A Novel Biometric-based Authentication Scheme with Privacy Protection

Li Huixian
School of Computer Science and Engineering
Northwestern Polytechnical University
Xi'an, China
e-mail: lihuixian@nwpu.edu.cn

Pang Liaojun
The Ministry of Education Key Lab. of Comput.
Networks and Information Security, Xidian University
Xi'an, China
e-mail: ljpang@mail.xidian.edu.cn

Abstract—**Since biometric data are unique and permanent characteristics of individuals, the privacy protection of biometric authentication schemes has become a common concern of the public. Recently, Tang et al. proposed a biometric-based authentication scheme in an attempt to solve the privacy concerns. However, their scheme cannot resist the attack of tamper. Motivated by these concerns, in this paper, we proposed a new biometric-based authentication scheme, which achieves identity privacy and transaction untraceability.. Its security is based on the semantic security of the ElGamal algorithm. Analysis results show that our scheme is higher in efficiency than Tang et al. scheme does, and meanwhile, it can resist the tamper attack. It is concluded that the proposed scheme is more secure and more practical than the existing ones.**

Keywords-biometric-based authentication; privacy protection; untraceability; tamper attack

I. INTRODUCTION

Biometric-based authentication is the automatic identity verification, based on individual physiological or behavioural characteristics, such as fingerprints, voice, face and iris. Since biometrics is extremely difficult to forge and cannot be forgotten or stolen, Biometric authentication offers a convenient, accurate, irreplaceable and high secure alternative for an individual, which makes it has advantages over traditional cryptography-based authentication schemes. It has become a hot interdisciplinary topic involving biometric and Cryptography [1].

Biometric data is personal privacy information, which uniquely and permanently associated with a person and cannot be replaced like passwords or keys. Once an adversary compromises the biometric data of a user, the data is lost forever, which may lead to a huge financial loss. Hence, one major concern is how a person's biometric data, once collected, can be protected. Another concern is that if the same type biometric data of a user is used to register in different applications, there is an inevitable link for the user's activities in these applications. That is to say, the user's activities may be tracked from one application to the next by cross-matching biometric databases [2].

So the privacy protection of biometric data has become a common concern of the public. To some extent, the privacy problem affects the degree of approval of the biometric authentication [3]. How this problem can be solved has become one of challenges in biometric-based authentication.

II. RELATED WORKS

Currently, there are many works which deal with privacy protection of biometric data in biometric-based authentication schemes. Dodis et al. [4] proposed the secure sketch scheme to protect biometric template. In their scheme, a biometric template is used to produce secure auxiliary data Pub which reveals no useful information about the template. In the verification phase, the secret key can be recovered given the capturing fresh biometric data and Pub together. However, Boyen et al. [5] pointed out that secure sketch schemes are secure only under the passive adversary model. If an adversary can replay any message of the protocol, the authentication is not secure. Ratha et al. [2] proposed the concept of the cancelable biometrics in an attempt to solve the revocation of biometric information. They used some one-way function to transform the original biometric data, and the transformed biometric template is stored in a database. If the transformed template is stolen, a new transformed template can be produced only using another transformation function. But in this method, users need to protect a secret parameter, which violates the original intent of easy key management for biometric-based authentication.

The above methods are focused on the security of biometric templates. However, just as Tang et al. [6] said, "privacy may mean much more than the adversary cannot recover the user's biometric template". Recently, Bringer et al. [7] proposed a biometric-based authentication scheme by exploiting Goldwasser-Micali and Paillier cryptosystems in order to protect the sensitive relationship between a biometric feature and relevant pseudorandom user names. But their scheme needs Hardware Security Module HSM to store the secret keys which increases the cost of realization. In [6], Tang et al. proposed a biometric-based remote authentication scheme, which attempt to solve the identity privacy and transaction anonymity. But this scheme is not secure because it cannot resist the temper attack (this will be analyzed in the section IV).

In this paper, we improve Tang et al.'s scheme and present a new biometric-based authentication scheme. The new proposed scheme can not only protect the identity privacy and transaction anonymity but also resist the temper attack.

978-0-7695-3744-3/09 $25.00 © 2009 IEEE
DOI 10.1109/IAS.2009.304

The rest of the paper is organized as follows. In section 3 we describe the security model for biometric-based authentication. In section 4 we review Tang et al.'s scheme and analyze its security problem. In section 5 we propose a new biometric-based authentication scheme. In section 6 we analyze the security of the proposed scheme. Section 7 concludes the paper.

