一种基于身份的在线交易支付安全协议框架*)

陈 舜 姚 前 谢 立
(南京大学软件新技术国家重点实验室 南京 210008)

摘 要 利用椭圆曲线GDH群上的双线性,构建了一种基于身份的三方弱型签密协议,提供密文鉴别、报文机密、签名非否认等安全特性,摆脱了PKI体系的约束,提高了计算效率,为在线交易和支付提供一种安全高效的一体化解决方案。

关键词 身份,在线交易,电子支付,安全协议

Online Transaction and Payment Security Scheme Based on ID

CHEN Shun YAO Qian XIE Li
(The National Key Laboratory of New Software Technology, Nanjin University, Nanjin 210008)

Abstract Using the bilinear property of pairing on the elliptic GDH group, a 3- party weak signcryption scheme based on ID is proposed. It getts ride of the restriction of PKI system and surpasses the traditional one to one identification model having the securities such as cyphertext identification, message confidentiality, signature nonrepudiation, with high efficiency of computation, thereby providing a kind of integration solution for the online transaction and payment.

Keywords Identification, Online transaction, Electronic payment, Security scheme

交易和支付的安全性,作为电子商务的瓶颈,一直未找到有效的解决方案。过去几年,在交易安全方面,试图利用CA证书,实现身份认证[1],但未取得预期效果。其原因一是CA并不能提供实质上的安全性[2];二是PKI体系成本高,在大范围内实现高效的相互认证十分困难[3];三是效率低,交易和支付指令十分简短,而CA证书过长,严重影响处理效率。在支付安全方面,也没有大的突破[4]。电子钱包、电子支票、电子货币等方式,只能用于小额支付,不能用于大额结算[5]。万事达、微软等6大企业专门为信用卡支付开发的安全电子交易(Secure Electronic Transaction,SET)协议,需要专用系统,始终未得普及[6]。近5年来,电子支付没有太大的进展[7]。电子商务涉及多个主体,现实中的安全方案往往是在主体间两两解决的,交易和支付是分开考虑的,这就不可避免地增加了复杂性,降低了可用性。寻求不基于CA的、高效的、一体化的安全交易与支付方案,是目前业界共同关心的问题。

1 基于身份的密码体制

为了摆脱CA的限制,早在1984年,Shamir就提出了基于身份(ID)的签名体制[8],但基于ID的加密体制一直是公开问题,这就使得构建基于ID的安全协议十分困难。差不多在同一时期,Miller和Kobliz发现,定义在有限域上的椭圆曲线上的点构成的群上,离散对数的计算要困难得多。也就是说,对Diffie-Hellman问题的攻击要困难得多。这意味着建立在这类群上的加密体制,使用的密钥要小得多,加密效率可以大大提高[9]。

以上两个方面如果能结合在一起,不就能提供基于ID的高效、安全体制了吗?2000年,希望终于出现了。这一年,Joux发现,椭圆曲线群上双点映射(Pairing)的双线性(Bilinear)特征,可应用于密钥交换中[10]。也是在这一年,Sakai等人发现,双线性特征也可应用于签名[11]。2001年,Boneh和Franklin发现,这种双线性还可以用于构建基于ID的加密协议(BF协议)[12],使得自1984年以来一直存在的公开问题得以解决。2002年,Cha和Cheon设计了一个完整的基于双线性的方案,在安全性上达到了一般性的要求(CC协议)[13]。

这样一来,基于ID的密码体制就有了基础。其中一个重要的方向,是签密(Signcryption)协议的发展。以前的方案中,签名和加密是分开进行的。1997年Zheng提出,在一个逻辑步骤中,同时完成签名与加密,可以有效节约开销,这就是签密的概念[14]。2002年,Malone-lee将Zheng的签密概念用于ID环境下的安全体制中,第一次提出了基于ID的签密方案[15]。此后,Libert和Quisquater的方案[16]、Lynn的方案[17]、Nalla和Reddy的方案[18]虽然在完整性、鉴别性等方面各有所长,但都是仅限于两个主体间的协议。

2 三方间基于身份的签密方案

能否将以上的新思路应用到在线交易与支付中来呢?在这种环境下,涉及到3个主体:客户(Client)、银行(Bank)和商家(Agent),如图1所示。涉及到交易和支付两类业务,需要综合考虑。

