Securing Computerized Personal Identification Data with Confidentiality and Non-repudiation Capabilities Based on Programmable System on Chip (PSoC) Technology

Sung-Tsun Shih[1], Chian-Yi Chao [2], Chin-Ming Hsu [3]

[1]Department of Electronic Engineering, Cheng Shiu University, Kaohsiung, Taiwan
[2]Department of Electronic Engineering, Kao Yuan University, Kaohsiung, Taiwan
[3]Department of Information Technology, Kao Yuan University, Kaohsiung, Taiwan
stshih@csu.edu.tw

Abstract: In this study, a cipher/decipher based on programmable system-on-chip (PSoC) technology is proposed to prevent unauthorized people from revealing and abusing users' computerized personal identification data (PID) during transit and at rest. The proposed PSoC-based cipher/decipher consists of a Public Key Infrastructure (PKI) authentication protocol, a programmable microcontroller named AT89S51 single chip, and an application specific integrated chip (ASIC) named EPF10K Field Programmable Gate Array (FPGA) device. The PKI authentication protocol with the registration and transaction processes for verification/identification is used to secure the encrypted PID data transmitted on the Internet. The programmable microcontroller mainly programs the encrypting/decrypting codes and the ASIC device is implemented with the stream cipher's logical operations, including, segmentation, exclusive or (XOR), and rotation. This design supports off-line encryption of numerous users' PID. The proposed approach has been simulated using C programming language running on a 1,500MHz Pentium PC with 512 MB of RAM. From the experimental results, the size of the ciphertext, the size of the key stream, and the encryption time are dependent on the secret key, nonce, and plaintext; the design of ASIC hardware device is of low hardware cost and low design complexity; and the software of PSoC-based cipher/decipher could provide better code density. Conclusively, using certificates and dynamic cookies for verification/identification ensures that only authorized users can obtain the access to their personnel record.
[Sung-Tsun Shih, Chian-Yi Chao, Chin-Ming Hsu. **Securing Computerized Personal Identification Data with Confidentiality and Non-repudiation Capabilities Based on Programmable System on Chip (PSoC) Technology.** Life Science Journal. 2011; 8(4):916-922] (ISSN:1097-8135). http://www.lifesciencesite.com.

Keywords: Computerized personal identification data, cipher/decipher, PKI, and authentication.

1. Introduction

Privacy means an ability to protect personal secrets and/or a state of being hidden from public view [1-2]. Before the advent of computers, privacy protection was usually achieved by using key locks to protect physical resources. With the developed computer and Internet technologies, the traditional key locks are not effective for privacy protection because most organizations, including commercial and social organizations, store data on computers. Specifically, data is shared among different institutions via the Internet and a large amount of commerce is electronically conducted. These advanced technologies are able to bring more convenience to life but also bring an increased risk of abusing or disclosing personal data, thereby resulting in the privacy threat: identity theft.

Identity theft is usually initiated by disloyal insiders or adversaries who steal one's identifying data stored in a database or transmitted on a network [3]. Currently, identity theft is one of the fastest growing crimes in the United States. An estimated 500,000 to 700,000 Americans fall victims to identity theft every year, and losses resulting from identity theft cost around 3.5 billion dollars in 2002 and the losses rose to over 8 billion dollars in 2006 [4-5]. In other countries, this problem is just as urgent as in the United States. One risk of abuse or improper disclosure of personal data may occur in e-commerce services. For example, an individual may register his identity information including name, address, social security number, and account details in an institution's database. The administrator of the institution will use the registration information to make decisions on supplying data in response to service requests from the user. In the absence of effective protection on users' personal data, their identity information is susceptible to being misused by unauthorized users or organizations. Consequently, an individual may acquire a bad reputation due to improper disclosure of his personal data, thus requiring extra money, time, and effort to recover one's reputation and credit standing. Benner, Givens, and Mierzwinski [6] have investigated that an average of $808 and 175 hours of effort is needed for a person to put things right.

Cryptography is commonly classified into three parts: un-key, secret key, and public key cryptography. Un-key cryptography uses a function to map, hash, or transform a message into different

presentation by mathematical operations, such as permutations and involutions, for data integrity. Secure hash algorithm (SHA) [7] and message digest (MD5) [8] are two typical researches which usually condense a message of any size down to a small fixed-size block of messages by using bitwise logical AND, inclusive-OR, eXclusive-OR, and complement operations.

