Research Article

A Novel Verifiable Multisecret Sharing Scheme in Wireless Multimedia Sensor Networks

Xianfeng Guo¹ and Qing Luo²

¹ College of Computer Science and Technology, Southwest University for Nationalities, Chengdu 610041, China
² Sichuan Conservatory of Music, Chengdu 610021, China

Correspondence should be addressed to Xianfeng Guo; guoxianf@126.com

Received 25 January 2013; Accepted 9 April 2013

Academic Editor: Muhammad Khurram Khan

Copyright © 2013 X. Guo and Q. Luo. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper presents a secure and practical verifiable multi-secret sharing scheme with application on multimedia sensor networks. By utilizing the merits of biometric cryptography, the proposed scheme can reliably conceal private information and overcome the shortcoming of the traditional cryptography. Security analysis shows that the proposed scheme provides secure, robust, and trustworthy verification of dealer and participants over insecure wireless multimedia sensor networks.

1. Introduction

Wireless multimedia sensor networks (WMSNs) have started to receive a lot of attention very recently due to their potential to be deployed flexibly in various applications with lower costs [1, 2]. As WMSNs are widely deployed in remote and hostile environments to transmit sensitive information by broadcast, sensor nodes are prone to node compromise attacks and security issues such as data confidentiality and integrity are extremely important. Hence, security becomes a very serious concern in WMSNs protocols. But unfortunately sensor nodes have limited power, computation, storage, and communication capabilities; they impose several constraints on the algorithm and protocol that can be effectively deployed for such systems. In this scenario, most of the traditional security mechanisms are useless. Thus, the research of new efficient security techniques is needed [3–5].

In order to keep the secret efficiently and safely, in 1979, Shamir [6] and Blakley [7] first developed the concepts of the secret sharing (SS) scheme, respectively. In such a scheme, the dealer splits the secret into shares among participants, and sends the share to the corresponding participant. As a result, any t out of the n participants can cooperate to resume the secret, but any less than t out of the n participants cannot get any useful information about the secret by any way. A threshold secret sharing scheme has many practical applications, such as opening a bank vault, launching a nuclear, or authenticating an electronic funds transfer. Later, several multisecret sharing schemes were proposed [8–12]. In a multisecret sharing scheme, there are multiple secrets to be shared during one secret sharing process. In 2004, Yang et al. (YCH) [13] proposed a novel multisecret sharing (MSS) scheme, which is based on a two-variable one-way function. Besides efficient computation for practice, the scheme has the following merits: (1) several secrets can be shared during one secret sharing process; (2) the dealer need not redistributes a fresh shadow after the secrets have been reconstructed. But YCH scheme does not have the property of verification. That is to say, neither dealer nor participants cheating can be detected. As for dealer cheating, the dishonest dealer can prevent any certain participant from obtaining the true secret by distributing a fake shadow to him/her [14]; and the participants cheating, a malicious participant may provide a fake shadow to other participants, which makes the malicious participant the only one who gets to reconstruct the true secret [15]. In a secret sharing involving multiple dealers, the property of verifiability is more desirable since these dealers are mutually distrusted.

In 2005, Shao and Cao (SC) [16] proposed a verifiable multisecret sharing (VMSS) based on YCH and the intractability of the discrete logarithm. However, the speed of SC scheme is not competitive [17]. In 2007, Zhao et al.
(ZZZ) [18] proposed another practical VMSS based on YCH. ZZZ scheme perform the verification phase by utilizing RSA cryptosystem and a Diffie-Helman key agreement method. Though ZZZ scheme significantly reduced the computation costs of the whole system, it is required that the dealer reconstructs a RSA cryptosystem once the secrets have been reconstructed. Later on, Dehkordi and Mashhadi (DM) [17] proposed an efficient VMSS scheme to improve the performance of SC scheme. Compared to ZZZ scheme, DM scheme just constructs one RSA cryptosystem in the whole system and the dealer verification is not required. But any participant has to compute \( t - 1 \) modular exponential computing to verify others’ secret shadow. It is still very time-consuming. In addition, it is difficult to protect private keys from attackers in the password-based verification system [19].