III. Preliminary Definitions

A. *Biometric System Structure*

In our scheme, following the ideas of [6], the system structure of biometric-based remote authentication is described as in figure 1.

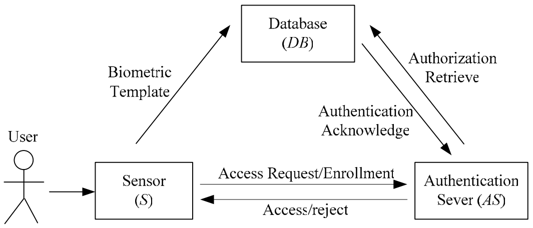

Figure 1. System structure of biometric-based authentication.

The system structure includes the following four types of components:

- Human user, who use his biometric feature to authenticate himself to an authentication server.
- Sensor client *S*, which captures the raw biometric data and extracts a biometric template, and communicates with the service provider.
- Authentication server *AS*, which stores username identifiers and deals with the human user's authentication by querying the database.
- Database *DB*, which stores the biometric information for users.

Different from traditional structure, where the authentiction server dominates the database, the database is assumed to be independent from the authentication server to protect the user's privacy against a malicious server or a malicious database.

B. *Assumptions*

We make the following assumptions.

Assumption 1. Liveness assumption. We assume that, with a high probability, the biometric template captured by the sensor and used in the system is from a living human user. In other words, it is difficult to produce a fake biometric template that can be accepted by the sensor.

Assumption 2. Honest sensor client assumption. We assume that the sensor client is always honest and trusted by all other components, which can extend the liveness assumption from the sensor to its environment.

Assumption 3. Outside adversary assumption. With respect to the authentication service, authentication server is trusted by human users to make the right decision, and database is trusted by human users and the authentication server to store and provide the right biometric information. Only an outside adversary may try to impersonate an honest human user.

Assumption 4. Non-colluding assumption. With respect to privacy concerns, both authentication server and database are assumed to be malicious which means they may deviate from the protocol specification, but they will not collude. In reality, an outside adversary may also pose threats to the privacy concerns, however, it has no more advantage than a malicious system component.

C. *Security Model*

The security requirements [8] of the biometric-based authentication scheme that we want to achieve are the following:

(1) *Privacy*: None of the component (and no passive attacker observing communications) gets enough information to reconstruct an identity/biometric feature pair. More precisely, none of the component can distinguish whether a particular measurement belongs to a particular person.

This privacy attribute implies that, for any personal username, the adversary knows nothing about the corresponding biometric information. It also assures that, if the same person has several enrollments, the adversary cannot find any linkability between these enrollments.

(2) *Untraceability*: Except for the authentication server, none of the other component (and no passive attacker observing communications) gets enough information to recognize a previously authenticated user. More precisely, the database cannot distinguish whether two authentication requests belong to the same person.

The untraceability attribute means that, for every query issued by the authentication server, a malicious database knows nothing about which user is authenticating himself to the authentication server.

IV. Review of Tang et al.'s Scheme

In this section, we will introduce Tang et al.'s scheme briefly, and then analyze its security.

A. *Tang et al.'s Scheme*

This scheme includes two phases.

1) *Enrollment phase:*

The parameters are listed below:

– *C*(Sensor)'s key pair: (pk_c, sk_c),
– *DB*(Database)'s ElGamal key pair: (pk_{db}, sk_{db}),
– *S*(Service provider)'s ElGamal key pair: (pk_s, sk_s),
– User U_i's username: ID_i,
– U_i's reference biometric template: b_i,
– U_i's sketch: $sketch_i$ = SS(b_i).

Here, *pk* denotes the public key, and *sk* denotes the secret key. The generator of the ElGamal algorithm is g_s.

U_i registers ID_i at *S*, and registers B_i at *DB*, where B_i = $\text{Enc}((g_s)^{ID_s \| ID_i \| b_i}, pk_s)$ = (B_{i1}, B_{i2}).

