

利用双线性映射构建高效身份认证方案

刘连浩, 屈步云

(中南大学 信息科学与工程学院, 长沙 410083)

(syqbystory@163.com)

摘要:基于双线性映射以及椭圆曲线上的离散对数难题,提出了一种认证过程中不需要密钥生成中心介入的用户间身份认证方案,并扩展到有多个密钥生成中心的情形。该方案与已有方案相比具有更少的计算量与通信次数,且实现了双向认证;最后证明所提出的方案在椭圆曲线离散对数难解假设下能有效抵抗伪造用户攻击,冒充攻击和重放攻击,具有较好的安全性。

关键词:双线性映射;基于身份的加密;身份认证

中图分类号: TP309 **文献标志码:** A

Efficient identification scheme with bilinear map

LIU Lian-hao, QU Bu-yun

(School of Information Science and Engineering, Central South University, Changsha Hunan 410083, China)

Abstract: Concerning the discrete logarithm problem of elliptic curve and bilinear mapping, an identification scheme was proposed, and then it was extended to multi-KGC situation. The proposed scheme required less computation and communication than the existing ones and realized mutual authentication. Given the condition of the intractability of the elliptic curve discrete logarithm problem, the proposed scheme was proved secure against forged user attack, impersonation attack and replay attack.

Key words: bilinear mapping; identity-based encryption; identification

0 引言

目前主要的认证系统基本上是针对服务器和用户之间的认证,但现实中存在用户和用户间进行认证的需求,比如战机敌我识别系统中战机间的认证识别。2001 年,在 Boneh 和 Franklin^[1]利用双线性映射实现了基于身份的密码体制后,人们开始利用身份加密体制思想构建认证协议。2004 年, Kurosawa 等^[2]首次给出了基于身份的身份认证方案的形式化定义及其标准模型与安全性证明,并于 2005 年提出了首个标准模型下基于身份的身份认证方案^[3]。2008 年 Chin 等^[4]也给出了一个基于身份的身份认证方案且证明了安全性。但这些都只实现了单向认证,如果扩展到双向认证需要较多的通信次数和计算量。为此,本文提出一种可以在用户间认证的基于身份的双向认证方案,并将该方案扩展到有多个密钥生成中心(Key Generate Center, KGC)的情形,最后给出了方案的安全性证明并比较了效率。

1 双线性映射

假设 G_1 是阶为 q (q 是一个大素数) 的椭圆曲线上的点所构成的循环加群, G_2 是 q 阶循环乘群, G_1 和 G_2 上的离散对数问题都是计算上困难的。

定义 1 双线性映射。映射 $e: G_1 \times G_1 \rightarrow G_2$ 被称为是一个双线性映射^[5], 如果它满足下面三个性质:

1) 双线性。对于 G_1 中的所有点都有:

$$e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q),$$

$$e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2),$$

$$\text{或者 } e(aP, bQ) = e(P, Q)^{ab}, a, b \in Z_q.$$

2) 非退化性。如果 P 是 G_1 的生成元,那么 $e(P, P)$ 是 G_2 的一个生成元,或者说 $e(P, P) \neq 1$, 这里 1 是 G_2 的单位元。

3) 可计算性。存在一个有效的算法,对所有的 $P, Q \in G_1$, $e(P, Q)$ 能够被有效计算。

椭圆曲线离散对数难题是指已知 $P, aP \in G_1$, 求解 a 的问题。本文提出的身份认证方案是基于椭圆曲线离散对数难题在计算上不可解这一假设。

2 基于 ID 的身份认证方案

结合基于双线性映射的身份密码体制^[1]思想,提出基于身份的身份认证系统。在只有一个 KGC 情形下, KGC 不但要生成用户的私钥,而且还要验证用户身份,以及建立传输用户私钥的安全通道。显然要单个 KGC 来完成这些任务在用户较多的情形下负担繁重,由此引入多个 KGC 执行用户注册及密钥分发的任务,同时那些在各 KGC 注册的用户间也能进行身份认证。首先给出单 KGC 情形下的身份认证方案。

2.1 单 KGC 下的用户认证

此方案包括系统参数建立、用户密钥生成及认证交互过程。

1) 系统参数建立。此过程由 KGC 完成, KGC 生成前述的阶为素数 q 的群 G_1 和 G_2 以及 G_1 上的双线性映射 $e: G_1 \times G_1 \rightarrow G_2$, 选取任意一个生成元 $P \in G_1$ 和一个抗碰撞的安全哈希函数 H 。随后 KGC 选择一个随机数 $s \in Z_q^*$ 作为系统的主密钥并保密保存, 计算 $P_{pub} = sP$ 。KGC 公布系统参数为 $\langle G_1, G_2, q, P, P_{pub}, e, H \rangle$ 。

