A Secure ECC-based Electronic Medical Record System

Kun-Lin Tsai*, Fang-Yie Leu, Tien-Han Wu, Shin-shiuan Chiou, Yu-Wei Liu, and Han-Yun Liu
Tunghai University, Taichung City, Taiwan

Abstract

In recent years, portable devices and wireless communication have been popularly used by people in their everyday lives. In fact, with these facilities, due to their usage convenience and mobility, the instantaneity of inpatient care can be significantly improved. Also, many hospitals utilize cloud systems to store electronic medical records (EMRs). One of the purposes is allowing authorized personnel to access these records anytime and anywhere. Meanwhile, owning to personal privacy, the security of transmitting and accessing these records is one of the critical issues in maintaining and delivering them. In a cryptosystem, when we increase the length of an encryption key, the security level of the protected system will be higher. But the computation time is also lengthened and data transmission performance is then worsened. Compared with a popular cryptosystem, the RSA, under the same security level, Elliptic Curve Cryptography (ECC) requires shorter length of a key than RSA does. That means it is more suitable being used by portable devices to encrypt delivered data. Therefore, in this paper, we propose a secure EMR service system, named the ECC-based Secure EMR System (ESEMR for short) which employs a cloud database, an ECC integration unit, a smart card, and portable devices to provide users with a secure environment for EMR transmission. The ECC integration unit which integrates a 256-bit ECC chip, wireless transceiver, smart card interface, and USB interface for fast computing and reducing the communication load of a portable device can also securely protect the EMRs when they are delivered between the cloud system and the portable device so as to enhance their transmission security and the patient care quality.

Keywords: elliptic curve cryptography, electronic medical record, communication security, cloud database

1 Introduction

In the past decades, communication technology has rapidly progressed. The integration of healthcare, wireless communication and sensing technology has been more popular than before. Currently, a lot of healthcare related systems, such as patient physiological signal recording system [11, 13], homecare system [5, 6], medical imaging system [16, 15], and electronic medical record system [18, 19], have been developed. These systems transmit data through networks so that users can instantly and conveniently access them when necessary. However, due to maintaining patients' privacy and data security, electronic medical records (EMRs for short) need to be securely transmitted through networks. [21, 9] pointed out the challenges of using cloud database to store health information. Medical data are not only simply related to patients' privacy, but also directly affect the accuracy of a physician's diagnoses. To protect EMRs from being divulged in their transmission, a cryptosystem is often required.

Traditional RSA techniques have been successfully applied to many applications [10, 4, 3]. However, the enormous keys and complicated computation usually restrict the possibility of porting them to portable devices. Elliptic Curve Cryptography (ECC for short) proposed by Koblitz and Miller [8, 22] has gradually been accepted by and implemented in cryptosystems. Under the same security level, ECC features a shorter encryption-key length than other cryptosystems do. This feature is more obvious when

Journal of Internet Services and Information Security (JISIS), volume: 4, number: 1, pp. 47-57

*Department of Electrical Engineering, Tunghai University, No. 1727, Sec. 4, Taiwan Blvd., Xitun Dist. Taichung City 407, Taiwan, Tel: +886-4-23590121(ext.33905), Email: kltsai@thu.edu.tw

the security demands of a system increase. In this case, the computational capability of hardware equipments with the ECC encryption function can be fully utilized to enhance the communication security.

The ECC-based cryptosystems have been successfully applied to healthcare systems, such as the internal applications of real-time monitoring and communication of physiological signals [12, 7], medical imaging transmission [14], and electronic medical record delivery [20]. [12] applied ECC to a wireless sensor network (WSN), which adopted Zigbee for healthcare. Such a system senses a patient's physiological data with Zigbee sensors in a ward, and transmits the data to the hospital database, from which the medical personnel can access the patient's information when necessary so as to monitor the patient's health condition in a real time manner. In order to ensure the patient's privacy, the information needed to be encrypted before being transmitted among the database, the sensors and the monitoring end devices. Nevertheless, the processing power of a Zigbee processor is limited. So if RSA is applied to such a processor, the encryption/decryption performance of the WSN may fall short of user's expectation. Therefore, Elliptic Curve Digital Signature Approach (ECDSA) and the central security system were proposed to help the exchange of security keys [12]. [7] provided wireless sensor networks for medical personnel to instantaneously access patients' physiological information through portable devices. When the physiological data of a patient was abnormal, the portable device would send an alert to the user and medical personnel. With group distinction, wireless sensors transmit data to a data collector, which further transmits the data to the managers. The delivery of patients' physiological data is then more quickly and accurately. [14] utilized the Montgomery algorithm and radix-4 Booth algorithm to design a 163-bit ECC structure, which is substituted for the RSA, to process, and medical images store, and then transmit to users with the format of Digital Imaging and Communications in Medicine (DICOM), consequently making the hardware resource usage more efficiently.

