混合可验证加密签名体制及应用

顾纯祥, 张亚娟, 祝跃飞
(河南郑州 1001信箱 770号, 信息工程大学信息工程学院, 河南郑州 450002)

摘 要: 在要求高效的密钥管理和中等的安全性的情况下, 基于身份公钥密码已成为代替基于证书的公钥密码的一个很好的选择. 本文在基于身份系统中, 引入少数几个采用公钥证书实体充当裁决者, 从而提出混合可验证加密签名的概念, 并在 Cheon基于身份签名体制的基础上, 构造了一个有效的混合可验证加密签名体制; 随后, 本文讨论了混合可验证加密签名体制的安全模型, 并在随机谕示模型下, 基于双线性映射的计算性 Diffie-Hellman问题难解性假设, 证明本文体制是可证安全的. 本文体制可用于构造基于身份的优化公平签名交换协议, 这在电子商务等领域有着广泛的应用.

关键词: 基于身份密码; 混合可验证加密签名; 双线性映射; 可证安全.
中图分类号: TP309, TN918 文献标识码: A 文章编号: 0372-2112 (2006) 05-0878-05

A Mixed Verifiably Encrypted Signature Scheme and It's Applications

GU Chun-xiang, ZHANG Ya-juan, ZHU Yue-fei
(School of Information Engineering, Information Engineering University, Zhengzhou, Henan 450002, China)

Abstract ID-based public key cryptography can be a good alternative for certificate-based public key setting, especially when efficient key management and moderate security are required. This paper proposes a primitive called mixed verifiably encrypted signature scheme (MVESS) and presents an efficient MVESS based on the ID-based signature scheme due to Cheon, *et al*. Then, we provide some theoretical discussions for the security model for MVESSs, and show that our new scheme can be proven to secure with the hardness assumption of the computational Diffie-Hellman problem of pairings in the random oracle model. Our new scheme can be used as blocks to build efficient ID-based optimistic fair signature exchange protocols, which can be widely used in signing digital contracts, e-payment and other electronic commerce.

Key words ID-based cryptography; mixed verifiably encrypted signatures; bilinear maps; provable security

1 引言

早在 1984年, Shamir[1]就提出基于身份密码体制的思想: 将用户公开的身份信息 (如 e-mail地址、IP地址、名字等等) 作为用户公钥/私钥对的公钥部分, 用户私钥由一个称为私钥生成者 (PKG) 的可信第三方生成. 相对 PKI/CA技术, 基于身份的密码体制无须公钥证书的管理与鉴别, 在应用中带来极大的便利. 近年来, 随着双线性映射和相关计算问题的提出, 以及椭圆曲线上 Weil对和 Tate对在其中的成功应用[3], 基于身份的密码体制研究获得了长足的发展. 一方面, 新的各种基于身份的加密、签名体制[2~4]纷纷出台, 另一方面, 其安全性证明理论也日趋成熟. 在一些安全的基于身份签名体制的基础上, 人们又设计了一些具有一定应用背景的新的密码体制, 如基于身份盲签名、基于身份代理签名、基于身份环签名等等.

可验证加密签名体制是一种特殊的数字签名体制, 其核心思想是: 用户 A可以向用户 B发送利用可信第三方 (TTP)公钥加密过的加密签名, B可以验证加密签名的有效性, 但在没有 TTP帮助的情况下, B得不到原始签名. 可验证加密签名体制可以用来构造一些公平签名交换协议, 这在电子合同、电子支付等电子商务领域有着广泛的应用. 近年来, 可验证加密签名体制的构造[5~7], 以及以可验证加密签名为核心的公平签名交换协议[5,8,9]的研究, 成为当前学术界研究的热点之一.

本文提出混合可验证加密签名的概念, 并在文献 [2] 中基于身份签名体制的基础上, 构造了一个可证安全的混

收稿日期: 2005-06-20; 修回日期: 2005-12-30
基金项目: 国家自然科学基金 (No. 90204015, No. 60473021); 国家 973重点基础研究发展规划 (No. G1999035804)

合可验证加密签名体制. 本文第二节对新体制进行了详细描述, 并分析了其效率; 第三节讨论了混合可验证加密签名体制的安全模型, 对新体制进行了严格的安全性证明; 第四节以本文体制为核心组件, 提出了一个优化的公平签名交换协议; 文章最后对全文进行了总结.