2) *Verification phase*

a) C extracts U_i's biometric template b_i^* and computes $b_i' = \mathrm{Rec}(b_i^*, sketch_i)$. If $\mathrm{H}(b_i^*, b_i') \le \lambda$, C sends *(ID_i, M_{i1}, M_{i2}, σ_i)* to *S,* where

$$X_i = \mathrm{Enc}((g_s)^{ID_s \| ID_i \| b_i'}, pk_s),$$
$$M_{i1} = \mathrm{Enc}(X_{i1}, pk_{db}),\ M_{i2} = \mathrm{Enc}(X_{i2}, pk_{db}),$$
$$\sigma_i = \mathrm{Sign}(ID_s \| M_{i1} \| M_{i2}, sk_c).$$

Otherwise, *C* aborts the operation.

b) *S* gets the index *i* for *ID_i*, and forwards *(M_{i1}, M_{i2}, σ_i)* to *DB*.

c) *DB* verifies the signature σ_i. If the verification succeeds, *DB* decrypts M_{i1}, M_{i2} to X_i. For every 1≤*l*≤*N*, *DB* randomly selects $s_t \in \mathbb{Z}_{q_s}$ and computes

$$R_t = (X_i \varnothing B_l)^{s_t} = ((X_{i1}/B_{l1})^{s_t}, (X_{i2}/B_{l2})^{s_t}).$$

d) *S* runs a PIR protocol to retrieve R_i. If *Dec(R_i, sk_s)* = 1, *S* accepts the request; otherwise rejects it.

B. Security Analysis

In Tang et al.'s scheme, an adversary can pass verification by tempering the related R_i to be the ElGamal ciphertext corresponding to the plaintext 1. In the following, we give an explanation of this problem.

In the step *c)* of the above verification process, B_l and X_i are ElGamal ciphertexts. Let k_l is the selected random number for B_l and $P_l = (g_s)^{ID_s \| ID_l \| b_l}$. According to the ElGamal algorithm, we have $B_l = (B_{l1}, B_{l2}) = (g_s^{k_l}, P_l \cdot pk_s^{k_l})$. Let k_i is the selected random number for X_i and $P' = (g_s)^{ID_s \| ID_i \| b_i'}$, and according to the ElGamal algorithm, we get $X_i = (X_{i1}, X_{i2}) = (g_s^{k_i}, P_i' \cdot pk_s^{k_i})$. From B_l and X_i, we rewrite R_t as follows:

$$\begin{aligned} R_t &= (X_i \varnothing B_l)^{s_t} \\ &= ((X_{i1}/B_{l1})^{s_t}, (X_{i2}/B_{l2})^{s_t}) \\ &= ((g_s^{k_i}/g_s^{k_l})^{s_t}, (P_i' \cdot pk_s^{k_i}/P_l \cdot pk_s^{k_l})^{s_t}) \\ &= (g_s^{(k_i-k_l)\cdot s_t}, (P_i'/P_l)^{s_t} \cdot pk_s^{(k_i-k_l)\cdot s_t}) \\ &\overset{\text{Let } r=(k_i-k_l)\cdot s_t}{=} (g_s^r, (P_i'/P_l)^{s_t} \cdot pk_s^r). \end{aligned}$$

It is obvious that R_t is the ElGamal encryption result of the plaintext $(P_i'/P_l)^{s_t}$ with a random number $r = (k_i - k_l) \cdot s_t$. If $(P_i'/P_l)^{s_t} = 1$, the verification succeeds. However, since pk_s is public and *r* is a random number, the encryption result of 1 is easy to construct. That is to say, even if an adversary has not the biometric template of user U_i, it can pass the verification by modifying R_i or all R_l(1≤*l*≤*N*) to be ElGamal encryption results of the plaintext 1.

V. The Proposed Scheme

A. Description of The Proposed Scheme

In this section, based on the ElGamal scheme, we propose a new biometric-based authentication scheme with privacy protection. This scheme is consists of two phases also: enrollment phase and verification phase. Then we will describe these phases in details.

1) Enrollment phase

Every component in figure 1 initializes its parameters as follows.

– *S*(Sensor) produces a key pair (pk_s, sk_s) for a signature scheme (Sig, Ver), and publishes pk_s.

– *DB* generates an Elgamal key pair (pk_{db}, sk_{db}), where $pk_{db} = (\mathbb{G}_q, g, y_{db})$, $y_{db} = g^{x_{db}}$, and $sk_{db} = x_{db}$, and publish pk_{db}.

– *AS*(Authentication Server) generates an Elgamal key pair (pk_{as}, sk_{as}), where $pk_{as} = (\mathbb{G}_q, g, y_{as})$, $y_{as} = g^{x_{as}}$, and $sk_{as} = x_{as}$, and publishes pk_{as}.