2) 用户密钥生成。用户需将自己的身份信息 ID 提交给 KGC 进行注册, KGC 在对用户身份的合法性和唯一性进行离线验证通过后, 计算 $E_{ID} = H(ID)$, $S_{ID} = ((s + E_{ID})^{-1} \bmod q) \cdot P$,

收稿日期:2009-01-12;修回日期:2009-03-02。

作者简介:刘连浩(1959-),男,湖南澧县人,教授,博士,主要研究方向:网络与信息安全; 屈步云(1984-),男,湖南邵阳人,硕士研究生,主要研究方向:网络与信息安全。

(在极不可能出现的情形 $(s + E_{ID}) \bmod q = 0$ 下, KGC 会要求用户更换 ID), 并将私钥 S_{ID} 通过一个安全渠道分发给用户。

3) 认证过程。需进行认证的用户 A 和 B 间的认证过程包括如下所述的交互步骤:

步骤 1 用户 A 随机选取一随机数 R , 并计算 $X_A = R \cdot S_A$, 然后将 (X_A, ID_A) 作为认证请求信息发送给用户 B , 并临时存储 X_A (这里 ID_A 表示用户 A 的身份, S_A 表示用户 A 的私钥, 下同);

步骤 2 用户 B 收到 A 发送的请求认证信息后, 也随机选取一随机数 N , 进行如下计算 (其中的 “ $|$ ” 符号表示连接符, 下同): $X_B = N \cdot S_B$, $K_{BA} = e(X_A, H(ID_A) \cdot P + P_{pub})^N$, $V_{BA} = H(ID_A | ID_B | X_A | X_B | K_{BA})$; B 将 (X_B, ID_B, V_{BA}) 作为请求响应信息发送给用户 A , 同时临时存储 X_A, X_B, K_{BA} 作后续认证过程备用;

步骤 3 用户 A 收到 B 发送的信息后, 进行如下计算: $K_{AB} = e(X_B, H(ID_B) \cdot P + P_{pub})^R$, $V_{AB} = H(ID_A | ID_B | X_A | X_B | K_{AB})$; 然后通过比较 V_{AB} 与 V_{BA} 的值的异同来决定是否通过对用户 B 的身份认证, 如果相同, 则认可 B 的身份, A 再计算 $V_{AB}' = H(ID_B | ID_A | X_B | X_A | K_{AB})$ 并将 (ID_A, V_{AB}') 作为对用户 B 的认证响应发送给 B ; 否则, 做出拒绝的决定并终止本次认证过程;

步骤 4 在收到 A 传回的信息后, B 结合存储的 X_A, X_B, K_{BA} 计算出 $V_{BA}' = H(ID_B | ID_A | X_B | X_A | K_{BA})$, 然后通过比较 V_{AB}' 与 V_{BA}' 值的异同做出认可或者拒绝 A 的身份的决定。

至此, 用户 A 和 B 完成了双向身份认证, 认证过程结束。

2.2 多 KGC 下的用户认证

本节我们给出存在多个 KGC 执行用户注册及密钥分发的任务的环境下, 在不同 KGC 注册的用户间也能进行身份认证的方案。

1) 系统参数建立。假定存在一个顶级 KGC 生成整个系统所需的参数 G_1, G_2, q, P, e , 抗碰撞的安全哈希函数 H , 并选择随机数 $s \in \mathbb{Z}_q^*$ 作为系统的主密钥, 计算 $P_{pub} = sP$ 。然后 KGC 公布系统参数 $(G_1, G_2, q, P, P_{pub}, e, H)$ 。与单 KGC 情形不同的是这里引入了多个二级 KGC, 记为 KGC_i , 顶级 KGC 负责验证 KGC_i 的合法性和各 KGC_i 身份的唯一性, 并将系统主密钥 s 分发给分 KGC_i 共享, 由各分 KGC_i 负责处理用户的注册事宜。每个 KGC_i 除了拥有系统主密钥 s 外, 还各自选择一个 s_i 作为自己的私钥, 控制用户注册过程中用户密钥的生成。

