Biometric based Network Security using MIPS Cryptography Processor

Kirat Pal Singh
Senior Project Fellow
Council of Scientific and Industrial Research (CSIR) – Central Scientific Instruments Organization (CSIO)
CSIR-CSIO, Ministry of Science & Technology,
Chandigarh-160030
Email – kirataddiwal15@gmail.com

***Abstract*—The empowerment in network on chip (NOC) and System on chip (SOC) in Microelectronics and Sensors have developed the various wireless communication Network technologies. In the past few years, many researchers have been focusing on building system architecture of network monitoring to improve the technical requirement specially designed for network security. Less research was found in providing the strong biometric based network security system to provide bulletproof security. The popular MIPS based cryptography processor is used for hardware and software products and standards require big cryptography keys length for higher security level. The major weakness of Normal cryptography system based on asymmetric algorithms need the storage of secret keys. Stored keys are often protected by poorly selected user passwords that can either be guessed or obtained through brute force attacks. Combining biometric with MIPS cryptography processor is as a possible solution. In this paper I propose a new approach to network security using MIPS based crypto processor based on contactless palm vein biometric system. This approach takes into account NOC constraints and its topology. It provides more security with less key length and there is no need to store any private key anywhere.**

Keywords— Biometric, Network Security, Cryptograph, MIPS Processor, System on Chip.

I. Introduction

We are living in cyber age, where most of the information is produced with the help of computers and computer networks, which provides platform to do e-commerce tasks, online banking, and sharing of information and many more, and while more than two parties communicate to each other then they worry about confidentiality, data integrity, non-repudiation and privacy etc. [1]. In order to mitigate these issues, we can apply cryptography with biometrics. Cryptography is a kind of secret writing by which two parties can communicate with secret messages [2]. Most of the researches have demonstrated that biometric is the ultimate solution for identification and authentication, since it is proved as reliable and universally acceptable identification/authentication methods in many application areas [3].

Due to the popularity of biometrics and cryptography, the information security is becoming as a common demand in all applications area. Biometric is referred as automatic system that uses measurable, physical or physiological characteristics or behavioral traits to recognize the identity of an individual. Biometrics offers greater security in identification/ authentication system. However, the security level of the network can be further enhanced using cryptography and biometrics.

To secure the communication currently there are two popular kinds of cryptographic protocol namely symmetric key and public key protocol. In symmetric key protocol such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES) [2], a common key is used by both sender and receiver for encryption and decryption. This system provides high speed but have the drawback that a common key must be established for each pair of participants. In public key protocol there are two keys, public key and private key by which message can be encrypted and decrypted. One is kept private by owner and used for decryption. The other key is published to be used for encryption. Some of the most useful example of the public key cryptography is AES, RSA and Digital Signature Algorithm (DSA) [4]. Although, these algorithms of asymmetric crypto-systems are slower than that of the symmetric crypto-systems but they provide high level security. Due to comparative slowness of the public key cryptography algorithms, dedicated hardware support is desirable. MIPS crypto processor is used in most of the network and standards that uses public key cryptography for encryption, decryption and digital signature. The length of the keys for MIPS has been increased in recent years, and this is putting a heavier load on the application of MIPS crypto processor. It creates extra computation cost and processing overhead. However, other crypto processor compared to MIPS, offers higher security per bit with smaller key size. It provides higher security per bit. Since normal crypto processor has smaller key size, hence it also reduced the computation power, memory and bandwidth. Therefore, in this paper a model has been proposed for network security using MIPS crypto processor with biometric.

