·安全技术· 文章编号:1000-3428(2017)03-0172-04 文献标志码:A 中图分类号:TP309

通用可组合的群签名协议

赵 晨,俞惠芳,李建民

(青海师范大学 计算机学院,西宁 810008)

摘 要: 目前群签名协议大多只局限于单个协议执行的安全性,在多协议环境下安全性减弱。为此,研究通用可组合模型框架下的群签名在多个协议并发执行时的安全性。由于在通用可组合的模型框架下可以模块化地分析协议,因此利用此框架定义群签名协议的理想函数,提出可以实现此理想函数的群签名协议,并证明此协议的安全性和不可伪造性。基于离散对数问题给出通用可组合的群签名协议实例。分析结果表明,该协议的安全性适用于多协议执行的并发环境。

关键词: 群签名;理想函数;并发执行;安全性;不可伪造性

中文引用格式: 赵 晨,俞惠芳,李建民. 通用可组合的群签名协议[J]. 计算机工程,2017,43(3):172-175.

英文引用格式: Zhao Chen, Yu Huifang, Li Jianmin. Universally Composable Group Signature Protocol[J]. Computer Engineering, 2017, 43(3): 172-175.

Universally Composable Group Signature Protocol

ZHAO Chen, YU Huifang, LI Jianmin

(School of Computer, Qinghai Normal University, Xining 810008, China)

【Abstract】 At present, most group signature is only secure in the standard alone. Its security becomes weak in multiple protocol environment. In view of this, the security of group signature protocol is studied in the multiple concurrent execution under the universally composable framework. Since the protocol can be analyzed modularly under the universally composable framework, an ideal function of group signature protocol is defined in this framework. Then a group signature protocol is proposed to realize the ideal function, and its universally composable security as well as unforgeability is also proved. Furthermore, a concrete instance of this universally composable group signature protocol is given. Analysis results show that this protocol security is suitable for applications in multiple concurrent environment.

【Key words】 group signature; ideal function; concurrent execution; security; unforgeability

DOI: 10.3969/j.issn.1000-3428.2017.03.029

0 概述

1991 年,文献[1]提出了群签名的概念,群签名需要签名者使用私钥对消息进行签名,获得公钥的可信用户对签名消息公开验证。在群签名方案中,参与者包括多个群成员和一个群管理员,任何一个群成员可以代表群整体对消息进行签名的同时身份不被暴露,当签名消息发生争议的时候仅有群管理员可以追踪到签名者的身份。1992 年,文献[2]提出了一种基于 RSA 的门限群签名方案。1997 年,文献[3]提出了一种适用于大群体的群签名方案。文献[4]提出了一种基于离散对数问题的群签名方案。2000 年,文献[5]提出了一种高效的群签名方案。文献[6]提出了一种基于椭圆曲线的群签名方案。文献[7]提出了一种基于中国剩余定理的群签名方案。2005 年,文献[8]提出了一种基于 ACJT 成员撤销的群签名方案。文献[9]提出了一种一般化的向前安全群签名方案。

随着群签名在电子选举、电子投标以及不可追踪的电子现金系统等电子政务和电子商务中的广泛应用,群签名在多个协议中并发执行的安全性需要考虑。文献[10]提出了一种关于密码协议安全性的新范式,称之为通用可组合安全性框架。目前,在此框架下对数字签名的研究主要涉及普通的数字签名[11]、盲签名[12]、门限签名[13]、身份数字签名[14]以及环签名[15],尚未有公开的文献对群签名的通用可