2.1 弱签密概念

电子商务中,为了提供强不可否认性,必须为事后的审裁留下足够的证据。为了实现这个目的,签名的结果应发送给第三方,由第三方保管。在我们的系统中,由于存在3个主体,可以互为第三方。只要让证据保存者对证据的保存是符

*)Supported by Key Science and Technology Project of the National Plan Under Grant No:2001BA102A04(国家十五科技攻关项目:编号2001BA102A04)。陈 舜 博士生,主要研究领域为分布式系统、信息安全;姚 前 博士生,主要研究领域为信息安全;谢 立 教授,博士生导师,主要研究领域为分布式系统、并行计算、信息安全。

合自己安全利益的，这种第三方就比一般的中性第三方还具有可信性。为了实现这一点，就必须对一般的签密方案作出改进。在普通的签密方案中，签名和加密在一个逻辑步骤中完成，非否认性和机密性是一次提供的。这样一来，签名的直接证据就没有了[19]。所以，绝大多数签密方案不能直接应用于电子商务中。为了既保存证据，又利用签密的有效性，我们采用先签名再加密的方法。发送方先用自己的密钥对消息进行签名，再用接收方的公钥进行加密。但在这两步中，基础参数是共用的。接收方收到密文后，先用自己的私钥解开报文，得到发送方的签名后，一是进行签名确认，二是将这一签名送与第三方保存。这就与传统的签名后再加密有所不同。传统的签名后再加密是完全不同的两个计算，在参数上是不关联的。这里提出的方案，既满足了证据的要求，又增加了协议的紧凑性，利用了签密的效率。因此，这种签密方案可称为弱型签密方案。

2.2 三方间流程定义

A(Agent)、B(Bank)和C(Client)三方之间，有多种方式可以交换信息。设计信息交换流程的根本原则，是交换次数尽可能少。我们认为，一般的在线交易与支付中，只需要6次通信，就可以完成三方间的业务往来，如图1所示。

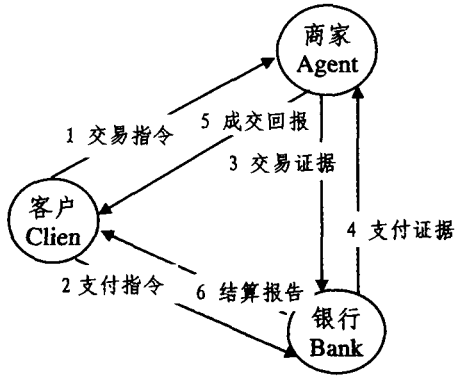

图1 三方间信息交换流程

以上各步关系如下：

第一步，C将交易指令M1传给A；C用自己的私钥对M1签名，得签名Z1；用A的公钥对M1和Z1加密，得密文E1；将E1传给A。

第二步，C将支付指令M2传给B；C用自己的私钥对M2签名，得签名Z2；用B的公钥对M2和Z2加密，得密文E2；将E2传给B。

第三步，A用自己的私钥解开E1，得签名Z1和交易指令M1；验证Z1，若Z1有效，向交易所继续传送指令，同时将Z1传给B。

第四步，B用自己的私钥解开E2，得签名Z2和交易指令M2；验证Z2，若Z2有效，将Z2传送A，既作为C向B发出支付指令的证据，也作为B向A作出的支付承诺。

第五步，如果A从B处获取的支付承诺与交易指令匹配，则将成交结果通知客户，确证交易达成。

第六步，如果B从A处获取的交易证据与支付指令匹配，则进行结算，并将结算结果通知客户。

下面给出具体的协议框架。

2.3 三方弱型签密协议(3-IBSE)

我们以CC的签名方案和BF的加密方案为要件，提出一种三方间的签密协议框架。一般情况下，商家或银行的计算能力远大于客户，在线交易的推动者也主要是商家。因此，公钥生成(PKG)由商家承担。

2.3.1 定义及系统参数设置

定义1 G_1 和 G_2 为群，阶为 q，q 为素数，存在非退化的可有效计算的映射 $\hat{e}:G_1\times G_1\to G_2$。这一映射必须是双线性的，即对所有的 $P_1,P_2\in G_1$，所有的 $a,b\in Z_q^*$，都有 $\hat{e}(aP_1,bP_2)=\hat{e}(P_1,P_2)^{ab}$。

