软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(4):928−940 [doi: 10.3724/SP.J.1001.2012.04024]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

多元合同签署协议*

孙艳宾[1+], 谷利泽[1], 卿斯汉[2], 郑世慧[1], 杨义先[1]

[1](北京邮电大学 网络与交换技术国家重点实验室 信息安全中心,北京 100876)

[2](北京大学 软件与微电子学院,北京 102600)

Multiplex Contract Signing Protocol

SUN Yan-Bin[1+], GU Li-Ze[1], QING Si-Han[2], ZHENG Shi-Hui[1], YANG Yi-Xian[1]

[1](Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

[2](School of Software and Microelectronics, Peking University, Beijing 102600, China)

+ Corresponding author: E-mail: ybsun@foxmail.com

Sun YB, Gu LZ, Qing SH, Zheng SH, Yang YX. Multiplex contract signing protocol. *Journal of Software*, 2012,23(4):928−940. http://www.jos.org.cn/1000-9825/4024.htm

Abstract: Utilizing the Cha-Cheon's identity-based signature scheme, a provably secure identity-based verifiably encrypted signature (VES) scheme is proposed. Utilizing the proposed scheme and identity-based proxy verifiably encrypted signature (PVES) scheme, a novel multiplex contract signing protocol is also proposed. The original signer or proxy signer uses VES or PVES to realize the interaction and certification of the commitment message in the information exchange process. The proposed scheme does not need the zero-knowledge proof and excessive computation. An optimized trusted third party who participates in the protocol extracts the formal signature from the VES or PVES only when problem occurs. The performance analysis results show that the scheme satisfies non-repudiation, timeliness and fairness.

Key words: proxy signature; contract signing protocol; random oracle model; fairness

摘 要: 利用 Cha-Cheon 的基于身份的签名方案提出了一个可证安全的基于身份的可验证加密签名(verifiably encrypted signature,简称 VES)方案,并利用该方案和基于身份的代理可验证加密签名(proxy verifiably encrypted signature,简称 PVES)方案提出了一个新颖的多元合同签署协议.信息交换过程中,原始签名者或代理签名者分别利用 VES 或 PVES 实现承诺消息的交换与认证,并未使用复杂的零知识证明系统,从而有效避免了大量运算.当争议发生时,可信第三方从 VES 或 PVES 中恢复出有效的合同签名,以保证签署者的公平性.安全性分析结果表明,协议满足不可否认性、时效性以及公平性.

关键词: 代理签名;合同签署协议;随机预言模型;公平性

中图法分类号: TP309 **文献标识码**: A

* 基金项目: 国家自然科学基金(60970135, 90718001, 60821001); 国家重点基础研究发展计划(973)(2007CB310704)
收稿时间: 2010-08-13; 定稿时间: 2011-03-21
CNKI 网络优先出版: 2011-05-12 11:47, http://www.cnki.net/kcms/detail/11.2560.TP.20110512.1147.006.html

随着电子商务的发展,合同签署协议受到广泛关注,即签署者双方通过网络共同签署某个电子合同.作为公平交换协议的一种,合同签署协议需要满足公平性,即签署者双方要么都得到对方的有效合同,要么得不到.Pagnia 等人[1]证明,如果交换协议不引入可信第三方(trusted third party,简称 TTP),就不能实现真正的公平性.如,无 TTP 参与的逐步交换协议[2,3]与并发签名协议[4,5]仅实现了弱公平性.因此,合同签署协议必须引入 TTP 来协助签署者公平地完成协议签署.根据 TTP 介入的程度和介入的方式,把 TTP 分为以下两大类:On-Line TTP 和 Off-Line TTP.其中,On-Line TTP 需要介入交换过程帮助参与者完成公平交换;而 Off-Line TTP 正常情况下不介入交换过程,只有当发生纠纷时才介入,以保证参与者在公平性的情况下结束协议.后文中出现的 TTP 如无特殊说明,即为 Off-Line TTP.

Asokan 等人[6]首先引入可验证加密签名(verifiably encrypted signature,简称 VES)方案这一概念提出了乐观公平交换协议的概念,即协议正常执行过程中不引入 TTP,只有当纠纷发生时 TTP 才介入.作为设计公平交换协议的基本模块,可验证加密签名的核心思想是,用户 A 向用户 B 发送利用 TTP 公钥加密过的签名,B 可以验证加密签名的有效性,但在没有 A 或 TTP 帮助的情况下,B 得不到原始签名;当争议发生时,TTP 可以从 VES 中恢复出用户的原始签名.此后,这种 VES 思想[6]在文献[7,8]中得到了推广.然而,由于在其交换过程中引入了复杂的交互零知识证明系统,效率较低.

为了提高效率,Boneh 等人[9]基于聚合签名的思想首先提出了非交互的可验证加密签名方案.用户利用可验证加密签名实现消息的交换与认证,并未使用复杂的交互零知识证明系统.此后,作为设计合同签署协议[10,11]以及公平交换协议[12−14]的基本模块,设计非交互的可验证加密签名方案受到广泛关注[15−23].其中,文献[15–17,19,23]中分别利用基于身份的密码体制构造了可验证加密签名方案,由于无需公钥证书的管理与鉴别,给实际应用带来了极大的便利.

本文首先利用 Cha-Cheon 的基于身份的签名方案(简称 Cha-Cheon 签名方案)[24]构造了一个高效、实用的基于身份的可验证加密签名(VES)方案.其主要思想是,在 Cha-Cheon 签名方案的基础上增加了一个包含 TTP 公钥的参数,以实现签名的加密与认证,保证在有争议发生时 TTP 能够利用其私钥从中恢复出签名.在随机预言模型中,我们对此方案进行了证明.在假设 CDH 问题困难的情况下,该方案是可证安全的.同时,我们将新 VES 方案与文献[15–17,19,23]中的 VES 方案进行了效率对比,除与文献[15]中 VES 方案相当以外,效率优于文献[16,17,19,23]中的 VES 方案.

现实中,人们经常需要将自己的某些权力委托给可靠的代理人,让代理人代表本人去行使这些权利.委托签名权力的传统方法是使用印章,因为印章可以在人们之间灵活地传递.在电子化的信息社会,同样会遇到委托签名权力的问题.Mambo 等人提出的代理签名方案[25]给出了解决这个问题的一种方法,指定的代理签署者可以代表原始签署者生成有效的代理签名.最近,Zhang 等人结合代理签名和可验证加密签名的思想提出了代理可验证加密签名(proxy verifiable encrypted signature,简称 PVES)[26]这一概念.

本文利用新提出的 VES 方案和 Zhang 等人的 PVES 方案[26]构造了一个新颖的多元合同签署协议(multiple contract signing protocol,简称 MCSP).参与合同签署协议的用户可以是原始签署者和代理签署者,因此,主签署协议中签署双方分为:原始签署者与原始签署者、原始签署者与代理签署者以及代理签署者与代理签署者 3 种情况.协议的主要思想是,第 1 轮,用户利用 VES 或 PVES 实现消息的交换与认证;第 2 轮,用户交换合同签名;该方案中,用户与 TTP 之间无需进行特殊注册,当争议发生时,才需 TTP 的介入,以保证用户的公平性.安全性分析表明,MCSP 满足不可否认性,同时还满足时效性和公平性.

1 预备知识

1.1 双线性对及相关定义

设 G_1,G_2 分别具有相同素数阶 q 的加法和乘法循环群,P 是 G_1 的生成元.假设离散对数问题在 G_1 和 G_2 上是难解的,则称具有下列性质的映射 $e:G_1\times G_2\to G_2$ 为双线性对.

(1) 双线性性:对任意的 $P,Q\in G_1$ 和 $a,b\in Z_q$ 有 $e(aP,bQ)=e(P,Q)^{ab}$;

(2) 非退化性:存在元素 $P,Q\in G_1$ 使得 $e(P,Q)\neq 1$;

(3) 可计算性:存在有效算法可计算 $e(P,Q)$,对任意 $P,Q\in G_1$.

此类双线性对即为 Boneh 等人[27]提出的可利用的双线性对(admissible bilinear pairing).

