

一种高效的基于身份的签密方案

王大星¹, 滕济凯²

(1 滁州学院数学系 信息与计算科学研究所, 安徽 滁州 239000; 2 中国科学院 软件研究所, 北京 100190)

摘 要: 签密能够在一个合理的密码协议中同时完成数字签名和公钥加密两种功能, 减少了通信成本. 利用椭圆曲线的双线性对性质, 提出了一种基于身份的签密方案. 该方案同时满足签密方案所具有的机密性、不可伪造性、前向安全性, 而且能抵抗信息接收方的欺骗攻击. 通过分析和比较, 该方案具有很好的安全性和较高的效率.

关键词: 签密; 基于身份的密码体制; 双线性对; 前向安全

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2010)07-0057-03

An Efficient ID-based Signcryption Scheme

WANG Da-xing¹, TENG Ji-kai²

(1 Institute of Information and Compute Science, Department of Mathematics of Chuzhou University, Chuzhou 239012, China; 2 Institute of Software, the Chinese Academy of Sciences, Beijing 100190, China)

Abstract: Signcryption can combine both the functions of digital signature and public key encryption in a logical cryptography protocol, at lower computational costs and communication. A new efficient identity-based signcryption scheme was proposed by characteristics of bilinear map of elliptic curve. This scheme can satisfy the confidentiality, unforgeability and forward security required by signcryption. What's more, the scheme is secure against dishonest recipient. This scheme is also very efficient and secure after analyzing and being compared with other schemes.

Key words: signcryption; identity-based cryptograph; bilinear map; forward security

1 引言

近几年来, 基于身份的密码体制成为密码学界的一个研究热点. 这种密码体制最初是由 Shamir^[1]于 1984 年提出, 其目的是为了简化密钥管理. 在基于身份的密码体制中, 用户的公钥是直接从其身份信息(如姓名、身份证号、E-mail 地址等)得到, 而私钥则是由一个称为私钥生成中心(PKG)的可信方生成. 自 1984 年来, 人们相继提出了许多实用的基于身份的签名方案, 一个满意的基于身份的加密方案是由 Boneh 和 Franklin^[2]利用椭圆曲线上的双线性对设计的.

由于签密和基于身份的密钥体制具有很多优点, 于是, 人们开始研究基于身份的签密方案. 文献[3]中定义了基于身份的签密方案的安全模型, 利用

双线性对构造了第一个基于身份的签密方案, 该方案提供了消息的保密性和签名的不可伪造性. 文献[4]中提供了机密性和前向安全性, 但是不满足公开验证性, 且其签密的运算效率较低. 文献[5]中设计了一个能同时满足公开验证性和前向安全性的签密方案, 然而签密的密文较长, 并且不满足其他一些特性.

本文利用双线性对提出了一个新的基于身份的具有前向安全的签密方案, 该方案可以在基于身份的密码体制中运行, 而且还可以使接受者在不作任何转换的情况下由任意第三方来验证密文消息的来源. 由于使用预处理算法, 方案效率较高, 密文长度较短.

2 双线性对知识及困难问题假设

设 G_1, G_2 为两个阶均为大素数 q 的群. 其中 G_1 是一个加法循环群, G_2 是一个乘法循环群. 设 P

收稿日期: 2009-06-05; 修回日期: 2009-08-05

基金项目: 国家自然科学基金项目(90604034); 滁州学院科研基金资助项目(2008kj011B)

是 G_1 的任意一个生成元. 假设离散对数问题(DLP)在 G_1 和 G_2 中都是困难的. 密码学中的双线性对是指一个满足下列性质的映射:

$$e: G_1 \times G_1 \rightarrow G_2$$

双线性: 对于 $\forall P, Q, R \in G_1, a, b \in F_q^*$ 有:

$$(1) e(P + Q, R) = e(P, R)e(Q, R);$$

$$(2) e(P, Q + R) = e(P, Q)e(P, R);$$

$$(3) e(aP, bP) = e(P, P)ab.$$

非退化性: 存在 $P, Q \in G_1$, 使 $e(P, Q) \neq 1$, 即双线性映射 e 不能将 $G_1 \times G_1$ 中所有的对映射到 G_2 中的单位元.

