计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2019.20180130
56(5):1101-1111,2019

通用可复合的 ElGamal 型广播多重签密协议

李建民[1,3]　俞惠芳[2]　谢　永[4]
[1](青海省气象台　西宁　810001)
[2](西安邮电大学通信与信息工程学院　西安　710121)
[3](青海师范大学计算机学院　西宁　810008)
[4](青海大学计算技术与应用系　西宁　810003)
(940721138@qq.com)

ElGamal Broadcasting Multi-Signcryption Protocol with UC Security

Li Jianmin[1,3], Yu Huifang[2], and Xie Yong[4]
[1](*Metorological Observatory of Qinghai Province*, *Xining* 810001)
[2](*School of Communication and Information Engineering*, *Xi'an University of Posts & Telecommunications*, *Xi'an* 710121)
[3](*School of Computer*, *Qinghai Normal University*, *Xining* 810008)
[4](*Department of Computer Technology and Application*, *Qinghai University*, *Xining* 810003)

Abstract Multi-signcryption means two or more parties sign the same message, moreover, the length of signcryption cannot linearly increase for the increasing of the number of signers. Although ordinary ElGamal multi-signature satisfies the unforgeability, however, it can't resist joint attack of multiple signers. In order to overcome the shortcomings of existing ElGamal multi-signature, the authors integrate the techniques of ElGamal multi-signature and signcryption to present a new ElGamal broadcasting multi-signcryption (EBMSC) protocol. We also describe its algorithm definition and security model, and prove its semantical security under the discrete logarithm (DL) and computation Diffie-Hellman (CDH) assumptions in the random oracle model (ROM). At the same time, we define the ideal function and the real protocol of EBMSC protocol under the universally composalble (UC) security framework, and then prove that the real protocol can realize the ideal function of EBMSC protocol. It also proves that the real protocol is unforgeable under unforgeability against adaptive chosen message attacks. Finally, the efficiency comparison between EBMSC protocol and existing protocols is given. Analysis results show our protocol not only is more efficient than existing protocols but also implements the function of multi-signcryption in UC security framework. Our protocol can be suitable for applications in e-commerce, contract signing, online transaction and financial accounting.

Key words ElGamal multi-signature; ElGamal broadcasting multi-signcryption (EBMSC); semantical security; random oracle model; universally composalble (UC) security

摘　要　多重签密是指2个以上参与方对同一则消息进行签密,并且要求签密结果不能因为签密者数目增多而呈线性增长.普通的ElGamal型多重签名虽然具有不可伪造性,但不能抵制多个签名者的联合

收稿日期:2018-02-21;**修回日期**:2018-09-26
基金项目:国家自然科学基金项目(61363080,61572303,61772326);青海省基础研究计划项目(2016-ZJ-776)
This work was supported by the National Natural Science Foundation of China (61363080, 61572303, 61772326) and the Project of Basic Research of Qinghai Province (2016-ZJ-776).
通信作者:俞惠芳(yuhuifang@qhnu.edu.cn)

攻击.为了克服现有 ElGamal 型多重签名的缺点,将 ElGamal 型多重签名和公钥签密组合在一起研究.提出了一种新的 ElGamal 型广播多重签密(ElGamal broadcasting multi-signcryption, EBMSC)协议,并给出了该协议的算法定义和安全模型,也在随机预言模型中证明了该协议在离散对数和计算性 Diffie-Hellman 假设下是语义安全的;然后在通用可复合框架下定义了 ElGamal 型广播多重签密协议的理想函数和现实协议,进而证明了现实协议能够实现广播多重签密协议的理想功能,同时还证明了现实协议是满足选择消息攻击下的不可伪造性;最后给出了 ElGamal 型广播多重签密协议与其他协议的效率比较.结果表明:该协议不仅在效率上要优于现有方案,而且在通用可复合框架下实现了多重签密功能.该协议适合应用在电子商务、合同签署、网上交易和财务出账等方面.

关键词 ElGamal 多重签名;ElGamal 型广播多重签密;语义安全;随机预言模型;通用可复合安全

中图法分类号 TP309

多重签名[1]是指 2 个以上的签名者对同一则消息进行签名,同时要求签名的长度不会因为签名者数目增多而呈线性增长,该类方案在电子商务领域被广泛应用.目前多重签名主要使用 RSA(rivest shamir adleman)[2]、ElGamal[3-4]、双线性对[5]、离散对数[6-7]等思想来设计.1994 年 Harn[8]提出了 Meta-ElGamal 多重签名.1996 年 Wu 等人[9]依据签名的签署顺序不同,将多重签名区分为顺序多重签名和广播多重签名.顺序多重签名意味着签名者必须按照特有的顺序依次对消息进行签名;广播多重签名是指签名者不必拘泥于固有的顺序,按广播的方式对消息进行签名,由收集者合并且输出签名.广播多重签名相比顺序多重签名应用更为广泛,ElGamal 型多重签名的安全性基于 DL(discrete logarithm)问题的难解性,满足不可伪造性,缺点是不具备签名者的身份验证,不能抵制多个签名者的联合攻击.

1997 年 Zheng[10]提出了签密方案.签密方案相对于传统的签名方案而言,能够同时完成签名和加密 2 项功能.签名方案只是确保设计方案的不可伪造性,在安全性分析时,只要方案满足选择消息攻击的不可伪造性,那么就说设计的方案是语义安全的.签密方案能够在一个合理的逻辑步骤内同时完成签名和加密,在安全性分析时,不仅要分析方案的保密性,还要分析方案的不可伪造性.

2002 年 Baek 等人[11]对 Zheng 的签密方案进行了改进,同时给出了随机预言模型下的安全性证明.2011 年 Fan 等人[12]改进了 2002 版本的签密方案,在 Hash 函数的输入中添加了接收方和发送方的公钥.近年来,越来越多的学者将签密和具有特殊性质的签名结合起来进行研究,使用不同的认证方法来认证用户公钥[13-19].2016 年周才学[20]指出很多签密方案还存在安全问题,同时他认为在解签密算法的验证等式中不应出现明文信息,加密部分应该包含发送者的公钥或身份信息,签名部分应包含接收者的公钥或身份信息,在无证书密码体制的签名部分中不要让部分私钥和秘密值之间只是存在简单的线性关系.

UC(universally composalble)安全框架[21]满足协议的模块化设计要求,可以单独用来设计协议.只要协议满足 UC 安全性,则可以保证和其他协议并发组合运行的安全性.设计一个 UC 安全协议,首先要将协议所希望完成的功能抽象为一个理想函数,该理想函数相当于现实世界中一个不可攻破的可信第三方.2003 年 Canetti 等人[22]纠正了自己在 2001 年提出的签名理想函数的定义,通过添加 SID(session identifier)来编码签名者的身份,允许被收买的签名者对合法的签名进行验证,对公钥、签名、验证消息进行储存;2007 年 Kristian 等人[23]利用用户友好交互提出了一个安全消息传递理想函数,给出了签密的理想函数;2012 年 Canetti 等人[24]提出了不经意传输(oblivious transfer, OT)协议的理想函数,同时给出了使用 OT 协议的双向认证协议的通用方法.国内对 UC 安全的研究也取得了一些成果,冯涛等人[25]利用可否认加密体制和可验证平滑投影 Hash 函数提出了一个 UC 安全的高效不经意传输协议;苏婷等人[26]基于密钥注册模型形式化定义了签密协议的安全模型(即签密协议的理想函数),设计了一般化的签密协议,给出了 UC 框架下的证明;张忠等人[27]形式化定义了信息处理集合和无线射频识别(radio frequency identification, RFID)组证明的理想函数,然后设计了一个组证明 RFID 协议,证明了该协议安全地实现了理想功能;田有亮等人[28]利用身份签密机制提出了一个 UC 安全的群通信协议,解决了多播群组通信的组合安全问题,

之后,他们又设计了一个通用可组合的安全多方计算协议[29],即在 UC 框架下能实现公平的安全两方计算协议,使人们认为的两方公平安全计算不能实现的问题得到解决.

