International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.217-230
http://dx.doi.org/10.14257/ijsia.2015.9.11.21

Implementation of Schnorr Signcryption Algorithm on DSP

Aya Elshobaky [1], Mohamed Rasslan[2] and Shawkat Guirguis[3]

[1]*Alexandria University, Alexandria, Egypt*
[2]*Electronics Research Institute, Giza, Egypt*
[3]*Alexandria University, Alexandria, Egypt*
[1]*aya.elshobaky@gmail.com,*
[2]*mohamedraslan@eri.sci.eg,*
[3]*shawkat_g@yahoo.com*

Abstract

The lack of data security in public mobile telecommunication system increases the need for a strong data protection and security mechanisms. Cryptography is considered as one of the key elements that provides security for mobile systems. Signcryption algorithm, which is based on public key cryptography, provides both confidentiality and authenticity in one step. Moreover, hardware implementations of cryptographic algorithms provide scalable solutions to enhance the level of security of the existing hardware.
In this paper, we present a case study on using a DSP board to construct a secure communication channel. We use the constructed DSP board as a hardware cryptosystem to increase the security of transmitted data using any mobile communication system. We evaluate the performance by computing the consumed time by encryption/decryption process, while implementing the Schnorr Signcryption scheme on a DSP. Furtheremore, we propose an enhanced model of applying multiple DSP using pipelines and parallelization technique to decrease the consumed time in the whole process.

Keywords*: Schnorr Signcryption, Cryptosystem, DSP,Secure wireless system*

1. Introduction

Over the last few years, mobile wireless communication has rapidly emerged throughout the world and had a very rapid increase in the number of subscribers. As an extension of mobile technology, users are able to send and receive data across the world using the mobile communication networks [5].

Due to the increasing number of users in mobile wireless communication networks, there is a growing demand of security deployment. Data security is critical for most businesses and even for some individual users such as, client information, payment information, personal files, and bank account details. This type of information can be replaced and potentially damaged if it falls into the wrong hands (by losing it to hackers). Malware infections, exploits from corporate espionage, or any other malicious activity coul have catastrophic consequences. Thus, we have to identify areas of vulnerability and develop strategies for securing important data and information systems.
Data security needs an overall strategy and risk assessment. This allow us to identify the risk that we might face. Since data could be compromised in many ways, the best security measure against misuse or theft involves, is to identify a combination of technical measures and physical security. Users should implement clearly defined polices into their infrastructure to protect data communication availability, integrity and confidentiality [11]. Third parties should not be able to identify or track mobile terminals, also should not be able to perform traffic analysis [8]. Authenticated encryption algorithm, should be applied on the transferred data in order to achieve data confidentiality, data authenticity and protection aginest reply attack.

ISSN: 1738-9976 IJSIA

2. Information Security

Information security refers to the processes and methodologies which are designed and implemented to protect any form of confidential, private and sensitive information or data aginest unauthorized access, such as misuse, disclosure, destruction, modification, or disruption of data. The information security aims to protect the availability, privacy, and integrity of data through the use of digital signature and encryption algorithms.

In modern cryptography, the definition of new basic primitives and their security properties has been one of the primary activities of the last few decades. The data confidentiality and data integrity are considered as two of the most important functions of modern cryptography. Confidentiality can be achieved by using encryption algorithms or ciphers, whereas integrity can be provided by the use of authentication techniques [5]. Two of the cornerstones of modern cryptography are public key encryption as implemented via public-key cryptosystems and digital signatures as implemented by signature schemes. a

Public key cryptosystems are a concealment mechanism, which employs the cryptosystems to enable the first party (the sender) to encrypt a confidential message to a second party (the receiver) without the need to share an initial secret. The sender knows the public key of the reciver. The reciver keeps the secret key hidden. On the other hand, the digital signatures are an integrity mechanism which enable the sender to send a message with a signature tag that verifies the origin of the message to any receiver (verifier). The verifier knows the public key of the sender (signer). There are very high number of variations of the concepts of public-key cryptosystems and digital signature schemes, many properties have been added through the definition and characteristics of this primitive. Moreover, efficient implementations of them and their variations have been investigated. These primitive have been implemented as important underlying components in various security protocols that are used to secure computing and communications infrastructure.

While transmitting data between two tparties (sender and receiver) through any wireless communication channel, confidentiality is provided by encryption algorithms, and the authentication of data is guaranteed by digital signatures. In the traditional paradigm to achieve both confidentiality and authenticity in any secure system, we must use signature followed by encryption namely before a message is sent out from sender to receiver. The sender of the message would sign it using the digital signature scheme, and then encrypt the signed message by using a private key encryption algorithm under a randomly chosen message encryption key. The random message encryption would then be encrypted using the recipient's public key. These cryptographic operations are performed in the order of signature-then-encryption [9, 13]. This approach consume machine cycle and also introduce expanded bits to the original message, moreover it consume a comparable amount of computational time required for signature verification and decryption. Using the current standard signature-then-encryption, the cost of delivering a message in an authenticated and secure way, will consume the sum of the cost for the digital signature and that for the encryption. For wireless communication system, such approach is posing a problem where the efficiency will decrease in terms of computational time and communication overhead which considered as a critical issue [14].

Most of the cryptographic algorithms are divided broadly into two groups, Symmetric key cryptographic algorithm where the same key is used both parties, and the asymmetric cryptographic algorithm which there are two keys private key and public key, the private key is kept secure at the receiver side and the public key is announced to the public. One of the main problems of applying the cryptography algorithms is to preserve the protection of the private key, as it must be secure during its lifetime and beyond. Any

software which requires access to the private key must ensure that the key is protected from hackers. Most of the existing technology fail to keep a strong assurance of the protection of private keys in the software environment [5].