To overcome the drawback and pitfall of only-password-based verification of YCH scheme, in this paper, we present an efficient and practical VMSS by using biometric data, for example, palmprint, with application on wireless multimedia sensor networks. In the verification phase of the proposed scheme, the time consuming modular exponentiation computations, for example, Diffie-Helman or RSA, are eliminated. This scheme allows participants and dealer to cooperate in choosing secret shadows. It can effectively perform dealer and participants’ verification. Moreover, the computation cost, security, and efficiency of the presented scheme are embarking for the real application in the practical environment.

Rest of the paper is organized as follows: Section 2 briefly reviews YCH scheme. Section 3 presents the efficient and practical palmprint-based VMSS scheme with application on wireless multimedia sensor networks. Section 4 performs performance analysis of the proposed scheme. Conclusions are given in Section 5.

### 2. Review of YCH Schemes

Function \( f(r, x) \) denotes any two-variable one-way Hash function and \((P_1, P_2, \ldots, P_k)\) denotes \( k \) secrets to be shared among \( n \) participants. Before the secret sharing, the dealer randomly chooses \( n \) secret shadows \( s_1, s_2, \ldots, s_n \) and distributes them to every participant over a secret channel. Then the dealer performs the following steps.

#### (2.1) If \( k \leq t \).

(a) Choose a big prime \( Q \) and construct \((k - 1)\)th degree polynomial \( h(x) \) mod \( Q \):

\[
h(x) = P_1 + P_2 x + \cdots + P_k x^{k-1} + a_1 x^k + a_2 x^{k+1} + \cdots + a_{k-1} x^{2k-1} \mod Q,
\]

where \( 0 < P_1, P_2, \ldots, P_k, a_1, a_2, \ldots, a_{k-1} < Q \).

(b) Compute \( y_i = h(f(r, s_j)) \mod Q \) for \( i = 1, 2, \ldots, n \).

(c) Publish \((r, y_1, y_2, \ldots, y_n)\).

#### (2.2) If \( k > t \).

(a) Choose a big prime \( Q \) and construct \((k - 1)\)th degree polynomial \( h(x) \) mod \( Q \):

\[
h(x) = P_1 + P_2 x + \cdots + P_k x^{k-1} \mod Q,
\]

where \( 0 < P_1, P_2, \ldots, P_k < Q \).

(b) Compute \( y_i = h(f(r, s_j)) \mod Q \) for \( i = 1, 2, \ldots, n \).

(c) Compute \( h(i) \mod Q \) for \( i = 1, 2, \ldots, k - t \).

(d) Publish \((r, y_1, y_2, \ldots, y_n, h(1), h(2), \ldots, h(k - t))\).

If at least \( t \) participants pool their pseudo shadows \( f(r, s_j) \) for \( i = 1, 2, \ldots, t \), then the polynomial \( h(x) \mod Q \) can be uniquely determined as follows.

1. If \( k \leq t \)

\[
h(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} (x - f(r, s_j)) \mod Q
\]

\[
= P_1 + P_2 x + \cdots + P_k x^{k-1} + a_1 x^k + a_2 x^{k+1} + \cdots + a_{k-1} x^{2k-1} \mod Q.
\]

2. If \( k > t \)

\[
h(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} (x - f(r, s_j)) \mod Q
\]

\[
\times \prod_{l=1, l \neq f(r, s_j)}^{k-t} (x - l) \mod Q
\]

\[
+ \sum_{i=1}^{k-t} h(i) \prod_{j=1, j \neq i}^{k-t} (x - l) \mod Q
\]

\[
\times \prod_{l=1, l \neq f(r, s_j)}^{t} (x - f(r, s_j)) \mod Q
\]

\[
= P_1 + P_2 x + \cdots + P_k x^{k-1} \mod Q.
\]

Then the shared secrets \( P_1, P_2, \ldots, P_k \) are recovered.

### 3. The Proposed Palmprint-Based VMSS Scheme

In this section we will propose a new palmprint-based VMSS scheme with application on wireless multimedia sensor networks. The verification is based on matching of the palmprint template. The notations \((P_1, P_2, \ldots, P_k)\) and \( f(r, x) \) in this scheme are the same as those of Section 2. Define \( D \) and \( M = \{M_i\}_{i=1}^n \) are dealer (Server) and set of participants respectively.
3.1. Architecture of Wireless Multimedia Sensor Networks. Figure 1 shows the developed architecture of the secure wireless multimedia sensor networks by utilizing the proposed biometric based VMSS. Each camera sensor node in the networks is battery-powered and has limited computation and wireless communication capabilities. The sink is a data collection and storage center equipped with sufficient computation and storage capabilities. Camera sensor nodes periodically send the captured images to the sink node. Then the sink nodes transport this information secretly with the data processor via carrier networks. The proposed scheme is mounting among the sink nodes.