定义2 $H_0:\{0,1\}^{k_1}\to G_1$；$H_1:\{0,1\}^{k_0+n}\to Z_q^*$；$H_2:G_2\to\{0,1\}^{k_0+k_1+n}$。其中，$k_0$ 是表示 G_1 中点的位数，k_1 是表示身份长度的位数，n 是需签名和加密的信息长度。

参数设置

A运行Setup，设置系统参数如下：

(0)选择群和散列函数：$G_1,G_2,q,\hat{e},H_0:\{0,1\}^{k_1}\to G_1$；$H_1:\{0,1\}^{k_0+n}\to Z_q^*$；$H_2:G_2\to\{0,1\}^{k_0+k_1+n}$；

(1) 选择点 P，使得 $\langle p\rangle=G_1$，即是一个循环群，P 是生成员；

(2) 在 Z_q^* 中任选 s，计算全局公钥 $Q_{TA}\leftarrow sp$。

密钥生成

(1) A运行Extract，根据U选择的身份标识 $ID_u\in\{0,1\}^{k_1}$；计算 U 的公钥 $Q_u\leftarrow H_0(ID_u)$，相应的私钥为 $S_u\leftarrow sQ_u$，即

$$A:ID_A\xrightarrow{H_0}Q_A\xrightarrow{s}S_A$$

$$B:ID_B\xrightarrow{H_0}Q_B\xrightarrow{s}S_B$$

$$C:ID_c\xrightarrow{H_0}Q_c\xrightarrow{s}S_c$$

(2)根据以上结果，A运行双点映射算法，计算以下值：

$w_{AB}=e(S_A,Q_B)$

$w_{AC}=e(S_A,Q_C)$

$w_{BA}=e(S_B,Q_A)$

$w_{BC}=e(S_B,Q_C)$

$w_{CA}=e(S_C,Q_A)$

$w_{CB}=e(S_C,Q_B)$

经过以上计算：A的签名密钥为 Q_A,S_A，加密密钥为 w_{AB},w_{AC}；B的签名密钥为 Q_B,S_B，加密密钥为 w_{BA},w_{BC}；C的签名密钥为 Q_C,S_C，加密密钥为 w_{CA},w_{CB}。

2.3.2 通信过程

每次交易是由C发起的，假定交易指令为 m_1，支付指令为 m_2，m_1 和 m_2 可以不同，但必须存在对应关系。以下按 m_1 和 m_2 的传送过程予以描述。

(1)m_1 的传送过程

①C到A的签密过程：交易指令(图2中通信1)

(a)C签名

- 在 Z_q^* 中任选 r_1，计算 $X_1\leftarrow r_1Q_A$；
- 计算 $h_1\leftarrow H_1(X_1\|m_1)$，计算 $Z\leftarrow(r_1+h_1)S_A$；
- 输出签名 (X_1,Z)，待加密；

(b)C加密

- 计算 $g_{CA}=(w_{CA})^{r_1}$；
- 计算 $y_1\leftarrow H_2(g_{CA})\oplus(Z\|ID_C\|m_1)$；
- 将密文 (X_1,y_1) 传给A；

(c)A解密

- 计算 $g_{CA}\leftarrow\hat{e}(X_1,S_A)$，$Z\|ID_A\|m_1\leftarrow y_1\oplus H_2(g_{CA})$；
- 将 m_1、签名 (X_1,Z) 和 ID_A 送予验证；

(d)A验证

- 计算 $h_1 \leftarrow H_1(X_1 \| m_1)$.；

- 检验 $\hat{e}(Z,P)=\hat{e}(X_1+h_1Q_A,Q_{TA})$是否成立。如不成立，拒绝报文；如成立，接受签名；

②A 向 B 加密传送 C 的签名：保存证据(图 2 中通信 3)

- 在 Z_q^* 中任选 r_2，计算 $X_2 \leftarrow r_2Q_A$；

- 计算 $g_{AB}=(w_{AB})^{r_2}$；

- 计算 $y_2 \leftarrow H_2(g_{AB}) \oplus (Z \| ID_C \| m_1)$；

- 传送密文(X_2, y_2)给 B；

(2)m_2 的传送

③C 到 B 的签密过程：支付指令(图 2 中通信 2)

