并发环境下可否认的环认证协议*

曾晟珂, 秦志光
(电子科技大学 计算机科学与工程学院, 成都 611731)

摘 要: 利用基于时限的承诺方案、非交互式零知识证明系统以及环签名算法,提出了一个可否认的环认证协议。在提出的协议中,即使环内所有成员的私钥都被俘获,协议的匿名性仍然保持。与相关的可否认的环认证协议相比,提出的协议通信轮数最少。证明表明,该可否认的环认证协议满足消息源匿名性、健壮性,并且在并发环境下仍然保持可否认性。

关键词: 并发可否认性; 可否认的环认证; 基于时限的承诺; 非交互式零知识证明系统
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2013)12-3745-04
doi:10.3969/j.issn.1001-3695.2013.12.059

Deniable ring authentication in concurrent setting

ZENG Sheng-ke, QIN Zhi-guang
(*School of Computer Science & Engineering, University of Electronic Science & Technology of China, Chengdu* 611731, *China*)

Abstract: Based on timed commitment, non-interactive zero-knowledge proof system and ring signature, this work proposed a deniable ring authentication protocol which adapted to concurrent setting. Although all the private keys of the group were corrupted, it also achieved the anonymity of this authentication protocol. Compared to the related works, the communication round of this protocol was optimal (only two rounds). The formal proof shows that this deniable ring authentication protocol satisfies source anonymity and soundness, and the deniability can hold in concurrent setting.

Key words: concurrent deniability; deniable ring authentication; timed commitment; non-interactive zero-knowledge proof

0 引言

认证协议允许消息的接收方能够验证该消息确实是由指定发送方发送的。数字签名算法可以有效地实现认证。在数字签名算法中,消息的发送方利用自己的私钥生成一个对该消息的签名,接收方使用发送方的公钥判断签名的有效性,从而接受或拒绝此次认证。由于这种认证方法需要使用发送方的公钥来实现,因此通过数字签名算法实现的认证具有可转移性。换句话说,任何人都能够相信发送方对该消息进行了认证,而发送方不能否认。在某些情况下,用户希望在为他人进行认证时保护自己的隐私,即发送方仅希望接收方相信认证,而在第三方面前,发送方可以否认认证。因此数字签名算法的公开可验证性不适合提供可否认的认证。

可否认的认证使得发送方在第三方面前可以否认认证,但该发送方的身份对于接收方来说却是公开的。可否认的环认证为发送方提供了匿名认证的机制。该机制将可否认的认证[1]与环签名[2]进行结合,使得接收方相信一个 Ad hoc 群体中的某个成员对消息进行了认证,却不知道具体是哪位成员。此外,接收方不能使任何第三方相信消息确实被认证了的事实,从而消息发送方实现了匿名可否认的认证。

在保护用户隐私的认证体制中,本文的研究重点在于如何为用户提供可以否认参与通信的技术。接收者相信消息确实被认证了,然而在整个通信的过程中,该认证却没有留下任何证据,使得第三方相信该认证发生过[1]。对可否认性的实现通常采用仿真技术。如果在发送者与接收者之间运行的通信副本能够被敌手仿真,那么此次认证就实现了认证的可否认性。由于第三方在真实的通信副本中的视图与在敌手模拟的通信副本中的视图是不可区分的,因此第三方无法相信发送方确实进行了此次认证,从而发送方能够成功否认。

1 相关工作

可否认的认证由 Dolev 等人[3]提出,Dwork 等人[1]对此进行了形式化的研究。在该文中,作者对可否认的认证定义为:接收方能够相信某消息确实被发送方认证,但是该认证过程却没有留下任何迹印,因此第三方不会相信该认证确实发生过。按照可否认的认证定义[1],学者们对可否认的认证作了深入研究,提出了相关的方案[4~7]。2002 年,Naor[8]将可否认的认证协议与环签名算法进行结合,提出了可否认的环认证协议。在可否认的环认证协议中,发送方实现了对消息进行匿名可否认的认证。然而,文献[8]中的协议没有考虑并发环境下的可否认性。Susilo 等人[9]基于环签名方案和 Chameleon 哈希函数,提出了非交互式的可否认的环认证方案。由于 Chameleon 哈希函数的性质,接收方可以模拟对于特定消息的认证过程,但是环签名算法的公开可验证性使得敌手无法模拟整个通信副本。因此文献[9]不能满足文献[1,8]中对可否认的认证定义。Dowsley 等人[10]提出的可否认的环认证协议优化了文献[8]的通信轮数,该协议的匿名性在所有成员的私钥都被俘获的情况下(即文献[8]中的 big brother 情况)仍然保持成立,并

收稿日期: 2013-02-25; **修回日期**: 2013-04-15 **基金项目**: 国家自然科学基金资助项目(61133016);国家重大专项项目(2011ZX03002-002-03)
作者简介: 曾晟珂(1982-), 女,重庆人,博士, 主要研究方向为密码学(zengshengke@gmail.com);秦志光(1956-), 男, 教授,博士,主要研究方向为计算机开放系统与网络安全性、信息系统安全、ITS(智能交通)、电子商务.

