

三接收方公钥密码系统

赵琉涛¹, 钟林², 刘吉东², 王彩群¹, 吴丹³

(1. 北京市计算中心, 北京 100094;

2. 北京北科融智云计算科技有限公司, 北京 100094;

3. 国家计算机网络应急技术处理协调中心, 北京 100089)

摘要: 提出一种三接收方公钥加密方案, 该方案中发送方对消息进行加密, 而三接收方均能够使用各自的私钥对消息进行解密。基于双线性映射, 构造出两个安全性不同的三接收方公钥加密方案。形式化证明如果间隙双线性 Diffie-Hellman 问题和计算性 Diffie-Hellman 问题是困难的, 则所提的两个方案分别具有选择明文攻击安全和适应性选择密文攻击安全。所提方案仅增加了一项指数运算和一项哈希运算, 就实现了 3 个独立的接收方, 因此该方案效率较高。分析表明, 该方案能够提高 TLS 协议的安全性并应用于分级监管公钥密码系统。

关键词: 三接收方; 公钥加密; 双线性映射; 间隙双线性 Diffie-Hellman 问题; 计算性 Diffie-Hellman 问题
中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020080

Triple receiver public key encryption cryptosystem

ZHAO Liutao¹, ZHONG Lin², LIU Jidong², WANG Caiqun¹, WU Dan³

1. Beijing Computing Center, Beijing 100094, China

2. Beijing Beike Rongzhi Cloud Computing Science and Technology Ltd., Beijing 100094, China

3. National Internet Emergency Center, Beijing 100089, China

Abstract: A triple receiver public key cryptosystem was proposed. In the cryptosystem, a sender encrypted a message and sent to three receivers, while the three receivers were able to decrypt the message with their own private keys. Based on bilinear map, two triple receiver public key encryption schemes with different security were constructed. If the gap bilinear Diffie-Hellman (GBDH) problem and the computational Diffie-Hellman (CDH) problem were proved formally to be intractable, then the two schemes proposed were semantically secure against chosen-plaintext attacks and against adaptive chosen ciphertext attacks respectively. The proposed scheme only added an exponential operation and a hash operation, and constructed three independent receivers which had a high efficiency. Analyses show that proposed scheme can improve the security of TLS protocol and apply to hierarchical

收稿日期: 2020-03-20; 修回日期: 2020-05-06

通信作者: 吴丹, wdan1985@126.com

基金项目: 2020 年北京市科学技术研究院财政专项

Foundation Item: Finance Special Project of Beijing Academy of Science and Technology in 2020

论文引用格式: 赵琉涛, 钟林, 刘吉东, 等. 三接收方公钥密码系统[J]. 网络与信息安全学报, 2020, 6(6): 128-136.

ZHAO L T, ZHONG L, LIU J D, et al. Triple receiver public key encryption cryptosystem[J]. Chinese Journal of Network and Information Security, 2020, 6(6): 128-136.

public key cryptosystems.

Key words: triple receiver, public key encryption, bilinear map, gap bilinear Diffie-Hellman problem, computational Diffie-Hellman problem

1 引言

1976年, Diffie-Hellman 首次提出公钥密码学, 开创了现代密码学的新领域。随后, Rivest、Shamir 和 Adleman 提出第一个实用的 RSA 公钥密码方案。在公钥加密可证明安全方面, Naor 和 Dolev 等提出可证明安全但低效的公钥加密方案; 随后, 在随机预言机模型下, Boneh 和 Franklin 提出高效的身份基公钥加密。

公钥加密方案不断发展, 从可证明安全到高效性。但是当今社会的发展产生许多新的应用场景, 如区块链、5G、物联网。这些新的应用场景需要功能更加丰富的公钥加密方案。上述公钥加密方案均围绕安全性和效率的视角开展, 缺乏从多接收方的视角发展, 而该方向是至关重要的。

考虑以下两个典型的应用场景。

① Alice 需要将同一段数据 m 加密发送给 Bob 和 Carol, 则 Alice 需要使用 Bob 与 Carol 的公钥对该段数据加密, 并使用零知识证明协议证明这两段密文包含的消息 m 是相等的。因此, Bob 和 Carol 能够确保收到了与对方相同的消息。但是, 如果 Alice 需要将同一段数据发送给 Bob、Carol 和 Dave, 则 Alice 需要使用两次零知识证明协议。该过程将导致用户需要进行计算复杂度较高的零知识证明和较长的数据发送与存储, 因此效率较低。

② 在一个典型的监管密码系统中, 发送方 Alice 加密消息 m 并发送给接收方 Bob。如果管理员需要查看 Bob 的密文数据, 则 Alice 还需要使用管理员的公钥将消息 m 加密发送给管理员并附带一段零知识证明数据, 从而导致效率较低。

针对上述两个典型的应用场景, 已有研究提出类似的解决方案。Diament 等^[1]提出一种双接收方公钥密码方案, 该方案使用了两个群上的双线性映射^[2-3]。类似于将 Diffie-Hellman 密钥交换协议扩展为 ElGamal 加密方案^[4-5], Diament 将三方一轮 Diffie-Hellman 密钥交换协议^[6]扩展为双接收方公钥加密方案。因此, 对于上述两个典型应用场景, 如果 Alice 将数据加密发送给 Bob 和