可计算性: 对于所有的 $P, Q \in G_1$, 存在一个有效的多项式时间算法来计算 $e(P, Q)$. 有限域中超椭圆曲线上的 Weil Pairing 和 Tate Pairing 都可以用来构造双线性对.

本文所提签密方案基于以下困难问题:

定义 1 椭圆曲线离散对数问题(ECDLP). 给定一条定义于有限域 F_q 上的椭圆曲线 E 和 E 上的两点 $P, Q \in E(E_q)$, 寻找一整数 x , 使在 E 中有 $xP = Q$.

定义 2 计算性 Diffie-Hellman 问题(CDHP). 已知 P, aP, bP , 其中 $a, b \in Z_q^*$, 计算 abP . 到目前为止, 上述两个问题都没有多项式时间的有效算法可以解决.

定义 3 可判别 Diffie-Hellman 问题(DDHP). 给定 (P, aP, bP, cP) , $a, b, c \in Z_q^*$, 如果有 $c = ab$ 成立, 则称 (P, aP, bP, cP) 为有效 Diffie-Hellman 元组.

3 前向安全的签密方案

3.1 系统的建立及符号说明

令 H_1, H_2 和 H_3 为安全的密码学 hash 函数, $H_1: \{0, 1\}^* \rightarrow G_1, H_2: G_2 \rightarrow \{0, 1\}^n, H_3: \{0, 1\}^n \times G_2 \rightarrow Z_q^*$, 令 $E_{(\cdot)}(\cdot), D_{(\cdot)}(\cdot)$ 为长度为 n 的明/密文的加/解密算法. 令 P 是 G_1 的一个生成元, 私钥生成器(PKG)选择 $S \in {}_R Z_q^*, P_{\text{pub}} = sP$. 主密钥就是 s (保密, 只有 PKG 知道), 系统参数是 $\{G_1, G_2, q, n, p, P_{\text{pub}}, \hat{e}(\cdot, \cdot), H_1(\cdot), H_2(\cdot), H_3(\cdot, \cdot), E_{(\cdot)}(\cdot), D_{(\cdot)}(\cdot)\}$. 现假设用户将自己的身份信息 $ID \in \{0, 1\}^*$ 递交给 PKG, PKG 计算用户的公钥 $Q_{\text{ID}} = H_1(ID) \in G_1$, 用户的签密密钥 $S_{\text{ID}} = s^{-1}Q_{\text{ID}}$, 解密密钥 $D_{\text{ID}} = sQ_{\text{ID}}$, PKG 发送 $\{S_{\text{ID}}, D_{\text{ID}}\}$ 给用户.

3.2 签密方案

现假设 A 要签密一份消息 $m \in \{0, 1\}^n$ 给 B , 则 A 遵循以下步骤:

(1) 随机选择 $x \in {}_R Z_q^*$, 并计算 $X_A = xQ_{\text{ID}_A}$;

(2) 计算:

$$\hat{k}_1 = \hat{e}(X_A, P), \hat{k}_2 = H_2[\hat{e}(X_A, Q_{\text{ID}_B})];$$

(3) 密文 $c = E_{k_2}(m)$;

(4) 签名 $r = H_3(c, \hat{k}_1), S = (x - r)S_{\text{ID}_A}$;

(5) 最后 A 要签发的密文为 $\sigma = (c, r, S)$.

3.3 解密及验证签名算法

B 收到 m 的签密 $\sigma = (c, r, S)$ 后, 按照如下的步骤进行解密并验证签名:

(1) 计算 $R'_A = rQ_{\text{ID}_A}$, 并计算

$$\hat{k}'_1 = \hat{e}(S, P_{\text{pub}})\hat{e}(R'_A, P)$$

$$\hat{k}'_2 = H_2[\hat{e}(S, D_{\text{ID}_B})\hat{e}(R'_A, D_{\text{ID}_B})];$$

(2) 恢复消息 $m = D_{k'_2}(c)$;

(3) 验证签名, 计算 $r' = H_3(c, \hat{k}'_1)$, 如果 $r' = r$, 则接受消息, 否则拒绝.