Although the security and convenience of data transmission in a hospital have been largely enhanced, the exchange of medical records among hospitals is still time-consuming. In fact, ECC can be used as a part of a security system for encrypting EMRs. In [20], EMRs are marked with Digital Watermarking and ECC is used to encrypt digital pictures/images before they are transmitted. Basically, the images and medical records do not need to be transmitted separately. So before transmission, patients' medical records are concealed in their medical images to improve the security level of the protected system. The computation for encrypting patients' medical records was also largely reduced, but the quality of accessing medical records in a hospital had been remarkably promoted since users could master the patients' physiological data online.

Even though EMRs are feasible under the securely enhanced environment, the required hardware resources also increase because of the increasing demands of future applications. Generally, enormous computation can be performed on servers or personal computers with powerful processors. But it is not easy for portable devices to do this. Different from previously proposed systems which proceeded computation with expensive processors, in this paper, a secure EMR service system, named the ECC-based Secure EMR system (ESEMR for short), is proposed to improve the security level of an EMR system. The ESEMR not only provides its users with higher security than traditional encryption/decryption algorithms do, but also reduces the amount of computation performed on its terminal devices. The latter can significantly prolong a portable device's available time. The ESEMR also provides high mobility so that the medical personnel can effectively access the past or current medical records for transfer and referral for emergent patients everywhere through networks. This is achieved by allowing medical personnel to connect to the ESEMR with their portable devices.

The rest of this paper is organized as follows. Section 2 briefly introduces ECC theory and the applications of the encryption/decryption on finite field Galois GF(2^m). Section 3 presents the applications of the proposed structure, including the cryptosystem and the wireless network. The security analysis is described in Section 4. Section 5 concludes the paper.

Table 1: Comparison of the key lengths for the RSA and ECC given the same security level [2]

Time to break (MIPS years)	RSA/DSA key size (bits)	ECC key size (bits)	RSA/ECC key size ratio
104	512	106	4.8:1
109	768	132	5.8:1
1011	1024	160	6.4:1
1020	2048	210	9.8:1
1079	21000	600	35.0:1

2 Elliptic Curve Cryptography

ECC is composed of the fields operated on an elliptic curve. An elliptic curve in cryptography is a set of points (x, y) that satisfies Eq. (1),

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 \tag{1}$$

where x and y belong to a finite field. The comparison of the key lengths of the RSA and ECC is shown in Table 1 [9], in which the column named Time to break indicates the time required to break the encryption/decryption system with MIPS processors; RSA/DSA key size and ECC key size are, respectively, the key lengths of RSA/DSA and ECC encryption/decryption algorithms. The key size ratio is defined as the ratio of RSA/DSA key size over ECC key size. Apparently, given the same security level, ECC requires shorter key length.

Galois field is a finite field representing the series p^n. Since the eigenvalue used for Galois field on the elliptic curve is 2, Eg. (1) can be simplified to the elliptic equation with eigenvalue=2, and the field named binary finite field is shown in Eq. (2).

$$y^2 + xy = x^3 + ax^2 + b \tag{2}$$

When operating in the finite binary field GF(2^m), the variables x and y and the parameters a and b in Eq. (2) are the elements of GF(2^m), and b$\neq$0. Point addition is widely applied to the ECC structure, and can be defined as Definition 1.

Definition 1:

Let P=(x_P, y_P), Q=(x_Q, y_Q), and R=(x_R, y_R) be the points of an elliptic curve

$$y^2 + xy = x^3 + ax^2 + b$$

and R=P+Q.

