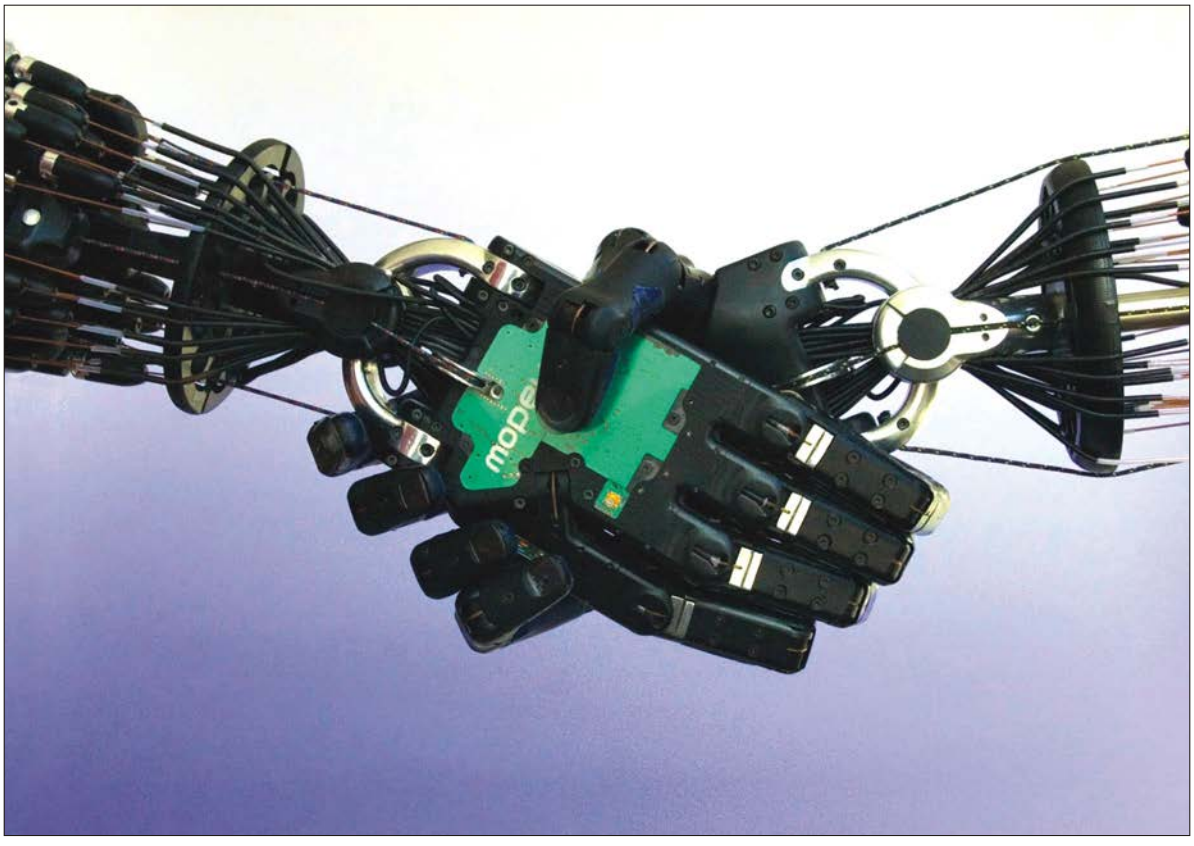

Journal of Artificial Intelligence

ISSN 1994-5450

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Artificial Intelligence 6 (2): 134-144, 2013
ISSN 1994-5450 / DOI: 10.3923/jai.2013.134.144

Design and Development of Secret Session Key Generation using Embedded Crypto Device-ARM-LPC 2148

