INFORMATICA, 2009, Vol. 20, No. 1, 139–150

Robust Key Exchange Protocol between Set-Top Box and Smart Card in DTV Broadcasting

Eun-Jun YOON
School of Electrical Engineering and Computer Science, Kyungpook National University
1370 Sankyuk-dong, Buk-gu, Daegu 702-701, South Korea
e-mail: ejyoon@tpic.ac.kr

Kee-Young YOO *
Department of Computer Engineering, Kyungpook National University
1370 Sankyuk-dong, Buk-gu, Daegu 702-701, South Korea
e-mail: yook@knu.ac.kr

Received: July 2006; accepted: June 2008

Abstract. Secure communication between set-top boxes (STBs) and smart cards is directly related to the benefit of the service providers and the legal rights of users, while key exchange is the essential part of a secure communication. In 2004, Jiang *et al.* proposed a key exchange protocol for STBs and smart cards based upon Schnorr's digital signature protocol and a one-way hash function. This paper, however, demonstrates that Jiang *et al.*'s protocol is vulnerable to an impersonation attack and does not provide perfect forward secrecy. In addition, in order to isolate such problems, we present a new secure key exchange protocol based on a one-way hash function and Diffie–Hellman key exchange algorithm.

Keywords: cryptography, smart card, key exchange, set-top box, cryptanalysis, DTV broadcasting.

1. Introduction

With the rapid digitization of television broadcasting, conventional television media gradually has synthesized other forms of technology information and communication fields, in order to form a completely new and significant digital television industry. In digital television (DTV) broadcasting, service providers charge subscribing fee by scrambling the program with a conditional access system, as well as controlling the illegal reception of the charged program. A smart card can be used to decrypt the control words (CW) and then transfer to them back to a set-top box (STB), to descramble the scrambled program (Macq *et al.*, 1995; Tu *et al.*, 1999; Jiang *et al.*, 2004b).

Since most DTV broadcasting is unidirectional, there is no authentication between the head-end and the subscriber on line, so the service providers utilize authentication between the STB and smart card so as to protect their benefit. Secure communication

*Corresponding author

between them is vital to the security of the system, which directly affects the revenues for the service provider. While key exchange (Chen *et al.*, 2007; Tseng, 2007; Sakalauskas *et al.*, 2007; Chen *et al.*, 2008; Tseng *et al.*, 2008) is the essential part of secure communication, without mutual authentication in the communication between the STB and smart card, one smart card can be used in different STBs of the same type, which will cause McCormac Hack and smart card cloning problems (Kanjanarin *et al.*, 2001). McCormac Hack occurs when the data line between the smart card and STB is trapped and directed to another STB that acts as if it has the same smart card inside. Smart card cloning is the duplicating of a legal card to make many illegal cards that can allow the unauthorized receptiom of program. If a key exchange process is cracked by the attacker, the attacker can extract the key information of smart cards which can be used to duplicate many smart cards or redirect to other STBs. This will allow illegitimate subscribers to receive scrambled program. As determined, media providers suffer lost revenues in the amount of hundreds of millions of dollars each tear due to smart cards being cracked (Kogan *et al.*, 2003). Secure key exchange with mutual authentication is an essential part of secure communication, which will greatly improve the security of the system thus reducing the potential for loss.

In 2004, (Jiang *et al.*, 2004a) proposed a key exchange protocol for STBs and smart cards based upon Schnorr's digital signature protocol (Schnorr, 1990) and a one-way hash function. Jiang *et al.* claimed that their proposed protocol is not only dynamic, secure and mutually can be authenticated with less computations, but also it can prevent smart cloning and McCormac Hack problems (Kogan *et al.*, 2003). The current paper, however, demonstrates that Jiang *et al.*'s protocol is vulnerable to an impersonation attack and does not provide perfect forward secrecy (Steiner *et al.*, 1995). Furthermore, in order to resolve such problems, we present a new secure key exchange protocol based on a one-way hash function and the Diffie–Hellman key exchange algorithm (Diffie *et al.*, 1976; Menezes *et al.*, 1997).

