标准模型下基于身份的混淆乐观公平交换方案

戚 珉,陈 明
(宜春学院数学与计算机科学学院,江西宜春 336000)

摘 要: 为防止签名验证者利用部分签名取得不公平的优势,Huang 等人提出混淆乐观公平交换(Ambiguous Optimistic Fair Exchange,AOFE)方案及其一般构造方法,但是其构造方法没有考虑真实的用户环境.在基于 IBC(Identity-Based Cryptography)的用户环境下,文章提出基于身份的混淆乐观公平交换(ID-AOFE)方案构造方法、方案实例、及其选择身份安全模型.提出的 ID-AOFE 构造方法对 Huang 等人的 AOFE 方案进行了简化,采用具有信息提取功能的证据不可区分证明算法替换原方案模型中的基于标签加解密和零知识证明算法.ID-AOFE 安全模型以 Huang 等人的 AOFE 安全模型为基础,融合了选择身份安全模型,并对 ID-AOFE 方案的安全性进行了归纳和重新定义.在选择身份安全模型下,提出的 ID-AOFE 方案实例的公平性被规约到经典密码原语的安全性.此外,文章探讨了 ID-AOFE 方案的消息交互模型,就争端解决的方案和过程进行了重点分析.

关键词: 乐观公平交换;签名交换;基于身份密码学;非交互的证据不可区分证明;公平性;签名者的混淆;标准模型
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2020)08-1516-12
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.08.009

ID-Based Ambiguous Optimistic Fair Exchange in the Standard Model

QI Min,CHEN Ming
(*School of Mathematics and Computer Science,Yichun University,Yichun,Jiangxi* 336000,*China*)

Abstract: A generic ambiguous optimistic fair exchange(AOFE)scheme,a variant of OFE,is proposed by Huang et al. The AOFE scheme prevents signature verifiers from convincing anybody about the authorship of a partial signature generated by the signer. However,the AOFE scheme cannot be directly applied to an actual user environment. A generic AOFE scheme and an instantiation of the generic construction in an identity-based user environment were proposed in this paper. In the generic construction of identity-based AOFE(ID-AOFE),the tag-based encryption and zero-knowledge proof algorithms in Huang et al.'s AOFE was removed and the non-interactive witness indistinguishable proof algorithms extracting the hided witness via keys was employed. Furthermore,we summarized and redefined the security of the ID-AOFE scheme. Then,an ID-AOFE security model was defined based on the Huang et al.'s AOFE security model and the selective identity security model. Under the selective identity security model of ID-AOFE,the fairness of our scheme is reduced to the securities of several classical cryptographic primitives. In addition,this paper discussed the message interaction model of the ID-AOFE scheme,and analyzed the mechanism of dispute resolution.

Key words: optimistic fair exchange;signature exchange;identity-based cryptography;non-interactive witness indistinguishable proof;fairness;signer ambiguity;standard model

1 引言

乐观公平交换[1](Optimistic Fair Exchange,OFE)允许两方或多方在 TTP(Trusted Third Party)干预的情况下完成信息交换,实现交换的公平性.在 OFE 方案中,TTP 不必参与每次交换过程,仅当交易出现争端时才需

收稿日期:2018-09-28;修回日期:2020-05-08;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61662083);江西省教育厅科学技术研究项目(No.GJJ151037)

要 TTP 进行争端裁决,这样的 TTP 称为离线的可信第三方(off-line TTP).相对 on-line TTP 公平交换[2]来说,OFE 方案大大降低了 TTP 的工作负载,得到广泛研究,提出了大量具体的 OFE 方案[3,4].

基于 OFE 的签名交换协议[5,6]是一类典型的 OFE 协议,包含签名者 S、签名验证者 V 和 off-line TTP 三类角色.其基本原理是:由 S 产生待签名消息 M 的部分签名 σ_{SP}发送给 V;V 收到 σ_{SP}后产生 M 的完整签名 σ_{VF}发送给 S;S 收到 σ_{VF}后产生 M 的完整签名 σ_{SF}发送给 V;V 收到 σ_{SF}后交易顺利结束.如果上述交换过程出现异常,则由 S 或 V 发起争端解决协议,请求 TTP 进行争端裁决.

基于 OFE 的签名交换协议除满足签名的不可伪造性外,更重要的是实现签名交换的公平性.公平性的非形式化的定义如下:要么交换双方都正确接收来自交换对端的有效完整签名 σ_{SF}(或 σ_{VF}),要么双方都不能获得任何有用的信息.这里的"有用信息"是一种主观的描述.根据交换过程,验证者 V 收到 σ_{SP}后可以选择终止交换,此时,V 已经收到 S 产生的部分签名 σ_{SP},而 S 没有收到 V 的任何信息.因此,如何产生 σ_{SP}以及 σ_{SP}是否对 V 有用,是该类型协议一个重要的研究点.

早期的方法是采用可验证加密签名[7,8]机制生成 σ_{SP}.可验证加密签名机制能实现对原始签名的隐藏,即,可公开验证 σ_{SP}中包含 S 对 M 的有效签名,但是该签名被加密了,不能作为有效的完整签名 σ_{SF}.直观看来,采用可验证加密签名似乎能实现交换的公平性.但是,这类方案忽视了可验证加密签名的不可否认性.虽然可验证加密签名不是完整签名,但它包含了签名者 S 对某项事实的承诺,并且这项承诺是可公开验证的.设想这样一种应用场景:假设签名者 Alice 就一份电子合同 M 与签名验证者 Bob 发起 OFE 协议进行签名交换,Alice 首先采用可验证加密签名生成 M 的部分签名 σ_{SP}发送给 Bob;Bob 收到 σ_{SP}后,可选择与 Alice 完成交换,但是,不诚实的 Bob 可以终止与 Alice 的交换过程,利用 Alice 对 M 的承诺(σ_{SP})向 Alice 的竞争者(比如 Charlie)索取更有利于自身的合同条款,转而与 Charlie 完成新的交换协议.上述场景中,Alice 的合法权益遭受了侵害,不诚实的 Bob 利用协议的缺陷取得了不公平的优势.针对协议的这一缺陷,Garay 等人[9]提出了签名交换协议的滥用公平性,采用指定验证者签名机制生成部分签名 σ_{SP}.指定验证者签名[10]是指:只有指定的验证者 Bob 能够验证部分签名 σ_{SP}中包含签名者 Alice 对 M 的签名,而非指定的其他实体,比如 Charlie,仅能确认 σ_{SP}中要么含有 Alice 的签名或者是 Bob 的签名.采用指定验证者签名机制生成的 σ_{SP}不具有不可否认性,Bob 不能利用 σ_{SP}向 Charlie 证明 Alice 对 M 做出了承诺.随后,许多研究者对指定验证者签名及其在 OFE 中的应用进行了深入研究,提出了多种具体的方案[11~15].

为了解决上述问题,Huang 等人[16,17]提出混淆乐观公平交换(Ambiguous OFE,AOFE)概念,定义了签名者身份混淆属性,提出了 AOFE 的一般构造方法:采用证据不可区分证明和零知识证明技术[18]隐藏部分签名 σ_{SP}的签名者身份,使得与签名无关者不能区分 σ_{SP}的真实签名者.签名者身份混淆属性与滥用公平性本质相同.但是,指定验证者签名难于扩展应用到多方交换协议,而采用证据不可区分证明和零知识证明技术更易于扩展.考虑到签名交换双方在交换完成之前不希望泄露交易的任何信息,Wang 等人[19]对 AOFE 进行了增强,对交换的信息进行加密.Wang 等人的增强 AOFE 方案难于扩展到多方交换的应用场景.Huang 等人[20]进一步提出隐私保护的 OFE 方案 P2OFE.P2OFE 方案采用了验证者和 TTP 公钥双重加密策略防止 TTP 取得完整签名,使用交互式证明技术证明部分签名中包含一个有效的完整签名,显著增加了协议运行的开销,并且 P2OFE 方案难于扩展到多方交换环境.在 P2OFE 方案的基础上,Guo 等人[21]提出一种通用的 P2OFE 方案模型,但是没有给出具体的实例.

值得注意的是: Huang 等人[17]提出的 AOFE(记为 Huang-AOFE)一般构造方法基于选择密钥模型,没有考虑用户密钥的可信性问题.具体来讲,在 Huang-AOFE 方案的密钥生成算法中,TTP 和用户均自行生成公私钥,缺乏认证权威 CA 对密钥进行授信.因此,用户密钥缺乏可信任根,无法应用于真实的用户环境,例如,基于公钥基础设施或 IBC(Identity-Based Cryptography)[22]的用户环境.本文进一步研究 AOFE 方案,对 Huang 等人提出的一般构造方法进行简化和扩展,提出基于身份的 AOFE(ID-AOFE)方案模型及其构造实例.

IBC 体制是一种将用户身份标识(ID)作为用户公钥的非对称密码体制,由 Shamir[22]在 1984 年的美密会议上首次提出.在 IBC 系统中,PKG(Private Key Generation)根据用户 ID 用其主密钥为用户生成长期私钥,但不产生公钥证书,无需公钥基础设施支持.自 Boneh 等人[23]基于双线性对理论提出基于身份加密方案以来,IBC 体制得到广泛深入的研究.2007 年,RFC5091[24]发布,Boneh-Franklin[23](BF)算法被推荐为基于身份加密标准.IBC 体制作为 PKI 体制的补充,非常适合需要简化密钥管理结构的应用环境,比如复杂社交网络.

本文的主要工作是:公平交换协议广泛应用于复杂社交网络中,考虑到社交网络简化密钥管理的需求,提出基于 IBC 体制的 ID-AOFE 方案模型及其构造实例.首先,本文将 Huang 等人[17]提出的 AOFE 扩展到基于 IBC 的用户环境并做出简化.第二,在文献[17]安全模型的基础上,结合 Paterson 等人[25]的无随机预言机的

选择身份安全模型,定义了 ID-AOFE 方案的选择身份安全模型. 第三,基于 Paterson 等人[25]的 IBS 方案(Identity Based Signatures)、Boneh 等人[26]的 OTS 方案(One-Time Signature)和 Groth 等人[18]提出的 NIWI 算法(Non-Interactive Witness Indistinguishable)(记为 G-NIWI)算法,提出一种具体的 ID-AOFE 方案实例,并且在选择身份安全模型下将方案的各安全属性分别规约到 IBS、OTS 以及 NIWI 方案的安全性,实现了可证明安全. 第四,本文还详细讨论了 ID-AOFE 方案的消息交互模型,主要分析了争端解决的具体方案.