2　一个新的混合可验证加密签名体制

在实际应用中, 一个系统的裁决者通常是由若干相对固定的主体来承担, 且数目较少. 此时, 可以为这些充当裁决者的主体选取普通的公钥、私钥对, 并由可信的权威机构签发公钥证书, 而系统中其他普通用户仍采用基于身份的密钥. 由于裁决者数目较少, 系统仍然具有高效密钥管理的优势.

基于这一实际应用背景, 本文提出混合可验证加密签名体制的概念. 所谓“混合可验证加密签名”, 是指对基于身份的数字签名, 采用传统的基于证书的裁决者公钥进行可验证加密. 混合可验证加密签名提供了对基于身份密码系统中, 可验证加密签名及公平交换问题的另一种有效的解决途径.

2.1　双线性映射及计算性 Diffie-Hellman 问题

设 $(G_1, +)$和 $(G_2, \cdot)$, 分别为 q阶的加法循环群和乘法循环群. 若映射 $\hat{e}: G_1 \times G_1 \to G_2$ 具有如下性质:

(1)双线性: 对所有 $P, Q \in G_1$, $\alpha, \beta \in Z_q^*$, 满足 $\hat{e}(\alpha P, \beta Q) = \hat{e}(P, Q)^{\alpha\beta}$;

(2)非退化性: 对 G_1的生成元 P, $\hat{e}(P, P)$是 G_2的生成元;

(3)可计算性: 对任意的 $P, Q \in G_1$, 存在有效算法计算 $\hat{e}(P, Q)$,

则称 $\hat{e}$为可用的(admissible)[3]双线性映射. 利用椭圆曲线上的 Weil对或 Tate对便可构造可用的双线性映射.

设 P是 G_1的生成元, $a, b \in Z_q^*$. 考虑这样一个的数学问题: 输入 $P, aP, bP \in G_1$, 如何计算 abP? 该问题被称为计算性 Diffie-Hellman 问题(CDHP). 目前, 具有可用的双线性映射的群上, CDHP是公认的数学难题.

2.2　新体制描述

最近, JH Cheon, Y K im和 H J Yoon[2]提出了一个基于身份的签名体制(CKY 体制), 并证明了其安全性. 基于 CKY 体制, 本文构造了一个有效的混合可验证加密签名体制, 称之为 M ix-VESS, 由如下的多项式时间算法组成:

Setup: 参数生成算法, 由 *PKG* 完成. 输入安全参数 $k \in N$, 输出系统参数 para= $(G_1, G_2, q, \hat{e}, P, P_{pub}, H_1, H_2)$和系统主密钥 $s \in Z_q^*$, 其中 $P_{pub} = sP$, $H_1: \{0,1\}^* \to G_1^*$ 和 $H_2: \{0,1\}^* \times G_1 \to Z_q^*$ 为 *Hash* 函数.

Extract 私钥解析算法, 由 *PKG* 完成. 输入用户身份 $ID \in \{0,1\}^*$, *PKG* 计算 $Q_{ID} = H_1(ID)$, $D_{ID} = sQ_{ID}$, 以 D_{ID}作为用户私钥并通过安全信道传送给用户.

Adj_KGen: 裁决者密钥生成算法, 输入系统参数 para 随机选取 $s_A \in Z_q^*$, 计算 $P_A = s_A P$, 以 s_A 作为裁决者私钥, P_A 作为裁决者公钥.

Sign: 签名算法, 输入私钥 D_{ID}和消息 m, 随机选取 $r \in Z_q^*$, 计算 $U = rP$, $h = H_2(m, U)$, $V = rQ_D + hD_{ID}$. 输出 (U, V)作为对 m的签名.

Verify: 签名的验证算法, 验证者收到签名 (m, U, V), 计算 $h = H_2(m, U)$, 验证者接受签名, 当且仅当 $\hat{e}(P, V) = \hat{e}(U + hP_{pub}, H_1(ID))$.