基金项目: 国家自然科学基金(61363080);青海省应用基础研究基金(2016-ZJ-776)。

作者简介: 赵 晨(1992—),女,硕士研究生,主研方向为密码学、信息安全;俞惠芳,教授、博士;李建民,硕士研究生。

收稿日期: 2016-03-28 **修回日期:** 2016-05-16 **E-mail:** yuhuifang@qhnu.edu.cn

组合安全性进行研究。

本文在通用可组合的模型下定义一种新的理想函数,基于此函数和离散对数问题提出一个具体的协议实例,并在通用可组合的安全模型下研究该实例的安全性。

1　基础知识

1.1　通用可组合安全性框架

通用可组合安全性框架主要由现实模型、理想模型以及混合模型组成,通过交互式图灵机系统来实现。该安全框架主要用于描述和分析并发环境下密码协议的安全问题。

现实模型描述真实的协议运行,由现实协议 π、环境机 $\mathcal{Z}$ 以及现实世界的敌手 $\mathcal{A}$ 之间的交互构成。协议 π 是实现指定任务的一个程序,它由 n 方参与方 $P_1,P_2,\cdots,P_n$ 共同执行。理想模型描述协议运行的理想情况,同样由理想函数 $\mathcal{F}$、环境机 $\mathcal{Z}$ 以及虚拟攻击者 $\mathcal{S}$(也叫仿真器 $\mathcal{S}$)之间的交互构成。环境机 $\mathcal{Z}$ 作为一个交互式图灵机,模拟协议运行的整个外部环境,环境机 $\mathcal{Z}$ 可以与所有参与者以及敌手 $\mathcal{A}$ 和攻击者 $\mathcal{S}$ 直接通信,不允许与理想函数 $\mathcal{F}$ 直接通信。理想函数 $\mathcal{F}$ 被视为不可攻破可信的第三方,在交互过程中收到参与方消息后,通过程序计算后把结果返回给参与方。

混合模型以现实模型和理想模型作为基础,使得现实模型中协议可以访问理想模型的理想函数。在混合模型中,协议中的实体以及敌手可以和理想函数的副本进行交互,并通过 $\mathcal{F}_{\mathrm{id}}$加以区分理想函数的副本,而理想函数的副本之间能进行交互。

定义 1　2 个二元分布 X 和 Y 是不可区分的(记为 $X\approx Y$),如果对于任何 $c\in N$,都存在 $k_0\in N$,使得对于所有满足 $k>k_0$ 的 k 以及所有的 a,都有[8]:

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

定义 2　令 $n\in N$,$\mathcal{F}$ 是一个理想函数,π 是一个 n 方协议,C 是现实世界的敌手集合。如果对于任何 $\mathcal{A}\in C$ 都存在一个理想过程的敌手 $\mathcal{S}$ 使得对于任何环境机 $\mathcal{Z}$,都有[8]:

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

那么,称 π 安全实现了关于 C 的 $\mathcal{F}$。

定义 3　令 $\mathcal{F}$ 和 $\mathcal{G}$ 为理想函数,协议 π 运行在 $\mathcal{F}$-混合模型下,协议 ρ 可以安全实现 $\mathcal{F}$ 在 $\mathcal{G}$-混合模型下。那么对于任何敌手 $\mathcal{A}$,都存在一个敌手 $\mathcal{A}_{\mathcal{F}}$,使得对于任何的环境机 $\mathcal{Z}$,都有[8]:

$$EXEC^{\mathcal{F}}_{\pi},A_{\mathcal{F}},\mathcal{Z}\approx EXEC^{G}_{\pi^{\rho},A_{\mathcal{G}}},\mathcal{Z}$$

1.2　通用可组合的群签名协议

一个普通的通用可组合的群签名协议包括如下算法[5]:

1)初始化,输入一个安全参数 k,这个概率多项式算法输出群公钥 v 和群管理员私钥 S_{GM}。

2)加入,用户与群管理员进行交互,用户生成群成员私钥 S_i 和获得群管理员颁布的相应群成员证书 CE_i。

3)签名,输入群公钥 v、群成员证书 CE_i、群成员私钥 S_i 和消息 m,概率多项式算法输出签名 σ。

4)验证,概率多项式算法利用群公钥 v 和消息 m,验证签名 σ 是否为有效签名。

5)打开,在验证签名 σ 为消息 m 的有效签名基础上,利用群公钥 v 和群管理员私钥 S_{GM},概率多项式算法输出签名者的身份。

2　群签名协议的理想函数

$\mathcal{F}_{\mathrm{GSIG}}$和参与方 $P_1,P_2,\cdots,P_n$、群管理员 GM 以及敌手 $\mathcal{S}$ 一起运行,且与安全参数 k 相关,执行过程如下所示。

