

基于公钥广播加密的安全组播方案

陈礼青

(淮阴工学院 计算机工程学院, 江苏 淮安 223003)

(quietloner@sina.com)

摘 要:应用公钥广播加密进行安全组播的难点是如何更有效地权衡实现代价和安全性。通过引入身份标志区分各个接收者,并利用一组接收者的身份标志代替一般公钥广播加密方案中的组公钥,缩短了系统公钥参数的长度。将新的公钥广播加密方案应用到安全组播通信的过程表明,该方案有效降低了计算和通信代价,且达到了抗选择密文攻击的语义安全性。

关键词:组播;双线性对;密钥生成中心;组公钥

中图分类号: TP393.08 **文献标志码:** A

Secure multicast scheme based on public key broadcast encryption

CHEN Li-qing

(School of Computer Engineering, Huaiyin Institute of Technology, Huai'an Jiangsu 223003, China)

Abstract: The difficulty of utilizing public key broadcast encryption in secure multicast is keep balance between implementation cost and security. Taking identity to differentiate each receiver, and using a group of identities instead of group public key in general public key broadcast encryption schemes, the length of system public key parameters was shortened. The procedures of secure multicast communications utilizing the new scheme show that the new scheme is efficient in decreasing the cost of computation and communication, and reaches the semantic security that can fight against chosen ciphertext attack.

Key words: multicast; bilinear pairing; Key Generation Center (KGC); group public key

0 引言

组播^[1]是一种面向组接收者的高效通信方式,它通过在路由器上合并重复信息的传输,从而有效节约了带宽,降低了服务器的负担,可广泛地应用于多媒体远程教育、分布式系统、网络视频会议、视频点播等。安全组播的一个主要难点是如何确保只有合法的组注册用户才能接收到组播通信数据,从而达到访问控制的目的^[2-5]。

广播加密^[6]方案可以使一个广播源通过不安全的信道向一组接收者发送加密消息,并使得只有合法接收者才能解密消息,而任何非法接受者却不能。广播加密按密钥体系可分为对称密钥广播加密和公钥广播加密(Public Key Broadcast Encryption, PKBE)两类。前者只有体系中心可以向指定的接收者集合发送广播消息;而后者任何接收者(包括体系中心)都可以向指定的接收者集合发送广播消息。显然,PKBE的特点使得其很适合实现安全组播。本文在文献[7]所做工作的基础上提出了一个新的 PKBE 方案,缩短了原方案中的系统公钥参数的长度,对系统公钥参数长度和密文长度进行了更加灵活的折中,并将其应用到安全组播中,在降低计算和通信代价方面取得了较好的效果。

1 预备知识

1.1 双线性映射

设 G_1, G_2 都是阶为大素数 p 的乘法循环群。一个双线性映射 $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 必须满足如下性质:

双线性性 对于所有的 $P, Q \in G_1$, 以及 $a, b \in \mathbb{Z}_p^*$,

$$\hat{e}(P^a, Q^b) = \hat{e}(P, Q)^{ab}.$$

非退化性 若 g 是 G_1 的一个生成元, $\hat{e}(g, g) \neq 1_{G_2}$ 。

可计算性 存在一个有效的算法来计算 $\hat{e}(P, Q)$ 。

1.2 公钥广播加密

公钥广播加密一般由以下三个算法组成:

1) Setup (n): 对于系统中心, 输入接收者个数 n , 中心生成系统公钥参数 PK , 并为每个接收者生成对应的私钥 $d_i (i = 1, 2, \dots, n)$ 。

2) Broadcast (S, PK): 对于发送者, $S \subseteq \{1, 2, \dots, n\}$ 为所有接收者的任意一个子集, 输入子集 S 和系统公钥参数 PK , 广播源产生广播消息 $\langle \text{Header}, \text{Enc}_K(M) \rangle$ 。其中, Header 是用各指定接收者的公钥对话会话密钥 K 的加密, $\text{Enc}_K(M)$ 是采用对称加密算法以 K 为密钥对消息 M 的加密。下面讨论时, 密文特指 Header 。

