International Journal of Smart Home
Vol.7, No.5 (2013), pp.165-172
http://dx.doi.org/10.14257/ijsh.2013.7.5.17

Adapting a Novel Dual Authentication Method based on Smart Cards

Jeung-Seop Kim[1], Jong-Il Kim[2], Chang-Jin Seo* and Yong-Seok Jang[3]

[1]A2Tec Co., LTD. Yutongdanji-ro 24-gil, Buk-gu, Daegu, Korea
[2]A2Tec Co., LTD. Yutongdanji-ro 24-gil, Buk-gu, Daegu, Korea
*(Corresponding Author)
Department of Information and Telecommunications, SangMyung University, 300, Anseo-dong DongNam-gu, Cheon-An, ChungNam, Korea
[3]Daooldns Co., LTD. 1691, SanGyuk-Dong, Buk-gu, DaeGu, Korea
[1]jskim@a2tec.co.kr, [2]jikim@a2tec.co.kr,
**cjseo@smu.ac.kr, [3]ysjang@daooldns.co.kr*

Abstract

In this paper, adapting a novel dual authentication method based on smart cards in public networks is proposed. This method uses the ElGamal public key cryptosystem and extend Chaum–van Antwerpen's scheme to authenticate a signature between the signer and verifier using a dual protocol with a smart card that has tamper-resistant features. We propose the method to change the verification and disavowal protocol in Chaum–van Antwerpen's scheme to authenticate both the signer and verifier. With these modifications, attempts to reject or deny a valid signature between the signer and verifier can be prevented or detected with high efficiency

Keywords: *smart cards, public key cryptosystem, security*

1. Introduction

A digital signature must be verifiable in cases when a dispute arises as to whether a party signed a document, which is caused by either a signer trying to repudiate a valid signature or a fraudulent claimant. In either circumstance, an impartial third party should be able to resolve the matter equitably without the signer's secret information or private key. A digital signature is a number that is dependent on secret information known only to the signer, such as a signer's secret key, and is added on the document to be signed[1].

A digital signature scheme consists of signing and verification steps. A signer adds his signature, and a verifier checks the received signature. In this process, attacks may involve analyzing the algorithm or a weak point in the protocol. These attacks can be resolved by using more a secure crypto algorithm. However, it is more difficult to identify instances involving a signer's intentional denial or repudiation of a valid signature and a verifier's intentional denial of a received true signature.

To resolve the signer's repudiation or denial problem, Chaum and van Antwerpen introduced an undeniable signature scheme, which consists of a signing algorithm and verification and disavowal protocols[1-4]. In this scheme, signers cannot repudiate or deny a valid signature because they have participated in the verification of their signatures. However, there is a small probability that an invalid signature will be accepted as a valid signature or that a denial of a valid signature is computationally possible[11].

We propose a new undeniable signature scheme using a dual authentication protocol based

ISSN: 1975-4094 IJSH

on Chaum–van Antwerpen's scheme[12]. We modify the verification and disavowal protocols to make our scheme more reliable. We resolve the signer's intentional denial or repudiation of a valid signature and the verifier's intentional denial of a received true signature. Of course, our scheme is still based on computation, so accepting a wrong signature as valid or denial of a valid signature is still possible, but there is a smaller probability of this occurring.

The rest of this paper is organized as follows. Assumptions and notations related to our scheme are shown in Section 2, and we present our new scheme in Section 3. Then, we explain and analyze our scheme in Section 4. Finally, the conclusion is presented in Section 5.

