基于身份的多重签密方案

孟 涛,张鑫平,孙圣和
(哈尔滨工业大学,黑龙江哈尔滨 150001)

摘 要: 本文利用椭圆曲线上的双线性对提出一个新的基于身份的多重签密方案,解决以前的传统证书式多重签密方案的证书管理,传递等繁琐问题.并进行了安全性分析,在BDH问题是困难的假设下方案是安全的.签密能够在一个逻辑步骤内同时完成保密和认证两项功能,而其计算量和通信成本都要低于传统的"先签名后加密",在电子商务等方向有很好的应用前景.

关键词: 有序多重签密;基于身份的密码系统;双线性对
中图分类号: TN919.19 **文献标识码:** A **文章编号:** 0372-2112 (2007) 6A-115-03

Identity-Based Multi-Signcryption Scheme

MENG Tao, ZHANG Xin-ping, SUN Sheng-he
(*Harbin Institute of Technology, Harbin, Heilongjiang* 150001, *China*)

Abstract: Signcryption is a cryptographic protocol that combines both the functions of confidentiality and authentication in a logical step, and the computational costs and communication overheads should be lower than the traditional signature-then-encryption approach. So signacryption has good prospects in the direction of e-commerce. Based on bilinear pairing on Elliptic Curve, a new multi-signacryption scheme is proposed. The scheme could decrease the cost of building and managing public key infrastructures; the expense of the users' management of public-key and their certificates is avoided. We had a safety of analysis, that the proposed scheme is proved to be secure assuming the bilinear Diffle-Hellem problem is hard.

Key words: multi-signcryption; identity-based cryptosystem; bilinear pairings

1 引言

基于身份的密码体制是由Shamir[1]开创性提出的,在一个基于身份的密码体制中,每个用户的公钥可以由其唯一的身份信息(如姓名,性别)来确定,用户的私钥则由可信机构产生.1997年,Zheng Yuliang[2]提出了一个新概念:签密,并给出了具体的签密方案.该签密方案能在一个逻辑步骤内同时实现保密和认证两项密码功能,且其代价远远低于传统的"先签名再加密"的认证加密方法.这种高效性使签密得到了广泛的关注.自Zheng提出签密方案以来,又有很多方案被提出,并且签密概念也得到不断的扩展,如代理签密、多重代理签密、门限签密、基于身份的签密[3]等新概念被提出来.其中基于多个人共同完成对消息签密的需要,文献[4]提出了多重签密的概念,文献[5]又给出了具体的多重签密方案.但是这些文献[1]所提出的方案都是基于传统的证书式公钥方法的,其证书存在如何管理、传递、验证等多种问题.

文献[6]提出了基于身份的多重签密方案,将基于身份的密码系统引入多重签密.但是在文献[6]中,该方案没有签名验证操作,使得在多重签密中每一位签密者都无法验证其前一位签密者的真实性,所以其方案并不是很完善.本文利用双线性对提出一个新的基于身份的多重签密方案,采用了先验证签名以确保消息的可信性,然后进行消息解密的过程,并对所提方案给出了安全性分析.

2 预备知识

本节介绍椭圆曲线上双线性对的基本性质及其相关困难问题.

令 G_1 为由一个大素数 P 生成的 q 阶循环加法群,G_2 为具有相同阶 q 的循环乘法群,a 和 b 分别是乘法群 Z_q^* 中的元素.双线性对定义为满足下列性质的一个映射 $\hat{e}: G_1 \times G_1 \rightarrow G_2$:

(1)双线性.$\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$

(2)非退化性.存在 $P, Q \in G_1$,使得 $\hat{e}(P, Q)^{ab}$;

收稿日期:2007-09-17;修回日期:2007-12-13

(3)可计算性.对所有的 $P, Q \in G_1$,存在有效的算法计算 $\hat{e}(P, Q)$.

定义 2.1 离散对数问题(Discrete Logarithm Problem,简记为 DL 问题):给定两个元素 $P \in G_1$ 和 $Q \in G_1$,计算 $a \in Z_q^*$,使其 $Q = aP$ 成立.假设 G_1 和 G_2 这两个群中的离散对数问题都是困难问题.

定义 2.2 双线性 Diffi-Hellman 问题(Bilinear Diffi-Hellman Problem,简记为 BDH 问题):给定 (P, aP, bP, cP),计算 $\hat{e}(P, Q)^{abc} \in G_2$,这里 $a, b, c \in Z_q^*$ 是未知的整数.