3. Hardware Cryptosystem

Usually the process of applying cryptography algorithm on data to be transferred is applied using the same software and hardware machine that is used to transfer the secured data from sender to receiver. Software-based security solutions encrypt the data to protect it from theft. However, a malicious program or a hacker could corrupt the data in order to make it unrecoverable, making the system unusable. Another method could be used to increase the level of security, is to apply the cryptographic algorithm on an external hardware that is different from the hardware that process the transmitted secure data from sender to receiver, which is called hardware cryptosystem.

Hardware cryptosystem is more secure than the protection provided by the operating systems or any software as operating systems. Usually software programs are vulnerable to malicious attacks from viruses and hackers, the data saved on hard disks can be corrupted after a malicious access is obtained. Therefore, a completely secure system can be created using a combination of hardware-based security and secure system administration policies. Also, a hardware cryptosystem is considered as a good solution in many systems, which can provide high computing power as well as enhanced security features as the private key will be kept secure from introducers and hackers. Using hardware cryptosystem, Even if the system software has been attacked by any of the attack methods, the attacker will only be able to get the ciphering text, which has no value without the knowledge of the key used, as the key will be saved in an external hardware far enough from any hackers or introducers.

Embedded hardware, such as smart cards, and especially DSP (digital signal processors) is an ideal solution[5]. One of the main advantages of using DSP hardware using that it can provide more computing power and higher flexibility than that of VLSI chips or smart cards ,also it provides a low cost due to mass production. Another significant advantage is nearly every computer have a PCI interface and communication ports that support DSP boards[5].

We used in our research a DSP starter kit (DSK) for the TMS320C6416T (1GHz). The 6416 DSP start kit is an all-in-one evaluation platform for the TMS320C6416T Digital signal processor from Texas Instruments. It includes a target board that can be used as a reference design for interfacing the DSP to common devices as SDRAM, flash and a codec as well as special introductory version of TI's flagship Code Composer Studio development tools. An on-board JTAG emulator allows debug from Code Composer Studio through the PC's USB port. The DSP starter kit TMS320C6416T is a fixed point digital signal processor, has 1-GHz Clock Rate up to /1.67 -ns Instruction Cycle.

4. Signcryption Review

Various types of cryptographic systems could be applied to the external DSP starter kit, but each of them have different strengths and weaknesses. Typically, they are divided into two classes; those that are strong but slow to run, and those that are quick but less secure. Cryptographic systems can provide one or more of those services and it is important to distinguish between these, as some algorithms are more suited to particular tasks but not to others. When analyzing your requirements and risks, you need to decide which of these four functions should be used to protect your data: authentication, non-repudiation, confidentiality and integrity. To apply a suitable cryptography algorithm on external hardware and still having all the security functions and features to protect your data we choose the Signcryption cryptography algorithm.

Signcryption algorithm is a high performance cryptographic primitive that has been originally proposed and studied by Youliang Zheng in 1997, with the primary goal of reaching greater efficiency than that can be accomplished when performing the signature and encryption operations separately. It is the primitive that combines the functionality of digital signatures and that of public-key encryption for obtaining less computational and communicational cost. Signcryption is considered as a public key cryptographic method that achieves unforgeability and confidentiality while having a smaller overhead than that required by digital signature followed by public key encryption; which could be achieved by signing and encrypting a message in a single step[7]. Also, time and cost are of the highly demanded factors for any process in any wireless communication system. Through the use of Signcryption algorithm, we are incorporating a high security levels to the data to be transferred which will result in improving both the factors (*i.e*. the time and cost). IF we compare the Signcryption with other traditional schemes, such as encryption then signature or signature then encryption, we will find that the computation and communication cost in Signcryption have been reduced and expansion of information rate has also been greatly reduced, as a shorter signcrptext is most desirable in any real application environment as wireless communication environments.

The original Signcryption scheme in [10] is based on the discrete logarithm problem, but no security proof is given. Zheng's original construction was only proven secure by Baek et al. [15], who described a formal security model in a multi-user setting. A recent direction is to merge the concepts of identity-based cryptography [16,17] and Signcryption to design an efficient identity-based signcryption (IBSC) schemes.

There are two types of security in the security model of Signcryption, the insider security and the outsider security. The insider security means to protect against attacks from his partners private key to be exposed by an attacker's message from the ciphertext. Even if the receiver's private key is discovered, the attacker will not be able to know the real message from the ciphertext. The other type of security which is the outsider security, it means to keep protecting from the third party's attacks, as the attacker knows the public keys of the sender and receiver of the message[18].

There are different Signcryption schemes were proposed, each of them depends on different combination of public key encryption and digital signature algorithm, they are either public-key Signcryption or hybrid Signcryption. Example Elgammal Signcryption, Schnorr Signcryption, Proxy Sincryption, Libert-Quisquater's Signcryption schemes at PKC'2004 and SCN'2004 respectively and Yang-Wong-Deng's Signcryption scheme at ISC'2005.

5. Schnorr Signcryption Scheme

The Schnorr Signcryption algorithm consists of a combination of a public key encryption scheme and a digital signature scheme. We choose to implement the Schnorr Signcryption algorithm in our work. At the Base of this scheme that we implement here stands the Schnorr digital signature, which is a digital signature produced by the Schnorr digital signature algorithm. Mainly the Schnorr Signcryption algorithm is considered the simplest digital signature scheme to be provably secure in a random oracle model; it is efficient and generates short signatures [4].

