

基于无证书的可认证组密钥协商协议

刘小琼, 潘进, 刘琼
(西安通信学院, 陕西 西安 710106)

摘要:文中基于多线性表的性质,综合椭圆曲线上离散对数问题,提出一个新的基于无证书的多方密钥协商方案。新协议避免了传统的基于证书的方案中复杂的证书管理问题,解决了基于身份的组密钥协商方案中固有的密钥托管问题,实现了对通信各方的身份认证,有效防止了主动攻击。最后,通过计算验证了会话密钥的一致性,采用应用Pi演算对协议进行形式化分析验证了协议的安全性。和其它可认证组密钥协商协议相比,新方案用较小的计算开销换取了协议的更强安全性,协议的实用性大大增强。

关键词:组密钥协商;多线性表;无证书密码体制;形式化分析

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2012)05-0229-04

Certificateless-Based Authenticated Group Key Agreement Protocol

LIU Xiao-qiong, PAN Jin, LIU Qiong
(Xi'an Communications Institute, Xi'an 710106, China)

Abstract: An certificateless-based authenticated group key agreement protocol is proposed based on the property multilinear forms and elliptic curve discrete logarithm problem. The new scheme not only avoids the complex management of certificates in PKI scheme, but also avoids the key escrow issues inherited in the identity-based schemes effectively and prevents active attack by identity authentication. And then, the correctness of the session key is confirmed by computing, the formal analysis based on applied Pi calculus has shown fulfilled authentication and security. Compared with other authenticated group key agreement protocols, the newly proposed group key agreement protocol has better security with the cost of little computation and more stronger practicality.

Key words: group key agreement; multilinear forms; certificateless-based password system; formal analysis

0 引言

随着基于群组通信的网络应用飞速发展,群组通信系统的安全问题逐渐成为了社会关注的焦点。解决安全问题的手段有多种,其中安全高效的组密钥协商协议是一个重要途径。

目前,国内外的组密钥协商协议^[1-7]大都需要多轮通信,计算开销大,且没有实现身份认证,安全性不高。为了解决这些问题,研究者相继采用了基于证书的方案和基于身份的方案^[5,7-11],但是基于证书的方案中证书管理开销较大,基于身份的方案虽然避免了复杂的证书管理问题,但扩展性较差。2002年, Boneh和Silverberg首次提出了多线性表的概念,并采用其性质提出了一个多方密钥协商协议^[12]。由于该协议没

能实现对参与者的身份认证,仍存在中间人攻击。文献[13]采用PKI机制解决了身份认证问题但是证书管理复杂,2005年,文献[10]采用基于身份的方案进行了改进,但是安全性存在不足。近年来,国内学者针对采用多线性表进行多方密钥协商进行了研究和探讨^[11,14],并给出了对应的成员动态变化时组密钥更新的相关方法,但是仍然没有解决密钥托管问题,急需改进。

文中利用椭圆曲线上的离散对数问题和多线性表性质设计一个基于无证书的可认证组密钥协商协议,实现了组内成员的身份认证,解决了基于身份的方案中固有的密钥托管问题,最后通过形式化分析证明了协议的安全性。

1 预备知识

1.1 多线性表

Boneh和Silverberg首次提出了多线性表的概念。即映射 $e_n: G_1^n \rightarrow G_2$ 满足如下性质,则是一个 n 线性映射:

(1) G_1 和 G_2 是阶同为素数 q 的有限循环群;

收稿日期:2011-10-13;修回日期:2012-01-16

基金项目:国家自然科学基金(61179002);陕西省自然科学基金基础研究计划资助项目(2011JM8030)

作者简介:刘小琼(1985-),女,四川绵阳人,硕士研究生,研究方向为网络安全与对抗;潘进,教授,博士,博士生导师,研究方向为网络安全与对抗。

(2) 如果 $a_1, a_2, \dots, a_n \in Z_q^*$, 且 $x_1, x_2, \dots, x_n \in G_1$, 则有 $e_n(x_1^{a_1}, x_2^{a_2}, \dots, x_n^{a_n}) = e_n(x_1, x_2, \dots, x_n)^{a_1 a_2 \dots a_n}$;

如果 G_1, G_2 为椭圆曲线循环群, 则有 $e_n(a_1 \cdot x_1, a_2 \cdot x_2, \dots, a_n \cdot x_n) = e_n(x_1, x_2, \dots, x_n)^{a_1 a_2 \dots a_n}$;

(3) 映射 e_n 是非退化的, 若它满足如下性质: 即如果 $g \in G_1$ 是 G_1 的一个生成元, 则 $e_n(g, g, \dots, g)$ 是 G_2 的生成元。