定义 2.3 判定双线性 Diffie-Hellman 问题(Decisional Bilinear Diffie-Hellman problem,简记为 DBDH 问题)给定 (P, aP, bP, cP)和 $h \in G_2$,判断 $h = \hat{e}(P, P)^{abc}$是否成立,这里 $a, b, c \in Z_q^*$ 是未知的整数.

3 一个新的基于身份的多重签密方案

本节提出一个新的多重签密方案,具体过程如下:

U_V 为签密的验证者,$U_1, U_2, \cdots, U_n$ 为消息的签密者.每位签密者都通过密钥生成中心来生成自己的公私钥对.

Setup:设 G_1 为由一个大素数 P 生成的 q 阶循环加法群,G_2 为具有相同阶 q 的循环乘法群,$\hat{e}: G_1 \times G_1 \to G_2$ 为一个双线性映射.定义一个安全的对称加密算法 (E, D),定义三个安全的 Hash 函数 $H_1: \{0,1\}^* \to G_1$,$H_2: \{0,1\}^* \to Z_q^*$,$H_3: G_1 \to Z_q^*$.密钥生成中心(PKG)随机选择一个主密钥 $s \in Z_q^*$,计算 $P_{pub} = sP$.PKG 公开系统参数 $\{G_1, G_2, n, \hat{e}, P, P_{pub}, H_1, H_2, H_3\}$,保密主密钥 s.

Extract:用户将自己的身份信息 ID 发送到 PKG,PKG 计算用户相应的公私钥对,用户公钥为 $Q_u = H_1(ID)$,用户的私钥为 $S_u = sQ_u$.这里我们设 U_i 的身份为 ID_i,公钥为 Q_i,私钥为 S_i.

Signcryption:我们假设 $(U_1, U_2, \cdots, U_n)$ 为签密的顺序.且假设要签密的文件 m 被分成 n 份,每个签密者都有相应的文件 m_i.然后实施下列签密步骤:

第 1 步:(1) U_1 生成随机数 $k_1 \in Z_q^*$.

(2)计算 $R_1 = k_1 P$;

(3)计算 $w_1 = \hat{e}(P_{pub}, Q_V)^{k_1}$,并计算 $C_1 = E_{w_1}(m_1)$.

(4)计算 $T_1 = H_2(C_1) k_1 Q_1 + H_3(R_1) S_1$

第 2 步:将签名消息 (R_1, C_1, T_1) 发送到下一个签密者.

第 3 步:签密者 U_i 顺序如下:

(1)验证方程

$$e(T_{i-1}, P) = e(Q_{i-1}, R_{i-1})^{H_2(C_{i-1})} e(Q_{i-1}, P_{pub})^{H_3(R_{i-1})}$$

如方程不成立则拒绝签密,如成立则做如下步骤;

(2)生成随机数 $k_i \in Z_q^*$;

(3)计算 $R_i = k_i P$;

(4)计算 $w_i = \hat{e}(P_{pub}, Q_V)^{k_i}$,并计算 $C_i = E_{w_i}(m_i \| T_{i-1} \| C_{i-1} \| R_{i-1})$;

(5)计算 $T_i = H_2(C_i) k_i Q_i + H_3(R_i) S_i$;

Unsigncryption:U_V 收到 U_n 送来的签密消息 (R_n, C_n, T_n)后,首先计算 $H_2(C_n)$和 $H_3(R_n)$以及 $e(T_n, P)$,然后验证等式:$e(T_n, P) = e(Q_n, R_n)^{H_2(C_n)} e(Q_n, P_{pub})^{H_3(R_n)}$

如果等式成立,接收签名;如不成立,则拒绝签名.

验证的根据是式(1)的成立.

$$\begin{aligned} e(T_n, P) &= e(H_2(C_n) k_n Q_n + H_3(R_n) S_n, P) \\ &= e(H_2(C_n) k_n Q_n, P) e(H_3(R_n) S_n, P) \\ &= e(Q_n, k_n P)^{H_2(C_n)} e(Q_n, P_{pub})^{H_3(R_n)} \\ &= e(Q_n, R_n)^{H_2(C_n)} e(Q_n, P_{pub})^{H_3(R_n)} \end{aligned} \quad (1)$$

一旦验证者 U_V 证实了签密 (R_n, C_n, T_n)是有效的,那么他可以利用自己的私钥 S_V 根据式(2)从签密中恢复明文消息.

$$e(R_n, R_V) = e(k_n P, S_V) = e(P, S_V)^{k_n} = e(P_{pub}, Q_v)^{k_n} = w_n \quad (2)$$

通过计算 $D_{w_n}(C_n) = m_n \| T_{n-1} \| C_{n-1} \| R_{n-1}$,计算出 m_n,且可根据 $(R_{n-1}, C_{n-1}, T_{n-1})$得到 m_{n-1},以此类推可以得到全部的消息 m.

