

基于椭圆曲线的多方密钥协商协议

高隆¹, 唐春明¹, 张永强²

(1. 广州大学数学与信息科学学院, 广东 广州 510000;

2. 数安时代科技股份有限公司, 广东 广州 510000)

摘要: 密钥协商协议是在公开的信道上, 2 个或者多个参与方之间进行的共享密钥机制。利用安全单向函数, 设计了一种基于椭圆曲线的多方密钥协商协议, 协议能够满足密钥交换协议的安全特性, 并且具有较高的计算效率。

关键词: 多方密钥协商协议; 椭圆曲线; 安全单向函数; 离散对数

中图分类号: TP309.2; TP309.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00056

Multi-parties key agreement protocol based on elliptic curve

GAO Long¹, TANG Chun-ming¹, ZHANG Yong-qiang²

(1. School of Mathematics and Information Science, Guangzhou University, Guangzhou 510000, China;

2. Number of Times Polytron Technologies Inc., Guangzhou 510000, China)

Abstract: The key agreement protocol is a shared key mechanism between two or more participants in a public channel. A multi key agreement protocol based on elliptic curve was designed by using the secure one-way function. The protocol was based on password authentication. The protocol designed can satisfy the security characteristics of the key exchange protocol, and has high computing efficiency.

Key words: multi-parties key agreement protocol, elliptic curve, hash function, discrete logarithm

1 引言

随着计算机和网络的发展, 信息安全已经成为一个重要课题。在开放的网络中, 用户用密钥加密要交换的消息是实现信息安全的重要方法。密钥协商是 2 个或者多个参与方在公开的信道中, 协商建立一个共享的秘密密钥。在 1976 年以

前, 人们在通信领域的观念是: 如果不事先进行秘密共享是无法进行安全保密通信的, 即在通信前要先进行密钥共享。1976 年, 第一个现代密钥交换协议 Diffie-Hellman^[1]的提出, 打破了人们的传统观念, 使用户可以在完全公开的信道上进行秘密共享。DH 协议的安全性是基于在有限域上离散对数的难解性, 该协议没有进行认证, 容易

收稿日期: 2016-03-07; 修回日期: 2016-04-23。通信作者: 唐春明, 395033429@qq.com

基金项目: 国家自然科学基金资助项目 (No.11271003); 广东省自然科学基金资助项目 (No.2015A030308016); 广东省教育厅基础研究重大基金资助项目 (No.2014KZDXM044); 教育部高等学校博士学科点专项科研联合基金资助项目 (No.20134410110003)

Foundation Items: The National Natural Science Foundation of China (No.11271003), The Natural Science Foundation of Guangdong Province (No.2015A03030816), Major basic Research Project of Guangdong Provincial Department of Education (No.2014KZDXM044), The Ministry of Education in Colleges and Universities Specialized Research Fund for the Doctoral Program (No.20134410110003)

受到中间人的攻击,为了弥补没有认证这一漏洞,学者提出了认证密钥协商协议,本文协议主要是基于口令。

基于口令的多方密钥协商协议允许参与者利用低熵的口令进行密钥协商,这种通信方式的优势在于参与者无需存储高熵的难以记忆的密钥即可完成密钥协商,建立会话密钥。近年来,已经有一些基于口令的多方密钥协商协议^[2-4]被提出,但这些协议大多建立在“同口令认证模型”基础上,即假设它们事先会共享一个秘密口令。文献[5]提出2种新的基于口令协商协议,建立在不同口令认证上,即每个用户只与服务器共享口令。文献[6]利用安全单向函数构造了一种基于椭圆曲线的三方密钥协商协议,并利用分组的思想推广到了多方。文献[7]是基于身份认证的利用双线性对构造的多方密钥协议,但在协议过程中也利用了“相同的口令”这一思想。本文在文献[6]的基础上结合文献[7]利用安全单向函数提出一种新的基于椭圆曲线的密钥协商协议,协议是建立在“不同口令认证”的基础上,协议过程相对简单,计算速度相对较快。

2 预备知识

2.1 Diffie-Hellman 密钥协商方案 (CDH)

公开域参数包括群 $(G, \cdot)$ 和阶为 q 的元素 $g \in G$, 假设有 A、B 2 个用户进行协商。

- 1) 用户 A 选取一个随机数 $a, 0 \leq a \leq n-1$, 然后计算 $K_A = g^a$ 并将 K_A 发送给 B。
- 2) 用户 B 选取一个随机数 $b, 0 \leq b \leq n-1$, 然后计算 $K_B = g^b$ 并将 K_B 发送给 A。
- 3) 用户 A 计算 $K = (g^b)^a$, 用户 B 计算 $K = (g^a)^b$, 很明显 $K = (g^a)^b = (g^b)^a = g^{ab}$ 为共享密钥。

