文章编号:1001 - 9081(2007)05 - 1033 - 02

基于 ECC 的高效可认证组密钥协商协议

余昭平,康 斌
(信息工程大学 电子技术学院,河南 郑州 450004)
(kb5702@tom.com.cn)

摘 要:基于椭圆曲线密码体制(ECC),建立了一个高效可认证的组密钥协商协议。该方案具有如下特点:(1)协议仅需要两轮交互,就可以实现组密钥协商;(2)利用类 ElGamal 密码系统,无需使用密钥分享技术,因此减轻了各参与方的计算量与通信负担;(3)协议能够抵抗自适应选择消息攻击。

关键词:密钥协商;组密钥协商;椭圆曲线;自适应选择消息攻击
中图分类号:TP393 **文献标识码**:A

Efficient authenticated group key agreement protocol based on ECC

YU Zhao-ping, KANG Bin
(*Institute of Electronic Technology, Information Engineering University, Zhengzhou Henan* 450004, *China*)

Abstract: An efficient authenticated group key agreement protocol was proposed based on elliptic curve. This scheme is characterized by the following properties: (1) Participants only need two-round communications to get the group key; (2) Based on ElGamal encryption system, the computational overheads and the communication costs are lessened without key sharing technique; (3) The scheme is effective against adaptive chosen-message attack.

Key words: key agreement; group key agreement; elliptic curve; adaptive chosen-message attack

0 引言

加密、签名、密钥协商及密钥保管是密码学研究的主要内容。早在 1978 年,Diffie 和 Hellman[1] 基于两个参与方的前提下,提出了一个两方密钥协商协议。组密钥协商协议(Group Key Agreement)则是指多个参与方共同商定一个组密钥,使得非组内成员无法计算出该密钥。通常,组中每个成员都有一个基于公钥基础设施(PKI)的密钥(公钥、私钥),他们利用有关认证协议把各自提供的参数安全地广播出去,最后,每个成员利用自己的私钥以及组中所有成员提供的参数,计算出一个共同的组密钥。非组内成员虽然能够通过窃听等手段获得成员在网络间传递的参数,但却无法计算出相应的组密钥。组密钥协商机制在诸如电话会议、网格计算等需要多方参与的工作任务中有着广泛的应用。

在一个理想的组密钥协商协议中,每个成员的地位应该是平等的,在计算过程中无先后之分。文献[2~4]中提供的协议都要求参与人依照一定的顺序参与计算,故影响了协议的效率。密钥协商机制的安全性模型是由 Bellare、Rogaway[2] 以及 Blake-Wilson 等人[3] 建立并完善的。文献[5]提出的协议是以 Diffie-Hellman 假设为基础的。Joux[6] 曾提出了一个基于椭圆曲线双线性对的单轮三方密钥协商方案。Burmester 和 Desmedt[7] 提出了一个仅需要两轮的组密钥协商方案。2004 年,王志伟、谷大武[8] 提出了一个基于树结构和门限思想的组密钥协商协议。在 PKC2004 会议上,Bresson 和 Catalano[9] 提出了一个可认证的组密钥协商方案,其安全性是基于离散对数的困难性及 Shamir 密钥分享方案的安全性。虽然该协议利用了 ElGamal 密码系统,比起其他基于 Diffie-Hellman 问题的组密钥协商协议提高了一定的效率,但是由于方案多次用到插值与赋值运算,因而增大了各方的计算量与系统的通信开销。

组密钥协商协议通常都是把一些公认为安全的双方协议推广到多方的情形,在攻击者无法得到任何一个成员私有输入的假设下,其安全性证明都可以直接规约到基础方案的安全性。因此,组密钥协商协议设计的困难性主要在于效率。对于大的群组来说,密钥协商过程中的计算量、通信量和轮数是至关重要的。通信开销往往是一个方案的重要参数,成为决定其性能的主要因素,也是一个当前应用的最大瓶颈。

