Available online at www.sciencedirect.com
ScienceDirect
Chaos, Solitons and Fractals xxx (2007) xxx–xxx
CHAOS SOLITONS & FRACTALS
www.elsevier.com/locate/chaos

Identifying attributes and insecurity of a public-channel key exchange protocol using chaos synchronization

S. Han [a,*], E. Chang [a], T. Dillon [a], M. Hwang [b], C. Lee [c]

[a] *Curtin University of Technology, G.P.O. Box U1987 Perth, WA 6845, Australia*
[b] *National Chung Hsing University, Kuo Kuang Road, Taichung, Taiwan, ROC*
[c] *Asia University, Lioufeng Road, Wufeng Shiang, Taichung, Taiwan, ROC*

Accepted 30 October 2007

Abstract

Klein et al. proposed a key exchange protocol using chaos synchronization. The first protocol comprises two parties with chaotic dynamics that are mutually coupled and undergo a synchronization process, at the end of which they can use their identical dynamical state as an encryption key. From cryptographic point of view, their key exchange protocol is a key agreement protocol. Klein et al. claimed that their key agreement can be carried out over a public channel. In order to increase the key space and decrease the precision of the calculation, they made an extension of the system to a network of N Lorenz equations. In this paper, we will provide a cryptanalysis of their key agreement protocol. We will first point out some weaknesses, and then show that their protocol is not secure against several attacks including impersonation attack.

1. Introduction

A secure key exchange protocol can help communication parties to establish shared secret keys [1,20]. Generally speaking, such shared secret keys are used as session keys to transfer an encryption/decryption key between the intended parties or directly to encrypt confidential information that are critical to them. Therefore, building secure key exchange protocols over public channels is one of the primitive goals in modern cryptography and information security [12,20]. Diffie-Hellman key exchange protocol is the first protocol for generating a shared secret key [20]. New key agreement protocols which improved the original Diffie-Hellman protocol have been proposed [12].

However, prior to the protocol introduced in [17], most existing secure key exchange protocols are based on traditional number theory [19]. Some are based on the integer factoring problem; others are based on the discrete logarithm problem. A general question is whether it is possible to build a secure key exchange protocol without using traditional number theory.

Due to the development of the analog and discrete chaotic dynamical systems, they have been utilized to design various cryptosystems as well as the analysis of some schemes security [2–11,13–19,21–24]. For the analog chaotic

* Corresponding author.
E-mail address: s.han@curtin.edu.au (S. Han).

0960-0779/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.chaos.2007.10.050

dynamical systems [15,18,22,23], the communication parties need to agree on some secret parameters in most of the known chaotic cryptographic systems. Some parameters had to be transferred privately. After this private agreement, the two chaotic systems synchronize by exchanging signals over a public channel. In order to use chaos synchronization to build a secure key change protocol over a public channel without prior private agreement, Klein et al. proposed a public channel key exchange protocol based on chaos synchronization [17].

The first protocol comprises two parties with chaotic dynamics that are mutually coupled and undergo a synchronization process, at the end of which they can use their identical dynamical state as an encryption key. From cryptographic point of view, their key exchange protocol is a key agreement protocol. Klein et al. claimed that their key agreement can be carried out over a public channel. In order to increase the key space and decrease the precision of the calculation, they made an extension of the system to a network of N Lorenz equations.

Klein et al. analyzed their protocol in two different attacks: (1) Regularly following attack (RFA), which means that in a key agreement protocol based on chaotic systems, an RFA attacker, who knows all the details of the model and listen to any communication between the parties A and B, can get synchronization with A and B; (2) embedded signal attack (ESA), which means that in a key agreement protocol based on chaotic systems, an ESA attacker, who tries to analyze the transmitted signal by embedding the signal in a space, defined by signals transmitted in different time steps, can recover the x values of the system. From the cryptanalysis point of view, the two attacks are passive attacks, where an adversary attempts to prevent or compromise a protocol from achieving its goals by merely observing honest entities carrying out the protocol.

From a security point of view, it is not enough that a key exchange/agreement protocol can withstand some passive attacks. Besides the passive attacks, a secure key agreement (exchange) protocol should also be able to withstand the active attacks, where an adversary additionally subverts the communications by injecting, deleting, altering or replaying messages [20]. Therefore, the Klein et al. key exchange protocol should be measured by some active attacks and the related desirable security attributes.