2 背景知识

2.1 困难问题与假设

本文方案基于以下困难数学问题及假设,简要描述如下,详细内容请参考文献[18,25,26].

双线性映射:给定大素数 p,阶为 p 的循环群 G_1 和 G_2,g 是 G_1 的 1 个生成元,如果 $e:G_1\times G_1\rightarrow G_2$ 是从 G_1 到 G_2 的 1 个有效的双线性映射,那么满足以下条件.

(1)双线性:给定 $u,v\in G_1$ 和任意的 $a,b\in\mathbb{Z}_p$,满足 $e(u^a,v^b)=e(u,v)^{ab}$.

(2)非退化性:$e(g,g)\neq 1$.

(3)可计算性:给定任意的 $u,v\in G_1$,存在多项式时间算法能成功计算 $e(u,v)$.

CDH(Computational Diffie-Hellman)问题:对于任意未知的 $a,b\in\mathbb{Z}_p$,给定 $g,g^a,g^b\in G_1$,求解 g^{ab}.

CDH 假设:不存在多项式时间算法能成功求解 CDH 问题.

BDH(Bilinear Diffie-Hellman)问题:对任意未知的 $a,b,c\in\mathbb{Z}_p$,给定 $(g^a,g^b,g^c)\in G_1^3$,计算 $e(g,g)^{abc}$.

BDH 假设:不存在多项式时间算法能成功求解 BDH 问题.

q-SDH(Strong Diffie-Hellman)问题:给定 $(g,g^{\alpha},g^{\alpha^2},\cdots,g^{\alpha^q})\in G_1^{q+1}$,计算输出 $(w,g^{\frac{1}{w+\alpha}})$. 其中,$w\in\mathbb{Z}_p$,$\alpha\in\mathbb{Z}_p$ 为一未知的随机数.

q-SDH 假设:不存在多项式时间算法能成功求解 q-SDH 问题.

DLIN(Decisional Linear)假设:在存在多项式时间敌手 A 的条件下,如果 $\Pr[(p,G_1,G_2,e,g)\leftarrow G_{\mathrm{DLIN}}(1^{\kappa});a,b,r,s\leftarrow\mathbb{Z}_p:A((p,G_1,G_2,e,g),g^a,g^b,g^{ra},g^{sb},g^{r+s})=1]\approx\Pr[(p,G_1,G_2,e,g)\leftarrow G_{\mathrm{DLIN}}(1^{\kappa});a,b,r,s,t\leftarrow\mathbb{Z}_p:A((p,G_1,G_2,e,g),g^a,g^b,g^{ra},g^{sb},g^t)=1]$ 成立,则 DLIN 假设成立.

2.2 基于身份的 AOFE 方案及其安全模型

2.2.1 基于身份的 AOFE 方案

文献[17]提出 AOFE 方案的一般构造方法,由 $\mathrm{Setup}^{\mathrm{TTP}}$、$\mathrm{Setup}^{\mathrm{User}}$、PSig、PVer、Sig、Ver 和 Res,7 个算法组成,简要描述如下.

$\mathrm{Setup}^{\mathrm{TTP}}$:输入公开参数 PM 和安全参数 κ,仲裁者运行算法 $\xi.\mathrm{Kg}(1^{\kappa})$ 生成公私钥对 $(pk_{\mathrm{TA}},sk_{\mathrm{TA}})$,运行 $\Pi.\mathrm{Kg}(1^{\kappa})$ 算法产生公共参考串 crs,然后发布 $APK=(pk_{\mathrm{TA}},crs)$ 作为他的完整公钥,秘密保存其私钥 $ASK=sk_{\mathrm{TA}}$.

$\mathrm{Setup}^{\mathrm{User}}$:每个用户运行算法 $\delta.\mathrm{Kg}(1^{\kappa})$ 生成各自用于签名的公私钥对 $(PK_i=pk_i,SK_i=sk_i)$.

Psig:给定待签名的消息 M 和一个签名验证者 U_j,签名者 U_i 按照下面的方法产生一个部分签名.

(1)$(otvk,otsk)\leftarrow\mathrm{OTS.Kg}(1^{\kappa})$:生成一对用于一次签名算法的新的秘钥对,$otsk$ 为签名秘钥,$otvk$ 为验证公钥.

(2)$\sigma\leftarrow\delta.\mathrm{Sig}(SK_i,otvk)$:采用基于长期私钥的签名算法对一次签名算法的公钥 $otvk$ 进行签名.

(3)$c\leftarrow\xi.\mathrm{Enc}(pk_{\mathrm{TA}},otvk,\sigma;r)$:选择随机值 r,以 $otvk$ 为标签,使用仲裁者公钥 pk_{TA},采用基于标签的加密算法加密 σ,得到密文 c.

(4)$\pi\leftarrow\Pi.\mathrm{Prv}(crs,(pk_{\mathrm{TA}},PK_i,PK_j,c,otvk),(\sigma,r))$:使用证据$(\sigma,r)$产生零知识证明 π.

(5)$\delta\leftarrow\mathrm{OTS.Sig}(otsk,c\parallel\pi\parallel M\parallel PK_i\parallel PK_j)$:使用一次签名秘钥 $otsk$ 对消息$(c\parallel\pi\parallel M\parallel PK_i\parallel PK_j)$进行签名.

最后,输出部分签名 $\sigma_{\mathrm{P}}=(c,\pi,\delta,otvk)$.

PVer:收到 U_i 对消息 M 的部分签名 $\sigma_{\mathrm{P}}=(c,\pi,\delta,otvk)$,验证者验证等式 $\mathrm{OTS.Ver}(otvk,\delta,c\parallel\pi\parallel M\parallel PK_i\parallel PK_j)=1$ 和 $\Pi.\mathrm{Ver}(crs,(pk_{\mathrm{TA}},PK_i,PK_j,c,otvk),\pi)=1$ 是否成立. 若任一等式不成立,则拒绝该部分签名,否则接受.

Sig:给定待签名消息 M 和签名验证者 U_j,签名者 U_i 调用 Psig 算法输出完整签名 $\sigma_{\mathrm{F}}=(\sigma,\sigma_{\mathrm{P}})$.

Ver:收到 U_i 对消息 M 的完整签名 $\sigma_{\mathrm{F}}=(\sigma,(c,\pi,\delta,otvk))$,验证者 U_j 验证等式 $\mathrm{PVer}(M,(c,\pi,\delta,otvk),\{PK_i,PK_j\},APK)=1$ 和 $\delta.\mathrm{Ver}(pk_i,\sigma,otvk)=1$ 是否成立. 若任一等式不成立,则拒绝,否则接受签名.

Res:当收到来自 U_j 的消息 $\sigma_{\mathrm{P}}=(c,\pi,\delta,otvk)$,并且 U_j 声称 σ_{P} 是由 U_i 生成的,TTP 首先调用 PVer 算法验证 σ_{P} 的有效性. 如果验证 σ_{P} 无效,则返回$\perp$;否则,计算 $\sigma\leftarrow\xi.\mathrm{Dec}(sk_{\mathrm{TA}},otvk,c)$,验证等式 $\delta.\mathrm{Ver}(pk_i,\sigma,otvk)=1$ 是否成立,若等式成立,则返回 σ 给 U_j,否则返回$\perp$.

上述 AOFE 方案构造方法采用了选择密钥模型,没有考虑真实应用场景中用户密钥的可信性问题. 也就是说,TTP 和用户密钥均为自我生成,没有一个密钥认证权威(PKI 体制的 CA,或 IBC 体制的 PKG)对密钥进行授信,这样的密钥无法应用于真实的网络环境. 本文

研究基于 IBC 体制的 AOFE 方案,在上述方案的基础上,提出 ID-AOFE 方案框架.

ID-AOFE 方案由 Setup、$\mathrm{KGen}^{\mathrm{TTP}}$、$\mathrm{KGen}^{\mathrm{User}}$、PSig、PVer、Sig、Ver 和 Res,8 个算法组成,有密钥生成中心 PKG、off-line TTP 和用户三类角色.

Setup:输入安全参数 κ,PKG 产生系统公开参数 PM 和主密钥 msk.

$\mathrm{KGen}^{\mathrm{TTP}}$:首先提交 off-line TTP 的身份 ID_{TA},PKG 产生仲裁者的公私钥对$(pk_{\mathrm{TA}},sk_{\mathrm{TA}})$,并通过秘密信道返回给他,其中,$pk_{\mathrm{TA}}=ID_{\mathrm{TA}}$;然后,TTP 运行 $\Pi.\mathrm{Kg}(1^{\kappa})$算法产生公共参考串 crs 及其对应的抽取密钥 sk_{Tc},发布 $APK=(pk_{\mathrm{TA}},crs)$作为其完整公钥,秘密保存其私钥 $ASK=(sk_{\mathrm{TA}},sk_{\mathrm{Tc}})$.

$\mathrm{KGen}^{\mathrm{User}}$:提交用户身份 ID_i,PKG 产生用户公私钥对(pk_i,sk_i),并通过秘密信道返回给用户,其中,$pk_i=ID_i$.

Psig 算法与 Huang-AOFE 方案类似,主要的不同包括:删掉了第(3)步,不再使用基于标签的加密算法对 σ 进行加密;第(4)步则采用 NIWI 算法替换零知识证明.

其它算法与 AOFE 方案类似,这里不再赘述,方案的具体构造方法参考本文第 3 节.