The Schnorr Signcryption scheme is based on The Huang-Chang Scheme, which is a combination of ElGamal encryption scheme and the Schnorr digital signature scheme [9]. There are four phases in this scheme: setup, Signcryption, Unsigncryption and conversion. In the setup phase, system parameters are set. At the same time, a sender Alice and a receiver Bob register their public keys with a certificate authority (CA). In the Signcryption phase, the signer Alice sincrypts a message for a specified receiver Bob. Using the Unsigncrption algorithm, Bob checks whether the whole ciphertext is generated by Alice.

In the event of a dispute, Bob converts a valid ciphertext into a publicly verifiable signature to convince a judge (or any third party) that the ciphertext is indeed generated by Alice [9]. Furthermore the Huang-Chang scheme which is the combination of the ElGamal encryption scheme and the Schnorr signature scheme at the same time is widely believed that the ElGamal cryptosystem is very secure, and the security of the Schnorr signature scheme is proved to be equivalent to the discrete log problem [9]. We note that the Huang-Chang scheme is indeed satisfying the unforgeability and non-repudiation requirements of any cryptographic algorithm [12].

The Schnorr Signcryption scheme consists of five stages: Setup, KeyGen sender, KeyGen receiver, Signcryption and Unsigcryption.

Setup: Generate the following parameters:

p: a large prime, q: a large prime factor of (p -1), g: an integer with order q modulo p.

h( ): a one way secure hash function.

KH: a keyed one way hash function.

(E,D): the encryption and decryption function of symmetric key cipher (in this work, the ELGamal Public key is chosen as the encryption and decryption algorithm).

KeyGen sender: Xa: signer A's private key and Ya: signer A's public key,

where Ya = g^{-Xa} mod p. (1)

KeyGen receiver: Xb: signer B's private key and Yb: signer B's public key,

Where Yb = g^{-Xb} mod. (2)

Signcryption: Calculate K = h(Yb^{Xa}) mod p. (3)

Split K in to K1 and K2 of appropriate length.

Calculate r = KH_{K2}(m). (4)

Calculate s = x+(r * Xa) mod q.

Calculate c = E_{K1}(m) ElGamal Encryption of the plaintext with the key K1. (5)

Alice the Sender "A" sends (r,s,c) to Bob the receiver "B".

Unsigncryption: To recover the plaintext m from (r,s,c), the receiver 'B' computes the following operations:

Calculate the hash function K= hash(($g^s * Y_a^r$)$^{-Xb}$ mod p. (6)

Split K into K1 and K2 , and Compute m = D^{K_1}(c). (7)

where m is assumed to be a valid message if KHk_2(m) = r. (8)

As mentioned above, ElGamal encryption algorithm is used for both encryption and decryption operations. ElGamal algorithm is an asymmetric key encryption algorithm for public key cryptography; its security depends on the presumed difficulty of the computing discrete logs in a large prime modulus. It has an advantage that Elgamal encryption so probabilistic, means that the same plaintext gives a different ciphertext each time it is encrypted. It consists of three main components: the key generator, the encryption algorithm, and the decryption algorithm.

Key generation: Choose a random z from {1,…, q} and Compute h = g^z. (9)

Encryption: Choose y from {1,….., q-1}, Calculate V1 = g^z mod q. (10)

Calculate W = Y_b^z mod q. (11)

Convert the secret message m into an element m' of G.

Calculate V2 = (W.m) mod q. (12)

The ciphertext is (V1,V2).

Decryption: Calculate the shared secret S = V_1^z and Compute m' = $V_2 . S^{-1}$. (13)

Which it could convert back into the plaintext message m, where S^{-1} is the inverse of S in the group G.

6. Cryptographic Hardware VS. Cryptographic Software

To illustrate the difference between the implementation of the cryptographic software system and the cryptography cryptosystem, we describe the difference between the flow of data between sender and receiver in each case. Suppose we have the sender Alice want to send a very important message to receiver Bob, so she will use one of the Signcryption schemes to encrypt the data before sending it to Bob through the wireless communication channel. There are 2 cases she can use, first encrypt and send the ciphertext using the same hardware machine, and the other case to encrypt and send the ciphertext using two different hardware machines.

In the first case, while Alice uses the same hardware machine and same processor to encrypt data to send it to Bob, she will encrypt the data using the Schnorr Sgincryption encryption algorithm to generate the ciphertext that will be transferred through channel using the wireless transmitter of a communication system; both processes ciphering and transmitting are processed on the same hardware machine. On the other side Bob will receive the ciphered data from the channel using the wireless receiver communication system, then will decipher the data again using the Schnorr Unsigncrytion algorithm, both processes receiving and deciphering are processed on the same hardware machine.

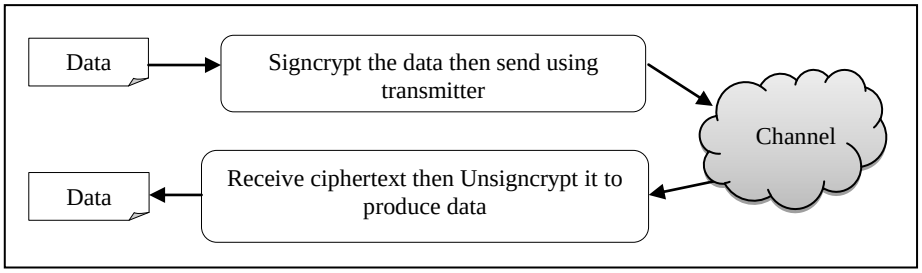

Figure 1. Cryptography Software System

In the second case, while Alice uses two different machine processors to encrypt and transmit data, she will use the DSP starter kit (DSK) TMS320C6416T to encrypt the data using the Schnorr Signcryption algorithm, the ciphered data will be transmitted from the DSP to the transmitter communication system using the PC's USB port. The transmitter system will send the ciphered data through the communication channel to Bob. Using the receiver of communication system, Bob will receive the ciphered data, then transfer it to the DSP using the PC's USB port to decrypt it using the Schnorr Unsigncryption algorithm and generate the original message.