本文结合自认证公钥和 Meta-ElGamal 多重签名协议的思想,在 UC 框架下设计了一个 ElGamal 型广播多重签密(ElGamal broadcasting multi-signcryption, EBMSC)协议,进而在 UC 安全框架下分析了该协议的安全性.也给出了 ElGamal 型广播多重签密协议的 UC 安全性证明.

1 预备知识

1.1 困难假设

定义 1. DL 假设.设 G 是阶为素数 p 的循环群, g 是 G 的一个生成元.已知 (p,G,w),找到一个 $a\in\mathbb{Z}_p^*$,使得 $w\in g^a$ 是困难的.

定义 2. CDH 假设.设 G 是素数阶 p 的循环群,g 是 G 的一个生成元.已知 $(g^a,g^b\in G^*$,其中 $a,b\in\mathbb{Z}_p^*)$,找到 $g^{ab}\in G$ 是困难的.

1.2 UC 安全框架

UC 安全框架是由现实模型、理想模型和混合模型组成.在 UC 框架中,用交互式图灵机(interactive turing machine, ITM)来描述协议的参与方、敌手和环境机等实体.每个 ITM 的运行都被限定在概率多项式时间内.在现实模型中,包括了参与方 P、敌手 A、协议 π 和环境机 Z 等实体,参与方 P 不仅诚实地执行协议 π,而且相互之间还可以直接通信.在理想模型中,包括了参与方 P、模拟者 S、理想函数 F 和环境机 Z 等实体.和现实模型不一样的是,参与方 P 相互之间不能直接通信,而是通过理想函数 F 来转发信息,现实模型和理想模型的外部环境 Z 相同.由于模块化的设计思想,只要证明某个协议能满足 UC 安全性,则和其他协议并发运行也能保证其安全性.

定义 3. 不可区分性[21].X 和 Y 是 2 个不可区分的二元分布集合(记作 $X\approx Y$),如果任何 $c\in\mathbb{N}$ 都有 $k_0\in\mathbb{N}$,使得所有 $k>k_0$ 和所有的 a,都有:

$$|Pr(X(k,a)=1)-Pr(Y(k,a)=1)|<k^{-c}.$$

定义 4. UC 仿真[21].设 $n\in\mathbb{N}$,令 F 是理想函数,π 具有 n 个参与方的协议,τ 是现实中某类敌手.若对任何现实攻击者 $A\in\tau$ 都存在一个理想过程中的敌手 S,使得任何环境机 Z 都不能区分它是与 (π,A) 交互还是与 (F,S) 交互,则称 π 安全实现了 F,记作:

$$IDEAL_{F,S,Z}\approx REAL_{\pi,A,Z}.$$

定义 5. 组合定理[21].令 F 和 G 是理想函数,π 是 F-混合模型下的一个协议,ρ 协议在 G-混合模型下可以安全地实现 F.则对于任何敌手 A_G,都存在一个 A_F,使得对于任何环境机 Z,都有:

$$EXEC^F_{\pi,A_F,Z}\approx EXEC^G_{\pi_r,A_G,Z}.$$

1.3 基于离散对数的多重签名回顾

Harn[8]利用离散对数提出了一种有效的多重签名方案.假设 n 个签名者对同一消息 m 进行签名.

1) 每一个签名者 u_i 从 $[1,p-1]$ 中随机选取 k_i,计算 $r_i=\alpha_i^{k_i} \bmod p$,然后将 r_i 广播给所有的签名者.一旦来自所有签名者的 $r_i(i=1,2,\cdots,n)$,汇聚在广播通道中,每一签名者计算 r 的值:

$$r=\sum_{i=1}^{n} r_i \bmod p.$$

2) 签名者 u_i 用秘钥 z_i 和 k_i 对消息 m 运行签名算法.即 $s_i=(z_i(m'+r)-k_i) \bmod p$,其中 $0\leqslant s_i\leqslant p-2$ 和 $m'=f(m)$.签名者把元组 (m,s_i) 发送给消息收集者.

3) 收集者收到来自各个 u_i 的签名 (m,s_i),验证 $y_i^{m'+r}=r_i\alpha^{s_i} \bmod p$,这里 $m'=f(m)$,y_i 是 u_i 的公钥.

4) 消息收集者将对通过验证的消息进行合并:$s=(s_1+s_2+\cdots+s_n) \bmod p$,得到完整的签名 (r,s).

5) 验证者计算公钥:$y=\prod_{i=1}^{n} y_i \bmod p$.

6) 验证 $y^{m'+r}=r\alpha^s \bmod p$,这里 $m'=f(m)$.

2 EBMSC 协议的形式化定义

2.1 EBMSC 算法定义

一个 EBMSC 协议由 4 个算法组成:参与方包括消息发起者或签密收集者 U_C、签密者 $U_1,U_2,\cdots,U_n$、接收者 U_V.

系统设置算法:输入安全参数 1^k,生成系统主密钥 s 和系统参数 $params$.

密钥提取算法:身份 ID_u 的用户随机选择秘密钥生成其公钥 y_u,而密钥生成中心(key generator central, KGC)随机选择秘密钥 η_u,然后根据用户身份 ID_u 和公钥 y_u 生成其部分私钥 T_u,之后安全的形式发给用户.用户收到部分私钥 T_u 后,计算完整私钥 x_u.

多重签密算法:输入系统的参数 $params$、明文 m、签密者 U_i 的私钥 x_i 及接收者 U_V 的公钥 y_V,输出多重签密密文 σ.

解签密算法:输入密文 σ、参数 $params$、签密者 U_i 的公钥 y_i 及接收者 U_V 的私钥 x_V,输出明文 m 或者解签密符号 $\perp$.

2.2 安全模型

一个 EBMSC 协议有 2 类敌手,即 A_1 和 A_2. 敌手 A_1 无法得到系统的主密钥,但是可以替换用户的公钥(敌手 A_1 相当于模拟了不诚实的用户);敌手 A_2 可以得到系统的主密钥,但不能替换用户的公钥(敌手 A_2 相当于模拟了恶意的 KGC).

定义 6. 如果存在任何多项式有界的敌手 A_1 和 A_2 赢得游戏 IND-CCA2-I 和 IND-CCA2-II 的优势是可忽略的,则称 EBMSC 协议是具有适应性选择密文攻击下的不可区分性(indistinguishability against adaptive chosen ciphertext attacks, IND-CCA2).

IND-CCA2-I:这是挑战者 C 和敌手 A_1 之间的交互游戏.

初始化. C 运行系统设置算法得到系统参数 $params$ 和系统主密钥 s,之后将系统参数 $params$ 发给 A_1,但保留主密钥 s.

阶段 1. A_1 进行多项式有限次询问.

公钥询问:当收到 A_1 的公钥询问时,C 运行密钥提取算法中的用户公钥生成算法得到 y_i,返回给 A_1.

部分私钥提取询问:A_1 可以请求身份 ID_u 的部分私钥询问,C 运行密钥提取算法中的部分密钥生成算法得到 T_u,之后把 T_u 返回给 A_1.

私钥提取询问:A_1 可以请求身份 ID_u 的私钥询问,C 运行密钥提取算法中的私钥生成算法得到 x_u,之后把 x_u 返回给 A_1.

签密询问:A_1 收到(ID_i, ID_V, m)的签密询问时,C 通过调用签密算法得到多重签密密文 σ,之后将 σ 发给 A_1.

解签密询问:A_1 收到(ID_i, ID_V, σ)时,C 通过调用解签密算法得到的消息 m_i 之后返给 A_1.

挑战阶段. A_1 生成 2 个等长的消息(m_0, m_1)及 2 个身份(ID_i^*, ID_V^*),但要求接收者 ID_V^* 的部分私钥不能被询问. C 随机选择 $\delta \in \{0,1\}$,然后执行对 δ 的多重签密,之后将 δ^* 发给 A_1.