重复(a)到(d)，只不过用 m_2 取代 m_1，用 B 取代 A。

(e)C 签名

对 m_2 的签名过程如下：

- 在 Z_q^* 中任选 r_1，计算 $X_1 \leftarrow r_1Q_A$；

- 计算 $h_1 \leftarrow H_1(X_1 \| m_2)$，计算 $Z \leftarrow (t_1+h_1)S_A$；

- 输出签名(X_1, Z)，待加密；

(f)C 加密

- 计算 $g_{CB}=(w_{CB})^{r_1}$；

- 计算 $y_1 \leftarrow H_2(g_{CB}) \oplus (Z \| ID_C \| m_2)$；

- 将密文(X_1, y_1)传给 B；

(g)B 解密

- 计算 $g_{CB} \leftarrow \hat{e}(X_1,S_B)$，$Z \| ID_A \| m_2 \leftarrow y_1 \oplus H_2(g_{CB})$；

- 将 m_2、签名(X_1, Z)和 ID_A 送予验证；

(h)B 验证

- 计算 $h_1 \leftarrow H_1(X \| m_2)$；

- 检验 $\hat{e}(Z,P)=\hat{e}(X+h_1Q_A,Q_{TA})$是否成立。如不成立，拒绝签名；若成立，转入下一步。

④ B 向 A 传送 C 的签名：支付承诺(图 2 中通信 4)

重复③，只不过交换 A 与 B 的位置。

- 在 Z_q^* 中任选 r_2，计算 $X_2 \leftarrow r_2Q_A$；

- 计算 $g_{BA}=(w_{BA})^{r_2}$；

- 计算 $y_2 \leftarrow H_2(g_{BA}) \oplus (Z \| ID_C \| m_1)$；

- 传送密文(X_2, y_2)给 A；

完成交易(图 2 中通信 5)

① A 收到来自 B 的(X_2, y_2)：

- 计算 $g_{BA}=\hat{e}(X_2,S_A)$；

- 计算 $y_2 \oplus H_2(g_{BA})$，得 Z 和 m_2；

- 如果 m_1 和 m_2 匹配，保存 Z，并将成交结果报告 C。

② 成交报告的传送方式类似通信 1。

完成支付(图 2 中通信 6)

