Secret Share Based Key Pre-Distribution Scheme

Sergey V. Belim [1,2]
[1]Omsk State Technical University
11 Mira avenue, 644050, Omsk, Russia
[2]Siberian State Automobile
and Highway University
5 Mira avenue, 644080, Omsk, Russia
sbelim@mail.ru

Svetlana Yu. Belim
Omsk State Technical University
11 Mira avenue, 644050, Omsk, Russia
svbelim@gmail.com

Abstract

The key pre-distribution scheme including an encryption key co-generation protocol is proposed. The key pre-distribution scheme is formed based on the Blom's scheme. The Shamir secret sharing threshold scheme (3,4) is used for the key generation protocol. The basic scheme and protocol for two users are discussed. Generalization this scheme for an arbitrary number of users is performed. The correctness of the scheme is proved.

1 Introduction

Key pre-distribution schemes are widely used in devices with limited resources. Sensor networks and IoT devices use such schemes. The key pre-distribution scheme reduces the amount of information in the device memory. Devices store key materials. The key distribution server generates key materials and sends them to users through secure communication channels. Users store key materials in secure mode. Cryptographic keys are calculated based on key materials. Key materials and open user information are used to calculate keys. The two key pre-distribution schemes are most widely used. KDP scheme uses set theory [1]. Blom's scheme uses polynomial theory over finite fields [2]. Blom's scheme is actively used in wireless networks [3, 4, 5]. The KDP scheme is applicable to large networks consisting of subnets [6, 7, 8].

We highlight one important disadvantage of all key pre-distribution schemes. This disadvantage is the complete trust of users. The user can calculate the encryption key without the consent of another user. Leakage the key information of one user leads to leakage of all keys this user. Other users cannot prevent this leak. We propose a key pre-distribution scheme that includes a participant interaction protocol to generate a common key. This protocol allows other users to block a compromised user.

2 Basic scheme

We propose a protocol first with only two participants A and B. We use Shamir's scheme to divide the secret [14]. We limit ourselves to a threshold scheme $(3, 4)$. The polynomial $F(x)$ of degree 2 is necessary to implement this scheme. All calculations are performed in the ring Z_p. p is a prime number.

$$F(x) = a_2x^2 + a_1x + a_0.$$

In: Sergei S. Goncharov, Yuri G. Evtushenko (eds.): Proceedings of the Workshop on Applied Mathematics and Fundamental Computer Science 2021 , Omsk, Russia, 24-04-2021, published at http://ceur-ws.org

The coefficients of polynomial a_0, a_1, a_2 are chosen randomly. The polynomial is stored on the key distribution server and is secret. Server selects random numbers x_{1A}, x_{2A}, x_{1B}, $x_{2B} \in Z_p$. The server generates key materials for each user.

Key materials for user A are calculated based on numbers x_{1A}, x_{2A}.

$$k_{1A} = F(x_{1A}), \quad k_{2A} = F(x_{2A}).$$

Key materials for user B are calculated based on numbers x_{1B}, x_{2B}.

$$k_{1B} = F(x_{1B}), \quad k_{2B} = F(x_{2B}).$$

The server sends key content to users over a secure channel.

$$S \to A : (x_{1A}, k_{1A}), (x_{2A}, k_{2A}),$$
$$S \to B : (x_{1B}, k_{1B}), (x_{2B}, k_{2B}).$$

If user A initiates a communication channel with user B, then he sends him one parts of the secret k_{1A}.

$$A \to B : A, (x_{1A}, k_{1A}).$$

If user B agrees to create a secure information channel, then he compiles and solves a system of linear equations with respect to b_0, b_1, b_2.

$$\begin{cases} b_0 + b_1 x_{1B} + b_2 x_{1B}^2 = k_{1B}, \\ b_0 + b_1 x_{2B} + b_2 x_{2B}^2 = k_{2B}, \\ b_0 + b_1 x_{1A} + b_2 x_{1A}^2 = k_{1A}. \end{cases}$$