这里的 CDH 通常指的是计算 Diffie-Hellman 问题,这个困难问题是基于有限域上离散对数的难解性,即 $g^x = u$, 求解 x 是困难的。同样的基于椭圆曲线上的 Diffie-Hellman 协议也是基于有限域上离散对数的难解性,即 $nP = m$, P 是椭圆曲线上的基点,求解 n 是困难的。

2.2 密钥协商协议的安全特性

由于密钥协商协议是在公开的网络情况下各

个参与者得到的共享密钥的解决方法,协议的安全性至关重要,文献[8]给出了一般的协议需要满足的安全性。

已知密钥安全 (known-key security)。由于共享密钥中含有每个参与者由随机数生成器生成的短私钥,故每次协议生成的密钥都是唯一的,以前的密钥泄露,攻击者也不会知道现在正在交换的密钥。

完美前向保密性 (perfect forward secrecy)。如果一个参与者或者多方参与者长期使用的私钥长期泄露,也不会影响在此之前生成的共享密钥,这就是完美前向保密性。

密钥不可控制性 (key control property)。由于共享密钥是用各方参与者共同协商产生,无论是哪方都不能对协商的共享密钥预先控制其选定的值。

抵抗密钥泄露攻击 (resist key leakage attack)。协议要能抵抗如下攻击:假设用户 A 的私钥长期泄露,那么攻击者能够假扮 A 用户欺骗其他用户,但是不能扮演其他用户欺骗用户 A。

密钥共享可知性 (key sharing)。参与协议的任何一个用户都不可能在不知晓的情况下进行共享密钥或者某几个用户在某个用户不知晓的情况下进行密钥共享。

2.3 参数设定

假定 E 是定义在有限域 $GF(q)$ 上的椭圆曲线; $\#E(GF(q))$ 表示满足 $a \in Z_n^*$ 方程的椭圆曲线上的点的个数。 P 为椭圆曲线 E 的一个阶为素数 n 的基点, G_1 是由 P 生成的循环加法群。 $f: P \rightarrow Z_n^*$ 表示椭圆曲线上的一个离散点 P 到 Z_n^* 的安全单向函数, H 是散列函数, E_{pw} 表示用口令进行加密, T 表示时戳, $sig_i(m)$ 表示用户的签名。 S 为协议中唯一的服务器,是用户与服务器的共享口令,只有用户与服务器知道。

3 协议过程

在文献[6]中,三方协议过程大概如下。

- 1) 用户 A 随机选择一个参数,计算 $K_A = ap$, 并发送给 B。
- 2) 用户 B 随机选择一个参数 $b \in Z_n^*$, 计算 $K_B = bp$, 并发送给 A。
- 3) 用户 A 计算密钥 $K = f(aK_B)p$, 并发送给 C。

4) 用户 C 随机选择一个参数 $c \in Z_n^*$, 计算 $K_C = cp$, 并分别发送给 A 和 B。

5) 用户 A 计算 $K_{ABC} = f(abp)cp$, 用户 B 计算 $K_{ABC} = f(abp)cp$, 用户 C 计算 $K_{ABC} = cK = f(abp)cp$, 这样就得到了三方共享密钥。

文献[6]中的三方协议流程如图 1 所示。

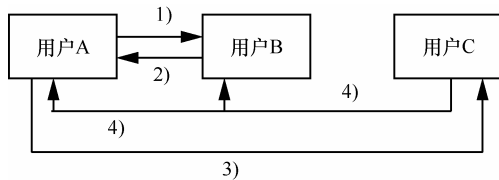


图1 文献[6]三方协议流程

下面给出在文献[6]的基础上, 受文献[7]启发设计的一种多方密钥交换协议, 假设有 n 个用户进行协商, 参数如 2.3 节中的参数, 这里的用户都是安全可信用户, 协议过程如下。

1) 用户 $\{U_1, U_2, \dots, U_n\}$ 随机选取 $x_i \in Z_q^*$, 计算 $Z_i = x_i P$, 广播 $(m_i, \text{sig}_i(H(m_i)))$, $m_i = ID_i \parallel ID_j \parallel Z_i \parallel T (1 \leq j \leq n, i \neq j)$ 。

2) 先验证签名再计算自己的份额 $\alpha_i = f(x_i x_{i+1} P) x_{i+2} P$, 并且计算 $C_i = E_{pw_i}(\alpha_i)$, 把 $(m_i', \text{Sig}_i(H(m_i')))$, $m_i' = ID_i \parallel s \parallel C_i \parallel T (1 \leq j \leq n, i \neq j)$ 发送给服务器 S。

3) 服务器 S 先验证签名再利用每个用户共享的 pw_i 解密得到 α_i , 并且计算 $K_i = E_{pw_i}(\sum \alpha_j) (1 \leq j \leq n, i \neq j)$, 然后广播 K_i 。

4) 每个参与者在接收到 K_i 后, 各自计算会话密钥为 $K = \alpha_i + \sum \alpha_j = \sum_{i=1}^n \alpha_i = f(x_1 x_2 P) x_3 P + \dots + f(x_n x_1 P) x_2 P$ 。