3) Decryption ($S, i, d_i, \text{Header}, PK$): 对于接收者, 输入 ($S, i, d_i, \text{Header}, PK$), 若接收者 i 在指定接收者子集 S 中, 则算法输出会话密钥 K 。

1.3 攻击模型

利用攻击者 $A_{\text{Adversary}}$ 与挑战者 $C_{\text{Challenger}}$ 之间的游戏来定义密文 (即 Header) 的安全性。 $A_{\text{Adversary}}$ 与 $C_{\text{Challenger}}$ 都以接收者个数 n 作为输入。此攻击模型定义的是 PKBE 方案对于被动攻击者的选择密文安全性。具体攻击模型如下^[5]:

1) Init: $A_{\text{Adversary}}$ 任意选择一个其准备攻击的子集 $S^* \subseteq \{1, 2, \dots, n\}$ 。

2) Setup: $C_{\text{Challenger}}$ 运行 PKBE 方案中的 Setup 算法生成公

钥 PK 和各个接收者的私钥 $d_i (i = 1, 2, \dots, n)$ 。 $C_{\text{Challenger}}$ 将 PK 和不在 S^* 中的接收者的私钥 $d_j (j \notin S^*)$ 发送给 $A_{\text{Adversary}}$, $A_{\text{Adversary}}$ 将以这些信息作为下一步查询阶段的输入。

3) Query Phase I: $A_{\text{Adversary}}$ 向 $C_{\text{Challenger}}$ 发送解密请求 (u, S, Header) , 其中 $S \subseteq S^*, u \in S, C_{\text{Challenger}}$ 以元组 $(S, u, d_u, \text{Header}, PK)$ 为输入, 运行 PKBE 方案中的 Decryption 算法, 并将结果返回给 $A_{\text{Adversary}}$ 。

4) Challenge: $C_{\text{Challenger}}$ 以元组 (S^*, PK) 为输入, 运行 PKBE 方案中的 Broadcast 算法生成元组 $\langle \text{Header}^*, \text{Enc}_K(M) \rangle$ 。 $C_{\text{Challenger}}$ 随机选择 $b \in \{0, 1\}$, 设置 $K_b = K$, 并随机选择 K_{1-b} 。然后 $C_{\text{Challenger}}$ 以元组 $\langle \text{Header}^*, \text{Enc}_{K_b}(M) \rangle$ 传送给 $A_{\text{Adversary}}$ 。

5) Query Phase II: 类似于 Query Phase I, $A_{\text{Adversary}}$ 继续自适应地向 $C_{\text{Challenger}}$ 发送解密请求, 但要求 $\text{Header} \neq \text{Header}^*$ 。

6) Guess: $A_{\text{Adversary}}$ 根据本地掌握的信息, 最终输出一个对 b 的猜测值 $b' \in \{0, 1\}$ 。若 $b' = b$, 则 $A_{\text{Adversary}}$ 在这轮游戏中获胜。

定义 $A_{\text{Adversary}}$ 在上面的游戏中的获胜优势为 $\text{Adv}_{A_{\text{Adversary}}, n}^{\text{PKBE}} = \left| \Pr[b = b'] - \frac{1}{2} \right| < \varepsilon$ 。

1.4 复杂性假设

定义 1 一个 PKBE 方案具有抗选择密文攻击的语义安全性, 是指对于任何多项式时间算法的攻击者 $A_{\text{Adversary}}$, $\text{Adv}_{A_{\text{Adversary}}, n}^{\text{PKBE}}$ 都可以忽略。

定义 2 l -BDHE 问题。令 G_1 是乘法循环群, g, h 为 G_1 两个生成元, 给定 $(2l+1)$ 元组 $\langle g, h, g^a, g^{a^2}, \dots, g^{a^l}, g^{a^{l+2}}, \dots, g^{a^{2l}} \rangle \in G_1^{2l+1}$, 求 $\hat{e}(g, h)^{a^{l+1}}$ 。