定义 1(CDH 问题[28]). 设 P 是 G_1 的生成元,给定 $aP,bP\in G_1,\forall a,b\in Z_q^*$,计算 abP.

1.2 多元合同签署协议模型

多元合同签署协议的参与者包括:原始签署者或代理签署者,TTP.

定义 2. 一个多元合同签署协议包括 11 个多项式算法以及 3 个协议,具体描述如下:

- 参数设定.系统参数 $param$、密钥生成中心(KGC)的会话密钥 s 和公钥 P_{pub}、TTP 的私钥和公钥对 (x_{TTP},P_{TTP}),公布 P_{pub} 与 P_{TTP}.这里,TTP 与 KGC 不同.
- 密钥提取.给定用户身份 ID,KGC 利用用户身份和会话密钥 s 计算用户私钥 D_{ID},并发送给用户.
- 代理授权.分别给定原始签署者和代理签署者的身份 ID_X 和 ID_{XP}.原始签署者利用授权文件 m_{Xw} 生成 (S_X,R_X),向代理签署者授权.代理签署者利用(S_X,R_X)计算代理签名密钥 S_{XP}.
- 普通签名.给定消息 m,用户私钥 D_{ID},签署者输出普通签名 V=Sign(D_{ID},m).
- 普通签名验证.验证算法 Verify(m,V,ID)以消息 m、签名 V 以及用户身份 ID 为输入,输出 1(接收)或 0(拒绝).
- 可验证加密签名.给定消息 m、用户私钥 D_{ID} 以及 TTP 公钥 P_{TTP},签署者输出可验证加密签名:
$$W=\text{VES-Sign}(D_{ID},P_{TTP},m).$$
- 可验证加密签名验证.验证算法 VES-Verify(m,W,ID,P_{TTP})以消息 m、可验证加密签名 W、用户身份 ID 以及 TTP 公钥 P_{TTP} 为输入,输出 1(接受)或 0(拒绝).
- 代理签名.给定消息 m、代理签名密钥 S_{XP}、参数 R_X、授权文件 m_{Xw},代理签署者输出代理签名:
$$V_P=\text{P-Sign}(m,ID_X,ID_{XP},S_{XP},R_X,m_{Xw}).$$
- 代理签名验证.验证算法 P-Verify$(m,V_P,ID_X,ID_{XP},R_X,m_{Xw})$以消息 m、代理签名 V_P、原始签署者身份 ID_X、代理签署者的身份 ID_{XP}、授权参数 R_X、授权文件 m_{Xw} 为输入,输出 1(接受)或 0(拒绝).
- 代理可验证加密签名.给定消息 m、原始签署者身份 ID_X、代理签署者的身份 ID_{XP}、代理签名密钥 S_{XP}、参数 R_X、授权文件 m_{Xw} 以及 TTP 公钥 P_{TTP},代理签署者输出代理可验证加密签名:
$$W_P=\text{PVES-Sign}(ID_X,ID_{XP},S_{XP},R_X,m_{Xw},P_{TTP},m).$$
- 代理可验证加密签名验证.验证算法 PVES-Verify$(W_P,ID_X,ID_{XP},R_X,m_{Xw},P_{TTP},m)$以消息 m、代理可验证加密签名 W_P、原始签署者身份 ID_X、代理签署者的身份 ID_{XP}、参数 R_X、授权文件 m_{Xw} 以及 TTP 公钥 P_{TTP} 为输入,输出 1(接受)或 0(拒绝).
- 主签署协议.用户为原始签署者或代理签署者.第 1 阶段,签署者利用 VES 或 PVES 实现承诺消息的交换与认证;第 2 阶段,交换合同签名.根据协议执行情况,签署者可以要求 TTP 执行取消或争端解决子协议.
- 取消子协议.当协议第 1 阶段有争议发生时,发起者要求 TTP 执行取消子协议.
- 争端解决子协议.当协议第 2 阶段有争议发生时,签署者要求 TTP 执行争端解决子协议.

定义 3. 如果普通签名、可验证加密签名、代理签名以及代理可验证加密签名是不可伪造的,则多元合同签署协议是不可否认的.

2 多元合同签署协议

在详细描述多元合同签署协议之前,我们首先引入符号标记:"$M_1\|M_2$"表示消息 M_1 与 M_2 的级联,$M_1[M_2]$表示消息 M_1 或 M_2.符号 Mes_A 表示消息"取消协议(abort the protocol)",Mes_RI 表示消息"要求无效(request is invalid)",Mes_RD 表示消息"争端解决(resolve dispute)";l 表示一次性协议标签(签署者身份、TTP 身份等相关信息

的哈希值);T表示协议运行的有效期(由协议的发起者选定).同时,假设签署者与TTP之间为安全信道,签署者之间为不安全信道.为方便描述协议的主要过程,协议中签署者之间的交互信息未作加密处理,为原始信息,具体实施可通过公钥加密系统加密后进行交互.协议的具体执行过程如下:

- 参数设定.给定(G_1,G_2,e,q,P,Q),其中,Q为G_1的另一个生成元.随机选择$s\in Z_q^*$,令$P_{pub}=sP$.选择哈希函数$H_1:\{0,1\}^*\to G_1$, $H_0,H_2:\{0,1\}^*\to Z_q^*$.TTP随机选择$x_{TTP}\in Z_q^*$作为私钥,计算公钥$P_{TTP}=x_{TTP}P$.系统参数为$param=\{G_1,G_2,e,q,P,Q,P_{pub},P_{TTP},H_1,H_2\}$,其中,$s$为会话密钥,$x_{TTP}$为TTP的密钥.
- 密钥提取.给定用户身份$ID_X\in(0,1)^*$,计算$Q_X=H_1(ID_X)\in G_1$,$D_X=sQ_X$.KGC根据此算法生成用户的私钥D_X,并通过安全信道发送给用户.
- 代理授权.分别给定原始签署者U_X和代理签署者U_{XP}的身份ID_X和ID_{XP}.原始签署者随机选择$r_X\in Z_q^*$,计算$S_X=H_0(R_X,m_{Xw})D_X+r_XQ$,$R_X=r_XP$,$m_{Xw}$为$U_X$向$U_{XP}$授权的文件.然后,$U_X$通过安全信道发送$(S_X,R_X)$及$m_{Xw}$给$U_{XP}$.$U_{XP}$验证等式$e(S_X,P)=e(Q_X,H_0(R_X,m_{Xw})P_{pub})e(Q,R_X)$是否成立:如果成立,$U_{XP}$计算代理签名密钥$S_{XP}=S_X+H_0(R_X,m_{Xw})D_{XP}$,即$S_{XP}=H_0(R_X,m_{Xw})(D_X+D_{XP})+r_XQ$;否则,$U_{XP}$要求$U_X$重新进行授权.
- 普通签名(Sign).给定密钥D_X,签名消息M,原始签署者U_X选择$r_{X1},r_{X2}\in Z_q^*$,并计算

  $$C_{X1}=r_{X1}Q_X,C_{X2}=r_{X2}P,h_X=H_2(M\|C_{X2},C_{X1}),V_X=(r_{X1}+h_X)D_X,$$

  其中,(V_X,C_{X1},C_{X2})为消息M的签名.很容易看出,去掉参数C_{X2}即为Cha-Cheon签名.
- 普通签名验证(Verify).给定消息M的普通签名(V_X,C_{X1},C_{X2}),验证者计算$Q_X=H_1(ID_X)$,$h_X=H_2(M\|C_{X2},C_{X1})$,然后验证等式$e(V_X,P)=e(P_{pub},C_{X1}+h_XQ_X)$是否成立:如果成立,$(V_X,C_{X1},C_{X2})$为签署者关于消息$M$的有效签名;否则,无效.
- 可验证加密签名(VES-Sign).给定密钥D_X,签名消息M,原始签署者U_X随机选择$r_{X1},r_{X2}\in Z_q^*$,根据Sign算法计算(V_X,C_{X1},C_{X2}),然后计算$W_X=V_X+r_{X2}P_{TTP}$,其中,(W_X,C_{X1},C_{X2})为消息M的可验证加密签名.
- 可验证加密签名验证(VES-Verify).给定消息M的可验证加密签名(W_X,C_{X1},C_{X2}),验证者首先计算$Q_X=H_1(ID_X)$,$h_X=H_2(M\|C_{X2},C_{X1})$,然后验证等式$e(P,W_X)=e(P_{pub},C_{X1}+h_XQ_X)e(C_{X2},P_{TTP})$是否成立:如果成立,$(W_X,C_{X1},C_{X2})$为原始签名者关于消息$M$的有效可验证加密签名;否则,无效.
- 代理签名(P-Sign).给定代理签名密钥S_{XP},签名消息M,代理签署者U_{XP}随机选择$r_{XP1},r_{XP2}\in Z_q^*$,计算

  $$C_{XP1}=r_{XP1}(Q_X+Q_{XP}),C_{XP2}=r_{XP2}P,h_{XP}=H_2(M\|C_{XP2},C_{XP1}),V_{XP}=H_0(R_X,m_{Xw})^{-1}(r_{XP1}+h_{XP})S_{XP},$$