将文献[8]中的通信轮数由 6 轮降低为 4 轮。然而与文献[8]相似,文献[10]依然没有最终解决如何满足并发环境中的可否认性。

本文考虑如何在并发环境下构造可否认的环认证协议。在该协议中,消息发送方可以实现匿名认证。该认证不会留下任何证据,因此,发送方可以否认通信。换句话说,认证协议中的通信副本可以被一个仿真器模拟。此外,要求该可否认性在并发环境下同样成立。基于此目的,本文利用基于时限的承诺方案,构造了一个在并发环境下安全的可否认的环认证协议。该协议构造简单,协议的匿名性满足 big brother 情况,且通信轮数仅为 2 轮。

2 预备知识

2.1 非交互式零知识证明系统

非交互式零知识证明系统(NIZK)允许证明者 P 通过一个证明使得验证者 V 相信一个论断的真实性,而整个证明不透露除了论断本身的任何信息。对于一个 NP 语言 L,任何属于 L 的论断 x 都拥有一个证据 w,因此该证据能够使其拥有有效的证明 $x \in L$。(x,w) 组成一个二元关系 $\mathbb{R}$。对于 NP 语言 L,关系 $\mathbb{R}$ 的 NIZK 证明系统一般由公共参考串 σ,证明者 P 和验证者 V 组成。给定 $(x,w) \in \mathbb{R}$,P 输入 (σ,x,w),输出证明 π。V 输入 (σ,x,π),输出“接受/拒绝”。

定义 1 如果 (P,V) 是一个非交互式零知识证明系统,那么对于 NP 语言 L,二元关系 $\mathbb{R}$,以下性质成立:

a)完整性。对于任何 $x \in L$,$(x,w) \in \mathbb{R}$,以及任何 $\sigma \in \{0,1\}^{l(\gamma)}$,$V_\sigma(x,P_\sigma(x,\pi))=1$ 成立,其中 γ 为安全参数。

b)健壮性。对于任何敌手 A,$\Pr[V_\sigma(x,\pi)=1:(x,\pi) \leftarrow A(\sigma),\sigma \leftarrow \{0,1\}^{l(\gamma)}]$ 是可忽略的。

c)零知识性。对于任何敌手 A,存在一个仿真器 M,使得 A 在真实的证明系统中的视图与在 M 仿真的证明系统中的视图是不可区分的。

2.2 基于时限的承诺方案

基于时限的承诺方案由 Boneh 等人[11]提出,是标准承诺方案的扩展。在基于时限的承诺方案中,被承诺的值仅仅在时间 t 内是安全的。而当 $T>t$ 后,被承诺的值可以被强力打开。对于基于时限的承诺方案来说,被承诺的值只在有限时间内对接收者保密。该承诺方案可以应用于合同签订[11]、公平交换[12]以及可否认的认证[13,14]。

2.2.1 基于时限的承诺算法的定义

假设承诺者 Alice 向接收者 Bob 运行一个对于串 $S \in \{0,1\}^n$ 的基于时限的承诺算法,该承诺算法满足 (T,t,ε) 安全。通过该承诺算法,Alice 可以向 Bob 证明被承诺的值是串 S。如果 Alice 拒绝向 Bob 揭示 S,那么 Bob 可以在时间 $T>t$ 后强力获得 S。而在时间 t 内,Bob 从承诺结果中成功得到 S 的概率最多为 ε。一个 (T,t,ε) 安全的承诺算法 TC = (TCom, TO, TFO) 包括以下三个阶段:

a)承诺阶段 TCom。Alice 对串 $S \in \{0,1\}^n$ 运行基于时限的承诺算法,然后将承诺的结果 c 发送给 Bob。

b)打开阶段 TO。一段时间后,Alice 向 Bob 揭示 c 中承诺的值 S,并使得 Bob 在协议完成后拥有证明 π。该证明 π 让任何人相信 S 是 c 中被承诺的值。

c)强力打开阶段 TFO。如果 Alice 拒绝与 Bob 进行打开算法,那么 Bob 可以强力打开 c 并获得 c 中被承诺的值 S 以及证明 π。该强力打开算法运行的最长时间是 T。