C. Mohan Raj, M. Mathan Kumar, D. Manivannan and A. Umamakeswari
SASTRA University Tamilnadu, India

Corresponding Author: C. Mohan Raj, SASTRA University Tamilnadu, India

ABSTRACT

Wireless networks are capable solutions for many industrial and commercial applications. However, a wireless node endures with lots of constraints such as low computation ability, little memory, partial energy resources and so on. In secure communication, different numbers of end devices are used to share the information between wireless devices and also are protected with the help of crypto algorithm and secret keys. The secret keys play a very important role than the algorithm, to ensure the security of the information between different numbers of users. When members of a group need to accept the similar information security and are permitted to dynamically join or leave the group, security entails not only sharing of a secret among lots of users but also be worried with security services like confidentiality, integrity of information as the connection changes. Whenever the system changes, the system manager is responsible to change the secret and supporting keys and to send back the updated keys to the group members. These different numbers of secret keys used in the end devices are generated using software and hardware techniques. In this study the different numbers of secret keys are generated using hardware. LPC 2148 are used to generate the random secret session key with real time parameters, event driven circuits and temperature measurement unit. In all the scenarios, the randomness, issues in hardware are analyzed and discussed.

Key words: Embedded system, LPC 2148, cryptography, crypto-device, secret key, PRNG

INTRODUCTION

When the message is communicated through the wireless medium between interconnected computers, it is not confident that the message is transmitted more securely. The wireless medium used for transmission is not only accessible to the single user, but many users will use the radio standard for the data transmission at the same instance. So, there will be many devices to be accommodated, required for the transmission usage will also get increase with an increase in data storage. In order to provide the secrecy of the message, the secret key is used. The key is the random value, used to convert the message into an unreadable format. Many software techniques, hardware techniques (Guler and Ergun, 2012) are used to protect the message from eavesdropping. At the same time, apart from cipher techniques, to enhance the crypto system, the different number of secret key is used to defend the information from hackers. The message is used at different locations in the same applications. The hackers may get the information from the storage, transmission and at the receiving end. Of all the places, the establishment of security must be important with different number of keys or same keys. Depends on the number of users, the size

of the message to be transmitted and architecture pattern, the numbers of secret keys required are determined (Lee *et al*., 2009). Insecure communication, related to keying-key generation, key distribution, key update, Lifetime of the keys are important issues (Eberle *et al*., 2005). In this study, the keys are generated using hardware techniques, to achieve more security and reliability. When commercial embedded devices are used as the medium for the message transmission between the computers, it is not much easier for the attackers to crack the process happening in the medium. So, there will be high security.

In this study, embedded device is acting as a crypto device in which used to generate the secret keys. Keys are generated by implementing the cipher algorithms using confusion and diffusion principle. This process generally called as crypto-system. The crypto-system is nothing but encrypt the data in unreadable format through embedded device. In decryption, reverse process in crypto system is done and retrieve the original data with the help of embedded device. The crypto algorithm classified into symmetric and asymmetric. In symmetric cipher, the same key is used for both encryption and decryption. Another one is the public key cryptography (Lee *et al*., 2009), which is the asymmetric method, where the different keys are used. Encryption uses public key whereas, the decryption uses private key. The symmetric cipher is further classified into stream and block cipher. The stream cipher (Batina *et al*., 2003) is the cipher method that takes the K-key with n-bit length and is then stretched into long Keystream. This Keystream is then XORed with the plain text to produce the cipher text. In decryption, the same Keystream is generated and is XORed with cipher text to regain the plain text. In a block cipher, the plain text is split into fixed size blocks and generates the fixed size cipher text. The cipher text is obtained by iterating the round function where the function depends on the output of previous round. Different algorithms can be used for decryption. The key is the value used to convert the plain text into encrypted text. The key can be of any forms like character, numeric, special character or combination of all. There are many types of keys used in the encryption process. Security has to rely on both the key and algorithm that are used in cipher techniques. Instead of loading key to the encryption device manually, the secret key must be generated from the same embedded device (Batina *et al*., 2003) for their own data conversion process. It is more efficient than to use a separate key generator (Guler and Ergun, 2012) for generating key for every instance.