2. Assumptions and Notations

In this paper, ***S*** denotes a signer, ***V*** is a verifier, and ***ADV*** is an adversary. Let $p = (2q + 1)$ be a random prime number such that q is a prime number. The discrete logarithm problem in $\boldsymbol{Z_p}$ is assumed to be computationally infeasible [5-7, 13]. α, which belongs to $\boldsymbol{Z_p}^*$, is an element of order q. Let $1 \le a$, $b \le (q - 1)$, $\beta = \alpha^a \bmod p$, and $\beta' = \alpha'^b \bmod p$, where a is ***S***' secret value and b is ***V***'s secret value. ***ID*** indicates identification information, which can consist of ***S***' secret and unique information from ***S***' smart card. $\boldsymbol{S_k}$ is a secret key maintained by ***V***'s system. We assume that a pseudo random number generator (PRNG) exists and is available in both ***S***' smart card and ***V***'s system. $\boldsymbol{A} \rightarrow \boldsymbol{B} : \boldsymbol{M}$ means that ***A*** sends message ***M*** to ***B***, and all data transmission is secure. Smart cards are tamper-resistant, and no one can obtain the content of smart cards unethically [8, 9, 14].

3. Proposed Undeniable Signature Scheme Using a Dual Authentication Protocol with Smart Cards

In our scheme, p, α, β, α', β', and public elements are publicly known to ***S*** and ***V*** who participate in our scheme. Our scheme consists of four processes: registration, signing, verification, and disavowal. In these processes, the verification and disavowal process are very important, so our scheme must prevent ***S*** from denying a valid signature and ***V*** from accepting forgery as a valid signature. It must also prevent ***V*** from denying that it received ***S***' true signature signed by using these two processes. The following is a detailed description of all four processes in our scheme, beginning with registration and ending with disavowal.

Registration Process: To register ***S***' smart card, ***S*** must submit its ***ID*** to ***V***'s system. Then, ***V***'s system receives the registration data ***REG*** for ***S***, as shown in Figure 1.

$$REG = (ID)^{S_k} \bmod p$$

Figure 1. Registration Algorithm

V sends REG to S in a secure manner. REG data is stored on both V's system and S' smart card and is used to authenticate the cardholder. This registration process can be done when S' smart card is issued by V.

Signing process: Our signing algorithm is similar to the signing algorithm in Chaum–van Antwerpen's scheme. In this process, it is important that a digital signature is generated inside S' smart card. Further, all public elements needed for this process are stored on S' smart card and in V's system. The signing process is performed as shown in Figure 2.

1. ***S*** calculates $y = x^a \bmod p$, where x is a message to be signed.
2. ***S*** generates r_s, where $r_s \in \boldsymbol{G}$ is a random number, timer, or nonce that is chosen by ***S***.
3. $\boldsymbol{S} \rightarrow \boldsymbol{V}$:$(x, y, r_s)$

Figure 2. Signing Algorithm

In Figure 2, we add procedure 2 to the signing algorithm of Chaum–van Antwerpen's scheme. S' random number rs is the value used to check that the verifier received the true signature exactly.

Verification Process: This process is similar to the verification protocol in Chaum–van Antwerpen's scheme, which is done with S' cooperation. However, our scheme bi-directionally authenticates S and V as well as V and S. This process differentiates our scheme from Chaum–van Antwerpen and Lee's schemes [10, 15]. The verification process is performed as shown in Figure 3.

1. ***V*** calculates $w = (r_s)^b \bmod p$, $u = \boldsymbol{f}(r_s, \boldsymbol{REG}) \bmod (p - 1)$, and $y' = x'^b \bmod p$.
2. ***V*** generates r_v, where $r_v \in \boldsymbol{G}$ is a random number, timer, or nonce that is chosen by ***V***.
3. $\boldsymbol{V} \rightarrow \boldsymbol{S}$:$(w, u, r_v, x', y')$.

