

Key Sharing Scheme based on One Weighted Threshold Secret Sharing

SeongMin Yoo*, PyungKoo Park**, JinSeop Shin*, JaeCheol Ryou *

*Department of Computer Engineering, Chungnam National University, Daejeon, Korea

**Convergence Network Research Laboratory, ETRI, Daejeon, Korea

mingoon@home.cnu.ac.kr, parkpk@etri.re.kr, whiter1cka@gmail.com, jcryou@home.cnu.ac.kr

Abstract—Secret sharing scheme is a cryptographic technology that safely manages password keys by dividing them into segments. Existing (k, n) threshold secret sharing scheme has a problem of allowing recovery of original secret information by collecting k or more random segments among divided secret information segments. To resolve such problem, this paper proposes a one weighted threshold secret sharing scheme. That is, by granting weighted value on a secret segment, original secret information cannot be recovered by collecting k or more segments, as long as the segment applied with weighted value is not included in the collection.

Keywords—Secret Sharing, Key Management, Cryptography

I. INTRODUCTION

In cryptography, the issue of how safely a password key can be managed is as important as the cryptographic algorithm. If password key is stored in a place as a single key, it is exposed more to computer and network security vulnerabilities.

Secret sharing scheme is one of solutions to solve this problem. It is a cryptographic technology that safely maintains and manages secret information by dividing it into segments. That is, a single secret is divided into several pieces and separately stored in different places to disperse the risk to security breaches.

The most fundamental approach to secret sharing is the method proposed by Shamir[1] and Blakley[2] in 1979. Among n participants sharing secret information segments, original secret information can be restored by gathering k or more random participants. In this method, secret information cannot be restored with less than k participants. It is referred to as (k, n) threshold scheme.

(k, n) threshold scheme can restore original secret information by collecting any k segments among n secret

segments. Therefore, there is an advantage of tolerating fault when not all n segments can be collected (computer breakdown, network error) during restoration of original secret information.

However, looking from the perspective of attackers, this advantage accompanies a problem of recovering original secret information by stealing k or more random segments. Accordingly, there is a cost problem of having to manage security breaches in all places that store secret segments. The reason for such problems is because all segments of secret information have identical weight.

This paper proposes a one weighted threshold secret sharing scheme to resolve such problems. We propose a weighted threshold is given to a segment. Original secret information cannot be restored by collecting k or more segments, as long as the weighted segment is not included.

This paper is composed of the following. First, Chapter 2 explains existing (k, n) threshold schemes. Chapter 3 explains the one weighted threshold secret sharing scheme proposed in this paper. Chapter 4 conducts an estimation of the proposed method, and Chapter 5 is conclusion.

II. RELATED WORKS

Shamir proposed a (k, n) threshold scheme based on polynomial interpolation[1]. That is, if k points given on a 2-dimensional plane are known, the unique polynomial $q(x)$ with $k-1$ degrees that passes through all of these points can be determined. Secret segment is calculated from random polynomial $q(x)$. If secret information D_s is assumed as a point passing through the y -axis of a 2-dimensional plane, a random polynomial $q(x)$ with $k-1$ degrees can be determined. Also, n points passing through $q(x)$ are used as segments of secret information. When restoring original secret information D_s , k or more segments D_i must be collected. Unique polynomial

$q(x)$ is determined using lagrange interpolation. Also, original secret information D_s is calculated from the determined $q(x)$.

Blakely proposed a (k, n) threshold scheme based on geometric scheme, where k number of k -dimensional hyperplanes cross at one point[2]. That is, two straight lines not parallel on a 2-dimensional plane intersect at a point. Three planes not parallel on a 3-dimensional space also intersect at a point. Therefore in Blakely's method, secret information is the intersection of k k -dimensional hyperplanes. Segments of secret information are the union of k -dimensional hyperplanes that pass through this intersection point. Original secret information can be restored by collecting k or more k -dimensional hyperplanes and calculating their intersection.

Mignotte[3] and Asmuth-Bloom[4] each proposed a (k, n) threshold scheme based on Chinese remainder theorem. In Chinese remainder theorem, when relative prime integers $m_1, m_2, \dots, m_k$ are given, unique S modular k that satisfies $S < \prod_{i=1}^k m_i$ can be determined[0].

Using such property, m_i is generated as segments of secret information. Original secret information is restored using Chinese remainder theorem. In the methods suggested by (k, n) threshold schemes explained earlier, all segments of secret information have identical weight. Accordingly, original secret information is exposed once k or more random segments are stolen by an attacker.