2.2.2 时限承诺算法的安全属性

一个 (T,t,ε) 安全的时限承诺算法满足以下安全属性:

a)绑定性(binding)。不存在 $S' \neq S$,使得对 S' 运行承诺方案后,得到与对 S 运行承诺算法相同的承诺结果 c。

b)健壮性(soundness)。对于承诺的结果 c,一定存在一个强力打开算法,在不超过 T 的时间里能恢复被承诺的值 S。

c)秘密性(privacy)。对于一个概率多项式时间的敌手 A,在时间 $t<T$ 内,不能从承诺的结果 c 中恢复出被承诺的值 S。

2.3 环签名方案

在环签名方案[2]中,签名者可以代表他所在的群体匿名地生成一个签名。验证者通过输入该群体内所有成员的公钥,判断该签名的有效性。环签名算法让验证者相信签名的生成者来自于该群体,却无法辨认是群体中的哪一位成员对消息进行了签名。因此环签名算法保护了签名者的隐私。

2.3.1 环签名算法的定义

环签名算法一般由以下三个算法构成:

a)密钥生成算法 $\mathrm{KGen}(1^\gamma)$。给定安全参数 γ,输出成员 i 的公钥 vk_i 和私钥 sk_i。

b)环签名算法 $\mathrm{RSig}(m,R;sk_k)$。假设群体 $R=\{vk_1,vk_2,\cdots,vk_n\}$,签名者为环 R 中的成员 $k(vk_k \in R)$。给定消息 m,签名者 k 的私钥 sk_k。该算法输出环签名 $\alpha \leftarrow \mathrm{RSig}(m,R;sk_k)$。

c)环验证算法 $\mathrm{RVer}(m,R,\alpha)$。给定 (m,R,α),验证者判断 α 是否是一个对于 (m,R) 有效的签名。

2.3.2 环签名算法的安全属性

一个安全的环签名算法 RSig 需要满足无条件匿名性和不可伪造性。

1)无条件匿名性 区分者 D 不能通过一个给定的环签名判断其真实的生成者。形式化地,D 可以从挑战者处得到一组公钥 $U=\{vk_i\}_{i=1}^{\chi}$,也可以向挑战者作签名询问和俘获私钥的询问(即获得 U 中成员的私钥)。最后,D 将选择一条新鲜的消息 m^*、环 $R^*(R^* \subseteq U)$ 以及索引 $(i_0,i_1) \in R^*$。挑战者投掷一枚均匀的硬币 $b \leftarrow \{0,1\}$,并利用私钥 sk_{i_b} 生成签名 $\alpha^* \leftarrow \mathrm{RSig}(m^*,R^*;sk_{i_b})$。得到 α^* 后,D 将输出 b'。如果 $|\Pr[b'=b]-1/2|$ 是可以忽略的,那么称环签名算法 RSig 满足无条件匿名性。

2)不可伪造性 如果敌手 F 没有得到环 R^* 中成员的私钥,那么敌手 F 不能生成一个对于 (m^*,R^*) 有效的签名。形式化地,F 可以从挑战者处得到一组公钥 $U=\{vk_i\}_{i=1}^{\chi}$,也可以向挑战者作签名询问和俘获私钥的询问(即获得 U 中成员的私钥)。最后,F 选择一条新鲜的消息 m^* 和一个环 $R^*(R^* \subseteq U)$,并生成签名 α^*。要求 F 没有对 m^* 作过签名询问,也没有对 R^* 中的成员作过俘获私钥的询问。如果 $\Pr[1 \leftarrow \mathrm{RVer}(m^*,R^*,\alpha^*)]$ 是可以忽略的,那么称环签名算法 RSig 满足不可伪造性。

3 可否认的环认证模型

3.1 可否认的环认证协议的定义

可否认的环认证协议由发送者、接收者和一组参与者组

成。假设所有的参与者包括发送者和接收者的公钥能够被任何人访问,且这些公钥由统一的密钥生成算法生成。当接收者希望发送者对消息 m 进行认证时,发送方首先随机选择一些参与者,这些参与者以及发送方的公钥组成环 R。发送方代表环 R,完成对消息 m 的认证。协议结束后,接收方要么接受发送方对消息 m 的认证,要么拒绝认证。

3.2　可否认的环认证协议的安全模型

可否认的环认证协议是指接收方相信消息 m 已被环 R 中的某个成员认证,但不知道具体是哪位成员认证了该消息。并且,接收方不能使得第三方相信消息 m 被环 R 中的成员认证这个事实。可否认的环认证协议需要同时实现消息源隐藏性和可否认性。本节将形式化地刻画可否认的环认证协议的安全模型。该模型由完整性、健壮性、消息源隐藏性和并发可否认性这四个属性构成。