If $P \neq Q$,

$$(x_R, y_R) = (\lambda^2 + \lambda + x_P + x_Q + a, \lambda f(x_P + x_R) + x_R + y_P) \tag{3}$$

where λ=(y_Q+y_P)/(x_Q+x_P).

If P=Q,

$$(x_R, y_R) = (\lambda^2 + \lambda + a, x_P^2 + (\lambda + 1)x_R) \tag{4}$$

where λ=x_P+y_P/x_P.

Since encryption/decryption is performed on the points of binary finite field, when the multiplication is beyond the binary finite field, we need to recalculate the remainder with binary finite field polynomials. The elliptic curve equation and a start point G_S are required for encrypting/decrypting with the binary finite field structure. A private key n_x needs to be selected for calculating the public key $Px_x = n_x G_S$ before ciphertext is transmitted.

When wishing to transmit data *Pm* to user B, user A selects a positive random integer k and computes the kG_S value. Next, B's public key *Pxb* is used to compute kPx_b, and the transmitted ciphertext *Cm* is (kG_S, $Pm + kPx_b$). When receiving *Cm*, B calculates ($Pm + kPx_b$)-$n_b(kG_S)$. As Px_b=n_bG_S, B can obtain *Pm*, where *Pm*=($Pm + kPx_b$)-$n_b(kG_S)$=(Pm+$k(n_bG_S)$)-$n_b(kG_S)$.

3 The Proposed System

As shown in Figure 1, the ESEMR consists of an ECC integration unit, a smart card, a terminal device, and a cloud database. The cloud database stores the public keys and the start parameter G_s for hospital personnel and EMRs for patients. The smart card keeps the encryption/decryption key for hospital personnel. An authorized hospital personnel, with either a portable device or a personal computer, inserts his/her smart card into the ECC integration unit, and inputs his/her own key to log in the ECC integration unit. After that, he/she can download the data stored in the cloud database or upload data to the database both through the encryption/decryption circuits provided by the ECC integration unit. The terminal device, either a personal computer or a portable device, is used to input or display patients' medical data.

3.0.1 ECC integration unit

The ECC integration unit as the kernel of the ESEMR is responsible for encrypting/decrypting EMRs. As shown in Figure 1, it comprises an ECC encryption/decryption chip, a smart card reader, USB controller, and wireless transceiver. The relationship among these components is shown in Figure 2. The wireless transceiver is utilized to deliver data in the employed wireless network. In this study, the wireless network module, i.e., Zigbee, which features low power consumption and low costs, is suitable for portable devices to process, receive and transmit data. The USB controller is connected to portable devices through the USB protocol. The reasons for using the USB protocol, rather than Bluetooth or Wi-Fi, are three-fold, 1) providing high-speed data transmission; 2) avoiding exposing plaintext to the wireless network; 3) being able to be connected to most portable electronic products because of its high compatibility. Smart Card Reader takes charge of retrieving user's security parameters, including the user ID, the private key, and the ElGamal digital signature, from the smart card. ECC encryption/decryption chip encrypts the plaintext into a ciphertext, and decrypts the plaintext from the ciphertext.

3.0.2 The encryption/decryption processes

When a user would like to upload a patient's medical records to the cloud database, the ECC integration unit sends a message to the cloud database to request a connection. Then, as shown in Figure 3, the user inputs an EMR, which is the plaintext, denoted by *Pm*, to the ECC integration unit, in which the ECC encryption/decryption chip encrypts Pm with a positive random integer k and the cloud database's public key P_{CD} to generate ciphertext *Cm*. The ECC integration unit retrieves the user's private key n_u from the smart card and generates an ElGamal digital signature. A prime number p and a primitive root g of p are selected, and an integer between 2 and $p-2$ is required for nu to calculate $A \equiv g^{n_u} \pmod{p}$.