The remainder of this paper is organized as follows: Section 2 briefly reviews Jiang *et al.*'s protocol and then, two security problems are outlined in Section 3. The proposed protocol is presented in Section 4, while Section 5 and 6 discuss the security and the efficiency of the proposed protocol. Section 7 offers a conclusion for the paper.

2. Review of Jiang *et al.*'s Protocol

This section briefly reviews Jiang *et al.*'s key exchange protocol with mutual authentication based upon Schnorr's signature and a one-way hash function, for the secure communication between STBs and smart cards. Some notations used in their protocol and in our proposed protocol are defined as follows.

- ID_c: the smart card identity of user;
- PW: the secret and possible weak user password;
- ID_s: the identity of the STB;
- x_s: a secret key of the STB;

- p, q: 512 bits and 140 bits public primes p and q, such that $q|p-1$ in order to guarantee the security of the system;
- g: a public, primitive element in $GF(p)$;
- x_c, y_c: the private key and the public key of a smart card, respectively;
- a, b: session-independent random exponents $\in [1, q-1]$ chosen by the smart card and the STB, respectively;
- CW: a control word;
- $E(\cdot)$: a symmetrical encryption algorithm for encrypting CW, for example, $E_k(CW)$ and $E_k^{-1}(CW)$ means encrypting CW with key k and decrypting CW with key k, respectively;
- $h(\cdot)$: a secure one-way hash function whose output length is 128 bits;
- $\oplus$: the bitwise-or exclusion operation.

Jiang *et al.*'s protocol consists of five phases: Registration, login, mutual authentication, key agreement, and CW transmission. Fig. 1 shows Jiang *et al.*'s protocol. The protocol works as follows.

2.1. *Registration Phase*

When a user subscribes to the charge program with his smart card identity ID_c and password PW for registration, the subscriber management system (SMS) (Jiang *et al.*, 2004b; Kamperman *et al.*, 2001) will do the following:

(1) compute $R = h(ID_c \oplus x_s) \oplus h(PW)$;
(2) choose two public primes p and q as in Schnorr's protocol (Schnorr, 1990);
(3) compute $y_c = g^{-x_c} \bmod p$;

Shared Information: y_c, p, q, g, $h(\cdot)$.
Information held by User: ID_c, PW, Smart card(R, g, ID_c, ID_s, $h(\cdot)$, $E(\cdot)$).
Information held by the STB: ID_s, x_s.

Smart Card		**STB**
Input ID_c,PW $X \leftarrow R \oplus h(PW)$ Select $t, r \in Z_q$ $T \leftarrow g^t \bmod p$		
$Y \leftarrow h(T, ID_c, ID_s)$	$X, T, Y, r, ID_c \longrightarrow$	Check $X \stackrel{?}{=} h(ID_c \oplus x_s)$
		$M \leftarrow h(ID_s \oplus r)$
Check $M \stackrel{?}{=} h(ID_s \oplus r)$	$\longleftarrow M, e$	Select $e \in [0, 2^k)$
$d \leftarrow t + ex_c \bmod q$		
$SK \leftarrow h(r, e, ID_c, ID_s)$	$d \longrightarrow$	Check $Y \stackrel{?}{=} h(g^d y_c^e, ID_c, ID_s)$
$SK \leftarrow h(r, e, ID_c, ID_s)$ $CW_e \leftarrow E_{SK}(CW)$	$CW_e \longrightarrow$	$CW \leftarrow E_{SK}^{-1}(CW_e)$

Common Session key $SK = h(r, e, ID_c, ID_s)$

Fig. 1. Jiang *et al.*'s key exchange protocol.

(4) store $R, g, ID_c, ID_s, h(\cdot), E(\cdot)$ as well as the master private key (MPK) (Jiang *et al.*, 2004b; Kamperman *et al.*, 2001) and other account information in the smart card and then issues it to the user.

2.2. *Login Phase*

When a user wants to receive the subscribed program, he or she must attach his smart card to his STB and input the ID_c and PW. The smart card then does the following:

(1) generate two random numbers t and r in Z_q^*;
(2) compute $T = g^t \bmod p$ and $Y = h(T, ID_c, ID_s)$. All of the above work can be pre-computed in the idle time of the last running period;
(3) compute $X = R \oplus h(PW)$;
(4) send login request message $\{X, Y, r, ID_c\}$ to the STB for login.