2) 用户密钥生成。要注册的用户需将自己的身份信息 ID_U 提交给 KGC_i , KGC_i 对用户身份的合法性和唯一性进行离线验证, 为防止不同 KGC_i 为同一 ID 分发密钥, 每个 KGC_i 都将自己的唯一的身份标识连接在用户提交的 ID_U 之后作为用户的 ID, 然后计算 $E_{ID} = H(ID)$, $S_{ID} = ((s + s_i + E_{ID})^{-1} \bmod q) \cdot P$ (在极不可能出现的情形 $(s + s_i + E_{ID}) \bmod q = 0$ 下, KGC 会要求用户更换 ID), 将 S_{ID} 作为用户的密钥和 $P_{pubi} = s_i P$ 一起通过安全渠道传送给用户。

3) 认证过程。在不同二级 KGC 注册的用户 A, B 之间的双向身份认证过程如下 (这里假定 A 已向 KGC_i 成功注册, B 已向 KGC_j 注册, 该过程也适合于在同一 KGC_i 注册的用户 A, B 间的认证)。

① 用户 A 随机选取一随机数 R , 并计算 $X_A = R \cdot S_A$, 然后将 (X_A, ID_A, P_{pubi}) 作为认证请求信息发送给用户 B , 并临时存储 X_A ;

② 用户 B 在收到 A 的信息后, 也随机选取一随机数 N , 进行如下计算: $X_B = N \cdot S_B$, $K_{BA} = e(X_A, H(ID_A) \cdot P + P_{pubi} + P_{pub})^N$, $V_{BA} = H(ID_A | ID_B | X_A | X_B | K_{BA})$; 随后 B 将 $(X_B, ID_B, V_{BA}, P_{pubj})$ 作为响应信息发送给用户 A , 同时临时存储 X_A, X_B ,

K_{BA} 用作后续认证过程备用;

③ 用户 A 收到 B 的信息后, 进行如下计算: $K_{AB} = e(X_B, H(ID_B) \cdot P + P_{pubj} + P_{pub})^R$, $V_{AB} = H(ID_A | ID_B | X_A | X_B | K_{AB})$; 然后比较 V_{AB} 与 V_{BA} 的值的异同来决定是否通过对用户 B 的身份认证, 如果相同, 则认可 B 的身份, A 再计算 $V_{AB}' = H(ID_B | ID_A | X_B | X_A | K_{AB})$ 并将 (ID_A, V_{AB}') 作为对用户 B 的认证响应发送给 B ; 否则, 做出拒绝的决定并终止认证过程;

④ 在收到 A 传回的信息后, B 计算出 $V_{BA}' = H(ID_B | ID_A | X_B | X_A | K_{BA})$, 而后与第 (3) 步类似, 通过比较 V_{AB}' 与 V_{BA}' 值的异同做出认可或者拒绝 A 的身份的决定。

至此, 用户 A 和 B 完成对对方的身份认证过程, 认证过程结束。

3 认证的正确性证明与安全性

3.1 正确性证明

首先证明所提出的方案的正确性, 即实现了身份认证的功能。

证明 方案的认证正确性是由如下运算来保证的, 在单 KGC 情形下, 由于:

$$K_{AB} = e(X_B, H(ID_B) \cdot P + P_{pub})^R = e((s + H(ID_B))^{-1} \cdot P, H(ID_B) \cdot P + s \cdot P)^{RN} = e(P, P)^{RN};$$

$$K_{BA} = e(X_A, H(ID_A) \cdot P + P_{pub})^N = e((s + H(ID_A))^{-1} \cdot P, H(ID_A) \cdot P + s \cdot P)^{NR} = e(P, P)^{NR};$$

从而能够得到 $K_{AB} = K_{BA}$, 进而有 $V_{AB} = V_{BA}$ (或 $V_{AB}' = V_{BA}'$), 所以对于合法的用户我们能够正确地识别出彼此的身份。

同理, 对多 KGC 情形有:

$$K_{AB} = e(X_B, H(ID_B) \cdot P + P_{pubj} + P_{pub})^R = e((s + s_j + H(ID_B))^{-1} \cdot P, H(ID_B) \cdot P + s_j \cdot P + s \cdot P)^{RN} = e(P, P)^{RN};$$

$$K_{BA} = e(X_A, H(ID_A) \cdot P + P_{pubi} + P_{pub})^N = e((s + s_i + H(ID_A))^{-1} \cdot P, H(ID_A) \cdot P + s_i \cdot P + s \cdot P)^{NR} = e(P, P)^{NR};$$