In this study, key generators are used to generate the keys in cryptography by means of the embedded device. The random number generator is used to generate the random number which cannot be predicted with the previous value that's generated. It can be generated by means of the Truly Random Method (Dawson and Gustafson, 1998), Pseudo-Random Method or by Quasi-Random method. Pseudo-Random Number Generator (PRNG) is also called Deterministic Random Bit Generator (Dawson and Gustafson, 1998) which is used for generating the random with the use of some initial values. It is easier to implement in the embedded device wherein several peripherals are available to get the physical parameter as the initial value. Whenever, the key length increases, it is very difficult for the attackers to identify the predictable sequence of random value. When this key length is defined and generated by the embedded crypto device, it will be more secure than the ordinary one. Embedded devices have different set of inputs, outputs and processing section. When these devices are used as the crypto device wherein many tedious processes have to be configured in the device to make it act as the crypto device, but the device can be act as the medium between the computers for security purpose (Vaslin *et al*., 2009).

Some cases software encryption also provides the privacy data residing by using the system CPU for performing the encryption and decryption and also cryptographic operation. The

advantage includes the ability to use software for multiple applications like message encryption and digital signature applications. Hardware encryption is a process in which the data is pushed into encrypt device wherein functions are loaded into the device and that makes the process of encryption and the cipher will be produced. It is more advantageous of using hardware than software because it protects the security components like Malware and root kits (Song *et al*., 2011). It is more scalable and has the greater throughput and cost-effective system.

The LPC 2148 (LPC214x user manual, 2010) Microcontroller is the 16/32-bit ARM7TDMI-S RISC processor which provides the embedded system with high speed flash memory of about 32 kB to 512 kB and also On-Chip RAM of 8 to 40 kB. Maximum CPU clock available for the controller is 60 MHZ for settling time 100 μsec. CPU operating voltage is 3.0 to 3.6 V. The oscillating frequency for the LPC2148 is from 1 to 25 MHZ. The LPC2148 uses AMBA High Performance Bus (AHB) interface for interrupt control. The ARM core follows the little-endian byte order. LPC 2148 has various serial communication interfaces ranging from USB 2.0 full speed device, multiple UART's, SPI (Serial Peripheral Interface), SSP to I^2C's which is suitable for communication gateways and protocol support, soft modems, low end image processing, providing high processing power and large buffer size. Various 32-bit timer, two 10-bit channel ADC's, DAC and PWM channel, nine edge sensitive interrupts mainly using in the medical and industrial control application.

In this study LPC2148 (http://nskelectronics.com/files/lpc2148_user_manual.pdf) acts as the embedded crypto device and is used for generating n-number of keys with the use of peripheral interface in the device. Usually, the hackers will try to attack the crypto-device which is used for the data encryption but in this case LPC2148 is the embedded device acting as the crypto-device when it is necessary for key generation for the crypto applications. This is more reliable and less power consumption when compared to the other processor that are available. It is more secure and it will take time for the attackers understand the working process in the device. Figure 1 shows you the functionality of the crypto device.

The embedded system is the budding field of engineering product and development that involves the computation with physical constraints. These physical constraints arise through two kinds of interaction (1) reaction of physical environment and (2) execution of the physical environment. Reaction constraints specify on jitter, deadline and throughput. Execution constraints rely on processor speed, power and hardware failure rate. Another major challenge in the embedded system is optimization of the system. The optimization depends on the microprocessor,