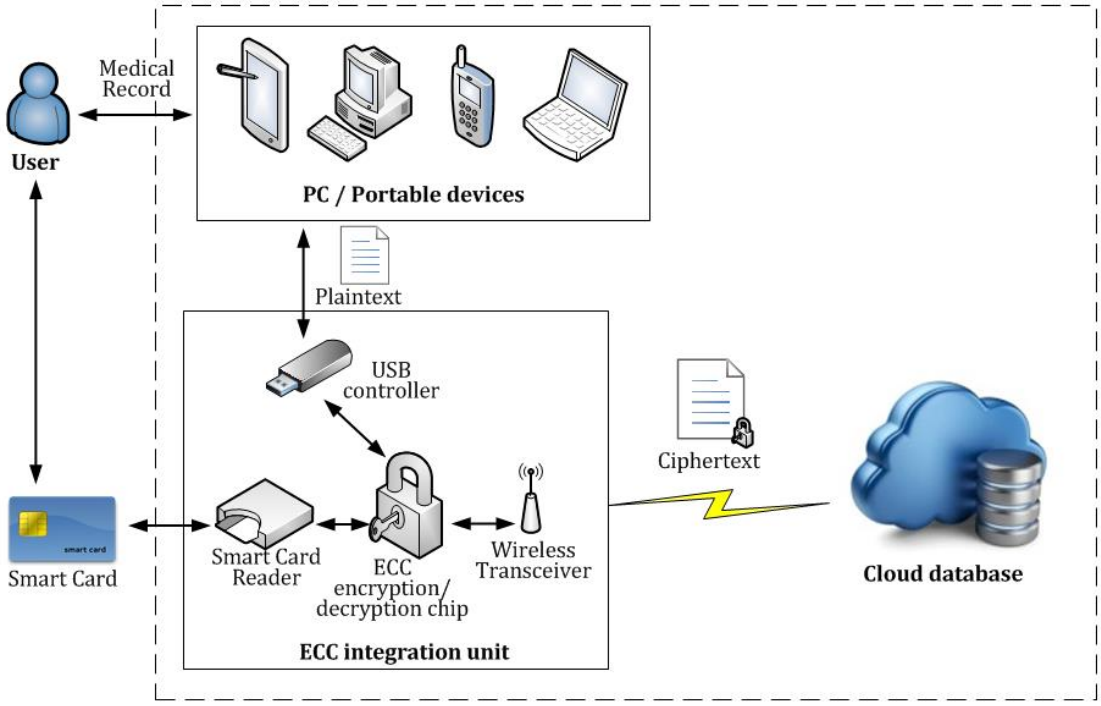

Figure 1: The ESEMR architecture

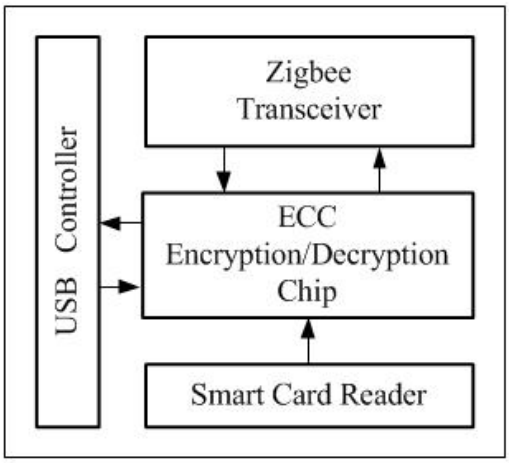

Figure 2: The structure of the ECC integration unit

After publicizing (p, g, A), a positive integer w satisfying gcd(w, p-1)=1 is randomly selected to calculate $r \equiv g^w \pmod{p}$ and $S^* \equiv w^{-1}(Cm - n_u r) \pmod{p-1}$. The signature s=(Cm, r, s^*) is then transmitted to the cloud database. The cloud database compares $V1(\equiv A^r r^{S^*} \pmod{p})$ with V2$(\equiv g^{Cm} \pmod{p})$ to verify the integrity and accuracy of the ElGamal digital signature. If they are identical, indicating that the ElGamal digital signature is verified, the decryption is performed by employing G_S and the key n_{CD} stored in the cloud database, and the plaintext of the medical records is then stored in the database.