VE_Sign: 可验证加密签名算法, 输入私钥 D_{ID}消息 m和裁决者公钥 P_A, 随机选取 $r_1, r_2 \in Z_q$, 计算 $U_1 = r_1 P$, $h = H_2(m, U_1)$, $U_2 = r_2 P$, $V = r_1 Q_{ID} + hD_{ID} + r_2 P_A$. 输出 (U_1, U_2, V)作为对 m的可验证加密签名.

VE_Verify: 可验证加密签名的验证算法, 验证者收到 m的可验证加密签名 (U_1, U_2, V)后, 计算 $h = H_2(m, U_1)$, 验证者接受签名, 当且仅当:

$$\hat{e}(P, V) = \hat{e}(U_1 + hP_{pub}, H_1(ID))\,\hat{e}(U_2, P_A).$$

Adjudicate 裁决算法, 由 *PKG* 完成. 输入裁决私钥 s_A, 签名者身份 ID, 消息 m及相应有效可验证加密签名 (U_1, U_2, V), 计算 $V_1 = V - s_A U_2$, 输出对 m 的普通数字签名 (U_1, V_1).

注: 该体制的算法组中, (Setup, Extract, Sign, Verify)组成了文献[2]中的基于身份签名体制.

2.3　效率分析

从可验证加密签名的构造上看, 以交互式零知识证明方式实现, 一般需要多次数据通信及模指数运算[5,8], 本文体制的签名过程和验证过程无需任何数据通信. 最近, D Boneh[6]和 A Nenadic[7]分别提出了非交互的可验证加密签名体制. 对基于双线性映射的体制, 记 M 为 $(G_1, +)$中标量乘法, $\hat{e}$为双线性映射 $\hat{e}(\cdot, \cdot)$的计算; 对基于 RSA的体制, 记 Exp为模指数运算, 忽略其它计算的耗费, 本文体制和文献[6, 7]的效率比较如下:

	VE_Sign	*VE_Verify*	*Adjudicate*
本文体制	5M	3$\hat{e}$+ 1M	1M
Boneh[6]	3M	3$\hat{e}$	1M
Nenadic[7]	6Exp	2Exp	1Exp

和 Boneh体制相比, 本文体制效率略低(增加了 1至 2个 $(G_1, +)$中标量乘法, 但决定效率的关键运算——$\hat{e}(\cdot, \cdot)$运算的次数并没有增加, 而且本文体制中的标量乘法可以通过预运算来提高效率). 同 Nenadic体制相比, 本文体制可利用椭圆曲线点群及其 Weil对或 Tate对来实现, 这将具有一定的效率和带宽的优势[10]. 此外, Boneh体制和 Nenadic体制都是完全基于公钥证书的, 对公钥证书的有效性验证将带来可观的计算量和开销; 而在混合系统中, 只有少量的裁决者采用证书, 主体用户采用基于身份的密码, 因此系统将具有密钥管理方面的明显优势. 当然, 基于身份的密码具有密钥托管问题, 即 PKG 知道用户的私钥, 这一不足可以通过门限密码的方法在一定程度上得以

弥补.

3 安全模型及 Mix-VESS的安全性证明

安全性是密码体制设计所应考虑的一个核心问题. 文献[6]提出可验证加密签名体制除了基本签名体制的安全性要求以外, 还应满足:

(1)可验证加密签名的不可伪造性: 伪造一个新的可验证加密签名是困难的.

(2)不透明性(opacity): 由对消息 m 的可验证加密签名得到对 m 的普通签名是困难的.

本文对[6]中的安全模型作了进一步扩展, 建立了混合可验证加密签名体制的安全模型, 并证明了本文体制的安全性.

3.1 正确性分析

作为一个有效的可验证加密签名体制, 首先应满足正确性要求. Mix-VESS的正确性可验证如下: 对任意的消息及相应可验证加密签名 $(m, (U_1, U_2, V))$,

$$\begin{aligned}\hat{e}(P, V) &= \hat{e}(P, r_1H_1(ID) + hD_{ID} + r_2P_A)\\ &= \hat{e}(P, r_1H_1(ID) + hD_{ID}) \cdot \hat{e}(P, r_2P_A)\\ &= \hat{e}((r_1 + hs)P, H_1(ID)) \cdot \hat{e}(r_2P, P_A)\\ &= \hat{e}(U_1 + hP_{pub}, H_1(ID)) \cdot \hat{e}(U_2, P_A)\end{aligned}$$

从而有: $VE\_Verify(ID, m, P_A, (U_1, U_2, V)) = 1$.