2.2.2　ID-AOFE 方案安全模型

文献[17]定义了 AOFE 方案的选择密钥安全模型,在此基础上,结合 Paterson 等人[25]提出的标准模型下的选择身份安全模型,本文定义 ID-AOFE 方案的选择身份安全模型,简要描述如下.

首先定义 ID-AOFE 方案的主要安全属性,包括:签名者身份不可区分性、部分签名不可伪造性、完整签名完美隐藏性、完整签名不可伪造性,分别与文献[17]中 2.1 节定义的安全属性相对应.

签名者身份不可区分性:是指给定一个与(U_i,U_j)相关的有效部分签名 σ_{P},在没有取得有效的完整签名的情况下,验证者 U_j不能向任何其他用户证明 σ_{P}是由 U_i产生的. 签名者身份不可区分性是 AOFE 方案区别于普通 OFE 方案的关键属性,即,防止部分签名的接收者利用部分签名取得不公平的优势. 例如:U_j利用 σ_{P}向 U_i的其他竞争者证明 U_i对某项事实做出了承诺,以期争取有利于自身的条件.

部分签名不可伪造性:是指签名者 U_i不能成功伪造一个有效的部分签名,使得(即使在仲裁者的帮助下)诚实的验证者 U_j不能提取有效的完整签名. 也就是说,只要 σ_{P}是 U_i产生的一个可验证有效的部分签名,那么,在仲裁者的帮助下,诚实的 U_j一定能提取有效的完整签名.

完整签名完美隐藏性:是指在没有签名者和仲裁者的帮助下,验证者不能从部分签名中提取出有效的完整签名.

完整签名不可伪造性:是指给定(U_i,U_j,M),在没有签名者 U_i参与的情况下,任何其他实体(包括 TTP 和 U_j)不能成功伪造 U_i对 M 的有效完整签名.

此外,文献[17]还定义了签名不可区分属性(resolution ambiguity),是指在理想情况下,NIWI 算法(Huang-AOFE 方案采用基于标签的加密算法)的输入(包含原签名)与 Res 算法的输出(NIWI 算法提取的签名)在计算上不可区分. 根据文献[18]的分析和证明 NIWI 算法满足正确性,其输入和输出是完全一致的,在计算上不可区分. 可见,签名不可区分性属于算法正确性而非安全性,因此,本文安全模型不包含该属性.

下面,我们给出 ID-AOFE 方案的选择身份安全模型,定义敌手 $\mathrm{A}_i\in\{\mathrm{A}_1,\mathrm{A}_2,\mathrm{A}_3,\mathrm{A}_4\}$与模拟器 C 之间的游戏($\mathrm{A}_i$分别描述 4 种安全属性模拟游戏中的敌手).

C 首先构造模拟环境,然后模拟 ID-AOFE 方案的各算法对 A_i的询问做出应答,并给出一个问题挑战;A_i自适应地提交多项式时间有界的询问,最后,对 C 给出的挑战做出应答. 以签名者身份不可区分性为例,模拟过程如下.

C 构造模拟环境:

$PM\leftarrow\mathrm{Setup}\ (1^{\kappa})$;

$(APK,ASK)\leftarrow\mathrm{KGen}^{\mathrm{TTP}}(1^{\kappa})$;

$(pk_{ID},sk_{ID})\leftarrow\mathrm{KGen}^{\mathrm{User}}(PM)$.

A 选择挑战者身份(ID_i^*,ID_j^*),并提交询问:

$\sigma_{\mathrm{P}}\leftarrow\mathrm{Psig}(ID_i,ID_j,M)$;

$\sigma_{\mathrm{F}}\leftarrow\mathrm{Sig}(ID_i,ID_j,M)$;

$\sigma_{\mathrm{F}}\leftarrow\mathrm{Res}(ID_i,ID_j,\sigma_{i,\mathrm{P}},\sigma_{j,\mathrm{F}})$.

挑战:

$b\leftarrow_{\mathrm{R}}\{0,1\}$;

$$\sigma_{\mathrm{P}}^{*}\leftarrow\begin{cases}\mathrm{Psig}(ID_i^*,ID_j^*,M^*),\text{if } b=0\\ \mathrm{Psig}(ID_j^*,ID_i^*,M^*),\text{if } b=1\end{cases}$$

A 输出 $b'\in(0,1)$,如果 $b'=b$ 则赢得游戏.

在模拟过程中,如果 A 没有提交 $\mathrm{Psig}(ID_i^*,ID_j^*,M^*)$询问,或者 A 提交了 $\mathrm{Res}(ID_i^*,ID_j^*,\sigma_{\mathrm{P}}^*,\#)$询问,则模拟失败.

如果不存在多项式时间敌手 A 能赢得上述游戏,那么,ID-AOFE 方案在选择身份模型下满足签名者身份不可区分性.

其它安全属性模拟过程与上述过程类似,详细证明过程见本文 4.2 节.

定义 1　如果 ID-AOFE 方案在选择身份模型下满足签名者身份不可区分性、部分签名不可伪造性、完整签名完美隐藏性、完整签名不可伪造性,那么,ID-AOFE

方案具有交换公平性.

3 ID-AOFE 方案

3.1 密码学原语

本节简要介绍本文方案所采用的密码学原语,包括 IBS、OTS 和 NIWI 方案.

给定系统公开参数 $PM=(G_1,G_2,e,g,g_1,g_2,Q,u',\boldsymbol{U},m',\boldsymbol{M},H_1,H_2,H_3,F,F')$. PM 由 Setup 算法生成,其中,$e:G_1\times G_1\to G_2$ 为满足定义的双线性映射,g 是 G_1 的生成元;$\alpha\in\mathbb{Z}_p$ 和 $g_2\in G_1$ 由 PKG 随机选择,$g_1=g^{\alpha}$,$Q=e(g_1,g_2)$,(g_1,g_2,Q) 为 PKG 公钥,主密钥为 g_2^{α};$(u',m')\in G_1^2$,向量 $\boldsymbol{U}=(u_i)$ 和 $\boldsymbol{M}=(m_j)$ 由 PKG 随机选择,长度分别为 n_u 和 n_m 且满足 $(u_i,m_j)\in G_1^2$;$H_1:\{0,1\}^*\to\{0,1\}^{n_u}$,$H_2:\{0,1\}^*\to\{0,1\}^{n_m}$ 和 $H_3:\{0,1\}^*\to\mathbb{Z}_p$ 为密码 Hash 函数,H_1 和 H_2 分别用于将用户身份和待签名消息映射到大小为 n_u 位和 n_m 位的消息空间;$F(ID)=(u'\prod_{d\in\mu_{ID}}u_d)$ 和 $F'(M)=(m'\prod_{j\in\varpi_M}m_j)$ 将身份 ID 和消息 M 分别映射到 G_1 上的一个随机成员,$\mu_{ID}\subseteq\{1,\ldots,n_u\}$ 表示 $H_1(ID)$ 中比特值等于 1 的位置 d 的集合,$\varpi_M\subseteq\{1,\ldots,n_m\}$ 表示 $H_2(M)$ 中比特值等于 1 的位置 j 的集合.

3.1.1 基于身份的签名方案

本文采用 Paterson 等人[25]提出的标准模型下的 IBS 方案(记为 P-IBS). 自提出以来,P-IBS 方案得到了广泛的研究和应用. 基于 P-IBS 方案,已提出大量扩展的密码方案,包括标准模型下的基于身份认证密钥协商方案、群签名方案、代理签名方案等等. P-IBS 方案简要描述如下.

P-IBS. Sig(PM,sk_{ID},M):输入公开参数 PM、签名密钥 $sk_{ID}=(sk_{ID,1},sk_{ID,2})$(密钥生成算法见本文 3.2 节)和待签名消息 M,随机选择 $s\in\mathbb{Z}_p$,计算 $\sigma_1=sk_{ID,1}\cdot(F'(M))^s$,$\sigma_2=g^s$,令 $\sigma_3=sk_{ID,2}$,则签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$.

P-IBS. Ver(PM,ID,σ,M):输入公开参数 PM、签名者身份 ID、签名 σ 和消息 M,验证等式 $e(\sigma_1,g)=Q\cdot e(F(ID),\sigma_3)\cdot e(F'(M),\sigma_2)$ 是否成立,若等式成立则接受签名,否则拒绝.

3.1.2 一次签名方案

本文采用 Boneh 等人[26]提出的标准模型下的短签名方案(记为 B-OTS). B-OTS 方案签名消息短、计算开销低.

B-OTS. Sig$(PM,otsk,M)$:输入公开参数 PM、签名密钥 $otsk=x\in\mathbb{Z}_p$ 和待签名消息 M,令 $h=H_3(M)$,计算签名 $\delta=g^{\frac{1}{x+h}}$.

B-OTS. Ver$(PM,otvk,\delta,M)$:输入公开参数 PM、公钥 $otvk=g^x$、签名 δ 和待签名消息 M,令 $h=H_3(M)$,验证等式 $e(\delta,g^x\cdot g^h)=e(g,g)$ 成立则接受该签名,否则拒绝.

3.1.3 非交互证据不可区分性证明方案

Groth 等人[18]提出一种标准模型下的非交互证明系统,能实现基于双线性映射群的证据不可区分证明和零知识证明. 我们采用 G-NIWI 方案提供证据的不可区分证明和对完整签名的隐藏. G-NIWI 方案实现了在当前密码学领域已得到应用的各类双线性映射群上的非交互证明,实现了群上的双线对运算、标量乘法运算以及整数域上的二次方程,同时还能实现表达式的逻辑(与/或)运算. G-NIWI 方案包含三个算法:Π. Prv,证明产生算法,生成关于隐藏证据 σ 的不可区分证明 π;Π. Ver,验证算法,验证 π 是否成立;Π. Open,提取算法,利用提取密钥 sk_{Tc} 从 π 中提取隐藏的证据 σ.