---

4. ***S*** tests whether the received u is a valid value. If u is a valid value, ***S*** continues the verification process.
5. ***S*** calculates $z = (r_v)^a \bmod p$, $t = \boldsymbol{f}(r_v, \boldsymbol{REG}) \bmod (p - 1)$, $g = wy'^{l'}\beta'^{m'} \bmod p$, where l' and m' are random numbers in $\boldsymbol{Z}_q^*$ and are selected by ***S***.
6. $\boldsymbol{S} \rightarrow \boldsymbol{V}$:$(z, t, g)$
7. ***V*** tests whether the received t is a valid value. If t is a valid value, ***V*** continues the verification process.
8. ***V*** calculates $c = zy^l\beta^m \bmod p$, where l and m are random numbers in $\boldsymbol{Z}_q^*$ and are selected by ***V***, and $h = (g^{k'} \bmod p)$, where $k' = b^{-1} \bmod q$.
9. $\boldsymbol{V} \rightarrow \boldsymbol{S}$:$(c, h)$
10. ***S*** authenticates ***V*** as a true verifier, if and only if $h \equiv r_s x'^{l'} \alpha'^{m'} \pmod{p}$.
11. ***S*** calculates $d = (c^k \bmod p)$, where $k = a^{-1} \bmod q$.
12. $\boldsymbol{S} \rightarrow \boldsymbol{V}$:$(d)$
13. ***V*** verifies y as a valid signature if and only if $d \equiv r_v x^l \alpha^m \pmod{p}$.

Figure 3. Verification Algorithm

In Figure 3, ***f*** is a one-way function that is known to ***S*** and ***V***. We modified Chaum–van Antwerpen's scheme to authenticate both ***S*** and ***V*** dually. We use two values, *w* for the validation of ***V*** and *u* for verifying ***V***'s cooperation, and additional two values, *t* for the validation of ***S*** and *z* for verifying ***S***' cooperation over his/her signature.

Disavowal Process: This process is essential to our scheme because ***S*** can settle ***V***'s denial of the reception of the true signature and ***V*** can settle ***S***' denial of his/her valid signature. In our scheme, ***S*** and ***V*** dually verify ***V*** and ***S***' denial. The disavowal process is performed as shown in Figure 4.

17. ***V*** calculates $w = (r_s)^b \bmod p$, $u = \boldsymbol{f}(r_s, \boldsymbol{REG}) \bmod (p - 1)$, and $y' = x'^{b} \bmod p$.
18. ***V*** generates r_v, where $r_v \in \boldsymbol{G}$ is a random number, timer, or nonce that is chosen by ***V***.
19. $\boldsymbol{V} \rightarrow \boldsymbol{S}:(w, u, r_v, x', y')$

1. ***S*** tests whether the received *u* is a valid value. If *u* is a valid value, ***S*** continues the verification process.
2. ***S*** calculates $z = (r_v)^a \bmod p$, $t = \boldsymbol{f}(r_v, \boldsymbol{REG}) \bmod (p - 1)$, $g = w\, y'^{l'} \beta'^{m'} \bmod p$, where l' and m' are random numbers in $\boldsymbol{Z}_q^*$ and are selected by ***S***.
3. $\boldsymbol{S} \rightarrow \boldsymbol{V}:(z, t, g)$
4. ***V*** tests whether the received *t* is a valid value. If *t* is a valid value, ***V*** continues the verification process.
5. ***V*** calculates $c = zy^l\beta^m \bmod p$, where *l* and *m* are random numbers in $\boldsymbol{Z}_q^*$ and are selected by ***V***, and $h = (g^{k'} \bmod p)$, where $k' = b^{-1} \bmod q$.
6. $\boldsymbol{V} \rightarrow \boldsymbol{S}:(c, h)$
7. ***S*** verifies that *h* is not congruent to $r_s\, x'^{l'} \alpha'^{m'}$ (mod *p*).
8. ***S*** calculates $d = (c^k \bmod p)$, where $k = a^{-1} \bmod q$, and $G = w\, y'^{n'} \beta'^{e'} \bmod p$, where n' and e' are random numbers in $\boldsymbol{Z}_q^*$ and are selected by ***S***.
9. $\boldsymbol{S} \rightarrow \boldsymbol{V}:(d, G)$
10. ***V*** verifies that *d* is not congruent to $r_v x^l \alpha^m$ (mod *p*).
11. ***V*** calculates $H = G^{k'} \bmod p$, $k' = b^{-1} \bmod q$, and $C = zy^n\beta^e \bmod p$, where *n* and *e* are random numbers in $\boldsymbol{Z}_q^*$ and are selected by ***V***.
12. $\boldsymbol{V} \rightarrow \boldsymbol{S}:(H, C)$
13. ***S*** calculates $D = (C^k \bmod p)$, where $k = a^{-1} \bmod q$.
14. ***S*** verifies that *H* is not congruent to $r_s\, x'^{n'} \alpha'^{e'}$ (mod *p*). Therefore, ***S*** concludes that ***V*** is a false verifier if and only if
$$(h\alpha^{-m'} / r_s)^{n'} \equiv (H\alpha^{-e'} / r_s)^{l'} \bmod p.$$
15. $\boldsymbol{S} \rightarrow \boldsymbol{V}:(D)$
16. ***V*** verifies that *D* is not congruent to $r_v x^n \alpha^e$ (mod *p*). Therefore, ***V*** concludes that *y* is a forgery if and only if
$$(d\,\alpha^{-m} / r_v)^n \equiv (D\alpha^{-e} / r_v)^l \bmod p.$$

