Journal of Computer Science 10 (10): 1924-1928, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1924.1928 Published Online 10 (10) 2014 (http://www.thescipub.com/jcs.toc)

SOPC BASED WIRELESS REMOTE PATIENT MONITORING USING ULTRA LIGHTWEIGHT CRYPTOGRAPHY

A. Arun and P. Nirmal Kumar

Electronics and Communication Engg , Anna University, Chennai, India

Received 2014-02-09; Revised 2014-02-17; Accepted 2014-05-08

ABSTRACT

Remote Patient Monitoring (RPM) provides flexible and powerful patient surveillance through wearable devices at anytime and anywhere. This can be achieved by using a Body Sensor Network (BSN), which is deployed on a human body for monitoring the healthcare. The mobile healthcare management with increased feasibility and handiness introduced several noteworthy challenges for the provider, policy makers, patient and hospitals. A significant challenge is to provide round-the-clock healthcare services to those patients who require it via wearable medical devices. In addition to this, the sensors collect the personal medical data where the security and privacy are important components in RPM. As a result, one of the most significant and challenging concern to deal with is how to secure the personal information of the patients and to eliminate their privacy issue. This study presents System on Programmable Chip (SoPC) implementation of Remote Patient Monitoring System (RPM) with Ultra Lightweight algorithms for security issues. Humming Bird 2 (HB-2), PRESENT and HIGHT algorithms were implemented since the wearable medical devices require fewer areas to achieve portability. The comparison results shows that Degree of Confusion of HB-2 is 50.43 which outstand the other, the efficiency of the entire algorithm implemented in SoPC are higher comparing with conventional Field Programmable Gate Array (FPGA) implementation. The comparison was extended and in Particular, power and area consumption of HB-2 is less than PRESENT and HIGHT algorithm, which is more suitable for RPM devices.

Keywords: Hummingbird, Hight, Present, Body Sensor Network, System on Programmable Chip (SoPC), FPGA

1. INTRODUCTION

The sensor and wireless communication technologies are evolving rapidly and capturing new area of application in healthcare domain. The wide range of medical application (Alliance., 2007) leads to popularity and powerfulness of Medical Sensor Network (MSN). This network allows the enhancement of health monitoring system in healthcare facility and hospitals. The use of MSN for healthcare monitoring create a new way of providing Remote user to monitor the patient called as Remote Patient Monitoring (RPM) (Ren *et al*., 2010). A Body Sensor Network (BSN) is a significant component in this supervising scheme. These sensors which are fixed in the patient body or wicker in to the patient's clothes will continuously collect data by travelling with the patient. The BSN will continuously collect data, creates additional privacy and security demands on following the fact "always on. The users or patients have flexibility and mobility which can be dominated by wearable sensors, which enable the patient to have maximum freedom while still receiving the professional supervision of medical representatives. The foreword of mobile technology and wireless make mobile electronic healthcare systems more feasible and realistic. There are many cryptographic algorithm namely KLEIN, KATAN, TEA, HIGHT, PRESENT and family of Humming Bird have been proposed for RFID applications. The key issue for the implementation of cryptographic algorithm in RFID application is that the

Corresponding Author: A. Arun and P. Nirmal Kumar, Electronics and Communication Engg , Anna University, Chennai, India

algorithm should consume less area and low power. This requirements lead to the implementation of Ultra Lightweight cryptography from the previous one (Lightweight Cryptography). The FPGA implementation of both lightweight and ultra lightweight cryptography has been proposed. This survey have been paved the path for Remote Patient Monitoring (RPM) where the secured communication between the wearable sensors and remote user (Medical Professional) should be maintained. To achieve the portability of the wearable sensor the ultra lightweight cryptographic algorithm has been implemented since they require less area. The evolution of hardware implementation of cryptographic algorithm starts with digital signal processor which is dominated by Field Programmable Gate Array (FPGA) (Abdelkrim *et al*., 2012).

The cryptographic implementation is well suited in FPGA (Kaps, 1998) but hindrance in the implementation is FPGA will produce high efficiency in standalone process (i.e., implementation of cryptographic algorithm only). The efficiency of the implementation will be reduced in application like data acquisition and control where multi tasking is major concern. Alas RPM falls on this category of application, where several sensors have been used for detecting the biological signals of the patient, data processing were made before transmitting to remote place (medical representative here). In this study, we have implemented several cryptographic algorithms in SoPC (Bakthavatsalam and Mehata, 2014) which dominates the FPGA implementation in Remote Patient Monitoring (RPM) system (i.e., Data Acquisition and Control) applications.