II. Previous Works

The main problem of asymmetric cryptography is the management of private key. No one should be able to access someone else’s private key. They need to store in such a place which is protected from unauthorized accessing. This is vulnerable for attacking by hackers. This creates big problem in asymmetric cryptography. Thus it can be solved by the use of biometric template. Private Key can be generated directly by the biometric template. Since private key can be generated

[1] A Preliminary version of this work appeared in the Proc. of QSHINE’13, LNICST Springer Link [12]

dynamically from one's biometric template, so there is no need to store private key anymore and network becomes more secure and safe. But there are very little work has been done in the field of AES with the help of biometric. Some of the suggested approaches are given. [1]. However these biometrics have lots of issues regarding training, capturing image, easily obscured by eyelashes, eyelids, lens and reflections from the cornea, lack of existing data deters ability, cost, voice can be captured while uttering the password, a camera can photograph an iris from across the room, and fingerprints left on surfaces can be lifted hours later etc. For some individuals, the iris image capturing is very difficult. Iris recognition system requires lots of memory to be stored. It is easily absurd by eyelash, eyelids, lens and reflection from the cornea. People are not much familiar with iris recognition system yet, so there are lots of myths and fears related to scanning the eye with light source. Iris recognition system works on the basis of acquisition of iris image, but acquisition of an iris image needs more training and attractiveness than most other biometrics. It cannot be verified by human too. The most problem with iris recognition system is its expensiveness. I have generated cryptographic key from user's face features and then the key has been applied in DES algorithm for encryption and decryption purposes and same way it have generated cryptographic key from user's voice while speaking a password[13], but no further implementation of key has been described on their paper.

Related application are as palm vein print is extremely difficult to forge and therefore contributes to a high level of security, because the technology measures hemoglobin flow through veins internal to the body.

We are generating cryptography keys from user's palm vein and then the generated key are used as user's secret keys for AES. Hence in proposed method we are using palm vein as a secret key instead of other biometric.

III. Biometric Security Consideration

While potentially offering significant security benefits, a biometric system is only one of many security tools available. Depending on the application, an environment or circumstance may or may not benefit from a biometric system. Understanding the operational requirements of the situation is necessary to determine if a biometric system can be used to meet a security need. The use of biometrics will not solve all of a system's security problems, but when properly implemented, a biometric system should be one part of overall security architecture. [5]

There is no single biometric modality that is best for all applications. Many factors must be taken into account when implementing a biometric system including location, security risks, task, expected number of users, user circumstances, existing data, etc. It is also important to note that biometric modalities are in varying stages of maturity and therefore may offer varying levels of security, ease of implementation, and user convenience.

Biometric systems alone do not currently provide adequate security for high assurance applications. When biometric systems (something you are) are combined with other security mechanisms (something you have and something you know), those systems can provide significant security benefits. However, the biometric system must be implemented correctly for the specific application.

IV. Biometric-Based Security Approaches for Data Authentication

Biometric is a technique commonly known as the automatic identification or verification of an individual by his or her physiological or behavioural characteristics. Biometric approach uses an intrinsic characteristic of the human body as the authentication identity to secure the distribution of a cipher key within NOC communications. Because of the data that are detected, collected and transmitted in NOC is comparatively sensitive, an ideal biometric trait should present 100% reliability, user friendly, fast operation and low cost. Besides, it is postulated that the utilized biometric should satisfy the following properties indicated in TABLE 1[6].

Table 1 Biometric Properties

Properties	Description
Universal	Possessed by the majority, if not the entire population.
Distinctive	Sufficiently different in any two individuals.
Permanent	Sufficiently invariant, with respect to the matching criterion, over a reasonable period of time.
Collectable	Easily collected and measured quantitatively.
Effective	Sufficiently invariant, with respect to the matching criterion, over a reasonable period of time.
Acceptable	Yield a biometric system with good performance that is given limited resources in terms of power consumption, computation complexity and memory storage, the characteristic should be able to be processed at a fast speed with recognized accuracy.
Invulnerable	Relatively difficult to reproduce such that the biometric system would not be easily circumvented by fraudulent acts.

V. Importance of the Research Problem

Today's microelectronics technology provides designers the possibility to integrate a large number of different functional blocks, usually referred as cores, into a single integrated circuit (IC). Such a design style allows designers to reuse previous designs and will lead therefore to shorter time-to-market and reduced cost. Such a system-on-chip (SoC) approach is very attractive from the designers' perspective. Testing of such systems, on the other hand, is a problematic and time consuming task, mainly due to the resulting IC's complexity and the high integration density [7].