从而 $K_{AB} = K_{BA}$, 进而有 $V_{AB} = V_{BA}$ (或 $V_{AB}' = V_{BA}'$), 对于合法的用户也能正确地识别出彼此的身份。

所以我们提出的方案在两种情形下均能实现对用户身份的认证。

3.2 安全性分析

一个高效实用的认证协议必须是安全的, 下面我们对提出的基于身份的身份认证方案进行安全性分析并证明其安全性。

结论 1 认证方案能抵抗伪造用户攻击。

证明 对单 KGC 情形而言, 假设某一潜在攻击者 U , 期望通过给定的公开参数自行生成公私密钥对 ID_U 和 S_U 试图欺骗合法用户 A 来通过身份认证, 根据 3.1 节的分析, U 提供的 ID_U 和 S_U 应能满足 $K_{AU} = e(X_U, H(ID_U) \cdot P + P_{pub})^R = e(M \cdot S_U, (H(ID_U) + s) \cdot P)^R = e(P, P)^{RM}$ (假定 M 为 U 在认证过程中选择的随机数), 从而使得用户 A 计算出来的 V_{AU} 与 U 发送的 V_{UA} 一致而通过验证; 亦即 U 提供的 S_U 应满足 $S_U = (H(ID_U) + s)^{-1} \cdot P$, 而根据系统公开的信息, U 只知道哈希函数 H 以及用于求逆的模数 q , 要想再得到系统的主密钥 s , U 将面临已知 P 和 $P_{pub} = s \cdot P$ 求 s 的问题, 这就将问题转化到求解椭圆曲线离散对数这一难题, 在基于椭圆曲线离散对数难题不可解的假设下, 保障了认证方案的安全性, 使得潜在的攻击者 U 无法通过伪造身份来欺骗合法用户, 认证方案在单 KGC 情形能抵抗伪造用户攻击。同理, 对多 KGC 情形而言, U 提供的 S_U 应能满足 $S_U = (H(ID_U) + s + s_i)^{-1} \cdot P$, 同单 KGC 情形的分析一样, 他仍然无法提供正确的 s 来达到攻破方案欺骗用户认可其身份的目的, 因而多 KGC 情形也能抵抗伪造用户攻击。

结论2 认证方案能抵抗冒充攻击。

证明 由结论1的证明可知,一方面攻击者 U 对已在KGC注册的用户的身份 ID ,无法自行生成对应的用户密钥;另一方面,由于系统使用的哈希函数的强抗碰撞性, U 无法找到另一个不同于 ID 的 ID' ,使得 $H(ID) = H(ID')$ 从而通过向KGC提交 ID' 注册来获得身份为 ID 的用户的密钥,因而 U 无法冒充其他用户,因而所提出的方案能抵抗冒充攻击。

结论3 认证方案能抵抗重放攻击。

证明 在提出的两个情形中,用户交互认证过程引入的随机数因子能很好地防止重放攻击。就单KGC情形而言,假设某一潜在的攻击者 U 窃听了用户 A 和 B 认证的全过程并获得了他们之间传送的所有数据,如果 U 用所窃听到的 A 发起认证时发送给 B 的信息再次发送给 B ,由于每次认证过程中所采用的随机数都不同, B 回复给 U 的响应信息已是相对于另一个随机数 N' 而产生的, U 窃听到的上一次 A 回复给 B 的应答信息已不能再用于此次认证过程来通过 B 的认证;类似地,在随机数因子的保护下, U 也无法用窃听到的信息欺骗 A ,单KGC情形能有效抵抗重放攻击。同理多KGC情形与单KGC情形在认证过程的一致性,使得多KGC情形也能抵抗重放攻击。

结论1~3表明了所提出的认证方案能有效防止主动攻击;同时由于认证过程中引入了随机数因子使得每次认证时发送的信息都不一样,而在椭圆曲线离散对数难题不可解的假设下即使敌手窃取到认证的消息也无法提取有用信息实施攻击,因而方案也能防被动攻击,通过分析证明了方案有较好的安全性。

3.3 效率分析与比较

方案只使用了双线性映射以及通用的哈希函数,具有较高的实现效率。表1给出了本文的方案与文献[3]及文献[4]的基于双线性映射的方案就认证过程中所需要的一些主要运算的运算次数和通信次数进行了对比。在这些均基于双线性映射的方案中,本文的方案对耗时较多的对运算和指数运算的次数比文献[3]及文献[4]的方案都要少;另外方案的通信次数均为3,但前两个方案都只实现了单向认证,因而本文的方案在计算量与通信次数需求上明显优于其他两个方