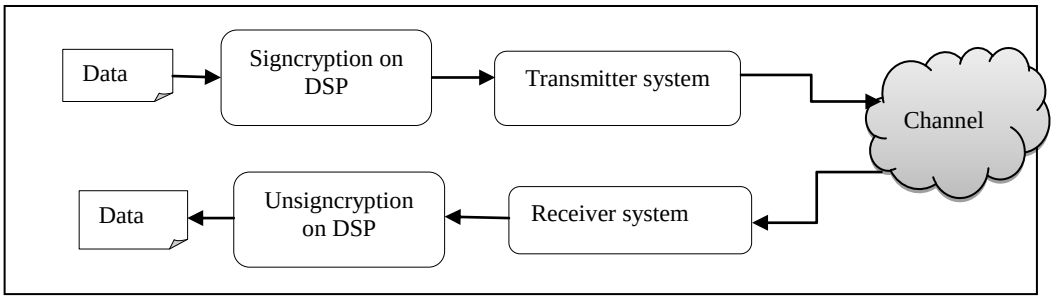

Figure. 2. Cryptography Cryptosystem

In our work, we evaluate the performance of the hardware cryptosystem that increase the security of transferring secure data between two tiers using mobile communication channel as the LTE system. We implemented the whole Schnorrr Signcryption algorithm

on the DSP starter kit (DSK) TMS320C6416T using the code composer studio, which is an integrated development environment (IDE) that supports TI'S microcontroller and embedded processor portfolio. The original message is encrypted using the Schnorr Signcryption algorithm on the DSP kit then, we transferred the encrypted data from the DSP to the LTE transmitter Using the PC's USB port. The LTE transmitter system transfer encrypted data through the channel to the LTE receiver system. The receiver transfered the encrypted data to the DSP using PC's USB port to decrypt data using the Shnorr Unsigcryption algorithm and generate the original message. In Figure 3 and Figure 4, we illustrate a flowchart of the applied scheme implemented on the DSP processor.