In this paper, we will provide a cryptanalysis of their key agreement protocol. We will first point out some weaknesses, and then show that their protocol is not secure against several attacks including impersonation attack. With the presented impersonation attack on that protocol and the discussions on the security attributes, it should be useful to the field of chaos synchronization and its application to cryptography and information security.

2. Brief review of Klein et al.'s key exchange protocol

2.1. Review of the protocol

We adopt the similar notations in Klein et al.'s key exchange protocol (we name it as the KMKW key exchange protocol) to give a brief review of their scheme [17]. We only review their first key agreement protocol with two Lorenz systems. For the second protocol, please refer to [17] for the details.

Consider two Lorenz systems, A and B, coupled by their x value,

$$\frac{dx_A}{dt} = 10(y_A - x_A) + K[f_B(t) - f_A(t)], \tag{1}$$

$$\frac{dx_B}{dt} = 10(y_B - x_B) + K[f_A(t) - f_B(t)], \tag{2}$$

$$\frac{dy_A}{dt} = 28x_A - y_A - x_A z_A, \quad \frac{dy_B}{dt} = 28x_B - y_B - x_B z_B, \tag{3}$$

$$\frac{dz_A}{dt} = x_A y_A - \frac{8}{3} z_A, \quad \frac{dz_B}{dt} = x_B y_B - \frac{8}{3} z_B, \tag{4}$$

where K is the coupling strength between the two systems, and $f(t)$ is a nonlinear function based on x at previous time steps: $f(t) = f(x(t-\tau_1), x(t-\tau_2)\ldots)$.

Each party initializes its variables with secret random values. Use of $x(t-\tau)$ as the coupling signal is not secure, therefore they suggested using a nonlinear function of the variable x at previous time steps, $f(t)$, as described above. Which nonlinear function f should be used? On one hand, $f(t)$ should enable synchronization. On the other hand, if $f(t)$ is linear in $x(t-\tau)$, it will be easy to reveal the state of the system. Therefore, the authors of [16] added a small perturbation to the main signal, constructed from two time delayed values $x(t_1)$ and $x(t_2)$ [18], where $t_1 = t - \tau_1$ and $t_2 = t - \tau_2$,

$$f(t) = x(t_1) + \mathrm{sgn}[x(t_1)]A[x(t_1) - x(t_2)]^2 \tag{5}$$

where $\mathrm{sgn}[x(t_1)]$ ensures an average mean for the perturbation around $x(t_1)$.

Please cite this article in press as: Han S et al., Identifying attributes and insecurity of a public-channel key ..., Chaos, Solitons & Fractals (2007), doi:10.1016/j.chaos.2007.10.050

3. Insecurity of the KMKW key exchange protocol

In this section, we will demonstrate Klein et al.'s key exchange/agreement protocol is not as secure as they claimed [17]. Thus, we will present several security issues in Klein et al.'s public channel key agreement protocol. These issues are those of most concerned in the design of a public channel key exchange protocol.

3.1. Security issue 1 in the KMKW key exchange protocol

From the construction of the Klein et al. key agreement, it is known that there is no entity authentication involved in the process of key agreement. As a result, Klein et al. key agreement protocol does not have the key-compromise impersonation resilience property [20]. This property means if a malicious entity E compromises an entity's private key (with regard to the key agreement in [17], it is one of the initial states), the entity E cannot masquerade as a third party to the entity whose private key was compromised.

3.2. Security issue 2 in the KMKW key exchange protocol

Perfect forward secrecy means that a key agreement protocol can keep the secrecy of previous session keys if static private keys are compromised. The unique secret element of each party (Alice as well as Bob)in the Klein et al. key exchange protocol is the initial state variable $x_{\text{Alice}}^{\text{initial}}$ (as well as $x_{\text{Bob}}^{\text{initial}}$). On the other hand, the perfect forward secrecy is defined only with respect to static private keys (See page 496 in Ref. [20]). Therefore, the Klein et al. key exchange protocol does not involve any static private key. As a result, their protocol does not have the perfect forward secrecy.