4 安全性与效率分析

椭圆曲线的选择: 文献[9]给出了椭圆曲线密码体制的安全性分析, 文献[10]给出了一种构造安全椭圆曲线的有效方法。根据文献[9,10], 选择一条安全的椭圆曲线, 在安全椭圆曲线的基础上, 椭圆曲线上离散对数的难解性能够有效地保证密钥参数在通信过程中的安全保密性。

由于该协议的共享密钥是由每个参与者的随机数生成的短私钥构成, 故每次协议生成的密钥

都是唯一的, 并且每次重新开始协议, 用户的短暂私钥都会不一样, 故满足已知密钥安全性和完美前向安全性和密钥不可控性。

该协议采用签名认证, 故满足抵抗密钥泄露攻击和抵抗不知晓密钥共享。

该协议在发送消息中采用了跟文献[6]一样的安全手段, 故具有跟文献[6]中协议一样的能够抵抗消息重放、防篡改、防中间人攻击等安全性质。

文献[6]把协议推广到 n 方中采用的是分组, 过程会相对复杂, 人数越多, 轮数就会越多, 而本文只需要 2 轮。文献[7]利用双线性对计算自己的份额, 相当于进行一次点乘跟一次双线性对计算, 而本文是利用了安全单向函数计算自己的份额, 虽然每个用户计算自己的份额时进行了 2 次点乘和一次单向函数运算, 但计算时间依然小于文献[7]中的计算自己份额的时间, 故具有较高的计算效率。

5 结束语

本文在文献[6]的基础上受到文献[7]启发, 提出了一种比较高效的多方密钥协商协议, 协议利用了签名机制、口令认证, 具有较高的安全性质。这个协议的安全性是建立在用户都是诚实可信的前提下进行的, 假设用户不诚实可信, 就会泄露共享密钥, 当然这会是以后的研究工作。

参考文献:

- [1] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE transactions on Information Theory, 1976, 22(6):644-645.
- [2] ABDALLA M, BRESSON E, CHEVASSUT O, et al. Password-based group key exchange in a constant number of rounds[C]//The 9th International Workshop on Theory and Practice in Public Key Cryptography. c2006: 427-442.
- [3] ABDALLA M, POINTCHEVAL D. A scalable password-based group key exchange in a constant number of rounds[C]//The 9th International Workshop on Theory and Practice in Public Key Cryptography. c2006: 332-347.
- [4] BRESSON E, CHEVASSUT O, POINTCHEVAL D. Group Diffie-Hellman key exchange secure against dictionary attacks[C]//ASIACRYPT'02, Berlin. 2002: 497-514.
- [5] BYUN J, LEE D. N-party encrypted Diffie-Hellman key exchange using Diffie-Hellman passwords[C]//ACNS'05. c2005: 75-90.
- [6] 谢环, 左黎明, 汤鹏志. 一种基于椭圆曲线的多方密钥交换

- 协议[J].信阳师范学院学报, 2011,10(4):13-15.
- XIE H, ZUO L M, TANG P Z. A multi-parties secret key exchange protocol based on elliptic curve[J]. Journal of Xinyang Normal University, 2011, 10(4):13-15.
- [7] 赵婷, 王晓峰, 王尚平, 等. 基于身份的可认证多方密钥协商方案[J].计算机工程, 2008, 34(6): 164.
- ZHAO T, WANG X F, WANG S P, et al. Multi-parties secret key agreement based on authentication[J]. Computer Engineering, 2008, 34(6): 164.
- [8] SIMON B W, JOHNSON D, MENEZES A. Key agreement protocols and their security analysis[C]//The 6th IMA International Conference on Cryptography and Coding. c1997:30-45.
- [9] 刘培, 滕玲莹, 余堃, 等. 椭圆曲线密码体制的安全性分析[J]. 计算机工程与设计, 2006,27(16):2943-2945.
- LIU P, TENG L Y, SHE X, et al. Security analysis of elliptic curve cryptosystem[J]. Computer Engineering and Design, 2006,27(16): 2943-2945.
- [10] 吴开贵, 吴中福. 一种安全椭圆曲线的有效构造方法[J]. 计算机科学, 2006, 33(4):108-110.
- WU K G, WU Z F. An effective method of security elliptic curve[J]. Computer Science, 2006,33(4):108-110.
- [11] 徐秋亮, 李大兴. 椭圆曲线密码体制[J].计算机研究与发展, 1999, 36(11):1281-1288.
- XU Q L, LI D X. Elliptic curve cryptosystem[J]. Computer Research and Development, 1999, 36(11):1281-1288.

作者简介:



高隆 (1991-), 男, 湖南衡阳人, 广州大学硕士生, 主要研究方向为信息安全、密码学。



唐春明 (1972-), 男, 湖南怀化人, 博士, 广州大学教授、博士生导师, 主要研究方向为信息安全、密码学。

张永强 (1976-), 男, 四川成都人, 博士, 数安时代科技股份有限公司高级工程师, 主要研究方向为信息安全。