2. CRYPTOGRAPHY ALGORITHMS

2.1. Humming Bird-2

The Humming Bird-2 has key of size 128 bit. The internal state R (128-bit) is initialized by 64 bit Initialization Vector IV. The computational process includes addition modulo, exclusive OR and mixing function f(x) which is non linear and it is performed on 16-bit words. The f(x) can be computed by following operations Equation 1 to 3:

$$S(x) = S_1(x_0)|S_2(x_1)|S_3(x_2)|S_4(x_3) \quad (1)$$

$$L(x) = x \oplus (x<<<6) \oplus (x<<<10) \quad (2)$$

$$f(x) = L(S(x)) \quad (3)$$

where, L (x) denotes linear transformation and S(x) denote S-box computation. The internal state of Humming Bird-2 is initialized using R (0) = (IV_1,IV_2,IV_3,IV_4,IV_1,IV_2,IV_3,IV_4) for I = 0, 1, 2,3 to find t1,t2,t3 which is used to update register R_1, R_2, R_3 , R_4.

2.2. Present

The Present algorithm (Bogdanov *et al*., 2007) has a block length of 64 bits with varying key size 128 or 80 bits. The XOR operation to form a round key consumes 31 rounds and final round is used for process of whitening (Alizadeh *et al*., 2012). The overall algorithm is as follows:

```
Generate round keys ()
for i = 1 to 31 do
add round key (state, $K_i$)
sBox layer (state)
pBox layer (state)
end for
add round key (state, $K_{32}$).
```

2.3. Hight

The decryption process of hight algorithm (Hong *et al*., 2006) is similar to encryption process so we are focusing on the encryption process, which consists of round function, key scheduling, initial and final transformation. The algorithm is as follows, where SK and WK denotes sub key and whitening key:

```
Hight encryption (P, MK) {
Key scheduler (MK, WK, SK);
Hight encryption (P, WK, SK) {
Initial transformation (P, $X_0$, WK3, WK2, WK1, WK0);
For i = 0 to 31{
Round function ($X_i$, $X_{i+1}$, $SK_{4i+3}$, $SK_{4i+1}$, $SK_{4i}$); }
Final transformation (WK7, WK6, WK5, WK4, X32, C);
} }
```

3. IMPLEMENTATION OF THE PROPOSED SYSTEM

The **Fig. 1** shows SoPC (proposed) implementation of Remote Patient Monitoring (RPM) system. The execution of SoPC method include two Nios-II processor which is economy (i.e., consist of 600-700 LE's). The CPU-II acts upon data encryption where algorithm for ciphering the text will be in software level which is stored in SDRAM and right of entry is by SDRAM Controller. On the other hand, CPU-I leads the data control and acquisition progression independently. The system is fashioned using SoPC builder available with Altera Quartus since it lends a hand to build System on Programmable Chip in minute.

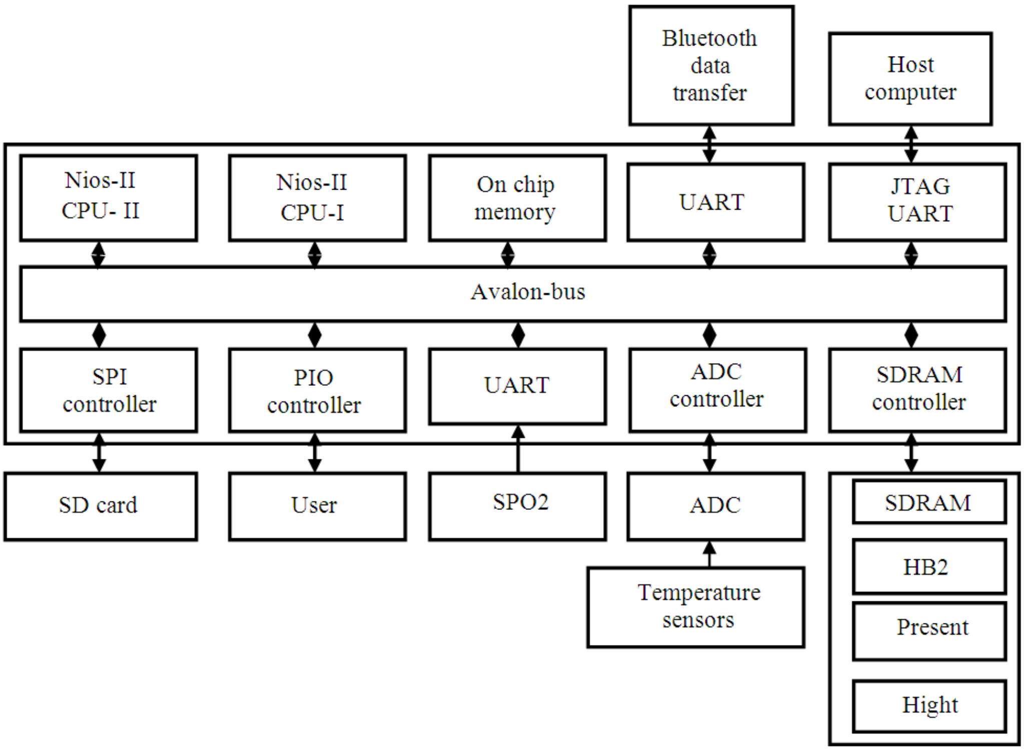

Fig. 1. Proposed system architecture (SoPC)