1)完整性　对于消息 m 以及环 R,如果发送者 A(A 的公钥 $vk_A \in R$)与接收者 B 诚实地执行该协议,那么接收者 B 拒绝此次认证的概率是可忽略的。

2)健壮性(不可伪造性)　敌手 C 可以向发送者 A 询问对一组消息 $m_1, m_2, \cdots$ 关于环的认证副本。如果 C 能够成功地使得接收者 B 相信消息 $m^* \notin \{m_i\}_{i=1,2,\cdots}$ 被环 R^* 中的某个成员认证,那么 C 将破坏认证协议的健壮性。要求 $vk_A \in R^*$ 且 R^* 中的所有成员都未被敌手 C 俘获。如果 C 成功的概率可以忽略,那么可否认的环认证协议满足健壮性。

3)消息源隐藏性　接收者 B 可以得到环 R 中的所有成员的私钥。随后 B 任意选择一个消息 m^*、环 R^*,以及 R^* 中的两个参与者 P_0 和 P_1 进行挑战。挑战者投掷一枚均匀的硬币 $b \leftarrow \{0,1\}$,并选择 P_b 完成对消息 m^* 关于环 R^* 的认证。对于 P_b 生成的认证副本,接收者 B 需要判断此次认证真实执行者的身份,即 B 输出 b'。如果 $|\Pr[b'=b]-1/2|$ 的概率是可忽略的,那么可否认的环认证协议满足消息源隐藏性。

4)并发可否认性　如果一个(恶意的)接收方 B 不能让第三方相信发送方 A 对消息 m 进行了认证,那么该认证协议满足可否认性。也就是说,存在一个算法可以模拟敌手 C 对于此次通信的副本,且该模拟的通信副本与真实的通信副本是不可区分的。现在在并发环境中考虑可否认性。C 与发送方 A 运行一个并发的交互,该交互包含与 A 进行的多次认证通信,且这些通信被 A 任意地交错执行。如果在并发环境下,C 与发送方 A 的认证通信还能被模拟,那么可否认的环认证协议满足并发可否认性。形式化地,把 C 与发送方 A 进行的真实认证通信记为 T^{real},把 C 与 A 之间被模拟的认证通信记为 T^{sim}。如果存在区分者 D,使得 $|\Pr[D(\text{view}(C,T^{\text{sim}}))=1]-\Pr[D(\text{view}(C,T^{\text{real}}))=1]|$ 可以忽略,那么并发可否认性成立。

4　具体方案

4.1　可否认的环认证协议

本节将提出一个基于时限承诺算法的可否认的环认证协议 $\text{DRA}_{\text{timed}}$。该构造的主要思想是:接收者 B 首先利用 (T,t,ε) 安全的时限承诺算法对其私钥进行承诺,并提供一个非交互式零知识证明(该证明用来保证被承诺的值一定是他的私钥)。在验证该证明的有效性后,发送者 A 随机选取一组参与者 P_i,并将这些参与者与自己以及接收者 B 的公钥组成一个环 $R=\{vk_A, vk_B, vk_{P_1}, \cdots, vk_{P_n}\}$。随后,$A$ 用自己的私钥 sk_A 对 B 需要验证的消息 m 生成一个代表环 R 的环签名并完成认证。如果 A 在不超过时间 t 内完成该认证,那么 B 接受此认证。由于利用了环签名的无条件匿名性,协议 $\text{DRA}_{\text{timed}}$ 满足消息源匿名性。另一方面,当时间 $T>t$ 时,基于时限的承诺算法失效,任何人都可以从 B 的承诺中获得 B 的私钥并生成一个对于消息 m、环 R 的环签名。因此发送者可以否认对消息的认证。下面是基于时限承诺算法的可否认的环认证协议 $\text{DRA}_{\text{timed}}$ 的具体构造。

1)系统建立　所有参与者 P_i 以及发送者 A 和接收者 B 都公开自己的公钥。假设这些公钥都是通过统一的密钥生成算法产生,并且所有人都可以访问到这些公钥。对于每次的认证,B 都运行密钥生成算法生成他的公私钥对关于环 $(vk_B, sk_B)=(v_0,s_0)\leftarrow\text{KGen}(1^\gamma)$。对于每次的认证,$A$ 从所有参与者中随机选取公钥关于环 vk_i,并将这些公钥组成环 $R=\{vk_A, vk_{P_1}, vk_{P_2}, \cdots\}=\{v_1, v_2, \cdots, v_n\}$。假设 A 的公钥 $v_k \in R$,v_i 对应的私钥为 s_i。