G-NIWI 证明系统比较复杂,限于论文篇幅,本文不作详述. 本文仅涉及线性对积等式 $\boldsymbol{a}\cdot\boldsymbol{\sigma}=t_T$ 的不可区分证明,下面就本文采用的具体算法做简要阐述. 其中,$\boldsymbol{a}:=(a_1,a_2,\cdots,a_n)\in G_1^n$ 为 n 个非隐藏证据的矢量,$\boldsymbol{\sigma}:=(\sigma_1,\sigma_2,\cdots,\sigma_n)\in G_1^n$ 为 n 个隐藏证据的矢量,$\boldsymbol{a}\cdot\boldsymbol{\sigma}=\prod_{i=1}^{n}e(a_i,\sigma_i)=t_T\in G_2$.

注:文献[18]中的叙述采用加法群和加法运算符,本文则采用乘法群和乘法运算符.

Soundness string:$\boldsymbol{u}:=(u_1,u_2,u_3)$,$u_1=(g^{\rho},\mathrm{O},g)$,$u_2=(\mathrm{O},g^{\lambda},g)$,$u_3=u_1^{r}u_2^{s}=(g^{r\rho},g^{s\lambda},g^{r+s})$,令 O 表示群 G_1 的幺元,$\rho,\lambda\in\mathbb{Z}_p^*$,$r,s\in\mathbb{Z}_p$. $\boldsymbol{u}$ 用于隐藏证据的承诺,$sk_{\mathrm{Tc}}=(\rho,\lambda)$ 为提取密钥.

Witness-indistinguishability string:$\boldsymbol{v}:=(v_1,v_2,v_3)$,$v_1=u_1,v_2=u_2,v_3=u_3\cdot(\mathrm{O},\mathrm{O},g^{-1})=(g^{r\rho},g^{s\lambda},g^{r+s-1})$. $\boldsymbol{v}$ 用于证据不可区分证明.

Π. Prv:首先计算对隐藏证据 $\sigma_i,i\in(1,\cdots,n)$ 的承诺 $d_i=\iota(\sigma_i)\cdot\zeta_i\circ\boldsymbol{u}$. 其中,$\iota(\sigma_i):=(\mathrm{O},\mathrm{O},\sigma_i)$,$\zeta_i=(\zeta_{i,1},\zeta_{i,2},\zeta_{i,3})$ 从 $\mathbb{Z}_p$ 中随机选择,$\zeta_i\circ\boldsymbol{u}=\prod_{j=1}^{3}u_j^{\zeta_{i,j}}$. 然后计算 $\pi_i=\prod_{j=1}^{3}a_i^{\zeta_{i,j}},i\in(1,\cdots,n)$,令 $\boldsymbol{\pi}=(\pi_1,\cdots,\pi_n)$,$\boldsymbol{d}:=(d_1,d_2,\cdots,d_n)$,输出证明 $(\boldsymbol{d},\boldsymbol{\pi})$.

Π. Ver:对于等式 $\boldsymbol{a}\cdot\boldsymbol{\sigma}=t_T$,及其证明 $(\boldsymbol{d},\boldsymbol{\pi})$,验证等式 $\iota(\boldsymbol{a})\bullet\boldsymbol{d}=\iota_T(t_T)\cdot\iota(\boldsymbol{\pi})\bullet\boldsymbol{v}$ 是否成立,若等式成立则接受,否则拒绝. 其中,函数 $\iota_T(t_T):=\begin{pmatrix}1&1&1\\1&1&1\\1&1&t_T\end{pmatrix}$,运算符 $\bullet:G_1^3\times G_1^3\to G_2^9$,即

$$\boldsymbol{x}\bullet\boldsymbol{y}:=\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}\bullet\begin{pmatrix}y_1\\y_2\\y_3\end{pmatrix}=\begin{pmatrix}e(x_1,y_1)&e(x_1,y_2)&e(x_1,y_3)\\e(x_2,y_1)&e(x_2,y_2)&e(x_2,y_3)\\e(x_3,y_1)&e(x_3,y_2)&e(x_3,y_3)\end{pmatrix}.$$

Π. Open:令承诺 $d_i:=(d_{i,1},d_{i,2},d_{i,3})\in G_1^3$,抽取密

钥 $sk_{\mathrm{Tc}}=(\rho,\lambda)$,计算 $\ell(d_i):=d_{i,3}d_{i,1}^{-1/\rho}d_{i,2}^{-1/\lambda}=\sigma_i$,输出隐藏证据 $\boldsymbol{\sigma}:=(\sigma_1,\sigma_2,\cdots,\sigma_n)$.

3.2　ID-AOFE 方案提出

基于 P-IBS 方案、B-OTS 方案和 G-NIWI 方案,提出一种标准模型下的 ID-AOFE 方案,具体描述如下.

Setup:输入安全参数 κ,PKG 产生系统公开参数 $PM=(G_1,G_2,e,g,g_1,g_2,Q,u',\boldsymbol{U},m',\boldsymbol{M},H_1,H_2,H_3,F,F')$ 和主密钥 $msk=g_2^{\alpha}$.

$\mathrm{KGen}^{\mathrm{TTP}}$:仲裁者 TTP 提交其身份 ID_{TA} 给 PKG,PKG 产生 TTP 的公私钥对 $(pk_{\mathrm{TA}}=ID_{\mathrm{TA}},sk_{\mathrm{TA}}=(sk_{\mathrm{TA},1},sk_{\mathrm{TA},2})=(g_2^{\alpha}\cdot(F(ID_{\mathrm{TA}}))^{r_{\mathrm{TA}}},g^{r_{\mathrm{TA}}}))$,并通过秘密信道返回给 TTP. 其中,$r_{\mathrm{TA}}\in\mathbb{Z}_p$ 由 PKG 随机选择. 收到 sk_{TA} 后,TTP 计算 $e(sk_{\mathrm{TA},1},g)=Q\cdot e(F(ID_{\mathrm{TA}}),sk_{\mathrm{TA},2})$ 是否相等来验证私钥的正确性. 如果验证等式成立,则接受 sk_{TA} 作为自己的私钥,否则重新申请私钥. TTP 运行 $\Pi.\mathrm{Kg}(1^{\kappa})$ 算法产生公共参考串 $crs=(F,H,X,Y,Z,X',Y',Z',\theta)$,及抽取密钥 sk_{Tc},其中,$(F,H,X,Y,Z,X',Y',Z')\in G_1^8$,$\theta\leftarrow\text{P-IBS.Sig}(PM,sk_{\mathrm{TA}},F\parallel H\parallel X\parallel Y\parallel Z\parallel X'\parallel Y'\parallel Z')$ 为 TTP 对 crs 的签名. TTP 发布 $APK=(pk_{\mathrm{TA}},crs)$ 作为他的完整公钥,秘密保存其私钥 $ASK=(sk_{\mathrm{TA}},sk_{\mathrm{Tc}})$.

$\mathrm{KGen}^{\mathrm{User}}$:提交用户 U_i 的身份 ID_i,PKG 产生 U_i 的私钥 $sk_i=(sk_{i,1},sk_{i,2})=(g_2^{\alpha}\cdot(F(ID_i))^{r_i},g^{r_i})$,公钥为 $pk_i=ID_i$,通过秘密信道返回 sk_i 给 U_i. 其中,$r_i\in\mathbb{Z}_p$ 由 PKG 随机选择. U_i 通过计算等式 $e(sk_{i,1},g)=Q\times e(F(ID_i),sk_{i,2})$ 是否相等来验证私钥的正确性.

Psig:给定待签名消息 M 和签名验证者 U_j,签名者 U_i 按照下面的方法产生部分签名.

(1)随机选择 $x\in\mathbb{Z}_p$,令 $otsk=x$,$otvk=g^x$.

(2)产生 $otvk$ 的 P-IBS 签名 $\sigma_i\leftarrow\text{P-IBS.Sig}(PM,sk_i,otvk)$,即 $\sigma_i=(\sigma_{i,1},\sigma_{i,2},\sigma_{i,3})=(sk_{i,1}(F'(H_2(otvk)))^{s_i},g^{s_i},sk_{i,2})$. 其中,$s_i\in\mathbb{Z}_p$ 由 U_i 随机选择.

(3)采用 G-NIWI 算法产生证据 $(\sigma_{i,1},\sigma_{i,3})$ 的不可区分证明 $\pi\leftarrow\Pi.\mathrm{Prv}(PM,APK,(Q_i,Q_j,Q_v,\sigma_{i,2}),(\sigma_{i,1},\sigma_{i,3}))$. 其中,$Q_i=F(ID_i)$,$Q_j=F(ID_j)$,$Q_v=F'(H_2(otvk))$. π 证明存在(隐藏证据)$(\sigma_{i,1},\sigma_{i,3})$ 使得下列表达式成立.

$$e(\sigma_{i,1},g)=Q\cdot e(Q_i,\sigma_{i,3})\cdot e(Q_v,\sigma_{i,2})\ \vee$$
$$e(\sigma_{i,1},g)=Q\cdot e(Q_j,\sigma_{i,3})\cdot e(Q_v,\sigma_{i,2})$$

(4)采用 B-OTS 算法产生一次签名 $\delta\leftarrow\text{B-OTS.Sig}(PM,otsk,\pi\parallel M\parallel ID_i\parallel ID_j\parallel\sigma_{i,2}\parallel T)$. 其中,$T$ 为时间参数.

输出部分签名 $\sigma_{i,\mathrm{P}}=(\pi,\delta,\sigma_{i,2},otvk,T)$.

Pver:收到 U_i 对消息 M 的部分签名 $\sigma_{i,\mathrm{P}}$,验证者验证等式 $\text{OTS.Ver}(PM,otvk,\delta,\pi\parallel M\parallel ID_i\parallel ID_j\parallel\sigma_{i,2}\parallel T)=1$ 和 $\Pi.\text{Ver}(PM,APK,(g,Q,Q_i,Q_j,Q_v,\sigma_{i,2}),\pi)=1$ 是否成立,若验证通过则接受部分签名,否则拒绝.