Carol, 或发送方 Alice 将数据发送给接收方 Bob 和管理员, 则不需要使用零知识证明协议^[7-8]。因此, 该方案极大地降低了计算复杂度和数据长度, 从而使协议运行效率较高。但是, 如果 Alice 需要将数据发送给 3 个接收方或公钥加密系统中有两个管理员, 则需要在 Diament 方案的基础上再使用一次零知识证明协议才能够满足期望的功能。但是, 零知识证明协议将极大降低 Diament 方案的效率, 使 Diament 方案实用性较差。如果使用门限密码系统^[9-10], 则系统效率较低, 且需要多个接收方合作才能够对密文进行解密。

针对应用场景二, 如果使用分级加密方案^[11-12], 则能够在一定程度上满足场景二的需求。在分级加密方案中, 管理员分发密钥给下级用户。发送方使用下级用户的公钥对消息加密, 则接收方和管理员均能够解密。但是, 该方案的缺点在于管理员拥有了下级用户的私钥, 下级用户数据的安全性不仅取决于算法的安全性, 还取决于管理员对私钥的保密性和管理员的诚实性。如果管理员不够诚实可靠, 则下级用户的消息是不安全的。此外, 管理员拥有大量的下级用户私钥, 且管理员的根密钥非常重要, 容易导致攻击者对管理员进行各种攻击, 如拒绝服务攻击^[13-14]或对根密钥进行攻击。

因此, 本文提出一种高效的三接收方公钥密码方案。该方案中, 存在 3 个独立的接收方。发送方使用 3 个独立的接收方的公钥对消息进行加密, 则 3 个接收方均能够使用各自的私钥对消息解密。该过程不需要零知识证明协议对消息的一致性进行证明, 因为该过程中消息加密生成的密文具有多功能性, 使三接收方的私钥均能够解密密文。本文方案是对 Diament 方案的进一步扩展, 而几乎不降低效率。本文提出的方案仅需要在 Diament 方案的基础上额外添加一项指数运算和一项哈希运算, 因此该方案效率较高。

2 研究现状

Diament^[1]等提出一个双接收方公钥密码系

统。该系统中的两个独立接收方能够使用各自的私钥对发送方生成的密文进行高效解密。如果其中一个接收方为管理员,则该公钥加密方案具有较好的监管应用。Diament 等使用 REACT 转换^[15],在缺口双线性 Diffie-Hellman 假设下^[16],将方案从选择明文攻击安全增强到适应性选择密文攻击安全。但基于 Groth-Sahai 证明系统^[17]构造高效的双接收方密码系统需要约 100 个群元素。随后,Chow 等^[18]对 Diament 提出的双接收方公钥加密方案进一步形式化,定义了双接收方公钥加密方案的可靠性(soundness)以确保两个独立的接收方能够解密获得相同的明文信息。该可靠性使双接收方公钥加密方案成为一个强大的密码学原语,如允许完美不可延展性和明文可识别性。

同时,双接收方密码系统能够解决安全难题(security puzzles),Zhang 等^[19]构造基于身份基加密方案对该安全难题进行了类似的解决。Back^[20]和 Zhang^[21]等研究了安全的结合公钥加密方案与关键词搜索公钥加密方案。Rogaway^[22]研究在保护密文长度的情况下,安全地结合选择明文攻击安全和选择密文攻击安全的公钥加密。最后,Wu 等^[23]研究了自组织广播加密方案,方案中任意发送方能够加密消息并发送给一个自组织群,且群中接收方能够独立解密而不需要可信第三方。但该方案仅考虑了选择明文攻击安全。

3 预备知识

3.1 双线性映射

本文方案需要使用双线性映射,以下对双线性映射进行简要介绍。

(1) $(G_1, *)$, $(G_2, *)$, $(G_T, *)$ 是 3 个循环群,其阶为大素数 p 。

(2) 群 G_1 的生成元为 g_1 , 群 G_2 的生成元为 g_2 。

(3) 双线性映射 $e: G_1 \times G_2 \rightarrow G_T$ 具有如下性质。

1) 双线性: 任意 $u \in G_1, v \in G_2, a, b \in \mathbb{Z}$, $e(u^a, v^b) = e(u, v)^{ab}$ 。

2) 非退化性: $e(g_1, g_2) \neq 1$, 因此 $e(g_1, g_2)$ 是群 G_T 的生成元。

如果 $G_1 = G_2$, 则称 e 为对称双线性映射,否则称之为非对称双线性映射。本文方案使用对称双线性映射。

3.2 困难问题

本文方案的安全性依赖于以下 4 个相关的复杂性假设,该假设使用群上的离散对数困难问题。

(1) 计算性 Diffie-Hellman 困难问题(computational Diffie-Hellman (CDH) problem): 给定 3 个群元素 $g, g^a, g^b \in G_1$, 其中 $a, b, c \in \mathbb{Z}$, 寻找一个群元素 $h \in G_1$, 使以下等式成立。

$$h = g^{ab} \quad (1)$$

(2) 双线性 Diffie-Hellman 困难问题(bilinear Diffie-Hellman (BDH) problem): 给定 4 个群元素 $g, g^a, g^b, g^c \in G_1$, 其中 $a, b, c \in \mathbb{Z}$, 寻找一个群元素 $g' \in G_T$, 使以下等式成立。