定义 3 判定 l -BDHE 问题。事先给定 $\alpha \in Z_p^*$ 和 G_1 的两个生成元 g, h , 记 $g_i = g^{\alpha^i} \in G_1$, 令 $y_{g, \alpha, l}$ 为 $(2l-1)$ 元组 $(g_1, g_2, \dots, g_l, g_{l+2}, \dots, g_{2l})$, 并随机选择 $R \in G_1$, 判断 $R = \hat{e}(g_{l+1}, h)$ 是否成立。

定义输出 $b \in \{0, 1\}$ 的攻击者 $B_{\text{Adversary}}$ 在多项式时间 t 内解决 G_1 中的判定 l -BDHE 问题的优势为 ε , 若:

$$\left| \Pr[B_{\text{Adversary}}(h, g, y_{g, \alpha, l}, \hat{e}(g_{l+1}, h)) = 0] - \right.$$

$$\left. \Pr[B_{\text{Adversary}}(h, g, y_{g, \alpha, l}, R) = 0] \right| \geq \varepsilon$$

此时判定 l -BDHE 问题又可记为判定 (t, ε, l) -BDHE 问题。

复杂性假设 判定 (t, ε, l) -BDHE 问题是困难问题, 即不存在一个多项式时间 t 的算法能以不可忽略的概率 (至少为 ε) 解决 G_1 中的判定 l -BDHE 问题。

2 基于公钥广播加密的安全组播方案

2.1 Boneh PKBE 方案

文献[7]提出了两个 PKBE 方案: Special Case 和 General Case, 其优点是私钥和密文长度都比较短。在第一个方案 (Special Case) 中, 私钥和密文长度均为 $O(1)$, 系统公钥参数长度和各接收者的计算代价都为 $O(n)$ 。在第二个方案 (General Case) 中, 对系统公钥参数和密文长度的复杂性进行了折中, 均为 $O(\sqrt{n})$, 而私钥长度仍为 $O(1)$ 。这两个方案都存在系统公钥参数和密文长度与接收者个数成线性增长关系的缺点。以 General Case 为例, 它实际上由一组并行的 Special Case 构造而成, 因此系统公钥参数的长度不能小于子组

个数。

本文将在第二个方案 General Case 的基础上作一些改进, 先简要介绍一下 General Case 中的 PKBE 方案。此方案中, 一个有 n 个接收者的组被划分为各有 B 个接收者的 A 个子组, 即 $A = \lceil n/B \rceil, |S_a| = B, 1 \leq a \leq A$ 。 G_1 是阶为 p 的双线性群, 生成元为 g 。

1) Setup(n): 中心选择秘密随机值 $\alpha \in Z_p$, 计算 $g_i = g^{\alpha^i} \in G_1 (i = 1, 2, \dots, B, B+2, \dots, 2B)$ 。然后选择 A 个随机值 $\gamma_1, \gamma_2, \dots, \gamma_A \in Z_p$, 并计算 $v_1 = g^{\gamma_1}, v_2 = g^{\gamma_2}, \dots, v_A = g^{\gamma_A} \in G_1$ 。 v_a 为第 a 个子组 S_a 的组公钥, 用于向 S_a 中的接收者发送消息。中心生成系统公钥参数 PK 如下:

$$PK = \langle g, g_1, g_2, \dots, g_B, g_{B+2}, \dots, g_{2B}, v_1, v_2, \dots, v_A \rangle \in G_1^{A+2B}$$

中心为每个接收者生成私钥 $d_i = g_b^{\gamma_a} \in G_1, i \in \{1, 2, \dots, n\}, i = (a-1)B + b$ 。 d_i 又可进一步整理为 $d_i = v_a^{b^a}$ 。

2) Broadcast(S, PK): 广播源选择秘密随机值 $t \in Z_p$, 设置会话密钥 $K = \hat{e}(g_{B+1}, g)^t \in G_2$, 并生成 Header 如下:

$$\text{Header} = \left(g^t, \left(v_1 \cdot \prod_{j \in S_1} g_{B+1-j} \right)^t, \left(v_2 \cdot \prod_{j \in S_2} g_{B+1-j} \right)^t, \dots, \left(v_A \cdot \prod_{j \in S_A} g_{B+1-j} \right)^t \right) \in G_1^{A+1}$$