Sig:给定待签名消息 M 和签名验证者 U_j,签名者 U_i 计算 $(\sigma_i,\sigma_{i,\mathrm{P}})\leftarrow\text{Psig}(PM,APK,sk_i,ID_i,ID_j,M)$,输出完整签名 $\sigma_{i,\mathrm{F}}=(\sigma_i,\sigma_{i,\mathrm{P}})$.

Ver:收到 U_i 对消息 M 的完整签名 $\sigma_{i,\mathrm{F}}$,验证者 U_j 验证 $\text{PVer}(PM,APK,ID_i,ID_j,M,\sigma_{i,\mathrm{P}})=1$ 和 $\text{P-IBS.Ver}(PM,ID_i,\sigma_i,otvk)=1$ 是否成立,若验证通过则接受签名,否则拒绝.

Res:当收到来自 U_j 的消息 $(\sigma_{i,\mathrm{P}},\sigma_{j,\mathrm{F}})$,并且 U_j 声称 $\sigma_{i,\mathrm{P}}$ 是由 U_i 生成的,仲裁者首先检查当前时间是否超过 U_i 设置的时间 T,若时间超过则返回 $\perp$;否则调用算法 PVer 和 Ver 分别验证 $\sigma_{i,\mathrm{P}}$ 和 $\sigma_{j,\mathrm{F}}$ 的有效性. 如果验证 $\sigma_{i,\mathrm{P}}$ 或 $\sigma_{j,\mathrm{F}}$ 无效,则返回 $\perp$;否则,抽取 $\sigma_i\leftarrow\Pi.\text{Open}(PM,APK,sk_{Tc},\pi)$,验证签名 $\text{P-IBS.Ver}(PM,ID_i,\sigma_i,otvk)=1$ 成立,则返回 σ_i 给 U_j,否则返回 $\perp$.

3.3　ID-AOFE 方案消息交互模型

本节讨论 ID-AOFE 方案的消息交互模型,包含 7 个步骤,分为正常签名交换和争端解决两个阶段,见图 1.

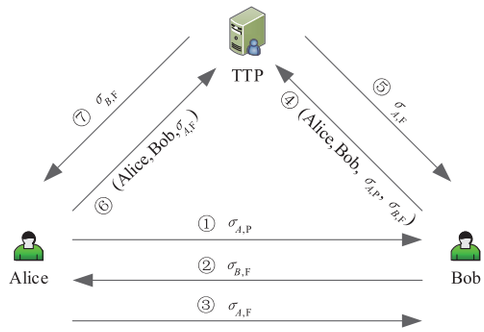

图1　ID-AOFE方案的消息交互模型

第一个阶段是正常签名交换,由步骤① ~ ③组成. 首先由交换的发起者 Alice 按照 Sig 算法产生关于消息 M 的签名 $\sigma_{A,\mathrm{F}}=(\sigma_A,\sigma_{A,\mathrm{P}})$,并将部分签名 $\sigma_{A,\mathrm{P}}$ 发送给签名的接收者 Bob. 收到 $\sigma_{A,\mathrm{P}}$ 后,Bob 调用 PVer 算法验证部分签名,若验证不正确则终止,否则调用 Sig 算法产生对 M 的完整签名 $\sigma_{B,\mathrm{F}}$,并发送给 Alice. 收到 $\sigma_{B,\mathrm{F}}$ 后,Alice 将完整签名 $\sigma_{A,\mathrm{F}}$ 发送给 Bob. 若上述步骤正常完成,协议成功完成,否则进入争端解决阶段.

争端解决分为以下两个独立的部分,分别针对 Alice 和 Bob 发起的争端请求.

第一部分由步骤④和⑤组成,用于 TTP 响应 Bob 发起的争端请求. 当第②步,Bob 发送完整签名 $\sigma_{B,\mathrm{F}}$ 后,未收到 Alice 的完整签名 $\sigma_{A,\mathrm{F}}$,则进入第④步,请求争端解决. TTP 调用 Res 算法进行争端处理. 注意,本文引入时间参数 T(见 Psig 算法),要求第④步在 T 时间之前完成,即,TTP 验证当前时间是否超过参数 T 所规定的时间,若超过,则无论 $\sigma_{A,\mathrm{P}}$ 是否验证正确都返回 $\perp$. 因此,T 应当设置合理,否则 Bob 可以退出交换. 见图 2.

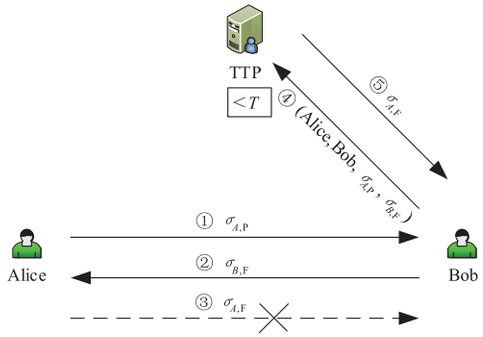

图2 Bob发起的争端请求

第二部分由步骤⑥和⑦组成,用于 TTP 响应 Alice 发起的争端请求. 当第①步,Alice 发送部分签名 $\sigma_{A,P}$ 后,未收到 Bob 的完整签名 $\sigma_{B,F}$,则进入第⑥步,请求争端解决. TTP 首先检查他自己的数据库,查找是否存在由 Bob 发起的争端请求与该请求匹配,并且最终返回了 $\sigma_{A,F}$给 Bob. 若存在记录(Alice,Bob,$\sigma_{A,F}$,$\sigma_{B,F}$)则返回 $\sigma_{B,F}$给 Alice,否则返回⊥. 注意,Alice 的争端请求应当在她设定的时间 T 之后,确保 Bob 已经完成了他的争端请求. 见图 3.

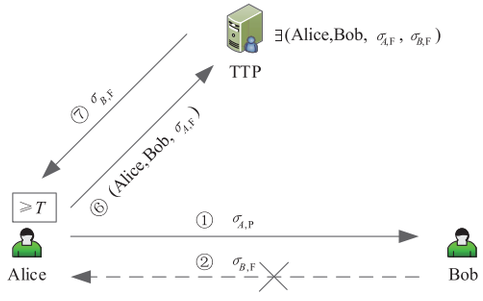

图3 Alice发起的争端请求

注意,作为 ID-AOFE 交换的接收方,Bob 无需提供关于部分签名的不可区分证明. 为了降低方案的计算量,可以简化 Bob 的签名计算过程,取消部分签名计算(包括复杂的证据不可区分证明),而直接调用 P-IBS 签名算法产生对 M 的签名 $\sigma_{B,F}\leftarrow$P-IBS. Sig (PM,sk_B,$M \parallel ID_A \parallel ID_B$).

4 ID-AOFE 方案分析

4.1 ID-AOFE 方案的有效性分析

由图 1 可知,在正常情况下,Alice 和 Bob 都诚实地按照协议执行,且信道可靠(未遭受恶意攻击),经过步骤①~③,交换双方均能获得对方对消息 M 的完整签名($\sigma_{A,F}$,$\sigma_{B,F}$),且签名的有效性和不可伪造性由 P-IBS、B-OTS 和 G-NIWI 算法保证.

如果交换过程出现异常,例如交换一方有意欺骗或敌手恶意攻击,将进入争端解决阶段. 总结起来,争端解决可以分为两类情形:第一类是 Alice 向 Bob 发送了部分签名 $\sigma_{A,P}$后没有收到 Bob 返回的完整签名 $\sigma_{B,F}$,此时由 Alice 发起争端请求(见图 3);第二类是 Bob 收到 Alice 的部分签名 $\sigma_{A,P}$后向 Alice 发送了完整签名 $\sigma_{B,F}$,但是未收到 Alice 的完整签名 $\sigma_{A,F}$而发起争端请求(见图 2). 针对 Bob 的争端请求,TTP 首先检查请求的时间是否符合要求($<T$),然后验证 Alice 的部分签名和 Bob 的完整签名,若所有验证有效,则从 $\sigma_{A,P}$中抽取 Alice 的完整签名 $\sigma_{A,F}=(\sigma_A,\sigma_{A,P})$返回给 Bob,并存储相应的争端解决记录(Alice,Bob,$\sigma_{A,F}$,$\sigma_{B,F}$). 对于 Alice 的争端请求,成功与否取决于 Bob 是否成功地完成了争端解决并获得了有效的 $\sigma_{A,F}$,因此,Alice 的争端请求通常在 Bob 之后($\geqslant T$). 如果 Bob 由 TTP 处成功获得 $\sigma_{A,F}$,那么 Alice 也能获得有效的 $\sigma_{B,F}$;否则 Alice 不能获得有效的 $\sigma_{B,F}$,此时 Alice 未取得 Bob 的任何信息,而 Bob 仅获得 Alice 的部分签名. Bob 虽获得了 Alice 的部分签名,但是 $\sigma_{A,P}$中隐含的 Alice 对签名的承诺 σ_A被 TTP 的公钥加密,并且 G-NIWI 算法证明相同的承诺也可能是由 Bob 自己产生的,这就避免了 Bob 利用 Alice 的部分签名谋取不正当利益,破坏公平性. 同样的,争端解决的有效性由 P-IBS、B-OTS 和 G-NIWI 算法保证.

值得注意的是时间参数 T 的设置. 需要考虑一种极端的情况:当恶意的 Alice 收到 Bob 的完整签名后(步骤②完成),完全阻断 Bob 与 TTP 间的通信,使得 Bob 不能成功完成争端请求. 在真实网络环境下,要想长时间地阻断 Bob 与 TTP 间的通信是不可能的,因此,在实际应用中,T 设置为一个合理的时间值.

综上所述,本文提出的 ID-AOFE 方案具有有效性.

4.2 ID-AOFE 方案的安全性分析

定理 1 如果 CDH、SDH 和 DLIN 假设成立,那么本文提出的 ID-AOFE 方案在标准模型和选择身份模型下满足交换公平性.

定理 1 由引理 1~引理 5 推导可得.

引理 1 如果 CDH、SDH 和 DLIN 假设成立,那么 P-IBS 和 B-OTS 方案在标准模型下满足签名不可伪造性,G-NIWI 方案在标准模型下实现了证据可提取、正确性(Perfect Soundness)和证据不可区分性(Composable witness indistinguishability).