3.3. Security issue 3 in the KMKW key exchange protocol

In this subsection, we will present an impersonation attack on Klein et al.'s key agreement protocol. The details are as the following:

1. Choose random initial states
   - 1.1 Alice chooses randomly her private initial states x_A^{initial}, y_A^{initial} and z_A^{initial}.
   - 1.2 Bob chooses randomly his private initial states x_B^{initial}, y_B^{initial} and z_B^{initial}.
2. Alice runs her chaotic systems
$$\frac{dx_A}{dt} = 10(y_A - x_A) + K[f_B(t) - f_A(t)], \tag{6}$$
$$\frac{dy_A}{dt} = 28x_A - y_A - x_A z_A, \tag{7}$$
$$\frac{dz_A}{dt} = x_A y_A - \frac{8}{3} z_A \tag{8}$$
   and sends $x_A^{t_i}$, $y_A^{t_i}$ and $z_A^{t_i}$ to Bob.
   - 2.1 Before Bob receives them, Eve intercepts $x_A^{t_i}$, $y_A^{t_i}$ and $z_A^{t_i}$.
   - 2.2 Eve chooses two pairs of different initial states $\{x_{BE1}^{\text{initial}}, y_{BE1}^{\text{initial}}, z_{BE1}^{\text{initial}}\}$ and $\{x_{BE2}^{\text{initial}}, y_{BE2}^{\text{initial}}, z_{BE2}^{\text{initial}}\}$. Because of the randomness of all the initial states, the following relationship holds with high (non-negligible) probability:
$$x_{BEj}^{\text{initial}} \neq x_B^{\text{initial}} \tag{9}$$
$$y_{BEj}^{\text{initial}} \neq y_B^{\text{initial}} \tag{10}$$
$$z_{BEj}^{\text{initial}} \neq z_B^{\text{initial}} \tag{11}$$
     where $j = 1, 2$.
3. Eve uses the following chaotic systems
$$\frac{dx_{BE1}}{dt} = 10(y_{BE1} - x_{BE1}) + K[f_A(t) - f_{BE1}(t)], \tag{12}$$
$$\frac{dy_{BE1}}{dt} = 28x_{BE1} - y_{BE1} - x_{BE1} z_{BE1}, \tag{13}$$
$$\frac{dz_{BE1}}{dt} = x_{BE1} y_{BE1} - \frac{8}{3} z_{BE1}, \tag{14}$$

Please cite this article in press as: Han S et al., Identifying attributes and insecurity of a public-channel key ..., Chaos, Solitons & Fractals (2007), doi:10.1016/j.chaos.2007.10.050

and

$$\frac{dx_{BE2}}{dt} = 10(y_{BE2} - x_{BE2}) + K_2[f_B(t) - f_{BE2}(t)], \tag{15}$$

$$\frac{dy_{BE2}}{dt} = 28x_{BE2} - y_{BE2} - x_{BE2}z_{BE2}, \tag{16}$$

$$\frac{dz_{BE2}}{dt} = x_{BE2}y_{BE2} - \frac{8}{3}z_{BE2}, \tag{17}$$

where

- The coefficients of $f_{BE1}(t)$ and $f_B(t)$ are the same parameters but with different initial states

$$x_{BE1}^{\text{initial}} \neq x_B^{\text{initial}} \tag{18}$$

as their input.

- $K_2 \gg K$.
- The coefficients of $f_{BE2}(t)$ and $f_A(t)$ are the same parameters.

With her own initial states x_{BE1}^{initial}, y_{BE1}^{initial} and z_{BE1}^{initial}, Eve runs the above chaotic system Eqs. (12)–(14) on $\{x_A^{t_i}, y_A^{t_i}, z_A^{t_i}\}$ to get $x_{BE1}^{t_i}$, $y_{BE1}^{t_i}$ and $z_{BE1}^{t_i}$.

- 3.1 Eve sends $x_{BE1}^{t_i}$, $y_{BE1}^{t_i}$ and $z_{BE1}^{t_i}$ to Alice.
- 3.2 With her own another initial states x_{BE2}^{initial}, y_{BE2}^{initial} and z_{BE2}^{initial}, Eve runs

$$\frac{dx_{BE2}}{dt} = 10(y_{BE2} - x_{BE2}) + K_2[f_B(t) - f_{BE2}(t)], \tag{19}$$

$$\frac{dy_{BE2}}{dt} = 28x_{BE2} - y_{BE2} - x_{BE2}z_{BE2}, \tag{20}$$

$$\frac{dz_{BE2}}{dt} = x_{BE2}y_{BE2} - \frac{8}{3}z_{BE2}, \tag{21}$$

to get $\{x_{BE2}^{t_i}, y_{BE2}^{t_i}, z_{BE2}^{t_i}\}$.