广播源输出广播消息 $\langle \text{Header}, \text{Enc}_K(M) \rangle$ 。

3) Decryption($S, i, d_i, \text{Header}, PK$): 假设 Header 可表示为 (C_0, C_1, \dots, C_A) , 则指定接收子集中的一个接收者可通过如下计算恢复出会话密钥 K :

$$K = \hat{e}(g_i, C_a) / \hat{e}\left(d_i \cdot \prod_{j \in S_a, j \neq b} g_{B+1-j+b}, C_0\right)$$

接收者获得会话密钥 K 后可进一步解密出消息 M 。

2.2 改进后的 PKBE 方案

2.2.1 PKBE 方案描述

原方案中广播需要利用指定接收者的下标序号, 故广播源必须掌握与每个接收者相关联的系统公钥参数的下标序号。改进后的 PKBE 方案通过引入身份标志以区分各个接收者, 并利用一组接收者的身份标志代替原方案中的组公钥, 缩短了原方案中系统公钥参数的长度, 在系统公钥参数长度和密文长度之间进行了更加灵活的折中。原方案中的下标序号即可用作身份标志。改进后的方案具体描述如下:

1) G_1 是阶为 p 的双线性群, g 为 G_1 的生成元。假设接收者个数为 n , 并将其划分为 A 个子组, 每个子组含 B 个接收者。即 $A = \lceil n/B \rceil$, 且 $B \ll n$ 。中心选择一个安全 Hash 函数 $H: \{0, 1\}^* \rightarrow G_1$ 。

2) Setup(n): 各个接收者各自对应一个任意的身份标志, 此处为简便起见, 将方案中各个接收者的下标序号直接用作身份标志。中心选择秘密随机值 $\alpha \in Z_p$, 计算 $g_i = g^{\alpha^i} \in G_1 (i = 1, 2, \dots, B, B+2, \dots, 2B)$ 。

假设 S_a 表示接收者的下标序号从 $aB+1$ 到 $(a+1)B$ 的子组, 子组规模为 B , 即 $|S_a| = B$ 。中心生成系统公钥参数 PK 如下:

$$PK = \langle g, g_1, g_2, \dots, g_B, g_{B+2}, \dots, g_{2B} \rangle \in G_1^{2B}$$

第 i 个接收者可表示为 $i = (a-1)B + b$, 其中 $1 \leq a \leq A, 1 \leq b \leq B$ 。下标序号 i 和 a 用作接收者的身份标志。子组 S_a 的组身份标志可表示为 $aB+1 \parallel aB+2 \parallel \dots \parallel (a+1)B \parallel a$, 其

中 $1 \leq a \leq A$ 。下面将把子组 S_a 的组身份标志记为 GID_a , 则中心为每个接收者生成私钥 $d_i = H(GID_a)^{a_i \bmod B} (i \in \{1, 2, \dots, n\})$ 。

3) Broadcast(S, PK): 广播源选择秘密随机值 $t \in Z_p$, 设置会话密钥 $K = \hat{e}(g_{B+1}, g)^t \in G_2$, 并生成 Header 如下:

$$Header = (g^t, (H(GID_1) \cdot \prod_{j \in S_1} g_{B+1-j})^t, (H(GID_2) \cdot \prod_{j \in S_2} g_{B+1-j})^t, \dots, (H(GID_A) \cdot \prod_{j \in S_A} g_{B+1-j})^t)$$

广播源输出广播消息 $\langle Header, Enc_K(M) \rangle$ 。

4) Decryption($S, i, d_i, Header, PK$): 假设可表示为 (C_0, C_1, \dots, C_A) , 则一个指定接收者可通过如下计算, 用其私钥 d_i 和其他公共参数从 Header 中恢复出会话密钥 K :

$$K = \hat{e}(g_b, C_a) / \hat{e}(d_i \cdot \prod_{j \in S_a, j \neq b} g_{B+1-j+b}, C_0)$$