2.3. *Mutual Authentication Phase*

Upon receiving the login request, the STB and the smart card need to do the following steps to realize mutual authentication:

1. First, the STB first checks the validity of ID_c. If it is invalid, the STB rejects this request.
2. The STB checks to see whether $X = h(ID_c, x_s)$ is true. If it is true, the STB receives the login request and takes the next step; otherwise, this login request is rejected.
3. The STB chooses a random number e, where $0 \leqslant e \leqslant 2^k$ and computes $M = h(ID_s, r)$, where the length of k is 72 bits as suggested by Schnorr (Schnorr, 1990).
4. The STB sends $\{M, e\}$ to the smart card for identifying.
5. The smart card computes $M' = h(ID_s, r)$ and checks to see whether $M' = M$ is true, if it is true, the STB's identity is accepted and the next step is taken, otherwise this communication is denied.
6. The smart card computes $d = t + ex_c \bmod q$ and sends it to the STB.
7. The STB checks to see whether $Y = h(g^d y_c^e, ID_c, ID_s)$ is true. If it is true, the STB accepts the smart card; otherwise the STB rejects the smart card.

2.4. *Key Agreement Phase*

If mutual authentication is determined to be successful for both STB and smart card, then the following equation is used to compute a common session key $SK = h(r, e, ID_c, ID_s)$, which includes both the random number chosen by the STB and the smart card.

2.5. *CW Transmission Phase*

After decrypting the CW, the smart card uses the SK to encrypt it as $CW_e = E_{SK}(CW)$ and sends the CW_e back to the STB in order to descramble the program. The STB can decrypt the CW as $CW = E_{SK}^{-1}(CW_e)$.

3. Cryptanalysis of Jiang *et al.*'s Protocol

This section demonstrates that Jiang *et al.*'s protocol is vulnerable to an impersonation attack and that it does not provide perfect forward secrecy.

3.1. *Impersonation Attack*

This subsection demonstrates that Jiang *et al.*'s protocol is vulnerable to an impersonation attack, where an attacker can easily impersonate other legal users (or the STB) in order to obtain a useful information. This happens because an attacker can easily obtain the common session key SK of the user (or the STB) in the mutual authentication phase. First, suppose that E is an attacker who knows the STB's ID_s. Usually, because the STB's identity ID_s does not require safety, E can easily get the target STB's ID_s by various attack methods, such as the stolen-verifier attack (Lin *et al.*, 2003) and server data eavesdropping (Yang *et al.*, 2003). By using the STB's ID_s in the mutual authentication phase, E can compute the common session key SK between the STB and the smart card as follows.

1. Suppose that E has eavesdropped a valid message $(X, T, Y, r, ID_c, M, e, d)$ from an open network. Then, C can easily compute the common session key $SK = h(r, e, ID_c, ID_s)$ by using the values r, e, ID_c and ID_s.
2. In the CW transmission phase, E chooses a modified CW', computes a forged $CW_e = E_{SK}(CW')$, and sends it to the STB.
3. It is easy to check whether the STB will decrypt the forged message CW_e, as $CW' = E_{SK}^{-1}(CW_e)$. As a result, the STB will accept the attacker's CW', thus making Jiang *et al.*'s protocol insecure.
4. Furthermore, after intercepting the CW_e from the user in the CW transmission phase, and since E can obtain the CW by decrypting CW_e by using SK, as $CW = E_{SK}^{-1}(CW_e)$, E can also impersonate the STB to the user in the CW transmission phase. Therefore, Jiang *et al.*'s protocol is obviously vulnerable to an impersonation attack.

3.2. *Perfect Forward Secrecy Problem*

Perfect forward secrecy (Steiner *et al.*, 1995) is a very important security requirement that is needed to evaluate a strong protocol. A protocol with perfect forward secrecy assures that even if one entity's long-term key (e.g. user password) is compromised, it will never reveal any old fresh session keys which were used before. For example, the well-known Diffie–Hellman key agreement protocol (Diffie *et al.*, 1976) can provide perfect forward secrecy.