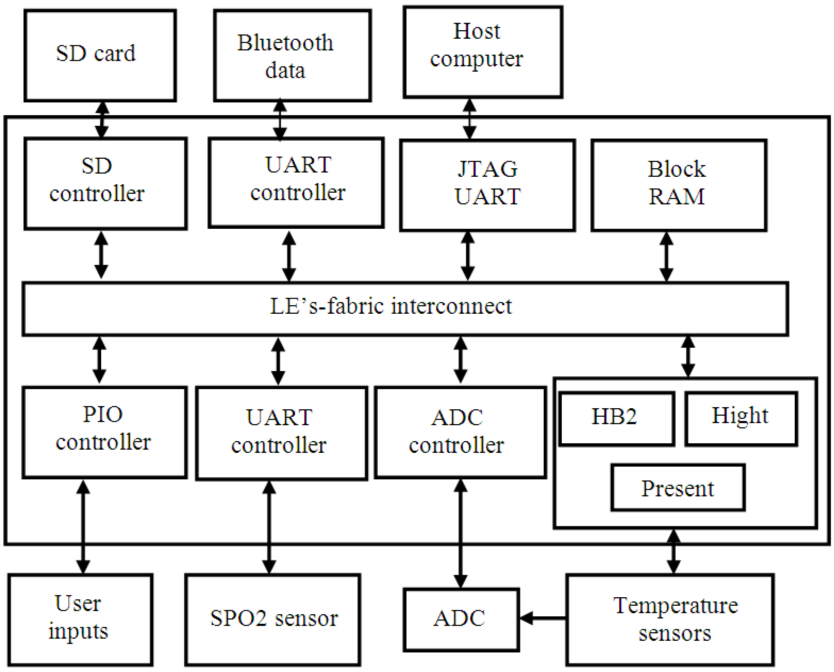

Fig. 2. Conventional system architecture (FPGA)

Two sorts of IP cores are granted in the system model. They are, IP's built from Altera SoPC builder and the user's customized IP that can be added to the SoPC builder IP menu. This work utilizes both types of IP's which act as a hardware block when implemented in compatible FPGA's. The data transmission from sensors (Temperature and SPO2) to CPU I is accomplished by UART.

The SD card will hold the information of the patient at every stage and update periodically which can be accessed by SPI controller. The CPU-I will retrieve the value from temperature sensor after the practice of Analog to Digital Converter (ADC) through respective controller. If abnormal value (i.e., 5% increases in this case) is monitored by the system then CPU-I will transfer the data (activity of patient) in progress to the remote place (i.e., medical representative here) after encrypting using resourceful algorithm by the use of CPU-II. At this time, the host computer also accessed by the use of JTAG UART. The patient can make use of switch which is marked as user inputs (in figure) at rigorous condition. This will act as a panic button which is tracked by CPU-I and accessed using PIO controller. On the other hand, FPGA (conventional) realization of Remote Patient Monitoring (RPM) system is shown in **Fig. 2**. In contrast to SoPC implementation, Fabric Interconnect made up of logic elements are used for intra-process communications.

The area utilization of the RPM realized using conventional method will suffer degradation since the number of controllers (PIO, UART, ADC and SD) will occupy more logic elements, where as SoPC implementation needs interfacing for the same. The power consumption will be increased as a result of additional logic element utilization. Due to controller concern, parallel execution of multitasking lack in FPGA execution, on this chance the SoPC implementation will win the contest.

4. RESULTS

The proposed system is evaluated under two circumstances; one is based on efficacy of the cryptographic algorithm and subsequently compares the SoPC based outcome with FPGA implementation. The implementation is done on the cyclone IVE EP4C22 device. The Degree Of Confusion (DOC) for different cryptographic algorithm is tabulated on **Table 1**. The process of confusion makes key so complex, which increases the difficulty level to deduce the key even when an attacker knows the statistics.

The Humming Bird-2 confuses more and battle better against the attackers. The logic elements consumption of various ultra lightweight algorithms is tabulated in **Table 2** and comparison chart for the same is shown in **Fig. 3**. The HB-2, HIGHT and PRESENT entail 1570, 2159 and 3220 logic elements in that order. The HB-2 needs 28% lesser area than hight and 52% in case of present. The system on Programmable Chip integrates the whole architecture with in a single chip thereby reduces the execution time and increases the efficiency. Also it reduces the energy consumption in the system. The efficiency of Remote Patient Monitoring (RPM) system in terms of throughput and power for SoPC realization is compared with conventional FPGA implementation as in **Table 3**. The variation in throughput is increased by nearly 23% in HB-2 and 15, 12% in hight and present respectively.