Figure 4. Disavowal Algorithm

In Figure 4, f is a one-way function that is known to S and V, as in the verification process. In the disavowal algorithm, if one of the tests in stage 10 or 17 fails, S cannot credit V, and if one of the tests in stage 13 or 20 fails, V cannot verify y as S' valid signature. Moreover, if we analyze the results of the tests at stage 17 or 20, we can see that two different values were used.

4. Security Analysis

An undeniable signature scheme must prevent forgeries of ***S***' signature and resolve ***S***' attempt to deny a valid signature. Further, this scheme must also prevent ***V*** from denying the reception of ***S***' true signature. Our scheme performs these two basic functions, and is based on the discrete logarithm problem. However, computing the discrete logarithm over finite fields is very difficult and complex. Therefore, is very difficult for ***ADV*** to compute *a* from the equation $y = x^a \bmod p$ or $\beta = \alpha^a \bmod p$, and to compute *b* from the equation $y' = x'^b \bmod p$ or $\beta' = \alpha'^b \bmod p$ [5, 6, 7, 16].

However, even though ***ADV*** still cannot make ***S***' valid signature, our scheme is inherently vulnerable to accepting an invalid signature as a valid one. That is, there is a very small probability that ***V*** may accept *Y* as a valid signature for message *x*, where $Y \neq x^a \bmod p$. The same problem is also inherent in Chaum–van Antwerpen's scheme with probability $1/q$[2].

In our scheme, the signing algorithm does not differ from that in Chaum–van Antwerpen's scheme. Accordingly, our scheme might still regard an invalid signature as a valid one. Figure 5 shows a detailed description of the probability of accepting a fraudulent signature as a valid one.

First, each possible challenge *g* and *c* in the verification and disavowal processes corresponds to exactly *q* ordered pairs (r_s, l', m') and (r_v, l, m), respectively. This is because y', β', y, and β are elements of the multiplicative group ***G*** of the prime order *q*.