Secret key cryptography, symmetric cryptography, encrypts/decrypts a message using a secret key shared between two communicating parties. A typical example named data encryption standard (DES) uses a secret key to transform a plaintext which is grouped into contiguous fix-length blocks via substitution and permutation operations. The length of the ciphertext is the same as that of the plaintext. However, it is insecure because a DES key can be recovered in 56 hours [9]. Niinimaki and Forsstron [10] proposed an electronic prescription system using this cryptography, which stored a secret key in a smart card to prevent hackers or unauthorized people from disclosing users' passwords. In general, such type of cryptography performs efficiently but it has key distribution problem. Several researches [11-15] have proposed key-exchange-based authentication protocols coupled with symmetric-key techniques to solve the key distribution problem. This kind of password- and PKI-based key-exchange protocol technology mainly uses a shared session key to prevent the password from guessing attack with the computation-efficiency capability. However, it requires periodically changing passwords for better security.

Public key cryptography, asymmetric cryptography, encrypts/decrypts a message by using a mathematically related key pair, a public key and private key, in which the key used for encryption is different from decryption. The public key is open publicly and the private key needs to be held only by its owner securely. This cryptography is usually used for key encryption/decryption, digital signature generation, and key exchange. RSA [16], DSA [17], and Diffie-Hellman [18] use this cryptography for data encryption/decryption, data authentication, and key exchange. RSA is based on integer factorization operations whereas DSA and Diffie-Hellman are based on discrete logarithm operations. Blobel and Pharow [19] proposed a public key cryptosystem that stored the keys in a smartcard to protect medical data from network intruders. Meyer and Lundgren [20] produced the digital signature of an individual's authentication code to increase the security of healthcare networks. Ohta and Okamoto [21] introduced multi-signature schemes based on elliptic curve mathematics to ensure the security of digital signatures. However, this cryptography requires time-consuming computations in generating keys.

Menasce [22] examined the security performance of cryptographic algorithm/key-length combinations. As Menasce points out, the security methods based on cryptographic technology have constraints on the key size used to meet certain security requirements. In general, the processing time of the symmetric key encryption is exponentially faster than that of the public key encryption. The symmetric key encryption with a secret key shared between two certified users has key management and distribution problems because the quantity of keys increases with the square of the number of communicating parties. In addition, the use of cryptography-based security mechanism usually needs intensive mathematical computation in deriving or generating keys. A great quantity of memory used to store public parameters is needed when the number of classes or nodes increases. For the conventional authentication techniques based on hard mathematical operations, the use of larger key sizes results in better security but the processing time will be increased greatly.

In order to improve the disadvantages mentioned above, this study proposes a PSoC-based security mechanism to prevent unauthorized disclosure and improper modification of one's computerized personal data during transit and at rest. The proposed privacy technology not only minimizes the quantity of RAM usage to store temporary parameters but also implements simple mathematical operations at a small expense of hardware to process data efficiently.

2. Proposed Research

Figure 1 shows the PKI-based system overview of securing computerized personal data during transit and at rest. It consists of four components: E-commerce certificate authority (ECA), affiliated E-commerce merchant database, users' authentication server, and PSoC-based cipher/ decipher at user terminal. The ECA manages the certificates and public-private key pairs. The database stores users' encrypted personal identification data (PID). The authentication server interacts with the ECA, encrypted PID database, and PSoC-based user terminal via the authentication protocol. It handles verification/identification processes and stores temporary processed data in the PID buffer. An individual can utilize an IC token or a keyboard to access his PID. The principles of the proposed PSoC-based cipher/decipher and PKI-based authentication protocol are detailed below.

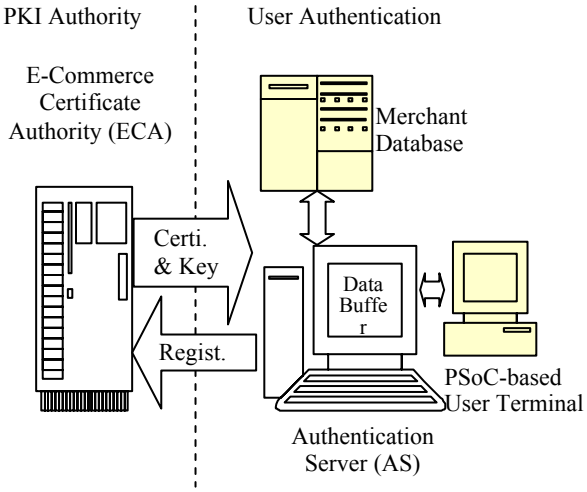


Figure 1. PKI-based system overview of securing computerized personal data during transit and at rest

2.1. PSoC-Based Cipher/Decipher

As shown in Figure 2, the proposed PSoC-based cipher/decipher consists of three components: a database system, an 89S51-based programmable microcontroller, and an FPGA device for encryption/decryption. The database system stores uses' computerized personal data; the 89S51-based programmable microcontroller is used to program the encryption/decryption codes; and the FPGA device allows users to implement encryption/decryption algorithm at a small expense of hardware such as EPF10K20RC240-4.