3.2. Initialization Phase. Figure 2 shows an overall flowchart of the initialization phase. For $i = 1, 2, \ldots, n$ participant $M_i$ first randomly chooses his private key $s'_i$ and submits to the dealer $D$. $M_i$ also imprints his palmprint image at the camera sensor nodes, and then initialization system performs the following operations.

1. Dealer $D$ randomly chooses a corresponding secret shadow $s_i$ and computes $f(s'_i, s_i)$.

2. Write $M_i$, $B_i$ and $V_i = f(s'_i, s_i) \oplus B_i$ into the memory of the corresponding sink node, where $B_i$ is the palmprint template of $M_i$. For more details on calculate $V_i = f(s'_i, s_i) \oplus B_i$, the reader can refer to [20].

3.3. Construction Phase. The dealer $D$ chooses a random number $r$ and performs the following steps.

1. If $k \leq t$.
   
   a. Chooses a big prime $Q$ and constructs $(t-1)$th degree polynomial $h(x)$ mod $Q$:
   
   \[
   h(x) = P_1 + P_2 x + \cdots + P_k x^{k-1} + a_1 x^k + a_2 x^{k+1} + \cdots + a_{t-k} x^{t-1} \mod Q,
   \]
   
   where $0 < P_1, P_2, \ldots, P_k, a_1, a_2, \ldots, a_{t-k} < Q$.

   b. Compute $y_i = h(f(r, f(s'_i, s_i))) \mod Q$ for $i = 1, 2, \ldots, n$.

   c. Publish $(r, y_1, y_2, \ldots, y_n)$.

2. If $k > t$.
   
   a. Choose a big prime $Q$ and construct $(k-1)$th degree polynomial $h(x)$ mod $Q$:
   
   \[
   h(x) = P_1 + P_2 x + \cdots + P_k x^{k-1} \mod Q,
   \]
   
   where $0 < P_1, P_2, \ldots, P_k < Q$.

   b. Compute $y_i = h(f(r, f(s'_i, s_i))) \mod Q$ for $i = 1, 2, \ldots, n$.

   c. Compute $h(\ell) \mod Q$ for $i = 1, 2, \ldots, k-t$.

   d. Publish $(r, y_1, y_2, \ldots, y_n, h(1), h(2), \ldots, h(k-t))$.

3.4. Verification Phase. By utilizing the published $r$ and the secret shadow $s_i$, each participant $\{M_i\}_{i=1}^n$ can compute his secret share $f(r, f(s'_i, s_i))$. If participants $\{M_i\}_{i=1}^t$ pool their shares $f(r, f(s'_i, s_i))$ and identity $M_i$, dealer $D$ can perform the following verifications.

   Computes $f(r, f(s'_i, s_i))$ and compares $f(r, f(s'_i, s_i)) = f(r, f(s'_i, s_i))$. If they are equal, $D$ believes that $M_i$ is honest.

   Furthermore, $f(s'_i, s_i)$ is composed of the private key $s'_i$ of $M_i$ and the secret shadow $s_i$ of $D$, therefore the dealer verification is unnecessary.

3.5. Recovery Phase. The security of a recovery phase is based on the palprint cryptosystem. Suppose participants $\{M_i\}_{i=1}^t$ want recovery the shared secret $(P_1, P_2, \ldots, P_k)$, $M_i$ (for $i = 1, 2, \ldots, t$) imprints his palprint to the camera sensor and the recovery system performs the following operations (the framework of this phase are shown in Figure 3).

   1. By utilizing the input palprint image, generate $M_i$’s palprint template $B_i'$. 

   Figure 1: System architecture of the multimedia sensor network with VMSS.
(2) The sink node then performs matching process of $B'_i$ with $B_j$. If yes, compute $f(s'_i, s_j) = V_i \oplus B_j$ and send $(f(r, f(s'_i, s_j)), M_j)$ to the recovery system. If no, the recovery is aborted.