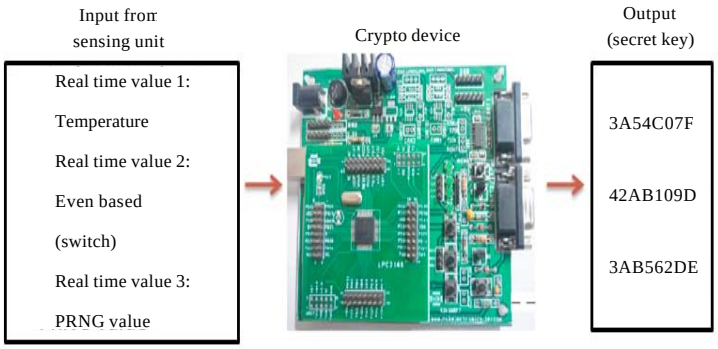

Fig. 1: Functional block of crypto device

ASIP or microcontroller that is going to be used as well as it depends on the performance factor, power dissipation and other metrics in the system. When there is increasing in computing power of Silicon-On-Chip and in Network-On-Chip technologies together. It will lead to the integration of critical and non-critical applications on a single chip. It reduces the communication cost, increase in hardware reliability and also will increase in the rational and cost effective system. In many embedded applications, key management technology plays a very important role to enforce the security services. For that, different schemes like pair wise, LU matrix are used (Doraipandian *et al*., 2011). This hardware based key generator will generate pure random key value to enrich the system requirements related with security. Security plays a vital role in embedded systems. Since embedded systems are more vulnerable to malicious attacks (Batina *et al*., 2003). Also embedded system provides security for the end users, only the authorized end user allowed to access the device for data processing. These attacks are characterized by remote vs proximity based attacks, software vs hardware based attacks, active vs passive attacks and reversible vs irreversible attacks and fault based detection and intrusion issues (Cheng and Agrawal, 2007).

Security features have to be indulged in the fields of communication such as data protection, security audit, identification and authentication. In order to achieve the security requirements like confidentiality, integrity and authentication, the hardware based key generators are developed by using LPC 2148 low power ARM processor.

PROPOSED WORK

In this proposed system, LPC 2148 ARM processor is the crypto device used to generate secret keys as per our system requirements. In this study the system design is divided into four major modules, these are True random real time value; True Random Nonce (Initial Vector); Event Driven based and master crypto device. The LPC 2148 device is used to generate these three different secret random values which acts as the random source for the master crypto device. The general system functionalities are explained in this section. The output 1 from crypto device 1 and output 2 from crypto device 2 are XORed, then it also XORed with the result of third crypto device value (Manivannan and Sujarani, 2010). The Master crypto device will compute the final process in Key permutation like shifting and direct permutation (Cheng and Agrawal, 2007). Finally, the random secret key is obtained from the master crypto device and it will be used for security purpose. This scenario is explained in the following section.

Figure 2 shows the block diagram of the complete structure of proposed work, where the inputs are given to the crypto device in different stages by the physical parameters, random source and

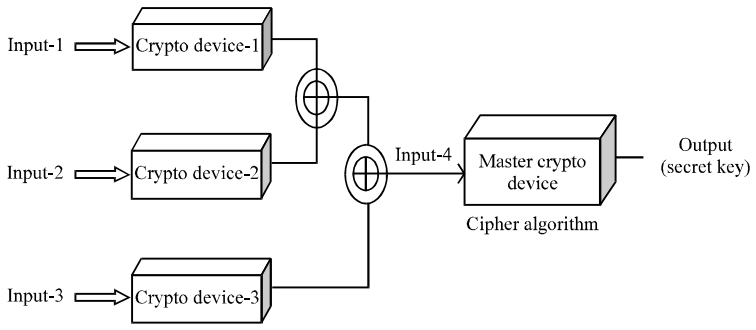

Fig. 2: Cipher process in embedded crypto device

standard ADC value and that values are processed in different crypto device. The each and every output from the crypto device (Guler and Ergun, 2012) is processed as our system designed and that acquired value is given to the Master crypto device as the input. In master device, the crypto algorithm is stored, based on that, data will be processed in the crypto device (Hani *et al*., 2006), finally the random secret key is generated for each clock.