$$g' = e(g, g)^{abc} \quad (2)$$

(3) 判决性 Diffie-Hellman 困难问题(decision bilinear Diffie-Hellman (DBDH) problem): 给定群元素 $g, g^a, g^b, g^c \in G_1$, 其中 $a, b, c \in \mathbb{Z}$ 和 $h \in G_T$, 判断以下等式是否成立。

$$h = e(g, g)^{abc} \quad (3)$$

如果等式成立,则称 (P, aP, bP, cP, h) 为有效的 DBDH 五元组。

(4) 间隙双线性 Diffie-Hellman 困难问题(gap bilinear Diffie-Hellman (GBDH) problem): 预言机 Oracle 能够在多项式时间内判断 (P, aP, bP, cP, h) 是否为有效的 DBDH 五元组。攻击者在有限次访问预言机 Oracle 的情况下,不能在多项式时间内解决 BDH 困难问题。

4 方案设计

4.1 选择明文安全的三接收方公钥加密方案 Enc_i

(1) 初始化: 令 e 为对称双线性映射 $e: G_1 \times G_1 \rightarrow G_T$, g_1 为群 G_1 的生成元, 哈希函数 H_1 将长度为 $2n$ 的消息映射为固定长度 n 的随机数, $H_1: \{0,1\}^{2n} \rightarrow \{0,1\}^n$; 哈希函数 H_2 将群 G_T 中的元素映射为固定长度 n 的随机数, $H_2: G_T \rightarrow \{0,1\}^n$ 。

(2) 密钥生成: 用户 1 的私钥为 $SK_1 = a \in \mathbb{Z}_n$, 公钥为 $PK_1 = g_1^a \in G_1$; 用户 2 的私钥为 $SK_2 = b \in \mathbb{Z}_n$, 公钥为 $PK_2 = g_1^b \in G_1$; 用户 3 的私钥为 $SK_3 = c \in \mathbb{Z}_n$, 公钥为 $PK_3 = g_1^c \in G_1$; 用户

4 的私钥为 $SK_4 = d \in \mathbb{Z}_n$, 公钥为 $PK_4 = g_1^d$ 。

(3) 加密: 加密过程实现用户 1 对长度为 n 的消息 $m \in \{0,1\}^n$ 加密, 则用户 2、用户 3、用户 4 能够使用各自的私钥解密出消息 m 。

首先, 用户 1 选择随机数 $r_1 \in \{0,1\}^n$ 、用户 1 的私钥 $SK_1 = a$ 和用户 2 的公钥 $PK_2 = g_1^b \in G_1$, 随机数 α 的计算如式(4)所示。

$$\alpha \leftarrow H_1(PK_2^a, r_1) \quad (4)$$

然后, 用户 1 选择消息 m 、用户 3 的公钥 PK_3 和用户 4 的公钥 PK_4 , 计算如式(5)所示。

$$\begin{aligned} C_1 &\leftarrow r_1, C_2 \leftarrow g_1^\alpha, \\ C_3 &\leftarrow PK_3, C_4 \leftarrow m \oplus H_2(e(PK_3, PK_4)^\alpha) \end{aligned} \quad (5)$$

令 $C = (C_1, C_2, C_3, C_4)$, 则密文为 C 。用户 1 将密文 C 发送给用户 2、用户 3、用户 4。

(4) 解密: 用户 2、用户 3、用户 4 使用各自的私钥对密文 C 进行解密。

用户 2 解密: 用户 2 选择局部密文 C_1 、用户 1 的公钥 PK_1 和用户 2 的私钥 $SK_2 = b$, 计算如式(6)所示。

$$H_1(PK_1^b, C_1) = H_1(g_1^{ab}, r_1) = \alpha \quad (6)$$

然后, 用户 2 选择局部密文 C_4 、用户 3 的公钥 PK_3 和用户 4 的公钥 PK_4 , 计算如式(7)所示。

$$m \leftarrow C_4 \oplus H_2(e(PK_3, PK_4)^\alpha) \quad (7)$$

公式推导如下。

$$\begin{aligned} C_4 \oplus H_2(e(PK_3, PK_4)^\alpha) &= \\ m \oplus H_2(e(PK_3, PK_4)^\alpha) \oplus H_2(e(PK_3, PK_4)^\alpha) &= \\ m \oplus 0 &= m \end{aligned}$$

用户 3 解密: 用户 3 选择局部密文 C_2, C_3, C_4 和用户 3 的私钥 $SK_3 = c$, 计算如式(8)所示。

$$m \leftarrow C_4 \oplus H_2(e(C_2, PK_4)^c) \quad (8)$$

公式推导过程如下。

$$\begin{aligned} C_4 \oplus H_2(e(C_2, PK_4)^c) &= \\ m \oplus H_2(e(PK_3, PK_4)^\alpha) \oplus H_2(e(g_1^a, PK_4)^c) &= \\ m \oplus H_2(e(g_1^c, g_1^d)^\alpha) \oplus H_2(e(g_1^a, g_1^d)^c) &= \\ m \oplus H_2(e(g_1, g_1)^{cd\alpha}) \oplus H_2(e(g_1, g_1)^{adc}) &= \\ m \oplus 0 &= m \end{aligned}$$