– U_i chooses his username ID_i and registers it at authentication server *AS*. U_i chooses a secret number c_i randomly, and computes $d_i = c_i + ID_{as} \| ID_i \| b_i$, where b_i is U_i's reference biometric template. Then U_i registers W_i at *AS*, and B_i at *DB*, where

$$W_i = \mathrm{Enc}(g^{c_i}, pk_{as}) = (W_{i1}, W_{i2}),$$
$$B_i = \mathrm{Enc}(g^{d_i}, pk_{as}) = (B_{i1}, B_{i2}).$$

2) Verification phase

In verification phase, any user U_i can start an authentication session to the authentication server. The steps are as follows:

a) *S* extracts U_i's fresh biometric feature b_i^* and sends (ID_i, M_{i1}, M_{i2}, σ_i) to *S*, where

$$X_i = \mathrm{Enc}((g)^{ID_s \| ID_i \| b_i^*}, pk_{as}),$$
$$M_{i1} = \mathrm{Enc}(X_{i1}, pk_{db}), M_{i2} = \mathrm{Enc}(X_{i2}, pk_{db}),$$
$$\sigma_i = \mathrm{Sig}(ID_{as} \| M_{i1} \| M_{i2}, sk_s).$$

b) Authentication server A*S* gets the index *i* for ID_i, and forwards (M_{i1}, M_{i2}, σ_i) to *DB*.

c) *DB* verifies the signature σ_i. If the verification succeeds, *DB* decrypts M_{i1}, M_{i2} to X_i. For every 1≤*l*≤*N*(*N* is the number of users), *DB* computes

$$R_l = (B_l \varnothing X_i) = ((B_{l1}/X_{i1}), (B_{l2}/X_{i2})).$$

d) A*S* runs a PIR protocol to retrieve R_i. Then *AS* decrypts R_i and W_i separately, and compares the results. If Dec(R_i, sk_{as}) = Dec(W_i, sk_{as}), *AS* accepts the request; otherwise rejects it.

B. Remarks on Performance

Subsequently, we give a simple remark on the performance of the proposed scheme. First, we investigate the computational complexity. In our scheme, modular exponentiations are the most time-consuming operations. *DB* performs one exponentiations (decrypt M_{i1}, M_{i2} to X_i) in the proposed scheme, however, in Tang et al. scheme *DB* performs $O(N+1)$ exponentiations (here, one exponentiations refers to decrypting M_{i1}, M_{i2} to X_i). Obviously, the quantity of computation of *DB* is reduced largely in our scheme. The sensor client *S* needs to perform 6 exponentiations and sign one message for each authentication request, which is the same as that in Tang et al. scheme. The authentication server *AS* needs to conduct two exponentiations (decrypt two message), which is only one more exponentiation than that of service provider *SP* in Tang et al. scheme. To sum up, our scheme is $N-1$ exponentiations less than Tang et al. scheme. So the proposed scheme is high in efficiency. In addition, the communication complexity of the proposed scheme is dominated by the PIR protocol [9].

VI. Security Analysis of the Proposed Scheme

The proposed scheme has the same advantages as those of Tang et al.'s scheme, that is, it achieves identity privacy against malicious authentication server and transaction untraceability against malicious data base, based on the semantic security of the ElGamal scheme. What's more, the new one can resist the tamper attack of adversary, which will be shown by the following theory.

Theory 1. The proposed scheme can prevent an adversary from tampering R_i (computed by *DB*).

Proof: First, Let r_l and r_i are the selected random numbers for B_l and X_i, respectively, and we have

$$B_l = (B_{l1}, B_{l2}) = (g^{r_l}, g^{d_l} \cdot pk_{as}^{r_l}),$$

$$X_i = (X_{i1}, X_{i2}) = (g^{r_i}, g^{ID_{as}\|ID_i\|b_i^*} \cdot pk_{as}^{r_i}).$$

We rewrite R_l as

$$\begin{aligned} R_l &= (B_l \varnothing X_i) \\ &= ((B_{l1}/X_{i1}), (B_{l2}/X_{i2})) \\ &= ((g^{r_l}/g^{r_i}), (g^{d_l} \cdot pk_{as}^{r_l}) / (g^{ID_{as}\|ID_i\|b_i^*} \cdot pk_{as}^{r_i})) \\ &= (g^{(r_l - r_i)}, g^{(d_l - ID_{as}\|ID_i\|b_i^*)} \cdot pk_{as}^{(r_l - r_i)}) \\ &\overset{\text{Let } v = r_l - r_i}{=} (g^{v}, g^{(d_l - ID_{as}\|ID_i\|b_i^*)} \cdot pk_{as}^{v}). \end{aligned}$$