  其中,$(V_{XP},C_{XP1},C_{XP2},R_X,m_{Xw})$为消息$M$的代理签名.
- 代理签名验证(P-Verify).给定消息M的代理签名$(V_{XP},C_{XP1},C_{XP2},R_X,m_{Xw})$,验证者首先计算$Q_X=H_1(ID_X)$,$Q_{XP}=H_1(ID_{XP})$,$h_{XP}=H_2(M\|C_{XP2},C_{XP1})$,然后验证等式

  $$e(P,V_{XP})=e(P_{pub},h_{XP}(Q_X+Q_{XP})+C_{XP1})\cdot e(R_X,Q)^{H_0(R_X,m_{Xw})^{-1}}$$

  是否成立:如果成立,$(V_{XP},C_{XP1},C_{XP2},R_X,m_{Xw})$为消息$M$的有效代理签名;否则,无效.
- 代理可验证加密签名(PVES-Sign).给定代理签名密钥S_{XP}、签名消息M,代理签署者U_{XP}随机选择$r_{XP1},r_{XP2}\in Z_q^*$,根据P-Sign算法计算$(V_{XP},C_{XP1},C_{XP2},R_X,m_{Xw})$,然后计算

  $$W_{XP}=V_{XP}+r_{XP2}P_{TTP},$$

  其中,$(W_{XP},C_{XP1},C_{XP2},R_X,m_{Xw})$为消息$M$的代理可验证加密签名.
- 代理可验证加密签名验证(PVES-Verify).给定消息M的代理可验证加密签名$(W_{XP},C_{XP1},C_{XP2},R_X,m_{Xw})$,验证者首先计算$Q_X=H_1(ID_X)$,$Q_{XP}=H_1(ID_{XP})$,$h_{XP}=H_2(M\|C_{XP2},C_{XP1})$,然后验证等式

  $$e(P,W_{XP})=e(P_{pub},h_{XP}(Q_X+Q_{XP})+C_{XP1})\cdot e(R_X,Q)^{H_0(R_X,m_{Xw})^{-1}}\cdot e(C_{XP2},P_{TTP})$$

  是否成立:如果成立,$(W_{XP},C_{XP1},C_{XP2},R_X,m_{Xw})$为消息$M$的有效代理可验证加密签名;否则,无效.
- 主签署协议

假设合同签署者双方已经商榷好所要签署的电子合同为$m\in\{0,1\}^*$,签署者双方分为:原始签署者与原始签

署者、代理签署者与原始签署者以及代理签署者与代理签署者 3 种情况,且每种情况对应一个子签署协议.假设执行协议之前,代理签署者已得到原始签署者的授权.3 个子签署协议的具体过程如下:

子协议 1. 签署双方均为原始签署者.不失一般性,假设协议发起方为原始签署者 U_A,响应方为原始签署者 U_B,协议的主要过程为:

Step 1. $U_A \rightarrow U_B$:(l,T,W_A,C_{A1},C_{A2});

Step 2. $U_B \rightarrow U_A$:(W_B,C_{B1},C_{B2});

Step 3. $U_A \rightarrow U_B$:V_A;

Step 4. $U_B \rightarrow U_A$:V_B.

详细情况为:

Step 1. 首先,原始签署者 U_A 选择一个协议执行的有效期 T,计算一次性协议标签 l,令 $M=m||l||T$,根据 VES-Sign 算法计算消息 M 的可验证加密签名:随机选择 $r_{A1},r_{A2} \in Z_q^*$, 计算

$$C_{A1}=r_{A1}Q_A,C_{A2}=r_{A2}P,h_A=H_2(M||C_{A2},C_{A1}),V_A=r_{A1}+h_AD_A,W_A=V_A+r_{A2}P_{TTP}.$$

然后发送(l,T,W_A,C_{A1},C_{A2})给 U_B.其中,(V_A,C_{A1},C_{A2})为消息 M 的普通签名,(W_A,C_{A1},C_{A2})为消息 M 的可验证加密签名.

Step 2. 当 U_B 接收到(l,T,W_A,C_{A1},C_{A2})后,如果不同意有效期 T,则不发送任何消息,退出协议;否则,U_B 根据 VES-Verify 算法验证等式 $e(P,W_A)=e(P_{pub},C_{A1}+h_AQ_A)\cdot e(C_{A2},P_{TTP})$是否成立:如果不成立,$U_B$ 退出协议;否则,U_B 计算消息 $M=m||l||T$ 的可验证加密签名:随机选择 $r_{B1},r_{B2} \in Z_q^*$, 根据 VES-Sign 算法计算(V_B,W_B,C_{B1},C_{B2}),然后发送可验证加密签名(W_B,C_{B1},C_{B2})给 U_A.

Step 3. 如果 U_A 在 T 之前未收到 U_B 的可验证加密签名,U_A 要求 TTP 执行取消子协议或在 T 之后退出协议.当 U_A 在 T 之前接收到(W_B,C_{B1},C_{B2})后,U_A 根据 VES-Verify 算法验证等式 $e(P,W_B)=e(P_{pub},C_{B1}+h_BQ_B)\cdot e(C_{B2},P_{TTP})$是否成立:如果成立,$U_A$ 发送其合同签名 V_A 给 U_B;否则,U_A 要求 TTP 执行取消子协议.

Step 4. 如果 U_B 在 T 之前未收到 U_A 的合同签名,则 U_B 要求 TTP 执行争端解决子协议.当 U_B 在 T 之前接收到 U_A 的合同签名 V_A 后,根据 Verify 算法验证等式 $e(P,V_A)=e(P_{pub},C_{A1}+h_AQ_A)$是否成立:如果成立,则 U_B 发送其合同签名 V_B 给 U_A;否则,U_B 要求 TTP 执行争端解决子协议.

最后,如果 U_A 在 T 之前未收到 U_B 的合同签名,则 U_A 要求 TTP 执行争端解决子协议.当 U_A 在 T 之前接收到 U_B 的合同签名 V_B 后,根据 Verify 算法验证等式 $e(P,V_B)=e(P_{pub},C_{B1}+h_BQ_B)$是否成立:如果成立,协议结束;否则,$U_A$ 要求 TTP 执行争端解决子协议.

子协议 2. 协议签署双方为代理签署者与原始签署者.不失一般性,假设协议发起方为代理签署者 U_{AP},响应方为原始签署者 U_B,协议的主要过程如下:

Step 1. $U_{AP} \rightarrow U_B$:$(l,T,W_{AP},C_{AP1},C_{AP2},R_A,m_{Aw})$;

Step 2. $U_B \rightarrow U_{AP}$:(W_B,C_{B1},C_{B2});

Step 3. $U_{AP} \rightarrow U_B$:V_{AP};

Step 4. $U_B \rightarrow U_{AP}$:V_B.