生成密钥:在第一次激活过程中,期望收到来自某参与方 P_i 的一个消息($KeyGen$, sid),首先验证 $sid=(P_i,sid')$。如果验证成功,那么把消息($KeyGen$,sid)交给敌手 $\mathcal{S}$。否则,忽略请求。

如果收到来自敌手 $\mathcal{S}$ 的消息($Verification\ Key$, sid,v),那么把消息($Verification\ Key$,sid,v)发送给 P_i 并记录下元组(P_i,v)。这个阶段必须一次完成,并且忽略来自其他参与方的消息($KeyGen$,sid)。

加入:一旦收到来自某参与方 P_i 的一个消息($Join$,sid),首先验证 $sid=(P_i,sid')$。如果验证成功,那么把消息($Join$,sid)交给敌手 $\mathcal{S}$。否则,忽略请求。

如果收到来自敌手 S 的消息($Joined$,sid,id,S_i,CE_i),检查(id,S_i,CE_i,0)是否已经被储存。如果已经被储存,那么向 P_i 输出错误消息并且停机。否则,把消息($Joined$,sid,id,S_i,CE_i)发送给 P_i 并把(id,S_i,CE_i,1)储存。

生成签名:一旦收到来自某参与方 P_i 的一个消息($Sign$,sid,m),首先验证 $sid=(P_i,sid')$。如果验证成功,那么把消息($Sign$,sid,m)发送给敌手 $\mathcal{S}$,否则,忽略请求。

如果收到来自敌手 $\mathcal{S}$ 的消息($Signature$,sid,m,

σ),检查($m,\sigma,v,0$)是否已经被储存。如果已经被储存,那么向 P_i 输出错误消息并且停机,否则,把消息($Signature,sid,m,\sigma$)发送给 P_i 并把消息($m,\sigma,v,1$)储存。

验证签名:一旦收到来自某参与方 P_j 的一个消息($Verify,sid,m,\sigma,v'$),首先验证 $sid=(P_j,sid')$。如果验证成功,那么把消息($Verify,sid,m,\sigma,v'$)发送给敌手 $\mathcal{S}$,否则,忽略请求。

如果收到来自敌手 $\mathcal{S}$ 的消息($Verified,sid,m,\varphi$),那么执行分以下情况:

1)如果 $v'=v$ 且($m,\sigma,v,1$)已经被储存,那么设置 $f=1$。

2)如果 P_j 未被收买且($m,\sigma',v,1$)没有被储存,那么设置 $f=0$。

3)如果(m,σ,v',f')已经被储存,那么设置 $f=f'$。

4)否则,设置 $f=\varphi$ 并把(m,σ,v',φ)储存。

最后,把消息($Verified,sid,m,\sigma,f$)输出给 P_j。

打开:一旦收到群管理员 GM 的消息($Open,sid,m,\sigma,f$),首先验证 $sid=(GM,sid')$ 和 $f=1$。如果验证成功,那么把消息($Open,sid,m,\sigma,f$)发送给敌手 $\mathcal{S}$;否则,忽略请求。

之后,如果收到来自敌手 $\mathcal{S}$ 的消息($Opened,sid,m,\sigma,f,id$),那么把 id 发送给群管理员 GM。

3 群签名协议的安全性分析

推理 1 群签名协议 π_Σ 可以安全实现理想函数 $\mathcal{F}_{\text{GSIG}}$。

证明:令 $\mathcal{A}$ 为现实敌手。构造理想敌手 $\mathcal{S}$,使得对于任何环境机 $\mathcal{Z}$ 不能区分出是 $\mathcal{F}_{\text{GSIG}}$ 与 $\mathcal{S}$ 在理想模型中的交互,还是 π_Σ 与 $\mathcal{A}$ 在现实过程中的交互。理想敌手 $\mathcal{S}$ 仿真环境机 $\mathcal{Z}$、敌手 $\mathcal{A}$ 以及参与方 $P_1,P_2,\cdots,P_n$ 群管理员 GM 之间的交互。