According to the International Technology Roadmap for Semiconductors (ITRS), by the end of the decade, SoC, using 50-nm transistors operating below one volt, will grow to 4 billion transistors running at 10 GHz [8]. Such SoCs, based on nanometer-technologies, will most likely suffer from fault effects and new sources of errors that make them unfit for dependable systems, unless a high degree of fault tolerance and error compensation is built into such systems.

As indicated by several authors and the ITRS, nanometer SoCs will most likely not have an economic yield if all transistors must be functional [9]. Furthermore, deep sub-micron technologies will suffer from single event upsets (SEUs) caused by electromagnetic interference and by radioactive particles that trigger non-permanent faults. Finally, the specifically higher strain on materials caused by higher current densities and higher field strength is likely to cause wear-out effect in the field of operation. A design and test technology that may facilitate dependable systems on hardware that is not highly dependable is therefore becoming a must.

A major concern for such multi-billion transistor SoCs is also communication infrastructure, connecting the cores. To prevent the design of the communication architecture from becoming the bottleneck in the design of future SoCs, this communication architecture itself must be compositional and scalable. For that reason the on-chip interconnect will increasingly be implemented as a network-on-chip (NoC), complete with network interfaces, routers, and packet or circuit switching [10], [11]. Testing such systems shares all the problems related to testing modern nanometer SoCs, and introduces also some additional challenges due to the new issues, such as increased long wiring, that is much more vulnerable to timing errors and crosstalk. Therefore, for very large NoCs, additional test strategies, such as those applied in FPGAs should also be included.

A. Data Authentication Model

In the proposed model, the message authentication code can be generated with the input of biometric feature and hashes that are calculated based on the original message. Then, the message will be sent to the destination. At the destination point, if the received signal matches statistically, it will be accepted and authenticated. Otherwise, the message is denied and discarded. The key point of this technique is to utilize the statistically same biometric information at both ends without any synchronization to secure data distribution within Network. Figure 1 shows the proposed biometric-MIPS based security for data authentication in NOC.

There are several types of biometric systems to choose from when implementing an access control system. Which one(s) we recommend depends on your specific requirements. For physical access control applications, we almost always recommend using the biometric system in conjunction with other security mechanisms, such as card readers, PINs, and/or an attentive guard. For logical access control, biometric systems can provide some added security, but these also should be used in conjunction with other security mechanisms, such as passwords and/or tokens. We do not recommend using a biometric system in place of a password or other established security mechanism for logical access, but only as an added layer of security.

B. Architecture of MIPS crypto processor

The single chip MIPS crypto processor consists of various components like Datapath, Data I/O unit, Control Unit, Memory unit, Crypto Specific Unit, Dependency Resolver and Arithmetic Logic Unit. The dedicated data processing block consist of Datapath and Crypto IP core (coprocessor) that performs the128-bit AES cipher operation and a 64-bit DES/TDES cipher or decipher operation. Advanced Encryption Standard (AES) algorithm operates on 128bits block size by using cipher keys with lengths 128, 192 and 256 bits for encryption process respectively. The incoming data and key are stored in a matrix called state matrix and all the operations are performed over the state matrix [12]. Data Encryption Standard (DES) and Triple DES is a Symmetric crypto algorithm, which operates on 64-bit block size with 16 rounds. The input plaintext, cipher keys and output cipher text are of 64-bit. The main operation in DES and TDES is bit permutation and substitution in one round which is performed by the permutation unit. Datapath processing unit performs the 5 stages pipelining process inside the processor. It consists of Program Counter, 32-bit General Purpose Registers, Key Register and Sign Extender Unit. The program counter unit updates the values available at its input bus at every positive edge clock cycle and also fetches the next instruction from the instruction ROM memory. The registers are read from the General purpose register and the opcode is passed to the control unit which asserts the required control signals. Sign extension is used for calculating the effective address. The data and instruction memory have capability of storing 256 bytes and each byte is referred by the address in between 0 to 256. The address is represented by 8-bits.