详细情况为:

Step 1. 首先代理签署者 U_{AP} 选择一个协议执行的有效期 T,计算一次性协议标签 l,令 $M=m||l||T$,根据 PVES-Sign 算法,利用代理签名密钥 S_{AP} 计算消息 M 的代理可验证加密签名:随机选择 $r_{AP1},r_{AP2} \in Z_q^*$, 计算

$$C_{AP1}=r_{AP1}(Q_A+Q_{AP}),C_{AP2}=r_{AP2}P,h_{AP}=H_2(M||C_{AP2},C_{AP1}),V_{AP}=H_0(R_A,m_{Aw})^{-1}(r_{AP1}+h_{AP})S_{AP},W_{AP}=V_{AP}+r_{AP2}P_{TTP}.$$

然后发送$(l,T,W_{AP},C_{AP1},C_{AP2},R_A,m_{Aw})$给 U_B.其中,$(V_{AP},C_{AP1},C_{AP2},R_A,m_{Aw})$为代理签名,$(W_{AP},C_{AP1},C_{AP2},R_A,m_{Aw})$为代理可验证加密签名.

Step 2. 当 U_B 接收到$(l,T,W_{AP},C_{AP1},C_{AP2},R_A,m_{Aw})$后,如果不同意有效期 T,则不发送任何消息,退出协议;否则,U_B 根据 PVES-Verify 算法验证等式:

$$e(P,W_{AP})=e(P_{pub},h_{AP}(Q_A+Q_{AP})+C_{AP1})\cdot e(R_A,Q)^{H_0(R_A,m_{Aw})^{-1}}\cdot e(C_{AP2},P_{TTP})$$

是否成立.如果不成立,U_B 退出协议;否则,U_B 计算消息 $M=m||l||T$ 的可验证加密签名:随机选择 $r_{B1},r_{B2}\in Z_q^*$, 根据 VES-Sign 算法计算(V_B,W_B,C_{B1},C_{B2}),然后发送可验证加密签名(W_B,C_{B1},C_{B2})给 U_{AP}.

Step 3. 如果 U_{AP} 在 T 之前未收到 U_B 的可验证加密签名,U_{AP} 要求 TTP 执行取消子协议或在 T 之后退出协议;当 U_{AP} 在 T 之前接收到(W_B,C_{B1},C_{B2})后,根据 VES-Verify 算法验证等式 $e(P,W_B)=e(P_{pub},C_{B1}+h_BQ_B)\cdot e(C_{B2},P_{TTP})$ 是否成立:如果成立,U_{AP} 发送其代理签名 V_{AP} 给 U_B;否则,U_{AP} 要求 TTP 执行取消子协议.

Step 4. 如果 U_B 在 T 之前未收到 U_{AP} 的代理合同签名,则 U_B 要求 TTP 执行争端解决子协议;当 U_B 在 T 之前接收到 U_{AP} 的代理合同签名 V_{AP} 后,根据 P-Verify 算法验证等式:

$$e(P,V_{AP})=e(P_{pub},h_{AP}(Q_A+Q_{AP})+C_{AP1})\cdot e(R_A,Q)^{H_0(R_A,m_{Aw})^{-1}}$$

是否成立:如果成立,则 U_B 发送其合同签名 V_B 给 U_{AP};否则,U_B 要求 TTP 执行争端解决子协议.

最后,如果 U_{AP} 在 T 之前未收到 U_B 的合同签名,则 U_{AP} 要求 TTP 执行争端解决子协议;当 U_{AP} 在 T 之前接收到 U_B 的合同签名 V_B 后,根据 Verify 算法验证等式 $e(P,V_B)=e(P_{pub},C_{B1}+h_BQ_B)$是否成立:如果成立,协议结束;否则,$U_{AP}$ 要求 TTP 执行争端解决子协议.

若把 Step 1 与 Step 2、Step 3 与 Step 4 对调,且原始签名者选择有效期,则协议即为原始签名者为发起者的情况.其详细过程与上述描述类似,这里不再赘述.

子协议 3. 协议签署双方均为代理签署者.不失一般性,假设协议发起方为代理签署者 U_{AP},响应方为代理签署者 U_{BP},协议的主要过程如下:

Step 1. $U_{AP}\rightarrow U_{BP}$:$(l,T,W_{AP},C_{AP1},C_{AP2},R_A,m_{Aw})$;

Step 2. $U_{BP}\rightarrow U_{AP}$:$(W_{BP},C_{BP1},C_{BP2},R_B,m_{Bw})$;

Step 3. $U_{AP}\rightarrow U_{BP}$:V_{AP};

Step 4. $U_{BP}\rightarrow U_{AP}$:V_{BP}.

详细过程为:

Step 1. 首先,U_{AP} 选择一个协议执行的有效期 T,计算一次性协议标签 l,令 $M=m||l||T$,随机选择 $r_{AP1},r_{AP2}\in Z_q^*$, 根据 PVES-Sign 算法计算消息 M 的代理签名和代理可验证加密签名$(V_{AP},W_{AP},C_{AP1},C_{AP2},R_A,m_{Aw})$,然后发送代理可验证加密签名$(l,T,W_{AP},C_{AP1},C_{AP2},R_A,m_{Aw})$给 U_{BP}.

Step 2. 当 U_{BP} 接收到 U_{AP} 的消息$(l,T,W_{AP},C_{AP1},C_{AP2},R_A,m_{Aw})$后,如果不同意有效期 T,则不发送任何消息,退出协议;否则,U_{BP} 根据 PVES-Verify 算法验证等式:

$$e(P,W_{AP})=e(P_{pub},h_{AP}(Q_A+Q_{AP})+C_{AP1})\cdot e(R_A,Q)^{H_0(R_A,m_{Aw})^{-1}}\cdot e(C_{AP2},P_{TTP})$$

是否成立:如果不成立,U_{BP} 退出协议;否则,U_{BP} 随机选择 $r_{BP1},r_{BP2}\in Z_q^*$, 根据 PVES-Sign 算法计算$(V_{BP},W_{BP},C_{BP1},C_{BP2},R_B,m_{Bw})$,然后将代理可验证加密签名$(W_{BP},C_{BP1},C_{BP2},R_B,m_{Bw})$发送给 U_{AP}.

Step 3. 如果 U_{AP} 在 T 之前未收到 U_{BP} 的代理可验证加密签名,则 U_{AP} 要求 TTP 执行取消子协议;当 U_{AP} 在 T 之前接收到 U_{BP} 的消息$(W_{BP},C_{BP1},C_{BP2},R_B,m_{Bw})$后,根据 PVES-Verify 算法验证等式:

$$e(P,W_{BP})=e(P_{pub},h_{BP}(Q_B+Q_{BP})+C_{BP1})\cdot e(R_B,Q)^{H_0(R_B,m_{Bw})^{-1}}\cdot e(C_{BP2},P_{TTP})$$

是否成立:如果成立,U_{AP} 发送其代理合同签名 V_{AP} 给 U_{BP};否则,U_{AP} 要求 TTP 执行取消子协议.

Step 4. 如果 U_{BP} 在 T 之前未收到 U_{AP} 的代理合同签名,则 U_{BP} 要求 TTP 执行争端解决子协议;当 U_{BP} 在 T 之前接收到 U_{AP} 的代理合同签名 V_{AP} 后,根据 P-Verify 算法验证等式

$$e(P,V_{AP})=e(P_{pub},h_{AP}(Q_A+Q_{AP})+C_{AP1})\cdot e(R_A,Q)^{H_0(R_A,m_{Aw})^{-1}}$$

是否成立:如果成立,U_{BP} 发送其代理合同签名 V_{BP} 给 U_{AP};否则,U_{BP} 要求 TTP 执行争端解决子协议.

最后,如果 U_{AP} 在 T 之前未收到 U_{BP} 的代理合同签名,则 U_{AP} 要求 TTP 执行争端解决子协议;当 U_{AP} 在 T 之前接收到 U_{BP} 的代理合同签名 V_{BP} 后,根据 P-Verify 算法验证等式:

$$e(P,V_{BP})=e(P_{pub},h_{BP}(Q_B+Q_{BP})+C_{BP1})\cdot e(R_B,Q)^{H_0(R_B,m_{Bw})^{-1}}$$

是否成立:如果成立,协议结束;否则,U_{AP}要求 TTP 执行争端解决子协议.

