One-way group key agreement protocol for end-to-end web email encryption

Jyh-haw Yeh
Dept. of Computer Science
Boise State University
Boise, Idaho 83725, USA

1 One-way group key agreement protocol for email encrytpion

Assume ID_0 is the email sender's identity (for example email address) and let ID_i, for $i = 1, 2, \ldots, n$, denote the identity for each email recepient in a group with n people.

Key generation by email sender

1. The email sender picks a random number r and computes
$$x_i = e(S_0, rH(ID_i)) \in G_2, \forall i = 0, 1, 2, \ldots, n \quad (1)$$
2. The email sender generates the encryption key K by
$$K = \oplus_{\forall i=0,1,\ldots,n}(x_i) \quad (2)$$
3. The email sender also computes $y_i, \forall i = 1, 2, \ldots, n$, as follows.
$$y_i = \oplus_{\forall j \neq i}(x_j) \quad (3)$$
4. The email sender encrypts the email using the secret key K and then sends the encrypted email out along with $(r, y_1, y_2, \ldots, y_n)$.

Key re-generation by each email recepient

Upon receiving the email from ID_0, each recepient ID_i can compute the secret key K by the following equation.
$$K = y_i \oplus e(rH(ID_0), S_i) \quad (4)$$
since

$$\begin{aligned}
& y_i \oplus e(rH(ID_0), S_i) \\
=& y_i \oplus e(rH(ID_0), sH(ID_i)) \\
=& y_i \oplus e(sH(ID_0), rH(ID_i)) \\
=& y_i \oplus e(S_0, rH(ID_i)) \\
=& y_i \oplus x_i \\
=& (\oplus_{\forall j \neq i}(x_j)) \oplus x_i \\
=& K
\end{aligned}$$

Example

Assume a person ID_0 would like to send an email to two other persons ID_1 and ID_2.

1. ID_0 picks a random number r and computes

$$\begin{cases} x_0 = e(S_0, rH(ID_0)) \\ x_1 = e(S_0, rH(ID_1)) \\ x_2 = e(S_0, rH(ID_2)) \end{cases}$$

2. ID_0 generates the encryption key

$$K = x_0 \oplus x_1 \oplus x_2 = e(S_0, rH(ID_0)) \oplus e(S_0, rH(ID_1)) \oplus e(S_0, rH(ID_2))$$

3. ID_0 computes

$$\begin{cases} y_1 = x_0 \oplus x_2 = e(S_0, rH(ID_0)) \oplus e(S_0, rH(ID_2)) \\ y_2 = x_0 \oplus x_1 = e(S_0, rH(ID_0)) \oplus e(S_0, rH(ID_1)) \end{cases}$$

4. ID_0 encrypts the email using the key K and sends (r, y_1, y_2) along with the email.

5. For the two recepients, ID_1 computes

$$\begin{aligned} &= y_1 \oplus e(rH(ID_0), S_1) \\ &= x_0 \oplus x_2 \oplus e(rH(ID_0), S_1) \\ &= x_0 \oplus x_2 \oplus e(sH(ID_0), rH(ID_1)) \\ &= x_0 \oplus x_2 \oplus e(S_0, rH(ID_1)) \\ &= x_0 \oplus x_2 \oplus x_1 \\ &= K \end{aligned}$$

and ID_2 computes

$$\begin{aligned} &= y_2 \oplus e(rH(ID_0), S_2) \\ &= x_0 \oplus x_1 \oplus e(rH(ID_0), S_2) \\ &= x_0 \oplus x_1 \oplus e(sH(ID_0), rH(ID_2)) \\ &= x_0 \oplus x_1 \oplus e(S_0, rH(ID_2)) \\ &= x_0 \oplus x_1 \oplus x_2 \\ &= K \end{aligned}$$

Thus, both email recepients can derive the same key K that was originally generated by the email sender ID_0.