阶段 2. A_1 可以像阶段 1 那样进行多项式有界次询问,但仍然要求 ID_V^* 的私钥不能被询问,此外不能做 σ^* 的解签密询问.

最后,输出 $\delta' = \{0,1\}$作为对 δ 的猜测. 如果 $\delta' = \delta$,则 A_1 赢得游戏.

IND-CCA2-II: 前面各阶段和敌手 A_1 一样,只是敌手 A_2 最后赢得游戏的条件是 ID_V^* 的私钥不能被询问,而且不能做 σ^* 的解签密询问,除非接收者 ID_V^* 的公钥被替换.

定义 7. 如果存在任何多项式有界的敌手 A_1 和 A_2 赢得游戏 UF-CMA-I 和 UF-CMA-II 的优势是可忽略的,则称 EBMSC 协议是具有适应性选择消息攻击下的不可伪造性(unforgeability against adaptive chosen message attacks, UF-CMA).

UF-CMA-I:C 和伪造者 A_1 之间的交互游戏.

初始化. C 运行系统设置算法得到系统参数 $params$ 和系统主密钥 s,之后将系统参数 $params$ 发给 A_1,但保留主密钥 s.

训练. A_1 进行的多项式有界次询问和定义 6 中 IND-CCA2-I 的阶段 1 一样.

伪造. 当询问结束后,A_1 输出伪造的多重签密密文$(ID_i^*, ID_V^*, \sigma^*)$. 询问期间,不能做 ID_i^* 的部分私钥询问. 如果密文通过解签密验证,则定义 A_1 在游戏中获胜.

UF-CMA-II:C 和伪造者 A_2 之间的交互游戏.

初始化. C 运行系统设置算法得到系统参数 $params$ 和系统主密钥 s,之后将系统参数 $params$ 发给 A_2,但保留主密钥 s.

训练. A_2 进行的多项式有界次询问和定义 6 中 IND-CCA2-II 游戏的阶段 1 一样.

伪造. 询问结束后,A_2 输出伪造多重签密密文$(ID_i^*, ID_V^*, \sigma^*)$. 询问期间,不能做 ID_i^* 的秘密钥询问. 如果 σ^* 通过解签密验证,则定义 A_2 在游戏中获胜.

3 一个具体的 EBMSC 协议

3.1 初始化(*Setup*)

密钥生成中心(KGC)随机选择大素数 p, g 是 $\mathbb{Z}_p^*$ 上阶为 p 的生成元. 定义 4 个安全 Hash 函数 $H_1: \{0,1\}^* \times \mathbb{Z}_p^* \to \mathbb{Z}_{p-1}^*$, $H_2: \{0,1\}^l \times \mathbb{Z}_p^* \to \mathbb{Z}_{p-1}^*$, $H_3: \mathbb{Z}_p^* \to \{0,1\}^l$, $H_4: \{0,1\}^* \times \mathbb{Z}_p^{*3} \to \mathbb{Z}_{p-1}^*$. KGC 随机选择系统主密钥 $s \in \mathbb{Z}_{p-1}^*$,计算系统公钥 $P_{Pub} = g^s \bmod p$. 最后 KGC 保密系统主密钥 s,公开系统参数$(p, g, l, P_{Pub}, H_1, H_2, H_3, H_4)$.

3.2 密钥生成(*Extract*)

1) 用户 U_i 随机选择 $k_i \in \mathbb{Z}_{p-1}^*$,并进一步计算公钥 $y_i = g^{k_i} \bmod p$,之后返回给 KGC.

2) KGC 选择 $\eta_i \in_R \mathbb{Z}_{p-1}^*$,计算 $\lambda_i = g^{\eta_i} \bmod p$, $T_i = (\eta_i + sH_1(ID_i, \lambda_i, y_i)) \bmod (p-1)$,将$(\lambda_i, T_i)$返回给用户 U_i.

3) 用户 U_i 验证 $g^{T_i}=\lambda_i(P_{\text{Pub}})^{H_1(ID_i,\lambda_i,y_i)} \bmod p$,如果等式成立,则 U_i 计算 $x_i=k_iT_i \bmod (p-1)$,并把 x_i 作为其私钥.通过以上步骤,签密者 U_i 将得到公私钥(x_i,y_i),接收者 U_V 将获得公私钥(x_V,y_V).

3.3 广播多重签密(*MultiSC*)

签密者 U_i 选择 $r_i\in_R\mathbb{Z}_{p-1}^*$,计算 $\alpha_i=g^{r_i} \bmod p$.然后广播给其他的签密者,通过下面步骤得到密文,并发送给签密收集者 U_C.

1) $\alpha=\prod_{i=1}^{n}\alpha_i \bmod p$.

2) $h=H_2(m,\alpha)$.

3) $W_i=y_V^{T_V}g^{x_i} \bmod p$.

4) $C_i=m\oplus H_3(W_i)$.

5) $\mu_i=H_4(m,T_i,T_V,W_i)$.

6) $\beta_i=(k_i(\mu_i+T_i+h\alpha)-r_i) \bmod (p-1)$.

7) 输出$(\alpha_i,\alpha,\beta_i,h,T_i,T_V,C_i)$,通过验证 $y_i^{\mu_i+T_i+h_\alpha}=\alpha_i g^{\beta_i} \bmod p$ 是否成立,若等式成立,则计算:

$$\beta=\sum_{i=1}^{n}\beta_i \bmod (p-1).$$

8) 签密收集者 U_C 将进一步输出签密密文 $\sigma=(\alpha,\beta_i,h,T_i,T_V,\{C_1,C_2,\cdots,C_n\})$ 给接收者 U_V.

3.4 解签密(*USC*)

接收者 U_V 收到签密密文 σ 后,执行步骤.

1) $W_i=g^{x_V}y_i^{T_i} \bmod p$.

2) $m=C_i\oplus H_3(W_i)$.

3) $\mu_i=H_4(m,T_i,T_V,W_i)$.

4) 验证:$y^{h\alpha+\sum_{i=1}^{n}(\mu_i+T_i)}=\alpha g^{\beta} \bmod p$,其中,$y=\prod_{i=1}^{n}y_i \bmod p$,若等式成立,则接受明文 m;否则,输出$\perp$符号表示广播多重签密无效.

3.5 正确性分析

可通过验证等式确保所提协议的正确性:

$$W_i=y_V^{T_V}g^{x_i} \bmod p=g^{k_VT_V}g^{k_iT_i} \bmod p=g^{x_V}y_i^{T_i} \bmod p.$$

$$\alpha g^{\beta}=\frac{\alpha g^{\sum_{i=1}^{n}k_i(\mu_i+T_i+h\alpha)}}{g^{\sum_{i=1}^{n}r_i}} \bmod p=\frac{\alpha g^{\sum_{i=1}^{n}k_i(\mu_i+T_i)}y^{h\alpha}}{g^{\sum_{i=1}^{n}r_i}}$$

$$\bmod p=y^{h\alpha+\sum_{i=1}^{n}(\mu_i+T_i)} \bmod p.$$

3.6 ROM 下的安全性分析

3.6.1 保密性

在随机预言模型(ROM)下的安全性分析,我们参考文献[18]的思路.

定理 1. 在 ROM 中,如果没有任何多项式有界的敌手 A_1 能以不可忽略的优势 ε 赢得定义 6 中的游戏 IND-CCA2-I(至多进行 q_i 次 H_i 询问($i=1,2,3,4$),q_{PK} 次公钥替换询问,q_{PSK} 次部分私钥提取询问,q_{SK} 次私钥提取询问,q_{SC} 次签密询问,q_{USC} 次解签密询问),则存在一个挑战者 C 能至少以 ε' 的优势解决 CDH 问题,这里:

$$\varepsilon'\geqslant\frac{\varepsilon}{e(q_{SK}+q_{PSK})q_3}.$$

证明. 给定一个随机的 CDH 问题实例(p,g,g^a,g^b),其中 $a,b\in\mathbb{Z}_p^*$,目标为了计算 $g^{ab} \bmod p$.为了达到这个目标,A_1 作为 C 的子程序在交互游戏中充当敌手.游戏开始之时,C 运行 $Setup(1^k)$,得到参数:

$$params=\{p,g,l,P_{\text{Pub}}=g^a,H_1,H_2,H_3,H_4\},$$

同时将 $params$ 发给 A_1.在交互游戏中,表 L_1 到 L_4 用于记录 H_1 至 H_4 的询问与应答值,L_k 用于记录公私钥的询问与应答值.