敌手 $\mathcal{S}$ 运行过程如下所示。

生成密钥:当收到来自 $\mathcal{F}_{\text{GSIG}}$ 的一个消息($KeyGen,sid$)后,$\mathcal{S}$ 运行初始化算法 $setup(1^k)$,生成群公钥 v 和群管理员私钥 S_{GM},把 v 输出给 $\mathcal{F}_{\text{GSIG}}$。若某参与方 P_i 被收买,敌手 $\mathcal{A}$ 以参与方 P_i 的身份把($KeyGen,sid$)发送给 $\mathcal{F}_{\text{GSIG}}$。

如果敌手 $\mathcal{A}$ 收到消息($KeyGen,sid$),可以获得验证密钥 v,把($Verification\ Key,sid,v$)发送给 $\mathcal{F}_{\text{GSIG}}$。

加入:当收到来自 $\mathcal{F}_{\text{GSIG}}$ 的一个消息($Join,sid$)后,运行算法 $Join$,把群成员证书 CE_i 输出给 $\mathcal{F}_{\text{GSIG}}$。如果参与方 P_i 和 GM 同时被收买时,敌手 $\mathcal{A}$ 分别伪装成 P_i 或者群管理员 GM 与 $\mathcal{F}_{\text{GSIG}}$ 进行交互。

生成签名:当收到来自 $\mathcal{F}_{\text{GSIG}}$ 的一个消息($Sign,sid,m$)后,运行签名算法 $Sign$,得到 $\sigma=sig(v,CE_i,m)$,把($Signature,sid,m,\sigma$)输出给 $\mathcal{F}_{\text{GSIG}}$。如果参与方 P_i 被收买,敌手 $\mathcal{A}$ 以参与方 P_i 的身份把($Sign,sid,m'$)发送给 $\mathcal{F}_{\text{GSIG}}$。

随后,当 $\mathcal{A}$ 接收到($Sign,sid,m'$)时,可以获得签名 σ',把($Signature,sid,m',\sigma'$)发送给 $\mathcal{F}_{\text{GSIG}}$。当签名者被收买时,参与方产生的密钥和对 m 的签名过程都由敌手 $\mathcal{A}$ 控制,因此,对于环境 $\mathcal{Z}$ 并不能区分现实过程和理想模型。

验证签名:当收到来自 $\mathcal{F}_{\text{GSIG}}$ 的一个消息($Verify,sid,m,\sigma,v'$)后,运行验证算法 ver,得到 $\varphi=ver(v,m,\sigma)$,把($Verified,sid,m,\varphi$)输出给 $\mathcal{F}_{\text{GSIG}}$。若参与方 P_j 被收买,敌手 $\mathcal{A}$ 以参与方 P_j 的身份把($Verify,sid,m',\sigma',v'$)发送给 $\mathcal{F}_{\text{GSIG}}$,随后,当 $\mathcal{A}$ 接收到($Verify,sid,m',\sigma',v'$)时,可以获得验证结果 φ,把($Verified,sid,m',\varphi$)发送给 $\mathcal{F}_{\text{GSIG}}$。当验证者收买时,环境机 $\mathcal{Z}$ 并不能区分(m,σ)与(m',σ'),因此,对于环境机 $\mathcal{Z}$ 并不能区分现实过程和理想模型。

签名者和验证者都被收买时,情况与上述 2 种情况相似。

在正常情况下,现实环境下签名者对消息进行签名,并将签名发送给验证者验证,验证者验证签名的有效性。理想环境中仿真器 $\mathcal{S}$ 对真实过程进行仿真,仿真签名过程和验证过程,同样发送签名和验证结果,因而,环境机 Z 不能区分出是 $\mathcal{F}_{\text{GSIG}}$ 与 $\mathcal{S}$ 在理想模型中的交互,还是 π_Σ 与 $\mathcal{A}$ 在现实过程中的交互,因此,协议 π_Σ 可以安全实现理想函数 $\mathcal{F}_{\text{GSIG}}$。