接收者获得会话密钥 K 后可进一步解密出消息 M 。

2.2.2 PKBE 方案的正确性证明

方案的正确性证明如下 ($i = (a-1)B + b$):

$$\begin{aligned} & \hat{e}(g_b, C_a) / \hat{e}(d_i \cdot \prod_{j \in S_a, j \neq b} g_{B+1-j+b}, C_0) = \\ & \frac{\hat{e}(g^{ab}, (H(GID_a) \cdot \prod_{j \in S_a} g_{B+1-j})^t)}{\hat{e}(H(GID_a)^{a_i \bmod B} \cdot \prod_{j \in S_a, j \neq b} g_{B+1-j+b}, g^t)} = \\ & \frac{\hat{e}(g^{ab}, (g_{B+1-b})^t) \cdot \hat{e}(g^{ab}, (H(GID_a) \cdot \prod_{j \in S_a, j \neq b} g_{B+1-j})^t)}{\hat{e}(H(GID_a)^{ab} \cdot \prod_{j \in S_a, j \neq b} g_{B+1-j+b}, g^t)} = \\ & \frac{\hat{e}(g_{B+1}, g)^t \cdot \hat{e}(g^{ab}, H(GID_a) \cdot \prod_{j \in S_a, j \neq b} g_{B+1-j})^t}{\hat{e}(H(GID_a)^{ab} \cdot \prod_{j \in S_a, j \neq b} g_{B+1-j+b}, g)^t} = \\ & \frac{\hat{e}(g_{B+1}, g)^t \cdot \hat{e}(g, H(GID_a)^{ab} \cdot \prod_{j \in S_a, j \neq b} g_{B+1-j+b})^t}{\hat{e}(H(GID_a)^{ab} \cdot \prod_{j \in S_a, j \neq b} g_{B+1-j+b}, g)^t} = \\ & \hat{e}(g_{B+1}, g)^t = K \end{aligned}$$

2.2.3 PKBE 方案的安全性证明

定理 1 假设是 H 一个随机预言器, 则对于任何的正整数 $n, B (n \gg B)$, 则改进后的 PKBE 方案 (t, ε, n) 是语义安全的, 若判定 (t', ε, n) -BDHE 困难问题假设在随机预言模型下的群 G_1 中是成立的, 其中 $t' = t + q_H$, 而 q_H 为 H -Queries 的查询次数。

证明 假设给定参数 B , 存在一个多项式时间 t 算法的攻击者 $A_{\text{Adversary}}$, 且 $Adv_{A, n}^{\text{PKBE}} > \varepsilon$, 构造算法 B_{Alg} , 其以优势 ε 解决 G_1 中的 B -BDHE 问题。 B_{Alg} 以随机的 B -BDHE 挑战 $(g, H, y_{g, \alpha, B}, Z)$ 作为输入, 其中 $y_{g, \alpha, B} = (g_1, g_2, \dots, g_B, g_{B+2}, \dots, g_{2B})$, Z 为 $\hat{e}(g_{B+1}, h)$ 或者 G_1 中的一个随机值 $g_i = g^{\alpha_i} \circ B_{\text{Alg}}$ 与 $A_{\text{Adversary}}$ 交互式运行如下:

1) Init: B_{Alg} 运行 $A_{\text{Adversary}}$, 并获得 $A_{\text{Adversary}}$ 准备挑战的子集 S_d 。

2) Setup: B_{Alg} 首先选择一个随机值 α , 计算 $g_i = g^{\alpha_i}$, 生成系统公钥参数 PK :

$$PK = \langle g, g_1, g_2, \dots, g_B, g_{B+2}, \dots, g_{2B}, H \rangle$$

然后 B_{Alg} 选择一个随机值 u_a , 计算 $H(GID_i)$ 如下 ($i = (a-1)B + b, 1 \leq a \leq A, 1 \leq b \leq B$):

$$H(GID_i) = g^{u_a} \left(\prod_{j \in S_a} g_{B+1-j} \right)^{-1}$$

计算 $H(GID_i), B_{\text{Alg}}$ 计算出不在子集 S_d 中的接收者的私钥 $d_i (i \notin S_d)$ 如下:

$$d_i = g_b^{u_a} \left(\prod_{j \in S_d} g_{B+1-j+b} \right)^{-1}$$

事实上, $d_i = (g^{u_a} \left(\prod_{j \in S_a} g_{B+1-j+b} \right)^{-1})^{\alpha_b} = H(GID_i)^{\alpha_b}$, 因此 B_{Alg} 有足够的值可以计算出私钥 $d_i \circ B_{\text{Alg}}$ 将 PKZ 和 $d_i (i \notin S_d)$ 发送给 $A_{\text{Adversary}}$ 。

3) H -Queries: $A_{\text{Adversary}}$ 向随机预言器 H 查询组身份标志的 Hash 值。为应答这些查询请求, B_{Alg} 需要维护一张表项为元组 $\langle GID_i, h_i \rangle$ 的表 $H_{\text{list}} \circ B_{\text{Alg}}$ 在应答 H -Queries 之前, 首先将 Setup 阶段计算出的 $h_i = g^{u_a} \left(\prod_{j \in S_a} g_{B+1-j} \right)^{-1}$ 设置为表 H_{list} 的前 A 项: $\langle GID_1, h_1 \rangle, \langle GID_2, h_2 \rangle, \dots, \langle GID_A, h_A \rangle$ 。若 GID_i 已经向 H 查询过, 则 H 返回表 H_{list} 中已有的 $h_i = H(GID_i)$; 否则, H 选择 G_1 中的一个随机值 h_i , 并将 h_i 作为查询结果返回给 $A_{\text{Adversary}}, B_{\text{Alg}}$ 同时将此表项 $\langle GID_i, h_i \rangle$ 添加到表 H_{list} 中。

4) Challenge: B_{Alg} 为生成挑战需要计算 $Header = \langle h, h^{u_1}, h^{u_2}, \dots, h^{u_A} \rangle$ 。其随机选择 $b \in \{0, 1\}$, 然后设置 $K_b = Z$, 并为 K_{1-b} 选择一个 G_1 中的随机值 h 。 B_{Alg} 将挑战 $\langle Header, K_b, K_{1-b} \rangle$ 发送给 $A_{\text{Adversary}}$ 。当 $Z = \hat{e}(g_{B+1}, h)$ 时, 则对 $A_{\text{Adversary}}$ 的挑战 $\langle Header, K_b, K_{1-b} \rangle$ 便是真实攻击行为中一个合法的挑战。假设 $t \in Z_p$ 未知, 且 $h = g^t$, 则对于 $i = 1, 2, \dots, A$, 有

$$\begin{aligned} h^{u_a} &= (g^{u_a})^t = (g^{u_a} \left(\prod_{j \in S_a} g_{B+1-j} \right)^{-1} \left(\prod_{j \in S_a} g_{B+1-j} \right))^t = \\ &= (H(GID_i) \prod_{j \in S_a} g_{B+1-j})^t \end{aligned}$$

因此, 用会话密钥 $\hat{e}(g_{B+1}, g^t)$ 加密的 Header 的真实性可检验如下:

$$\hat{e}(g_{B+1}, g^t) = \hat{e}(g_{B+1}, h) = Z = K_b$$

5) Guess: $A_{\text{Adversary}}$ 产生一个猜测值 $b' \in \{0, 1\}$ 。若 $b' = b$, B_{Alg} 输出 0, 此时 $Z = \hat{e}(g_{B+1}, g^t) = \hat{e}(g_{B+1}, h)$; 否则, B_{Alg} 输出 1, 此时 Z 为 G_1 中的随机值。