基于椭圆曲线密码体制(ECC),本文建立了一个高效可认证组密钥协商协议。它具有如下特点:(1)系统建立在椭圆曲线密码体制下,具有短密钥、速度快、安全性高、计算量低的特点;(2)协议仅需要两轮交互,就可实现组密钥协商;(3)利用 ElGamal 密码系统,不需要使用密钥分享技术,减轻了各参与方的计算量与通信负担;(4)协议能够抵抗自适应选择消息攻击。

1 可认证组密钥协商协议模型

可认证组密钥协商协议模型可以从下面三个方叙述[9]:

1)组的结构

我们考虑的组是静态的,即在执行协议之前,每个成员 P_i 都知道组中成员的数目及其他成员的个人信息(包括身份 ID_i、公钥 PK_i)。在协议执行过程中,组中成员的构成不会发生变化。每个成员都有自己的公/私钥对(PK_i,SK_i),并有相应的签名及验证方案 $Sign_{SK_i}(\cdot)$,$Very_{PK_i}(\cdot)$。各个成员能够同时在网络上发送消息,无先后之分。

2)攻击者的能力

假设攻击者 A 能够控制网络,它可以窃听到各个成员之

收稿日期:2006 - 11 - 14;**修订日期**:2007 - 02 - 07 **基金项目**:现代通信国家重点实验室基金资助项目(51436020405JB5205)
作者简介:余昭平(1962 -),男,安徽宿松人,教授,博士,主要研究方向:密码理论、信息安全; 康斌(1983 -),男,陕西咸阳人,硕士研究生,主要研究方向:协议分析、密码理论.

间传递的信息。如果需要的话,它还可以篡改乃至替换信道上的信息。

3) 安全要求

每个成员记为 $P_i(i = 1,2,\cdots,n)$,任务标识符记为 t,P_i 在任务 t 中计算出的密钥记为 $sk_i^t, i \in \{1,2,\cdots,n\}$,在任务 t 中计算出的组密钥记为 sk^t。一个组密钥协商协议称之为安全的,需要满足如下要求:

(1) 正确性:在攻击者 A 没有阻塞网络的情况下,组中每个成员最后计算出的密钥 $sk_i^t, i \in \{1,2,\cdots,n\}$,满足 $sk_i^t = sk^t$。

(2) 一致性:组密钥变量 sk 在密钥空间 K 中的分布是一致的。

(3) 不可伪造性:攻击者 A 无法计算出 sk^t。

2 一个高效可认证组密钥协商协议

系统建立:记协议中每个成员 $P_i(i = 1,2,\cdots,n)$ 提供认证时的签名/验证密钥为 (SK_i, VK_i)。p 为大素数,E 是有限域 F_p 上的椭圆曲线,$P \in E$ 是 E 上的基点,P 的阶是素数 L(大于 160 位的素数),$H(\cdot)$ 为 F_p 上的无碰撞单向杂凑函数(散列值位数在 160bit 以上)。ID 是当前任务的标识。每个成员 P_i 随机选取 $x_i \in [1, L-1]$ 作为自己的私钥,其相应的公钥为 $y_i = x_i P$。

第一轮:每个成员 P_i:

(1) 随机选取 $a_i \in [1, L-1]$,对每个 $j = 1,2,\cdots,n (j \neq i)$,随机选取 $k_{(i)} \in [1, L-1]$,计算 $M_i = a_i P$,$C_{i,j} = (A_{i,j}, B_{i,j}) = (k_{(i)}P, k_{(i)}y_j + M_i)$;

(2) 把 $C_{i,j}, \sigma_{i,j} = Sign_{SK_i}(C_{i,j}, ID)$ 发送给成员 P_j,$j \in \{1,2,\cdots,n\} (j \neq i)$。

第二轮:P_j 收到 $(C_{i,j}, \sigma_{i,j})$ 后,$i = 1,2,\cdots,n (i \neq j)$:

(1) 对所有收到的数据及其签名进行验证,如果验证未通过便中止协议;