- 3.3 Eve sends $\{x_{BE2}^{t_i}, y_{BE2}^{t_i}, z_{BE2}^{t_i}\}$ to Bob.

4. After receiving $\{x_{BE1}^{t_i}, y_{BE1}^{t_i}, z_{BE1}^{t_i}\}$, Alice repeats Step 2. From Alice's point of view, $x_{BE1}^{t_i}$, $y_{BE1}^{t_i}$ and $z_{BE1}^{t_i}$ come from Bob.
5. Eve repeats Step 2.1, 2.2 and Step 4.
6. After receiving $\{x_{BE2}^{t_i}, y_{BE2}^{t_i}, z_{BE2}^{t_i}\}$, Bob runs the systems

$$\frac{dx_B}{dt} = 10(y_B - x_B) + K[f_A(t) - f_B(t)], \tag{22}$$

$$\frac{dy_B}{dt} = 28x_B - y_B - x_B z_B, \tag{23}$$

$$\frac{dz_B}{dt} = x_B y_B - \frac{8}{3}z_B, \tag{24}$$

to get $\{x_B^{t_i}, y_B^{t_i}, z_B^{t_i}\}$.

- 6.1 Bob sends $\{x_B^{t_i}, y_B^{t_i}, z_B^{t_i}\}$ to Alice.
- 6.2 Eve intercepts $\{x_B^{t_i}, y_B^{t_i}, z_B^{t_i}\}$ and does not let it arrive at Alice.
- 6.3 Eve runs Eqs. (19)–(21) on $\{x_B^{t_i}, y_B^{t_i}, z_B^{t_i}\}$ and sends the output to Bob.

By repeating (with small adaptation to) the above procedures, we can see that Eve and Alice will get synchronization by their first state variable. On the other hand, because of $K_2 \gg K$, Bob and Eve as well as Alice will never get synchronization by their first state variable. Therefore, Klein et al.'s original key exchange protocol has no impersonation attack resilience.

4. Security attributes of a public channel key exchange protocol

In the research community of chaotic synchronization communications, no work has been done to give a full and formal security analysis on key exchange (key agreement) protocols. In this paper, we will present a reasonable full list of security attributes and measure which security attributes Klein et al.'s KMKW key agreement protocol has.

Please cite this article in press as: Han S et al., Identifying attributes and insecurity of a public-channel key ..., Chaos, Solitons & Fractals (2007), doi:10.1016/j.chaos.2007.10.050

Authentication mechanism for an key-exchange (key agreement) protocol means an key agreement protocol can provide authentication which assures the communicated parties are the intended ones. The problem with the Klein et al. key agreement protocol is that a party Alice may be setting up a secure session key with someone impersonating her intended party Bob. Because the private and public keys are generated on the fly, there is no way to prove Alice has a secure session with the intended party unless the key agreement protocol adds a method for user authentication.

The Klein et al. key exchange protocol is over a public channel. This property is perfect since the communication parties do not need to rely on a secret channel to transfer information. Also, to establish a session key over a public channel is the fundamental task in order to use symmetric cryptographic encryption systems.

Impersonation attack resilience means that a key agreement protocol can prevent any man-in-the-middle attacker from replacing/relaying the communication data (transferred between the two intended parties, say Alice and Bob) that results in a session key being established between the attacker and Alice (or Bob), one of the two intended parties. The Klein et al. key exchange protocol does not have this property. This is analyzed in Section 3 of this letter.

Guessing attack resilience means that an attacker can not guess out one of the ephemeral private keys or an established session key with non-negligible probability. Guessing attack resistance was also discussed in [6]. From the construction of the Klein et al. key exchange protocol, we know that their protocol has this property, sine the ephemeral private keys $x_{\text{Alice}}^{\text{initial}}$ and x_{Bob}^{initial} (if two parties are Alice and Bob) are some random variable states of the systems.

Theory foundation of the Klein et al. key exchange protocol is based on chaos synchronization. This is the first key exchange protocol over public channel which is based on chaotic synchronization instead of number theory.

Key-compromise impersonation resilience for a key agreement protocol means that if a party Alice's (static) private key is exposed, it does not enable an attacker to impersonate other entities to Alice. This property is not available to the Klein et al. key exchange protocol since their protocol does not involve any static private key.