用户 4 解密: 用户 4 选择局部密文 C_2, C_3, C_4 和用户 4 的私钥 $SK_4 = d$, 计算如式(9)所示。

$$m \leftarrow C_4 \oplus H_2(e(C_2, PK_3)^d) \quad (9)$$

公式推导过程如下。

$$\begin{aligned} C_4 \oplus H_2(e(C_2, PK_3)^d) &= \\ m \oplus H_2(e(PK_3, PK_4)^\alpha) \oplus H_2(e(g_1^a, PK_3)^d) &= \\ m \oplus H_2(e(g_1^c, g_1^d)^\alpha) \oplus H_2(e(g_1^a, g_1^d)^d) &= \\ m \oplus H_2(e(g_1, g_1)^{cd\alpha}) \oplus H_2(e(g_1, g_1)^{acd}) &= \\ m \oplus 0 &= m \end{aligned}$$

4.2 适应性选择密文安全的三接收方公钥加密方案 Enc₂

(1) 初始化: 令 e 为对称双线性映射 $e: G_1 \times G_1 \rightarrow G_T$, g_1 为群 G_1 的生成元, 哈希函数 H_1 将长度为 $2n$ 的消息映射为固定长度 n 的随机数, $H_1: \{0,1\}^{2n} \rightarrow \{0,1\}^n$; 哈希函数 H_2 将群 G_T 中的元素映射为固定长度 n 的随机数, $H_2: G_T \rightarrow \{0,1\}^n$; 哈希函数 H_3 将长度为 n 的数据映射为固定长度 n 的随机数, $H_3: \{0,1\}^n \rightarrow \{0,1\}^n$; 哈希函数 H_4 将长度为 n 的数据映射为固定长度 n 的随机数, $H_4: \{0,1\}^{4n+t} \rightarrow \{0,1\}^n$, 其中, t 指双线性群 G_T 点位置字符串表达长度。

(2) 密钥生成: 密钥生成过程与选择明文安全的三接收方公钥加密方案中的密钥生成过程相同。

(3) 加密: 首先, 用户 1 选择随机数 $r_1 \in \{0,1\}^n$ 、用户 1 的私钥 $SK_1 = a$ 和用户 2 的公钥 $PK_2 = g_1^b \in G_1$, 随机数 α 的计算如式(10)所示。

$$\alpha \leftarrow H_1(PK_2^a, r_1) \quad (10)$$

然后, 用户 1 选择消息 m 、随机数 $r_2 \in \{0,1\}^n$ 、用户 3 的公钥 PK_3 和用户 4 的公钥 PK_4 , 计算如式(11)所示。

$$\begin{aligned} C_1 &\leftarrow r_1, C_2 \leftarrow g_1^\alpha, C_3 \leftarrow PK_3, \\ C_4 &\leftarrow r_2 \oplus H_2(e(PK_3, PK_4)^\alpha) \\ C_5 &\leftarrow m \oplus H_3(r_2), \\ C_6 &\leftarrow H_4(r_2, m, C_4, C_5, e(PK_3, PK_4)^\alpha) \end{aligned} \quad (11)$$

其中, C_6 为密文校验位。令 $C = (C_1, C_2, C_3, C_4, C_5, C_6)$, 则密文为 C 。用户 1 将密文 C 发送给用

户 2、用户 3、用户 4。

(4) 解密。用户 2、用户 3、用户 4 使用各自的私钥对密文 C 进行解密。

用户 2 解密：用户 2 选择局部密文 C_1 、用户 1 的公钥 PK_1 和用户 2 的私钥 $SK_2 = b$ ，计算如式(12)所示。

$$H_1(PK_1^b, C_1) = H_1(g_1^{ab}, r_1) = \alpha \quad (12)$$

然后，用户 2 选择局部密文 C_4 、用户 3 的公钥 PK_3 和用户 4 的公钥 PK_4 ，计算如式(13)所示。

$$r_2 \leftarrow C_4 \oplus H_2(e(PK_3, PK_4)^\alpha) \quad (13)$$

最后，用户 2 选择局部密文 C_5 ，计算如式(14)所示。

$$\begin{aligned} m &\leftarrow C_5 \oplus H_3(r_2), \\ C_6' &\leftarrow H_4(r_2, m, C_4, C_5, e(PK_3, PK_4)^\alpha) \end{aligned} \quad (14)$$

如果哈希函数 H_4 输出 C_6' ，使 $C_6' = C_6$ 成立，则接受消息 m ，否则拒绝。

用户 3 解密：用户 3 选择密文 C_2, C_3, C_4 和用户 3 的私钥 $SK_3 = c$ ，计算如式(15)所示。

$$r_2 \leftarrow C_4 \oplus H_2(e(C_2, PK_4)^c) \quad (15)$$

然后，用户 3 选择局部密文 C_5 ，计算如式(16)所示。

$$\begin{aligned} m &\leftarrow C_5 \oplus H_3(r_2), \\ C_6' &\leftarrow H_4(r_2, m, C_4, C_5, e(PK_3, PK_4)^\alpha) \end{aligned} \quad (16)$$