(4) B 发送 $(\hat{k}'_2, m, \sigma)$ 给第三方.

第三方则通过以下步骤验证:

(1) 计算 $\hat{k}'_1 = \hat{e}(S, P_{\text{pub}})\hat{e}(Q_{\text{ID}_A}, P)^r, r' = H_3(c, \hat{k}'_1)$.

(2) 当且 $r = r'$ 仅当时接受密文;

(3) 当且仅当 $m = D_{k'_2}(c)$ 接受消息的可靠性.

4 新方案的效率提高

还可以在上述新的签密方案中作适当的修正, 使其效率有所提高:

随机选择 $x \in {}_R Z_q^*$, 计算 $k'_1 = \hat{e}(Q_{\text{ID}_A}, P)^x, k'_2 = H_2[\hat{e}(Q_{\text{ID}_A}, Q_{\text{ID}_B})^x]$. 然后 A 再执行相同的步骤. 这样, $\hat{e}(Q_{\text{ID}_A}, P)$ 可以预先计算, 因为它独立于消息和收方 B . 虽然增加了点乘运算和一次指数运算, 但是其效率相对于文献[4]有所提高.

5 新方案的分析

5.1 安全性分析

5.1.1 一致性

可以验证方案中的验证等式的一致性.

$$\begin{aligned} \hat{k}'_1 &= \hat{e}(S, P_{\text{pub}})\hat{e}(rQ_{\text{ID}_A}, P) \\ &= \hat{e}(xS_{\text{ID}_A}, P_{\text{pub}})\hat{e}(rS_{\text{ID}_A}, P_{\text{pub}})^{-1}\hat{e}(Q_{\text{ID}_A}, P)^r \\ &= \hat{e}(Q_{\text{ID}_A}, P)^x. \end{aligned}$$

$$\begin{aligned}\hat{k}'_2 &= H_2[\hat{e}(S, D_{ID_B})\hat{e}(rQ_{ID_A}, Q_{ID_B})] \\ &= H_2[\hat{e}(xS_{ID_A}, D_{ID_B})\hat{e}(rS_{ID_A}, \\ &\quad D_{ID_B})^{-1}\hat{e}(Q_{ID_A}, Q_{ID_B})^r] \\ &= H_2[\hat{e}(Q_{ID_A}, Q_{ID_B})^x].\end{aligned}$$

5.1.2 不可伪造性

由于 $r = H_3(c, \hat{k}'_1)$, $S = (x - r)S_{ID_A}$, 所以由 Hash 函数的单向性和无碰撞性, 敌方即使掌握某个消息 m 的签密, 也不能伪造另外一个签密消息 $m' \neq m$. 只有发方 A 拥有 S_{ID_A} , 才能计算出 S . 我们的方案在自适应选择消息攻击下, 具有不可伪造性.

5.1.3 机密性和前向安全性

对于一个被动攻击者来说, 仅仅知道 σ 和 $\hat{k}'_1$, 要计算出 x 需要解决双线性对的困难问题, 从而不能计算出 $\hat{e}(Q_{ID_A}, Q_{ID_B})^x$, 故不能解密密文. 在签名中, 已知 r 和 S_{ID_A} , 由 S 计算出 x 需要解决离散对数问题. 所以, 方案在自适应选择密文攻击下, 具有机密性和前向安全性^[6].