1.2 椭圆曲线离散对数问题

设任意两点 $P, Q \in E(F)$, 若已知对某个整数 m 有 $Q = mP$ 成立, 由 P, Q 及 E 求出 m 的问题称为 E 上的椭圆曲线离散对数问题。

2 基于无证书的可认证组密钥协商方案

2.1 系统初始化及参数设置

设 G_1, G_2 分别是 q 阶的椭圆曲线有限循环群, 其中 q 是大素数, $e_n: G_1^n \rightarrow G_2$ 为 n 线性映射。定义两个 Hash 函数: $H_1: \{1, 0\}^* \rightarrow G_1, H_2: G_2 \rightarrow \{1, 0\}^n$ 。组成员分别用 U_1, U_2, \dots, U_n 来表示, 其中任意成员 U_i 的身份为 ID_i 。PKG 随机选择 $s \in Z_q^*$, 并将 s 作为系统私钥秘密保存, 计算系统公钥 $P_{\text{PKG}} = s \cdot P$, 其中 P 为 G_1 的生成元。同时, PKG 给域中每个成员分发部分私钥, 给成员 U_i 分发 $D_i = s \cdot Q_i$, 其中: $Q_i = H_1(ID_i) \in G_1$ 。各成员 U_i 分别选定一个秘密参数 $x_i \in Z_q^*$ 作为自己的长期私钥, 则组内任意成员 U_i 完整的私钥为 $S_i = \langle D_i, x_i \rangle$, PKG 公开系统参数 $(G_1, G_2, e_n, P, q, H_1, H_2, P_{\text{PKG}})$ 。

2.2 密钥协商与认证过程

假定有 $m(m \leq n)$ 个组成员参加会话密钥协商, 其密钥协商与认证过程如下:

(1) 成员 $U_i (i=1, \dots, m)$ 随机秘密选取 $r_i \in Z_q^*$, 私有密钥 $x_i \in Z_q^*$, 计算并广播 $kk_i = r_i \cdot Q_i, kk_i' = x_i \cdot P (kk_i, kk_i' \in G_1)$ 给组内其他成员 $U_j (j=1, \dots, m \text{ 且 } j \neq i)$; 成员 U_i 收到其他成员发来的 kk_j, kk_j' 消息后, 计算密钥 $K_i = e_n(kk_1, \dots, kk_{i-1}, kk_{i+1}, \dots, kk_m, r_i \cdot D_i, \overbrace{P, \dots, P}^{n-m \uparrow P})$, $K_i' = e_n(kk_1', \dots, kk_{i-1}', kk_{i+1}', \dots, kk_m', x_i \cdot \overbrace{P, P, \dots, P}^{n-m \uparrow P}) (K_i, K_i' \in G_2)$, 再通过进一步计算得到共同的会话密钥 $k = H_2(K_i || K_i')$ 。

(2) 成员 $U_i (i=1, \dots, m)$ 用计算得到的会话密钥 k 对称加密 ID_i 及其秘密选取的随机数即 $e_i = \{ID_i, r_i^{-1}\}_k$, 再广播给组内其他成员 $U_j (j=1, \dots, m \text{ 且 } j \neq i)$; 成员 U_j 收到其他成员发来的消息 e_i 后, 首先利用自己计算出来的会话密钥 k 解密消息, 然后利用解密得到的 ID_i 计算 $Q_i = H_1(ID_i)$, 并与 $r_i^{-1} \cdot kk_i$ 的计算结果进行对比验证, 若所有成员都通过此验证, 则组会

话密钥协商过程结束。

2.3 会话密钥的一致性验证

根据多线性映射函数的性质容易得到如下等式:

$$\begin{aligned} & K_{i(i=1, \dots, m)} \\ &= e_n(kk_1, \dots, kk_{i-1}, kk_{i+1}, \dots, kk_m, r_i \cdot D_i, \overbrace{P, \dots, P}^{n-m \uparrow P}) \\ &= e_n(r_1 \cdot Q_1, \dots, r_{i-1} \cdot Q_{i-1}, r_{i+1} \cdot Q_{i+1}, \dots, r_m \cdot Q_m, r_i \cdot (s \cdot Q_i), \overbrace{P, \dots, P}^{n-m \uparrow P}) \\ &= e_n(Q_1, \dots, Q_{i-1}, Q_{i+1}, \dots, Q_m, Q_i, \overbrace{P, \dots, P}^{n-m \uparrow P})^{r_1 r_2 \dots r_m r_i s} \\ &= e_n(Q_1, Q_2, \dots, Q_m, \overbrace{P, \dots, P}^{n-m \uparrow P})^{r_1 r_2 \dots r_m s} \\ & K_{i(i=1, \dots, m)} \\ &= e_n(kk_1', \dots, kk_{i-1}', kk_{i+1}', \dots, kk_m', x_i \cdot P, \overbrace{P, \dots, P}^{n-m \uparrow P}) \\ &= e_n(x_1 \cdot P, \dots, x_{i-1} \cdot P, x_{i+1} \cdot P, \dots, x_m \cdot P, x_i \cdot P, \overbrace{P, \dots, P}^{n-m \uparrow P}) \\ &= e_n(\overbrace{P, \dots, P}^{n-m \uparrow P}, \overbrace{P, P, \dots, P, P}^{n \uparrow P})^{x_1 x_2 \dots x_m x_i} \end{aligned}$$