In Jiang *et al.*' protocol, if the STB's identity ID_s acts as the STB's secret key, the above-mentioned impersonation attack cannot succeed because an attacker E cannot know the secure value ID_s. Nevertheless, Jiang *et al.*'s protocol still does not provide perfect forward secrecy because once the identity ID_s of the STB is disclosed, all previous

fresh session keys will also be opened and hence previous communication messages will be learned. In Jiang *et al.*'s protocol, suppose an attacker E obtains the identity ID_s from the compromised STB and intercepts the transmitted values $(X, T, Y, r, ID_c, M, e, d)$, then E can easily compute the common session key $SK = h(r, e, ID_c, ID_s)$ and the values r, e, ID_c and ID_s. Obviously, Jiang et al.'s protocol does not provide perfect forward secrecy.

4. Proposed Key Exchange Protocol

This section proposes an improvement of Jiang *et al.*'s key exchange protocol. The proposed protocol also consists of five phases: Registration, login, mutual authentication, key agreement, and CW transmission. Fig. 2 shows the proposed protocol. The protocol works as follows.

4.1. *Registration Phase*

When a user subscribes to the charge program with his smart card identity ID_c and password PW for registration, the SMS will do the following:

(1) compute $R = h(ID_c \oplus x_s) \oplus PW$;
(2) store $R, g, ID_s, h(\cdot), E(\cdot)$ as well as the MPK and other account information in the smart card and this is issued to the user.

Shared Information: p, q, g, $h(\cdot)$.
Information held by User: ID_c, PW, Smart card($R, g, ID_s, h(\cdot), E(\cdot)$).
Information held by the STB: ID_s, x_s.

Smart Card		**STB**
Input ID_c,PW Select $a \in Z_q$ $A \leftarrow g^a \bmod p$ $X \leftarrow R \oplus PW$ $Y \leftarrow h(X, A, ID_c, ID_s)$	$ID_c, Y, A \longrightarrow$	Compute $h(ID_c \oplus x_s)$ Check $Y \stackrel{?}{=} h(h(ID_c \oplus x_s), T, ID_c, ID_s)$ Select $b \in Z_q$ $B \leftarrow g^b \bmod p$ $K \leftarrow (A)^b \bmod p$
$K \leftarrow (B)^a \bmod p$	$\longleftarrow B, M$	$M \leftarrow h(K, A, ID_c, ID_s)$
Check $M \stackrel{?}{=} h(K, A, ID_c, ID_s)$ $D \leftarrow h(K, B, ID_c, ID_s)$		
$SK \leftarrow h(K, ID_c, ID_s)$	$D \longrightarrow$	Check $D \stackrel{?}{=} h(K, B, ID_c, ID_s)$ $SK \leftarrow h(K, ID_c, ID_s)$
$CW_e \leftarrow E_{SK}(CW)$	$\longrightarrow CW_e$	$CW \leftarrow E_{SK}^{-1}(CW_e)$

Common Session key $SK = h(K, ID_c, ID_s)$

Fig. 2. Proposed key exchange protocol

4.2. *Login Phase*

When a user wants to receive the subscribed program, he or she must attach his smart card to his STB and input his ID_c and PW. Then, the smart card then does the following:

(1) generate a random number a in Z_q^* and $A = g^a \bmod p$ is computed. All of this work can be pre-computed in the idle time of last running period;
(2) compute $X = R \oplus h(PW)$ and $Y = h(X, A, ID_c, ID_s)$;
(3) send a login request message $\{ID_c, Y, A\}$ to the STB in order to login.

4.3. *Mutual Authentication Phase*

Upon receiving the login request, the STB and the smart card need to do the following steps in order to realize mutual authentication:

1. The STB first checks the validity of ID_c. If it is invalid, the STB rejects this request.
2. The STB computes $h(ID_c \oplus x_s)$ and checks to see whether $Y = h(h(ID_c \oplus x_s), A, ID_c, ID_s)$ is true. If it is true, the STB receives the login request and takes the next step; otherwise, this login request is rejected.
3. The STB generates a random number b in Z_q^* and computes $B = g^b \bmod p$.
4. The STB computes $K = A^b = g^{ab} \bmod p$ and $M = h(K, A, ID_c, ID_s)$. Then, the STB sends $\{B, M\}$ to the smart card for identifying.
5. The smart card computes $K = B^a = g^{ab} \bmod p$ and $M' = h(K, A, ID_c, ID_s)$, and checks to see whether $M' = M$ is true, if it is true, the STB's identity is accepted and the next step is taken, otherwise this communication is denied.
6. The smart card computes $D = h(K, B, ID_c, ID_s)$ and sends it to the STB.
7. The STB checks to see whether $D = h(K, B, ID_c, ID_s)$ is true. If it is true, the STB accepts the smart card; otherwise the STB rejects the smart card.