引理 1 分别在文献[18,25,26]中得到证明,本文不再赘述.

引理 2 如果 P-IBS、B-OTS 和 G-NIWI 方案在标准模型下是安全的,那么本文提出的 ID-AOFE 方案在标准模型和选择身份模型下实现了签名者不可区分性.

证明 签名者不可区分性由 G-NIWI 算法保证. 假设 P-IBS 和 B-OTS 算法具有不可伪造性,如果敌手 A 能区分证明 π 中隐藏的证据 σ_i是由某个具体的签名者

ID_i所生成,那么可以构造一个区分器 D 攻破 G-NIWI 算法的证据不可区分性,下面描述模拟过程.

输入安全参数 κ,模拟器 C 构造模拟环境,输出公开参数 PM,并构造 G-NIWI 算法证据不可区分性(文献[18]的定义 4)环境(G,K,S,P,V):

$$\Pr[(gk,sk)\leftarrow G(1^\kappa);crs\leftarrow K(gk,sk):A(gk,crs)=1]\approx \Pr[(gk,sk)\leftarrow G(1^\kappa);crs'\leftarrow S(gk,sk):A(gk,crs')=1].$$

其中,K 是真实环境下的仲裁者 $KGen^{TTP}$算法,而 S 是模拟环境下的仲裁者 $KGen^{TTP}$算法,P 和 V 分别是证明产生算法和验证算法. 上面的表达式表明,对于敌手 A 来说,K 和 S 的输出在概率分布上不可区分.

区分器 D 与敌手 A 进行如下交互. A 选择用于挑战的签名者身份 ID_i^* 和验证者身份 ID_j^*,自适应地提交多项式时间有界的询问,D(在 C 的帮助下,比如用户私钥的取得)模拟相应算法做出应答.

$Psig(ID_i,ID_j,M)$ 询问. ID_i为签名者身份,ID_j为验证者身份,M 为待签名消息. D 产生 B-OTS 算法的公私钥对$(otvk,otsk)$,调用 P-IBS 算法生成 $otvk$ 的签名 $\sigma_i\leftarrow$ P-IBS. $Sig(PM,sk_i,otvk)$;询问预言机 $O_{G\text{-}NIWI}$($O_{G\text{-}NIWI}$由模拟器 C 来构造,模拟 G-NIWI 算法输出)取得证据 σ_i的不可区分证明 π;调用 B-OTS 算法生成一次签名 $\delta\leftarrow$ B-OTS. $Sig(PM,otsk,\pi\parallel M\parallel ID_i\parallel ID_j\parallel\sigma_{i,2}\parallel T)$,并返回部分签名 $\sigma_{i,P}=(\pi,\delta,\sigma_{i,2},otvk,T)$作为应答.

$Sig(ID_i,ID_j,M)$ 询问. 执行 $Psig(ID_i,ID_j,M)$ 询问,取得 $\sigma_{i,F}$并返回给 A.

$Res(ID_i,ID_j,\sigma_{i,P},\sigma_{j,F})$ 询问. 根据 Res 算法,如果 $\sigma_{i,P}$是 ID_i的一个有效的部分签名且 $\sigma_{j,F}$是 ID_j的一个有效的完整签名,那么,D 询问 $O_{G\text{-}NIWI}$并输出 ID_i的完整签名 $\sigma_{i,F}$,否则输出$\perp$.

在询问阶段,D 构造一个身份不可区分挑战并从 C 处获得一个 G-NIWI 证据不可区分挑战. D 收到 A 提交的 $Psig(ID_i^*,ID_j^*,M^*)$ 询问,随机选择 B-OTS 算法的公私钥对$(otvk,otsk)$以及一个随机的 $b\in(0,1)$. 如果 $b=0$,D 调用 P-IBS 签名算法生成 $\sigma_i^0\leftarrow$P-IBS. $Sig(PM,sk_i^*,otvk)$,其中,sk_i^* 为 ID_i^* 的私钥;如果 $b=1$,产生 $\sigma_i^1\leftarrow$ P-IBS. $Sig(PM,sk_j^*,otvk)$,其中,sk_j^* 为 ID_j^* 的私钥. D 提交(σ_i^0,σ_i^1)给 C,C 构造 G-NIWI 证据不可区分挑战:随机选择 $c\in(0,1)$,如果 $c=0$,输出 $\pi^c\leftarrow P(gk,crs,s,\sigma_i^c)$,否则输出 $\pi^c\leftarrow$P(gk,crs',s,σ_i^c). 其中,s 为表达式:

$$e(\sigma_{i,1}^c,g)=Q\cdot e(Q_i^*,\sigma_{i,3}^c)\cdot e(Q_v^*,\sigma_{i,2}^c)\vee$$
$$e(\sigma_{i,1}^c,g)=Q\cdot e(Q_j^*,\sigma_{i,3}^c)\cdot e(Q_v^*,\sigma_{i,2}^c),$$
$$Q_i^*=F(ID_i^*),Q_j^*=F(ID_j^*),$$
$$Q_v^*=F'(H_2(otvk)).$$

注意,D 生成 σ_i^0 和 σ_i^1 时需要采用相同的随机数,也就是说,令 $\sigma_i^0=(\sigma_{i,1}^0,\sigma_{i,2}^0,\sigma_{i,3}^0)$,$\sigma_i^1=(\sigma_{i,1}^1,\sigma_{i,2}^1,\sigma_{i,3}^1)$,则 $\sigma_{i,2}^0=\sigma_{i,2}^1$,这是因为 π^c只隐藏了与身份相关的证据$(\sigma_{i,1}^c,\sigma_{i,3}^c)$而没有隐藏 $\sigma_{i,2}^c$. 最后,D 计算一次签名 $\delta\leftarrow$B-OTS. $Sig(PM,otsk,\pi^c\parallel M^*\parallel ID_i^*\parallel ID_j^*\parallel\sigma_{i,2}^b\parallel T)$,并返回部分签名 $\sigma_{c,P}^*=(\pi^c,\delta,\sigma_{i,2}^b,otvk,T)$作为身份不可区分挑战. 从敌手 A 的视角来看,当 $c=0$ 时,$\sigma_{c,P}^*$为 ID_i^* 的一个有效部分签名;而 $c=1$ 时,$\sigma_{c,P}^*$为 ID_j^* 的一个有效部分签名.

询问结束后,A 返回其猜测 $b'\in(0,1)$,D 将 b'作为对 G-NIWI 算法证据不可区分性挑战的应答. 由模拟过程可知,如果 A 成功,则 D 也成功.

在模拟过程中,如果 A 没有提交 $Psig(ID_i^*,ID_j^*,M^*)$询问,或者 A 提交了 $Res(ID_i^*,ID_j^*,\sigma_{c,P}^*,\#)$询问,则模拟失败. 假设 A 提交了 q_p次 Psig 询问和 q_r次 Res 询问,且 A 成功赢得身份不可区分挑战的概率为 ε,那么 D 成功赢得 G-NIWI 证据不可区分挑战的概率为

$$\varepsilon'\geqslant\left(1-\frac{1}{q_p}\right)\left(1-\frac{1}{q_r}\right)\varepsilon.$$

证毕.

引理 3　如果 P-IBS、B-OTS 和 G-NIWI 方案在标准模型下是安全的,那么本文提出的 ID-AOFE 方案在标准模型和选择身份模型下满足部分签名不可伪造性.

证明　部分签名不可伪造性可规约为敌手 A 攻破 G-NIWI 算法的正确性或者 P-IBS 和 B-OTS 算法的不可伪造性.

输入安全参数 κ,模拟器 C 构造模拟环境,输出公开参数 PM. C 与 A 进行如下交互.

A 选择用于挑战的身份 ID_i^* 和 ID_j^*,自适应地提交多项式时间有界的询问 $Psig(ID_i,ID_j,M)$,$Sig(ID_i,ID_j,M)$和 $Res(ID_i,ID_j,\sigma_{i,P},\sigma_{j,F})$,C 模拟相应算法做出应答(应答方法参照引理 2 的证明).

最后,A 输出一个与(ID_i^*,ID_j^*,M^*)相关的伪造的部分签名 $\sigma_{i,P}^*=(\pi^*,\delta^*,\sigma_{i,2}^*,otvk^*,T^*)$.

如果 $\sigma_{i,P}^*$在询问过程中未曾出现过,且 $PVer(PM,APK,ID_i^*,ID_j^*,M^*,\sigma_{i,P}^*)=1$,那么 A 赢得游戏.

显然,A 在三种情况下可赢得游戏:①A 伪造了 ID_i^* 或 ID_j^* 对 $otvk^*$的有效的 P-IBS 签名;②$otvk^*$来自 Psig 询问(也就是说,A 从 C 处取得了 ID_i^* 或 ID_j^* 对 $otvk^*$的 P-IBS 签名),并且 A 伪造了一次签名 $\delta^*\leftarrow$ B-OTS. $Sig(PM,otsk^*,\pi^*\parallel M^*\parallel ID_i^*\parallel ID_j^*\parallel\sigma_{i,2}^*\parallel T^*)$,其中,$otsk^*$为与 $otvk^*$配对的签名密钥(注意,对 A 来说,$otsk^*$未知);③在未取得 ID_i^* 或 ID_j^* 对 $otvk^*$的有效的 P-IBS 签名的情况下,A 随机选择 $\sigma_i^*=(\sigma_{i,1}^*,\sigma_{i,2}^*,\sigma_{i,3}^*)$并伪造了 G-NIWI 证明 π^*,使得 $\Pi.Ver(PM,APK,(g,Q,Q_i^*,Q_j^*,Q_v^*,\sigma_{i,2}^*),\pi^*)=1$.

针对上述三种情况,C 可以构建算法 F 利用 A 分别

攻破 P-IBS 和 B-OTS 算法的不可伪造性,以及 G-NIWI 算法的正确性. 下面以第①种情况为例,说明如何构造算法 F.