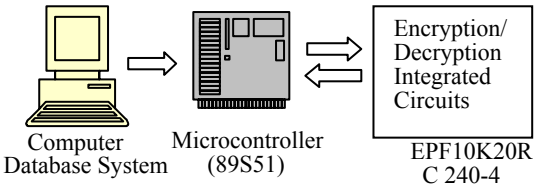


Figure 2. PSoC-based cipher/decipher

2.1.1. Database System

In this study, we assume that the database system stores users' personal identification information and order information for E-commerce application. The format of personal identification information contains an individual's user name, password, sex (female/male), date of birth, social security number, address, and E-mail. The format of the order information contains product name, product identification, date of order, quantity, price, payment method, status, and total price.

2.1.2. AT89S51 Programmable Microcontroller

Figure 3 shows the circuit schematic of 89S51-based programmable microcontroller. As shown in Figure 3, the user's personal identification is transmitted from the computer database system to the 89S51 microcontroller byte by byte at first. The 89S51 stores the received PID and then passes the received data to the input of the FPGA. After all the PID data are stored in the ROM of the 89S51, the 89S51 sends the encrypting/decrypting codes based on the algorithm as given in the authors' previous study, stream cipher [23], byte by byte to the input of the FPGA device via the PORT 0 of the 89S51. The FPGA device processes the received machine codes to generate the encrypted PID; the encrypted PID are then sent byte by byte back to the 89S51 via PORT 2, stored in the 89S51's ROM, and transmitted back to the computer via the RS232.

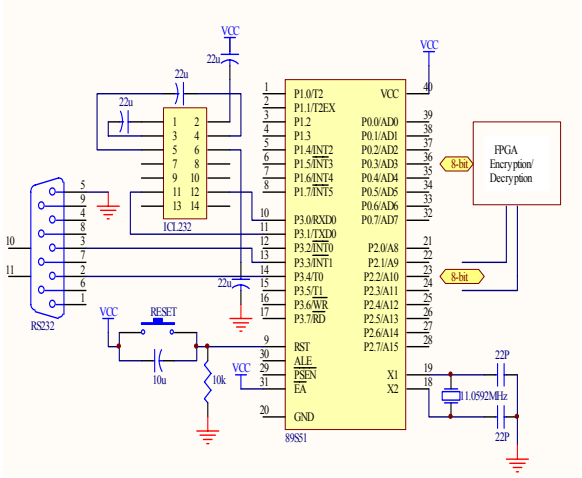


Figure 3. Circuit schematic of AT89S51 programmable microcontroller

2.1.3. The Design of FPGA Device

The hardware structure of the encryption/ decryption FPGA device is shown in Figure 4, which includes 6 units: decoding, addressing, register, ALU, memory, and buffers. The decoding unit decodes 8-bit input machine code into three parts: 2-bit instruction, 2-bit addressing mode, and 4-bit operand. Table 1 illustrates the instruction sets used in the FPGA device. There are four kinds of instruction sets: MOV, XOR, Shifting, and Rotating and four kinds of addressing modes: register, register/memory, memory /register, and direct. In addition, there are seven different registers: A, B, C, D, MBR (data buffer register), MAR (address buffer register), and MOR (output buffer register). The 4-bit operand can be either register or address. The memory has 64 bytes. The ALU typically can execute a range of standard arithmetic and logic instructions.