4.4. *Key Agreement Phase*

If mutual authentication is passed successfully for both the STB and the smart card, then the following equation is used to compute a common session key $SK = h(K, ID_c, ID_s)$, which includes both the random number chosen by the STB and the smart card.

4.5. *CW Transmission Phase*

After decrypting the CW, the smart card uses SK to encrypt it as $CW_e = E_{SK}(CW)$ and sends CW_e back to the STB in order to descramble the program. The STB can decrypt the CW as $CW = E_{SK}^{-1}(CW_e)$.

5. Security Analysis

This section provides the determining proof of the proposed protocol. First, the security terms (Menezes *et al.*, 1997) needed for the analysis of the proposed protocol are defined as follows.

DEFINITION 1. A weak secret key (user's password PW) is the value of low entropy $W(k)$, which can be guessed in polynomial time.

DEFINITION 2. A strong secret key (STB's secret key x_s) is the value of high entropy $S(k)$, which cannot be guessed in polynomial time.

DEFINITION 3. The discrete logarithm problem (DLP) is as follows. Given a prime p, a generator g of Z_p^*, and an element $\beta \in Z_p^*$, find the integer α, $0 \leq \alpha \leq p-2$, such that $g^\alpha \equiv \beta(\mathrm{mod}p)$.

DEFINITION 4. The Diffie–Hellman problem (DHP) is the following: Given a prime p, a generator g of Z_p^*, and an element $g^a(\mathrm{mod}p)$ and $g^b(\mathrm{mod}p)$, find $g^{ab}(\mathrm{mod}p)$.

DEFINITION 5. A secure one-way hash function $y = h(x)$ is the following: Given x to compute y is easy and given y to compute x is hard.

1. In the proposed protocol, a session key $SK = h(K, ID_c, ID_s)$ is generated as the output of a one-way hash function, whose input is the concatenation of K, ID_c and ID_s. K is the only factor known to both entities and without these information, the attacker can't compute the session key by the eavesdropped message.
2. In the proposed protocol, the STB does not need to store the smart card's secure information (e.g. user password PW), which can prevent an attack on the STB in order to get the password of the smart card.
3. Due to the fact that a one-way hash function is computationally difficult to invert, it is extremely hard for any attacker to derive the STB's secret key x_s from $h(ID_c \oplus x_s)$. Even if the smart card of the user is picked up by an attacker, it is still difficult for the attacker to derive x_s.
4. For each communication, mutual authentication and key exchange are needed to reach a dynamic session key, for which both entities provide key seed information (i.e. a and b), which can resist a replay attack and an impersonated attack, as well as to avoid the perfect forward security problem. Moreover, at each time, the session key SK is different, which can increase the difficulty in attacking the encryption algorithm with a known plain-text attack.
5. In the proposed protocol, since the Diffie–Hellman key exchange algorithm is used to generate a session key g^{ab}, perfect forward secrecy is ensured because an attacker with a compromised STB secret key x_s is only able to obtain the g^a and g^b from an earlier session. In addition, it is also computationally infeasible to obtain the session key g^{ab} from g^a and g^b, as it is a discrete logarithm problem and a

Diffie–Hellman problem, respectively. Therefore, the proposed protocol provides perfect forward secrecy.