User B calculates the common encryption key based on the numbers b_0, b_1, b_2. The function from the three variables $h(x, y, z)$ is used to find the key. This function is open and known to all participants.

$$k_{BA} = h(b_0, b_1, b_2).$$

User B then sends one part of the secret k_{1B} to user A.

$$B \to A : (x_{1B}, k_{1B}).$$

User A compiles and solves a system of linear equations from three unknown c_0, c_1, c_2.

$$\begin{cases} c_0 + c_1 x_{1A} + c_2 x_{1A}^2 = k_{1A}, \\ c_0 + c_1 x_{2A} + c_2 x_{2A}^2 = k_{2A}, \\ c_0 + c_1 x_{1B} + c_2 x_{1B}^2 = k_{1B}. \end{cases}$$

User A calculates the common encryption key based on the numbers c_0, c_1, c_2.

$$k_{AB} = h(c_0, c_1, c_2).$$

We prove that both users will receive the same key.

$$k_{AB} = k_{BA}.$$

We consider the system of equations for user A.

$$\begin{cases} c_0 + c_1 x_{1A} + c_2 x_{1A}^2 = F(x_{1A}), \\ c_0 + c_1 x_{2A} + c_2 x_{2A}^2 = F(x_{2A}), \\ c_0 + c_1 x_{1B} + c_2 x_{1B}^2 = F(x_{1B}). \end{cases}$$

User A obtains the coefficients of the polynomial $F(x)$ when solving this system of equations.

$$c_0 = a_0, \quad c_1 = a_1, \quad c_2 = a_2.$$

We consider the system of equations for user B.

$$\begin{cases} b_0 + b_1 x_{1B} + b_2 x_{1B}^2 = F(x_{1B}), \\ b_0 + b_1 x_{2B} + b_2 x_{2B}^2 = F(x_{2B}), \\ b_0 + b_1 x_{1A} + b_2 x_{1A}^2 = F(x_{1A}). \end{cases}$$

User B obtains the coefficients of the polynomial $F(x)$ when solving this system of equations.

$$b_0 = a_0, \quad b_1 = a_1, \quad b_2 = a_2.$$

Both users receive the same set of numbers.

$$b_0 = c_0, \quad b_1 = c_1, \quad b_2 = c_2.$$

Users receive the same keys.

$$k_{AB} = h(c_0, c_1, c_2) = h(b_0, b_1, b_2) = k_{BA}.$$

Protocol reliability is based on a threshold scheme (3,4). Both users, as a result of receiving key materials from the server, own two parts of the secret. Users receive a third part of the secret during messaging. Three parts of the secret allow you to restore the full secret. The attacker has the ability to intercept only messages between users, so he can take possession only two parts of the secret. This information is not sufficient to calculate the encryption key.

3 Scheme for an arbitrary number of users

We modify our scheme for an arbitrary number of users. All calculations are performed in the ring Z_p. p is a prime number. The server generates a unique number a_i for each user u_i ($a_i \in Z_p$). Numbers a_i are stored in public on the server. The server ensures that these numbers remain unchanged. The server generates a polynomial from three variables $F(x, y, z)$. The polynomial $F(x, y, z)$ is kept secret. We write the polynomial $F(x, y, z)$ as a polynomial from one variable x with coefficients dependent on the variables y and z. The degree of the polynomial over the variable x is 2.

$$F(x, y, z) = f_2(y, z)x^2 + f_1(y, z)x + f_0(y, z).$$

The functions $f_2(y, z)$, $f_1(y, z)$, $f_0(y, z)$ are polynomials. We enter the requirement of symmetry $F(x, y, z)$ over the variables y and z.

$$F(x, y, z) = F(x, z, y).$$

This requirement leads to symmetry of polynomials $f_2(y, z)$, $f_1(y, z)$, $f_0(y, z)$ over variables y and z.

$$\begin{gathered} f_0(y, z) = f_0(z, y), \\ f_1(y, z) = f_1(z, y), \\ f_2(y, z) = f_2(z, y). \end{gathered}$$

The degree of polynomials $f_2(y, z)$, $f_1(y, z)$, $f_0(y, z)$ depends on the number of users. The polynomial coefficients $f_2(y, z)$, $f_1(y, z)$, $f_0(y, z)$ are random numbers.