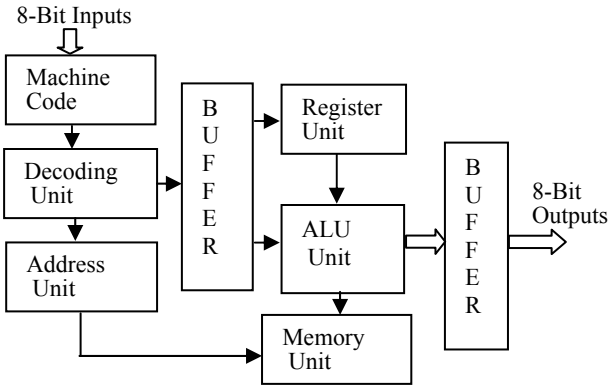


Figure 4. Hardware structure of encryption/ decryption FPGA

Table 1. Instruction sets

Instructions	Modes	Machine Codes in Hex
MOV	R, R Add R/Add Add/R	00 - 0F 10 - 1F 20 – 2F 30 – 3F
XOR	R, R Add R/Add Add/R	40 - 4F 50 - 5F 60 – 6F 70 – 7F
LS LSC LR LRC	R R R R	80– 8F 90– 9F A0 - AF B0 - BF
RS RSC RR RRC	R R R R	C0– CF D0– DF E0 - EF F0 – FF

2.2. PKI-Based Authentication Protocol

As illustrated in Figure 5, the proposed online PKI-based E-commerce transaction protocol consists of the registration process and transaction process. The definitions of the notations used throughout in this subsection are listed below.

U, M : user, merchant

ECA : E-commerce certificate application

C_U, C_M : user's certificate, merchant's certificate

$E_{K_{UM}}(PID_i)$: the PID_i ciphertext, where $E_{K_{UM}}$ denotes a secret key encryption algorithm (e.g. DES) with the secret key K_{UM} shared by the U and the M

$P_{d_C}[K]$: the CA's signature, where P_{d_C} denotes a public key encryption algorithm with the CA's private key d_C; K is an individual's public key

O_I, C_I, $D(O_I)$, $D(C_I)$: order information, card information (e.g. Name, N_C, and valid date), digest of O_I, digest of C_I

PID_i, PID_{i+1} : i^{th} transaction identifier, $i+1^{th}$ transaction identifier

Note that the PID_i and PID_{i+1} are automatically generated by taking the PID_0 of the U as the initial value through the random number generator stored in the U's and M's database.

As shown in Figure 5(a), the U (M) sends the paper application to the ECA to initialize a registration process. The U (M) will receive the PSoC-based cipher/decipher, the C_U (C_M), and the public-private key pair from the ECA, where the C_U (C_M) basically includes a K, $P_{d_C}[K]$, and other parameters. The PSoC-based cipher/decipher contains the user information, a session secret key generator, encryption/decryption algorithm, and a dynamic personalized identifier generator. The U (M) uses it to produce the $D(O_I)$, $D(C_I)$, and $E_{K_{UM}}(PID_i)$. The procedures of authorizing an online e-transaction, as shown in Figure 5(b), are described in the following.

Step 1: Requiring an online E-commerce transaction

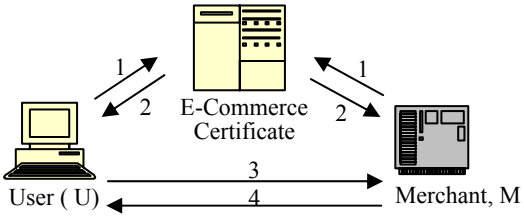
The U sends the C_U, O_I, $D(O_I)$, $D(C_I)$, $P_{K_G}(C_I)$, and $E_{K_{MB}}(PID_i)$ to the M's website via the Internet to request an e-transaction.

Step 2: Verifying the U's identity

Upon the confirmation of the validity of the C_U, if the U is identified and the decrypted C_I of the U is legitimate and the decrypted PID_i is valid, the M sends the acknowledgement back to the U.

Step3: Updating PID_{i+1} in the U's and M's database

Upon the reception of the acknowledgement from the M, the U updates the PID_{i+1} in its database system and the M updates the PID_{i+1} in its database, respectively.



Note. 1. The paper application form;
2. The PSoC-based cipher/decipher, certificate, and public-private key.
3. The application form via the Internet
4. Acknowledgement

(a)

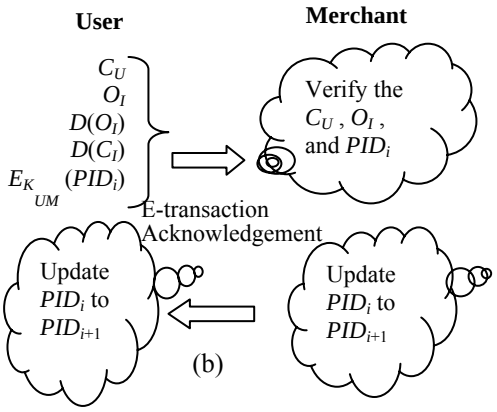


Figure 5. Proposed PKI-based E-commerce transaction; (a) the registration; (b) the transaction process.