6. Regarding smart card cloning and McCormac Hack problems (Kogan *et al.*, 2003), when an attacker uses his cloned smart card to another the STB, since there is no STB's ID_s or x_s in the cloned smart card and the hash function $h(\cdot)$ in the STB is different than that of the smart card, the mutual authentication phase can not pass.
7. When an attacker redirects one smart card's communication message to another one, the STB has no information of the session key SK without mutual authentication and key exchange, so the STB can't decrypt the message that was redirected from the other smart card.
8. The user can freely change his smart card's password from PW to PW' just by replacing and storing R with R' in the smart card, where $R' = R \oplus PW \oplus PW'$, which can improve the security of the smart card as well as prevent children from watching the charged program by itself. So, even with smart card, a user who doesn't know the password still can't receive the program.

6. Efficiency Analysis

This section analyzes the efficiency of the proposed key exchange protocol. Table 1 gives computational costs of proposed protocol and Jiang *et al.*'s protocol in the registration, login, mutual authentication, key agreement and CW transmission phases.

In the registration phase, the proposed protocol does not need the computation costs of modular exponentiation unlike Jiang *et al.*'s protocol. In the mutual authentication phase, 5 times one-way hash function operations and 3 times modular exponentiation operations are need to resist our proposed impersonation attack and to provide the perfect forward secrecy. As a result, the proposed protocol also has same performance like Jiang *et al.*'s protocol as shown in Table 1. However, the proposed protocol is more secure than Jiang *et al.*'s protocol because the proposed protocol resists our proposed impersonation attack and provides the perfect forward secrecy.

7. Conclusions

Recently, Jiang *et al.* proposed a key exchange protocol for the STB and the smart card based upon Schnorr's digital signature protocol and a one-way hash function. The current paper, however, demonstrated that Jiang *et al.*'s protocol is vulnerable to an impersonation attack and does not provide perfect forward secrecy. Thus, we presented a new secure key exchange protocol based on a one-way hash function and the Diffie–Hellman key exchange algorithm in order to isolate such a problem and to provide perfect forward secrecy. As a result, in contrast to Jiang *et al.*'s protocol, the proposed protocol can securely perform key agreements for secure communication between the STB and smart card in the DTV broadcasting.

Table 1
Comparisons of computational costs on each phase

	Registration	Login	Mutual authentication	Key agreement	CW Transmission
Jiang *et al.*'s protocol	$2T(h)$ $2T(\oplus)$ $1T(e)$	$2T(h)$ $1T(\oplus)$ $2T(r)$ $1T(e)$	$4T(h)$ $1T(r)$ $2T(e)$	$2T(r)$	$2T(s)$
Proposed protocol	$1T(h)$ $2T(\oplus)$	$2T(h)$ $1T(\oplus)$ $1T(r)$ $1T(e)$	$5T(h)$ $1T(r)$ $3T(e)$	$2T(h)$	$2T(s)$

$T(h)$: computation cost of one-way hash function; $T(\oplus)$: computation cost of exclusive-OR operation; $T(s)$: computation cost of symmetric encryption; $T(r)$: computation cost of random number; $T(e)$: computation cost of modular exponentiation.

Acknowledgements. We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript. Eun-Jun Yoon was supported by 2nd Brain Korea 21 Project in 2008. Kee-Young Yoo was supported by the MKE(Ministry of Knowledge Economy) of Korea, under the ITRC support program supervised by the IITA(IITA-2008-C1090-0801-0026).

References

Chen, T.H, Horng, G. and K.C. Wu (2007). A secure YS-like user authentication scheme. *Informatica*, **18**(1), 27–36.

Chen, T.H, Horng, G. and C.S. Yang (2008). Public key authentication schemes for local area networks, *Informatica*, **19**(1), 3–16.

Diffie, W., and M. Hellman (1976). New directions in cryptography. *IEEE Trans. Inf. Theory*, **IT-22**(6), 644–654.

Jiang, T., Hou, Y. and S. Zheng (2004). Secure communication between set-top box and smart card in DTV broadcasting. *IEEE Trans. Consum. Electr.*, **50**(3), 882–886.

Jiang, T., Zheng, S. and B. Liu (2004). Key distribution based on hierarchical access control for conditional access system in DTV broadcast. *IEEE Trans. Consum. Electr.*, **50**(1), 225–230.

Kamperman, F., and B.V. Rijnsoever (2001). Conditonal access system interoperability through software downloading. *IEEE Trans. on Consumer Electronics*, **47**(1), 47–53.