① B 收到来自 A 的(X_2, y_2)：

- 计算 $g_{AB}=\hat{e}(X_2,S_B)$；

- 计算 $y_2 \oplus H_2(g_{AB})$，得 Z 和 m_2

- 保存 Z；如果 m_1 和 m_2 匹配，完成支付，并将支付报告传给 C。

② 支付报告的传送方式类似通信 2。

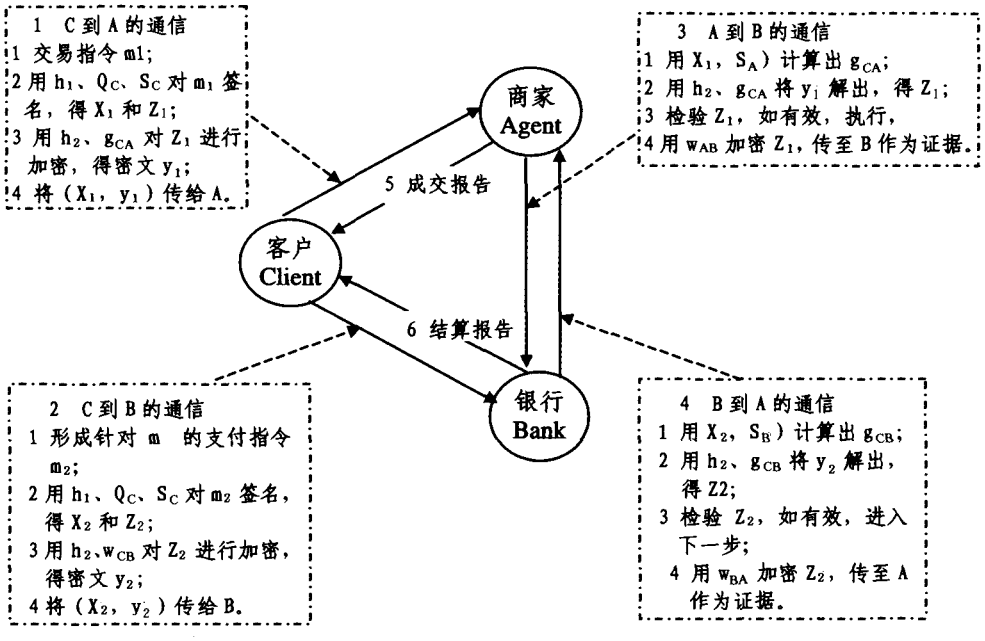

图 2　三方弱型签密协议框架

3　三方弱型签密协议的安全性

以上的三方弱型签密协议(3-IBSE)能提供的安全特性有：密文鉴别、报文机密以及签名非否认性。安全性证明的思路是：在某一方面(如密文鉴别)，如果 3-IBSE 能被敌手攻破(以某一概率)，则可以构建一个模拟器，利用敌手攻击时留下的信息，成功求解双线性 Diffie-Hellman(BDH)问题(以某一相关概率)。因此，只要 Diffie-Hellman 难题是公开的，3-IBSE 在所求证的方面就是安全的。

假设：H_0，H_1 和 H_2 都是 random oracles[20]。敌手对 H_i 的询问表示为 q_i，$i=0,1,2$；敌手对签名(加密)和解密(验证)的询问分别为 q_s 和 q_d；(P,aP,bP,cP)是要解的 BDH 难题。

3.1　密文鉴别

结论 1　如果存在敌手 A，以选择报文攻击(CMA)的方式，以 ϕ 的概率成功破解 3-IBSE 协议，则可以构建模拟器 B，在多项式时间内，以不低于 $P(B)$的概率求出 BDH 问题：

$$P(B) \geqslant \frac{(q-q_s(q_1+q_2+q_3))}{qq_0(q_0-1)(q_s+q_d)(q_2+q_s)}\phi$$

也就是说，一个 CMA 敌手，如果成功破解 3-IBSE，则可构建一个模拟器 B，利用攻击中留下来的信息，解决 BDH 问题(证明略)。

3.2　报文机密性

结论 2 如果存在敌手 A，以适应性选择密文攻击(ACCA)的方式，以 ϕ 的概率成功破解 3-IBSE 方案，则可以构建模拟器 B，在多项式时间内，以不低于 $P(B)$ 的概率求出 BDH 问题：

$$P(B)\geqslant\phi\frac{q-q_s(q_1+q_s)}{qq_0q_2}$$

(证明略)

3.3 签名非否认性

结论 3 如果存在敌手 A，以选择报文攻击(ACCA)的方式，以 ϕ 的概率成功破解 3-IBSE 方案，则可以构建模拟器 B，在多项式时间内，以不低于 P(B)的概率求出 DH 问题(BDH 与 DH 是等价的)：

$$P(B)\geqslant\phi^2\left(\frac{q-q_s(q_1+q_s)}{2qq_0(q_1+q_s)}\right)^2$$

(证明略)

以上三者结合在一起，提供了一种高强度的、侧重于防止内部攻击的框架协议，使得密文在传输过程中保持完整性。非指定的接收方不能解开密文；非指定的接收方不能验证签名，第三方拥有接收方的私钥也不能伪造签名；非指定的接收方不能解密密方，第三方拥有发送方的私钥也不能解读报文。也就是说，对外部的选择性报文攻击，具有存在性密文不可伪造性(ECU-OCMA)；对内部选择报文攻击具有存在性不可伪造性(EU-ICMA)；对于适应性选择密文攻击，报文具有语义安全性(SS-ACCA)。

4 三方弱型签密协议的效率及特点

3-IBSE 是专门针对电子商务提出的，与其他类似协议比较，突出了以下特点：

第一，大大提高了效率。效率体现在两个方面：一是单次通信中加密运算成本(时间或资源)的降低，二是总体通信次数的下降。

(1)在单次通信中，目前效率最高的签密协议是 Chen 和 Malone-Lee 于 2005 年初提出的[21](CM 方案)，与之相比的结果如表 1。

表 1 3-IBSE 与 CM 的效率比较(客户端视角)