2)可否认的环认证算法 $\text{DRA}_{\text{timed}}$　假设需要被认证的消息为 m,此次认证由 B 发起,A 选择的环 $R=\{v_1, v_2, \cdots, v_n\}$。

a)$B\rightarrow A$。B 选择一个 (T,t,ε) 安全的时限承诺算法 $\text{TC}=(\text{TCom},\text{TO},\text{TFO})$ 对自己的私钥 s_0 进行承诺并得到 $c=\text{TCom}(s_0)$。然后对 NP 语言 L_π 生成一个 NIZK 证明 π。其中语言 L_π 定义为

$$L_\pi=\{(c,v_0)\mid c=\text{TCom}(s_0)\wedge(v_0,s_0)\leftarrow\text{KGen}(1^\gamma)\}$$

B 将 $\text{flow}_1=(c,\pi)$ 发送给 A,并且 B 的计时器 t_0 开始工作。

b)$A\rightarrow B$。收到 $\text{flow}_1=(C,\pi)$ 后,A 首先验证 NIZK 证明 π 的有效性。如果无效,则拒绝;否则 A 运行环签名算法 $\text{RSig}(m,R';S_k)$。该算法生成一个对于消息 m、环 R' 有效的环签名 $\alpha\leftarrow\text{RSig}(m,R';S_k)$,其中 $R'=R\cup\{v_0\}$。A 将 $\text{flow}_2=\alpha$ 发送给 B。

如果 B 在时间 t 内接收到 flow_2 且 $1\leftarrow\text{RVer}(\alpha,m,R')$,那么 B 接受此次认证。

4.2　性能比较

按照文献[1,8]中对于可否认的认证的定义,Naor 提出了首个可否认的环认证协议[8]。该认证协议假设存在一个公钥加密算法,通信轮数为 4 轮。在文献[8]中,Naor 同样也考虑了一个拥有更强敌手的场景。该场景中,所有环成员的私钥都会被暴露,也就是所谓的 big brother 情况。Naor 利用基于身份的加密和广播加密,构造了一个满足 big brother 情况的可否认的环认证协议,通信轮数为 6 轮[8]。随后,Dowsley 等人利用可验证的广播加密算法,构造了一个同样满足 big brother 情况的可否认的环认证协议[10],将文献[8]中的通信轮数降低为 4 轮。本文利用基于时限的承诺算法,构造了一个可否认的环认证协议。本文所提出的协议同样满足 big brother 情况,且通信轮数仅为 2 轮。

表 1 从通信轮数、是否满足并发环境等方面对三个相关的可否认的环认证协议进行了比较。

表 1　三个相关协议的性能比较

协议	通信轮数	big brother	并发环境
文献[8]	6	满足	不满足
文献[10]	4	满足	不满足
本协议	2	满足	满足

4.3 安全性分析

协议 DRA_{timed} 满足安全模型中的四个属性,即完整性、健壮性、消息源隐藏性和并发可否认性。

1)完整性 它可以通过直接验证协议 DRA_{timed} 的执行来检验。当发送者 A 和接收者 B 都诚实执行该协议时,那么 B 将以压倒性的优势接受 A 对 m 的认证。

2)健壮性(不可伪造性) 假设存在破坏协议健壮性的敌手 C,C 可以向发送者 B 询问 A 关于环 R 对一组消息 m_1,m_2,…的认证副本。如果 C 能够使得接收者 B 相信消息 $m^* \notin \{m_i\}_{i=1,2,\cdots}$ 被环 R^* 中的某个成员认证,那么 C 就成功破坏了该认证协议的健壮性。假定 $(vk_A, vk_B) \in R^*$ 且 R^* 中的所有成员都未被敌手 C 俘获。

协议 DRA_{timed} 的健壮性由环签名方案的不可伪造性和基于时限的承诺方案的秘密性保证。由于基于时限的承诺方案的限制,健壮性只在时间 t 内成立。由于承诺方案的秘密性成立,B 的私钥在时间 t 内安全地隐藏在承诺值中,使得敌手 C 无法得到。如果敌手 C 能让接收者 B 接受某认证副本是对消息 m^* 关于环 R^* 的认证,那么表明认证副本是一个关于 (m^*, R^*) 有效的环签名。由于环 R^* 中的所有成员均未被敌手 C 俘获,且敌手 C 也未询问过对于消息 m^* 的认证副本,因此,如果 C 成功完成了认证,那么 C 伪造了一个有效的环签名,破坏了环签名算法的不可伪造性。具体的证明见定理 1。

定理 1 如果环签名算法 RSig 满足不可伪造性,并且时限承诺算法 TC = (TCom, TO, TFO) 是 (T, t, ε) 安全的,那么协议 DRA_{timed} 满足健壮性。