Kanjanarin, W., and T. Amornraksa (2001). Scrambling and key distribution scheme for digital television. In *IEEE International Conference on Networks*. pp. 140–145.

Kogan, N., Shavitt, Y. and A. Wool (2003). A practical revocation scheme for broadcast encryption using smart cards. In *Proc. of IEEE Symposium on Security and Privacy*. pp. 225–235.

Lin, C.L., and T. Hwang (2003). A password authentication scheme with secure password updating. *Computers & Security*, **22**(1), 68–72.

Macq, B., and J. Quisquater (1995). Cryptology for digital TV broadcasting, In *Proceedings of the IEEE*, **83**(6). pp. 944–957.

Menezes, A.J., Oorschot, P.C. and S.A. Vanstone (1997). *Handbook of Applied Cryptograph*. CRC Press, New York.

Sakalauskas, E., Tvarijonas, P. and A. Raulynaitis (2007). Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level. *Informatica*, **18**(1), 115–124.

Schnorr C.P. (1990). Efficient identification and signatures for smart cards, In *Crypto'89*, LNCS **435**. pp. 235–251.

Steiner, M., Tsudik, G. and M. Waidner (1995). Refinement and extension of encrypted key exchange. *ACM Operating Systems Review*, **29**(3), 22–30.

Tseng, Y.M. (2007). An efficient two-party identity-based key exchange protocol, *Informatica*, **18**(1), 125–136.

Tseng, Y.M., Wu, T.Y. and J.D. Wu (2008). A pairing-based user authentication scheme for wireless clients with smart cards. *Informatica*, **19**(2), 285–302.

Tu, F.K., Laih, C.S. and H.H. Tung (1999). On key distribution management for conditional access system on pay-TV system. *IEEE Trans. Consum. Electr.*, **45**, 151–158.

Yang, C.C., T.Y. Chang, T.Y. and J.W. Li (2003). Security enhancement for protecting password transmission. *IEICE Transactions on Communications*, **E86-B**(7). pp. 2178–2181.

E.-J. Yoon received his BSc degree in the School of Textile and Fashion Technology from Kyungil University in 1995; received his MSc degree in computer engineering from Kyungil University in 2002 and the PhD degree in computer science from Kyungpook National University in 2006, South Korea. He is now a full-time lecturer at Faculty of Computer Information, Daegu Polytechnic College, South Korea. His current research interests are cryptography, authentication technologies, smart card security, network security, mobile communications security, and steganography.

K.-Y. Yoo received his BSc degree in education of mathematics from Kyungpook National University in 1976 and the MSc degree in computer engineering from Korea Advanced Institute of Science and Technology in 1978, South Korea. He received the PhD degree in computer science from Rensselaer Polytechnic Institute in 1992, New York, USA. Currently, he is a professor at the Department of Computer Engineering, Kyungpook National University, South Korea. His current research interests are cryptography, authentication technologies, smart card security, network security, DRM security, and steganography. He has published over a hundred technical and scientific international journals on a variety of information security topics.

Robastinis apsikeitimo raktais tarp interaktyviosios skaitmeninės televizijos blokų ir intelektualiųjų kortelių protokolas

Eun-Jun YOON, Kee-Young YOO

Saugus ryšys tarp interaktyviosios skaitmeninės televizijos blokų ir intelektualiųjų kortelių yra susijęs su paslaugų tiekėjų pelnu ir vartotojų teisėmis. Ryšio svarbiausia dalis yra saugus apsikeitimas raktais. 2004 m. Jiang ir kt. pasiūlė interaktyviosios skaitmeninės televizijos blokų ir intelektualiųjų kortelių apsikeitimo raktais protokolą, kuriame panaudotas Schnorr'o skaitmeninio parašo protokolas bei vienos krypties santraukos funkcija. Šiame straipsnyje įrodyta, kad Jiang'o ir kt. protokolas yra pažeidžiamas ir neužtikrina reikalaujamo saugumo. Siekiant išvengti šių trūkumų, pasiūlytas naujas saugus apsikeitimo raktais protokolas, kuriame panaudota vienos krypties santraukos funkcija ir Diffie–Hellman'o apsikeitimo raktais protokolas.