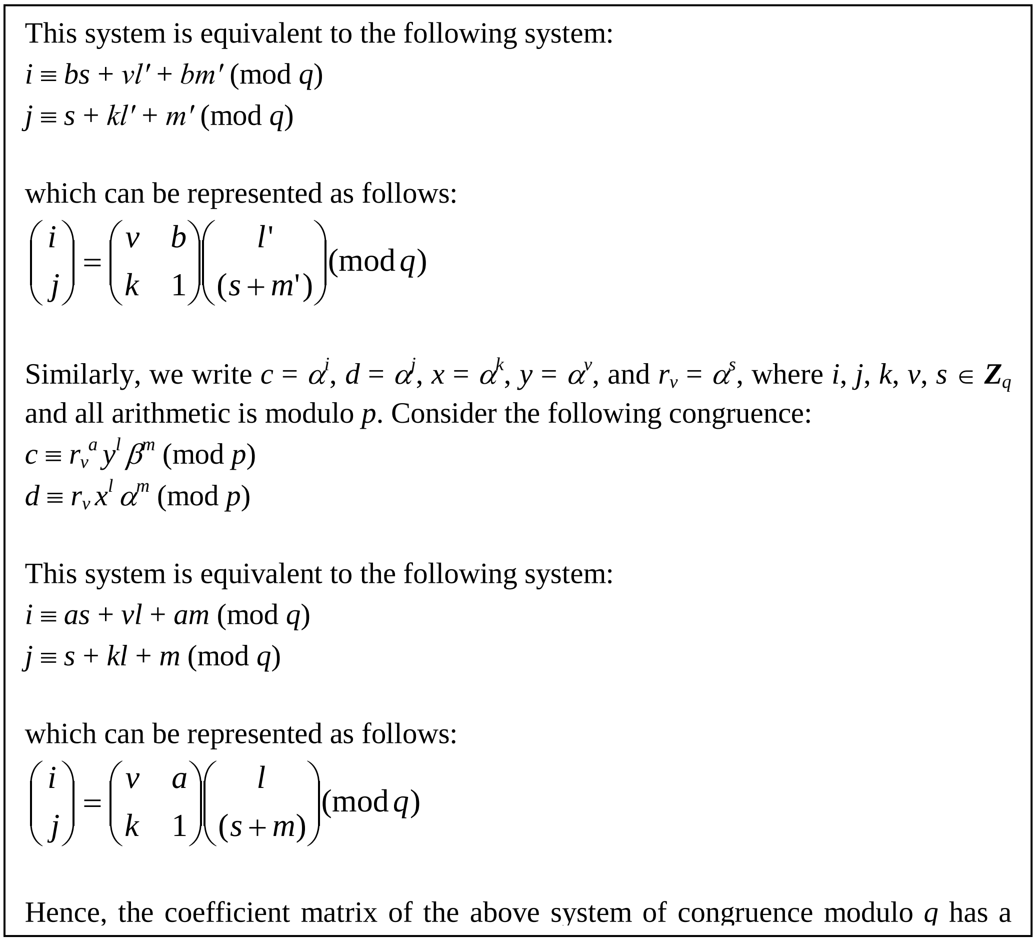
Second, ***V*** receives challenge *g* and has no way of knowing which of the *q* possible ordered pairs (r_s, l', m') is used to construct challenge *g*. Similarly, ***S*** receives challenge *c* and has no way of knowing which of the *q* possible ordered pairs (r_v, l, m) is used to construct challenge *c*.

Third, suppose that y' is not congruent to x'^b (mod *p*), β' is not congruent to α'^b (mod *p*), *y* is not congruent to x^a (mod *p*), and β is not congruent to α^a (mod *p*). Then, any possible response $d \in \boldsymbol{G}$ that ***V*** or ***S*** might give is consistent with exactly one of the *q* possible ordered pairs (r_s, l', m') or (r_v, l, m).

Because α' generates ***G***, any element of ***G*** has a power of α', where the exponent is defined uniquely modulo *q*. Thus, we write $g = \alpha'^i$, $h = \alpha'^j$, $x' = \alpha'^k$, $y' = \alpha'^v$, and $r_s = \alpha'^s$, where $i, j, k, v, s \in \boldsymbol{Z}_q$ and all arithmetic is modulo *p*. Consider the following congruence:

$$g \equiv {r_s}^b y'^{l'} \beta'^{m'} \pmod p$$

$$h \equiv r_s x'^{l'} \alpha'^{m'} \pmod p$$



This system is equivalent to the following system:
$i \equiv bs + vl' + bm'$ (mod q)
$j \equiv s + kl' + m'$ (mod q)

which can be represented as follows:

$$\begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} v & b \\ k & 1 \end{pmatrix} \begin{pmatrix} l' \\ (s+m') \end{pmatrix} (\mathrm{mod}\, q)$$

Similarly, we write $c = \alpha^i$, $d = \alpha^j$, $x = \alpha^k$, $y = \alpha^v$, and $r_v = \alpha^s$, where $i, j, k, v, s \in \boldsymbol{Z}_q$ and all arithmetic is modulo p. Consider the following congruence:
$c \equiv {r_v}^a y^l \beta^m$ (mod p)
$d \equiv r_v x^l \alpha^m$ (mod p)