如果哈希函数 H_4 输出 C_6' ，使 $C_6' = C_6$ 成立，则接受消息 m ，否则拒绝。

用户 4 解密：用户 4 选择密文 C_2, C_3, C_4 和用户 4 的私钥 $SK_4 = d$ ，计算如式(17)所示。

$$r_2 \leftarrow C_4 \oplus H_2(e(C_2, PK_3)^d) \quad (17)$$

然后，用户 4 选择局部密文 C_5 ，计算如式(18)所示。

$$\begin{aligned} m &\leftarrow C_5 \oplus H_3(r_2), \\ C_6' &\leftarrow H_4(r_2, m, C_4, C_5, e(PK_3, PK_4)^\alpha) \end{aligned} \quad (18)$$

如果哈希函数 H_4 输出 C_6' ，使 $C_6' = C_6$ 成立，则接受消息 m ，否则拒绝。

5 安全模型与形式化证明

如果攻击者从用户 3 和用户 4 角度对本文提出的两个方案进行攻击，则文献[1]已经证明公钥加密方案满足选择明文攻击安全，公钥加密方案满足适应性选择密文攻击安全。但是，本文提出的三接收方公钥密码系统中，攻击者还可能从用户 2 角度对方案进行攻击。因此，本节将证明如下定理。

定理 1 从用户 2 角度，如果计算性 Diffie-Hellman 问题是困难的，则在随机预言机模型下，本文提出的公钥加密方案满足选择明文攻击安全。

定理 2 从用户 2 角度，如果计算性 Diffie-Hellman 问题是困难的，则在随机预言机模型下，本文提出的公钥加密方案满足适应性选择密文攻击安全。

文献[15]提出 REACT 方案，将选择明文攻击安全的公钥加密方案转换为适应性选择密文攻击安全。本文提出的方案正是基于文献[15]的 REACT 转换对方案进行安全性提升的，即转换为适应性选择密文攻击安全。因此，如果本文提出的公钥加密方案从用户 2 角度满足选择明文攻击安全，则根据文献[15]，本文提出的公钥加密方案从用户 2 角度满足选择密文攻击安全。因此，本文仅对定理 1 进行安全性证明，而定理 2 的安全性证明参见文献[15]。

5.1 安全模型

从用户 2 角度，攻击者 $\mathcal{A}$ 有限次询问解密预言机之后，输出两个不同的消息。挑战者 $\mathcal{C}$ 对其中的任意一个消息加密，而攻击者 $\mathcal{A}$ 猜测挑战密文是对哪个消息的加密。形式化定义如下。

(1) 初始化：令 SP 为系统公共参数，挑战者 $\mathcal{C}$ 运行密钥生成算法，生成一对密钥 (SK, PK) 。

挑战者 $\mathcal{C}$ 将公钥 PK 发送给攻击者 $\mathcal{A}$ 。

(2) 询问阶段：攻击者 $\mathcal{A}$ 适应性地选择密文发送给挑战者 $\mathcal{C}$ ，挑战者 $\mathcal{C}$ 运行解密算法，并将解密结果发送给攻击者 $\mathcal{A}$ 。

(3) 挑战阶段：攻击者 $\mathcal{A}$ 输出两个长度相同而内容不同的消息 m_0, m_1 。挑战者 $\mathcal{C}$ 随机掷币 $\xi \in \{0, 1\}$ ，然后计算挑战密文 CT^* 。

$$CT^* = \left(\gamma^*, g_1^{H_1(g_1^r, \gamma^*)}, PK_3, m_\xi \oplus H_2(e(PK_3, PK_4)^{H_1(g_1^r, \gamma^*)}) \right) \quad (19)$$

挑战者 $\mathcal{C}$ 将挑战密文 CT^* 发送给攻击者 $\mathcal{A}$ 。

猜测阶段：攻击者 $\mathcal{A}$ 输出一个猜测值 ξ' 。如果 $\xi' = \xi$ ，则攻击者 $\mathcal{A}$ 赢得该博弈。

攻击者 $\mathcal{A}$ 赢得博弈的优势概率被定义为

$$\varepsilon = 2 \left(\Pr[\xi' = \xi] - \frac{1}{2} \right) \quad (20)$$

定义不可区分选择明文攻击安全 (IND-CPA)：从用户 2 角度，如果不存在攻击者 $\mathcal{A}$ 能够在 t 时间范围内以 ε 优势概率赢得上述博弈，则称该公钥加密方案在 IND-CPA 安全模型下是 (t, ε) 安全的。

5.2 形式化证明

假设存在一个攻击者 $\mathcal{A}$ 在 IND-CPA 安全模型下，在时间 t 内，以 ε 优势概率从用户 2 角度攻破公钥加密方案 Enc_1 ，则本文构造一个模拟器 $\mathcal{B}$ 能够在多项式时间内解决计算性 Diffie-Hellman 问题。给定一个循环群 (G_1, g_1, p) 上的问题实例 $(r_1, g_1, g_1^a, g_1^b, g_1^c, g_1^d)$ ，模拟器 $\mathcal{B}$ 调用 $\mathcal{A}$ 算法并进行如下运行。