Known key security means that a key agreement protocol means that if one session key is compromised, then neither the private keys nor session keys (both past and future) are compromised as a result. The Klein et al. key exchange protocol has this property, since their protocol uses a nonlinear function f of the variable x at previous time steps $f(t) = f(x(t-\tau_1), x(t-\tau_2)\ldots)$.

Perfect forward secrecy means that a key agreement protocol can keep the secrecy of previous session keys if static private keys are compromised. The Klein et al. key exchange protocol does not involve any static private key. Therefore, the perfect forward secrecy is not available to the Klein et al. key exchange protocol. In other words, perfect forward secrecy was proposed for those protocols which have both static private key and ephemeral key.

Unknown key-share resilience means that in a key agreement protocol any attacker cannot coerce honest parties Alice and Bob into establishing a session key where at least one of Alice and Bob does not know that the secret session key is shared with the other. For example, an adversary, say Eve, may coerce Bob into believing he shares the key with Eve, while he actually shares the key with Alice. The''key share'' with Alice is thus unknown to Bob. The Klein et al. key exchange protocol has this property. This is because that an unknown key-share attack takes place while both parties, say Alice and Bob, exchange their ephemeral (public) keys which are used to generate the shared secret key. From the construction of the Klein et al. key exchange protocol, we know that Alice and Bob do not need exchange their ephemeral keys $x_{\text{Alice}}^{\text{initial}}$ and x_{Bob}^{initial}.

Denial-of-service attack resilience means a key agreement protocol can prevent malicious party from exhausting the underlying server's resources. In Klein et al.'s key exchange protocol, if the coupling strength K is outside of the range $K_{\min} < K < K_{\max}$, then the chaotic synchronization can not be achieved. Therefore, the Klein et al. key exchange protocol has this property if the parameters of the chaotic systems are carefully chosen.

Static private keys are the long term private keys of a key agreement protocol which can provide service in generation of different session keys. From the construction of the Klein et al. key exchange protocol, we know that their protocol does not use any static private key.

Ephemeral private keys are the short term private keys of a key agreement protocol, which can only help to generate one session key. From the construction of the Klein et al. key exchange protocol, we know that the ephemeral private keys are the random initial states x_A^{initial} and x_B^{initial}.

Regularly following attack (RFA) resilience means that in a key agreement protocol based on chaotic systems, an RFA attacker, who knows all the details of the model and listen to any communication between the parties A and B, can not get synchronization with A and B. Klein et al. proved that their protocol has the regularly following attack resilience.

Embedded signal attack (ESA) resilience means that in a key agreement protocol based on chaotic systems, an ESA attacker, who tries to analyze the transmitted signal by embedding the signal in a space, defined by signals transmitted in different time steps. As Klein et al. analyzed, this attack can reduce to a brute force attack.

Please cite this article in press as: Han S et al., Identifying attributes and insecurity of a public-channel key ..., Chaos, Solitons & Fractals (2007), doi:10.1016/j.chaos.2007.10.050

Table 1
Summary of attributes that are related to the KMKW key exchange

Security attributes	KMKW key exchange
Authentication mechanism	Not available
Public channel	Yes
Pre-established secrets known to parties	No
Impersonation attack resilience	Not available
Theory foundation	Chaos synchronization
Key-compromise imporsonation resilience	Not available
Guessing attack resilience	Available
Perfect forward secrecy	Not available
Known key security	Yes
Unknown key-share resilience	Available
Denial-of-service attack resilience	Available
Static private keys	No
Ephemeral private keys	Yes
Regularly following attack resilience	Available
Embedded signal attack resilience	Available

Remark. In the above table, 'not available' denotes the KMKW key exchange protocol does not support authentication mechanism, impersonation attack resilience, key-compromise impersonation resilience and perfect forward secrecy. 'yes' means the KMKW key exchange protocol has the corresponding security properties or parameters. 'available' denotes the KMKW key exchange protocol supports the corresponding security attributes. 'no' means the KMKW key exchange protocol does not have the corresponding security properties or parameters.

5. Conclusions

The idea of Klein et al.'s key exchange (key agreement) is novel. However, there are several security issues need to address before it can be used in practice. Therefore, it is still an open problem to design a public channel key agreement protocol using chaotic dynamics that are mutually coupled and undergo a synchronization process, which can meet the security requirements reported in this paper.