- 取消子协议(abort sub-protocol)

如果发起方未收到响应方的(代理)可验证加密签名消息,或收到后验证未通过,则发起方要求 TTP 执行取消子协议.当发起方为原始签署者 U_A或代理签署者 U_{AP}时,取消子协议具体情况如下:

情况 1. 如果发起方为原始签署者 U_A,则响应方为 U_B或 U_{BP}时,主要过程为:

$U_A\rightarrow TTP$:$\{l,T,ID_A,ID_B[ID_{BP}],\mathrm{Mes}_A,V_{A\text{-}Abort}\}$

if (TTP's State=Dispute Resolve)

$TTP\rightarrow U_A/U_B[U_{BP}]$:$V_B[V_{BP}]/V_A$

else if (Request is invalid)

$TTP\rightarrow U_A$:Mes_{RI}

else

$TTP\rightarrow U_A/U_B[U_{BP}]$:$\{l,T,\mathrm{Mes}_A,V_{TTP\text{-}Abort}\}$

详细过程为:U_A根据 Sign 算法计算消息 $M_{A\text{-}Abort}=l||T||ID_A||ID_B[ID_{BP}]||\mathrm{Mes}_A$的签名 $V_{A\text{-}Abort}$,然后在 T之前将消息$\{l,T,ID_A,ID_B[ID_{BP}],\mathrm{Mes}_A,V_{A\text{-}Abort}\}$发送给 TTP.当 TTP 在 T之前接收到 U_A要求执行取消协议的消息后,如果 TTP 的状态处于争端解决状态,则 TTP 发送 $U_B[U_{BP}]$的合同签名 $V_B[V_{BP}]$给 U_A,发送 U_A的合同签名 V_A给 $U_B[U_{BP}]$;否则,TTP 根据 Verify 算法验证 $V_{A\text{-}Abort}$是否是 U_A对消息 $M_{A\text{-}Abort}$的有效签名:如果有效,则 TTP 根据 Sign 算法计算消息 $M_{TTP\text{-}Abort}=l||T||\mathrm{Mes}_A$ 的签名 $V_{TTP\text{-}Abort}$,然后通过安全信道分别发送消息$\{l,T,\mathrm{Mes}_A,V_{TTP\text{-}Abort}\}$给 U_A 与 $U_B[U_{BP}]$;若 $V_{A\text{-}Abort}$未通过验证,则 TTP 发送消息 Mes_{RI}给 U_A,并要求 U_A重新发送.

情况 2. 如果发起方为代理签署者 U_{AP},则响应方为 U_B或 U_{BP}时,主要过程为:

$U_{AP}\rightarrow TTP$:$\{l,T,ID_{AP},ID_B[ID_{BP}],\mathrm{Mes}_A,R_A,m_{Aw},V_{AP\text{-}Abort}\}$

if (TTP's State=Dispute Resolve)

$TTP\rightarrow U_{AP}/U_B[U_{BP}]$:$V_B[V_{BP}]/V_{AP}$

else if (Request is invalid)

$TTP\rightarrow U_{AP}$:Mes_{RI}

else

$TTP\rightarrow U_{AP}/U_B[U_{BP}]$:$\{l,T,\mathrm{Mes}_A,V_{TTP\text{-}Abort}\}$

该情况除 U_{AP}根据 PVES-Sign 算法计算 $V_{AP\text{-}Abort}$以外,其他与情况 1 描述类似,这里不再赘述.

- 争端解决子协议(dispute resolve sub-protocol)

如果某个签署者声称未收到另一签署者的(代理)合同签名或者收到的(代理)合同签名验证未通过,则可要求 TTP 执行争端解决子协议.假设 $X,Y\in\{A,B\}$,$X\neq Y$.由于参与合同签署的双方要求 TTP 执行争端解决子协议时需提交的消息不同,下面我们将分情况加以描述,具体过程如下:

情况 1. 假设原始签署者 U_X要求 TTP 执行争端解决子协议,则另一签署者为 U_Y或 U_{YP},主要过程为:

$U_X\rightarrow TTP$:$\{l,T,ID_X,ID_Y[ID_{YP}],m,(V_X,C_{X1},C_{X2}),(W_Y,C_{Y1},C_{Y2})[(W_{YP},C_{YP1},C_{YP2},R_Y,m_{Yw})],\mathrm{Mes}_{RD},V_{X\text{-}RD}\}$

if (TTP's State=Abort)

$TTP\rightarrow U_X/U_Y[U_{YP}]$:$\{l,T,\mathrm{Mes}_A,V_{TTP\text{-}Abort}\}$

else if (Request is invalid) $TTP\rightarrow U_X$:Mes_{RI}

else $TTP\rightarrow U_X/U_Y[U_{YP}]$:$V_Y[V_{YP}]/V_X$

详细过程:U_X 根据 Sign 算法计算 $M_{X\text{-}RD}=l||T||ID_X||ID_Y[ID_{YP}]||\mathrm{Mes}_{RD}$ 的签名 $V_{X\text{-}RD}$,然后发送消息$\{l,T,ID_X,ID_Y[ID_{YP}],m,(V_X,C_{X1},C_{X2}),(W_Y,C_{Y1},C_{Y2})[(W_{YP},C_{YP1},C_{YP2},R_Y,m_{Yw})],\mathrm{Mes}_{RD},V_{X\text{-}RD}\}$给 TTP 要求执行争端解决子协议.当 TTP 在 T之前收到消息后,如果 TTP 处于取消协议状态,则 TTP 分别发送取消协议信息$\{l,T,\mathrm{Mes}_A,V_{TTP\text{-}Abort}\}$给 U_X 和 $U_Y[U_{YP}]$;否则,TTP 分别验证 V_X 和 $W_Y[W_{YP}]$的有效性:如果验证通过,则 TTP 利用其私钥 x_{TTP} 计算

$V_Y=W_Y-x_{TTP}C_{Y2}[V_{YP}=W_{YP}-x_{TTP}C_{YP2}]$,恢复 $U_Y[U_{YP}]$的合同签名 $V_Y[V_{YP}]$,然后发送 $V_Y[V_{YP}]$给 V_X,发送 V_X给 $U_Y[U_{YP}]$;如果验证未通过,则 TTP 发送消息 Mes_{RI}给 U_X,并要求 U_X 重新发送.

情况 2. 假设代理签署者 U_{XP}要求 TTP 执行争端解决子协议,则另一签署者为 U_Y或 U_{YP},主要过程为:

$U_{XP}\rightarrow TTP$:$\{l,T,ID_{XP},ID_Y[ID_{YP}],m,(V_{XP},C_{XP1},C_{XP2},R_X,m_{Xw}),(W_Y,C_{Y1},C_{Y2})[(W_{YP},C_{YP1},C_{YP2},R_Y,m_{Yw})],\text{Mes}_{\text{RD}},V_{XP\text{-}RD}\}$

if (TTP's State=Abort)

$TTP\rightarrow U_{XP}/U_Y[U_{YP}]$:$\{l,T,\text{Mes}_{\text{A}},V_{TTP\text{-}Abort}\}$

else if (Request is invalid) $TTP\rightarrow U_{XP}$:Mes_{RI}

else $TTP\rightarrow U_{XP}/U_Y[U_{YP}]$:$V_Y[V_{YP}]/V_{XP}$

情况 2 的详细描述与情况 1 类似,这里不再赘述.

3 安全性分析

首先分析 VES 和 PVES 方案的正确性;其次,在随机预言模型中证明协议中 VES 和 PVES 方案及合同签名和代理合同签名的安全性;最后分析协议的时效性和公平性.

定理 1. 多元合同签署协议中,可验证加密签名方案和代理可验证加密签名方案满足正确性.

证明:由可验证加密签名方案和代理可验证加密签名方案的详细计算过程可知,两个方案都满足正确性(详细推论过程略). □

定理 2. 假设 CDH 问题是难解的,基于身份的普通签名方案在随机预言模型中是可证安全的.

证明:很容易看出,普通签名方案是在 Cha-Cheon 签名[24]基础上增加了一个参数后得到的,其目的是用来进行 VES 的验证及仲裁.而 Cha-Cheon 签名方案在随机预言模型中是可证安全的,因此普通签名方案在随机预言模型中是可证安全的(详细过程参见文献[24]). □

定理 3. 如果存在伪造者$\mathcal{F}$能够伪造基于身份的可验证加密签名,则存在算法$\mathcal{B}$能够利用伪造者$\mathcal{F}$求解 CDH 问题.