By utilizing the secret shadows $f(r, f(s'_i, s_j))$ (for $i = 1, 2, \ldots, t$) and the corresponding published values, the polynomial $h(x)$ mod $Q$ can be uniquely determined as follows.

(1) If $k \leq t$

$$h(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} \frac{x - f(r, s_j) - f(r, s_i)}{x - f(r, s_j)} \mod Q$$

$$= P_1 + P_2 x + \cdots + P_k x^{k-1} + a_1 x^k + a_2 x^{k+1} + \cdots + a_{k-1} x^{k-1} \mod Q. \tag{7}$$

(2) If $k > t$

$$h(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} \frac{x - f(r, s_j) - f(r, s_i)}{x - f(r, s_j)} \times \prod_{l=1, l \neq f(r,s_i)}^{k-1} \frac{x - l}{x - f(r, s_l)} \mod Q$$

$$= P_1 + P_2 x + \cdots + P_k x^{k-1} \mod Q. \tag{8}$$

Then the shared secrets $P_1, P_2, \ldots, P_k$ are recovered.

4. Performance Analysis

4.1. Security Analysis. The security of our proposed scheme is based on $(t, n)$ Shamir scheme and palmprint cryptography. In the rest of this section, some possible attacks will be raised and fought against to demonstrate the security of our scheme.

(1) If attacker Eve can use fewer points than $t$ to reconstruct the polynomial $h(x)$ mod $Q$, it is equal to Eve that has broken through the $(t, n)$ Shamir’s scheme successfully. In this point, it is infeasible to recover the secret shares of the proposed scheme by fewer points than $t$. 
(2) In this scheme, the dealer D cheating would be failed, because every secret shadow \( f(s'_i, s) \) is composed of the private key \( s'_i \) of participant \( \{M_i\}_{i=1}^n \) and the secret shadow \( s \) of D, either subtle differences of the secret will change \( f(s'_i, s) \) significantly. This is based on the sensitivity to initial condition of Hash function \( f(r, x) \).

(3) Suppose dishonest participant \( M_i \) gives a fake share \( f'(r, f(s'_i, s)) \) to prevent the shared secrets recovery, it will be detected by dealer D in verification phase. Dealer D can compare \( f(r, f(s'_i, s)) = f(r, f'(s'_i, s)) \) to insure its correctness. The security is depending on the collision-free property of chaotic Hash function \( f(r, x) \).

(4) Replay of the former round secret share \( f(r, f(s'_i, s)) \) can be exposed, because \( r \) is random selected in each round and Hash function \( f(r, x) \) is sensitivity to initial condition.

(5) Any intruder cannot get \( f(s'_i, s) \) because they cannot match the palmprint from the sensor nodes.

(6) The same as (5), the intruder cannot compute the secret share \( f(r, f(s'_i, s)) \) from the sink's data.

4.2. Computation Quality. Compared with the proposed YCH based VMSS schemes, such as DM scheme [17], ZZZ scheme [18] and SC scheme [16], the verification phase of our scheme is more efficient and suitable for using in the WMSNs. SC scheme requires some time consuming power products in the verification phase, so it is too complex to applicable on WMSNs. ZZZ scheme performs the verification phase by utilizing RSA cryptosystem and a Diffie-Helman key agreement method. It still requires \( t + 1 \) exponentiations to verify the validity of the secret shadows. And DM scheme just needs \( t - 1 \) modular exponential computing to verify others' secret shadow. The verification of our scheme is based on the collision-free one-way Hash function. Any participant requires only one chaotic Hash computation to verify his/her shadow’s validity, and \( t - 1 \) Hash computations to verify other participants’ shadows. Therefore, our scheme is more convenient for application on the WMSNs devices. Table 1 is for the comparison of these schemes.

| By          | For         | ZZZ scheme               | DM scheme               | Our scheme               |
|-------------|-------------|--------------------------|-------------------------|--------------------------|
| \( M_i \)   | Initialization | \( R_j = g^{r_i} \mod N \) | \( s'_i \mod N \)       | —                        |
| Dealer      | Construction | Construct a RSA cryptosystem | One Hash function       | One Hash function        |
| \( M_i \)   | Recovery     | \( I_i = R_i^{r_i} \mod N \) | One Hash function       | One Hash function        |
| \( M_i \)   | Verification | \( H_j^i = R_j \mod N \)_{j=1,i+j} \text{ exponents} | \( t \) Hash function   |                         |

5. Conclusion

We have proposed a novel and complete biometric-based verifiable multisecret sharing scheme with application on WMSNs. This scheme can conceal the secret shadow by palmprint cryptography and provide perfect verification. Performance analyses demonstrate it can achieve more functionality and satisfies all criteria.