The server selects two random numbers x_{1i} and x_{2i} ($i = 1,..., n$) for each user u_i. All numbers x_{1i} and x_{2i} must be unique. The server generates two parts of the secret for each user. Parts of the secret are polynomials from one variable z.

$$\begin{gathered} r_{1i}(z) = F(x_{1i}, a_i, z), \\ r_{2i}(z) = F(x_{2i}, a_i, z). \end{gathered}$$

The server calculates key materials for each user u_i (i=1, ..., n). Key materials include two numbers and two functions.

$$Key(u_i) = \{x_{1i}, x_{2i}, r_{1i}(z), r_{2i}(z)\}.$$

The polynomials $r_{1i}(z)$ and $r_{2i}(z)$ are transmitted as a set of coefficients. The server forwards key content to users via a secure channel.

If the user u_i wants to establish a connection with the user u_j, then a sequence of nine steps is performed.

1. The user u_i requests the number a_j from the server.
2. The user u_i calculates two numbers.

$$q_{1ij} = r_{1i}(a_j),$$
$$q_{2ij} = r_{2i}(a_j).$$

3. The user u_i forwards a message to the user u_j.

$$u_i \to u_j : (u_i, x_{1i}, q_{1ij}).$$

4. The user u_j requests a_i from the server and calculates two numbers.

$$q_{1ji} = r_{1j}(a_i),$$
$$q_{2ji} = r_{2j}(a_i).$$

5. The user u_j forwards a message to the user u_i.

$$u_j \to u_i : (u_j, x_{1j}, q_{1ji}).$$

6. The user u_j solves a system of linear equations relative to unknown b_0, b_1, b_2.

$$\begin{cases} b_2 x_{1j}^2 + b_1 x_{1j} + b_0 = q_{1ji}, \\ b_2 x_{2j}^2 + b_1 x_{2j} + b_0 = q_{2ji}, \\ b_2 x_{1i}^2 + b_1 x_{1i} + b_0 = q_{1ij}. \end{cases}$$

7. The user u_j calculates the pair key.

$$k_{ji} = h(b_0, b_1, b_2).$$

The function from the three variables $h = h(x, y, z)$ is an open part of the schema and is known to all participants.

8. The user u_i solves the system of linear equations with respect to c_0, c_1, c_2.

$$\begin{cases} c_2 x_{1i}^2 + c_1 x_{1i} + c_0 = q_{1ij}, \\ c_2 x_{2i}^2 + c_1 x_{2i} + c_0 = q_{2ij}, \\ c_2 x_{1j}^2 + c_1 x_{1j} + c_0 = q_{1ji}. \end{cases}$$

9. The user u_i calculates the pair key.

$$k_{ij} = h(c_0, c_1, c_2).$$

We prove that both users receive the same pair keys. We consider the system of user equations u_i.

$$\begin{aligned} q_{1ij} &= r_{1i}(a_j) = F(x_{1i}, a_i, a_j) = f_2(a_i, a_j)x_{1i}^2 + f_1(a_i, a_j)x_{1i} + f_0(a_i, a_j), \\ q_{2ij} &= r_{2i}(a_j) = F(x_{2i}, a_i, a_j) = f_2(a_i, a_j)x_{2i}^2 + f_1(a_i, a_j)x_{2i} + f_0(a_i, a_j), \\ q_{1ji} &= r_{1j}(a_i) = F(x_{1j}, a_j, a_i) = F(x_{1j}, a_i, a_j) = f_2(a_i, a_j)x_{1j}^2 + f_1(a_i, a_j)x_{1j} + f_0(a_i, a_j), \end{aligned}$$

