第34卷 第21期 计 算 机 工 程 2008年11月
Vol.34 No.21 Computer Engineering November 2008
·博士论文· 文章编号：1000—3428(2008)21—0026—02 文献标识码：A 中图分类号：TN918.2

基于椭圆曲线离散对数的无证书混合加密

赖 欣[1]，何大可[1]，黄晓芳[2]
(1. 西南交通大学信息安全与国家网格计算实验室，成都 610031；2. 北京邮电大学信息安全中心，北京 100876)

摘 要：基于椭圆曲线离散对数困难问题，结合KEM-DEM混合加密结构，提出一个新的无证书混合加密方案。采用椭圆曲线签名算法保证用户自主生成公钥的不可伪造性，利用用户公钥生成的会话密钥以对称加密算法加密明文，保证明文的机密性，对明文空间的大小没有严格限制。该方案主要涉及椭圆曲线上的点运算，与原有无证书加密方案中采用双线性对计算相比具有更高的执行效率。
关键词：椭圆曲线离散对数；无证书公钥；混合加密

Certificateless Hybrid Encryption Based on Elliptic Curve Discrete Logarithm

LAI Xin[1], HE Da-ke[1], HUANG Xiao-fang[2]
(1. Information Security and National Computing Grid Laboratory (IS&NC), Southwest Jiaotong University, Chengdu 610031;
2. Information Security Center, Beijing University of Post and Telecommunications, Beijing 100876)

【Abstract】Based on elliptic curve discrete logarithm problem and KEM-DEM hybrid encryption construction, a novel certificateless hybrid encryption scheme is proposed. Elliptic Curve Signature Algorithm(ECSA) is used to provide unforgeability of user public key. Owing to KEM-DEM construction user public key is used to generate session key and session key encapsulation. Plaintext is encrypted by symmetry encryption scheme with session key, which provides the confidentiality of plaintext without the strict limitation for plaintext message space. The main operations is point operation in elliptic curve. Compared with previous certificateless encryption schemes related to bilinear pairing operation the scheme is more efficient on computation.
【Key words】elliptic curve discrete logarithm; certificateless public key; hybrid encryption

1 概述

无证书公钥密码体制是介于传统公钥密码体制和基于身份公钥密码体制之间的一种特殊公钥密码体制，最初由文献[1]提出。在无证书公钥密码体制中，密钥生成中心生成用户的部分私钥，用户使用这个部分私钥和自己选取的秘密值独立生成自己的公钥和私钥。这样既消除了基于身份密码体制中的密钥托管问题，也无须使用传统公钥密码体制中的公钥认证中心发布和管理公钥证书。无证书公钥密码体制因其独特的优势被广泛研究，出现了许多无证书公钥加密方案和签名方案[2-5]，这些方案基于身份加密思想，且都建立在双线性对计算基础上，计算开销较大。另外大部分无证书公钥加密算法由于其特定的代数结构都对加密明文空间有所限制。

本文提出一个基于椭圆曲线离散对数的无证书混合加密方案。密钥生成中心生成的部分私钥被用于构建公钥，这样用户的公钥就由2部分构成：(1)工作公钥，由用户的私钥生成；(2)对工作公钥的签名，由密钥生成中心根据用户身份得到的部分私钥生成。发送者要加密消息时，首先验证公钥，验证成功后再创建会话密钥及其封装，并利用对称加密算法结合创建的会话密钥加密明文消息。本方案中对工作公钥的签名和验证采用椭圆曲线离散对数签名算法实现，因此，在计算复杂度上本方案远小于原基于双线性对计算实现的无证书加密方案，而相当于传统的基于离散对数公钥密码体制。同时在本方案中采用了KEM-DEM混合加密结构[6]，对于明文空间大小没有限制，在确保每次会话密钥的机密性的前提下，可以加密任意长度实际数据包，因此，本方案具有很好的密文扩展性。

2 相关知识

2.1 椭圆曲线离散对数问题

$E(F_q)$椭圆曲线离散对数问题(ECDLP)定义如下[7]：假设P是$E(F_q)$上的一个点，Q是$E(F_q)$上为P的倍数点，即存在整数$x>0$，使$Q=xP$，在已知P和Q的前提下，计算出x在计算上是不可行的，即

$$Prob[x\in F_q \mid (P,Q)\in E(F_q)\wedge(Q=xP)]=\varepsilon_{ECDLP}$$

其中，ε_{ECDLP}为可忽略量。

2.2 无证公钥加密的形式化定义

文献[5]提出了无证书公钥加密的形式化定义。一个无证书加密方案一般由7个算法组成：

(1)参数生成算法(Setup)：输入安全参数k，返回系统参数*params*和主密钥*masterkey*；

(2)部分私钥提取算法(Partial-Private-Key-Extract)：输入系统参数*params*和主密钥*masterkey*以及一个身份标识*ID*，输出部分私钥D_{ID}；