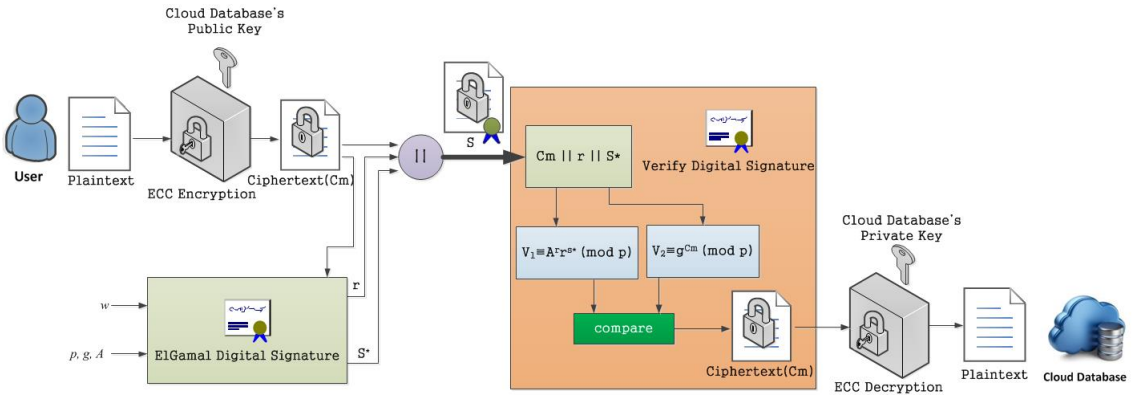

Figure 3: Plaintext encryption flow for uploading data to the cloud database

3.0.3 The EMR upload and download process

The EMR upload process as shown in Figure 4 consists of five steps.

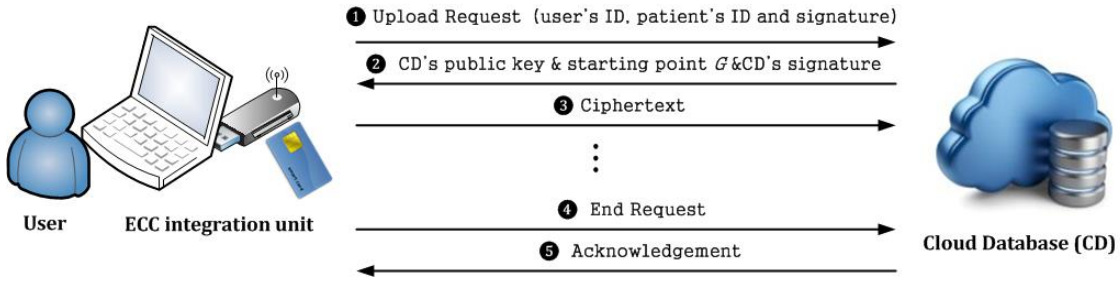

Figure 4: Upload data to the cloud database

1. When the ECC integration unit is connected to the cloud database, a request ($ID_{user} \parallel ID_{patient} \parallel r \parallel s^*$) is first sent to the cloud database, where ID_{user} is the user ID, $ID_{patient}$ is the patient's EMR number, and $r \parallel s^*$ is the ElGamal digital signature of the request.

2. The cloud database transmits $P_{CD} \parallel G_S \parallel r_{CD} \parallel s_{CD}*$ to the ECC integration unit, where P_{CD} is the public key of the cloud database and G_S is the start point of the chosen elliptic curve. Both are retrieved from the cloud database. $r_{CD} \parallel s_{CD}*$ is the ElGamal digital signature of the cloud database.

3. The ECC integration unit stores P_{CD} and G_S in its memory so that it can encrypt the uploaded records with them, and sends the ciphertext with ElGamal digital signature, i.e., $Cm \parallel r \parallel s^*$, to the cloud database.

4. After EMRs are delivered, an End Request, is then sent.

5. On receiving the End Request, the cloud database returns an Acknowledgement.

The process of downloading EMRs from the cloud database as shown in Figure 5 is consisted of four steps.

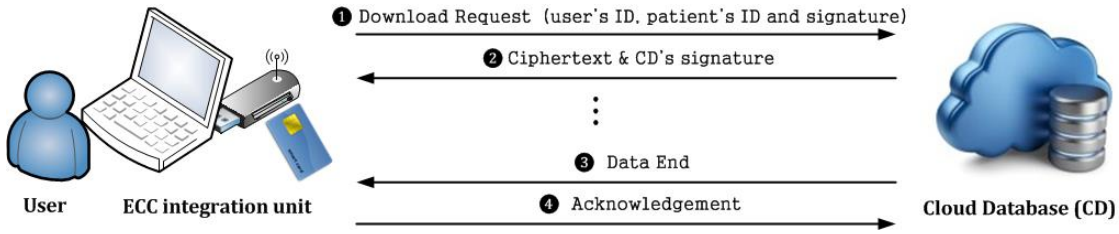

Figure 5: Download data from the cloud database

1. The ECC integration unit sends a Download Request message to the cloud database, including the user ID_{user}, the patient's EMR number $ID_{patient}$, and ElGamal digital signature $r \parallel s^*$. The format of the message is $ID_{user} \parallel ID_{patient} \parallel r \parallel s^*$.