证明 假设 F 是破坏协议 DRA_{timed} 的健壮性敌手,那么存在一个敌手 F' 将破坏环签名算法 RSig 的不可伪造性。F' 充当 F 的挑战者,给定 F' 一组公钥集合 $U = \{vk_1, vk_2, \cdots, vk_\chi\}$,$F'$ 的目标是伪造关于 (m, R) 的环签名,其中 $R \subseteq U$。当 F 向 F' 询问对消息 $\{m_i\}_{i=1,2,\cdots}$ 关于环 $R_i \cup \{vk_F\}$ $(R_i \subseteq U)$ 的环认证时,F' 对该认证的模拟如下:

a) $F \rightarrow F'$。F 利用自己的私钥 sk_F 生成承诺值 TCom (sk_F),并生成一个 NIZK 证明 π,然后将 $flow_1 = (TCom(sk_F), \pi)$ 发送给 F'。

b) $F' \rightarrow F$。由于时限承诺算法 TC = (TCom, TO, TFO) 是 (T, t, ε) 安全的,因此,F' 无法在时间 $t < T$ 内得到 sk_F。当 F' 需要为 F 返回 $flow_2 = RSig(m_i, R_i'; sk)$ 时(这里 $R_i' = R_i \cup \{vk_F\}$),F' 需要向它的环签名算法的挑战者询问关于 (m_i, R_i') 的环签名 α。得到该签名 α 后,F' 将 $flow_2 = \alpha$ 发送给 F。

最终,F 将挑战协议 DRA_{timed} 的健壮性。F 选择一条新鲜消息 $m^* \notin \{m_i\}_{i=1,2,\cdots}$ 以及环 R^*。如果 $R^* \not\subset U$,那么 F' 拒绝 F 的挑战。如果 F 成功破坏了协议 DRA_{timed} 的健壮性,那么说明 F 输出了一个关于 (m^*, R^*) 有效的环签名 α^*。由于 F 并未得到过关于 m^* 的环签名,也未得到集合 U 中成员的私钥,因此,有效的 α^* 暗示了 F' 成功破坏了环签名算法 RSig 的不可伪造性。由于环签名算法 RSig 是不可伪造的,从而推出矛盾,因此协议 DRA_{timed} 的健壮性成立。

3)消息源匿名性 该匿名性由环签名算法的无条件匿名性保证。假设存在破坏该匿名性的敌手 D,D 可以俘获任何参与者并且得到它们的私钥(即 big brother 情况)。随后,D 任意选择两个参与者 P_0 和 P_1、消息 m^* 以及环 R^* 作为挑战者。挑战者随机选取 P_b $(b = 0$ 或者 $b = 1)$,按照协议 DRA_{timed},模拟成员 P_b 对于消息 $m*$ 的环认证。也就是说,D 的挑战者使用 P_b $(b = 0$ 或者 $b = 1)$ 的私钥,生成对于 (m^*, R^*) 的环签名 $\alpha^* \leftarrow RSig(m^*, R^*; sk_{P_b})$。如果 D 能从签名 α^* 中输出 $b' = b$,那么表明 D 破坏了环签名算法的无条件匿名性(见 2.3.2 节),从而推出矛盾,因此协议 DRA_{timed} 满足消息源匿名性。

4)并发可否认性 如果在真实的消息发送者 A 和接收者 B 之间运行的通信副本能够在并发环境下被仿真,那么认证协议满足并发可否认性。

定理 2 如果时限承诺算法 TC = (TCom, TO, TFO) 满足 (T, t, ε) 安全,环签名算法 RSig 满足无条件匿名性且非交互式零知识证明系统 NIZK 满足健壮性,那么协议 DRA_{timed} 满足并发可否认性。