(3)设定秘密值算法(Set-Secret-Value)：输入参数

基金项目：国家部委基金资助项目
作者简介：赖 欣(1977－)，女，博士研究生，主研方向：密码学，信息安全；何大可，教授、博士生导师；黄小芳，博士研究生
收稿日期：2007-12-25 **E-mail：**lxrzg@163.com

$params$，输出一个秘密值 s_{ID}；

(4)设定私钥算法(Set-Private-Key)：输出参数 $params$，输出一个用户(全)私钥 SK_{ID}；

(5)设定公钥算法(Set-Public-Key)：输入参数 $params$、部分私钥 D_{ID}、秘密值 s_{ID}、私钥 SK_{ID}，输出一个公钥 PK_{ID}；

(6)加密算法(Encrypt)：输入参数 $params$、公钥 PK_{ID} 以及待加密消息 m，输出一个密文 c；

(7)解密算法(Decrypt)：输入参数 $params$、用户身份 ID、(全)私钥 SK_{ID} 以及待解密的密文 c，输出一个密文 m 或一个错误指示符。

3 基于椭圆曲线离散对数的无证书混合加密方案

本文基于椭圆曲线离散对数问题和无证书加密一般模型，提出一个新的无证书混合加密方案。方案的具体执行过程如下：

(1)密钥生成中心系统参数生成：选取一个基域 F_q，q 为一个大素数。选取一个定义在 F_q 上的椭圆曲线 $E(F_q)$ 和 $E(F_q)$ 上的一个生成元 P，其阶为一个可整除 $\#E(F_q)$ 的大素数 n。选择一个安全对称加密算法 (ENC_K, DEC_K)。选择 2 个密码安全 Hash 函数 $H:\{0,1\}^* :\to Z_q^*$，$H_1:\{0,1\}^* :\to \{0,1\}^K$，其中，$\{0,1\}^K$ 是对称加密使用的会话密钥空间。公开系统参数 $params=\{q,E(F_q),n,P,H,H_1,\{0,1\}^K,(ENC_K,DEC_K)\}$。

(2)密钥生成中心生成主密钥：中随机选取一个正整数 $s\in_R Z_n^*$，设主私钥为 $Msk=s$；计算主公钥 $Mpk=sP$；密钥生成中心保留主私钥 Msk，公开主公钥 Mpk。

(3)密钥生成中心生成部分私钥：用户将身份 ID 提交给密钥生成中心后，密钥生成中心随机选取一个正整数 $t\in_R Z_n^*$，计算 $T=tP=(x_T,y_T)$；计算 $e_{ID}=H(ID)+x_T \mod n$；计算 $w=(se_{ID}+t) \bmod n$。设部分私钥为 $D_{ID}=(T,w)$，通过安全信道将其传输给用户。

(4)用户私钥生成：随机选取一个正整数 $sk\in_R Z_n^*$，设用户私钥为 $SK_{ID}=sk$，用户自己保留。

(5)用户公钥生成：计算 $PK=skP=(x_{PK},y_{PK})$；随机选取一个正整数 $r\in_R Z_n^*$，计算 $Q=rP=(x_Q,y_Q)$；计算 $e_{PK}=H(x_{PK}\|y_{PK})+x_Q \bmod n$；计算 $u=(r-w\cdot e_{PK}) \bmod n$。设用户公钥为 $PK_{ID}=(PK,T,e_{PK},u)$，用户将 PK_{ID} 公开给系统其他 用户。

(6)加密，分为 3 个执行过程：

1)验证用户公钥的真实性，计算 $(x_Q',y_Q')=uP+(H(ID)+x_T \bmod n)\cdot e_{PK}\cdot Mpk+e_{PK}T$，计算 $e_{PK}'=H(x_{PK}\|y_{PK})+x_Q'$。如果 $e_{PK}'=e_{PK}$，验证成功；否则验证失败放弃加密。明显地，验证的正确性基于：