In the following section, each and every sub module in crypto device are explained. The first module the physical parameters like temperature, pressure and humidity are not constant; it varies according to the environmental change. The temperature sensor is used to sense the temperature (analog value) of the particular environment and is passed to the controller for the conversion process. The conversion process is done by the ADC converter in which analog value is converted to digital. The ADC conversion is classified into Direct-conversion method, Successive-Approximation method and Sigma-Delta method. The operating voltage of the ADC ranges from 3.0 to 5 V. The end result will be in the digital form which is used as the key input for the hardware KGU. The pseudo code of this process is as follows:

Pseudo code for crypto-device 1

```
Begin
    Initialize Baud-Rate
    Set the Desired frequency
    Calculate the value of the Divisor with the use of Baud-Rate and Frequency
ADC-initialize
    Set the control bit for ADC Process
UART-initialize
    Assign the Control Bit for serial transmission to perform
    Set the LSB and MSB bit for Data Transmission
Main
    Assign PINSEL for ADC Conversion and for Serial Transmission
    Check the ADC conversion by using the Data Register in the ADC
    Perform shifting and logical operation to store the result of the conversion
    Generate random value of 8-bit using
    A=: 8-bit arithmetic with 8-bit logical with 8-bit
    B=: 8-bit arithmetic with 8-bit logical with 8-bit
    8-bit value of ADC and Random vale converted to 32-bit output
End main
End
```

In second module cryptography, Initial Vector (IV) value is the fixed-size input that is typically random (or) pseudo-random. Randomization is more crucial for the encryption schemes to achieve the security. In this process, IV value is the source input and is processed with the different varying key value. It generates the output value which will be randomness to the input that is given. The block cipher (Dawson and Gustafson, 1998) is frequently used data encryption method where the plain text will be changed to the cipher block by adding some key value. In order to re-issue the addition key for every encryption, IV can be used. It will generate the random value which is added to the plain text to form the cipher text which will increase the security in the process. The pseudo code of this process is as follows:

Pseudo code for crypto-device 2

```
Begin
    Initialize Baud-Rate
    Set the Desired frequency
    Calculate the value of the Divisor with the use of Baud-Rate and Frequency
UART-initialize
    Assign the Control Bit for serial transmission to perform
    Set the LSB and MSB bit for Data Transmission
Main
    Assign PINSEL for Serial Transmission
    Generate random value of 32-bit using
    x=: 32-bit arithmetic with 32-bit logical with 32-bit
    y=: 32-bit arithmetic with 32-bit logical with 32-bit
    z=: 32-bit value output
End main
End
```

The third module in this study is about an event driven operation. The Dip-switches are used in which the task is executed based on the input state given by the switch. By using a switch, an N- combination of input states can be defined and based on the state in the switch, the process can be executed by the LPC2148 for generating n-number of n-bit random value. The input state can be defined by the user depending on their needs. It can be any sort of combinations in n×n. This generated value is the input for the hardware Key Generation Unit (KGU) (Manivannan and Sujarani, 2010). The operating temperature rating of the switch is -25 to 70°C. The pseudo code of this process is as follows:

Pseudo code for crypto-device 3

```
Begin
    Initialize Baud-Rate
    Set the Desired frequency
    Calculate the value of the Divisor with the use of Baud-Rate and Frequency
    Define the switch with corresponding PORT Address
UART-initialize
    Assign the Control Bit for serial transmission to perform
    Set the LSB and MSB bit for Data Transmission
Switch (8-pin DIP switch)
    If (switch condition is met)
        Return the corresponding switch value
    Else
        Return zero
Main
    Assign PINSEL for Serial Transmission
    x=: perform 8-bit arithmetic operation with the return value of the switch
    u=: 8-bit arithmetic with 8-bit to convert into 16-bit value
    v=: convert the 16-bit value to 32-bit value output
End main
End
```

In fourth module, the key generated by the event based process, real time value and initial vector value are processed together and the n-bit value is generated. The final value generated is placed in the single dimension array and is processed by the key crypto algorithm (like A5/1 Key