案,具有更好的性能。

表1 认证过程计算量及通信量对比

认证方案	对运算	指数运算	群内运算	哈希运算	通信次数
文献[3]	3	5	6	2	3
文献[4]	3	5	$n+4$	2	3
本文方案	2	2	6(单KGC) 8(多KGC)	4	3

注: n 为用户身份ID进行哈希后的汉明重量^[4]。

4 结语

提出了不同情形下的基于双线性映射的身份认证方案,实现用户与用户之间的身份认证,在用户认证过程中并不需要KGC的介入,而且第二种情形可以用于在不同KGC注册的用户之间进行身份认证识别,使得该方案非常适合于现代战时敌我识别等需要在个体间进行认证的应用领域。与已有方案相比,本文的方案需要更少计算量和通信次数,具有更好的效率。所提出的认证方案在椭圆曲线离散对数问题不可解的假设下,能有效抵抗假冒用户攻击,冒充攻击和重放攻击,具有很好的安全性能。

参考文献:

- [1] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]// Advances in Cryptology: CRYPTO 2001. Berlin: Springer, 2001: 213-229.
- [2] KUROSAWA K, HENG S H. From digital signature to ID-based identification/signature[C]// Public Key Cryptography: PKC 2004. Berlin: Springer, 2004: 248-261.
- [3] KUROSAWA K, HENG S H. Identity-based identification without random oracles[C]// Computational Science and Its Applications: ICCSA 2005. Berlin: Springer, 2005: 603-613.
- [4] CHIN J J, HENG S H, GOI B M. An efficient and provable secure identity-based identification scheme in the standard model[C]// Public Key Infrastructure. Berlin: Springer, 2008: 60-73.
- [5] 徐茂智,游林.信息安全与密码学[M].北京:清华大学出版社,2007.

(上接第1778页)

置的置乱和像素的替换,这起到了很好的扩散效果。同时,置乱阶段中的两个XOR操作也对扩散和置乱起了很大的作用。第三,改进算法中加密数据流 $\{b_x, b_y, b_z\}$ 不但与Lorenz混沌系统的初始条件有关,而且还与明文产生的向量 $Z = \{Z_1, Z_2, Z_3, \dots, Z_{N \times N}\}$ 有联系,这样便可有效地抵抗选择明文和已知明文攻击。而加密数据流 $\{b_x, b_y, b_z\}$ 的链式产生方式也能促成很好的扩散效应来抵抗选择明文攻击。

5 结语

本文首先指出了原加密算法中的缺点,之后分别在安全性和速度上提出了改进方案,最后对改进算法进行了理论分析和实验仿真。实验结果表明,改进算法在保持了原加密算法优点的同时,解决了原算法的缺陷;并且,改进算法能够在较少的轮数下就能取得很好的加密效果。

参考文献:

- [1] SUN F Y, LIU S T, LU Z W. Image encryption using high-dimension chaotic system[J]. Chinese Physics, 2007, 16(12): 3616-3623.
- [2] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps[J]. International Journal of Bifurcation and Chaos, 1998, 8

(6): 1259-1264.

- [3] LIAN S, SUN J, WANG Z. Security analysis of a chaos-based image encryption algorithm[EB/OL]. [2008-11-19]. <http://arxiv.org/pdf/cs/0608119>.
- [4] ZHANG L, LIAO X, WANG X. An image encryption approach based on chaotic maps[J]. Chaos, Solitons and Fractals, 2005, 24(3): 759-765.
- [5] CHEN G, MAO Y, CHUI C. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals, 2004, 21(3): 749-761.
- [6] GUAN Z, HUANG F, GUAN W. Chaos-based image encryption algorithm[J]. Physics Letters A, 2005, 346(1/3): 153-157.
- [7] GAO H, ZHANG Y, LIANG S, LI D. A new chaotic algorithm for image encryption[J]. Chaos, Solitons and Fractals, 2006, 29(2): 393-399.
- [8] PAREEK N K, PATIDAR V, SUD K K. Image encryption using chaotic logistic map[J]. Image Vision Computing, 2006, 24(9): 926-934.
- [9] 袁益民,盛利元,尚芳.基于TD-ERCS混沌系统的图像加密方法[J].计算机应用,2008,28(4):906-909.
- [10] 高洁,袁家斌,徐涛,等.一种基于混合反馈的混沌图像加密算法[J].计算机应用,2008,28(2):434-436.