证明 由于时限承诺算法 TC = (TCom, TO, TFO) 满足 (T, t, ε) 安全,假设存在一个仿真器 M,将在时间 T 后提取 c 中被承诺的私钥 s_0。因为得到了私钥(签名密钥)s_0,M 可以使用私钥 s_0 生成一个关于消息 m 的环签名 $\alpha' \leftarrow RSig(m, R; s_0)$。因此,$M$ 仿真的认证副本为 $Auth' = (flow_1', flow_2')$ 且 $flow_1' = flow_1$,$flow_2' = \alpha'$。由于环签名算法 RSig 的无条件匿名性成立,M 在 $flow_2'$ 中通过私钥 s_0 生成的环签名 α' 与在真实的认证情况下发送者 A 用其私钥 s_k 生成的环签名 $\alpha \leftarrow RSig(m, R; s_k)$ 的分布是不可区分的。因此 $flow_2' = flow_2$,即仿真器 M 仿真的认证副本 Auth′统计的等同于真实的认证副本 Auth。具体地,本文构造仿真器 M 来仿真此次认证。当从(恶意的)接收者 B 处收到 $flow_1 = (c, \pi)$ 后,M 冻结 B,并在时间 T 后获得被承诺的 s_0。该基于模拟的冻结技术由 Dwork 等人[1] 使用。由于非交互式零知识证明系统 NIZK 的健壮性成立,如果 π 是有效的 NIZK 证明,那么 c 中被承诺的值一定是 s_0。随后 M 使用 s_0 生成 $flow_2' = \alpha' \leftarrow RSig(m, R^*; s_0)$。由于环签名算法的无条件匿名性成立,用私钥 s_k 生成的环签名 α 与用私钥 s_0 生成的环签名 α' 的分布是不可区分的。因此 M 的仿真统计等同于真实的认证副本。也就是说,在真实的消息发送者 A 和接收者 B 之间运行的通信副本能够被 M 仿真。所以,协议 DRA_{timed} 满足并发可否认性。

5 结束语

本文提出了一个在并发环境下安全的可否认的环认证协议。该协议使用基于时限的承诺算法、非交互式零知识证明系统和环签名算法,构造了可否认的环认证协议。该协议构造简单,通信轮数仅为 2 轮。由于利用了基于时限承诺算法的特点,该环认证协议在并发环境下同样满足可否认性。

参考文献:

[1] DWORK C, NAOR M, SAHAI A. Concurrent zero-knowledge[M]. [S.l.]:Springer, 1998.

[2] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[C]// Proc of ASIACRYPT London: Springer-Verlag, 2001:552-565.

[3] DOLEV D, DWORK C, NAOR M. Non-malleable cryptography[J]. SIAM Journal on Computing, 2000, 30(2): 391-437.

[4] PASS R. On deniability in the common reference string and random oracle model[C]//Proc of CRYPTO. [S.l.]:Springer, 2003:316-337.

(下转第 3752 页)

消息(m,c_1)的部分盲签名(U,V^*)。

下面证明$(\mathrm{ID},m,c_1,U,V^*)$是可以通过验证的:计算$Q_{\mathrm{ID}}=H_1(\mathrm{ID})$,$h=H_2(\mathrm{ID},m,U)$,验证等式:

$$e(V^*,P)=e(\frac{H_3(c_1)}{H_3(c)}(V'^*+\beta h^* P_{\mathrm{pub}}),P)=$$

$$e(\frac{H_3(c_1)}{H_3(c)}(\alpha h^* k' P_{\mathrm{pub}}+H_3(c)S_{\mathrm{ID}}+\beta h^* P_{\mathrm{pub}}),P)=$$

$$e(\frac{H_3(c_1)}{H_3(c)}(\alpha\frac{H_3(c)}{H_3(c_1)}hk' P_{\mathrm{pub}}+H_3(c)S_{\mathrm{ID}}+\beta\frac{H_3(c)}{H_3(c_1)}hP_{\mathrm{pub}}),P)=$$

$$e((\alpha hk' P_{\mathrm{pub}}+H_3(c_1)S_{\mathrm{ID}}+\beta hP_{\mathrm{pub}}),P)=$$

$$e((\alpha hk' P_{\mathrm{pub}}+\beta hP_{\mathrm{pub}}),P)e(H_3(c_1)S_{\mathrm{ID}},P)=$$

$$e((\alpha hk'+\beta h)P,P_{\mathrm{pub}})e(H_3(c_1)Q_{\mathrm{ID}},P_{\mathrm{pub}})=$$

$$e(hU+H_3(c_1)Q_{\mathrm{ID}},P_{\mathrm{pub}})$$

5 结束语

针对三个可证明安全的数字签名方案[6,11,18],本文指出李志敏等人提出的基于证书的数字方案不可以抵抗任意第三方的伪造攻击,黄茹芬等人提出的基于证书的盲签名方案不可以抵抗公钥替换攻击,何俊杰等人提出的部分盲签名方案不可以抵抗协商公共信息攻击。

由于随机预言模型下的安全性并不等同于标准模型下的安全性,研究者倾向认为标准模型更接近于现实模型,所以在标准模型下可证明安全同时尽可能少地运用双线性对的数字签名方案是下一步需要重点关注的一个研究课题。

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C] //Proc of CRYPTO'84. Berlin: Springer,1984:47-53.

[2] GENTRY C. Certificate-based encryption and the certificate revocation problem [C]//Lecture Notes in Computer Science, vol 2656. Berlin: Springer-Verlag, 2003:272-293.