	CM	3-IBSE
参数设置(PKG)	确定 GDH 群后，选择全局参数 s 并计算出全局公钥 $Q_{TA}\leftarrow sP$	比 CM 多计算三项：一是客户 ID 的成点映射 $Q_u\leftarrow H_0(ID_u)$；二是客户私钥 $S_u\leftarrow sQ_u$；三是与客户间的双点映射值 w_{AB}。
密钥生成	通信前或通信时计算	由 PKG 负责计算，客户使用
签名	1 次 H_0 运算，1 次 H_1 运算，2 次标量乘。	1 次 H_1 运算，2 次标量乘。(少 1 次 H_0 运算)
加密	1 次 H_0 运算，1 次双点映射运行，1 次 H_2 运算。	1 次乘方运算，1 次 H_2 运算。(少 1 次 H_0 运算，少 1 次双点映射运算，多 1 次乘方运算)
解密	1 次双点映射运算，1 次解密运算。	1 次双点映射运算，1 次解密运算。
验证	1 次 H_0 运算，1 次标量乘运算，1 次点加运算，1 次双点映射运算。	1 次 H_0 运算，1 次标量乘运算，1 次点加运算，1 次双点映射运算。

从表 1 比较得知，与 CM 相比，客户端少两次成点映射(map to point)运算，少一次双点映射运算，多一次乘方运算。在基于双线性的密码体制中，成本最大的就是映射计算，而乘方运算可忽略不计。3-IBSE 在每次通信中避免了 3 次映射，大大提高了效率。之所以能实现这种改进，最根本的原因在于将计算任务放到了经纪端，从而简化了通信中的计算量，尤其是减轻了客户端的负担。

(2)不因保密而增加通信次数。在其他的非对称加密体制中，如基于 PKI 或 CA 的体制中，为了实现安全交换，要经过多次事先通信。但在 3-IBSE 中，直接进行交易和支付所必需的通信，不必另外增加数据交换的次数。

第二，提供了直接的非否认性证据。这里的签密方案，与普通的签密方案有所不同。在普通的签密方案中，为了尽可能减少计算，把签名和加密放在一个逻辑步骤中完成。但在本方案中，为了留下签名证据，提供直接的非否认性支持，是将签名和加密分步完成的。但这两步并非截然分开。一是签名和加密的环境参数是一样的，二是有的参数在两步中用的是同一个值。分步完成的目的，只是为了将签名分离出来，其他仍然是关联的，密文也是一体的。本质而言，这与签名后再加密仍然是完全不同的，也是与其他签密方案最大的不同之处，是为了实现在线交易和支付的特殊安全性需求而设计的。

第三，互为可信第三方。在非对称加密体制中，需要两种形式的第三方。一是可信第三方，由其对相对方提供身份证明；二是保存签名证据的第三方，处于中性位置，保存委托方的签名。在两两通信的体制中，这是一个很麻烦的问题。但在 3-IBSE 中，将业务的进行与证据的保存相结合，各自互为第三方，在减少通信量的同时，进一步提高了安全性。

第四，交易与支付紧密关联。传统的电子商务中，交易与支付安全是分开考虑的，不仅降低处理效率，还增加了安全隐患。3-IBSE 是一种紧凑的协议框架，有交易基础才会导致支付行为，有支付承诺才能完成交易活动，二者共同促进安全水平。而且，这种一体化的安排，使得在线交易和支付真正实现实时处理成为可能。

第五，综合考虑业务风险与技术风险。电子支付进展缓慢的一个重要原因，是试图用技术方案来解决业务风险。在 3-IBSE 中，我们将风险分解，用支付流程控制业务风险，用技术为支付流程做保障，有效地解决了在线支付的安全问题。