$$\begin{cases} c_2 x_{1i}^2 + c_1 x_{1i} + c_0 = f_2(a_i, a_j)x_{1i}^2 + f_1(a_i, a_j)x_{1i} + f_0(a_i, a_j), \\ c_2 x_{2i}^2 + c_1 x_{2i} + c_0 = f_2(a_i, a_j)x_{2i}^2 + f_1(a_i, a_j)x_{2i} + f_0(a_i, a_j), \\ c_2 x_{1j}^2 + c_1 x_{1j} + c_0 = f_2(a_i, a_j)x_{1j}^2 + f_1(a_i, a_j)x_{1j} + f_0(a_i, a_j). \end{cases}$$

We write this system of equations in matrix form.

$$\begin{pmatrix} x_{1i}^2 & x_{1i} & 1 \\ x_{2i}^2 & x_{2i} & 1 \\ x_{1j}^2 & x_{1j} & 1 \end{pmatrix} \begin{pmatrix} c_2 \\ c_1 \\ c_0 \end{pmatrix} = \begin{pmatrix} x_{1i}^2 & x_{1i} & 1 \\ x_{2i}^2 & x_{2i} & 1 \\ x_{1j}^2 & x_{1j} & 1 \end{pmatrix} \begin{pmatrix} f_2(a_i, a_j) \\ f_1(a_i, a_j) \\ f_0(a_i, a_j) \end{pmatrix}$$

The matrix in equality is a Vandermonde matrix. The Vandermonde determinant is not zero if all x_{1i} and x_{2i} are different. Therefore, we conclude that two vectors are equal.

$$\begin{pmatrix} c_2 \\ c_1 \\ c_0 \end{pmatrix} = \begin{pmatrix} f_2(a_i, a_j) \\ f_1(a_i, a_j) \\ f_0(a_i, a_j) \end{pmatrix}$$

$$c_2 = f_2(a_i, a_j),\ c_1 = f_1(a_i, a_j),\ c_0 = f_0(a_i, a_j).$$

We consider the system for user equations u_j.

$$\begin{aligned} q_{1ji} &= r_{1j}(a_i) = F(x_{1j}, a_j, a_i) = f_2(a_j, a_i)x_{1j}^2 + f_1(a_j, a_i)x_{1j} + f_0(a_j, a_i), \\ q_{2ji} &= r_{2j}(a_i) = F(x_{2j}, a_j, a_i) = f_2(a_j, a_i)x_{2j}^2 + f_1(a_j, a_i)x_{2j} + f_0(a_j, a_i), \\ q_{1ij} &= r_{1i}(a_j) = F(x_{1i}, a_i, a_j) = F(x_{1i}, a_j, a_i) = f_2(a_j, a_i)x_{1i}^2 + f_1(a_j, a_i)x_{1i} + f_0(a_j, a_i), \end{aligned}$$

$$\begin{cases} b_2x_{1j}^2 + b_1x_{1j} + b_0 = f_2(a_j, a_i)x_{1j}^2 + f_1(a_j, a_i)x_{1j} + f_0(a_j, a_i), \\ b_2x_{2j}^2 + b_1x_{2j} + b_0 = f_2(a_j, a_i)x_{2j}^2 + f_1(a_j, a_i)x_{2j} + f_0(a_j, a_i), \\ b_2x_{1i}^2 + b_1x_{1i} + b_0 = f_2(a_j, a_i)x_{1i}^2 + f_1(a_j, a_i)x_{1i} + f_0(a_j, a_i). \end{cases}$$