证明:下面我们说明$\mathcal{B}$如何利用伪造者$\mathcal{F}$来求解 CDH 问题.给定算法$\mathcal{B}$一个 CDH 问题的实例(P,aP,bP),目的是利用伪造者$\mathcal{F}$输出 abP.

Setup:算法$\mathcal{B}$运行协议中的 Setup 算法.令 $P_{pub}=aP$ 为 KGC 的公钥.$\mathcal{B}$随机选择 $x\in Z_q$,令 $Q=xP$,并发送相关的系统参数$(G_1,G_2,q,e,P,Q,P_{pub},H_1,H_2)$给$\mathcal{F}$.最后,$\mathcal{B}$随机选择索引 $l\in[1,q_{H_1}]$,其中,q_{H_1}表示至多进行 q_{H_1} 次 $H_1(\cdot)$预言询问.

$H_1(\cdot)$询问:当$\mathcal{F}$进行关于身份 ID_i 的 $H_1(\cdot)$预言询问时,如果 $I=l$,则$\mathcal{B}$回复 $H_1(ID_i)=bP$;如果 $i\neq l$,则$\mathcal{B}$随机选择 $t_i\in Z_q^*$,并回复 $H_1(ID_i)=t_iP$.

$H_2(\cdot)$询问:当$\mathcal{F}$询问预言 $H_2(\cdot)$时,$\mathcal{B}$随机选择 $h_i\in Z_q^*$ 作为回复.

Extract 询问:当$\mathcal{F}$询问提取预言 Extract 时,如果 $I=l$,则$\mathcal{B}$结束回复任何询问;如果 $i\neq l$,则$\mathcal{B}$回复

$$D_{ID_i}=sH_1(ID_i)=t_iP_{pub}.$$

Sign 询问:当$\mathcal{F}$询问关于消息 M_i、签名者身份为 ID_i 的签名预言时,$\mathcal{B}$进行如下计算:

(1) 随机选择 $h_i,\alpha\in Z_q^*$,并计算 $C_{i1}=\alpha P-h_iQ_i$;

(2) 令 $H_2(M_i\|C_{i2},C_{i1})=h_i$,其中,$C_{i2}\in_R G_1$;

(3) 令 $V=\alpha P_{pub}$;

(4) 输出签名(V_i,C_{i1},C_{i2},M_i).

VES-Sign 询问:当$\mathcal{F}$进行关于消息 M_i、签名者身份 ID_i 以及 TTP 的公钥 P_{TTP} 的可验证加密签名预言询问时,$\mathcal{B}$首先进行 Sign 预言询问,得到回复(V_i,C_{i1},C_{i2},M_i),然后进行如下计算:

(1) 计算 $W_i=V_i+x_{TTP}C_{i2}$;

(2) 输出可验证加密签名(W_i,C_{i1},C_{i2},M_i).

最后,$\mathcal{B}$返回(W_i,U_{i1},U_{i2},M_i)作为$\mathcal{F}$的可验证加密签名的预言询问.

Resolve 询问:当$\mathcal{F}$进行关于消息 M_i、签名者身份 ID_i 以及 TTP 的公钥 P_{TTP} 的可验证加密签名(W_i,C_{i1},C_{i2},M_i)的争端解决预言询问时,$\mathcal{B}$首先验证可验证加密签名(W_i,C_{i1},C_{i2},M_i)的有效性:如果无效,则终止;否则,$\mathcal{B}$计算

$$V_i=W_i-x_{TTP}C_{i2}.$$

输出:最后,如果$\mathcal{F}$输出一个有效的关于消息 M^*、签名者身份 ID_i^* 以及 TTP 的公钥 P_{TTP} 的可验证加密签名 (W^*,C_1^*,C_2^*,M^*), 要求:1) 未提交 ID^*进行过 Extract 询问;2) 未提交(ID^*,M^*)进行过 VES-Sign 询问.

根据 (W^*,C_1^*,C_2^*,M^*) 计算 $V^*=W^*-x_{TTP}C_2^*$,其中, (V^*,C_1^*,C_2^*,M^*) 是关于消息 M^*以及身份为 ID_i^* 的签名者的一个有效签名.运用分支定理[29],得到两个有效的可验证加密签名 (W^*,C_1^*,C_2^*,M^*) 和 (W'^*,C_1^*,C_2^*,M^*),其中,

$$e(W^*,P)=e(P_{Pub},C_1^*)e(P_{Pub},hQ_i^*)e(Q_{TTP},C_2^*),$$
$$e(W'^*,P)=e(P_{Pub},C_1^*)e(P_{Pub},h'Q_i^*)e(Q_{TTP},C_2^*).$$

由以上两个等式可得 $e(W^*-W'^*,P)=e(P_{Pub},(h-h')Q_i^*)$, 从而可得 $abP=(W^*-W'^*)/(h-h')$. □

定理 4. 如果某个敌手$\mathcal{F}$在没有签署者和 TTP 的帮助下能够从基于身份的可验证加密签名中提取出签署者的普通签名,则存在算法$\mathcal{B}$能够利用$\mathcal{F}$求解 CDH 问题.

证明:下面我们说明算法$\mathcal{B}$如何利用敌手$\mathcal{F}$来求解 CDH 问题.给定算法$\mathcal{B}$一个 CDH 问题的实例(P,aP,bP),目的是利用敌手$\mathcal{F}$输出 abP.

Setup:$\mathcal{B}$随机选择 $k_a,k_b\in Z_q^*$,令 $P_{pub}=k_aaP$ 为 KGC 的公钥,令 $P_{TTP}=aP$,发送相关系统参数$(G_1,G_2,q,e,P,Q,P_{pub},H_1,H_2)$给$\mathcal{F}$.

$H_1(\cdot)$询问:为了回答预言 H_1 的询问,$\mathcal{B}$建立一个列表,记作 H_1-List,其中,元素形式为 (ID_i,Q_{ID_i},s_i). 当$\mathcal{F}$进行关于身份 ID_i 的 $H_1(\cdot)$预言询问时,$\mathcal{B}$检查 H_1-List 中是否存在 (ID_i,Q_{ID_i},s_i): 如果存在,则返回 Q_{ID_i}; 否则,随机选择 $s_i\in Z_q^*$,并返回 $Q_{ID_i}=H_1(ID_i)=s_iP$ 作为预言询问的回答.

$H_2(\cdot)$询问:为了回答预言 H_2 的询问,$\mathcal{B}$建立一个列表,记作 H_2-List,其中,元素形式为(m_i,C_{i1},C_{i2},h_i).当$\mathcal{F}$进行(m_i,C_{i1},C_{i2})的 $H_2(\cdot)$预言询问时,$\mathcal{F}$首先检查 H_2-List 中是否存在(m_i,C_{i1},C_{i2},h_i):如果存在,则返回 h_i;否则,随机选择 $h_i\in Z_q^*$,令 $H_2(m_i\|C_{i2},C_{i1})=h_i$,返回 h_i 作为预言询问的回答.

Extract 询问:当$\mathcal{F}$提交关于身份 ID_i 的 Extract 预言询问时,$\mathcal{B}$令 $D_i=s_iP_{pub}(D_i=s_ik_aaP=k_aaQ_i)$,并返回 D_i 作为$\mathcal{F}$询问的结果.

VES-Sign 询问:$\mathcal{F}$提交消息 m_i、签名者身份 ID_i 以及 TTP 的公钥 P_{TTP} 进行可验证加密签名预言询问,$\mathcal{B}$首先进行如下计算:

(1) 令 $C_{i2}=bP$;

(2) 随机选择 $h_i,\alpha\in Z_q^*$,计算 $C_{i1}=k_a^{-1}\alpha P-h_iQ_i-k_a^{-1}C_{i2}$;

(3) 令 $h_i=H_2(m_i\|C_{i2},C_{i1})$;

(4) 计算 $W_i=\alpha P_{TTP}$.

返回(W_i,C_{i1},C_{i2},m_i)作为可验证加密签名预言询问的结果.