另一方面, $V_1 = V - s_AU_2 = V - r_2P_A = r_1H_1(ID) + hD_{ID}$.

$$\begin{aligned}\hat{e}(P, V_1) &= \hat{e}(P, r_1H_1(ID) + hD_{ID})\\ &= \hat{e}(U_1 + hP_{pub}, H_1(ID))\end{aligned}$$

即: $Verify(ID, m, Adjudicate(s_A, ID, m, (U_1, U_2, V))) = 1$.

3.2 可验证加密签名的不可伪造性

定义 1 混合可验证加密签名体制称为自适应选择消息、身份和裁决签名攻击下存在性不可伪造的(EUF-ACMISA), 如果对任意的概率多项式时间的攻击者 F和挑战者 C, F赢得下面试验的概率是可以忽略的:

(1)挑战者 C运行 $Setup(1^k)$, 生成的系统参数 $para$; 运行 $Adj_KGen(para)$生成裁决者密钥对 (P_A, s_A), 以 $(para, P_A, s_A)$作为 F的输入;

(2)F可以自适应的访问以下谕示:

Extract谕示 $E(\cdot)$: 对输入 ID, 该谕示解析出相应私钥 D_{ID}, D_{ID}以作为应答;

VE_Sign谕示 $VS(\cdot)$: 对输入用户身份 ID、消息 m, 该谕示返回以 D_{ID}为私钥对 m 的可验证加密签名 p.

Adjudicate谕示 $A(\cdot)$: 输入用户身份 ID、消息 m 以及可验证加密签名 p, 该谕示执行裁决算法并返回相应普通签名.

注 1 这里没有考虑攻击者访问普通签名谕示 $Sign(\cdot)$的能力, 因为 $Sign(\cdot)$可通过访问 $VS(\cdot)$和 $A(\cdot)$来模拟.

注 2 在随机谕示模型下, 攻击者还具有访问相应随机谕示的能力.

(3)F输出 (ID, m, p), 满足 ID 不曾作为 $E(\cdot)$谕示的输入, (ID, m)不曾作为 $VS(\cdot)$谕示和 $A(\cdot)$谕示的输入. 若 p是 ID 对 m 的有效可验证加密签名, 则 F赢得试验.

在安全性定义中, 攻击者 F在拥有 ID 对 m 的签名或可验证加密签名的条件下, 伪造出相同的 ID 对 m 的可验证加密签名, 并不被看作成功的伪造(此时, F以 (ID, m)访问过 $VS(\cdot)$谕示或 $A(\cdot)$谕示). 在实际中, 这样的伪造并不能形成 ID 对新消息 m 的签名或可验证加密签名.

定理 1 假设在随机谕示模型下, 存在 ACMISA攻击者 F_0, 在时间 T内, 对 Mix-VESS以概率 ε存在性可验证加密签名伪造成功, 则存在 ACMIA攻击者 F_1, 在与 T相当的时间内, 以不低于 ε的概率, 对 CKY体制存在性伪造攻击成功.

证明: 由 F_1 可以如下构造 CKY体制的 ACMIA攻击者 F_1:

(1)挑战者 C运行 CKY体制的初始化算法 $Setup(1^k)$, 以系统参数 $para$作为 F_1的输入.

(2)F_1 运行 $Adj\_KGen(para)$, 生成裁决者密钥对 (P_A, s_A).