推理 2 群签名协议 π_Σ 具有不可伪造性,若 π_Σ 可以安全实现理想函数 $\mathcal{F}_{\text{GSIG}}$。

证明:采用反正法证明。假设协议 π_Σ 可以安全实现理想函数 $\mathcal{F}_{\text{GSIG}}$,协议 π_Σ 可伪造的概率是不可忽略的。假设存在一个伪造者 $\mathcal{G}$。构造一个环境机 $\mathcal{Z}$ 和现实敌手 $\mathcal{A}$,对于任何的理想敌手 $\mathcal{S}$,环境机 $\mathcal{Z}$ 不能区分出是 $\mathcal{F}_{\text{GSIG}}$ 与 $\mathcal{S}$ 在理想模型中的交互,还是 π_Σ 与 $\mathcal{A}$ 在现实过程中的交互。

环境机 $\mathcal{Z}$ 输入消息($KeyGen,sid$)首次激活 P_i,其中 $sid=(P_i,0)$。当 $\mathcal{A}$ 要求 $\mathcal{Z}$ 对一个消息 m 签名时,则 $\mathcal{Z}$ 通过输入消息($Sign,sid,m$)激活 P_i,并把报告返回给 $\mathcal{A}$。当 $\mathcal{A}$ 要求 $\mathcal{Z}$ 对消息对(m,σ)验证时,

$\mathcal{Z}$ 首先验证 m 之前被签名过,若验证成功 $\mathcal{Z}$ 输出 0 并停机。接下来,环境机 $\mathcal{Z}$ 输入消息($Verify$,sid,m,σ,v')激活未被收买的参与方并把验证结果输出。

真实的敌手 $\mathcal{A}$ 等待参与方 P_i 被激活成功后公开验证公钥 v。随后,$\mathcal{A}$ 输入 v 来运行 $\mathcal{G}$。当 $\mathcal{G}$ 生成一个需要签名的消息 m 后,$\mathcal{A}$ 要求 $\mathcal{Z}$ 对消息 m 进行签名。当 $\mathcal{A}$ 收到来自 $\mathcal{Z}$ 的签名 σ 后,把签名 σ 发送给 $\mathcal{G}$。当 $\mathcal{G}$ 输出消息对(m',σ')时,则 $\mathcal{A}$ 要求 $\mathcal{Z}$ 对(m',σ')进行验证。若验证成功,则说明伪造者 $\mathcal{G}$ 伪造成功。因此,在这个假设下,伪造者 $\mathcal{G}$ 成功的概率是不可忽略的,即环境机 $\mathcal{Z}$ 的输出 1 的概率是不可忽略的。然而,在理想模型下,环境机 $\mathcal{Z}$ 输出 1 的概率是存在的。因此,假设不成立,协议 π_{Σ} 具有不可为造性。

4　协议实例

基于离散对数问题定义一个多元组的概率多项式算法 $\Sigma=(setup,open,sign,ver,open)$ 作为一个群签名协议。其中,设 $H()$ 是一个哈希函数,$\mathbf{G}$ 是一个阶为 g 的循环域。

1)$setup$:随机选取一个大素数 p,随机选取一个生成元 $g\in\mathbf{G}$ 和 $x\in\mathbf{Z}_p^*$,计算 $h=g^x$,群公钥 $v=(p,g,h)$ 和群管理员私钥 $S_{GM}=(p,g,x)$。

2)$join$:请求加入群的用户随机选取 $x_i\in\mathbf{Z}_p^*$,并发送给群管理员,随机群管理员选取 $y_i\in\mathbf{Z}_p^*$ 并把(id,x_i)储存,计算 $C_2=h^{y_i}x_i$,群成员私钥 $S_i=(y_i,C_2)$ 和群成员证书 $CE_i=(id,x_i)$。