2. The cloud database then verifies the ElGamal digital signature by comparing V1 and V2 mentioned above. When the verification is correct, the requested EMR is encrypted and transmitted to the ECC integration unit accompanied with cloud database's ElGamal digital signature. The format of the medical record is Cm=$(kG_S, Pm + kP_u)$.

3. An end message, a Data End, is further sent after all ciphered EMRs have been transmitted.

4. After receiving the last downloaded EMRs, the user returns an Acknowledgement to the cloud database

After receiving the ciphered medical records, the ECC encryption/decryption chip will retrieve the user key n_a from the smart card to decrypt the records. The plaintext is then transmitted to the user's terminal device through the USB controller. As the ECC integration unit is an outer-connection device, the hardware resources consumed by the portable device (if it is used) for downloading or uploading EMRs are less than that when the download or upload is performed directly on the portable device without employing the ESEMR as the security mechanism. In order to effectively ensure the data security, the EMRs transmitted from the cloud database to the ECC encryption/decryption chip and vice versa are encrypted. When the binary finite field GF(2^{256}) in the ECC structure is 256 bits, the security level is the same as that when the key length of the RSA structure is 3072 bits [1]. As the demands for security increase, the ECC integration unit provides the ECC structure with sufficient expanding space. Since the ECC integration unit is equipped with independent wireless network component, the transmission of EMRs does not occupy the data channel of the portable device. In addition to enhancing the transmission speed, the channel for EMR transmission is also securely protected.

4 The Security Analysis

In the following, we analyze the security of the ESEMR.

In the ElGamal digital signature process, the user chooses a random number w for $S^* \equiv w^{-1}(Cm - n_u r) \pmod{p-1}$. When the user signs two plaintexts with the same w, the hacker can use $S^* \equiv w^{-1}(Cm - n_u r) \pmod{p-1}$ to solve the simultaneous equations and then acquire the user's private key n_u. Thus, the number w, which is randomly generated by ECC integration unit, cannot be duplicated.

In the ECC encryption process, different messages are encrypted by using different encryption points of an elliptic curve. When the hacker grabs two or more encrypted messages, he/she still cannot obtain the user's private key n_u, the elliptic curve equation, and the start point G_S by solving the simultaneous equations.

A general attack method for ECC encryption system is Pollard Rho algorithm [17]. The time complexity of the Pollard Rho algorithm is $O(2^{n/2})$, where n is the key length of ECC encryption system. As mentioned above, in the ESEMR, the 256-bit key length is used for encryption, and the computing complexity for breaking ECC encryption system by using Pollard Rho algorithm is $O(2^{128})$.

Each user has his/her own ID_{user} and private key n_u, which are stored in his/her smart card. A hacker who has illegal ID_{user} or unavailable private key cannot generate valid ElGamal digital signature, and thus is unable to be successfully verified by the cloud database before accessing the patients' data. In fact, the user's ID_{user} and private key can be further protected by using modern smart card encoding scheme. If an eligible user A masquerades another eligible user B to login the system, and requires downloading patients' data, the cloud database encrypts the data with user B's public key, and deliver the ciphertext to user A. Since user B's private key is protected in his/her smart card, user A cannot decrypt the message. Therefore, the proposed ESEMR can resist insider attacks.

Our scheme is based on ECC encryption/decryption mechanism, and the cloud database has no need to store the password or a verification table. That is, the cloud database only maintains the secret parameters, and does not need a password table. Thus, the proposed ESEMR can resist the stolen-verifier attack and modification attack.

The authentication scheme is based on ECC and provides the proper mutual authentication between the user and the cloud database. In the first step of upload/download data to/from cloud database, the user's signature can be verified by computing V1 and V2, which are described in section 3.2. Then, in the second step, the cloud database's signature can also be verified by user in the same way.