(3)F_1 以 $(para, P_A, s_A)$为 F_0 的输入并调用 F_0, 如下模拟 F_0的各个谕示:

Hash函数谕示 $H_1(\cdot)$和 $H_2(\cdot)$: 对 F_0 的访问请求, F_1 以该请求的输入作为输入访问自己的相应 Hash函数谕示 $H_1(\cdot)$或 $H_2(\cdot)$, 并以所得到的应答作为对 F_0 的应答;

谕示 $E(\cdot)$: 对输入 ID, F_1 以 ID 作为输入访问自己的私钥解析谕示 $E(\cdot)$, 并以所得到的应答作为对 F_0 的应答;

谕示 $VS(\cdot)$: 对输入身份 ID和消息 m, F_1以 (ID, m)作为输入输入访问自己的签名谕示 $Sign(\cdot)$, 设得到应答为 (σ_1, σ_2), 随机选取 $r \in Z_q^*$, 以 $(\sigma_1, rP, \sigma_2 + rP_A)$作为对 F_0 的应答;

谕示 $A(\cdot)$: 输入用户身份 ID、消息 m 以及可验证加密签名 (U_1, U_2, V), F_1 以 $(U_1, V - s_AU_2)$作为应答.

(4)F_0 输出 $(ID, m, (U_1, U_2, V))$, 则 F_1 可输出 $(ID, m, (U_1, V_1))$, 其中 $V_1 = V - s_AU_2$.

若 F_0 的输出 $(ID, m, (U_1, U_2, V))$满足: ID 不曾作为 $E(\cdot)$谕示的输入, (ID, m)不曾作为 $VS(\cdot)$谕示和 $A(\cdot)$谕示的输入, 且 (U_1, U_2, V)是 ID 对 m 的有效可验证加密签名, 则 F_1可输出 $(ID, m, (U_1, V_1))$, 满足: ID 不曾作为 $E(\cdot)$谕示的输入, (ID, m)不曾作为 $Sign(\cdot)$谕示的输入, 且 (U_1, V_1)是 ID 对 m 的有效普通数字签名. 可见, 攻击者 F_1 成功的概率不低于攻击者 F_0 赢得试验的概率, 定理证明完毕.

3.3 可验证加密签名的不透明性

定义 2 混合可验证加密签名体制称为自适应选择消息、身份和裁决签名攻击下不透明的(OPA-ACMISA), 如果对任意的概率多项式时间的攻击者 F和挑战者 C, F赢得下面试验的概率是可以忽略的:

(1)挑战者 C运行 $Setup(1^k)$, 生成的系统参数 $para$; 运行 $Adj\_KGen(para)$, 生成裁决者密钥对 (P_A, s_A), 以 $(para, P_A)$作为 F的输入;

(2)F可以自适应的访问以下谕示: Extract谕示$E(\cdot)$、VE_Sign谕示 $VS(\cdot)$和 Adjudicate谕示 $A(\cdot)$, 在随机谕示模型下, F还具有访问相应随机谕示 $H_1(\cdot)$和 $H_2(\cdot)$的能力.

(3)F输出(ID, m, p, δ), 满足: ID 不曾作为 $E(\cdot)$谕示的输入, $(ID, m, \cdot)$不曾作为谕示 $A(\cdot)$的输入. 若 p和 δ分别是身份为 ID的用户对 m 的有效可验证加密签名和普通签名, 且以 (ID, m, p)访问谕示 $A(\cdot)$得到的应答为 δ则 F赢得试验.

注: 在定义中, 为保证 F的输出不是平凡的, 要求 F不曾以$(ID, m, \cdot)$访问过谕示 $A(\cdot)$, 但和定义 1不同, 这里 F可以以 (ID, m)访问谕示 $VS(\cdot)$.

定理 2　假设在随机谕示模型下, 存在 ACMISA攻击者 F_0, 在时间 T 内, 对 Mk-VESS以不可忽略的概率 ε赢得透明性试验, 记 F_0 访问谕示 $H_1(\cdot)$和 $VS(\cdot)$的次数分别为 n_{h1}和 n_{VS}, 则存在多项式时间的图灵机 F_1, 任意输入 $P, aP, bP \in G_1$, 在预期与 T 相当的时间内, 以概率 $\varepsilon/(n_{h1}n_{VS})$成功输出 abP.