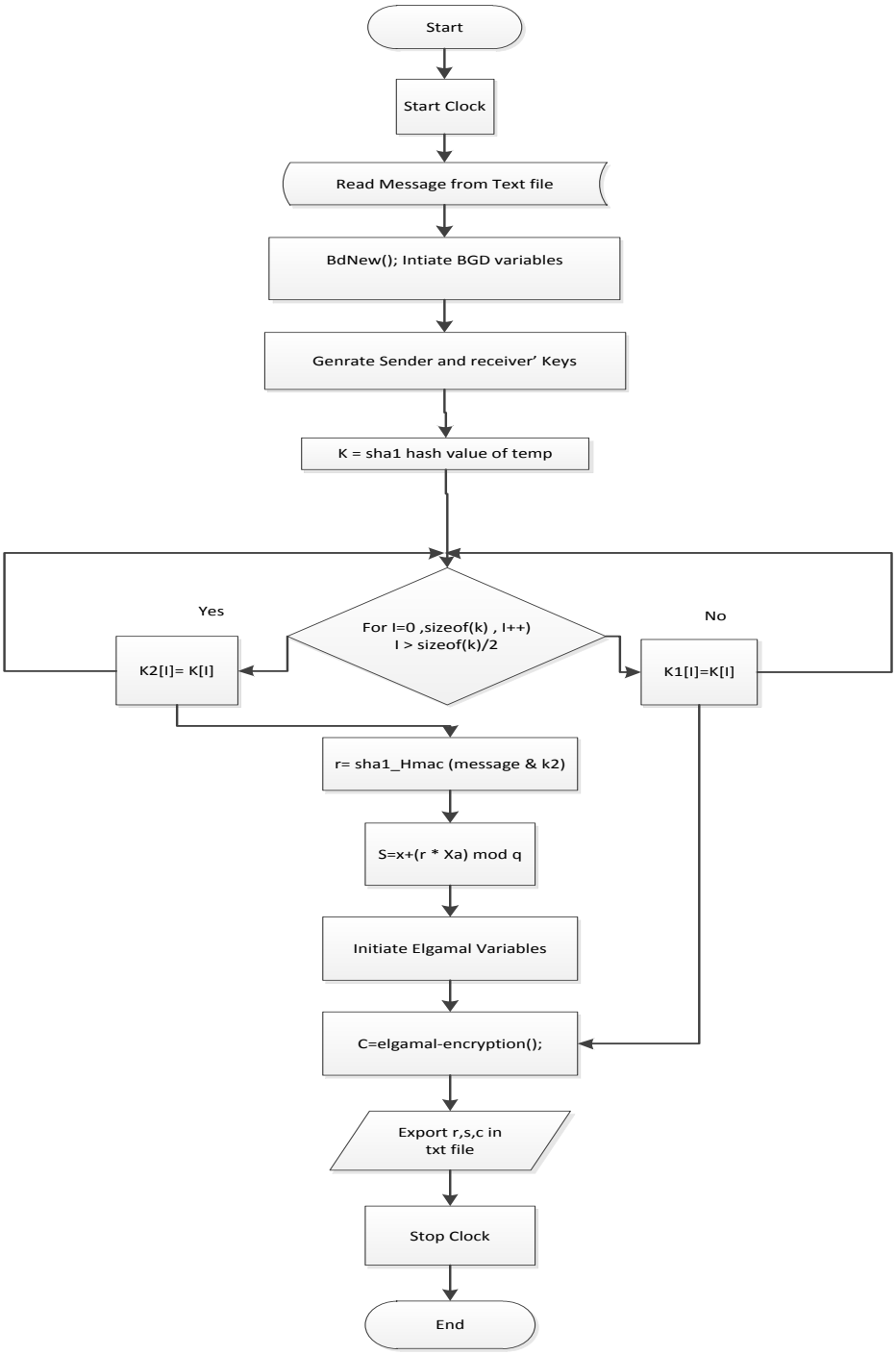

Figure 3. Flowchart of Schnorr Signcryption Encryption Implementation

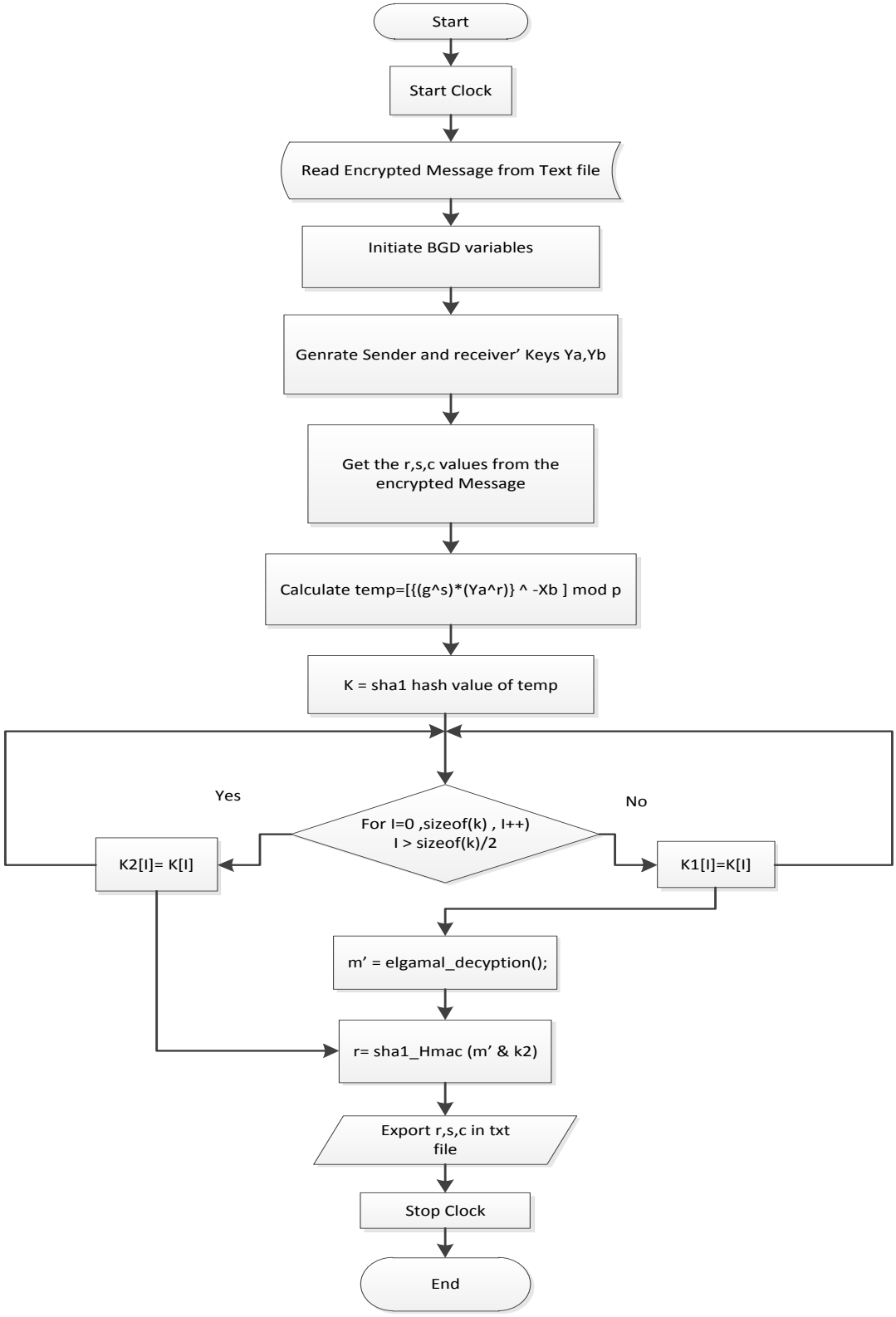

Figure. 4. Flowchart of Schnorr Unsigncryption Decryption Implementation

7. The Results of Applying Schnorr Sgincryption on DSP

We implemented the whole Schnorr Signcryption/Unsigncryption system using a DSP starter kit (DSK) by implementing each step sequentially using C programing language on the Code composer studio. We evaluated the performance of our system by computing the run time consumed while encrypting and decrypting data to be transferred through the LTE communication channel. We applied our system on the DSP starter kit (DSK) TMS320C6416T while compiling on the code using the Code Composer Studio. Here we shows in Table 1 the hardware specification of DSP starter kit (DSK) TMS320C6416T.

Table 1. Specifications of DSP Embedded Hardware

	DSP starter kit(DSK) specifications
Processor	1 GHZ
Ram	700 MB

As shown in Table 2 and Table 3, we generated five random messages and calculated the time consumed for both encrypting each message and decrypting the received message to recover the original message successfully.