$$\begin{pmatrix} x_{1j}^2 & x_{1j} & 1 \\ x_{2j}^2 & x_{2j} & 1 \\ x_{1i}^2 & x_{1i} & 1 \end{pmatrix} \begin{pmatrix} b_2 \\ b_1 \\ b_0 \end{pmatrix} = \begin{pmatrix} x_{1j}^2 & x_{1j} & 1 \\ x_{2j}^2 & x_{2j} & 1 \\ x_{1i}^2 & x_{1i} & 1 \end{pmatrix} \begin{pmatrix} f_2(a_j, a_i) \\ f_1(a_j, a_i) \\ f_0(a_j, a_i) \end{pmatrix}$$

$$\begin{pmatrix} b_2 \\ b_1 \\ b_0 \end{pmatrix} = \begin{pmatrix} f_2(a_j, a_i) \\ f_1(a_j, a_i) \\ f_0(a_j, a_i) \end{pmatrix}$$

$$b_2 = f_2(a_j, a_i),\ b_1 = f_1(a_j, a_i),\ b_0 = f_0(a_j, a_i).$$

We conclude the equality of numbers from the symmetry of polynomials f_0, f_1, f_2.

$$b_0 = c_0 = f_0(a_i, a_j),\quad b_1 = c_1 = f_1(a_i, a_j),\quad b_2 = c_2 = f_2(a_i, a_j).$$

Both users receive the same set of numbers. We conclude that the pair keys of both users are equal.

$$k_{ij} = h(c_0, c_1, c_2) = h(b_0, b_1, b_2) = k_{ji}.$$

4 Conclusion

The proposed scheme allows any user to control calculation of communication keys with it. This scheme has a level of compromise resistance equivalent to the Blom's scheme. Users can lock a compromised user without involving the key distribution server.

References

[1] C.J. Mitchell, . Piper. Key storage in Secure Networks. *Discrete and Applied Math*, 21:215–228, 1988.

[2] R. Blom. An optimal class of symmetric key generation systems. *Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques*:335-338, 1985.

[3] E. Shi, A. Perrig. Designing secure sensor networks. *IEEE Wireless Communications*, 11(6):38–43, 2004.

[4] Y. Liang, H. V. Poor, S. Shamai. Information Theoretic Security. *Found. Trends Commun. Inf. Theory*, 5:355–580, 2009.

[5] A. Parakh, S. Kak. Matrix based key agreement algorithms for sensor networks. *Fifth IEEE In-ternational Conference on Advanced Telecommunication Systems and Networks (ANTS)*:1–3, 2011.

[6] Y. Liu, M. Dong, K. Ota, A. Liu. ActiveTrust: secure and trustable routing in wireless sensor net-works. *IEEE Transactions on Information Forensics and Security*, 11(9):2013–2027, 2016.

[7] D. Zhao, K.-W. Chin, R. Raad. Approximation algorithms for broadcasting in duty cycled wire-less sensor networks. *Wireless Networks*, 20(8):2219–2236, 2014.

[8] X. Zheng, J. Wang, W. Dong, Y. He, Y. Liu. Bulk data dissemination in wireless sensor networks: analysis, implications and improvement. *IEEE Transactions on Computers*, 65(5):1428–1439, 2016.

[9] S.V. Belim, S.Yu. Belim. Mandatory access control implementation in the distributed systems. *Automatic Control and Computer Sciences*, 52(8):1124–1126, 2018.

[10] S.V. Belim, S.Yu. Belim. The modification of Blom's key predistribution scheme, taken into account simplex channels. *Automatic Control and Computer Sciences*, 52(8):1134–1137, 2018.

[11] S.V. Belim, S.Yu. Belim. Implementation of simplex channels in the Blom's keys pre-distribution scheme. *Journal of Physics: Conf. Series*, 1210:012008, 2019.

[12] S.V. Belim, S.Yu. Belim. Use the keys pre-distribution KDP-scheme for mandatory access control imple-mentation. *Journal of Physics: Conf. Series*, 1210:012009, 2019.

[13] S.V. Belim, S.Yu. Belim. Vector key pre-distribution scheme. *Journal of Physics: Conf. Series*, 1441:012033, 2020.

[14] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.