证明: 不失一般性, 假设对任意的 ID, F_0 在以 ID 作为输入(或部分输入)访问谕示 $E(\cdot)$、$VS(\cdot)$以及 $A(\cdot)$之前, 一定以 ID 访问过谕示 $H_1(\cdot)$. 由 F_0可如下构造求解 CDHP的多项式时间概率图灵机 F_1:

(1)挑战者 C调用可接纳双线性映射的参数生成器生成 $(G_1, G_2, q, \hat{e})$, 随机选取 $P, aP, bP \in G_1$, 以 $(G_1, G_2, q, \hat{e}, P, aP, bP)$作为 F_1 的输入.

(2)F_1 选取 Hash函数 $H_1: \{0,1\}^* \to G_1^*$ 和 $H_2: \{0,1\}^* \times G_1 = Z_q^*$; 随机选取 $s \in Z_q^*$, $P_{pub} = sP$, 令系统参数 $para = (G_1, G_2, q, \hat{e}, P, P_{pub}, H_1, H_2)$.

(3)F_1 随机选取 t和 z满足 $1 \leqslant t \leqslant n_{h1}$, $1 \leqslant z \leqslant n_{VS}$. 随机选取 $x_i \in Z_q^*$, $i = 1, 2, \ldots, n_{h1}$. 令 $v = 1$, $j = 1$ $P_A = lP$, VS_{list}为空.

(4)F_1 以 $(para, P_A)$作为 F_0 的输入并调用 F_0, 如下模拟 F_0 的各个谕示:

$H_1(\cdot)$: 对输入 ID, F_1 检查 $H_1(ID)$是否已定义. 若没有, 定义 $H_1(ID) = \begin{cases} \mu lP, & v = t \\ x_i P, & v \neq i \end{cases}$ 其中, $\mu \in_R Z_q^*$, 令 $ID_V \leftarrow ID$, $v \leftarrow v+1$. F_1 以 $H_1(ID)$作为对 F_0 的应答.

$H_2(\cdot)$: 对输入 (m, U), F_1 检查 $H_2(m, U)$是否已定义, 若没有, 随机选取 $h \in Z_q^*$, 定义 $H_2(m, U) = h$. F_1 以 $H_2(m, U)$作为对 F_0 的应答.

$E(\cdot)$: 对输入 ID_i, 若 $i = t$, F_1 令 $D_i = s\mu bP$; 否则, 令 $D_i = x_i P_{pub}$. 以 D_i 作为对 F_0 的应答.

$VS(\cdot)$: 对输入用户身份 ID_i 和消息 m,

(a)若 $i = t, j = z$ 随机选取 $r, h \in Z_q^*$, 计算 $U_1 = aP - hP_{pub}$, $U_2 = \mu(lP - aP)$, $V = \mu rlP$, 并将 $(i, j, \cdot, U_1, U_2, V)$添加到 VS_{list}中;

(b)否则, 随机选取 $r, y_j, h \in Z_q^*$, 计算 $U_1 = y_j P - hP_{pub}$, $U_2 = rP$, $V = y_j H_1(ID_i) + rP_A$, 并将 (i, j, r, U_1, U_2, V)添加到 VS_{list}中.

若 $H_2(m, U_1)$已定义, 则终止(发生了冲突); 否则, 令 $H_2(m, U_1) = h$, $j \leftarrow j+1$ 以 (U_1, U_2, V)作为该谕示的应答.

$A(\cdot)$: 输入 ID_i, 消息 m 及有效可验证加密签名 (U_1, U_2, V), 查询 VS_{list}获取相应项 (i, j, r, U_1, U_2, V)(或 $(i, j, \cdot, U_1, U_2, V)$), 由定理 1, 可验证加密签名是存在性不可伪造的, 因此, (U_1, U_2, V)一定在 VS_{list}列表中. 若 $i = t$且 $j = z$, F_1 失败并终止; 否则, 计算 $V_1 = V - rP_A$, 应答为 (U_1, V_1).

(5)若 F_0 输出 (ID_i, m, p, δ), F_1 查询 VS_{list}, 获取相应项 (i, j, r, p)或 $(i, j, \cdot, p)$, 若 $i \neq t$或 $j \neq z$, F_1 失败并终止; 否则, 设 $\delta = (U_1, V_1)$, F_1 可计算并成功输出 $abP = \mu^{-1}V_1$.