Obviously, $g^{(d_l - ID_{as}\|ID_i\|b_i^*)}$ is the decryption result of R_l. That we judge whether Dec(R_i, sk_{as}) = Dec(W_i, sk_{as}), in fact, is to decide whether $g^{(d_i - ID_{as}\|ID_i\|b_i^*)} = g^{c_i}$. If an adversary wants to pass verification by tampering R_i, he needs to know the value of g^{c_i} . He can try to get it from decrypting W_i, however, this will face the difficulty of breaking the ElGamal scheme. So the temper attack cannot success in the proposed scheme.

VII. Conclusions

In this paper we have pointed out that Tang et al.'s scheme is not secure and cannot resist the tamper attack, and proposed a new biometric-based authentication scheme. The proposed one considers the security and privacy for biometric data, and achieves identity privacy and transaction untraceability. Analysis results show that our scheme is higher in efficiency than Tang et al. scheme does, and meanwhile, it can resist the tamper attack. So the proposed scheme is more secure and more practical than the available ones do.

Acknowledgment

This work was partially supported by the National Natural Science Foundation of China under Grant No. 60803151, the Key Program of NSFC-Guangdong Union Foundation of China under Grant No.U0835004, NPU Foundation for Fundamental Research under Grant No. NPU-FFR-JC200819, NPU "Aoxiang Star" program, the Open Foundation of the Key Laboratory of Network and Information Security in Xidian University, Ministry of Education of China under Grant No. 2008CNIS- 07, the Natural Science Foundation of Shannxi Province under Grant No. 2007F37, and the National Science Foundation for Post-doctoral Scientists of China under Grant No. 20070410376.

References

[1] A.K. Jain, "Biometric Recognition", Nature, vol. 449, Sep. 2007, pp. 38-40, doi:10.1038/449038a.

[2] K. Nalini, R.S. Chikkerur, H.C. Jonathan, et al, "Generating Cancelable Fingerprint Templates", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, Apr. 2007, pp. 561-572, doi:10.1109/TPAMI.2007.1004.

[3] A. Watson, "Biometrics: Easy to Steal, Hard to Regain Identity", Nature, vol. 449, Oct. 2007, pp. 535, doi:10.1038/449535b.

[4] Y. Dodis, R. Ostrovsky, L. Reyzin, et al, "Fuzzy Extractor: How to Generate Strong Keys from Biometrics and Other Noisy Data", SIAM Journal on Computing, vol. 38, Mar. 2008, pp. 97-139, doi: 10.1137/060651380.

[5] X. Boyen, Y. Dodis, J. Katz, et al, "Secure Remote Authentication Using Biometric Data", Proc. of EUROCRYPT'05, LNCS 3494, Springer, Heidelberg, May 2005, pp. 147-163, doi: 10.1007/11426639_9.

[6] Q. Tang, J. Bringer, H. Chabanne, et al, "A Formal Study of the Privacy Concerns in Biometric-based Remote Authentication Schemes", Proc. of ISPEC'08, LNCS 4991. Sydney, Australia. Springer, Heidelberg, Mar. 2008, pp. 56-70, doi: 10.1007/978-3-540-79104-1_5.

[7] J. Bringer, H. Chabanne, "An Authentication Protocol with Encrypted Biometric Data", Proc. of AFRICACRYPT'08, LNCS 5023. Springer, Heidelberg, May 2008, pp.109-124, doi: 10.1007/978-3-540-68164-9_8.

[8] M. Barbosa, S. Cauchy, T. Brouard and S. Melo de Sousa, "Secure Biometric Authentication with Improved Accuracy", Proc. of the 13th Australasian conference on Information Security and Privacy, LNCS 5107, Springer Berlin, Heidelberg, Jun. 2008, pp. 21-36, doi: 10.1007/978-3-540-70500-0_3.

[9] C. Gentry, Z. Ramzan, "Single-database Private Information Retrieval with Constant Communication Rate", Proc. of 32nd International Colloquium on Automata, Languages and Programming, Springer, Berlin, Nov. 2005, pp. 803-815, doi: 10.1007/11523468.