Resolve 询问:当$\mathcal{F}$提交关于消息 m_i、签名者身份 ID_i 以及 TTP 的公钥 P_{TTP} 的可验证加密签名(W_i,C_{i1},C_{i2},m_i)进行争端解决预言询问时,$\mathcal{B}$进行如下计算:

(1) 首先询问关于身份 ID_i 的预言 Extract,获得 Q_{ID_i};

(2) 随机选择$\alpha\in Z_q$,并计算 $C'_{i1}=\alpha P$;

(3) 令 $V_i'=h_iD_i+\alpha P_{pub}$.

返回 (V_i',C'_{i1},C_{i2}) 作为争端解决预言询问的输出结果.

输出:最后,$\mathcal{F}$在已知签名者身份 ID^*以及 TTP 公钥 P_{TTP} 的情况下,从可验证加密签名 (W^*,C_1^*,C_2,m^*) 中提取

出签名 (V^*,C_1^*,C_2,m^*), 要求:(1) 未提交 (W^*,C_1^*,C_2,m^*) 进行争端解决预言询问;(2) 未提交 ID^*进行过 Extract 预言询问.

因此, (W^*,C_1^*,C_2,m^*) 和 (V^*,C_1^*,C_2,m^*) 满足上述条件,其中,$C_2=bP$,则有:

$$e(W^*,P)=e(P_{pub},hQ_i^*+C_1^*)e(C_2,P_{TTP}),$$

$$e(V^*,P)=e(P_{pub},hQ_i^*+C_1^*).$$

由以上两式可知,$e(P,W^*-V^*)=e(C_2,P_{TTP})=e(bP,aP)=e(P,abP)$,从而可得 $abP=W^*-V^*$. □

由定理 2~定理 4 可知,普通签名与可验证加密签名方案是不可伪造的.

定理 5. 代理签名方案与代理可验证加密签名方案是不可伪造的.

证明:由文献[26]中定理 1~定理 3 可知,如果存在某个敌手$\mathcal{F}$能够伪造代理合同签名,则存在算法$\mathcal{B}$能够利用$\mathcal{F}$求解 CDH 问题.如果存在敌手$\mathcal{F}$在没有签署者或 TTP 帮助下能够从代理可验证加密签名中提取出有效的代理合同签名,则存在算法$\mathcal{B}$能够利用$\mathcal{F}$求解 CDH 问题.

因此,合同签署协议中代理签名与代理可验证加密签名是不可伪造的(详细证明过程可参阅文献[26]). □

定理 6. 多元合同签署协议满足不可否认性.

证明:由定理 2~定理 4 可知,普通签名与可验证加密签名是不可伪造的;由文献[26]中的定理 1~定理 3 可知,代理签名与代理可验证加密签名是不可伪造的.因此,多元合同签署协议满足不可否认性. □

定理 7. 多元合同签署协议满足时效性.

证明:由详细协议具体执行过程可知,发起者首先发送(代理)可验证加密签名,且同时选择一个协议执行的有效期 T.因此,无论协议处于何种状态,在有效期 T 之后,协议都将结束.当签署者处于不公平情况时,可在 T 之前要求 TTP 执行取消子协议或争端解决子协议,以保证签署者公平性的情况下结束协议.因此,代理合同签署协议满足时效性. □

下面我们将讨论多元合同签署协议的公平性.为了方便讨论,我们不加区分地把参与协议签署的双方分别记作发起者和响应者,同时把可验证加密签名(VES)和代理可验证加密签名(PVES)统称为 VES,并将原始合同签名和代理合同签名称为合同签名.

定理 8. 多元合同签署协议满足公平性.

证明:下面分两个阶段讨论协议的公平性:阶段 1. 发起者已发送 VES 给响应者;阶段 2. 发起者已发送合同签名给响应者.

阶段 1. 发起者已发送 VES 给响应者.由协议的具体过程可知,响应者首先验证 VES 的有效性:如果无效,则响应者退出协议;否则,响应者将发送其有效 VES 给发起者.如果响应者收到发起者的有效 VES 之后,发送无效的 VES 或不发送 VES 给发起者,由定理 4 可知,响应者无法从 VES 中提取出有效的合同签名.因此,发起者可在等到 T 之后退出协议,也可要求 TTP 执行取消子协议结束签署协议.如果响应者想通过 TTP 执行争端解决子协议恢复发起者的合同签名,由争端解决子协议具体过程可知,响应者必须发送发起者的有效 VES 和自己的有效合同签名给 TTP.TTP 从中恢复出发起者的合同签名发送给响应者,同时把响应者的有效合同签名发送给发起者,以保证签署双方的公平性.因此,发起者发送有效 VES 给响应者之后,协议能够保证发起者和响应者在公平性的情况下结束协议.

阶段 2. 发起者发送合同签名给响应者.由协议的具体过程可知,发起者发送合同签名给响应者,此时可以认为发起者收到了响应者有效的 VES;否则,发起者将不会发送其合同签名给响应者.当响应者收到发起者合同签名后,首先验证其有效性:如果无效,则响应者要求 TTP 执行争端解决子协议恢复发起者的合同签名,保证其自身的公平性;如果有效,则响应者发送自己合同签名给发起者.然而,当响应者收到发起者的有效合同签名后,不发送其合同签名或发送无效合同签名给发起者.在这种情况下,发起者可要求 TTP 执行争端解决协议恢复响应者的合同签名,以保证自己的公平性.因此,当发起者发送其合同签名给响应者之后,协议能够保证发起者和响应者在公平性的情况下结束协议.

综上所述,多元合同签署协议满足公平性. □

4 VES 方案效率分析

表 1 所示为本文中新的 VES 方案与文献[15−17,19,23]中方案的效率对比.我们并未给出文献[23]中方案的计算量,该方案是无随机预言的 VES 方案,计算量较大.不失一般性,我们仅考虑最耗时的双线性对运算(记作 $\hat{e}$)与次耗时的标量乘法运算(记作 M).

Table 1 Efficiency comparison

表 1 效率对比

	签名	验证	VES 签名	VES 验证	仲裁
Zhang[15]	2M	$3\hat{e}$	3M	$3\hat{e}$	1M
Gu-Zhu[16]	$1\hat{e}+2$M	$2\hat{e}+1$M	$2\hat{e}+5$M	$3\hat{e}+1$M	$1\hat{e}+1$M
Zhang[17]	$1\hat{e}+2$M	$2\hat{e}+1$M	$2\hat{e}+4$M	$4\hat{e}+2$M	$1\hat{e}+1$M
Kwon-Lee[19]	$1\hat{e}+2$M	$2\hat{e}+1$M	$1\hat{e}+4$M	$3\hat{e}+1$M	$1\hat{e}+1$M
本文方案	3M	$2\hat{e}+1$M	4M	$3\hat{e}+1$M	1M

5 结束语

本文利用 Cha-Cheon 的基于身份的签名方案[24]设计了一个新的基于身份的可验证加密签名方案,并利用该方案和 Zhang 等人[26]提出的基于身份的代理可验证加密签名方案构造了多元合同签署协议.多元合同签署协议在消息交换过程中引入了 VES 和 PVES 来实现承诺的交换,并未使用复杂的零知识证明系统,有效避免了大量计算.VES 和 PVES 的可提取性保证在有争议发生时,TTP 能从中恢复出有效的合同签名,以保证用户的公平性.主签署协议由 3 个子签署协议组成,签署者可以是原始签署者或代理签署者.安全性分析表明,新的基于身份的可验证加密签名方案与代理可验证加密签名方案在随机预言模型中是可证安全的,因此协议满足不可否认性,同时还满足时效性和公平性.

致谢 非常感谢匿名评审专家对本文提出的建议.

References:

[1] Pagnia H, Gärtner FC. On the impossibility of fair exchange without a trusted third party. Technical Report, TUD-BS-1999-02, Darmstadt: Darmstadt University of Technology, Department of Computer Science, 1999.

[2] Goldreich O. A simple protocol for signing contracts. In: Chaum D, ed. Advances in Cryptology, Proc. of the CRYPTO'83. New York: Plenum Press, 1984. 133−136.

