Combining the Pre-Distribution Key Protocol with the Threshold Scheme

S V Belim¹, S Y Belim¹

¹Omsk State Technical University, 644050 Omsk, Russia

E-mail: sbelim@mail.ru

Abstract. In the article, the protocol for key pre-distribution using a threshold scheme is proposed. The Blom pre-distribution scheme is used as the basis. Shamir secret sharing scheme is used for threshold scheme. A polynomial of three variables is used to form key materials. Messaging between users is required to generate a key. The threshold scheme (3,4) is used to calculate the encryption key.

1. Introduction

The generation, distribution and storage of encryption keys are vulnerabilities for a secure computer network. If each user pair uses its own encryption key, then the key materials volume is large. This large data volume is stored and transmitted over secure communication channels. Providing these processes is a problem in networks with low performance devices. For example, a sensor network consists of such devices [1-6]. Pre-distribution schemes are the solution to this problem. Key materials are provided to each network user in these schemes. The server generates key materials and sends them to users through secure channels. Users keep key materials secret. Each user calculates the encryption key when establishing a connection with another user. Proprietary key materials and open information are used to compute the encryption key.

The key pre-distribution KDP-scheme [7] and the Blom’s scheme [8] are the most commonly used. The mathematical principles in these schemes are different. The KDP scheme uses set theory. The Blom’s scheme for keys pre-distribution uses polynomials over finite fields. These two schemes are actively used for the security of computer networks. Blom’s scheme is actively used in the security of wireless networks [9-11]. KDP scheme is used in large networks consisting of many subnets [12-14]. These pre-distribution key schemes allow modification to meet additional requirements. Requirements may consider security policy [15-18] or simplex communication channels [19,20].

The lack of control over the generation the encryption key is a drawback of these schemes. If some key materials have leaked in the system, then the thief can calculate all the keys of this user. Interaction with other users is not required. System security is improved if the protocol requires users to interact in key development.

2. Basic scheme

We enter a basic protocol for a system with two users A and B. We use the Shamir scheme for dividing the secret [21] based on the polynomial $F(x)$.

$$F(x)=a_2x^2+a_1x+a_0.$$
All calculations are performed in the ring $\mathbb{Z}_p$, $p$ is a prime number. The degree of the polynomial is two. We use a threshold scheme $(3,4)$. Various numbers $x_{1A}, x_{2A}, x_{1B}, x_{2B} \in \mathbb{Z}_p$ are chosen randomly. The Key Distribution Server $S$ generates key materials for each user based on the $F(x)$. Server $S$ sends key materials to users via a secure channel.

$S \rightarrow A$: $(x_{1A}, k_{1A} = F(x_{1A}))$, $(x_{2A}, k_{2A} = F(x_{2A}))$.

$S \rightarrow B$: $(x_{1B}, k_{1B} = F(x_{1B}))$, $(x_{2B}, k_{2B} = F(x_{2B}))$.

The shared key is generated as a result of messaging. User A initiates the common key generation. User A sends user B its own name and one of the secret parts sent by the server.

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

User B, having received this message, solves the system of equations with respect to unknown quantities $a_0, a_1, a_2$.

\[
\begin{align*}
   a_0 + a_1 x_{1B} + a_2 x_{1B}^2 &= k_{1B} \\
   a_0 + a_1 x_{2B} + a_2 x_{2B}^2 &= k_{2B} \\
   a_0 + a_1 x_{1B} + a_2 x_{1B}^2 &= k_{1A}
\end{align*}
\]

User B calculates the encryption key based on the values $a_0, a_1, a_2$. The encryption key is calculated using a function from three variables $h(x, y, z)$ known to both sides.

$k_{BA} = h(a_0, a_1, a_2)$

Then, user B sends one of the secret parts received from the server to user A.

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

User A, having received the message, compiles and solves a system of equations from three unknowns $a_0, a_1, a_2$.

\[
\begin{align*}
   a_0 + a_1 x_{1A} + a_2 x_{1A}^2 &= k_{1A} \\
   a_0 + a_1 x_{2A} + a_2 x_{2A}^2 &= k_{2A} \\
   a_0 + a_1 x_{1B} + a_2 x_{1B}^2 &= k_{1B}
\end{align*}
\]

Then, user A calculates the encryption key.

$k_{BA} = h(a_0, a_1, a_2)$

Both users A and B find the same coefficient values $a_0, a_1, a_2$. Users receive the same encryption keys.

$k_{AB} = k_{BA}$

Protocol persistence 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 when messaging. Three parts of the secret allow you to restore the full secret. An attacker can only intercept messages between users. Therefore, an attacker can receive only two parts of the secret. This information is not sufficient to calculate the encryption key.
3. Generalized scheme
We summarize the scheme for an arbitrary number of users. We map the number $a_i \in Z_p$ to each user $u_i$, $p$ – prime number. The polynomial $F(x,y,z)$ from the three variables is stored in secret on the server. We do all the calculations in $Z_p$.