In this paper, weighted threshold is granted to a segment to resolve such problem. As long as this weighted segment is not included, original secret information cannot be restored by stealing k or more segments.

III. ONE WEIGHTED THRESHOLD SECRET SHARING SCHEME

A. Decomposition of Secret Information

Decomposition process of the one weighted threshold secret sharing scheme proposed in this paper is as follows. First by assuming that secret information D_s is a point passing through the y -axis on a 2-dimensional plane, Eq. (1) can be defined by setting weighted segment D_w as a random point passing through the x -axis on a 2-dimensional plane.

$$\begin{aligned} D_s &= \{x_s, y_s\} \\ D_w &= \{x_w, y_w\} \\ \text{where, } x_s &= 0, y_w = 0 \end{aligned} \quad (1)$$

Secret information D_s and weighted segment D_w defined are used to determine random polynomial $f(x)$. The process of determining polynomial $f(x)$ is as follows. As in Eq. (2),

random polynomial $q(x)$ with $k-1$ degrees passing through secret information D_s is determined.

$$q(x) = \sum_{i=1}^{k-1} a_i x^i + a_0 \quad (2)$$

where, $a_0 = y_s, (a_1, \dots, a_{k-1})$ is random values

Then, by using weighted segment D_w , secret information D_s , and polynomial $q(x)$, random polynomial $f(x)$ with $k-1$ degrees passing through the point $\{x_w, y_s\}$ on a 2-dimensionanl plane can be determined as Eq. (3).

$$f(x) = q(x) - q(x_w) + a_0 \quad (3)$$

where, $a_0 = y_s$

Finally, $f(x)$ can be used to generate n secret segments D_i as in Eq. (4). In addition, $n+1$ segments composed of the generated segments and weighted segment D_w are dispersed and managed separately using different methods.

$$D_1 = \{1, f(1)\}, \dots, D_i = \{i, f(i)\}, \dots, D_n = \{n, f(n)\} \quad (4)$$

B. Reconstruction of Secret Information

Reconstruction process of the original secret information D_s is as follows. First, k or more secret segments D_i and weighted segment D_w are collected. Among them, k or more secret segments D_i are used to determine polynomial $f(x)$. Unique polynomial $f(x)$ with $k-1$ degrees can be determined as in Eq. (5) using lagrange interpolation[5].

$$f(x) = \sum_{j=1}^n \left[y_j \times \prod_{\substack{i=1 \\ (i \neq j)}}^n \left(\frac{x - x_i}{x_j - x_i} \right) \right] \quad (5)$$

Since the determined polynomial $f(x)$ passes through the point $\{x_w, y_s\}$ on a 2-dimensional plane, original secret information D_s can be calculated as in Eq. (6) using the weighted segment D_w .

$$D_s = \{0, f(x_w)\} \quad (6)$$

IV. ESTIMATION

A. Reasonability of Secret Share

In the one weighted threshold secret sharing scheme proposed in this paper, secret information D_s is dependent on weighted segment $D_w = \{x_w, 0\}$ and polynomial $f(x)$ because $D_s = \{0, f(x_w)\}$.

However, there is no correlation between weighted segment D_w and polynomial $f(x)$. This is because weighted segment D_w is a point on the x -axis on a 2-dimensional plane regardless of polynomial $f(x)$, and polynomial $f(x)$ can only be determined based on polynomial interpolation using k or more secret segments D_i .

Therefore, in order to find the original secret information D_s , both weighted segment D_w and unique polynomial $f(x)$ are required. Also, since the method proposed in this paper satisfies the fundamental condition of secret sharing scheme in that there is no correlation between original secret information and each segment (including weighted segment), it is a reasonable secret sharing scheme.

B. Fault Tolerance Capability

To explain fault tolerance capability of the proposed method, the degree of dependency (DoD) on segments of secret information required to restore the original secret information is defined according to the ratio of necessary segments as follows.

$$\text{DoD} = \frac{\text{Necessary segments}}{\text{Total segments}} \quad (7)$$

High dependence on segments means that more segments are needed to restore the original secret information. This means that the method becomes vulnerable to fault tolerance. Since threshold scheme was presented to resolve the problem of fault tolerance, low degree of dependency is desirable.

If secret information is managed as a single segment or there is no threshold, degree of dependency is '1' and all segments of secret information are needed to restore the original secret information.