Crypto Algorithm) which is most widely used in GSM mobile phones for the confidentiality. The data stored in the array are processed by the performing bit by bit logical operation and the processed value will be the final Key value that is going to be used in the encryption method for secure data transfer (Kulkarni and Bruhadeshwar, 2010). Even this process is more complicated way of generating the single key stream bit but it is easy to implement in the hardware and is proportional to the clock speed. The pseudo code of this process is as follows:

```
Pseudo code for master crypto-device:
    Begin
        Initialize Baud-Rate
        Set the Desired frequency
        Calculate the value of the Divisor with the use of Baud-Rate and Frequency
UART-initialize
        Assign the Control Bit for serial transmission to perform
        Set the LSB and MSB bit for Data Transmission
    Main
        Assign PINSEL for Serial Transmission
        C=: Key1 logical with Key2 logical with Key3
        Arr () =: C
        Arr (odd) =: Perform Logical with Arr (odd) value
        Arr (even) =: Perform Logical with Arr (even) value
        Arr (odd) Logical with Arr (even) to generate 32-bit Key value
End main
    End
```

In the final, the output from the master crypto device will generate the secret key at 32 bit values. This system may be extent as per system requirements and different key size like 64, 128, 256 and 512 bit may be obtained.

EXPERIMENTAL RESULT

Figure 3-7 gives you the clear idea about overall hardware setup and the output of the each Crypto-Device's.