(2) 计算

$$A_j = \sum_{i \neq j} A_{i,j}$$

$$B_j = M_j + \sum_{i \neq j} B_{i,j}$$

$$sk_{(j)} = B_j - x_j A_j = (u_j, v_j)$$

其中 u_j, v_j 分别表示 $sk_{(j)}$ 的横坐标与纵坐标;

(3) 计算 $S_j = H(u_j \| v_j \| ID)$ 及其签名 $Sign_{SK_j}(S_j, ID)$ 并把它们广播出去。

确认:如果每个成员的 $S_i(i = 1,2,\cdots,n)$ 都相同,则 P_i 记会议密钥为 $sk = H(u_i \| v_i)$。

3 分析与讨论

3.1 安全性分析

命题 1 协议是正确的。若组中每个成员 P_i ($i = 1,2,\cdots,n$) 在执行协议时都不产生错误,并且在攻击者 A 没有阻塞网络的情况下,所有成员最后各自计算出的密钥 sk 即为组密钥。

证明

由于

$$\begin{aligned} sk_{(i)} &= B_i - x_i A_i \\ &= M_i + \sum_{j \neq i} B_{j,i} - x_i \sum_{j \neq i} A_{j,i} \\ &= \sum_{i=1}^{n} M_i + \sum_{j \neq i} k_{(j)} y_i - \sum_{j \neq i} k_{(j)} x_i P \\ &= \sum_{i=1}^{n} M_i = (u, v) \\ &= sk_{(j)}, \quad i,j = 1,2,\cdots,n \end{aligned}$$

所以,组中每个成员 $P_i(i = 1,2,\cdots,n)$ 最后计算出的密钥即为组会话密钥 sk,因而协议正确。 证毕

命题 2 协议是一致性的。组密钥变量 sk 在密钥空间 K 中的分布是一致的。

证明 在最后确认阶段,每个成员把指纹 sk 当作组密钥,利用 Hash 的随机性可以直接得出组密钥变量在密钥空间分布的一致性。 证毕

命题 3 协议具有不可伪造性。上述组密钥协商方案能够抵抗自适应选择消息攻击。

证明 我们首先解释在自适应选择消息攻击下攻击者 A 的攻击能力。此时,攻击者 A 能够控制网络窃听到所有成员之间交换的数据,并且在协议未中断的情况下能够多次(在多项式时间内)要求任一成员执行相关计算。记攻击者 A 在第一轮得到的数据为

$$(C_{i,j}, \sigma_{i,j}), \quad i,j = 1,2,\cdots,n$$

由于 $C_{i,j} = (A_{i,j}, B_{i,j}) = (k_{(i)}P, k_{(i)}y_j + M_i)$ 利用了典型的基于 ECC 的类 ElGamal 加密方案,我们得知攻击者 A 恢复出某个 $M_i(i = 1,2,\cdots,n)$ 是椭圆曲线离散对数问题(ECDLP)。而相对来说,目前最好的求解 ECDLP 的算法是 Pollardρ 方法和 Pohling-Hellman 方法,其计算复杂度为 $O(\sqrt{n_p})$ (n_p 为点加群的阶)。但是,当 n_p 含有大素因子(比如,含长度 ≥ 160bit 的素因子)时算法失效[10]。所以攻击者 A 想从 $C_{i,j}$ 中得到某些秘密信息 M_i 是困难的。又因为

$$\sigma_{i,j} = Sign_{SK_i}(C_{i,j}, ID), \quad i,j = 1,2,\cdots,n$$

只是把 $C_{i,j}$ 作为 Hash 函数的一个独立输入项,根据 Hash 函数单向性假设,攻击者 A 也无法恢复出某个 $M_i(i = 1,2,\cdots,n)$。因而,攻击者 A 在第一轮攻击成功的概率是 $\mu(t_1, t_2, \cdots, t_n, n)$,其中 μ 是关于成员总数 n 与每个成员执行次数 t_i ($i = 1,2,\cdots,n$) 的可忽略函数。