阶段 1.A_1 进行多项式有界次适应性询问.

H_1 询问:C 从个身份 q_1 中选择第 i 个身份作为挑战的目标身份,A_1 发出 H_1 询问.如果 A_1 向 C 询问的 Hash 函数值已经在 L_1 中存在,则返回相应的值给 A_1;否则,C 选取 $\psi\in_R\{0,1\}$.如果 $\psi=1$,则将$(ID_i,y_i,-,\psi)$记录到 L_1 中;否则选择 $h_1\in_R\mathbb{Z}_{p-1}^*$,返回 $g^{h_1}=g^b$,将$(ID_i,y_i,\lambda_i,h_1,\psi)$记录到 L_1 表中.这里设 $\psi=0$ 的概率是 ρ,即 $\rho=Pr[\psi=0]$.

H_2 询问:A_1 发出 H_2 询问时.C 检查元组(m,α,h_2)是否存在于 L_2,如果存在,则返回 h_2;否则,C 随机选取 $h_2\in\mathbb{Z}_{p-1}^*$,然后将 h_2 发给 A_1,并将(m,α,h_2)记录到 L_2 中.

H_3 询问:A_1 发出 H_3 询问.C 检查元组(W_i,h_3)是否存在于 L_3 表中,如果存在,则返回 h_3;否则,C 随机选取 $h_3\in_R\{0,1\}^l$,然后将 h_3 发给 A_1,记录(W_i,h_3)到 L_3 中.

H_4 询问:A_1 发出 H_4 询问时,检查元组(m,T_i,T_V,W_i,μ)是否存在于 L_4 中,如果存在,则返回 μ;否则,C 选取 $h_4\in_R\mathbb{Z}_{p-1}^*$,然后将 h_4 发给 A_1,记录(m,T_i,T_V,W_i,μ)到 L_4 中.

公钥询问:收到 A_1 公钥询问时,C 随机选择 k_i,并计算公钥 $y_i=g^{k_i} \bmod p$,之后将其添加到 L_k 表中.

部分私钥询问:A_1 询问身份 ID_i 的部分私钥.若 $\psi=0$,则 C 选择 $T_i\in\mathbb{Z}_{p-1}^*$,$\lambda_i=g^{T_i(P_{\text{Pub}})-h_1} \bmod p$,将$(ID_i,T_i,\psi)$记录到 L_1 中,并返回 T_i;否则,放弃仿真.

私钥询问:A_1 询问身份 ID_i 的私钥.假设已经询问过 H_1 预言机.若 $\psi=0$,则返回完整私钥 $x_i=k_iT_i \bmod p$;否则,放弃仿真,之后将私钥添加到 L_k 中.

公钥替换询问:A_1 对身份 ID_i 进行公钥替换询问时.C 用(ID_i,y_i')来替换 L_k 中的原有记录.

多重签密询问:A_1 可对任何消息 m 及签密人的身份 ID_i、接收者的身份 ID_V 进行签密询问.假设在此之前已经做过 Hash 函数值询问和密钥提取询问.如果 $\psi=0$,则正常执行多重签密算法;否则执行操作:

1) 挑战者 C 选择 $r_i\in_R\mathbb{Z}_{p-1}^*$,计算:

$$\alpha_i=g^{r_i} \bmod p,$$

$$\alpha=\prod_{i=1}^{n}\alpha_i \bmod p.$$

继续执行操作:

2) 计算 $h=H_2(m,\alpha)$,$W_i=y_V^{T_V}g^{x_i} \bmod p$.

3) 计算 $C_i=m\oplus H_3(W_i)$.

4) 计算 $\mu_i=H_4(m,T_V,T_i,W_i)$.

5) 计算 $\beta_i=(k_i(\mu_i+T_i+h\alpha)-r_i) \bmod (p-1)$.验证:

$$y_i^{\mu_i+T_i+h\alpha}=\alpha_i g^{\beta_i} \bmod p$$

是否成立.如果成立,则计算:

$$\beta=\prod_{i=1}^{n}\beta_i \bmod p.$$

6) 计算 $y=\prod_{i=1}^{n}y_i \bmod p$.

7) 输出 $\sigma=(\alpha,\beta,h,T_i,T_V,\{C_1,C_2,\cdots,C_n\})$.

解签密询问:A_1 通过提供的多重签密密文,当 A_1 询问 σ 是否合法时,挑战者 C 先从表中查找出记录 y_i,再查找表 L_1.如果 $\psi=0$,则正常执行解签密算法;否则,挑战者 C 计算 $W_i=g^{x_V}y_i^{T_i} \bmod p$,$m=C_i^*\oplus H_3(W_i)$,$\mu_i=H_4(m,T_V,T_i,W_i)$,然后将$(W_i,m)$提交给预言机.如果:

$$y^{h\alpha+\sum_{i=1}^{n}(\mu_i+T_i)}=\alpha g^{\beta} \bmod p,$$

则通过解签密;否则认为不合法.

挑战阶段.通过上面的询问过后,如果 $\psi=0$.则放弃仿真;否则挑战者 C 随机选择 $\delta=\{0,1\}$,计算 $W_i^*=g^{x_V}y_i^{T_i^*} \bmod p$,$C_i^*=m_\delta\oplus H_3(W_i^*)$,然后提交多重签密密文 $\sigma=(\alpha,\beta^*,h,T_i^*,T_V^*,\{C_1^*,C_2^*,\cdots,C_n^*\})$.

阶段 2.A_1 可以像阶段 1 那样进行多项式有界次适应性询问.但是要求身份 ID_V 的私钥仍然不能被询问,此外不能做 σ^* 的解签密询问.

猜测.最后,输出 $\delta'=\{0,1\}$,用 δ' 作为对 δ 的猜测.如果 $\delta'=\delta$,那么 C 计算 $W_i^*=y_V^{T_V^*}g^{x_i^*}$,$C$ 输出

$$g^{ab}=g^{\frac{g^{W_i^*}-k_i^*T_i^*-\eta_V^*k_V^*}{k_V^*}} \bmod p$$

作为 CDH 问题实例的解答,原因如下:

$$W_i^*=y_V^{T_V^*}g^{x_i^*} \bmod p$$

$$\Updownarrow$$

$$g^{W_i^*}=(\eta_V^*k_V^*+k_V^*sh_1+k_i^*T_i^*) \bmod p$$

$$\Updownarrow$$

$$g^{ab}=g^{sh_1}=g^{\frac{g^{W_i^*}-k_i^*T_i^*-\eta_V^*k_V^*}{k_V^*}} \bmod p.$$

概率分析[14]在阶段 1 或阶段 2 挑战者 C 不放弃仿真的概率是 $\rho^{q_{SK}+q_{PSK}}$,即在密钥提取阶段,至少有一个身份 ID_V 的私钥 x_V 没被 A_1 询问,C 不放弃游戏的概率为 $1/e(q_{SK}+q_{PSK})$,同时,A_1 对 W_i^* 做 H_3 询问的概率为 $1/q_3$,那么 C 将成功.所以 C 解决 CDH 问题的概率是

$$\varepsilon'\geqslant\frac{\varepsilon}{e(q_{SK}+q_{PSK})q_3}.$$ 证毕.