参 考 文 献

1 蒋韬，伍评，徐正文. 基于 PMI 技术建立网上网上交易安全系统. 中国证券信息技术，2002(8)：46～48
2 Ellison C, Schneier B. Ten risks of PKI: What you are not being told about Public Key Infrastructure. Computer Security Journal, 2000, 16(1)
3 Nash A, Duane W, Joseph C, et al. PKI implementing and Managing E-Security. McGraw-Hill Companies, 2001. 216～249
4 Jakobsson M, Mraihi D, Tsiounis Y, et al. Electronic payment : Where do we go from here. In: Lecture Notes on Computer Science. Spring-Valag, 2004, 1740: 43～49
5 Dai Xiaoling, Grundy J. Three kinds of E-wallets for net-pay micro-payment system. In: Lecture Notes on Computer Science. Spring-Valag, 2004, 3306: 66～70
6 Chen Qingfeng, Zhang Chenggai, Zhang Shichao. Veryfying the payment authorization of SET protocol. In: Lecture Notes on Computer Science. Spring-Valag, 2003, 2690: 914～918
7 Lacoste G, Pfitzman B, Steiner M, et al, The electronic payment of framework. In: Lecture Notes on Computer Science. Spring-Valag, 2004, 1854: 185～211
8 Shamir A. Identity-based cryptosystems and signature schemes. In: Blakley G R, Chaum D, eds. Advances in Cryptology - CRYPTO 1984. Lecture Notes in Computer Science. Springer - Verlag, 1984, 196: 47～53
9 Miller V. Uses of elliptic curves in cryptography. In: Advances in Cryptology CRYPTO' 85, Lecture Notes in Computer Science (LNCS), Springer-Verlag, 1838. 385～394; Koblitz N, curve E cryptosystems, Mathematics of Computation, 1987, 48: 203～209

(下转第 270 页)

如下：

```
%ATTACHMENTS==[
                SQComIn1. PortName # # SQ-RAConIn1. RoleName.
                XZComIn2. PortName # # XZ-RAConIn1. RoleName.
                ]
```

SQClient 和 RAServer 之间的客户-服务器风格描述为：

组件：

$SQClient==[LB=y''\Rightarrow Request \wedge \$OLB=y''_1;$
$LB=y''_1\Rightarrow Computation_2 \wedge \$OLB=z'']$
$RAServer==[LB=w''\Rightarrow Provide \wedge \$OLB=v'']$

连接件：MP

$Sender==[LB=y\Rightarrow(c!w \wedge \$OLB=z)]$
$Receiver==[LB=y\Rightarrow(c?u \wedge \$OLB=z)]$

体系结构风格

$CS_2==\|[SQClient;RAServer]$

·中间过程与 CA 相近，因篇幅有限，详细代码在此就不列出了。

·证书申请组件

用户填写申请人信息及其 PIN 值，提交到子 RA 服务器。子 RA 服务器将申请人信息保存在证书申请库的证书申请表中，并将其状态值标记为“未审核”。RA 管理员审核申请人真实身份，若提交的申请人信息与其真实物理身份相符，则审核通过；否则审核不能通过。若用户的证书申请审核通过，则 RA 将证书申请表中该申请人状态值更新为“已审核”，将该申请转交给安全服务器。经过安全检查后，转交给系统的 RA 服务器，等待 CA 发放证书；反之，如果未通过审核，则子 RA 服务器将该申请人的信息从证书申请表中删除，并且将其对应的用户信息从用户表中删除。最后，子 RA 服务器将审核结果以电子邮件的方式发送给用户。

```
%PROS[
  %PROSCAapplication (% CHN ASYN m1 ( * , chout: NM): STRING;
                      % CHN ASYN m2 ( chin: NM, * ): STRING)
    ==[
      %ALG[
        %LOC[client_message,exam_value:STRING;
             tellmessage,delmessage,cm,ev,sh:STRING;
             ]
        LB=START=>$OLB=y1;
        LB=y1=>$O cm=0∧$OLB=y2;
        LB=y2∧m2 ? =>$OLB=y3;
        LB=y2∧¬m2 ? =>$OLB=y1;
        LB=y3=>$O m2 ? cm∧$OLB=y4;
        LB=y4=>$O client_message=cm∧$OLB=y5;
        LB=y5=>$O exam_value=0∧$OLB=y6;
        LB=y6=>$O cm=cm+exam_value∧$OLB=y7;
        LB=y7=>$O client_message=cm∧$OLB=y8;
        LB=y8=>$O m1 ! cm∧$OLB=y9;
        LB=y9=>$O ev=exam_vale∧$OLB=y10;
        LB=y10∧(sh=1)=>$OLB=y11;
        LB=y10∧(sh=0)=>$OLB=y15;
        LB=y11=>$O exam_value=1∧$OLB=y12;
        LB=y12=>$O cm=cm+exam_value∧$OLB=y13;
        LB=y13=>$O client_message=cm∧$OLB=y14;
        LB=y14=>$O m1 ! cm∧$OLB=y1;
        LB=y15=>$O tellmessage=1∧$OLB=y16;
        LB=y16=>$O tellmessage=tellmessage+sh∧$OLB=y17;
        LB=y17=>$O m1 ! tellmessage∧$OLB=y18;
        LB=y18=>$O delmessage=1∧$OLB=y19;
        LB=y19=>$() delmessage=delmessage+cm∧$OLB=y20;
        LB=y20=>$O m1 ! delmessage∧$OLB=y21;
        LB=y21=>$OLB=y1;
            ]
      ]
  ]
```