在第二轮中,攻击者 A 得到的数据是 $(S_i, Sign_{SK_i}(S_i, ID)), i = 1,2,\cdots,n$,由于 $S_i = H(u_i \| v_i \| ID)$,根据 Hash 函数的单向性假设,攻击者 A 同样无法恢复出杂凑函数的秘密输入项 (u_i, v_i),因而无法伪造可以通过验证的组密钥 sk。综上可知,该组密钥协商协议直接建立在基于 ECC 的类 ElGamal 加密方案的安全性及 Hash 函数单向性假设基础上,因而是安全的。 证毕

3.2 性能分析

下面,我们将本文方案与 Bresson 和 Catalano[9] 方案在计算量、所需时间、通信轮数和通信开销等方面做一详细的比较与分析(其中忽略 Hash 运算与有限域上模加运算的代价)。

为方便起见,用 $|l|$ 表示运算域中元素的长度,T_M、T_E 表示有限域上一次模乘(除)、模指数运算;T_{ECM}、T_{ECA} 表示椭圆曲线上一次标量乘与点(倍)加运算;T_L、T_C 表示构造 Lagrange 插值多项式与赋值运算。此外根据文献[11],可以推得不同运算量相对于有限域上模乘法运算量的比较关系如下:

$$T_{ECM} \approx 29T_M \qquad T_{ECA} \approx 0.12T_M \qquad T_E \approx 240T_M$$

(下转第 1057 页)

要计算当前用户击键特征向量与合法用户标准击键特征之间的灰色斜率关联度,其时间复杂度与基于特征向量的快速识别算法相当,是一种计算复杂度低、识别精度高的基于击键特征的用户身份认证方法。

4　结语

本文提出一种基于击键特征的用户身份认证方法,该方法利用遗传算法在训练样本集中确定能表征用户击键特征的标准特征向量,然后计算待识别用户的当前击键特征序列与标准特征向的灰色斜率关联度来识别合法用户和非法用户,实验表明,该算法性能显著优于基于特征向量、贝叶斯统计模型等算法,已经达到了神经网络方法、数据挖掘和支持向量机算法的最高水平。其识别过程只需要计算当前用户击键特征向量与合法用户标准击键特征之间的灰色斜率关联度,其时间复杂度与基于特征向量的快速识别算法相当,是一种计算复杂度低、识别精度高的基于用户击键特征的身份认证方法。

参考文献:

[1] GAINES R, LISOWSKI W, PRESS S. Authentication by keystroke timing: some preliminary results[EB/OL]. http://www.rand.org/pubs/reports/2006/R2526.pdf, 2006-10-10.

[2] LEGGETT J, WILLIAMS G, USNICK J. Dynamic identity verification via keystroke characteristics[J]. International Journal of Man-Machine Studies, 1991, 35(6): 859-870.

[3] SALEH B, CHARLES S, BASSAM H. Computer-access security systems using keystroke dynamics [J]. IEEE Transaction on Pattern Analysis and Machine Intelligence, 1990, 12(12): 1217-1222.

[4] DE RU WG, ELOFF JHP. Enhanced password authentication through fuzzy logic[J]. IEEE Expert, 1997, 12(6): 38-45.

[5] TAPIADOR M. Fuzzy keystroke Biometrics on Web Security[A]. AutoID'9 Proceedings, Workshop on Automatic Identification Advanced Technologies[C]. IEEE, 1999.133-136.

[6] BROWN M, ROGERS SJ. User identification via keystroke characteristics of typed names using neural networks [J]. International Journal of Man-Machine Studies, 1993, 39(6): 999-1014.

[7] CHO S, HAN C, HAN D, *et al*. Web-based keystroke dynamics identity verification using neural network [J]. Journal of Organizational Computing and Electronic Commerce, 2000, 10(4): 295-307.

[8] YU E, CHO S. Keystroke dynamics identity verification-its problems and practical solutions [J]. Computer & Security, 2004, 23(5): 428-440.

[9] GUVEN A, SOGUKPINAR I. Understanding users' keystroke patterns for computer access security[J]. Computer & Security, 2003, 22(8): 695-706.