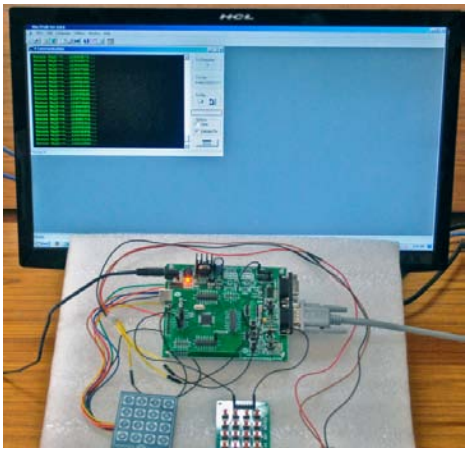

Fig. 3: Hardware setup of crypto device

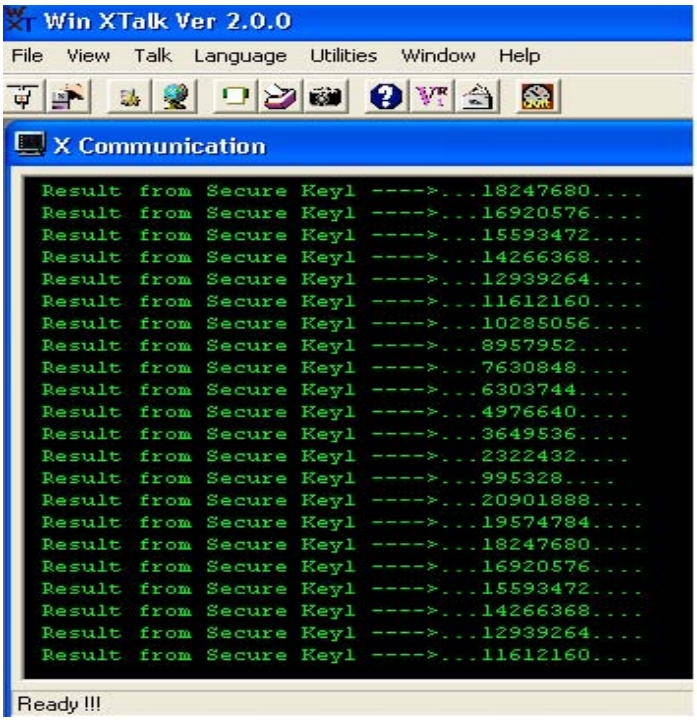

Fig. 4: Output of crypto device-1

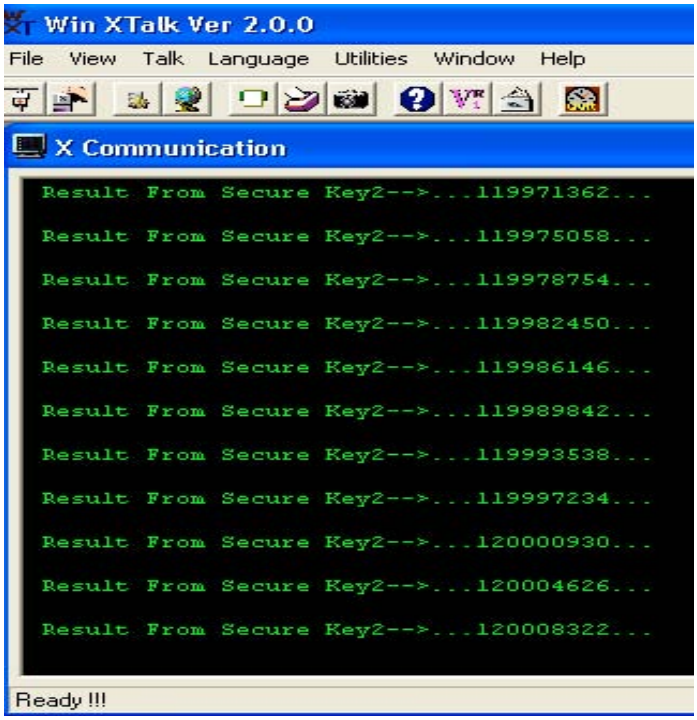

Fig. 5: Output of crypto device-2

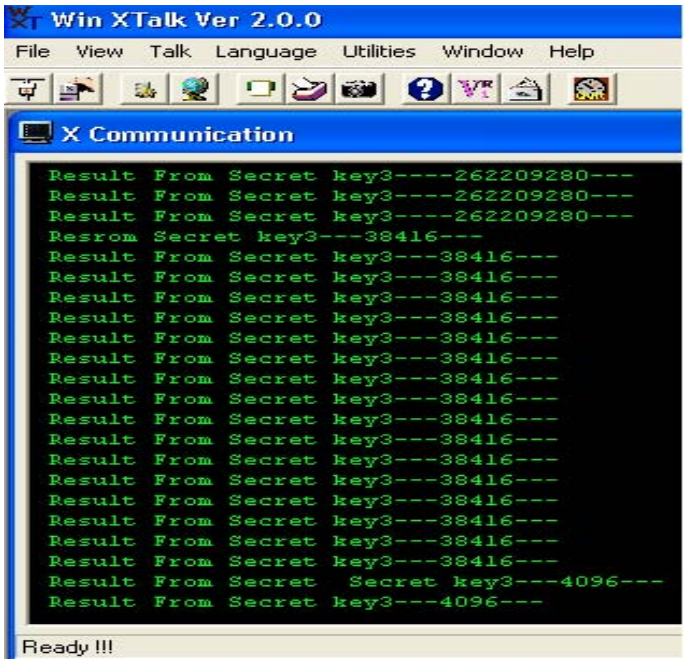

Fig. 6: Output of crypto device-3

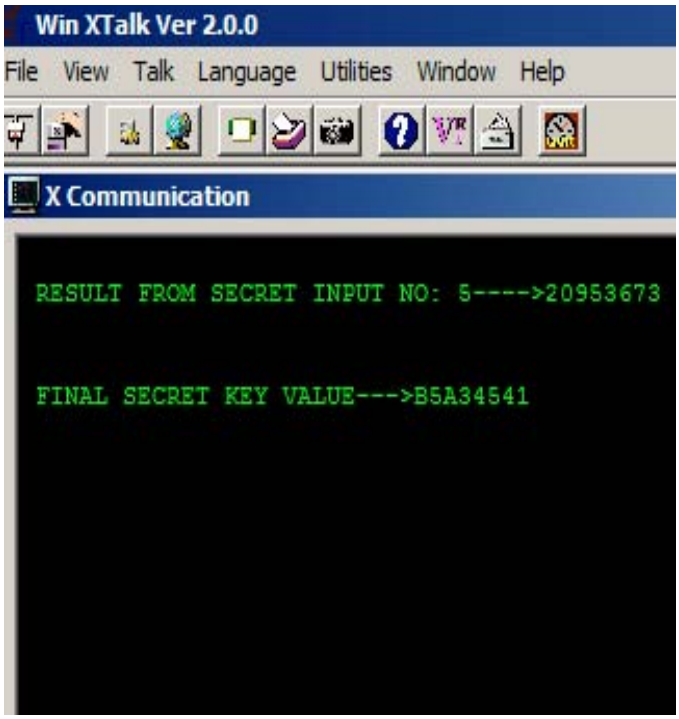

Fig. 7: Output of master crypto device

CONCLUSION

The secret key is generated purely randomly by the combination of TRNG and PRNG in the embedded device using LPC 2148 which cannot be predicted by the previous value. It processes the real time value of data processing to calculate the secret keys, also it more scalable and more reliable than existing techniques. It is more flexible to use embedded device as a key generator rather than using the crypto-device and is simple to use. It incorporates the features of hardware security to implement and generate the secret key value with highly secured secret value as the key. In order to increase the level of secrecy of the secret key source, the strength of the crypto algorithm, preloaded with the master crypto device may be changed as per system designer and requirement. It incorporates both true randomness and pseudo randomness for key generation process. When there is a failure of any event, it will not affect the entire process unit. The generation of key is basically a device oriented service in which LPC2148 provides the service to all the nodes by providing the corresponding key for data ciphering. The storage efficiency of this system is high because of the on-chip RAM and Flash memory of this crypto embedded device.

ACKNOWLEDGMENT

The research has been supported by the research and modernization funded project of SASTRA University-R&M/0008/SOC-001/2009-10.

REFERENCES

Batina, L., S.B. Ors, B. Preneel and J. Vandewalle, 2003. Hardware architectures for public key cryptography. Integr. VLSI J., 34: 1-64.