F_1 对 F_0的各谕示的模拟中, $H_2(m, U_1)$定义冲突只可能出现在攻击者已经以 (m, U_1)访问过 $H_2(\cdot)$谕示, 或两次 $VS(\cdot)$生成相同的 U_1. 在谕示 $VS(\cdot)$的模拟中, 由于 h 是随机选取的, F_1 因 $H_2(m, U_1)$发生冲突而终止的概率是可以忽略的. 若 F_0 攻击成功, 输出 (ID, m, p, δ), VS_{list}中相应项为 $(t, z, \cdot, p)$, 则 $\mu^{-1}V_1 = \mu^{-1}\mu abP = abP$. 由于 F_0 攻击成功, ID_t 不曾作为 $E(\cdot)$谕示的输入且 (ID_t, m)不曾作为 $A(\cdot)$谕示的输入, 因而 F_1 对 F_0 的各谕示的模拟的输出与 F_0 的各谕示的输出具有相同的概率分布.

在攻击过程中, 因为 t和 z是随机选取的, 因此成功计算并输出 abP 的概率为 $\varepsilon/(n_{h1}n_{VS})$. 定理证明完毕.

4　应用——基于身份的公平签名交换协议

在 Internet飞速发展的今天, 如何通过网络, 在两个互不信任的主体之间公平高效的交换数字签名, 是实现电子合同签署等电子商务活动面临的必须合理解决的问题之一. 所谓"公平"是指参与交换签名协议的双方, 在协议结束后, 要么任何一方都可以得到对方的有效签名, 要么双方都得不到对方的有效签名. 由于应用的广泛性, 公平签名交换协议一直是密码学研究中的一个热门课题.

混合可验证加密签名体制提供了基于身份密码系统中公平签名交换问题的另一种有效的解决途径. 利用上文构造的混合可验证加密签名体制, 可以设计出有效的优化公平签名交换协议.

4.1　协议描述

设 Alice和 Bob的身份分别为 ID_A 和 ID_B, 私钥分别为 D_A 和 D_B. Alice希望和 Bob公平的交换对消息 m 的签名. 可信第三方 TTP(裁决者)的公钥为 P_T(由某 CA中心颁发的公钥证书 $Cert_T$ 来保证其有效性), 私钥为 s_T. 协议的描述如下:

签名交换:

Step1　Alice 计算可验证加密签名 $p_A = VE\_Sign(D_A, m, P_T)$, 并将 (m, p_A)发送给 Bob

Step2: Bob 检验 (m, p_1) 的有效性, 若 $VE\_Verify(ID_A, m, P_T, p_1) \neq 1$, 则终止; 否则, Bob计算签名 $\delta_2 = Sign(D_B, m)$, 并将 δ_2 发送给 Alice.

Step3: Alice检验签名 δ_2 的有效性, 若 $Verify(ID_B, m, \delta_2) \neq 1$, 则终止; 否则, Alice计算签名 $\delta_1 = Sign(D_A, m)$, 并将 δ_1 发送给 Bob.

Step4: 若 Bob收到 δ_1, 且 $Verify(ID_A, m, \delta_1) = 1$, 则协议成功结束; 否则, Bob可以向可信第三方提请裁决.

裁决子协议:

Step1: Bob将 (m, p_1) 和发送给 TTP.

Step2: TTP 验证 p_1 和 δ_2 的有效性, 若 $VE\_Verify(ID_A, m, P_T, p_1) \neq 1$ 或 $Verify(ID_B, m, \delta_2) \neq 1$, 则终止; 否则, TTP 计算 $\delta_1 = Adjudicate(s_T, ID_A, m, p_1)$, 将 δ_1 发送给 Bob, 同时将 δ_2 发送给 Alice.

注: m 中应包含交换双方的身份 $(ID_A$ 和 $ID_B)$, 以确保只有 Bob才可以提请裁决.