定理 2. 在 ROM 中,如果没有任何多项式有界的敌手 A_2 能以不可忽略的优势 ε 赢得定义 6 中的游戏 IND-CCA2-Ⅱ(至多进行 q_i 次 H_i 询问$(i=1,2,3,4)$,q_{PK} 次公钥替换询问,q_{SK} 次私钥提取询问,q_{SC} 次签密询问,q_{USC} 次解签密询问),则存在一个挑战者 C 能够至少以 ε' 的优势解决 CDH 问题,这里:

$$\varepsilon'\geqslant\frac{1}{e(q_{PK}+q_{SK})}\varepsilon.$$

证明. 给定一个随机的 CDH 问题实例(p,g,g^a,g^b),其中 $a,b\in\mathbb{Z}_p^*$,目标为了计算 $g^{ab} \bmod p$.为了达到这个目的,A_2 作为 C 的子程序,在交互游戏 IND-CCA2-II 中充当敌手.游戏开始后,C 运行 $Setup(1^k)$,得到参数:

$$params=\{p,g,l,P_{Pub}=g^s,H_1,H_2,H_3,H_4\},$$

同时将 $params$ 发给 A_2.在游戏中,表 L_1 到 L_4 用于记录 H_1 至 H_4 的询问与应答值,L_k 用于记录公私钥的询问与应答值.

阶段 1.除了部分私钥询问,其他询问同定理 1.

挑战阶段. 通过上面的询问过后,若 $\psi=0$.则放弃游戏;否则挑战者 C 随机选择 $\delta\in\{0,1\}$,计算,$y_i=g^a$,$W_i^*=g^{x_V}g^{aT_i^*} \bmod p$,$C^*=m_\delta\oplus H_3(W_i^*)$,返回密文 $\sigma=(\alpha,\beta^*,h,T_i^*,T_V^*,\{C_1^*,C_2^*,\cdots,C_n^*\})$.

阶段 2. A_2 可以像阶段 1 那样进行多项式有界次适应性询问.但是要求身份为 ID_V 的私钥仍然不能被询问,并且不能做关于 σ^* 的解签密询问.

猜测. 最后,输出 $\delta'\in\{0,1\}$,用 δ' 作为对 δ 的

猜测. 如果 $\delta'=\delta$,那么挑战者 C 计算 $\beta_i^*=(k_i^*(\mu_i+T_i^*+h\alpha)-r_i^*) \bmod (p-1)$,即 C 输出

$$g^{ab}=\left(\frac{\alpha g^{\beta}}{y_{i=1}^{\sum_{i=1}^{n}(\mu_i+T_i^*)}}\right)^{-n\alpha} \bmod p$$

作为 CDH 问题实例的应答,因为:

$$\beta=\sum_{i=1}^{n}\beta_i \bmod p-1 \Leftrightarrow$$

$$g^{\beta}=g_{i=1}^{\sum_{i=1}^{n}(k_i^*(h_4+T_i^*+h\alpha)-r_i^*)} \bmod p \Leftrightarrow$$

$$g^{ab}=\left(\frac{\alpha g^{\beta}}{y_{i=1}^{\sum_{i=1}^{n}(h_4+T_i^*)}}\right)^{-n\alpha}.$$

概率分析在阶段 1 或阶段 2 挑战者 C 不放弃仿真的概率是 $\rho^{(q_{SK}+q_{PK})}$,因为不进行部分私钥询问,即 C 不放弃游戏的概率为 $1/\mathrm{e}(q_{PK}+q_{SK})$,同时,$A_1$ 对 W_i^* 做 H_3 询问的概率为 $1/q_3$,那么 C 将成功. 所以 C 解决 CDH 问题的概率是

$$\varepsilon'\geqslant\frac{\varepsilon}{\mathrm{e}(q_{SK}+q_{PSK})q_3}.$$ 证毕.

3.6.2 不可伪造性

定理 3. 如果任何多项式有界的敌手 A_1 和 A_2 赢得定义 7 中的游戏 UF-CMA-I 和 UF-CMA-II 的优势是可忽略的,则 EBMSC 协议具有适应性选择消息攻击下的不可伪造性(至多进行 q_i 次 H_i 询问 $(i=1,2,3,4)$,q_{PK} 次公钥替换询问,q_{PSK} 次部分私钥提取询问,q_{SK} 次私钥提取询问,q_{SC} 次签密询问,q_{USC} 次解签密询问),在 UF-CMA-I 中,则存在一个挑战者 C 至少能够以

$$\varepsilon'\geqslant\frac{1}{\mathrm{e}(q_{SK}+q_{PSK})q_{USC}}\varepsilon$$

的优势解决离散对数问题;在 UF-CMA-II 中,则存在一个挑战者 C 至少能够以

$$\varepsilon'\geqslant\frac{1}{\mathrm{e}q_{SK}q_{USC}}\varepsilon$$

的优势解决离散对数问题.

证明. 给定一个随机的离散对数问题实例(p,g,g^a),目标为了计算 $a\in\mathbb{Z}_p^*$,为了达到这个目的,A_1 作为挑战者 C 的子程序,在交互游戏 UF-CMA-I 中充当敌手,C 充当敌手 A_1 的挑战者.

在交互游戏开始之时,游戏开始后,C 运行 $Setup(1^k)$,得到参数:

$$params=\{p,g,l,P_{Pub},H_1,H_2,H_3,H_4\},$$

并将 $params$ 发给 A_1. 在游戏中,表 L_1 到 L_4 记录 H_1 至 H_4 的预言机,L_k 用于追踪公私钥的询问与应答值.

询问阶段. 和定理 1 相同.

伪造. 对于不同的敌手伪造的过程不一样.

1) A_1 输出一个伪造的广播多重签密密文 σ^*. 如果 A_1 没做过身份 ID_i^* 的私钥或部分私钥询问,σ^* 通过解签密验证,则 A_1 赢得定义 7 中 UF-CMA-I.

设 A_1 输出有效的伪造广播多重签密密文 $\sigma=(\alpha,\beta^*,h,T_i^*,T_V^*,\{C_1^*,C_2^*,\cdots,C_n^*\})$,$C$ 计算:

① $W_i^*=y_V^{T_V^*}g^{x_i^*}$.

② $P_{Pub}=g^a$.

调用预言机 H_1 可以得到 h_1,输出:

$$a=\frac{g^{W_i^*}-k_i^*T_i^*-\eta_V^*k_V^*}{k_V^*h_1}$$

作为离散对数问题实例的解答,原因如下:

$$W_i^*=y_V^{T_V^*}g^{x_i^*} \bmod p \Leftrightarrow$$

$$g^{W_i^*}=\eta_V^*k_V^*+k_V^*sh_1+k_i^*T_i^* \bmod p \Leftrightarrow$$

$$a=\frac{g^{W_i^*}-k_i^*T_i^*-\eta_V^*k_V^*}{k_V^*h_1} \bmod p.$$

分析 C 成功解决离散对数问题的概率,A_1 没做过 ID_i 的私钥或部分私钥询问的概率为

$$\varepsilon'\geqslant\frac{1}{\mathrm{e}(q_{SK}+q_{PSK})},$$

通过解签密验证的概率为 $1/q_{USC}$,所以 C 解决离散对数问题的概率为 ε',这里:

$$\varepsilon'\geqslant\frac{1}{\mathrm{e}(q_{SK}+q_{PSK})q_{USC}}\varepsilon.$$

2) A_2 输出有效的伪造广播多重签密密文 σ^*. 如果 A_2 没有做过 ID_i^* 的私钥询问,同时 σ^* 通过解签密验证,则 A_2 赢得定义 7 中 UF-CMA-II.

设 A_2 输出有效的伪造广播多重签密密文$(\alpha,\beta^*,h,T_i^*,T_V^*,\{C_1^*,C_2^*,\cdots,C_n^*\})$,这里:

① $\beta_i^*=(k_i^*(\mu_i+T_i^*+h\alpha)-r_i^*) \bmod (p-1)$.

② $W_i^*=y_V^{T_V^*}g^{x_i^*} \bmod p$.