Cheng, Y. and D.P. Agrawal, 2007. An improved key distribution mechanism for large-scale hierarchical wireless sensor networks. J. Ad Hoc Networks, 5: 35-48.

Dawson, E.P. and H.M. Gustafson, 1998. A method for measuring entropy of symmetric cipher key generators. Comput. Secur., 17: 177-184.

Doraipandian, M., E. Rajapackiyam, P. Neelamegan and A.K. Rai, 2011. An Efficient and Hybrid Key Management Scheme for three Tier Wireless Sensor Networks using LU Matrix. In: Advances in Computing and Communications, Abraham, A., J.L. Mauri, J.F. Buford, J. Suzuki and S.M. Thampi (Eds.). Springer, New York, USA., ISBN-13: 9783642227196, pp: 111-121.

Eberle, H., S. Shantz, V. Gupta, N. Gura, L. Rarick and L. Spracklen, 2005. Accelerating next generation public-key cryptosystems on General-purpose CPUs. IEEE Micro, 25: 52-59.

Guler, U. and S. Ergun, 2012. A high speed, fully digital IC random number generator. Int. J. Electron. Commun., 66: 143-149.

Hani, M.K., H.Y. Wen and A. Paniandi, 2006. Design and implementation of a private and public key crypto processor for next-generation it security applications. Malaysian J. Comput. Sci., 19: 29-45.

Kulkarni, S.S. and B. Bruhadeshwar, 2010. Key-update distribution in secure group communication. Comput. Commun., 33: 689-705.

Lee, J., Y. Bi, G.D. Peterson, R.J. Hinde and R.J. Harrison, 2009. HASPRNG: Hardware accelerated scalable parallel random number generators. Comput. Phys. Commun., 180: 2574-2581.

Manivannan, D. and R. Sujarani, 2010. Technologies light weight and secure database encryption using TSFS algorithm. Proceedings of the International Conference on Computing Communication and Networking Technologies, July 29-31, 2010, Karur, India, pp: 1-7.

Song, S., J. Zhang, X. Liao, J. Du and Q. Wen, 2011. A novel secure communication protocol combining steganography and cryptography. Procedia Eng., 15: 2767-2772.

Vaslin, R., G. Gogniat, J.P. Diguet, E. Wanderley, R. Tessier and W. Burleson, 2009. A security approach for off-chip memory in embedded microprocessor systems. Microprocess. Microsyst., 33: 37-45.