结束语 本文以时序逻辑语言 XYZ/E 对 CA 认证系统中两个关键组件，即认证机构 CA 和注册机构 RA 进行了描述和求精。整个过程在统一的时序逻辑框架下进行，保证了系统的语义一致性，从而提升了 CA 认证软件开发的可靠性。同时，引入组件技术，便于系统分阶段开发和未来的功能扩展。用时序逻辑语言 XYZ/E 对 CA 认证系统的软件体系结构进行描述和求精有利于对整个系统的分析、演化、管理。因此，下一步将在此基础上对已经完成的描述内容进行分析和验证等工作。

参 考 文 献

1 唐稚松. 时序逻辑程序设计与软件工程[M]. 北京：科学出版社，2002

2 刘俭云，戎玫，张广泉. XYZ/E 在 CA 认证系统中的一个初步应用[J]. 计算机工程与应用(已录用)

3 Moszko B. Executing Temporal Logic Programs. Cambridge University Press, 1986

4 汪立东，余祥湛，方滨兴. PKI 中几个安全问题的研究[J]. 计算机工程，2000，26(1)：14～15

5 陈鲁川，李善平. Linux 平台下公钥基础设施(PKI)的研究[J]. 计算机应用研究，2003，20(2)：93～94

6 张辉，杨岳湘，汪诗林. 数字校园中基于 LDAP 的统一用户身份管理技术研究[J]. 计算机工程与科学，2005，17(1)：14～16

(上接第 112 页)

10 A. Joux. A one round protocol for tripartite Diffie-Hellman. In: Bosma W, eds. Proceedings of Algorithmic Number Theory Symposium - ANTS IV. Springer-Verlag, 1987, 1838: 385～394

11 Sakai R, Ohgishi K, Kasahara M. Cryptosystems based on pairing. The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, January 2000

12 Boneh D Franklin M. Identity-based encryption from the Weil pairing. In: Kilian J, eds. Advances in Cryptology-CRYPTO 2001. Springer-Verlag, 2001, 2139: 213～229

13 Cha J C, Cheon J H. An identity-based signature from gap Diffie-Hellman groups. In: Desmedt Y, editor. Public Key Cryptography - PKC 2003. Lecture Notes in Computer Science. Springer - Verlag, 2002, 2567: 18～30

14 Zheng Y. Digital signcryption or how to achieve cost(signature & encryption)<< cost(signature) + cost(encryption). In: Kalishi B S Jr. eds. Advances in Cryptology - CRYPTO 1997. Lecture Notes in Computer Science. Springer - Verlag, 1997, 1294: 165～179

15 Malone-Lee J. Identity-based signcryption. Cryptology ePrint Archive: [Report 2002/098]. 2002. http://eprint.iacr.org/

16 Libert B, Quisquater J-J. Efficient signcryption with key privacy from gap diffie-hellman groups. In: F. Bao, R. H. Deng, and J. Zhou, eds. International Workshop on Practice and Theory in Public Key Crytography - PKG 2004. Lecture Notes in Computer Science. Springer - Verlag, 2004, 2947: 187～200

17 Lynn B. Authenticated identity-based encryption. Cryptology ePrint Archive: [Report 2002/072]. 2002. http://eprint.iacr.org/

18 Nalla D, Reddy K C. Signcryption scheme for identity-based cryptosystems. Cryptology ePrint Archive: [Report 2003/066]. 2003. http://eprint.iacr.org/

19 Malone-Lee J. Identity-based signcryption. Cryptology ePrint Archive: [Report 2002/098]. 2002. http://eprint.iacr.org/

20 Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In ACM Conference on Computer and Communications Security, ACM, 1993. 62～73

21 Chen Liqun, Malone-Lee J. Improved Identity-Based Signcryption. Public Key Cryptography(PKC), Lecture Notes on Computer Science Springer-Verlag, 2005, 3386: 362～379