[3] Garay JA, Pomerance C. Timed fair exchange of standard signatures. In: Wright RN, ed. Proc. of the 7th Int'l Financial Cryptography Conf. (FC 2003). Berlin, Heidelberg: Springer-Verlag, 2003. 190−207. [doi: 10.1007/978-3-540-45126-6_14]

[4] Chen LQ, Kudla C, Paterson KG. Concurrent signatures. In: Cachin C, Camenisch J, eds. Advances in Cryptology, Proc. of the EUROCRYPT 2004. Berlin, Heidelberg: Springer-Verlag, 2004. 287−305.

[5] Liu JW, Sun R, Kyung-Sup K. Fair exchange signature schemes. Science China (Information Sciences), 2010,53(5):945−953. [doi: 10.1007/s11432-010-0065-1]

[6] Asokan N, Schunter M, Waidner M. Optimistic protocols for fair exchange. In: Reifer DJ, ed. Proc. of the 4th ACM Conf. on Computer and Communications Security. New York: ACM Press, 1997. 7−17. [doi: 10.1145/266420.266426]

[7] Ateniese G. Efficient verifiable encryption (and fair exchange) of digital signature. In: Motiwalla J, Tsudik G, eds. Proc. of the 6th ACM Conf. on Computer and Communications Security. New York: ACM Press, 1999. 138−146. [doi: 10.1145/319709.319728]

[8] Camenisch J, Damgård IB. Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes. In: Okamoto T, ed. Advances in Cryptology, Proc. of the ASIACRYPT 2000. Berlin, Heidelberg: Springer-Verlag, 2000. 331−345.

[9] Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham E, ed. Advances in Cryptology, Proc. of the EUROCRYPT 2003. Berlin, Heidelberg: Springer-Verlag, 2003. 416−432. [doi: 10.1007/3-540-39200-9_26]

[10] Garay JA, Jakobsson M, MacKenzie PD. Abuse-Free optimistic contract signing. In: Wiener MJ, ed. Advances in Cryptology—CRYPTO'99. Berlin, Heidelberg: Springer-Verlag, 1999. 449−466.

[11] Wang GL. An abuse-free fair contract-signing protocol based on the RSA signature. IEEE Trans. on Information Forensics and Security, 2010,5(1):158−168. [doi: 10.1109/TIFS.2009.2035972]

[12] Zhou YB, Zhang ZF, Qing SH, Ji QG. A fair exchange protocol based on RSA signature scheme. Journal of software, 2004,15(7): 1049−1055 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/1049.htm

[13] Xu J, Zhang ZF, Feng DG. Constructing optimistic ID-based fair exchange protocols via proxy signature. Journal of Software, 2007, 18(3):746−754 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/746.htm [doi: 10.1360/jos180746]

[14] Shao ZH. Fair exchange protocol of Schnorr signatures with semi-trusted adjudicator. Computers and Electrical Engineering, 2010, 36(6):1035−1045. [doi: 10.1016/j.compeleceng.2010.03.005]

[15] Zhang ZF, Feng DG, Xu J, Zhou Y. Efficient ID-based optimistic fair exchange with provable security. In: Qing SH, Mao WB, Lopez J, Wang GL, eds. Proc. of the 7th Int'l Conf. on Information and Communications Security. Berlin, Heidelberg: Springer-Verlag, 2005. 14−26. [doi: 10.1007/11602897_2]

[16] Gu CX, Zhu YF. An ID-based verifiable encrypted signature scheme based on Hess's scheme. In: Feng DG, Lin DD, Yung M, eds. Proc. of the 1st SKLOIS Conf. on Information Security and Cryptology. Berlin, Heidelberg: Springer-Verlag, 2005. 42−52. [doi: 10.1007/11599548_4]

[17] Zhang JH, Zou W. A robust verifiably encrypted signature scheme. In: Zhou XB, *et al*., eds. Proc. of the Emerging Directions in Embedded and Ubiquitous Computing, EUC 2006 Workshops: NCUS, SecUbiq, USN, TRUST, ESO, and MSA. Berlin, Heidelberg: Springer-Verlag, 2006. 731−740. [doi: 10.1007/11807964_74]

[18] Li XX, Chen KF, Liu SL, Li SQ. Verifiably encrypted signatures without random oracles. Journal of Shanghai Jiaotong University (Science), 2006,E-1(2):230−235.

[19] Kwon S, Lee SH. An efficient ID-based verifiably encrypted signature scheme based on Hess's scheme. In: Dawson E, Wong DS, eds. Proc. of the 3rd Information Security Practice and Experience Conf. (ISPEC 2007). Berlin, Heidelberg: Springer-Verlag, 2007. 93−104. [doi: 10.1007/978-3-540-72163-5_9]

[20] Xin XJ, Li G, Dong QK, Xiao GZ. An efficient randomized verifiably encrypted signature scheme. Acta Electronica Sinica, 2008, 36(7):1378−1382 (in Chinese with English abstract).

[21] Yang HM, Sun SX, Xu JY. Efficient verifiably encrypted signature scheme without random oracles. Journal of Software, 2009, 20(4):1069−1076 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/555.htm [doi: 10.3724/SP.J.1001.2009.00555]

[22] Rückert M, Schröder D. Security of verifiably encrypted signatures and a construction without random oracles. In: Shacham H, Waters B, eds. Proc. of the 3rd Int'l Conf. on Pairing-based Cryptography (Pairing 2009). Berlin, Heidelberg: Springer-Verlag, 2009. 17−34.

[23] Zhang L, Wu QH, Qin B. Identity-Based verifiably encrypted signatures without random oracles. In: Pieprzyk J, Zhang F, eds. Proc. of the 3rd Provable Security Conf. (ProvSec 2009). Berlin, Heidelberg: Springer-Verlag, 2009. 76−89. [doi: 10.1007/978-3-642-04642-1_8]

[24] Cha JC, Cheon JH. An identity-based signature from gap diffie−Hellman groups. In: Desmedt YG, ed. Proc. of the 6th Int'l Workshop on Theory and Practice in Public Key Cryptography (PKC 2003). Berlin, Heidelberg: Springer-Verlag, 2003. 18−30.

[25] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation. In: Gong L, Stearn J, eds. Proc. of the 3rd ACM Conf. on Computer and Communications Security (CCS 1996). 1996. 48−57. [doi: 10.1145/238168.238185]

[26] Zhang JH, Liu CL, Yang YX. An efficient secure proxy verifiably encrypted signature scheme. Journal of Network and Computer Applications, 2010,33(1):29−34. [doi: 10.1016/j.jnca.2009.07.003]

[27] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. In: Kilian J, ed. Advances in Cryptology, Proc. of the CRYPTO 2001. Berlin, Heidelberg: Springer-Verlag, 2001. 213−229.

[28] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. Journal of Cryptology, 2004,17(4):297−319. [doi: 10.1007/s00145-004-0314-9]

[29] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. Journal of Cryptology, 2000,13(3):361−396. [doi: 10.1007/s001450010003]

附中文参考文献:

[12] 周永彬,张振峰,卿斯汉,季庆光.基于 RSA 签名的优化公平交换协议.软件学报,2004,15(7):1049−1055. http://www.jos.org.cn/1000-9825/15/1049.htm

[13] 徐静,张振峰,冯登国.利用代理签名构造基于身份的优化公平交换协议.软件学报,2007,18(3):746−754. http://www.jos.org.cn/1000-9825/18/746.htm [doi: 10.1360/jos180746]

[20] 辛向军,李刚,董庆宽,肖国镇.一个高效的随机化的可验证加密签名方案.电子学报,2008,36(7):1378−1382.

[21] 杨浩淼,孙世新,徐继友.一种无随机预言机的高效可验证加密签名方案.软件学报,2009,20(4):1069−1076. http://www.jos.org.cn/1000-9825/555.htm [doi: 10.3724/SP.J.1001.2009.00555]

孙艳宾(1980－),男,河北石家庄人,博士,主要研究领域为协议分析,数字签名.

谷利泽(1965－),男,博士,副教授,主要研究领域为数字签名技术及应用.

卿斯汉(1939－),男,研究员,博士生导师,主要研究领域为信息系统安全理论和技术.

郑世慧(1979－),女,博士,讲师,主要研究领域为密码分析和设计.

杨义先(1961－)男,博士,教授,博士生导师,主要研究领域为密码学,网络安全.