5 Conclusion

To rapidly and securely transmit the health information in a wireless network, the ESEMR, which utilizes the ECC security scheme to effectively encrypt EMRs, is proposed. It contains an ECC encryption/decryption chip, a Zigbee wireless network, a smart card reader, and a USB controller for users to access to the data stored in the cloud database through smart cards and the ECC integration unit. The high security provided and the less hardware resources consumed by the ECC enable the proposed system to be adopted by various platforms, not only ensuring the security, but also providing the convenience of cloud EMR exchange. Most recent EMR exchange systems focus on the security for both EMRs access and medical information exchange. When the demands for security increase, the enormous amount of computation for encryption/decryption would consume many more hardware resources. Compared with the previous research results, the proposed system, offering the security with outer-connection facility without consuming the hardware resources of the portable device, allows the facility to share its hardware resources to process other requested tasks, rather than just reserving its computation capabilities to the mentioned security issues.

References

[1] Recommendation on Key Management. NIST, DRAFT Special Publication 800–57, January 2003. `http://csrc.nist.gov/CryptoToolkit/kms/guideline-1-Jan03.pdf`.

[2] T. Abdurahmonov, E.-T. Yeoh, and H. M. Hussain. The implementation of elliptic curve binary finite field ($f(2^m)$) for the global smart card. In *Proc. of the 2010 IEEE Student Conference on Research and Development (SCOReD'10), Putrajaya, Malaysia*, pages 169–173. IEEE, December 2010.

[3] D. Caliskan. An application of rsa in data transfer. In *Proc. of the 5th International Conference on Application of Information and Communication Technologies (AICT'11), Baku, Azerbaijan*, pages 1–4. IEEE, October 2011.

[4] Z. Cao and L. Liu. A strong rsa signature scheme and its application. In *Proc. of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'07), Qingdao, China*, pages 111–115. IEEE, July 2007.

[5] S. T. Carvalho, L. Murta, and O. Loques. Variabilities as first-class elements in product line architectures of homecare systems. In *Proc. of the 4th International Workshop on Software Engineering in Health Care (SEHC'12), Zurich, Switzerland*, pages 33–39. IEEE, June 2012.

[6] Y.-G. Ha and Y.-C. Byun. A ubiquitous homecare service system using a wearable user interface device. In *Proc. of the 11th IEEE/ACIS 11th International Conference on Computer and Information Science (ICIS'12), Shanghai, China*, pages 649–650. IEEE, May 2012.

[7] T.-C. Hsiao, Y.-T. Liao, J.-Y. Huang, T.-S. Chen, and G.-B. Horng. An authentication scheme to healthcare security under wireless sensor networks. *Journal of Medical Systems*, 36(6):3649–2664, March 2012.

[8] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(77):203–209, January 1987.

[9] Z.-R. Li, E.-C. Chang, K.-H. Huang, and F. Lai. A secure electronic medical record sharing mechanism in the cloud computing platform. In *Proc. of the 15th International Symposium on Consumer Electronics (ISCE'11), Singapore*, pages 98–103. IEEE, June 2011.

[10] D. liang Liu, Y. ping Chen, and H. ping Zhang. Secure applications of rsa system in the electronic commerce. In *Proc. of the 2010 International Conference on Future Information Technology and Management Engineering (FITME'10), Changzhou, China*, pages 86–89. IEEE, October 2010.

[11] Y.-H. Lin, I.-C. Jan, P. C.-I. Ko, Y.-Y. Chen, J.-M. Wong, and G.-J. Jan. A wireless pda-based physiological monitoring system for patient transport. *IEEE Transactions on Information Technology in Biomedicine*, 8(4):439–447, December 2004.

[12] J. Misic. Enforcing patient privacy in healthcare wsns using ecc implemented on 802.15.4 beacon enabled clusters. In *Proc. of the 6th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'08), Hong Kong, China*, pages 686–691. IEEE, March 2008.

[13] A. Pantelopoulos and N. G. Bourbakis. A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, 40(1):1–12, January 2010.

[14] J. Park, J.-T. Hwang, and Y.-C. Kim. Fpga and asic implementation of ecc processor for security on medical embedded system. In *Proc. of the 2005 International Conference on Information Technology and Applications (ICITA'05), Sydney, Australia*, pages 547–551. IEEE, July 2005.