在 Psig 询问过程中,F 收到 P-IBS 算法的挑战 (ID_i^*, M^*)或(ID_j^*, M^*). A 输出 $\sigma_{i,\mathrm{P}}^*$后,F 调用 G-NIWI 算法从 $\sigma_{i,\mathrm{P}}^*$中提取 P-IBS 签名 σ_i^* 作为对挑战(ID_i^*, M^*)或(ID_j^*, M^*)的应答. 显然,如果 B-OTS 算法是不可伪造的,且 G-NIWI 算法满足正确性,那么,仅当 $\sigma_{i,\mathrm{P}}^*$是一个有效的部分签名时,σ_i^* 是一个有效的 P-IBS 签名. 假设 A 赢得游戏的概率为 ε,则 F 成功的概率为 $\varepsilon' \geqslant \frac{1}{2}\left(1-\frac{1}{q_{\mathrm{p}}}\right)\left(1-\frac{1}{q_{\mathrm{s}}}\right)\left(1-\frac{1}{q_{\mathrm{r}}}\right)\varepsilon$. 其中,$q_{\mathrm{p}}$和 q_{r}与引理 2 相同,q_{s}是 Sig 询问次数.

证毕.

引理 4 如果 P-IBS、B-OTS 和 G-NIWI 方案在标准模型下是安全的,那么本文提出的 ID-AOFE 方案在标准模型和选择身份模型下实现了完整签名的完美隐藏.

完整签名的完美隐藏属性由 G-NIWI 算法保证,即,如果本文提出的 ID-AOFE 方案不满足完整签名的完美隐藏属性,那么可以构造一个区分器 D 利用敌手 A 攻破 G-NIWI 算法的证据不可区分性. 也就是说,如果敌手 A 从部分签名的挑战 $\sigma_{i,\mathrm{P}}^*$中(在没有原始签名者和 TTP 协助的情况下)成功地提取了有效的完整签名 $\sigma_{i,\mathrm{F}}^* = (\sigma_i^*, \sigma_{i,\mathrm{P}}^*)$,那么,D 可以直接输出 σ_i^* 作为对 G-NIWI 算法的不可区分性挑战 π^* 的回答. 引理 4 的证明过程与引理 2 类似,这里不再详细阐述.

引理 5 如果 P-IBS、B-OTS 和 G-NIWI 方案在标准模型下是安全的,那么本文提出的 ID-AOFE 方案在标准模型和选择身份模型下实现了完整签名的不可伪造性.

证明 完整签名不可伪造性可规约为敌手 A 攻破 P-IBS 或者 B-OTS 算法的不可伪造性.

输入安全参数 κ,模拟器 C 构造模拟环境,输出公开参数 PM. C 与 A 进行如下交互.

A 选择用于挑战的身份 ID_i^* 和 ID_j^*,自适应地提交多项式时间有界的询问 $\mathrm{Sig}(ID_i, ID_j, M)$,$\mathrm{Psig}(ID_i, ID_j, M)$ 和 $\mathrm{Res}(ID_i, ID_j, \sigma_{i,\mathrm{P}}, \sigma_{j,\mathrm{F}})$,C 模拟相应算法做出应答.

$\mathrm{Psig}(ID_i, ID_j, M)$ 询问. 对该询问的应答分为两种情形:①生成 B-OTS 算法的公私钥对$(otvk, otsk)$,询问 P-IBS 预言机输出 $otvk$ 的签名 σ_i,调用 G-NIWI 算法取得证据 σ_i的不可区分证明 π,调用 B-OTS 算法生成一次签名 $\delta \leftarrow \text{B-OTS}.\mathrm{Sig}(PM, otsk, \pi \| M \| ID_i \| ID_j \| \sigma_{i,2} \| T)$;②询问 B-OTS 预言机,获得$(otvk, *)$,调用 P-IBS 算法获得 $otvk$ 的签名 $\sigma_i \leftarrow \text{P-IBS}.\mathrm{Sig}(PM, sk_i, otvk)$,调用 G-NIWI 算法取得证据 σ_i的不可区分证明 π,询问 B-OTS 预言机生成一次签名 δ. 最后,输出部分签名 $\sigma_{i,\mathrm{P}} = (\pi, \delta, \sigma_{i,2}, otvk, T)$作为应答.

$\mathrm{Sig}(ID_i, ID_j, M)$ 询问. 执行 $\mathrm{Psig}(ID_i, ID_j, M)$ 询问,取得 $\sigma_{i,\mathrm{F}}$并返回给 A.

$\mathrm{Res}(ID_i, ID_j, \sigma_{i,\mathrm{P}}, \sigma_{j,\mathrm{F}})$ 询问. 如果 $\sigma_{i,\mathrm{P}}$是一个有效的部分签名,则调用 G-NIWI 算法提取 $\sigma_{i,\mathrm{P}}$中的隐藏证据 σ_i,并返回 $\sigma_{i,\mathrm{F}} = (\sigma_i, \sigma_{i,\mathrm{P}})$给 A.

询问结束后,A 输出与(ID_i^*, ID_j^*, M^*)相关的伪造的完整签名 $\sigma_{i,\mathrm{F}}^* = (\sigma_i^*, \sigma_{i,\mathrm{P}}^*) = ((\sigma_{i,1}^*, \sigma_{i,2}^*, \sigma_{i,3}^*), (\pi^*, \delta^*, \sigma_{i,2}^*, otvk^*, T^*))$.

如果 $\sigma_{i,\mathrm{F}}^*$在询问过程中未曾出现过,且 $\mathrm{Ver}(ID_i^*, ID_j^*, M^*, \sigma_{i,\mathrm{F}}^*) = 1$,那么 A 赢得游戏.

下面,分两种情形分析 A 成功的概率. 一是 Psig 询问中的第①种情形,此种情形可规约为攻破 P-IBS 算法的不可伪造性;二是 Psig 询问中的第②种情形,此种情形可规约为攻破 B-OTS 算法的不可伪造性. 也就是说,A 若成功,要么伪造了 P-IBS 签名 $\sigma_i^* \leftarrow \text{P-IBS}.\mathrm{Sig}(PM, sk_i^*, otvk^*)$(这里的 $otvk^*$ 没有在 Psig 询问中出现过),要么伪造了 B-OTS 签名 $\delta^* \leftarrow \text{B-OTS}.\mathrm{Sig}(PM, otsk^*, \pi^* \| M^* \| ID_i^* \| ID_j^* \| \sigma_{i,2}^* \| T^*)$(其中,$otsk^*$ 对 A 来说未知,且与之对应的 $otvk^*$ 在 Psig 询问中出现过).

针对上述两种情形,C 构建算法 F 利用 A 分别攻破 P-IBS 和 B-OTS 算法的不可伪造性,下面以第①类情形为例,说明算法 F 的构建过程.

在 Psig 询问的第①类情形中,F 从 P-IBS 预言机收到 P-IBS 算法的挑战$(ID_i^*, otvk^*)$. A 输出 $\sigma_{i,\mathrm{F}}^* = (\sigma_i^*, \sigma_{i,\mathrm{P}}^*)$后,F 直接输出 σ_i^* 作为对 P-IBS 挑战的应答. 假设 A 赢得游戏的概率为 ε,则 F 成功的概率为 $\varepsilon' \geqslant \left(1-\frac{1}{q_{\mathrm{p}}}\right)\left(1-\frac{1}{q_{\mathrm{s}}}\right)\left(1-\frac{1}{q_{\mathrm{r}}}\right)\varepsilon$. 其中,$q_{\mathrm{p}}$,$q_{\mathrm{s}}$ 和 q_{r} 与前面相同.

证毕.

4.3 对比分析

根据相关文献,Zhang 等人[27]提出一种标准模型下可证明安全的 ID-OFE 方案,Youn 等人[28]提出一种基于 RSA 签名的 ID-OFE 方案. 这两种方案均采用可验证加密签名技术产生部分签名,由于没有考虑签名者身份不可区分性,恶意的接收者可以利用部分签名取得不公平的优势,破坏交换的公平性. 在隐私保护方面,Huang-AOFE 方案与本文方案能够对签名信息进行隐藏,但是不能对用户身份进行隐藏,具有一定的隐私保护性,而 Wang 等人[19]、Huang 等人[20]和 Guo 等人[21]在 AOFE 方案的基础上进行增强,重点加强对用户隐私的保护,实现用户身份的隐藏,在一些特定的场景下具有一定的应用价值,但是显著增加了方案的开销. 此外,

Loh 等人[29]提出了一种 Accountable OFE 方案框架模型和构造实例. Accountable OFE 方案重点关注“resolution ambiguous”属性(即签名不可区分属性)和“Accountability”属性,指出原始签名和争端解决阶段输出的完整签名应该有所区分,以防止签名者或者仲裁者的一些恶意行为. 但是,Accountable OFE 方案并没有考虑签名者身份不可区分性,恶意的接收者可以利用部分签名取得不公平的优势,破坏交换的公平性.

下面就 Huang-AOFE 方案[17]与本文方案进行简单对比. 表 1 将本文提出的 ID-AOFE 方案实例与 Huang-AOFE 方案实例在计算开销和通信开销方面进行了对比. 计算开销方面,表中列举了两种方案中主要采用的各类算法. 除 B-OTS 签名和 G-NIWI 算法在两种方案均有使用外,Huang-AOFE 方案还采用了基于标签的加解密 Tag-ENC 和零知识证明 G-NIZK,本文方案则采用了基于身份签名 P-IBS. 由于 Huang-AOFE 方案使用了 Tag-ENC 算法对部分签名进行加解密,因此,可以不再使用 G-NIWI 的证据提取算法(G-NIWI. Open). 表中,“E”表示群 G_1/G_2 上的模指数运算时间(这里没有严格区分两类群的计算次数,只记总数),“P”表示双线性对运算时间,“G”表示群 G_1 上的 1 个成员占用的字节数,“T”表示时间戳占用的字节数. “Sig/Ver”分别表示签名和验证算法,“Enc/Dec”分别表示加密和解密算法,“Prv/Ver/Open”分别表示证明产生算法、证明验证算法和证据提取算法.