3. Experimental Results

The proposed approach described above has been simulated using C programming language running on a 1,500MHz Pentium PC with 512 MB of RAM. Figure 6(a) shows a part of a user's personal identification data. Figure 6(b) shows the results of the encrypted *PID* by means of the *PW* = #qF!Lm2!, where

***P*$_{SSN}$ = A220F70346 (10 bytes)**
***PID* = TRACEY LI|M|1453 THUNDERBAY BROADWAY LOSANGELAS, USA|19900819|(042)22642993 (74 bytes)**

The author observes that the total size of the encrypted *PID* is 98 bytes, whereas that of the original *PID* is 84 bytes. This indicates that there is no overhead memory usage. One important feature is that the size of the ciphertext, the size of the key stream, and the encryption time are dependent on the secret key, nonce, and plaintext. This feature indicates that the proposed cipher is much more difficult for the statistical and differential cryptanalysis because the relationship among ciphertexts and key-stream numbers are dynamically associated for each encryption. Additionally, there is no influence on frequent record access because the encryption of numerous users' PID is done off-line.

Table 2 summarizes the definitions and countermeasures of four attacks for an opponent from inside or outside the system. One such type of attack is the brute-force attack. In the method proposed, it would take a hacker about 42,000 years to search the entire space of the key *PW* with no less than 8 keyboard characters [24]. Thus, it is difficult for hackers to break the keys. Another type of attack is the collaborative attack. In order to cooperatively reveal a user's identity, the function *F* has the security complexity of *O* (2^n) [25] with zero knowledge transmission of the key and *PID*. Thus, it is difficult to achieve collaborative attack. Moreover, because a random number, which is updated for each authentication trail, is used to produce a variant *PID* ciphertext and to protect the key *PW*. It is almost impossible to use the information from previous execution to disclose a user's PID and break the key to find out the *PID* by means of a large number of samples *PID* ciphertexts.

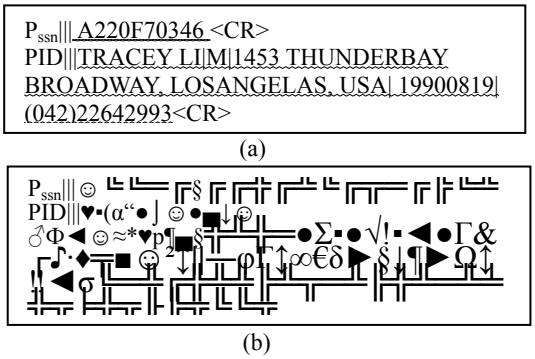


Figure 6. (a) Part of a user's PID; (b) results of the encrypted *PID* with the *PW* = #qF!Lm2!

Table 2. Definitions and countermeasures of four attacks for an opponent from inside or outside the system

Types of attacks	Definition	Principles to avoid attacks
Brute-force	An adversary searches the space of all possible keys.	Using the *PW* that is composed of keyboard characters
Collabo-rative	An adversary decrypts pieces of the ciphertext to extract the key without additional information.	Using several parameters to encrypt an EMR and zero knowledge transmission of the *PID* during transit and at rest.
Replay	Two adversaries are cooperatively trying to reveal the EMR without the patient's consent.	Using a random number, which is updated for each process, to produce a variant *PID* ciphertext and prevent the key *PW* from being easily disclosed.
Crypto-graphic	An adversary purports to be another using the information obtained from previous executions.	

4. Conclusions

This study proposes a programmable system-on-chip (PSoC)-based security technology to prevent unauthorized users from abusing or disclosing an individual's computerized personal identification data during transit and at rest. The proposed security technology includes two clams: One clam is that end-users and data owners must have more hands-on participation as safeguards. The other clam is that the protection technology must use trusted third parties to support origin verification, message integrity, and non-repudiation capabilities. In this study, the PKI verification/identification protocol is mainly used to secure the encrypted PID data transmitted on the Internet and support non-repudiation capability. The programmable microcontroller and ASIC technology are used for encryption/decryption and for stream cipher's implementation, which provides the confidentiality capability and supports the characteristic of off-line encryption of numerous users' PID. The proposed technology not only minimizes the quantity of RAM usage to store temporary parameters but also implements simple mathematical operations at a small expense of hardware to process data efficiently.