若 $(h, g, y_{g, \alpha, B}, Z)$ 是在 G_1 中随机选择的, 则概率 $Pr[B_{\text{Alg}}(h, g, y_{g, \alpha, B}, Z) = 0] = 1/2$ 。因此算法 B_{Alg} 可以至少 ε 的优势解决 G_1 中的 B -BDHE 问题:

$$|Pr[B_{\text{Alg}}(h, g, y_{g, \alpha, B}, Z) = 0] - 1/2| \geq \varepsilon$$

综上所述, 改进后的 PKBE 方案在随机预言模型下的判定 (t', ε, n) -BDHE 困难问题假设下是安全的。 证毕。

2.3 基于公钥广播加密的安全组播通信过程

改进后的 PKBE 方案适用于组成员较多的安全组播应用, 如分布式系统、网络视频会议等。这类组播应用的特点是整个组可按照地理区域划分为多个子组, 且各子组的成员数 B 有限, 即 $B \ll n$, 此外, 组内任何成员都可以向指定子组成员发起组播通信。基于公钥广播加密的安全组播体系结构如图 1 所示。图中的一组密钥生成中心 (Key Generation Center, KGC) 即为 PKBE 方案中的中心, 负责整个组播系统的初始化、组成员注册及系统公钥参数 PK 和各个组成员私钥的生成工作。

2.3.1 系统初始化及组成员注册

给定系统安全参数 $1^k (k = |p|)$, KGC 运行双线性 Diffie-

Hellman 参数生成算法 IG,生成如前定义的阶为大素数 p 的乘法循环群 G_1, G_2 , 以及一个双线性映射 $\hat{e}: G_1 \times G_1 \rightarrow G_2$, 选择 G_1 的一个生成元 g 。定义一个 Hash 函数 $H: \{0, 1\}^* \rightarrow G_1$ 。

希望加入组播组的用户向 KGC 注册成为组的合法成员。KGC 按照组成员所在的地理位置将整个大的组播组划分为多个子组, 为保证一定的通信效率, 各个子组的成员数应控制在 B 以内。假设整个组的成员数为 n , 则将其划分为 A 个子组, 每个子组含 B 个接收者。即 $A = \lceil n/B \rceil$, 且 $B \ll n$ 。 S_a 表示接收者的下标序号从 $aB+1$ 到 $(a+1)B$ 的子组, 第 i 个组成员可表示为 $i = (a-1)B + b$, 其中 $1 \leq a \leq A, 1 \leq b \leq B, i \in \{1, 2, \dots, n\}$ 。

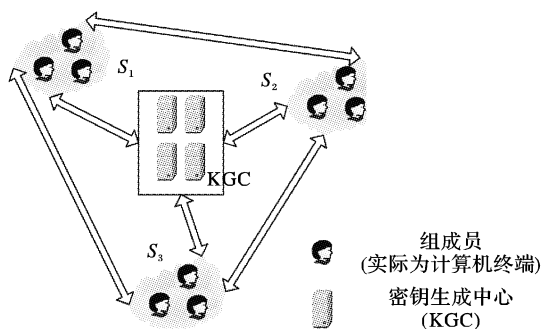


图1 基于公钥广播加密的安全组播体系结构

2.3.2 公钥及各个组成员私钥生成

KGC 注册运行 2.2 节中的 Setup(n) 算法,生成系统公钥参数 PK 以及各个组成员的私钥 d_i 。KGC 将 PK 作为公共参数

在整个组中发布, 并将私钥通过组成员注册时与 KGC 建立的秘密信道发送给各个组成员。

2.3.3 组播通信

假设子组 S_a 中有成员欲对整个组发送组播消息, 则其运行 2.2 节中的 Broadcast(S, PK) 算法, 选择随机值 $t \in Z_p$, 设置会话密钥 $K = \hat{e}(g_{B+1}, g)^t \in G_2$, 并生成 Header。采用对称加密算法 (如 AES) 将组播消息 M 用会话密钥 K 加密后, 连同 Header 生成最终的广播消息 $\langle \text{Header}, \text{Enc}_K(M) \rangle$ 。

各个指定接收的组成员在收到广播消息后, 运行 2.2 节中的 Decryption($S, i, d_i, \text{Header}, PK$) 算法, 结合自己的私钥提取出会话密钥 K 后, 便可进一步解密得到组播消息 M 。