$$uP+(H(ID)+x_T \bmod n)\cdot e_{PK}\cdot Mpk+e_{PK}T=(u+e_{PK}w)P=rP$$

2)生成会话密钥及其封装：随机选取一个正整数 $k\in_R Z_n^*$，计算 $K=H_1(kPK+kP)$；定义会话密钥的封装为 $C_1=kP$；

3)加密消息：对消息 M，计算 $C=ENC_K(M)$，输出密文 (C_1,C)。

(7)解密，分为 2 个执行过程：

1)恢复会话密钥：$K/\perp=H_1(skC_1+C_1)$；

2)解密消息：若上文的计算结果为 $\perp$，则输出错误指示；否则，计算 $M=DEC_K(C)$ 恢复明文。

4 安全性讨论

对于无证书加密方案需要从 2 方面考虑其安全性，即公钥的安全性和消息的保密性安全。

在本方案中，用户的发布的公钥为 $PK_{ID}=(PK,T,e_{PK},u)$，其中，PK 是最终参与会话密钥生成的工作公钥；T,e_{PK},u 是对 PK 的签名。因此，如果存在攻击者要伪造工作公钥，他必须要能够生成一对有效的伪工作公钥和签名对。现对攻击者的伪造签名能力进行分析，假设攻击者在椭圆曲线上随机选择一个伪工作公钥 $PK^*=(x_{PK^*},y_{PK^*})$，那么成功伪造用户公钥，就需要生成一个有效的伪工作公钥 PK^* 的签名。基于公开的系统参数首先攻击者可以从 Z_n^* 中随机选取一个正整数 r^*，并计算 $Q^*=rP=(x_{Q^*},y_{Q^*})$；攻击者可以计算得到 $e_{PK^*}=H(x_{PK^*}\|y_{PK^*})+x_{Q^*} \bmod n$；随后计算 $u^*=(r^*-w\cdot e_{PK}^*) \bmod n$ 来完成对伪工作公钥的签名，其中，w 是来自于密钥生成中心的秘密部分私钥，攻击者并不知道任何关于 w 的信息。本文考察攻击者是否可以伪造一个 w。密钥生成中心通过计算 $(se_{ID}+t) \bmod n$ 得到 w，其中，$e_{ID}=H(ID)+x_T \bmod n$，在已知 ID 和公开参数 T 的前提下是攻击者可计算的，余下的 s 是密钥中心的保密主私钥，t 是在 w 计算过程中密钥生成中心随机均匀选取的保密参数，且参数 t 在每次构建部分私钥的时候都仅使用一次，那么 $w=(se_{ID}+t) \bmod n$ 计算实质是主私钥和参数 t 为 e_{ID} 提供了一次性的签名计算，且主私钥 s 和参数 t 在信息论的意义上相互保护。如果在仅仅已知主公钥 $Mpk=sP$ 和公开参数 $T=tP$ 的前提下，攻击者能够成功的伪造 w，那么意味着用户可解决椭圆曲线上的离散对数问题。而已知椭圆曲线上的离散对数问题是困难的其概率是可以忽略的。在随机均匀选取 s 和 t 的条件下，攻击者最多以 $1/n^2$ 的概率猜中 s 和 t，从而计算的到 w，进而成功伪造 $u^*=(r^*-w\cdot e_{PK}^*) \bmod n$，而在 n 是一个大素数的条件下该概率是可以忽略的。

在本方案中通过对公钥的验证，以及产生的会话密钥来保证消息的机密性。发送者通过用户身份 ID，密钥生成中心的公开主公钥 Mpk 计算 $(x_Q',y_Q')=uP+(H(ID)+x_T \bmod n)\times e_{PK}\times Mpk+e_{PK}T, e_{PK}'=H(x_{PK}\|y_{PK})+x_Q'$，如果验证通过再进行会话密钥产生及封装，这样保证了公钥的真实性。随后发送者通过计算 $K=H_1(kPK+kP)$ 产生会话密钥，其中，k 是均匀随机选取的参数；PK 是从用公钥中抽离出的工作公钥。对消息的加密采用了对称加密算法利用会话密钥对消息进行加密保护。公开的密文为 (C_1,C)，其中，$C_1=kP$ 是会话密钥的封装；C 是明文加密的结果。对攻击者来说在只知道密文的前提下恢复明文消息是困难的，因为 $K=H_1(kPK+kP)$，攻击者可见的公开参数包括工作公钥 PK 和会话密钥封装 $C_1=kP$，而基于椭圆曲线对数困难问题攻击者通过 $C_1=kP$ 恢复出秘密参数 k 的概率是可以忽略的，即在 k 是均匀随机选取的前提下，攻击者猜测出 k 的概率是至多为 $1/n$。而对于接受用户，因为有私钥 $SK_{ID}=sk$，所以可以成功地通过获得的会话密钥封装 C_1 恢复会话密钥，即 $K=H_1(skC_1+C_1)$。对每一次加密都产生随机产生新的参数 k，从而得到新的会话密钥的前提下，利用对称加密算法加密消息相当于一次一密的加密方式，因为加密消息具有前向安全性，即使攻击者截获密文也无助于破解密文。

（下转第 37 页）