This system is equivalent to the following system:
$i \equiv as + vl + am$ (mod q)
$j \equiv s + kl + m$ (mod q)

which can be represented as follows:

$$\begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} v & a \\ k & 1 \end{pmatrix} \begin{pmatrix} l \\ (s+m) \end{pmatrix} (\mathrm{mod}\, q)$$

Hence, the coefficient matrix of the above system of congruence modulo q has a

Figure 5. Probability of Accepting a Fraudulent Signature as Valid and a False Verifier as a True One

As shown in Figure 5, the probability of accepting a fraudulent signature as valid is not improved. However, our scheme uses the s value prior to the verification or disavowal processes; however, the s value is infeasible to calculate because of the dependency on solving the discrete logarithm problem. If ***ADV*** obtains the value of (s + m') or (s + m), the complexity of deciding each value is dependent on the size of q. Therefore, we can say that our scheme is more secure and reliable than Chaum–van Antwerpen's scheme, not computationally but logically. In other words, our scheme is more secure and reliable because of the dependency on the pair of three challenges: s, l, m or s, l', m'. Further, our scheme is an improvement over Lee's scheme [10, 17, 18], which uses only one-way authentication and only one pair of three random numbers. Moreover, ***S***' smart card is tamper-resistant, so ***ADV*** cannot obtain ***REG*** or other information from ***S***' smart card unethically. Therefore, ***S*** or ***V***, who passes the verification or disavowal protocols, can hardly deny or repudiate a valid signature or deny the opposite credit.

5. Conclusion

We presented a new undeniable signature scheme, which is based on Chaum–van Antwerpen's scheme, using a dual authentication protocol with smart cards. Our scheme relies on the difficulty of computing discrete logarithm problems over finite fields, two pairs with three random challenges, and the tamper resistance of smart cards.

In Chaum–van Antwerpen's scheme, two random numbers are used when signers verify their signatures. However, there is a very small probability that an invalid signature might be accepted as a valid one. Lee's scheme uses three random numbers to lower the probability of errors. This additional random number is used to authenticate the signer's signature and check whether the signer is a legitimate user of the verifier's system. However, Lee's scheme authenticates only the signature received, so it does not know whether the verifier is a true verifier. Our scheme uses two pairs, each having three random numbers to bi-directionally authenticate both the signer and verifier. Further, our scheme uses the same transaction protocol states as Lee's scheme. Therefore, our scheme is more reliable and secure without loss of generality.

Acknowledgement

This work was supported by the SangMyung University Research Grants in 2013.

References

[1] Alfred J. Menezes, Handbook of Applied Cryptography, CRC Press**(1977)**

[2] Douglas R. Stinson, Cryptography Theory and Practice, CRC Press**(1995)**

[3] Bruce Schneier, Applied Cryptography. 2nd edition, John Wiley & Sons, Inc, ISBN:0471117099 **(1996)**

[4] D.Chaum, Undeniable signatures, Lecture Notes in Computer Science, Vol. 435. Pp. 212-216, DOI : 10.1007/0-387-34805-0_20 **(1990)**

[5] Leveque W., Elementary Theory of Numbers, Dover**(1990)**

[6] H.E. Rose, A course in number theory, Clarendon Press, ISBN:0198532628 **(1988)**

[7] M.R. Schroeder, Number theory in science and communication 2nd edition, Springer-Verlag**(1985)**

[8] W.Effing, Smart Card Handbook 2nd edition, John & Wiley Sons Inc, ISBN:0471988758 **(2000)**

[9] Zoreda, Jose Luis, Smart Cards, Artech House Inc, ISBN:0890066876 **(1994)**

[10] Lee Jongkook, A New Undeniable Signature Scheme Using Smart Cards, Lecture Notes in Computer Science, Vol. 1281. DOI : 10.1007/3-540-45325-3_36, Springer-Verlag, UK**(2001)**