③ $y_i=g^a \bmod p$.

分别调用预言机 H_2 和 H_4 得到 h 和 h_4. C 输出:

$$a=\frac{\beta}{nh\alpha}g^{\frac{\alpha}{\sum_{y_i=1}^{n}(h_4+T_i^*)}}$$

作为离散对数问题实例的应答,因为:

$$\beta=\sum_{i=1}^{n}\beta_i \bmod (p-1)\Leftrightarrow$$

$$g^{\beta}=g_{i=1}^{\sum_{i=1}^{n}(k_i^*(h_4+T_i^*+h\alpha)-r_i^*)} \bmod p\Leftrightarrow$$

$$a=\frac{\beta}{nh\alpha}g^{\frac{\alpha}{\sum_{y_i=1}^{n}(h_4+T_i^*)}}.$$

分析 C 成功解决离散对数问题的概率,A_2 没有

作过私钥询问的概率为 $1/\mathrm{e}q_{\mathrm{SK}}$，$\sigma^*$ 通过解签密验证的概率为 $1/q_{\mathrm{USC}}$，所以 C 解决离散对数问题的概率为 ε'，这里：

$$\varepsilon' \geqslant \frac{1}{\mathrm{e}q_{\mathrm{SK}}q_{\mathrm{USC}}}\varepsilon.$$ 证毕.

4 EBMSC 协议的 UC 安全性分析

4.1 理想函数 F_{EBMSC}

理想模型中，EBMSC 协议的理想函数 F_{EBMSC}、参与方 $P_1, P_2, \cdots, P_n$ 及敌手 S 一起运行，执行过程如下：

① 在收到$(KGC, Setup, sid)$请求后验证，若验证 $sid=(KGC, sid')$成功，则将此消息发送给敌手 S.

② 在收到敌手 S 回复的$(Setup, Verify, sid, params)$后，记录下 $Verify$.

③ 在收到 P_i 的(Key, sid, P_i)请求后，验证 $sid=(P_i, sid')$，若验证成功，则将此消息发送给敌手 S，然后收到敌手 S 回复的(P_i, sid, y_i).

④ 在收到 P_{V} 的$(Key, sid, P_{\mathrm{V}})$请求后，验证 $sid=(P_{\mathrm{V}}, sid')$，若验证成功，则将此消息发送给敌手 S. 在收到敌手 S 回复的 y_{V} 后，将 y_{V} 发送给 P_i. 一旦收到来自 P_i 的消息$(Key, sid, P_{\mathrm{V}})$，则将此消息发送给敌手 S，从敌手 S 处收到 y_i 时，将 y_i 发送给 P_{V}. 之后，忽略所有的$(Key, sid, P_i/P_{\mathrm{V}})$.

⑤ 在收到 P_i 多重签密者的$(MultiSC, sid, m, y'_{\mathrm{V}})$请求后，验证 $sid=(P_i, sid')$，若验证不成功，则将忽略发送过来的消息；否则，执行如下：

如果 $y_{\mathrm{V}}=y'_{\mathrm{V}}$，同时参与方 P_{V} 是诚实的，则发送$(MultiSC, sid, |m|)$给敌手 S，这里 $|m|$ 是消息长度；否则，发送$(MultiSC, sid, m)$给敌手.

当从敌手 S 处收到 σ 时，将$(MultiSC, sid, m, \sigma)$给 P_{V}，并存储(m, σ).

⑥ 在收到接受者 P_{V} 的(USC, sid, σ, y_i)请求后，验证 $sid=(P_{\mathrm{V}}, sid')$，若验证不成功，则将忽略发送过来的消息；否则，执行如下：

如果(m, σ)已经记录过，则验证 $Verify((params, sid, m, \sigma), f=1)$，并把$(m, f)$发给 S.

否则，将(USC, sid, σ, y_i)发给敌手 S，并从敌手 S 处得到 m，并以$(m, f=0)$的形式发送给 P_{V}.

4.2 协议 π_{EBMSC}

下面是设计的 ElGamal 型广播多重签密协议 $\pi_{\mathrm{EBMSC}}=(Setup, Extract, MultiSC, USC)$，在 UC 框架下该协议运行如下：

① 一旦收到$(KGC, Setup, sid)$消息请求，则验证 $sid=(KGC, sid')$，运行 $Setup(1^k)$ 得到$(s, params)$，返回参数 $params$.

② 收到(U, Key, sid)，运行 $Extract(params, s, ID)$，得到(x_{ID}, y_{ID})，然后将(x_{ID}, y_{ID})返回.

③ 收到$(MultiSC, m, y_{\mathrm{V}}, sid)$消息请求后，运行 $MultiSC(params, m, x_i, y_{\mathrm{V}})\rightarrow\sigma$，并将 σ 返回.

④ 收到(USC, sid, σ)，运行 $USC(params, m, y_i, x_{\mathrm{V}})$，得到消息 m，若收到$(Verify, sid, m, \sigma)$请求，则运行 $Verify(params, sid, m, \sigma)\rightarrow f$，并返回 f 的值.

4.3 UC 框架下协议的安全性证明

定理 4. 协议 π_{EBMSC} 实现了广播多重签密理想函数 F_{EBMSC}.

证明. 假设 A 为现实模型中的敌手. 现在构造一个理想敌手 S，使得对于任何环境机 Z 都不能区分是与 F_{EBMSC} 和 S 在理想模型下的交互，还是与 π_{EBMSC} 和 A 在现实过程中的交互. 理想敌手 S、环境机 Z、敌手 A 以及参与方 $P_1, P_2, \cdots, P_n$ 一起运行.

构造敌手 S：在理想过程中，敌手 S 可以调用 A 的副本来与 F_{EBMSC} 和 S 交互，模拟 A 在现实过程与协议 π_{EBMSC} 的交互. 首先，敌手 S 把输出带上的内容写到 A 的输入带上，并把 A 输出带的内容拷贝到 Z 的输出带上.

模拟签密者 P_i 和接收者 P_{V} 都不被入侵. 当 S 收到 F_{EBMSC} 的消息$(Setup, sid)$，运行 $Setup$ 算法生成公钥 y_{V}，并把消息$(Verify, v)$输出给 F_{EBMSC}. 当 S 收到来自 F_{EBMSC} 的一个消息$(MultiSC, sid, m)$，运行多重签密算法 $MultiSC$，得到签密 σ 并把$(MultiSC, sid, m)$输出给 F_{EBMSC}. 当 S 收到来自 F_{EBMSC} 的一个消息$(Verify, sid, m, \sigma, v')$后，运行验证签名算法 $Verify$，得到验证结果 f，把$(Verify, sid, m, f)$输出给 F_{EBMSC}. 现实环境下签密者对消息进行签密，并将签密结果发送给接收者. 接收者验证签密的有效性. 理想环境中仿真器 S 对真实过程进行仿真，仿真签密过程和验证过程，同样发送签密和验证结果，因而，环境机 Z 不能区分出是 F_{EBMSC} 与 S 在理想模型中的交互，还是 π_{EBMSC} 与 A 在现实过程中的交互.

模拟签密者 P_i 被入侵. 敌手 S 模拟 A 伪装成参与方 P_i 把$(Setup, sid)$发送给 F_{EBMSC}. 同样，当 S 收到来自 F_{EBMSC} 的消息$(Extract, sid)$后. 运行密钥生成算法 $Setup$，得到签密者公钥 y_i 并将其返回给 F_{EBMSC}. 当 S 收到来自 F_{EBMSC} 的消息$(MultiSC, sid)$，

运行多重签密算法,得到密文并将其返回给 F_{EBMSC}. S 模拟 A 入侵参与方 P_i,并将$(MultiSC,sid,m')$发送给 F_{EBMSC}. 同样,当 S 接收到$(MultiSC,sid,m')$时,可以得到多重签密 σ',即把$(MultiSC,sid,m',\sigma')$发送给 F_{EBMSC}. 由此看来,环境 Z 并不能区分现实过程和理想模型.