(1) 初始化：令系统公共参数为 $SP = (G_1, G_T, p, g_1, G_1 \times G_1 \rightarrow G_T)$ ，令哈希函数 H_1 为随机预言机，该随机预言机由模拟器 $\mathcal{B}$ 控制。模拟器 $\mathcal{B}$ 令公钥为 $PK_1 \leftarrow g_1^\alpha, PK_2 \leftarrow g_1^\beta, PK_3 \leftarrow g_1^\varphi, PK_4 \leftarrow g_1^\eta$ 。这 4 个公钥来自问题实例，其中 $\alpha = a, \beta = b, \varphi = c, \eta = d$ 。模拟器 $\mathcal{B}$ 将这 4 个公钥 PK_1, PK_2, PK_3, PK_4 发送给攻击者 $\mathcal{A}$ 。

(2) 询问阶段：攻击者 $\mathcal{A}$ 进行哈希值询问。模拟器 $\mathcal{B}$ 存储一个哈希值列表，该列表记录所有的询问与响应。在询问之前，该哈希值列表为空。

令 γ_i 为第 i 次的询问值。如果 γ_i 在哈希值列表中，则模拟器 $\mathcal{B}$ 使用哈希值列表中的值发送给攻击者 $\mathcal{A}$ 。否则，模拟器 $\mathcal{B}$ 随机选择 $\omega_i \in \{0, 1\}^n$ ，并计算 $r_i \leftarrow H(\omega_i, \gamma_i)$ 。模拟器 $\mathcal{B}$ 将 r_i 发送给攻击者 $\mathcal{A}$ 并将 $(\omega_i, \gamma_i, r_i)$ 存储到哈希值列表中。

(3) 挑战阶段：攻击者输出两个长度相同而内容不同的消息 m_0, m_1 和一个随机数 γ^* ，模拟器随机掷币 $\xi \in \{0, 1\}$ ，计算 $r^* \leftarrow H(g_1^r, \gamma^*)$ ，并令

挑战密文为

$$CT^* = \left(\gamma^*, g_1^{H_1(g_1^r, \gamma^*)}, PK_3, m_\xi \oplus H_2(e(PK_3, PK_4)^{H_1(g_1^r, \gamma^*)}) \right) \quad (21)$$

其中， g_1^r 来自问题实例。如果 $\gamma^* = H(g^{a \cdot b}, \gamma^*)$ ，则挑战密文为

$$CT^* = \left(\gamma^*, g_1^{H_1(g^{a \cdot b}, \gamma^*)}, PK_3, m_\xi \oplus H_2(e(PK_3, PK_4)^{H_1(g^{a \cdot b}, \gamma^*)}) \right) \quad (22)$$

因此，挑战密文 CT^* 能够看作通过随机掷币 $\xi \in \{0, 1\}$ 选择消息 $m_\xi \in \{m_0, m_1\}$ 和公开随机数 γ^* 加密生成。从攻击者角度而言，如果没有对 γ^* 进行哈希查询，则挑战密文 CT^* 是正确构造的。

(4) 猜测阶段：攻击者 $\mathcal{A}$ 输出一个猜测值或 $\perp$ 。挑战值被定义为

$$\omega^* = g^{a \cdot b} \quad (23)$$

模拟器 $\mathcal{B}$ 从哈希值列表中 $(\omega_1, \gamma_1, r_1), \dots, (\omega_{q_H}, \gamma_{q_H}, r_{q_H})$ 随机选择一个值 $\omega_i (1 \leq i \leq q_H)$ 作为挑战值的查询值。模拟器 $\mathcal{B}$ 直接使用该值解决 CDH 问题。这就完成了仿真过程与解决过程。

(1) 不可区分性仿真：上述说明仿真过程的正确性。仿真过程的随机性包括密钥生成过程中的随机数、对哈希询问的响应值和挑战值的生成，分别是

$$SK_1, SK_2, SK_3, SK_4, \omega_1, \dots, \omega_{q_H}, \xi \quad (24)$$

根据仿真环境，其中 4 个私钥 (SK_1, SK_2, SK_3, SK_4) 、哈希询问的响应值和挑战值均是随机选择的，因此仿真的随机性是满足的。因此该仿真与实际攻击是不可分区的。

(2) 仿真成功概率：在仿真过程中，不存在中断过程，仿真成功概率为 1。

攻破挑战密文的优势概率：如果 $r^* = H(g^{a \cdot b}, \gamma^*)$ ，则挑战密文

$$CT^* = \left(\gamma^*, g_1^{H_1(g^{a \cdot b}, \gamma^*)}, PK_3, m_0 \oplus H_2(e(PK_3, PK_4)^{H_1(g^{a \cdot b}, \gamma^*)}) \right) \quad (25)$$

是通过一个公开随机数 γ^* 和消息 m_0 加密生成的，而挑战密文

$$CT^* = \left(\gamma^*, g_1^{H_1(g^{ab}, \gamma^*)}, PK_3, m_1 \oplus H_2(e(PK_3, PK_4)^{H_1(g^{ab}, \gamma^*)}) \right) \quad (26)$$

是通过一个公开随机数 γ^* 和消息 m_1 加密生成的。如果攻击者没有对公开随机数 γ^* 进行哈希查询, 则 γ^* 是随机的且攻击者不知道该值, 因此攻击者没有攻破该挑战密文的优势概率。

(4) 找到解的优势概率: 根据攻击假设, 由于攻击者能够以 ε 的优势概率猜测出挑战者加密的消息 m_0 或 m_1 , 所以攻击者以 ε 的优势概率向随机预言机询问了 g^{ab} 。攻击者共询问 q_H 次预言机。因此, 在集合 $\{\omega_i, 1 \leq i \leq q_H\}$ 中, 挑战者 $\mathcal{C}$ 随机选择一个值 ω 等于 g^{ab} 的概率为 $\frac{\varepsilon}{q_H}$ 。