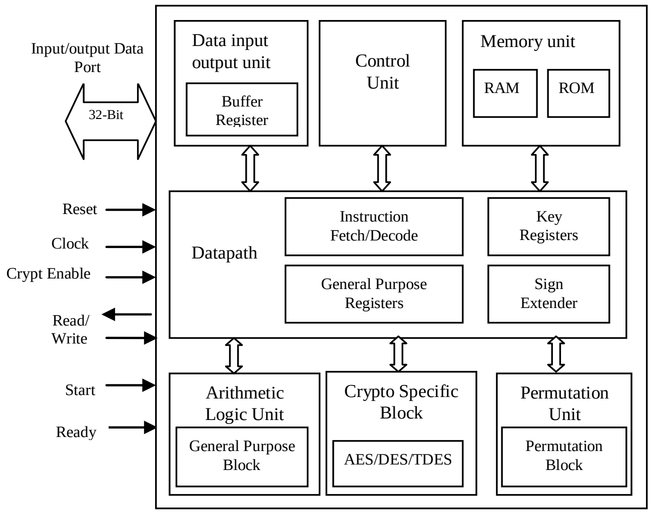

Fig. 1 . MIPS crypto processor [12]

The MIPS controller is the main core of the architecture which consists of control unit and ALU control signal unit. The function of controller is to controls the dedicated crypto block and performs the interface and specific operation with the external devices such as Memory, I/O bus interface controller. Single control unit controls the activities of other modules according to the instruction stored inside memory. The crypto specific block executes various other private and public key algorithms such as RSA, DSA, elliptic curve and IDEA with other application programs such as user authentication programs.

The arithmetic logic unit (ALU) performs the NOP (no operation), addition, subtraction, OR, NOR, set less than, shift left logic operation. The data and address calculations for load and store instruction are performed by ALU. The Load and Store instructions write to and read from the RAM memory in the memory unit while the ALU results and the data read from RAM are written in to the register file by the register type and Load instruction respectively. Data I/O has two different external interfaces which stored data initially at buffer registers or move data to output. The bit permutation operation has a big process part in DES and TDES algorithms as it improves diffusion properties. The incoming data is subjected to some bit position according to the permutation type. The dependency resolver block has a function to avoid stall by rearranging the instruction sequence and checking the successive instruction for their stall possibility by comparing their operands. This module handles both stalling as well as data forwarding of previous stage. In case of data dependency between two consecutive instructions the receiving instruction waits for one clock cycle. Thus dependency resolver controls the data forwarding in pipeline stages.

C. Importance of the proposed work for science

The general importance of this research for scientific and industrial community of microelectronics lays in the development of a new concepts, methods, algorithms and software for design of fault tolerant self-testable digital systems. As it was mentioned earlier, we have close cooperation with different Estonian companies that can use the expected results of the proposed project for improving their competitiveness in the world market. To develop novel NoC architectures and corresponding synthesis and analysis methods for systems, where the same on-chip network is used for functional-mode communication, as well as for test data transportation;

Secondly, the project has also educational aspects. The developed tools can be used for improving the quality of different test related courses in TUT and other universities. The obtained results can improve also the competence level of the group and to make it more attractive for different indian project teams. This would help to find additional funding from different sources. As a general result of this type of knowledge and technology transfer, the teaching environment at the Electronics Engineering Department will be continuously updated and held at the international level, which means great importance for educating students with professional skills on the international level. This fact will also have great importance for Indians in the long-term sense – in appearing of new competitive SMEs in the electronics industry.

VI. Result and Discussion

Research methods are based on using digital electronics, automata theory, Boolean differential algebra, graph theory, theory of algorithms, combinatorial optimization theory, data structures and computation theory and other related fields of electrical engineering, computer science, software engineering and technical diagnostics.

Traditional methods for implementing public key infrastructure, encryption and decryption techniques face lots of problem such as key management, key storing, key privacy etc. My proposed approach can handle such problems. Here I'm using biometric features as a private key so that there is no need to store any private key and also biometric has lots of merits over other biometrics (i.e., it is most user friendly and cheaper too). Biometric recognition also has some outstanding features like universality, permanence, uniqueness and accuracy. As I am using MIPS crypto processor, so we can achieve high level security with very shorter key size. Thus it also solves the key size problem. MIPS require very complex mathematical operation (because of Diffie-Hellman problem, which is harder than discrete logarithmic problem) therefore security strength per bit is also very high.