[15] P. Suapang, K. Dejhan, and S. Yimmun. Medical image archiving, processing, analysis and communication system for teleradiology. In *Proc. of the 2010 IEEE Region 10 Conference (TENCON'10), Fukuoka, Japan*, pages 339–345. IEEE, November 2010.

[16] P. Suapang, S. Yimmun, and A. Puditkanawat. Web-based medical image archiving and communication system for teleimaging. In *Proc. of the 12th International Conference on Control, Automation and Systems (ICCAS'11), Gyeonggi-do, Korea*, pages 172–177. IEEE, October 2011.

[17] P. C. van Oorschot and M. J. Wiener. Parallel collision search with cryptanalytic applications. *Mathematics of Computation*, 12(1):1–28, January 1999.

[18] Y. Wan and W. Perry. Lessons from method: A successful electronic medical record (emr) system implementation. In *Proc. of the 2011 IEEE International Conference on Intelligence and Security Informatics (ISI'11), Beijing, China*, pages 248–251. IEEE, July 2011.

[19] Y. Wu and H. Yang. An electronic medical records review system for mobile healthcare based on web services. In *Proc. of the 5th International Conference on Biomedical Engineering and Informatics (BMEI'12), Chongqing, China*, pages 1040–1044. IEEE, October 2012.

[20] Y. Zaz and L. E. Fadil. Enhanced epr data protection using cryptography and digital watermarking. In *Proc. of the 2011 International Conference on Multimedia Computing and Systems (ICMCS'11), Ouarzazate, Morocco*, pages 1–5. IEEE, April 2011.

[21] R. Zhang and L. Liu. Security models and requirements for healthcare application clouds. cloud computing. In *Proc. of the 3rd IEEE International Conference on Cloud Computing (CLOUD'10), Miami, Florida, USA*, pages 268–275. IEEE, July 2010.

[22] C. V. Zhou, C. Leckie, and S. Karunasekera. Use of elliptic curves in cryptography. In *Proc. of the 5th*

International Cryptology Conference (CRYPTO'85), Santa Barbara, California, USA, LNCS, volume 218, pages 417–426. Springer-Verlag, August 1986.

Author Biography

Kun-Lin Tsai received the B.S. degree in Computer and Information Science from Tunghai University, Taichung, Taiwan, R.O.C. in 1999, and the M.S. degree in computer science and information engineering from National Taiwan University, Taipei, Taiwan, R.O.C. in 2001, and the Ph.D. degree in Electrical Engineering from National Taiwan University in 2006. He was a postdoc of National Taiwan University of Science and Technology in 2007. He is currently an assistant professor at Department of Electrical Engineering of Tunghai University. He is the member of IEEE, IEICE, and IICM. He is also the editor in chief of IICM communication. His research interests include low power system design, smart home system, and SoC.

Fang-Yie Leu received his B.S., M.S. and Ph.D. degrees from National Taiwan University of Science and Technology, Taiwan, in 1983, 1986 and 1991, respectively, and another M.S. degree from Knowledge Systems Institute, USA, in 1990. His research interests include wireless communication, network security, Grid applications and Chinese natural language processing. He is currently a professor of Tunghai University, Taiwan, the director of database and network security laboratory of the University, the workshop chair of MCNCS and CWECS workshops, and the editorial board member of several international journals. He is also a member of IEEE Computer Society.

Tien-Han Wu received the Bachelor of Engineering degree in electrical engineering from Tunghai University, Taichung, Taiwan, in 2013. He is currently a graduate student at Department of Electrical Engineering of National Taiwan University. His research interests include cryptography, digital signature, and wireless security.

Shin-Shiuan Chiou received the Bachelor of Engineering degree in electrical engineering from Tunghai University, Taichung, Taiwan, in 2013. She is currently a graduate student at Department of Law for Science and Technology of National Tsing Hua University. Her main research interests include info-communications law, and energy law.

Yu-Wei Liu is currently a undergraduate student at Department of Electrical Engineering of Tunghai University. His research interests include cryptography, wireless security, and wireless communication.

Han-Yun Liu is currently a undergraduate student at Department of Electrical Engineering of Tunghai University. His research interests include cryptography, wireless security, and wireless communication.