5.1.4 接收方的欺骗攻击

因为第三方不一定能保证来自接收方的会话密钥 $\hat{k}'_2$ 的正确性, 所以不诚实的接收方能够随机地选取 $\hat{k}'_2$, 使得被签密后的消息 (c, r, S) 被解密成“明文” $m' \neq D_{H_2[\hat{e}(S, D_{ID_B})\hat{e}(Q_{ID_A}, Q_{ID_B})^r]}(c)$, 这个问题在相关文献^[5]中没有讨论. 尽管这种明文 m' 根本没有意义或者格式不正确, 但是我们仍然可以通过修改第三方的验证协议来抵抗这种攻击. 第三方在通过如下的交互协议之后, 可以自己计算出正确的会话密钥 $\hat{k}'_2$.

(1) 计算 $R'_A = rQ_{ID_A}, \hat{k}'_1 = \hat{e}(S, P_{pub})\hat{e}(R'_A, P)$,

$$r' = H_3(c, \hat{k}'_1)$$

(2) 当且仅当 $r = r'$ 时, 接受密文;

(3) 验证等式: $\hat{e}(zD_{ID_B}, P) = \hat{e}(zP_{pub}, Q_{ID_B})$,

其中 $z \in_R Z_q^*$.

(4) 验证等式: $\hat{e}(z^{-1}S, zP_{pub}) = \hat{e}(S, P_{pub})$;

(5) 计算: $\hat{k}'_2 = H_2(\hat{e}(z^{-1}S, zD_{ID_B})\hat{e}(R'_A, Q_{ID_B}))$;

(6) 当且仅当 $m = D_{\hat{k}'_2}(c)$ 表示消息可靠;

以上验证均成立, 则表示协议执行成功.

5.2 效率分析

签密需要 1 次 weil 对运算, 2 次指数运算和 1 次点乘运算; 而对于第三方的验证则需要 2 次 weil 对运算

和 1 次指数运算. 我们的方案的密文长度可表达为

$$|G_1| + |Z_q^*| + |m| + (|ID|)$$

也就是, 由 G_1 中的一个元素和 Z_q 中的一个元素, 以及一些消息比特和发方的身份信息所组成. 而方案^[7]的密文长度为

$$2|G_1| + |Z_q^*| + 2|m| + (|ID|)$$

相对与的方案文献^[4-6], 我们的方案效率有所提高.

6 结束语

本文提出了一个新的基于身份的签密方案, 与目前存在的基于身份的签密方案相比, 方案能够使得任何第三方可以验证, 并且能够抵抗信息接收方的欺骗攻击. 方案的效率更高, 通信成本也较低. 后面的工作是设计更有效的基于身份的签密方案和在标准模型下可证明安全的签密方案.

参考文献:

- [1] Shamir A. Identity - based cryptosystems and signatureschemes, Advances inCryptography - CRYPTO' 84 [C]// Lecture Notes in Computer Science 196. Berlin: Springer - Verlag, 1984: 47 - 53.
- [2] Boneh D, Franklin M. Identity - based encryption from theWeil pairing, advances in cryptography - CRYPTO 2001 [C]// Lecture Notes in Computer Science 2139. Berlin: Springer - Verlag, 2001: 213 - 22.
- [3] Malone - Lee J. Identity based signcryption[EB/OL]. [2009 - 05 - 10]. <http://eprint.iacr.org/2002/098.pdf>.
- [4] Xavier Boyen. Multipurpose identity - based signcryption: a swiss army knife for identity - based cryptography[J]. Lecture Notes in Computer Science, 2003(2729):382 - 398.
- [5] Benoît Libert, Jean - Jacques Quisquater. New identity based signcryption schemes from pairings[C]// IEEE Information Theory Workshop. France, Paris, 2003:155 - 158.
- [6] Florian Hess. Efficient identity based signature schemes based on pairings[J]. Lecture Notes in Comscience, 2003 (2595):310 - 324.
- [7] 宋文敏, 杨广林. 一个扩展的基于身份的签密方案[J]. 微电子学与计算机, 2006, 23(10):138 - 140.

作者简介:

王大星 男(1980 -), 硕士, 讲师. 研究方向为密码学与信息安全.

滕济凯 男(1980 -), 博士研究生. 研究方向为密码学.