表 1　AOFE 方案性能比较

	Huang-AOFE 方案	本文方案
B-OTS(Sig/Ver)	$1E/2P+2E$	$1E/2P+2E$
Tag-ENC(Enc/Dec)	$7E/2E$	0/0
P-IBS(Sig/Ver)	0/0	$2E/3P$
G-NIWI(Prv/Ver/Open)	$17E/13P+2E/0$	$24E/20P/6E$
G-NIZK(Prv/Ver)	$18E/39P$	0/0
计算开销总计	$49E+54P$	$35E+25P$
部分签名大小	$24G$	$6G+1T$

从表 1 可以看出,本文方案在计算开销和通信开销方面都远低于 Huang-AOFE 方案. 具体来看,零知识证明的算法开销明显大于其它算法,其验证算法的计算开销达到了 $39P$,其证明算法输出的证明包含 15 个 G_1 上的成员,该算法的使用明显增加了 Huang-AOFE 方案的计算和通信开销. 本文方案模型不再使用零知识证明算法,其总体性能比 Huang-AOFE 方案有显著提升.

5　结束语

本文将 AOFE 扩展到基于 IBC 的用户环境,提出 ID-AOFE 方案的构造模型、安全模型、及其具体的方案实例. 本文对 Huang-AOFE 方案模型进行了简化,采用具有信息提取功能的 NIWI 算法替换原方案模型中的基于标签加解密和零知识证明算法,在实现相同安全性的同时降低计算开销. 本文的 ID-AOFE 安全模型以 Huang 等人的 AOFE 安全模型为基础,融合了 Paterson 等人的选择身份安全模型,能将 ID-AOFE 方案的公平性规约到 IBS、OTS 和 NIWI 算法的正确性和安全性. 以标准模型下的 P-IBS、B-OTS 和 G-NIWI 方案为基础,本文构造了一个 ID-AOFE 方案实例,采用 ID-AOFE 选择身份安全模型对本文方案实例进行了分析,实现了可证明安全. 此外,本文详细分析了 ID-AOFE 方案的消息交互模型,就争端解决的方案和过程进行了重点阐述.

公平交换方案在复杂的社交网络中应用广泛,而在复杂网络中,同一实体往往拥有不同的身份和属性,采用单一的身份管理策略和证书化的复杂密钥管理体系(如 PKI)都具有一定的应用局限性. 基于属性密码学(Attribute-Based Cryptography,ABC)[30]能较好解决多属性管理的应用问题,基于 ABC 的 AOFE 方案及其安全模型是需要进一步研究的方向.

参考文献

[1] ASOKAN N, SCHUNTER M, WAIDNER M. Optimistic protocols for fair exchange[A]. Proceedings of the 4th ACM Computer and Communications Security Conference[C]. New York: ACM, 1997. 7 – 17.

[2] COX B, TYGAR D, SIRBU M. NetBill security and transaction protocol[A]. Proceedings of the first USENIX Workshop of Electronic Commerce[C]. New York: USENIX, 1995. 77 – 88.

[3] KREMER S. Formal analysis of optimistic fair exchange protocols[D]. Brussels, Belgium: University Libre de Bruxelles, 2003.

[4] 王彩芬,葛建华. 带脱线半可信第三方的公平非否认交换协议[J]. 电子学报,2002,30(2):286 – 288.
WANG Cai-fen, GE Jian-hua. A new fair non-repudiation protocol with off-line semi-trusted third party[J]. Acta Electronica Sinica, 2002, 30(2): 286 – 288. (in Chinese)

[5] ASOKAN N, SHOUP V, WAIDNER M. Optimistic fair exchange of digital signatures(extended abstract)[A]. Proceedings of the Advances in Cryptology-EUROCRYPT(LNCS1403)[C]. Berlin: Springer, 1998. 591 – 606.

[6] ASOKAN N, SHOUP V, WAIDNER M. Optimistic fair exchange of digital signatures[J]. IEEE Journal on Selected Areas in Communication, 2000, 18(4): 593 – 610.

[7] BOYD C, FOO E. Off-line fair payment protocols using convertible signatures[A]. Proceedings of the Advances in Cryptology-ASIACRYPT(LNCS1514)[C]. Berlin: Springer, 1998. 271 – 285.

[8] 辛向军,李刚,董庆宽,等. 一个高效的随机化的可验证加密签名方案[J]. 电子学报,2008,36(7):1378 – 1382.
XIN Xiang-jun, LI Gang, DONG Qing-kuan, et al. An efficient randomized verifiably encrypted signature scheme [J]. Acta Electronica Sinica, 2008, 36(7): 1378 – 1382. (in Chinese)

[9] GARAY J A, JAKOBSSON M, MACKENZIE P. Abuse-free optimistic contract signing[A]. Proceedings of the Advances in Cryptology-CRYPTO(LNCS1666)[C]. Berlin: Springer, 1999. 449 – 466.

[10] JAKOBSSON M, SAKO K, IMPAGLIAZZO R. Designated verifier proofs and their applications[A]. Proceedings of the Advances in Cryptology-EUROCRYPT(LNCS1070)[C]. Berlin: Springer, 1996. 143 – 154.

[11] 王晓峰,张璟,王尚平,等. 新的基于身份的广义指定验证者签名方案[J]. 电子学报,2007,35(8):1432 – 1436.
WANG Xiao-feng, ZHANG Jing, WANG Shang-ping, et al. A new ID-based universal designated verifier signature scheme[J]. Acta Electronica Sinica, 2007, 35(8): 1432 – 1436. (in Chinese)

[12] WANG Gui-lin. An abuse-free fair contract signing protocol based on the RSA signature[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(1): 158 – 168.

[13] HUANG Q, WONG D S, SUSILO W. A new construction of designated confirmer signature and its application to optimistic fair exchange(extended abstract)[A]. Proceedings of the Pairing-Based Cryptography(LNCS6487)[C]. Berlin: Springer, 2010. 41 – 61.

[14] HUANG Q, WONG D S, SUSILO W. Efficient designated confirmer signature and DCS-based ambiguous optimistic fair exchange[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(4): 1233 – 1247.

[15] HUANG Q, WONG D S, SUSILO W. The construction of ambiguous optimistic fair exchange from designated confirmer signature without random oracles[A]. Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography[C]. Berlin: Springer, 2012. 120 – 137.

[16] HUANG Q, YANG G M, WONG D S, et al. Ambiguous optimistic fair exchange[A]. Proceedings of the Advances in Cryptology-ASIACRYPT(LNCS5350)[C]. Berlin: Springer, 2008. 74 – 89.

[17] HUANG Q, YANG G M, WONG D S, et al. Ambiguous optimistic fair exchange: definition and constructions[J]. Theoretical Computer Science, 2015, 562(582): 177 – 193.

[18] GROTH J, SAHAI A. Efficient non-interactive proof systems for bilinear groups[A]. Proceedings of the Advances in Cryptology-EUROCRYPT(LNCS4965)[C]. Berlin: Springer, 2008. 415 – 432.

[19] WANG Y, AU M H, SUSILO W. Perfect ambiguous optimistic fair exchange[A]. Proceedings of the 14th International Conference on Information and Communications Security[C]. Berlin: Springer, 2012. 142 – 153.

[20] HUANG Q, WONG D S, SUSILO W. How to protect privacy in Optimistic Fair Exchange of digital signatures[J]. Information Sciences, 2015, 325: 300 – 315.

[21] GUO Q, CUI Y, ZOU X, et al. Generic construction of privacy-preserving optimistic fair exchange protocols[J]. J Internet Serv Inf Secur, 2017, 7(2): 44 – 56.

[22] SHAMIR A. Identity-based cryptosystems and signature schemes[A]. Proceedings of the Advances in Cryptology-CRYPTO(LNCS196)[C]. Berlin: Springer, 1985. 47 – 53.

[23] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[A]. Proceedings of the Advances in Cryptology-CRYPTO(LNCS2139)[C]. Berlin: Springer, 2001. 213 – 229.

[24] BOYEN X, MARTIN L. Identity-based cryptography standard(IBCS)#1: supersingular curve implementations of the BF and BB1 cryptosystems[R/OL]. http://www.ietf.org/rfc/rfc5091.txt, 2020.

[25] PARTERSON K G, SCHULDT J C N. Efficient identity-based signatures secure in the standard model[A]. Proceedings of the 11th Australasian Conference on Information Security and Privacy[C]. Berlin: Springer, 2006. 207 – 222.

[26] BONEH D, BOYEN X. Short signatures without random oracles[A]. Proceedings of the Advances in Cryptology-EUROCRYPT(LNCS3027)[C]. Berlin: Springer, 2004. 56 – 73.

[27] ZHANG Lei, WU Qian-hong, QIN Bo. Identity-based optimistic fair exchange in the standard model[J]. Security & Communication Networks, 2013, 6(8): 1010 – 1020.

[28] YOUN T K, CHANG K Y. ID-based optimistic fair exchange scheme based on RSA[J]. Etri Journal, 2014, 36(4): 673 – 681.

[29] LOH J C, HENG S H, TAN S Y. A generic framework for accountable optimistic fair exchange protocol[J]. Symmetry, 2019, 11(2): 285.

[30] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[A]. Proceedings of the 13th ACM Conference on Computer and Communications Security[C]. New York: ACM, 2006. 89 – 98.

作者简介

戚　珉　男. 1975 年 11 月出生,江西樟树人. 2000 年获南方冶金学院工学学士学位,2010 年获南昌大学软件工程硕士学位. 现为宜春学院副教授,主要从事计算机通信、信息安全等方面的研究工作.

E-mail:qm406@ qq. com

陈　明(通信作者)　男. 1978 年 5 月出生,重庆北碚人. 2007 年和 2011 年在重庆大学获工学硕士和工学博士学位. 现为宜春学院副教授,主要从事信息安全、安全协议分析与设计、物联网安全技术和在线教育等方面的研究工作.

E-mail:chenming9824@ aliyun. com