3 安全性与计算及通信代价分析

由 2.2.3 节可知, 本文提出的安全组播方案是语义安全的^[8-9]。

文献[9]中提出的组播方案同样基于子组划分思想以及双线性对, 在解决组可扩展性和动态变化方面取得了较好的效果。但在此方案中, 用户端要执行最复杂的 Pairing 计算, 这对于计算能力一般都较弱的用户是不可接受的, 而本文方案中所做的运算则相对要少很多。

令 Sm 表示标量乘法运算, Pa 表示 Pairing 运算, Iv 表示整数求逆运算, Ex 表示指数运算, Ha 表示 Hash 运算。假设整个组的成员数为 n , 将其划分为 A 个子组, 每个子组含 B 个接收者, 则两个方案的计算代价如表 1 所示。

表 1 两个方案计算代价比较

过程	文献[9]的方案		本文的方案	
	U_i	KGC	U_i	KGC
初始化	$(\ln n) \text{ Pa}$	$(4n+1) \text{ Sm} + n \text{ Iv}$	—	$(n+2B-1) \text{ Ex} + A \text{ Ha}$
组播通信	$(\ln n) \text{ Pa}$	$(\ln n) \text{ Sm} + (\ln n) \text{ Iv}$	发送者: $(A+1) \text{ Ex}$ 接收者: 2 Pa	—

在系统初始化及组成员注册阶段, KGC 要与各个组成员进行 n 次单播通信。组播通信即为一次广播过程。令 Un 表示单播过程, Br 表示广播过程。两个方案的通信量分别如表 2 所示。

表 2 两个方案通信代价比较

过程	文献[9]的方案	本文方案
初始化	$n \text{ Un}$	$n \text{ Un}$
组播通信	$\text{Un} + (\ln n) \text{ Br}$	Br

4 结语

本文在文献[7]的基础上, 提出了一个新的 PKBE 方案, 对系统公钥参数长度和密文长度进行了更加进一步的折中, 具有较高的灵活性, 适用于规模较大的动态对等组播应用。具体分析了基于新的 PKBE 方案的安全组播通信过程, 结果表明, 与已有的方案相比, 无论在安全性还是降低计算及通信代价方面, 新方案都取得了较好的效果。

参考文献:

- [1] DEERING S. RFC 1112, Host extensions for IP multicasting [S]. IETF, 1989.
- [2] MA CHUN-BO, AO JUN, LI JIAN-HUA. A novel verifier-based authenticated key agreement protocol [C]// ICIC 2007: The 3rd International Conference on Intelligent Computing, CCIS 2. Berlin:

Springer-Verlag, 2007: 1044–1050.

- [3] YOON E-J, YOO K-Y. A new key agreement protocol based on chaotic maps [C]// KES-AMSTA 2008: Second KES International Symposium on Agent and Multi-agent Systems: Technologies and Applications, LNAI 4953. Berlin: Springer-Verlag, 2008: 897–906.
- [4] LAUR S, PASINI S. SAS-based group authentication and key agreement protocols [C]// PKC 2008: 11th International Workshop on Practice and Theory in Public Key Cryptography, LNCS 4939. Berlin: Springer-Verlag, 2008: 197–213.
- [5] CHEN L, CHENG Z, Smart N P. Identity-based key agreement protocols from pairings [J]. International Journal of Information Security, 2007, 6(4): 213–241.
- [6] BERKOVITS S. How to broadcast a secret [C]// EUROCRYPT'91, LNCS 547. Berlin: Springer-Verlag, 1991: 535–541.
- [7] BONEH D, GENTRY C, WATERS B. Collusion resistant broadcast encryption with short ciphertexts and private keys [C]// CRYPTO 2005, LNCS 3621. Berlin: Springer-Verlag, 2005: 258–275.
- [8] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [C]// CRYPTO 2001, LNCS 2139. Berlin: Springer-Verlag, 2001: 213–229.
- [9] WANG LI-MING, WU CHUAN-KUN. Efficient key agreement for large and dynamic multicast groups [J]. International Journal of Network Security, 2006, 3(1): 8–17.