Table 2. Time Consumed While Encryption of Data Using Schnorr Signcrpytion Algorithm on DSP

	Schnorr Signcryption on DSP starter kit(DSK) in Sec
Message 1	0.247
Message 2	0.245
Message 3	0.245
Message 4	0.246
Message 5	0.247
Average	**0.246 sec**

Table 3. Time Consumed While Decryption of Data Using Unsigncrpytion Algorithm on DSP

	Schnorr Unsigncryption on DSP starter kit(DSK) in sec
Message 1	0.105
Message 2	0.103
Message 3	0.102
Message 4	0.076
Message 5	0.082
Average	**0.093 sec**

8. Proposed Enhancement Model Through Parallelization and Pipeline Techniques

One of the most efficient means of improving the performance in a hardware environment is Pipelining. The computational time of the Schnorr Signcryption algorithm could be improved using parallelizing of cryptographic algorithm, it could be accelerated using the pipelining algorithm [12]. Using 3 DSP processors in the implementation of the Schnorr Signcryption algorithm, we could decrease the computational time by distributing and divide each stage across the DSPs to accelerate the calculating operation time.

As mentioned in section 4, the Schnorr Signcryption scheme consists of five main stages: Setup, KeyGen sender, KeyGen receiver, Signcryption , Unsigcryption. The first three stages could be calculated parallel and sequentially using 2 processors. First will generate the p,q and g values using DSP1 then start to calculate the KeyGen of the sender and receiver in parallel using DSP1 and DSP2 as in Figure 5.

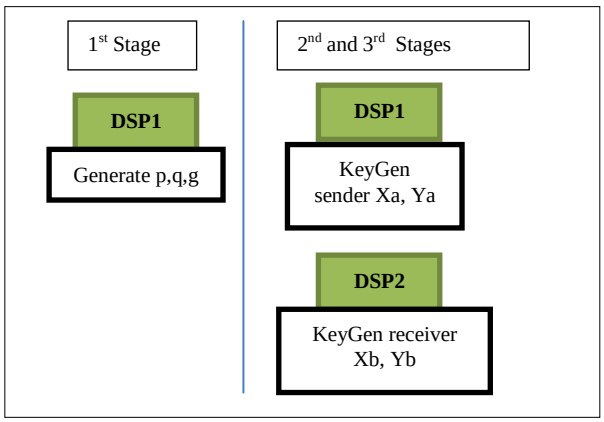

Figure 5. 1st, 2nd, and 3rd Stages of Pipeline Schnorr Signcryption

The Fourth Schnorr Signcryption scheme's stage can be parallelized in two levels of parallelization, 2 DSP processors will be used to pipeline in first level (Pipeline Level 1) in sender side and another 2 DSP processors will be used in receiver side for Unsigncryption. In the fourth stage, we calculate K1 and K2 sequentially using DSP1, then calculate r and s values using pipeline techniques using DSP1 and DSP2 as in Figure 6 [1]. At the second level (Pipeline Level 2) will calculate the c value which is in our case will be executed by Elgamal algorithm , the encryption operation of Elgamal could be divided into another three subtasks calculate V1 Using DSP1 in parallel while calculating W1 using DSP2 and V2 using DSP3 using pipeline as shown in Figure 6 [1].

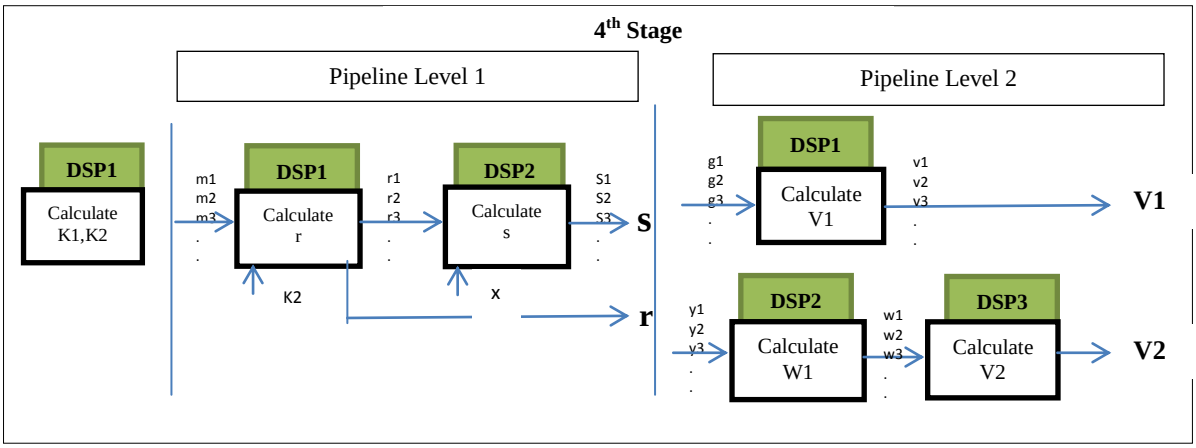

Figure 6. :4th Stage of Pipeline Schnorr Signcryption

The same behavior will be used in the 5th stage in the receiver side while calculating the Schnorr Unsigncryption scheme. Will calculate the K value using DSP1 sequentially, then split it into K1 and K2 using the same processor DSP1. After generating the k value, will start to discover the message using Elgammal decryption algorithm while

calculatings value using DSP1 and calculating m' value using DSP2 using the pipeline technique as shown in Figure 7.