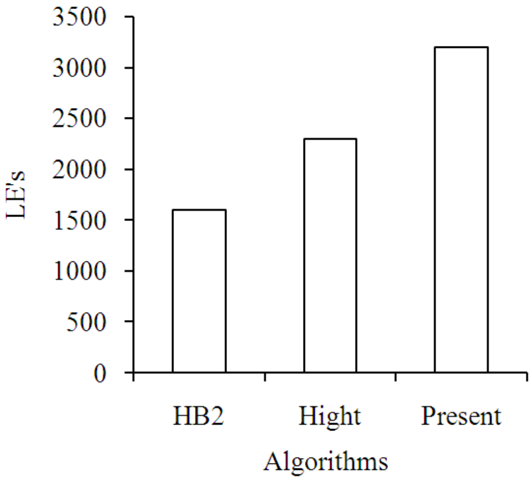

Fig. 3. Implementation of the cryptographic algorithm in cyclone FPGA and the comparison of logic elements

Table 1. DOC of cryptographic algorithm

Algorithm	Hight	Present	HB-2
Degree of confusion	48.17	48.05	50.43

Table 2. Efficiency computation in SoPC

Implementation	Algorithm	Efficiency (Throughput/LE)
FPGA	HB-2 HIGHT PRESENT	0.4035 0.2389 0.1577
SoPC	HB-2 HIGHT PRESENT	0.4635 0.2790 0.1779

Table 3. Throughput and power comparison of ciphers in SoPC and FPGA

	Algorithm	F_{max} (MHz)	Throughput (Gbps)	Power (mW)
Implementation	HB-2	159.20	633.60	1.93
FPGA	HIGHT	249.00	516.00	2.54
	PRESENT	253.00	508.00	5.00
	HB-2	168.92	727.81	1.36
SoPC	HIGHT	281.33	603.00	2.10
	PRESENT	294.41	579.47	3.45

The efficiency can be increased further by varying the key size. **Table 3** exemplify that power get reduced in SoPC level realization due to cutback of logic elements for the controllers.

5. CONCLUSION

This study compares the efficiency of Remote Patient Monitoring (RPM) system realized in both SoPC and FPGA level. To ensure the privacy of patient, we implement three types of ultra lightweight cryptographic algorithm. The confusion degree and area of HB-2 outstands the Present and Hight algorithms hence it is well suited for security of patient's data. Further, the SoPC level realization performs well under condition of parallel execution of multitasking process, moving in depth the throughput and power consumption of SoPC implementation is remarkable when compared to FPGA implementation. In future, we can deploy further sensors in SoPC architecture and can be re-programmed for some other patient with different parameters. We can extend the application to analyze the ECG and EEG of the patient and promote efficient and power aware NoC solution for the system in future to reduce the complexity.

6. REFERENCES

Alliance, Z., 2007. Personal, home and hospital care: technical requirements document.

Abdelkrim, H., S.B. Othman, A.K.B. Salem and S.B. Saoud, 2012. Dynamic partial reconfiguration contribution on system on programmable chip architecture for motor drive implementation. Am. J. Eng. Applied Sci., 5: 15-24. DOI: 10.3844/ajeassp.2012.15.24

Alizadeh, M., M. Salleh, M. Zamani, J. Shayan and S. Karamizadeh, 2012. Security and performance evaluation of lightweight cryptographic algorithms in RFID. Universiti Teknologi Malaysia.

Bakthavatsalam, G. and K.M. Mehata, 2014. A case for hybrid instruction encoding for reducing code size in embedded system-on-chips based on RISC processor cores. J. Comput. Sci., 10: 411-422. DOI: 10.3844/jcssp.2014.411.422

Bogdanov, A., L.R. Knudsen, G. Leander, C. Paar and A. Poschmann *et al*., 2007. PRESENT: An ultra-lightweight block cipher. Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems, Sept. 10-13, Vienna, Austria, pp: 450-466. DOI: 10.1007/978-3-540-74735-2_31

Hong, D., J. Sung, S. Hong, J. Lim and S. Lee *et al*., 2006. HIGHT: A new block cipher suitable for low-resource device. Int. Assoc. Cryptol. Res., 4249: 46-59. DOI: 10.1007/11894063_4

Kaps, J.P., 1998. High Speed FPGA architectures for the data encryption standard. MSc. Thesis, Worcester Polytechnic Institute.

Ren, Y., R.W.N. Pazzi and A. Boukerche, 2010. Monitoring patients via a secure and mobile healthcare system. IEEE Wireless Commun., 17: 59-65. DOI: 10.1109/MWC.2010.5416351