[10] 刘思峰. 灰色系统理论及其应用[M]. 第3版. 北京: 科学出版社, 2004.

[11] 邓聚龙. 灰理论基础[M]. 武汉: 华中科技大学出版社, 2002.

[12] SCHMITT LM. Theory of genetic algorithms [J]. TheoreticalComputerScience, 2001, 259(1): 1-61.

(上接第 1034 页)

表 1　组密钥协商方案的效率比较

	计算时间	模乘法运算量	轮数	通信开销
文献[9]	$(n^2+2n)T_E+3n^2T_M+nT_L+(n^2+n)T_C$	$(243n^2+480n)T_M+nT_L+(n^2+n)T_C$	3	$3n^2\|l\|+n\|l\|$
本文方案	$(n^2+2n)T_{ECM}+(3n^2-n)T_{ECA}$	$(29.36n^2+57.88n)T_M$	2	$2n^2\|l\|$

由表 1 可见:我们的方案在计算复杂度上只有 Bresson 和 Catalano[9] 方案的 1/8,在通信代价方面也只有它的近 1/2。因此,对于大的群组来说,我们的方案实现了更高的效率。

4　结语

基于椭圆曲线密码体制,提出了一个高效可认证的组密钥协商协议。协议仅需要两轮交互,就可以实现组密钥协商;利用类 ElGamal 密码系统,无需使用密钥分享技术;协议能够抵抗自适应选择消息攻击。与基于有限域上的离散对数相比,椭圆曲线上的离散对数计算更为困难。分析表明本文方案在计算复杂度与通信代价等方面比文献[9]具有更多的优势。

参考文献:

[1] DIFFIE W, HELLMAN ME. New directions in Cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[2] BELLARE M, ROGAWAY P. Entity Authentication and Key Distribution[A]. Crypto'93, LNCS 773[C]. Berlin: Springer-Verlag, 1994. 232-249.

[3] BLAKE-WILSON S, MENEZES A. Authenticated Diffie-Hellman key agreement protocols [A]. SAC'98, LNCS1556 [C]. Berlin: Springer-Verlag, 1998.339-361.

[4] BRESSON E, CHEVASSUT O, POINTCHEVAL D. Provably authenticated grou PDiffie-Hellman key exchange-the dynamic case [A]. Advances in Cryptology ASIACRPT'01 Proceedings, LNCS [C]. Berlin: Springer-Verlag, 2001. 290-309.

[5] BRESSON E, CHEVASSUT O, POINTCHEVAL D. Dynamic grou PDiffie-Hellman key exchange under standard assumptions[A]. Advances in Cryptology EUORCRPT'02 Proceedings, LNCS2332[C]. Berlin: Springer-Verlag, 2002. 321-336.

[6] JOUX A. A one-round protocol for tripartite Diffie-Hellman[A]. Proceedings of ANTS-4 Conference, LNCS1838 [C]. Berlin: Springer Verlag, 2000. 385-394.

[7] BURMESTER M, DESMEDT YD. A secure and efficient conference key distribution system[A]. Advances in Cryptology EUORCRPT'94 Proceedings, LNCS950[C]. Berlin: Springer-Verlag, 1995. 275-286.

[8] 王志伟, 谷大武. 基于树结构和门限思想的组密钥协商协议[J]. 软件学报, 2004, 15(6): 924-927.

[9] BRESSON E, CATALANO D. Constan round authenticated group key agreement via distributed computation[A]. Public Key Cryptography-PKC2004, LNCS2947[C]. Berlin: Springer-Verlag, 2004. 115-129.

[10] MIYAJI A. Elliptic curves over F_p suitable for cryptosystems[A]. Advances in Cryptology-AUSCRYPT'92 Proceedings, LNCS718[C]. Berlin: Springer-Verlag, 1993.479-491.

[11] LIN C, LEE C. Elliptic-Curve undeniable signature scheme[A]. Proceedings of the Eleventh National Conference on information Security[C]. 2001. 331-338.