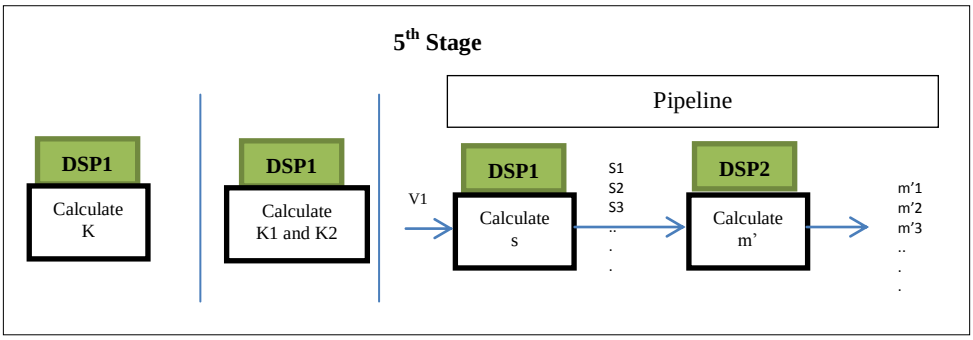

Figure 7. The 5th Stage of Pipeline Schnorr Signcryption

As shown in the above proposed technique while using parallelization and pipelining in Schnorr Sgincryption algorithm, some of the DSP processors will be idle part of the time, which lead to load imbalance. To avoid load imbalance we could use more than 1 processor cooperate in computing different instructions of some functions. For example in Unsigcryption stage while calculating the hash function K= hash $(g^s * Y_a^r)^{-xb}$ mod p, this task could be divided into four subtasks: exponential operation g^s, will improve the modular inverse exponential of the result. The first two subtasks of calculating the exponential are calculated once per each message, so it will be calculated sequentially. Then the third task which calculates the modular multiplication operation could be divided into three simple multiplications and one addition. As the modular multiplication operation is considered one most consuming operation time, it could be reduced by incorporating the idle processors in the execution of each modular multiplication operation [12].

9. Conclusion

We have proposed a method of integrating a DSP based hardware Schnorr Signcryption encryption algorithm with an existing wireless communication system to illustrate the channel between sender and receiver on both sides. The architecture can maintain positive feature of the wireless communication system while improving the security of data using the Schnorr Signcryption hardware encryption in a way that limits the overheads involved.

An external plug-in DSP board is chosen to maximize the convenience of the sender and the receiver security as the keys stored on this board are much more securely protected than keys stored in software on the PC or on the PC hard disk. Plugging a DSP card into the PCs internal PCI slot could reduce overheads in transmission and improve the overall speed of the system. The system's performance is fast enough for small to medium size messages, especially with Signcryption key lengths up to 1024 bits. Also the above tables showed that if we use an external DSP with higher processor specifications could decrease more and more the time consumed while cyphering and deciphering data which will lead to more applicable system to be applied in different applications in life.

Experimental results have shown that the TI optimizing compiler used in our project generates code that is poorly parallelized, which prove that when use pipelining will improve the performance and the time consumed in the whole system. Also, we proposed an enhanced model of the implementation of the Schnorr Signcryption algorithm by using three DSP hardware processors that work together using parallelization and pipeline

techniques, which could reduce the computation overhead in the Schnorr Signcryption algorithm, it reduces the computational time required to execute the algorithm with respect to its corresponding values of a sequential and parallel execution. Experience indicates that assembly coding of critical sections could also provide significant improvement of the overall system speed performance.

10. Pseudo Code

We present here a pseudo code of the implementation of the Schnorr Signcryption algorithm using C programing language on the DSP kit .

```
Transmitter
Start
Start clock
BIGD  p,q,g,Xa,Ya,Xb,Yb,x,r,s,c,k,k1,k2
Read message from text file and set it to in Message
bdPower(temp,g,Xa)  , the power g^-Xa in temp
bdModInv(Ya,temp,p) , the mode inverse of temp in Ya
bdPower(temp,g,Xb)  , the  power g^-Xb in temp
bdModInv(Yb,temp,p) , the mode inverse of temp in Yb
bdPower(temp,Yb,x)  , the  power Yb^x in temp
bdModulo(result,temp,p); set temp mod p in result
sha1_init(&ss)
ss= result
k= sha1_result(&ss)
For (I=0 , I<k.length , I++)
If I<(k.length/2)
k1[I]=k[I]
else
k2[I]=k[I]
hmacKey1 =k2
sha1_initHmac(&ss, hmacKey1 hmacKey1.length)
sha1_write(&ss, Message ,Message.Length)
r= sha1_resultHmac(&ss)
bdMultiply(temp,r,Xa)
bdAdd(temp,temp,x)
bdModulo(s,temp,q)
zintoz() intiate Elgammal varialbes zp,zg,zx,zk
ElGamal_encryption(Message, c, Message.length, c.length, zg, zx, zp,zk)
Stop clock
Time=start –stop
Display r,s,c ,Time
End.

Receiver:
Start
Start clock
BIGD  p,q,g,Xa,Ya,Xb,Yb,x,r,s,c,k,k1,k2
Read message from text file and set it to in EnMessage
bdPower(temp,g,Xa)  , the power g^-Xa in temp
bdModInv(Ya,temp,p) , the mode inverse of temp in Ya
bdPower(temp,g,Xb)  , the  power g^-Xb in temp
bdModInv(Yb,temp,p) , the mode inverse of temp in Yb
Split EnMessage into 3 arrays parR , parS and out
```


bdConvToDecimal(r, parR, parR.length)
bdConvToDecimal(s, parS, parS.length)
bdPower(temp1,g,s) , the power g^s in temp1
bdPower(temp2,Ya,r) , the power Ya^r in temp2
bdMultiply(temp3,temp1,temp2)
bdPower(temp3temp3,Xb)
bdModInv(kbh,temp3,p)
sha1_init(&v)
sha1_write(&v, kbh, sizeof(kbh))
k = sha1_result(&v)
For (I=0 , I< sizeof(k), I++)
If I<(sizeof(k) / 2)
k1[I]=k[I]
else
k2[I]=k[I]
zintoz() intiate Elgammal varialbes zp,zg,zx,zk
ElGamal_decryption(out, Message, sizeof(out),zg ,zk, zx, zp)
hmacKey1=k2
sha1_initHmac(&u, hmacKey1, sizeof(hmacKey1))
sha1_write(&u, Message , sizeof(message))
r = sha1_resultHmac(&u)
Stop clock
Time = Start-Stop
Display Time, r, s, Message
End.