3)$sign$:随机选取一个整数 $k\in N^*$ 且 $gcd(k,p-1)=1$,计算 $r=g^k \bmod p$,计算 $s=k^{-1}(H(m)-ry_i)\bmod(p-1)$,计算 $C_1=g^{y_i}$,签名 $\sigma=(m,s,r,C_1,C_2)$。

4)ver:验证 $g^{H(m)}=C_1^r r^s \bmod p$。如果成立,那么 $\varphi=1$;否则,$\varphi=0$。

5)$open$:验证 $x_i=C_2/C_1^x$。如果成立,那么输出 id;否则,输出错误。

5　结束语

群签名可以广泛应用于电子选举、电子政务及电子商务。在通用可组合安全性框架下模块化的研究协议,可以确保协议在多个协议并发执行时的安全性。本文在通用可组合的安全性框架下研究群签名协议,定义群签名协议的理想函数,并提出可实现此理想函数的群签名协议。也对此协议的通用可组合的安全性及不可伪造性进行证明。基于离散对数问题给出一个具体的通用可组合安全的群签名协议实例。分析结果表明,相比于现有的群签名协议,所提协议保证了在多协议并发执行时的安全性。群盲签名协议的通用可复合性研究是下一步的研究方向。

参考文献

[1] Chaum D,Heyst E. Group Signatures[C]//Proceedings of EUROCRYPT'91. Berlin,Germany:Springer-Verlag,1991:257-265.

[2] Desmedt Y, Frankel Y. Shared Generation of Authenticators and Signatures [C]//Proceedings of Advances in Cryptology-Crypto'91. Berlin, Germany: Springer-Verlag,1992:457-469.

[3] Camenisch J, Stadler M. Efficient Group Signature Schemes for Large Groups [C]//Proceedings of Advances in Cryptology-Crypto'97. Berlin, Germany: Springer-Verlag,1997:410-424.

[4] 王蜀洪,王贵林,鲍　丰,等. 一种基于离散对数的群签名方案[J]. 计算机工程,2005,31(9):143-144.

[5] Ateniese G,Camenisch J,Joye M,et al. A Practical and Provably Secure Coalition-resistant Group Signature Scheme[C]//Proceedings of Advances in Cryptology-CRYPTO'00. Berlin, Germany: Springer-Verlag, 2000: 255-270.

[6] 王泽成,张亚军,王精明. 一个基于椭圆曲线的群签名方案[J]. 天中学刊,2002,17(5):21-23.

[7] 陈泽文,张龙军,王育民,等. 一种基于中国剩余定理的群签名方案[J]. 软件学报,2004,32(7):1062-1065.

[8] 陈泽文,王继林,黄继武,等. ACJT 群签名方案成员撤销的高效实现[J]. 软件学报,2005,16(1):151-157.

[9] 陈少真,孙慧慧. 一般化的向前安全群签名方案[J]. 计算机工程,2009,35(2):175-179.

[10] Canetti R. Universally Composable Security: A New Paradigm for Cryptographic Protocols[C]//Proceedings of the 42nd IEEE Symposium on Foundation of Computer Science. Washington D. C., USA: IEEE Press,2001:136-145.

[11] Canetti R. Universally Composable Signature, Certification, and Authentication [EB/OL]. (2004-11-21). http://iacr.org/cryptodb/data/paper.php? pubkey=11952.

[12] Seiji D, Yoshifumi M, Tatsuaki O. Universally Composable Blind Signatures[J]. International Journal of Information Technology & Decision Making, 2011, 3(4):673-684.

[13] 洪　璇,陈克非,李　强. 通用可组合安全的门限签名协议[J]. 通信学报,2009,30(6):1-6.

[14] 禹　勇,李继国,伍　玮,等 基于身份签名方案的安全性分析[J]. 计算机学报,2014,30(11):1025-1029.

[15] 隗　云,熊国华,张兴凯,等. 环签名的通用可组合安全模型及其应用研究[J]. 小型微型计算机系统,2012,33(1):38-44.

编辑　刘　冰