模拟接收者 P_V 被入侵. 若参与方 P_V 被收买,敌手 S 可以模拟参与方的身份把$(Verify,sid,m',\sigma',v')$发送给 F_{EBMSC},随后,当 S 接收到$(Verify,sid,m',\sigma',v')$时,计算验证结果 f,把$(Verify,sid,m',\sigma',v',f)$ 发送给 F_{EBMSC}. 此时,环境机 Z 不能区分(m,σ)与(m',σ').

模拟签密者 P_i 和接收者 P_V 都被入侵. 当多重签密者 P_i 和解签密者 P_V 都被攻陷时,S 将获得双方的所有输入信息,即 Z 可产生真实的数据来仿真协议的运行.

综合上述 4 种情形,环境机 Z 不能区分出是 F_{EBMSC} 与 S 在理想模型中的交互,还是 π_{EBMSC} 与 A 在现实过程中的交互. 即协议 π_{EBMSC} 能够实现广播多重签密理想函数 F_{EBMSC}. 证毕.

定理 5. 在 UC 安全框架下,协议 π_{EBMSC} 满足选择消息攻击下的不可伪造性.

证明. 假设存在伪造者 F,则构造环境机 Z 和敌手 A,使得对于任何敌手 A,Z 都以不可忽略的概率区分它是与(π_{EBMSC},A)交互还是与(F_{EBMSC},S)交互.

构造环境机 Z. 当收到来自 A 的多重签密请求时,则 Z 激活 P_i,然后输出多重签密密文 σ,并返回给 A. 当收到来自 A 的解签密请求时,Z 激活 P_i,并输出(m,f)给 A.

构造敌手 A. 当 A 要求对消息 m 进行多重签密时,敌手 A 首先要求环境机 Z 对 m 进行多重签密,然后把多重签密密文 σ 给 F;当 F 需要对 σ' 解签密时,敌手 A 首先要求环境机 Z 对 σ' 进行解签密,然后把(m',f)返回给 A,再发给伪造者 F. 一旦 F 收到了 m',并且 $f=1$,则 F 伪造的多重签密是有效的,此时,Z 输出 $f=1$. 显然,如果 F 以可忽略的概率赢得了定理 3 中的 UF-CMA-I 和 UF-CMA-II 游戏,则 F 能够成功地伪造出有效的 F,假设伪造者 F 以可忽略的概率存在,则 Z 以可忽略的概率输出 $f=1$. 而在理想模型中,Z 输出 $f=1$ 的概率总是等于 0. 换句话说,如果存在这样的伪造者 F,Z 总以可忽略的概率区分它是与(π_{EBMSC},A)交互还是与(F_{EBMSC},S)交互,故与定理 5 的假设矛盾. 所以,不存在这样的伪造者 F,也就是说,在 UC 安全框架下,协议 π_{EBMSC} 满足选择消息攻击下的不可伪造性. 证毕.

5 性能分析

ElGamal 型广播多重签密协议的计算开销主要集中在模指数和 Hash 函数运算. 表 1 中 E 表示 1 次模指数运算,H 表示 1 次 Hash 函数运算,M 表示 1 次乘法运算. 本文方案与文献[30-33]中的方案效率比较如表 1 所示. 从表 1 中看出,本文分案明显好于文献[30,32-33],并且本文还实现了广播多重签密功能. 本文与文献[31]的效率相当,但文献[31]只实现了多重数字签名,而本文方案不仅实现了多重签密功能,还在 UC 框架证明了该协议是安全的.

Table 1 Efficiency of this Paper Compared with Others References

表 1 本文方案与其他文献的效率比较

Reference	Signature or Signcryption	Verify or Unsigncryption	Total
Ref[30]	2E+2M+H	9E+5M+2H	11E+7M+3H
Ref[31]	4E+6M+H	2E+2M+H	6E+8M+2H
Ref[32]	4E+2M+4H	5E+2M+3H	9E+4M+7H
Ref[33]	5E+4M+H	7E+3M+2H	12E+7M+3H
Our Scheme	4E+4M+3H	3E+2M+2H	7E+6M+5H

Notes: E: 1 exponential operation; M: 1 multiplication operation; H: 1 hash operation.

6 总 结

目前设计的 ElGamal 型广播多重签密协议的安全性一般是基于 DL 问题的难解性,虽然满足了不可伪造性,但是不具备签名者的身份验证,使得该类协议容易遭受多个签名者的联合攻击. 本文设计了一个新的 ElGamal 型广播多重签密协议,由于本文是采用自认证方式来认证用户的公钥,克服了密钥管理问题以及能够抵抗文献[5-7]的攻击. 在随机预言模型中证明了该协议在离散对数和 CDH 假设下是语义安全的. 为了使所提协议适应更加复杂的网络环境,本文引入 UC 安全技术,而在 UC 安全框架下分析了该协议的安全性. 我们定义了 ElGamal 型广播多重签密协议的理想函数 F_{EBMSC},进而证明了 UC 安全的 ElGamal 型广播多重签密协议的通

用可组合安全性.下一步将对集合相交协议进行研究.

参 考 文 献

[1] Itakura K, Nakamura K. A public-key cryptosystem suitable for digital multi-signatures [J]. NEC Research & Development, 1983,71(1): 474-480

[2] Zhang Jianhong, Wei Yongzhuang, Wang Yumin. Digital multisignatrues scheme based on RSA [J]. Journal on Communications, 2003, 24(8): 150-154 (in Chinese)
(张键红, 韦永壮, 王育民. 基于RSA的多重数字签名[J]. 通信学报, 2003, 24(8): 150-154)

[3] Li Zichen, Yang Yixian. ELGamal's multisignature digital signature scheme [J]. Journal of Beijing University of Posts and Telecommunications, 1999, 22(2): 30-34 (in Chinese)
(李子臣, 杨义先. ElGamal多重数字签名方案[J]. 北京邮电大学学报, 1999, 22(2): 30-34)

[4] Burmester M, Desmedt Y, Doi H, et al. A structured ELGamal-Type multisignature scheme [G] //LNCS 1751: Proc of the 3rd Int Workshop on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2000: 466-483

[5] Zhang Qiupu, Ye Dingfeng. Cryptanalysis and improvemen of an identity-based multi-signcryption scheme [J]. Acta Electronica Sinica, 2011, 39(12): 2713-2720 (in Chinese)
(张秋璞, 叶顶峰. 对一个基于身份的多重签密方案的分析和改进[J]. 电子学报, 2011, 39(12): 2713-2720)

[6] Lu Langru, Zeng Junjie, Kuang Youhua, et al. A new multisignature scheme based on discrete logarithm problem and its distributed computation [J]. Chinese Journal of Computers, 2002, 25(12): 1419-1420 (in Chinese)
(陆浪如, 曾俊杰, 匡友华, 等. 一种新的基于离散对数多重签名方案及其分布式计算[J]. 计算机学报, 2002, 25(12): 1419-1420)

[7] Han Xiaoxi, Wang Guilin, Bao Feng, et al. An attack to multisignature schemes based on discrete logarithm [J]. Chinese Journal of Computers, 2004, 27(8): 1147-1152 (in Chinese)
(韩小西, 王贵林, 鲍丰, 等. 针对基于离散对数多重签名方案的一种攻击[J]. 计算机学报, 2004, 27(8): 1147-1152)

[8] Harn L. New digital signature scheme based on discrete logarithm [J]. Electronics Letters, 1994, 30(5): 396-398

[9] Wu Tzongchen, Chou Shulin, Wu Tzongsun. Two ID-based multi-signature protocols for sequential and broadcasting architectures [J]. Computer Communications, 1996, 19 (9/10): 851-856

[10] Zheng Yuliang. Digital signcryption or how to achieve cost (signature and encryption) cost (signature) + cost (encryption) [C] //LNCS 1294: Proc of the 17th Annual Int Cryptology Conf. Berlin: Springer, 1997: 165-179