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

The functions $f_2(y,z), f_1(y,z), f_0(y,z)$ are also polynomials. The polynomial $F(x,y,z)$ must be symmetric with respect to the variables $y$ and $z$.

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

We conclude that the polynomials $f_2(y,z), f_1(y,z), f_0(y,z)$ are symmetric with respect to the variables $y$ and $z$.

$$f_0(y,z) = f_0(z,y)$$
$$f_1(y,z) = f_1(z,y)$$
$$f_2(y,z) = f_2(z,y)$$

The degree of polynomials $f_2(y,z), f_1(y,z), f_0(y,z)$ is determined by the number of subscribers participating in the scheme.

The server generates key materials for each user $u_i$ ($i=1, \ldots, n$). Two numbers $x_{i1}$ and $x_{i2}$ ($i=1, \ldots, n$) are selected arbitrarily for each user. All numbers for all users must be different. Each number must occur only once in the set \{ $x_{i1}, x_{i2}, x_{i2}, \ldots, x_{in}, x_{in}$ \}.

The server generates two secret components for each user. These components are functions from one variable $z$.

$$r_{1}(z) = F(x_{i1}, a_i, z),$$
$$r_{2}(z) = F(x_{i2}, a_i, z).$$

The server transmits key materials to each user $u_i$ ($i=1, \ldots, n$) over a secure channel. Key materials include four components.

$$Key(u_i) = \{ x_{i1}, x_{i2}, r_1(z), r_2(z) \}$$

Polynomials $r_{1}(z)$ and $r_{2}(z)$ are transmitted as coefficient vectors. When a user $u_i$ connects to a user $u_j$, a 7-step sequence is performed.

1. The user $u_i$ initiates the common key generation for symmetric encryption.
2. The user $u_i$ extracts $a_j$ from the open base and calculates two numbers.

$$q_1 = r_1(a_j)$$
$$q_2 = r_2(a_j)$$

3. The user $u_i$ forwards a message containing his name, number $x_{ij}$ and number $q_1$ to the user $u_j$.
4. The user $u_j$, having received the message, extracts the number $a_i$ from the common base and calculates two numbers.

$$q_1 = r_1(a_i)$$
$$q_2 = r_2(a_i)$$

5. The user $u_j$ forwards to the user $u_i$ a message containing its name, number $x_{ij}$ and number $q_1$. 


6. The user $u_j$ solves the system of equations.

\[
\begin{align*}
&b_2x_{1j} + b_1x_{1j} + b_0 = q_{1j}, \\
&b_2x_{2j} + b_1x_{2j} + b_0 = q_{2j}, \\
&b_2x_{ij} + b_1x_{ij} + b_0 = q_{ij}.
\end{align*}
\]

Unknown is a vector $b=(b_0, b_1, b_2)$. The user $u_j$ calculates the pair key based on the equation solution.

\[
k_{ji} = h(b_0, b_1, b_2)
\]

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

7. The user $u_i$ receives a message from the user $u_j$ and solves the system of equations.

\[
\begin{align*}
&c_2x_{1i} + c_1x_{1i} + c_0 = q_{1i}, \\
&c_2x_{2i} + c_1x_{2i} + c_0 = q_{2i}, \\
&c_2x_{ij} + c_1x_{ij} + c_0 = q_{ij}.
\end{align*}
\]

Unknown is a vector $b=(b_0, b_1, b_2)$. The user $u_i$ calculates the pair key based on the equation solution.

\[
k_{ij} = h(b_0, b_1, b_2)
\]

Both users receive the same key.

\[
\begin{align*}
&c_2 = b_2 = f_2(a_i, a_j), \\
&c_1 = b_1 = f_1(a_i, a_j), \\
&c_0 = b_0 = f_0(a_i, a_j).
\end{align*}
\]

We consider an example of using this scheme for three users.

We set the polynomial to form key materials. All calculations are performed in the $Z_{11}$.

\[
F(x, y, z) = f_2(y, z)x^2 + f_1(y, z)x + f_0(y, z),
\]

\[
\begin{align*}
&f_2(y, z) = y^2 + 2yz + z^2 - y - z, \\
&f_1(y, z) = 3yz + 2y + 2z + 3, \\
&f_0(y, z) = 2y^2 + 2z^2 - 4.
\end{align*}
\]

We set numbers for users.

\[
a_1 = 3, a_2 = 1, a_3 = 5.
\]

We calculate the key materials for user $u_1$. 
\( f_2(a_1,z)=6+5z+z^2, \)
\( f_1(a_1,z)=9, \)
\( f_0(a_1,z)=3+2z. \)

\( x_{11}=2, \quad x_{21}=3. \)

\( r_{11}(z)=F(x_{11}, a_1, z)=1+9z+6z^2, \)
\( r_{21}(z)=F(x_{21}, a_1, z)=7+z. \)

Key \((u_1) = \{x_{11}, x_{21}, r_{11}(z), r_{21}(z)\} = \{2, 3, (1,9,6), (7,1,0)\}\)

We calculate the key materials for user \(u_2\).