(5) 优势概率与时间开销: 解决 CDH 问题的优势概率为 $\frac{\varepsilon}{q_H}$ 。

令 T_s 为仿真过程所需时间开销, 该过程为常量, $T_s = O(1)$ 。因此, 模拟器 $\mathcal{B}$ 解决 CDH 问题所需时间开销为 $t + T_s$ 。定理 1 证明完毕。

6 方案对比

如表 1 所示, 将本文提出的方案与文献[1]中的方案进行对比。表 1 中, 第 2 至 4 列展示了方案的私钥、公钥和密文的长度; 第 5 至 8 列分别展示了加密算法复杂度、各个接收方的解密计算复杂度、接收方个数和算法基于的复杂性假设。

其中, E 是指数运算, P 是双线性映射, H 是哈希运算。如表 1 所示, 本文在文献[1]的基础上添加了 1 个接收方, 而用户的私钥和公钥长度均不变, 本文 CPA 安全方案和 CCA2 安全方案的密文长度仅增加 n 。在加密计算复杂度方面, 本

文 CPA 安全方案和 CCA2 安全方案均只增加了一项指数运算和一项哈希运算, 而没有增加映射运算。此外, 指数运算和哈希函数的运算效率较高。在解密计算复杂度方面, 用户 3 和用户 4 的解密复杂度与文献[1]中两个用户的解密复杂度相等, 而用户 2 的解密复杂度仅增加了一项指数运算和一项哈希运算, 该过程效率也较高。文献[1]的方案基于 DBDH 复杂性假设, 而本文额外增加了 CDH 复杂性假设。由于 CDH 复杂性假设是当前密码算法中最经典的困难问题, 因此该假设的引入不会导致算法安全性降低。

此外, 将本文方案与文献[1]中的方案进行实验测试。实验设备信息: 内核 x86_64 操作系统 Linux 4.17.6-1-ARCH, 运算芯片 Intel i5-7200U 2.50 GHz, 内存 8 GB。实验选择 SHA256 作为哈希函数的具体实现和使用超奇异椭圆曲线; 有限域为 512 bit, 离散对数安全范围为 1 024 bit, 椭圆曲线群的阶为 160 bit。如表 2 所示, 横向表示算法的加密时间和各个接收方的解密时间, 纵向表示本文和文献[1]提出的 CPA/CCA2 安全的方案。

实验结果表明, 本文提出的 CPA 安全方案加密时间相比文献[1]中的 CPA 安全方案加密所需时间仅增加约 0.54 ms; 该方案中额外添加的一个接收方的解密时间仅比其他接收方的解密时间增加约 0.54 ms。类似地, 本文提出的 CCA2 安全方案加密时间相比文献[1]中的 CCA2 安全方案加密所需时间仅增加约 0.55 ms; 本文方案中额外添加的一个接收方的解密时间仅比其他接收方的解密时间增加约 0.54 ms。因此, 本文提出的密码方案在添加一个接收方的情况下, 计算时间仅增加约 0.54 ms, 效率较高。

表 1 方案性能对比
Table1 Comparison of performance

安全方案	私钥长度	公钥长度	密文长度	加密算法复杂度	解密计算复杂度	接收方个数	复杂性假设
文献[1]CPA	n	p	$2p+n$	1E+1H+1P	1E+1H+1P, 1E+1H+1P	2	DBDH
文献[1]CCA2	n	p	$2p+3n$	1E+3H+2P	1E+3H+1P, 1E+3H+1P	2	DBDH
本文 CPA	n	p	$2p+2n$	2E+2H+1P	2E+2H+1P, 1E+1H+1P, 1E+1H+1P	3	CDH, DBDH
本文 CCA2	n	p	$2p+4n$	2E+4H+2P	2E+4H+1P, 1E+3H+1P, 1E+3H+1P	3	CDH, DBDH

表2 方案测试对比
Table 2 Comparison of test

安全方案	加密时间/ms	解密时间/ms		
文献[1]CPA	9.02	9.01	9.02	
文献[1]CCA2	17.51	9.02	9.03	
本文 CPA	9.56	9.56	9.01	9.02
本文 CCA2	18.06	9.56	9.03	9.04

7 应用分析

文献[1]提出使用双接收方的方案能够应用于缓解 TLS 协议^[24-26]的安全性问题,而本文提出的三接收方方案也能够类似运用于缓解 TLS 协议的安全性问题。此外,如果将本文方案中的用户 2 看作高级管理员,用户 3 看作一般管理员,用户 4 看作消息接收方,则本文提出的方案能够扩展为分级管理的公钥加密方案。如果要求发送方每次在消息加密过程中必须使用高级管理员(即用户 2)和部分使用一般管理员(即用户 3),则用户 2 能够监管所有接收方的消息,用户 3 能够监管部分密文消息。