[11] Baek J, Steinfeld R, Zheng Yuliang. Formal proofs for the security of Signcryption [C] //LNCS 2274: Proc of the 5th Int Workshop on Practice and Theory in Public Key Cryptosystems. Berlin: Springer, 2002: 80-98

[12] Fan Jia, Zheng Yuliang, Tang Xiaohu. A single key pair is adequate for the Zheng signcryption [C] //LNCS 6812: Proc of the 16th Australasian Conf on Information Security and Privacy. Berlin: Springer, 2011: 371-388

[13] Zhou Kai, Peng Changgen, He Jianqiong, et al. Provable secure trajectory privacy protection scheme for continuous queries in location-based services [J]. Netinfo Security, 2017, 17(1): 43-47 (in Chinese)
(周凯, 彭长根, 何建琼, 等. 可证明安全的LBS中连续查询的轨迹隐私保护方案[J]. 信息网络安全, 2017, 17(1): 43-47)

[14] Yu Huifang, Yang Bo. Identity-based hybird signcryption scheme using ECC [J]. Journal of Software, 2015, 26(12): 3174-3182 (in Chinese)
(俞惠芳, 杨波. 使用ECC的身份混合签密方案[J]. 软件学报, 2015, 26(12): 3174-3182)

[15] Zhou Yanwei, Yang Bo, Wang Qinglong. Provable secure leakage-resilient certificateless hybird signcryption scheme [J]. Journal of Software, 2016, 27(11): 2898-2911 (in Chinese)
(周彦伟, 杨波, 王青龙. 可证明安全的抗泄露无证书混合签密机制[J]. 软件学报, 2016, 27(11): 2898-2911)

[16] Shi Min, Ye Weiwei, Ou Qingyu. Identity-based authenticated protocol without bilinear pairing [J]. Netinfo Security, 2016, 16(10): 21-27 (in Chinese)
(矢敏,叶伟伟,欧庆于. 不需双线性对的基于身份的认证密钥协商协议[J]. 信息网络安全, 2016(10): 21-27)

[17] Li Jianmin, Yu Huifang, Zhao Chen. Self-certified blind signcryption protocol with UC security [J]. Journal of Frontiers of Computer Science and Technology, 2017, 11 (6): 932-940 (in Chinese)
(李建民, 俞惠芳, 赵晨. UC安全的自认证盲签密协议[J]. 计算机科学与探索, 2017, 11(6): 932-940)

[18] Yu Huifang, Yang Bo. Provably secure certificateless hybrid signcryption [J]. Chinese Journal of Computers, 2015, 37 (4): 804-813 (in Chinese)
(俞惠芳, 杨波. 可证安全的无证书混合签密[J]. 计算机学报, 2015, 37(4): 804-813)

[19] Yu Huifang, Yang Bo. Low-computation certificateless hybrid signcryption scheme [J]. Frontiers of Information Technology Electric Engineering, 2017, 18(7): 928-940

[20] Zhou Caixue. Cryptanalysis and improvement of some signcryption scheme [J]. Computer Engineering and Science, 2016, 38(11): 2246-2253 (in Chinese)
(周才学. 几个签密方案的密码学分析与改进[J]. 计算机工程与科学, 2016, 38(11): 2246-2253)

[21] Canetti R. Universally composable security: A new paradigm for cryptographic protocols [C] //Proc of the 42nd IEEE Symp on Foundation of Computer Science. Los Alamitos, CA: IEEE Computer Society, 2001: 136-145

[22] Canetti R, Lindaell Y, Ostrovky R, et al. Universally compusable two-party and multi-party secure computation [C] //Proc of the 34th Annual ACM Symp on Theory of Computing. New York: ACM, 2003: 219-233

[23] Kristian G, Lillian K. Universally composable signcryption [C] //LNCS 4582: EuroPKI 2007. Berlin: Springer, 2007: 346-353

[24] Canetti R, Dachman D, Vaikuntanathan V, et al. Efficient password authenticated key exchange via oblivious transfer [C] //LNCS 7293: Proc of the 15th Int Conf on Practice and Theory in Public Key Cryptograhy. Berlin: Springer, 2012: 449-466

[25] Feng Tao, Li Fenghua, Ma Jianfeng, et al. A new method for concurrent deniable authentication of UC Security [J]. Science in China Series F: Informations Sciences, 2008, 38 (8): 1220-1233 (in Chinese)
(冯涛, 李风华, 马建峰, 等. UC 安全的并行可否认认证新方法[J]. 中国科学 F 辑: 信息科学, 2008, 38(8): 1220-1233)

[26] Su Ting, Xu Qiuliang. UC secure signcryption protocol with public verifiability [J]. Journal of Southeast University: Natural Science Edition, 2008, 38 (Suppl): 55-58 (in Chinese)
(苏婷, 徐秋亮. 可证明安全的 UC 安全签密协议[J]. 东南大学学报: 自然科学, 2008, 38(增刊): 55-58)

[27] Zhang Zhong, Xu Qiuliang. Universal composable grouping-proof protocol for RFID tags in the Internet of things [J]. Chinese Journal of Computers, 2011, 34(7): 1188-1194 (in Chinese)
(张忠, 徐秋亮. 物联网环境下 UC 安全的组证明 RFID 协议[J]. 计算机学报, 2011, 34(7): 1188-1194)

[28] Tian Youliang, Ma Jianfeng, Peng Changgen, et al. Universally composable mechanism for group communication [J]. Chinese Journal of Computers, 2012, 35(4): 645-653 (in Chinese)
(田有亮, 马建峰, 彭长根, 等. 群组通信的通用可组合机制[J]. 计算机学报, 2012, 35(4): 645-653)

[29] Tian Youliang, Peng Changgen, Ma Jianfeng, et al. Universally composable secure multiparty computation protocol with fairness [J]. Journal on Communications, 2014, 35(7): 54-62 (in Chinese)
(田友亮, 彭长根, 马建峰, 等. 通用可组合公平安全多方计算协议[J]. 通信学报, 2014, 35(7): 54-62)

[30] Zhang Xinghua. A new multi-proxy multi-signature scheme based on discrete logarithm problem [J]. Computer Applications and Software, 2014, 31(2): 317-320 (in Chinese)
(张兴华. 一个新的基于离散对数问题的多重代理多重签名方案[J]. 计算机应用与软件, 2014, 31(2): 317-320)

[31] Cao Yang. ElGamal multiple digital signature scheme based on identity [J]. Bulletin of Science and Technology, 2015, 31(5): 197-199 (in Chinese)
(曹阳. 基于身份的 ElGamal 多重数字签名方案[J]. 科技通报, 2015, 31(5): 197-199)

[32] Wang Caifen, Jianghong, Yang Xiaodong, et al. Multi-message and multi-receiver hybrid signcryption scheme based on discrete logarithm [J]. Computer Engineering, 2016, 42 (1): 150-155 (in Chinese)
(王彩芬, 姜红, 杨小东, 等. 基于离散对数的多消息接收者混合签密方案[J]. 计算机工程, 2016, 42(1): 150-155)

[33] Hu Jianghong. A certificateless broadcasting multi-proxy signature scheme based on RSA [J]. Computer and Modernization, 2016(6): 113-116 (in Chinese)
(胡江红. 基于 RSA 的无证书广播多重代理签名方案[J]. 计算机与现代化, 2016(6): 113-116)

Li Jianmin, born in 1991. Received his master degree from Qinghai Normal University. Student member of CCF. His main research interests include information security and cryptography.

Yu Huifang, born in 1972. PhD. Professor and master supervisor of Xi'an University of Posts & Telecommunications. Senior number of CCF. Her main research interests include information security and cryptography.

Xie Yong, born in 1978. Received his PhD degree in computer science from Wuhan University, Wuhan, China, in 2016. Associate professor at the Department of Computer Technology and Application, Qinghai University. His main research interests include next generation Internet, network protocol and protocol security.