Conclusively, the advantages of the technology are three-fold. First, an agent can install a large number of encrypted users' personal identification data in their databases without excessive overhead processing time. Second, the hardware structure is of low hardware cost and low design complexity; the use of 8-bit instruction length allows better code density. Third, using certificates and dynamic cookies for verification/identification ensures that only authorized users can obtain the access to their personnel record. This work can be applied in E-commerce activity. An agent can store the keys in both the PSoC system and the agent's database for encryption/ decryption.

Corresponding Author:
Dr. Sung-Tsun Shih
Department of Electronic Engineering,
Cheng Shiu University,
Kaohsiung , Taiwan, R.O.C.
E-mail: stshih@csu.edu.tw

References

1 V. Senicar, B. Jerman-Blazic, T. Klobucar. Privacy-enhancing technologies—approaches and development. Computer Standards and Interfaces, 2003; 25(2): 147-158.

2 Available at: http://www.yourdictionary.com/ahd /p/p0568700.html

3 J. E. Matejkovic, K. E. Lahey. Identity theft: no help for consumers. Financial Services Review, 2001; 10: 221-235.

4 E. Wales. Identity theft. Computer Fraud & Security, 2003; 2: 5-7.

5 S. Hinde. Careless about privacy. Computers and Security, 2003; 22(4): 284-288.

6 J. Benner, B. Givens, E. Mierzwinski. Nowhere to turn: Victims speak out on identity theft. CALPIRG/Privacy Rights Clearinghouse Report, 2000.

7 Secure hash standard (SHA, FIPS PUB 180-1), 1995. Available at: http://www.itl.nist.gov/ fipspubs/fip180-1 htm

8 R. L. Rivest. The MD5 message digest algorithm. RFC 1321, 1992. Available at: http://www.faqs. org/ rfcs/ rfc1321.html

9 Available at: http://rsa.com/rsalabs/desz

10 J. Niinimaki, J. Forsstron. Approaches for certification of electronic prescription system. International Journal of Medical Informatics, 1997; 47(3): 175-182.

11 J. M. Fu, J. P. Lin, R. C. Wang. Provably secure password-based three-party key exchange protocol with computation efficiency. Life Science Journal, 2011; 8(4):394-401.

12 H. B. Chen, T. H. Chen, W.-B. Lee, C.-C. Chang. Security enhancement for a three-party encrypted key exchange protocol against undetectable on-line password guessing attacks. Computer Standards &Interfaces, 2008; 30(1-2):95-99.

13 H. Y. Chien, T. C. Wu. Provably secure password-based three-party key exchange with optimal message steps. The Computer Journal, 2009; 52(6):646-655.

14 T. F. Lee, J. L. Liu, M. J. Sung, S. B. Yang, C. M. Chen. Communication-efficient three-party protocols for authentication and key agreement. Computers & Mathematics with Applications, 2009; 58(4):641-648.

15 N. W. Lo, K. H. Yeh. Cryptanalysis of two three-party encrypted key exchange protocols. Computer Standards & Interfaces, 2009; 31(6):1167-1174.

16 R. Rivest, A. Shamir, Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communication of the ACM, 1978; 21(2): 120-126.

17 Digital signature standard (DSS, FIPS 186), 1994. Available at: http://www.itl.nist.gov /fipspubs/fip186. htm

18 W. Diffie, M. E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 1976; IT-22 (6): 644-654.

19 P. Blobel, P. Pharow. Experiences with health professional card. Proceedings on an Electronic Health Record Europe'97, London, UK, 1997; 29-39.

20 F. D. Meyer, P. A. Lundgren, G. D. Moor, T. Fiers. Determination of user requirements for the secure communication of electronic medical record information. International Journal of Medical Informatics, 1998; 49(1): 125-130.

21 K. Ohta, T. Okamoto. Multi-signature schemes secure against active insider attacks. IEICE Transactions on Fundamentals, 1999; E82-A(1): 21-31.

22 D. A. Menasce. Security performance. IEEE Internet Computing, 2003; 7(3):. 84-87.

23 H. M. Chao, C. M. Hsu. An Efficient Stream Cipher Using Variable Sizes of Key-Stream. The International Joint Conference on e-Commerce, e-Administration, e-Society, and e-Education, 2007; ISBN 987-986-83038-1-2.

24 Available at: http://www.cacr.math.uwaterloo.ca/hac/about/chap10.pdf

25 T. Zieschang. Combinatorial properties of basic encryption operations. Springer-Veriag, 1998; 14-26.

12/28/2011