Refrences

[1] A. Elshobaky, G. Elkabbany, M. Rasslan , S. Gurguis, "Implementation, Comparison, and Enhancement of Secure Communication Designs", Procedia Computer Science 37 **(2014)**, pp. 363 – 369.
[2] Savu, Laura. "Signcryption scheme based on schnorr digital signature", International Journal of Peer to Peer Networks (IJP2P) ,vol.3, no.1, **(2012**).
[3] T. Mshvidobadze, "Evolution mobile wireless communication and let networks", in Application of Information and Communication Technologies (AICT), 6th International Conference on **(2012)**, pp. 1-7.
[4] S. Laura, "Combining Public Key Encryption with Schnorr Digital Signature", Journal of Software Engineering & Applications, vol. 5, issue 2, **(2012)**, p102-108.
[5] Hu, J.; Hoang, X. D. & Khalil, I., 'An embedded DSP hardware encryption module for secure e-commerce transactions.', Security and Communication Networks vol 4, no. 8 , **(2011)**, pp. 902-909 .
[6] Zhou. X.,"Improved Signcryption Scheme with Public Verifiability", Pacific-Asia Conference on Knowledge Engineering and Software Engineering, IEEE **(2009)**, pp. 178–181.
[7] J. Zhang, Q. Geng, "Cryptoanalysis of Two Signcryption Schemes", Fifth International Conference on Information Assurance and Security, **(2009)**.
[8] B. Preneel, "Mobile and Wireless Communications Security", Katholieke Universiteit LeuvenDept. , IOS Press, NATO ASI on Aspects of Network and Information Security , pp 119-133,**(2008).**
[9] G. Wang, R. H. Deng, D. Kwak, SangJae Moon, "Security Analysis of Two Signcryption Schemes". Proceedings of 7th International Conference, ISC 2004, Palo Alto, CA, USA, September 27-29, **(2004)**, pp 123-133.
[10] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost(signature) + cost(encryption)", In Advances in Cryptology -CRYPTO'97, LNCS 1294, Springer-Verlag, **(1997)**, pp. 165-179.
[11] H. Federrath, Anja Jerichow, D. Kesdogan, Andreas Pfitzmann, "Security in Public Mobile Communication Networks", International Workshop on Personal Wireless Communications, Verlag der Augustinus Buchhandlung Aachen**, (1995),** pp. 105-116.
[12] Ghada F. El Kabbany, Heba K.Aslan, Mohamed M. Rasslan, "An Efficient Pipelined Technique for Signcryption Algorthims ", International Journal of Computer Science Issues (IJCSI),vol. 11, Issue 1, Jan. **(2014)** .
[13] A. Atanasiu, L. Savu, "Signcryption based on different Digital Signature Schemes".Journal of information systems and operations management Vol.6 , **(2012)**, pp 19-28.

[14] Y. Zheng, H. Imai, "How to construct efficient signcryption schemes on elliptic curves", Information Processing letters Vol.68, **(1998),** pp. 227-233.
[15] J. Baek, R. Steinfeld, Y. Zheng, "Formal proofs for the security of Signcryption", Journal of Cryptology Volume 2274 of the series Lecture Notes in Computer Science , February (2002), pp 80-98.
[16] A. Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology, CRYPTO'84, LNCS, vol. 196, Springer-Verlag, **(1984),** pp. 47–53.
[17] D. Boneh , M. K. Franklin, "Identity-Based Encryption from the Weil Pairing" , Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, August 19-23, **(2001**), pp. 213-229.
[18] C. How Tan, "Insider-secure Hybrid Signcryption SchemeWithout Random Oracles", Proceedings of the The Second International Conference on Availability, Reliability and Security, April **(2007),** pp.1148-1154

Authors

Aya Elshobaky has received her B. Tech. degree in Electrical and Electronic Enginering, in 2009 from the Faculty of Engineering, Alexandria University. Recently, she has completed her M. Tech. From the same university and her area of interest includes Security and Cryptography algorithms.

Shawkat K. Guirguis was born in 25th February, 1958, Alexandria, Egypt. He obtained the B.Sc. and M.Sc. degrees in Computer Science & Automatic Control, Faculty of Engineering, Alexandria University, 1981 and 1984 respectively with Grade: "Distinction with the degree of honor". In 1988 he obtained a Ph.D. in Electronics & Communication, Cairo University, Co-Supervised by Imperial College of Science & Technology, University of London, U.K. Currently he is Professor of Computer Science and Informatics, department of Information Technology, Institute of Graduate Studies & Research (IGSR), Alexandria University, Egypt. His current research interests include network and information security, data mining and cloud computing.

Mohamed Raslan is an Assistant Professor at Electronics Research Institute, Cairo, Egypt. He received the B.Sc., M.Sc.,and Ph.D. degrees from Cairo University and Ain Shams University, Cairo, Egypt, in 1999, 2006, 2010 respectively. His research interests include: Cryptology, Digital Forensics, and Networks Security.