Acknowledgments

This work described here was supported by the Fundamental Research Funds for the Central Universities, Southwest University for Nationalities (nos. I1NZYQ27 and I1NZYTH06), and the National Natural Science Foundation of China (no. 61105061).

References

[1] M. K. Khan and K. Alghathbar, “Cryptanalysis and security improvements of “two-factor user authentication in wireless sensor networks’’, Sensors, vol. 10, no. 3, pp. 2450–2459, 2010.
[2] X. Guo, J. Zhang, M. K. Khan, and K. Alghathbar, “Secure chaotic map based block cryptosystem with application to camera sensor networks,” Sensors, vol. 11, no. 2, pp. 1607–1619, 2011.
[3] X. He, M. Niedermeier, and H. de Meer, “Dynamic key management in wireless sensor networks: a survey,” Journal of Network and Computer Applications, vol. 36, no. 2, pp. 611–622, 2013.
[4] Q. Shi, N. Zhang, M. Merabti, and K. Kifayat, “Resource-efficient authentic key establishment in heterogeneous wireless sensor networks,” Journal of Parallel and Distributed Computing, vol. 73, no. 2, pp. 235–249, 2013.
[5] S. Qian, “A novel key pre-distribution for wireless sensor networks,” Physics Procedia, vol. 25, pp. 2183–2189, 2012.
[6] A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.
[7] G. Blakley, “Safeguarding cryptographic keys,” in Proceedings of the AFIPS National Computer Conference, pp. 313–317, AFIPS Press, 1979.
[8] C.-W. Chan and C.-C. Chang, “A scheme for threshold multisecret sharing,” Applied Mathematics and Computation, vol. 166, no. 1, pp. 1–14, 2005.
[9] Y.-F. Chen, Y.-K. Chan, C.-C. Huang, M.-H. Tsai, and Y.-P. Chu, “A multiple-level visual secret-sharing scheme without image size expansion,” Information Sciences, vol. 177, no. 21, pp. 4696–4710, 2007.
[10] H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng, “A practical \((t, n)\) multisecret sharing scheme,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 83, no. 12, pp. 2762–2765, 2000.
[11] J. He and E. Dawson, “Multisecret-sharing scheme based on one-way function,” Electronics Letters, vol. 31, no. 2, pp. 93–95, 1995.
[12] M. Liu, L. Xiao, and Z. Zhang, "Linear multi-secret sharing schemes based on multi-party computation," *Finite Fields and their Applications*, vol. 12, no. 4, pp. 704–713, 2006.

[13] C.-C. Yang, T.-Y. Chang, and M.-S. Hwang, "A (t,n) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483–490, 2004.

[14] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," in *Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science (FOCS ’85)*, pp. 251–260, 1985.

[15] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, no. 3, pp. 133–138, 1989.

[16] J. Shao and Z.-F. Cao, "A new efficient (t, n) verifiable multi-secret sharing (VMSS) based on YCH scheme," *Applied Mathematics and Computation*, vol. 168, no. 1, pp. 135–140, 2005.

[17] M. H. Dehkordi and S. Mashhadi, "An efficient threshold verifiable multi-secret sharing," *Computer Standards and Interfaces*, vol. 30, no. 3, pp. 187–190, 2008.

[18] J. Zhao, J. Zhang, and R. Zhao, "A practical verifiable multi-secret sharing scheme," *Computer Standards and Interfaces*, vol. 29, no. 1, pp. 138–141, 2007.

[19] M. K. Khan, J. Zhang, and L. Tian, "Chaotic secure content-based hidden transmission of biometric templates," *Chaos, Solitons and Fractals*, vol. 32, no. 5, pp. 1749–1759, 2007.

[20] X. Wu, K. Wang, and D. Zhang, "A cryptosystem based on palmprint feature," in *Proceedings of the 19th International Conference on Pattern Recognition (ICPR ’08)*, December 2008.
Submit your manuscripts at http://www.hindawi.com