4.2 公平性

本文协议可实现签名交换的公平性. 交换过程中, 在 Setp1结束时, 若 Alice向 Bob发送了有效的 p_1, 而没有收到 Bob发来的有效的签名 δ_2, 由于 Bob独自由 p_1 无法得到 δ_1, p_1 对 Bob没有价值, 双方都得不到对方得签名; 若 Bob以 (m, p_1) 和 δ_2 提交 TTP请求争端解决, TTP在验证 p_1 和 δ_2 有效性基础上, 计算 $\delta_1 = Adjudicate(s_T, ID_A, m, p_1)$; 并将 δ_1 发送给 Bob, 同时将 δ_2 发送给 Alice, 这样双方都可得到对方的有效签名. 在 Setp2或 Step3结束时, 若 Bob向 Alice发送了有效的 δ_2, 而没有收到 Alice发来的有效的签名 δ_1, Bob可以向 TTP请求裁决, 其结果是双方都得到对方的有效签名.

4.3 优化性 (optimistic)

在本协议中, TTP是工作在优化的方式. 即在正常情况下 (双方严格按签名交换协议执行, 没有争议发生), TTP并不参予双方的交换, 只是在争议发生时卷入协议来保证公平性. 在没有争议发生时, 协议的参予方只有 Bob和 Alice.

5 结论

可验证加密签名体制是构造公平签名交换协议的有效工具. 本文提出了一个有效的混合可验证加密签名体制, 并在随机谕示模型下, 基于 CDH假设, 证明了本文体制的安全性; 在此基础上, 以新体制为核心组件, 本文提出了一个基于身份的优化公平签名交换协议;

本文体制的可验证加密签名和验证算法, 以及协议中参与签名交换的双方都是使用基于身份的密码, 无需公钥证书的支撑, 从这个意义上讲, 本文体制和协议是基于身份的. 但严格的说, 基于身份的可验证加密签名方案应该是参与三方都是使用基于身份的密码体制, 而本文体制裁决方的密钥并非基于身份的. 如何在 Adjudicate的研究上取得突破, 将是进一步工作的方向.

参考文献:

[1] A Shamir. Identity-based cryptosystems and signature schemes[A]. In Proc Crypto'84[C]. LNCS 196, Springer-Verlag, 1984. 47-53.

[2] JH Cheon, Y Kim, H J Yoon. Batch verifications with ID-based signatures[A]. Proc ICISC'2004[C]. LNCS 3506, Springer-Verlag, 2005. 233-248.

[3] D Boneh, M Franklin. Identity-based encryption from the Weil pairing[A]. In Proc Crypto'2001[C]. LNCS 2139, Springer-Verlag, 2001. 213-229.

[4] JC Cha, JH Cheon. An identity-based signature from gap Diffie-Hellman groups[A]. In Proc PKC'2003[C]. LNCS 2567, Springer-Verlag, 2003. 18-30.

[5] N Asokan, V Shoup, M Waidner. Optimistic fair exchange of digital signatures[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 593-610.

[6] D Boneh, C Gentry, B Lynn, H Shacham. Aggregate and verifiably encrypted signature from bilinear maps[A]. In Proc, Eurocrypt'2003[C]. LNCS 2248, Springer-Verlag, 2003. 514-532.

[7] A Nenadic, N Zhang, B Cheetham, C Goble. An RSA-based security protocol for certified E-goods delivery [A]. Proc IEEE ITCC'2004[C]. IEEE Computer Society, 2004. 22-28.

[8] J Camenisch, V Shoup. Practice verifiable encryption and decryption of discrete logarithms[A]. Proc Crypto2003 [C]. LNCS2729, Springer-Verlag, 2003. 195-211.

[9] 李梦东, 杨义先, 马春光, 蔡满春. 利用双线性聚集签名实现公平的签名交换方案[J]. 通信学报, 2004, 25 (12): 59-64.

[10] P S L M Barreto, H Y Kim, M Scott. Efficient algorithms for pairing-based cryptosystems[A]. In Proc Crypto' 2002, LNCS 2442[C]. Springer-Verlag, 2002. 354-368.

作者简介:

顾纯祥 男, 1976年出生于安徽霍山, 信息工程大学博士研究生, 信息工程大学信息工程学院网络工程系教员, 主要研究方向为密码学与信息安全.
E-mail: gcxiang5209@yahoo.com.cn

祝跃飞 男, 1962年出生于浙江杭州, 信息工程大学信息工程学院教授, 博士生导师, 主要研究方向为密码学与信息安全.