In case of (k, n) threshold scheme, secret information is divided into n segments and k or more among n segments are required for restoration. In this case, degree of dependency on segments of secret information is ' k/n '.

Since weighted segment D_w was added to (k, n) threshold scheme of the one weighted threshold secret sharing scheme proposed in this paper, degree of dependency on segments of secret information is ' $(k+1)/(n+1)$ '.

DoD of the proposed method can be compared to single secret information and (k, n) threshold scheme as follows.

$$\frac{k}{n} \leq \frac{k+1}{n+1} \leq 1 \quad (8)$$

where, $k \leq n$

That is, while degree of dependency is increased by addition of D_w compared to (k, n) threshold scheme, it is still lower than cases in which secret information is managed as a single segment or there is no threshold.

C. Utility of Proposal

In case of the proposed method, the original secret information cannot be restored by collecting k or more segments if weighted segment is not included. Thus when looking from security perspective, security measures are only necessary in at least one or more storage place or network channel that include weighted segment, instead of k or more segments, to protect secret information from attackers. Operational cost is reduced.

Also, when collecting segments of secret information, access is controlled by authenticating the key consumer demanding segments. In this case, access control can be done simply by authenticating in the place that stores weighted segment.

V. CONCLUSIONS

In this paper, a one weighted threshold secret sharing scheme that can control restoration of original secret information by granting weighted value on a segment was proposed. By adding weighted segment D_w to the (k, n) threshold scheme of Shamir and making it impossible to restore original information without D_w , the proposed method resolved the problem on exposure of original secret information, which occurs when k or more random segments are stolen by an attacker.

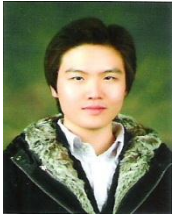
In addition, the proposed method has advantage of reducing security costs on segment storage places and network channels because original secret information can be protected by taking security measures in at least one or more places that store the weighted segment. When authentication of key consumer is required, access control can be easily done through authentication in the place that stores the weighted segment.

ACKNOWLEDGMENT

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2012-H301-12-4008) supervised by the NIPA(National IT Industry Promotion Agency)

REFERENCES

- [1] Shamir, A., "How to Share a Secret," Communications of the ACM, vol.11, pp.612-613, Nov. 1979.
- [2] Blakley, G.R., "Safeguarding cryptographic keys," Proc. AFIPS 1979 NCC, vol.48, pp.313-317, June 1979.
- [3] Mignotte, M., "How to share a secret, in: T. Beth, editor," Cryptography- Proceedings of the Workshop on Cryptography, Lecture Notes in Computer Science 149 (1983), pp.371-375., 1982.
- [4] Asmuth, C. A. and J. Bloom, "A modular approach to key safeguarding," IEEE Transactions on Information Theory IT-29, pp.208-210, 1983.
- [5] Berrut, J.-P. and Trefethen, L.N., "Barycentric Lagrange interpolation," SIAM Review, vol.46, no.3, pp.501-517, 2004.



SeongMin Yoo is a Ph.D. candidate in the Department of Computer Engineering at Chungnam National University in Republic of Korea. He received the B.S. degree in Computer Science & Engineering from Chungnam National University in 2010, the M.S. degree in Computer Engineering from same university in 2012. He is interested in most aspects of information security, both theoretical and practical, and his recent research is largely about applied crypto, networks security, and cloud service security.



PyungKoo Park is a senior engineer in the Electronics and Telecommunications Research Institute in Republic of Korea. He received the B.S. degree in Computer Engineering from Korea University in 1998, the M.S. degree in Computer Science from same university in 2000, and the Ph.D. degree in Computer Network and Security System at Chungnam National University in Korea. His research interests are Internet Security and Computer Networks.



JinSeop Shin is a M.S. candidate in the Department of Computer Engineering at Chungnam National University in Republic of Korea. He received the B.S. degree in Computer Science & Engineering from Chungnam University in 2012. His research interests are Smartphone Security, Cryptanalysis and Key Management Systems. His recent research is largely about Smartphone Security(in particular security in the Android OS).



JaeCheol Ryou is a professor in the Department of Computer Engineering at Chungnam National University in Korea. He received the B.S. degree in Industrial Engineering from Hanyang University in 1985, the M.S. degree in Computer Science from Iowa State University in 1988, and the Ph.D. degree in Electrical Engineering and Computer Science from Northwestern University in 1990. His research interests are Internet Security and Electronic Payment Systems.