\( f_2(a_2,z)=z+z^2, \)
\( f_1(a_2,z)=5+5z, \)
\( f_0(a_2,z)=9+2z. \)

\( x_{12}=1, \quad x_{22}=4. \)

\( r_{12}(z)=F(x_{12}, a_2, z)=3+6z+3z^2, \)
\( r_{22}(z)=F(x_{22}, a_2, z)=7+3z+7z^2. \)

Key \((u_2) = \{x_{12}, x_{22}, r_{12}(z), r_{22}(z)\} = \{1, 4, (3,6,3), (7,3,7)\}\)

We calculate the key materials for user \(u_3\).

\( f_2(a_3,z)=9+9z+z^2, \)
\( f_1(a_3,z)=6z+2, \)
\( f_0(a_3,z)=2+2z. \)

\( x_{13}=5, \quad x_{23}=6. \)

\( r_{13}(z)=F(x_{13}, a_3, z)=6+2z+5z^2, \)
\( r_{23}(z)=F(x_{23}, a_3, z)=8+8z+5z^2. \)

Key \((u_3) = \{x_{13}, x_{23}, r_{13}(z), r_{23}(z)\} = \{5, 6, (6,2,5), (8,8,5)\}\)

We consider the protocol for interaction between users \(u_1\) and \(u_2\).

\( u_1: q_{11}=r_{11}(a_2)=5, \)
\( u_1 \rightarrow u_2: \{u_1, 2, 5\}, \)
\( u_2: q_{12}=r_{12}(a_1)=10, \)
\( u_2 \rightarrow u_1: \{u_2, 1, 4\}, \)
\( u_2: 4c_2+2c_1+c_0=5, \)
\( c_2+c_1+c_0=4, \)
\( 16c_2+4c_1+c_0=2. \)
\(c_2=1, c_1=9, c_0=5.\)

\(k_{21}=c_2 \cdot c_1 \cdot c_0 = 1.\)

\(u_1: 4b_2+2b_1+b_0=5,\)
\(9b_2+3b_1+b_0=8,\)
\(b_2+b_1+b_0=10.\)

\(b_2=1, b_1=9, b_0=5.\)

\(k_{12}=b_2 \cdot b_1 \cdot b_0 = 1.\)

\[k_{12} = k_{21}\]

### 4. Conclusion

Combining the pre-distribution key scheme and the secret sharing scheme is proposed in this article. The Blom’s key distribution scheme is used as a basis. Shamir’s secret sharing scheme is added to the key distribution scheme. This new scheme is resistant to key compromising. Combining these two schemes allows the user to control the key generation process. The encryption key cannot be calculated without user input.

### References

[1] Eschenauer L, Gligor V D 2002 Proceedings of the 9th ACM conference on Computer and Communication Security 41
[2] Chan H, Perrig A, Song D 2003 Proceedings of IEEE Symposium on Security and Privacy 197
[3] Du W, Deng J, Han Y S, Varshney P K 2003 Proceedings of the 10th ACM Conference on Computer and Communication Security 42
[4] Liu D, Ning P 2003 Proceedings of 10th ACM Conference on Computer and Communications Security 52
[5] Liu D, Ning P 2003 Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks 72
[6] Anjum F 2006 Proceedings of WiSe 21
[7] Blom R 1985 EUROCRYPT’84 335
[8] Mitchell C J, Piper C 1988 Discrete and Applied Math. 21 215
[9] Shi E, Perrig A 2004 IEEE Wireless Communications 11(6) 38
[10] Liang Y, Poor H V, Shamai S 2009 Found. Trends Commun. Inf. Theory 5 355
[11] Parakh A, Kak S 2011 Fifth IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS) 1
[12] Liu Y, Dong M, Ota K, Liu A 2016 IEEE Transactions on Information Forensics and Security 11(9) 2013
[13] Zhao D, Chin K-W, Raad R 2014 Wireless Networks 20(8) 2219
[14] Zheng X, Wang J, Dong W, He Y, Liu Y 2016 IEEE Transactions on Computers 65(5) 1428
[15] Belim S V, Belim S Yu 2020 Journal of Physics: Conf. Series 1441 012033.
[16] Belim S V, Belim S Yu 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon) 1
[17] Belim S V, Belim S Yu 2019 Journal of Physics: Conf. Series 1210 012009
[18] Belim S V, Belim S Yu 2018 Automatic Control and Computer Sciences 52(8) 1134
[19] Belim S V, Belim S Yu 2019 Journal of Physics: Conf. Series 1210 012008
[20] Belim S V, Belim S Yu 2020 Automatic Control and Computer Sciences 54(8) 860
[21] Shamir A 1979 Commun. ACM 22(11) 612