Experimental investigations of new algorithms and procedures will be carried out by using the in-house software, as well as with professional CAD software from companies Cadence, Synopsys, Mentor Graphics, Xilinx and others that are available at the department and acquired via the department initiative. In the framework of research and development infrastructure development programmed we intend to build up also an environment for rapid prototyping (FPGA-based). This environment will be used for analysis and synthesis of different hardware platforms and has therefore crucial role for the project.

Conclusion

In this paper, a biometric-MIPS based security framework is proposed for data authentication within NOC. Specifically, the sender's key feature is selected as the biometric key for data authentication mechanism within NOC system. The main goal of the current research is to develop new methods, algorithms and software tools for designing biometric based high level security systems. The security system in NOC must be implemented with low computational complexity and high power efficiency. In this proposed approach, low cost authentication challenges are addressed specifically by using biometric information instead of cryptographic key distribution. Thus, it will certainly save resources while adequate security measures are employed.

References

[1] S. Mohammadi, S. Abedi, *"ECC based Biometric Signature: A new approach in electronic banking security"*, International Symposium on Electronic Commerce and Security (ISECS'07), doi:10.1109/ISECS.2008.98, pp. 763-766, 2008.

[2] William Stallings, *"Cryptography and Network Security Principles and Practices"*, PEARSON Prentice Hall, Edition Fourth, 2007.

[3] C. Nandini and B. Shylaja, *"Efficient Cryptographic key Generation from Fingerprint using Symmetric Hash Functions"*, International Journal of Research and Reviews in Computer Science (IJRRCS), Vol. 2, No. 4, August 2011.

[4] H.X.Mel,Doris Baker, *"Cryptography Decrypted"*, Addision-Wesley, Edition 2011.

[5] SNAC, *"Biometrics Security Considerations"*, Systems and Network Analysis Center Information Assurance Directorate, www.nsa.gov/snac.

[6] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, *"A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health"*, IEEE Communications Magazine, vol. 44, no. 4, pp. 73–81, 2006.

[7] B. T Murray, J. P. Hayes., *"Testing ICs: Getting to the core of the problem"*, IEEE Trans. Computer, Vol. 29, pp. 32-39, Nov. 1996.

[8] *"The International Technology Roadmap for Semiconductors"*, 2004 Edition. Semiconductor Industry Association, 2004.

[9] S.-K. Lu, C.-Y. Lee. , *"Modelling Economics of DFT and DFY: A Profit Perspective"*, IEE Proc.–Computers and Digital Tech., Vol. 151, No. 2, pp. 119-126, March 2004.

[10] L. Benini, G. De Micheli, *"Networks on Chips: A New SoC Paradigm"*, IEEE Computer, pp. 70-78, January 2002.

[11] B. Vermeulen, J. Dielissen, K. Goossens, *"Bringing Communication Networks on a Chip: Test and Verification Implications"*, IEEE Communications Magazine, pp. 74-81, September 2003.

[12] Kirat Pal Singh, Shivani Parmar, Dilip Kumar, *"Design of High Performance MIPS Cryptography Processor"*, QSHINE'13, Lecture notes of the Institute for Computer Science, Social Informatics and

Telecommunication Engineering, Springer link, Vol. 115, pp. 778-793, 2013.

[13] Sofia Najwa Ramli, Rabiah Ahmad, Mohd Faiza, Abdollah, Eryk Dutkiewicz, *"A Biometric-based Security for Data Authentication in Wireless Body Area Network (WBAN)"*, 15th international Conference on Advanced communication Technology (ICACT), IEEE, pp. 998-1001, Jan 2013.

[14] Dindayal mahto, Dilip Kumar yadav, *"Network Security using ECC with biometric"*, QSHINE'13, Lecture notes of the Institute for Computer Science, Social Informatics and Telecommunication Engineering, Springer link, Vol. 115, pp. 842-853, 2013.

[15] G. Jervan., *"Test and Fault Tolerance of Network-on-Chip Based Systems"*, Estonian Research Information System, 2009.