8 结束语

本文提出了三接收方公钥加密方案,该方案具有 3 个接收方;同时给出了具有选择明文攻击安全的公钥加密方案和具有选择适应性选择密文攻击安全的公钥加密方案;形式化证明了如果 DBDH 问题和 CHD 问题是困难的,则本文提出的两个三接收方公钥加密方案具有选择明文攻击安全和适应性选择密文攻击安全。对比表明,本文提出的方案与文献[1]中的方案具有相同的私钥和公钥长度,而密文仅增加 n 位、加密和解密计算复杂度仅增加一项指数运算和一项哈希运算,因此该方案效率较高。

参考文献:

- [1] DIAMENT T, LEE H K, KEROMYTIS A D, et al. The dual receiver cryptosystem and its applications[C]//Proceedings of the 11th ACM Conference on Computer and Communications Security. 2004: 330-343.
- [2] BONEH D, BOYEN X. Short signatures without random oracles and the SDH assumption in bilinear groups[J]. Journal of Cryptology, 2008, 21(2): 149-177.
- [3] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2001: 514-532.
- [4] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.
- [5] TSIOUNIS Y, YUNG M. On the security of ElGamal based encryption[C]//International Workshop on Public Key Cryptography. 1998: 117-134.
- [6] JOUX A. A one round protocol for tripartite Diffie-Hellman[C]//International algorithmic number theory symposium. 2000: 385-393.
- [7] DAMGÅRD I. On Σ -protocols[J]. Lecture Notes, University of Aarhus, Department for Computer Science, 2002.
- [8] RACKOFF C, SIMON D R. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack[C]//Annual International Cryptology Conference. 1991: 433-444.
- [9] DESMEDT Y G. Threshold cryptography[J]. European Transactions on Telecommunications, 1994, 5(4): 449-458.
- [10] BAUM C, DAMGÅRD I, OECHSNER S, et al. Efficient commitments and zero-knowledge protocols from ring-sis with applications to lattice-based threshold cryptosystems[J]. IACR Cryptology ePrint Archive, 2016, 2016: 997.
- [11] WEBER J W. Hierarchical encryption key system for securing digital media: U.S. Patent 7,480,385[P]. 2009-1-20.
- [12] BONEH D, BOYEN X, GOH E J. Hierarchical identity based encryption with constant size ciphertext[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2005: 440-456.
- [13] SCHUBA C L, KRSUL I V, KUHN M G, et al. Analysis of a denial of service attack on TCP[C]//Proceedings of 1997 IEEE Symposium on Security and Privacy. 1997: 208-223.
- [14] CARL G, KESIDIS G, BROOKS R R, et al. Denial-of-service attack-detection techniques[J]. IEEE Internet Computing, 2006, 10(1): 82-89.

- [15] OKAMOTO T, POINTCHEVAL D. REACT: rapid enhanced-security asymmetric cryptosystem transform[C]//Cryptographers' Track at the RSA Conference. 2001: 159-174.
- [16] OKAMOTO T, POINTCHEVAL D. The gap-problems: a new class of problems for the security of cryptographic schemes[C]//International Workshop on Public key Cryptography. 2001: 104-118.
- [17] GROTH J, SAHAI A. Efficient non-interactive proof systems for bilinear groups[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2008: 415-432.
- [18] CHOW S S M, FRANKLIN M, ZHANG H. Practical dual-receiver encryption[C]//Cryptographers' Track at the RSA Conference. 2014: 85-105.
- [19] ZHANG R, HANAOKA G, IMAI H. A generic construction of useful client puzzles[C]//Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. 2009: 70-79.
- [20] BAEK J, SAFARI-NAINI R, SUSILO W. On the integration of public key data encryption and public key encryption with keyword search[C]//International Conference on Information Security. 2006: 217-232.
- [21] ZHANG R, IMAI H. Generic combination of public key encryption with keyword search and public key encryption[C]//International Conference on Cryptology and Network Security. 2007: 159-174.
- [22] ROGAWAY P. Efficient instantiations of tweakable block ciphers and refinements to modes OCB and PMAC[C]//International Conference on the Theory and Application of Cryptology and Information Security. 2004: 16-31.
- [23] WU Q, QIN B, ZHANG L, et al. Ad hoc broadcast encryption[C]//2010 ACM Conference on Computer and Communications Security. 2010: 741-743.
- [24] DIERKS T, ALLEN C. The TLS protocol version 1.0[S]. 1999.
- [25] KRAWCZYK H, PATERSON K G, WEE H. On the security of the TLS protocol: a systematic analysis[C]//Annual Cryptology Conference. 2013: 429-448.
- [26] MAVROGIANNOPOULOS N, VERCAUTEREN F, VELICHKOV V, et al. A cross-protocol attack on the TLS protocol[C]//2012 ACM Conference on Computer and Communications Security. 2012: 62-72.

[作者简介]



赵疏涛（1979—），男，北京人，北京市计算中心研究员，主要研究方向为信息安全、区块链、高性能计算。

钟林（1987—），男，四川内江人，博士，北京北科融智云计算科技有限公司工程师，主要研究方向为公钥密码学、区块链技术。

刘吉东（1976—），男，山东长岛人，北京北科融智云计算科技有限公司工程师，主要研究方向为区块链技术及相关软件实施。

王彩群（1989—），女，河南商丘人，北京市计算中心高级工程师，主要研究方向为机器学习、区块链、计算材料。

吴丹（1985—），女，北京人，国家计算机网络应急技术处理协调中心助理研究员，主要研究方向为网络安全。