Acknowledgements

The authors thank the anonymous referees for their recommendation. This work is supported in part by the grants from the CBS and Curtin Research Office at Curtin University of Technology.

References

[1] Public-key Standard, IEEE P1363.
[2] Addabbo T et al. A feedback strategy to improve the entropy of a chao-based random bit generator. IEEE Trans Circ Syst I 2006;53(2):326–37.
[3] Alvarez G, Montoya F, et al. Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value. Chaos, Solitons & Fractals 2005;23(5):1749–56.
[4] Li Z, Xu D. A secure communication scheme using projective chaos synchronization. Chaos, Solitons & Fractals 2004;22(2):477–81.
[5] Tan XH, Zhang JY, Yang YR. Synchronization chaotic systems using backstepping design. Chaos, Solitons & Fractals 2003;16(1):37C45.
[6] Han S, Chang E. Chaotic map based key agreement with/out clock synchronization. Chaos, Solitons & Fractals. 2007, doi:10.1016/j.chaos.2007.06.030.
[7] Cuomo KM, Oppenheim A, Strogatz SH. Synchronization of Lorenz-based chaotic circuits with applications to communications. IEEE Trans Circ Syst II Analog Digit Signal Process 1993;40(10):626–33.
[8] Huang F, Guan Z. Cryptosystem using chaotic keys. Chaos, Solitons & Fractals 2005;23(3):851–5.

Please cite this article in press as: Han S et al., Identifying attributes and insecurity of a public-channel key ..., Chaos, Solitons & Fractals (2007), doi:10.1016/j.chaos.2007.10.050

[9] Kocarev L, Tasev Z. Public-key encryption based on chevyshev maps. In: Proceedings of the IEEE international symposium on circuits and systems, ISCAS 2003;3:28–31.
[10] Lei M, Meng G, Feng Z. Security analysis of chaotic communication systems based on Volterra-Wiener-Korenberg model. Chaos, Solitons & Fractals 2006;28(1):264–70.
[11] Hyang L, Wang M, Feng RP. Synchronization of generalized Henon map via backstepping design. Chaos, Solitons & Fractals 2005;23(2):617–20.
[12] Menezes A, Qu M, Vanstone S. In: Proceedings of workshops on selected areas in cryptography, 1995.
[13] Wei J, Liao X, Wong KW, Xiang T. A new chaotic cryptosystem. Chaos, Solitons & Fractals 2006;30(5):1143–52.
[14] Alvarez G, Montoya F, et al. Phys Lett A 2004;326:211.
[15] Pecora LM, Carroll TL. Synchronization in chaotic systems. Phys Rev Lett 1990;64(8):821–4.
[16] Han S. Security of a key agreement protocol based on chaotic maps. Chaos, Solitons & Fractals. 2007, doi:10.1016/j.chaos.2007.01.017.
[17] Klein E, Mislovaty R, Kanter I, Kinzel W. Public-channel cryptography using chaos synchronization. Phys Rev E 2005;72:016214.
[18] Pecora LM, Carroll TL. Circuit implementation of synchronized chaos with applications to communications. Phys Rev Lett 1993;71(65):65–8.
[19] Zheng B, Chen M, Zhou D. Chaotic secure communication based on particle filtering. Chaos, Solitons & Fractals 2006;30:1273–80.
[20] Menezes A, Oorschot P, Vanstone S. Handbook of applied cryptography. Boca Raton: CRC Press; 1997.
[21] Li C, Li S, Alvarez G, Chen G, Lo KT. Cryptanalysis of a chaotic block cipher with external key and its improved version. Chaos, Solitons & Fractals. 2006, doi:10.1016/j.chaos.2006.08.025.
[22] Feki M. An adaptive chaos synchronization scheme applied to secure communication. Chaos, Solitons & Fractals 2003;18:141–8.
[23] Carroll TL, Pecora M. Synchronizing chaotic circuits. IEEE Trans Circ Syst I Regular Papers 1991;38:453–6.
[24] Wong K. A fast chaotic cryptographic scheme with dynamic look-up table. Phys Lett A 2002;298:238–42.

Please cite this article in press as: Han S et al., Identifying attributes and insecurity of a public-channel key ..., Chaos, Solitons & Fractals (2007), doi:10.1016/j.chaos.2007.10.050