[3] KANG B G, PARK J H, HAHN S G. A certificate-based signature scheme[C]//Lecture Notes in Computer Science, vol 2964. Berlin: Springer-Verlag,2004:99-111.

[4] WU Wei, MU Yi, SUSILO W, *et al*. Certificate-based signatures revisited [J]. Journal of Universal Computer Science, 2009, 15(8):1659-1684.

[5] 李继国,钱娜,黄欣沂,等. 基于证书强指定验证者签名方案[J].计算机学报,2012,35(8):1579-1587.

[6] 李志敏,徐馨,李存华. 高效的基于证书数字签名设计方案 [J]. 计算机应用研究,2012,29(4):1430-1433,1444.

[7] CHAUM D. Blind signature for untraceable payments [C] //Proc of Advances in Cryptology-CRYPTO. Berlin: Plenum Press, 1983: 199-233.

[8] 刘亚丽,殷新春,陈决伟. 基于 ELGAMAL 前向安全的盲签名方案 [J].通信学报,2007,28(8A):48-53.

[9] 邱钢,王宏,肖鸿 等. 两种前向安全盲签名体制的安全性分析 [J]. 西安电子科技大学学报,2010,37(1):107-111.

[10] 周萍,何大可. 高效无可信 PKG 的新型盲签名方案[J]. 计算机应用研究,2012,29(2):626-629.

[11] 黄如芬,农强,黄振杰. 一类可证安全的基于证书盲签名[J]. 计算机应用研究,2012,29(12):4622-4625,4630.

[12] ABE M, FUJISAKI E. How to date blind signatures [C] //Proc of International Conference on Theory and Applications of Cryptology and Information Security. Berlin: Springer-Verlag,1996:244-251.

[13] CHOW S S M, HUI L C K, YIU S M. Two improved partially blind signature schemes from bilinear pairings[C]//Proc of the 10th Australasian Conference on Information Security and Privacy. Berlin: Springer-Verlag,2005:316-328.

[14] 李明祥,李峰,王涛. 部分盲签名综述[J]. 计算机应用研究,2012,29(12):4437-4440.

[15] 崔巍,辛阳,胡程渝. 高效的基于身份的(受限)部分盲签名方案 [J]. 北京邮电大学学报,2008,31(4):53-57.

[16] 李明祥,赵秀明,王洪涛. 对一种部分盲签名方案的安全性分析与改进[J]. 计算机应用,2010,30(10):2687-2690.

[17] 何俊杰,孙芳,祁传达. 基于身份的部分盲签名方案的分析与改进[J]. 计算机应用,2013,33(3):762-765.

[18] 何俊杰,王娟,祁传达. 安全高效的基于身份的部分盲签名方案 [J]. 计算机应用,2012,32(5):1388-1391.

[19] SHIM K A. An ID-based aggregated signature scheme with constant pairing computation[J]. Journal of Systems and Software, 2010, 83(10):1873-1880.

(上接第 3748 页)

[5] Di RAIMONDO M, GENNARO R, KRAWCZYK H. Deniable authentication and key exchange[C]//Proc of the 13th ACM Conference on CCS. New York:ACM Press, 2006:400-409.

[6] Di RAIMONDO M, GENNARO R, NAOR M. New approaches for deniable authentication[J]. Journal of Cryptology, 2009, 22(4): 572-615.

[7] DODIS Y, KATZ J, SMITH A. Composability and on-line deniability of authentication[C]//Proc of the 6th Theory of Cryptography Conference. Berling: Springer-Verlag, 2009:146-162.

[8] NAOR M. Deniable ring authentication[C]//Proc of the 22nd Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag, 2002481-498.

[9] SUSILO W, MU Yi. Non-interactive deniable ring authentication [C]//Proc of ICISC[S.l.]:Springer, 2004:386-401.

[10] DOWSLEY R, HANAOKA G, IMAI H, *et al*. Round-optimal deniable ring authentication in the presence of big brother[C]//Proc of the 11th International Conference on Information Security Applications Berlin:Springer-Verlag, 2011:307-321.

[11] BONEH D, NAOR M. Timed commitment[C]//Proc of CRYPTO. [S.l.]: Springer, 2000:236-254.

[12] GARAY J A, POMERANCE C. Timed fair exchange of standard signatures[C]//Proc of FC[S.l.]: Springer, 2003:190-207.

[13] JIANG Shao-quan. Dwork-Naor ZAP and its application in deniable authentication, revisited[C]//Proc of the 6th International Conference on Information Security and Cryptology. Berlin: Springer-Verlag, 2011:443-454.

[14] JIANG Shaoquan. Timed encryption with application to deniable key exchange[C]//Proc of the 9th Annual International Conference on TAMC. Berlin:Spring-Verlag, 2012:248-259.