user.

VI. CONCLUSION

By making use of this hybrid cryptographic algorithms based on SHA and AES provides a very high security.In case of mobile communication by adding the extra feature called comparision of message digest generated by SHA algorithm prevents the mobile from malware insertion and thus provides high security. And AES acts as a synchronizing signal to divert the call to the original user whenever the malware insertion is identified.Thus,the combination of these two algorithms(AES and SHA) provides a high security to attain communication.

VII. FUTURE SCOPE

A software can be built for this purpose consisting many algoriyhms and then as soon as it receives password and data,it computes the algorithms to be used and their sequence based on the password and apply it to the data and during decryption, follow the same process and input the encrypted text and passwords to decrypt.This would improve the efficiency of hybrid system greatly.

VIII. REFERENCES

[1]. J. Zhang, Y. Lin, Y. Lyu, and G. Qu, "A PUF-FSM Binding Schemefor FPGA IP Protection and Pay-Per-Device Licensing," ITIFS, Vol. 10,No. 6, pp. 1137-1150, June 2015.

[2]. Z. Zhang, et al., "Securing FPGA-based Obsolete Component Replacement for Legacy Systems," to appear in Proc. ISQED'18.

[3]. Ali E. TakiEl_Deen , "Design and Implementation of Hybrid Encryption, International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013.

[4]. Komal Rege, Nikita Goenka, PoojaBhutada, Sunil Mane, " Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA", International Journal of Computer Applications (0975 – 8887) Volume 71– No.22, June 2013.

[5]. M. Majzoobi, F. Koushanfar, and M.Potkonjak, "FPGA-oriented Security," Springer, New York, 2011.

[6]. R. Druyer, et al., "A survey on security features in modern FPGAs,"Proc. ReCoSoC'15, pp. 1-8,June 2015.

[7]. Federal Information Processing Standards. Secure Hash Standard. FIPS PUB 180-2, August 1, 2002. With changes, February 25, 2004,

[8]. Paul Kocher, Joshua Jaffe, and Benjamin Jun, “Differentialpower analysis,” in Advances in Cryptology CRYPTO 99, pp.789–789.

[9]. G. E. Suh and S. Devadas. Physical unclonablefunctionsfor device authentication and secret key generation.Proceedingsof the Design Automation Conference (DAC), pages 9–14,2007.

[10]. I. Verbauwhede and P. Schaumont, “Design methods for securityand trust,” in Design, Automation and Test in Europe Conferenceand Exhibition, 2007. DATE ’07, 2007, pp. 1–6.