4 方案安全性分析

首先我们相信 PKG 是可信的,不会泄露用户的信息.对于已完成的多重签密,若签密的消息 m_i 和签密次序已定,则 U_V 可以对此进行验证.由于 U_V 收到的多重签密可以通过签名的验证确认最后一个签密者,并解密得到消息 m_i.同时,U_V 可根据收到的多重签密依次验证和解密,从而获得其余所有签密者签密的消息.然后我们分析所提方案的安全性:

(1)消息的机密性:假如攻击者获得对消息 $m_i (1 \leqslant i \leqslant n)$的签密密文 (R_n, C_n, T_n).但是由于攻击者不知道 k_i, S_i, S_v,通过 $w_n = \hat{e}(P_{pub}, Q_V)^{k_n}$或者 $w_n = e(R_n, S_V)$计算 w_n 都必然遇到 BDH 问题,导致计算上不可行.从而攻击者得到消息 $m_i (1 \leqslant i \leqslant n)$也是计算上不可行的.

(2)消息的不可伪造性:攻击者(包括不诚实的签密者 U_i)试图伪造签密者 U_j 对消息 m_j 的签密 (R_j, C_j, T_j),则需通过解下列方程 $T_j = H_2(C_j) k_j Q_j + H_3(R_j) S_j$ 得到用户的私钥 S_j,但是由于方程中的 k_j 使得攻击者将面对离散对数问题.

5 结论

本文提出了一个利用椭圆曲线双线性对的基于身

份的多重签密方案,在新的多重签密方案中,签密的安全性基于 BDH 问题,且能够避免传统证书式方案中证书管理、传递等问题,能很好地应用到电子商务等实际应用领域.

参考文献:

[1] A Shamir. Identity-based cryptosystems and signatures schemes [J]. Crpto'84, LNCS-196:48 - 53.

[2] Y Zheng. Digital signcryption or how to achieve cost (signature & encryption) cost (signature) + cost (encryption) [J]. Advances in Cryptology-Crypto'97, LNCS-1294:165 - 179.

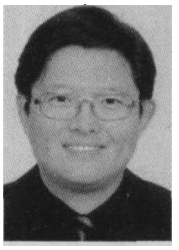
[3] F Li, Y Hu. An efficient identity-based signcryption scheme [J]. Chinese Journal of Computer, 2006, 29(9):1641 - 1647.

[4] S Mitomi, A Miyaji. A general model of multisignature schemes with message flexibility, order flexibility, and order verifiability [J]. IEICE Transactions on Fundamentals, 2001, E84-A(10): 88 - 99.

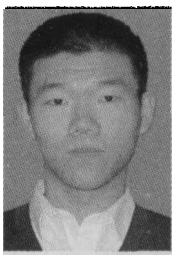
[5] S H Seo, S H Lee. A secure and flexible multi-signcryption scheme[J]. ICCSA 2004, LNCS-3046:689 - 697.

[6] 张串绒,肖国镇.利用身份和双线性对的多重签密方案[J].西安电子科技大学学报,2007,34(2):270 - 274.
Zhang Chuanrong, Xiao Guozhen. Multi-signcryption scheme using identity and bilinear pairing[J]. Journal of Xidian University, 2007, 34(2):270 - 274. (in Chinese)

作者简介:



孟　涛　男,1961 年 5 月出生,1983 年于国防科技大学获学士学位,1988 年于哈尔滨工业大学获工学硕士学位,现为哈尔滨工业大学自动化测试与控制研究所博士研究生.主要研究方向为阈下信道、隐藏通信、信息安全.
E-mail: gorgan@126.com



张鑫平　男,1983 年 1 月出生,2006 年于哈尔滨工业大学获工学学士学位,现为哈尔滨工业大学自动化测试与控制研究所硕士研究生.主要研究方向为多重签名、多重签密、信息安全.
E-mail: yijiasanko@163.com

孙圣和　男,1937 年 10 月出生,1961 年毕业于哈尔滨工业大学电机系研究生班,现为哈工大教授、博导,自动化测试与控制研究所所长.研究方向为信号处理、数字水印、自动化测试.
E-mail: sunshenghe@hit.edu.cn