[11] Sang-Soo Yeo, Sang-Jo Youk, Gil-cheol Park, Seok-soo Kim and Tai-hoon Kim, Physical Threat Description of Smart Card Protection Profile in Security Level 1st, IJSIA Vol. 1, No.2, pp. 99-104, http://www.sersc.org/journals/IJSIA/vol1_no2_2007/IJSIA-2007-01-02-10.pdf , October**(2007)**

[12] Chun-Li Lin, Ching-Po Hung, Cryptanalysis and Improvement on Lee-Chen's One-Time Password Authentication Scheme, IJSIA Vol. 2, No.2, pp. 1-8, http://www.sersc.org/journals/IJSIA/vol2_no2_2008/1.pdf, April**(2008)**

[13] Ludovic Piètre-Cambacédès, Pascal Sitbon, Cryptographic Key Management for SCADA Systems, Issues and Perspectives, IJSIA Vol. 2, No.3, pp. 31-40, http://www.sersc.org/journals/IJSIA/vol2 _no3_2008/4.pdf, July**(2008)**

[14] C. H. Wei and Y. H. Chin, Cryptanalysis of an efficient and secure event signature protocol for peer-to-peer massively multiplayer online games, IJSIA Vol. 3, No.3, pp. 1-8, http://www.sersc.org/journals/IJSIA/vol3_no3_2009/1.pdf , July**(2009)**

[15] Guoyan Zhang and Qiuliang Xu, Secret Key Awareness Security Public Key Encryption Scheme, IJSIA Vol. 5, No.4, pp. 49-58, http://www.sersc.org/journals/IJSIA/vol5_no4_2011/5.pdf, October **(2011)**

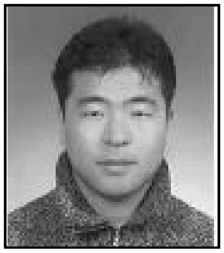
[16] KH. Lee, JH Park, Anonymity Certification Technique of a Smart Card base for Personal Information Protection, Journal of Korea Academia-Industrial Cooperation Society, vol. 13, no. 12, pp. 6071-6080, DOI: 10.5762/KAIS.2012.13.12.6071**(2012)**

[17] SS. Shin, KH. Han, Cryptanalysis and Enhancement of the An's Remote User Authentication Scheme using the Smart Cards, , Journal of Korea Academia-Industrial Cooperation Society, vol. 12, no. 10, pp. 4612-4617, DOI : 10.5762/KAIS.2011.12.10.4612 **(2011)**

[18] WC. Lee, JH Song, A Study on the Design of Data Crypto-Block adapted Smart Card, Journal of Korea Academia-Industrial Cooperation Society, vol. 12, no. 5, pp. 2317-232, DOI : 10.5762/ KAIS.2011.12.5.2317 **(2011)**

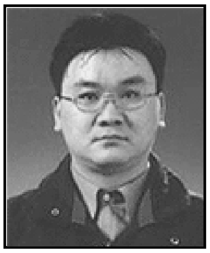
Authors

Jeung-Seop Kim received the M.S. degree from Kyungpook National University, Daegu, Korea, in 1999, and the Ph.D. degree from Kyungpook National University of Korea, in 2005, all in Computer Engineering. Now he is CEO, A2Tec co., Ltd.



Jong-Il Kim received the M.S. degree from Sunmoon University, ChungNam, Asan-si, Korea, in 2004, and the Ph.D. degree from Sunmoon University, in 2007, all in Computer Information and Sciences. Now he is Director of Research Institute, A2Tec co., Ltd.

Chang-Jin Seo received the M.S. degree from Busan National University, Busan, Korea, in 1999, and the Ph.D. degree from Busan National University of Korea, in 2003, all in Multimedia Engineering. Now He is an assistant professor in Information and Telecommunications faculty of Sangmyung University



Yong-Seok Jang received the M.S. degree from Kyungpook National University, Daegu, Korea, in 2001, and the Ph.D. degree from Kyungpook National University of Korea, in 2007, all in Computer Engineering. Now he is Director of Technology, Big Data Computing Research Group, Korea Information Processing Society and CEO, DAOOLDNS co., Ltd.