又因为 $k = H_2(K_i || K_i') = H_2(K_2 || K_2') = \dots = H_2(K_m || K_m')$, 易知组成员都可经计算得到相同的会话密钥 k , 从而验证了组会话密钥的一致性。

当各成员收到加密消息 e_i 后, 用计算出来的会话密钥 k 解密消息得到各自的 ID_i 和 r_i^{-1} , 然后再分别验证身份的真实性, 因为:

$$r_i^{-1} \cdot kk_i = r_i^{-1} \cdot (r_i \cdot Q_i) = Q_i = H_1(ID_i)$$

所以, 各组成员身份的真实性得到认证。

3 协议的安全性证明

3.1 协议的应用 pi 演算模型

采用应用 pi 演算来形式化建模所用到的函数和代数相等关系有^[14]:

fun $E/2$. (对称密钥加密函数)

reduc $D(x, E(x, y)) = y$. (对称密钥解密函数)

数)

fun $H1/1$. (单向散列函数)

fun $H2/1$. (群上元素映射函数)

fun $f/2$. (椭圆曲线上点乘运算)

fun $f1/1$. (倒数运算)

fun e/n . (多线性映射函数)

equation $e(f(x_1, y_1), \dots, f(x_{i-1}, y_{i-1}), f(x_{i+1}, y_{i+1}),$

$$\begin{aligned} & \dots, f(x_m, y_m), f(x_i, f(x, y_i)), \overbrace{P, \dots, P}^{n-m \uparrow P}) \\ &= e(f(x_1, y_1), \dots, f(x_{j-1}, y_{j-1}), f(x_{j+1}, y_{j+1}), \dots, f(x_m, y_m), \\ & f(x_j, f(x, y_j)), \overbrace{P, \dots, P}^{n-m \uparrow P}). \text{ (其中 } i, j=1, \dots, m \text{ 且 } i \neq j) \\ & \text{equation } f(f_i(x_i), f(x_i, y_i)) = y_i. \end{aligned}$$

在以上定义的基础上,可以建立如下协议模型,其中 I_i 代表任意一个组成员进程:

```

 $I_i = \text{key}_i(D_i).vr_i.x_i.$ 
let  $Q_i = H_1(ID_i)$  in
let  $kk_i = f(r_i, Q_i)$  in
let  $kk_i' = f(x_i, P)$  in
 $\bar{c} < \text{cons1}(kk_i, kk_i') >.$ 
 $c(\text{cons2}(kk_1, kk_1', \dots, kk_{i-1}, kk_{i-1}', kk_{i+1}, kk_{i+1}', \dots, kk_m,$ 
 $kk_m')).$ 
let  $K_i = e_n(kk_1, \dots, kk_{i-1}, kk_{i+1}, \dots, kk_m, f(r_i, D_i),$ 
 $\underbrace{P, \dots, P}_{n-m \uparrow P})$  in
let  $K_i' = e_n(kk_1', \dots, kk_{i-1}', kk_{i+1}', \dots, kk_m', f(x_i, P),$ 
 $\underbrace{P, \dots, P}_{n-m \uparrow P})$  in
let  $k_i = H_2((K_i || K_i'))$  in
let  $r_i^{-1} = f_1(r_i)$  in
let  $e_i = E\{k_i\}(ID_i, r_i^{-1})$  in
 $\bar{c} < \text{cons3}(e_i) >.$ 
 $c(\text{cons4}(e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_m)).$ 
let  $(= ID_j, r_j^{-1}) = D\{k_i\}(e_j)$  in  $(j = 1, 2, \dots, m \& j \neq i)$ 
if  $f(r_j^{-1}, kk_j) = H_1(ID_j)$  then
connect( $ID_1, ID_2, \dots, ID_m, k_i$ ).

```

系统进程 S 由所有组成员进程 $I_i (i = 1, 2, \dots, m)$ 并发组成,同时包括 PKG 进程,具体描述如下:

```

 $S = vID_1. vID_2. \dots vID_n. vs.$ 
let  $Q_i = H_1(ID_i)$  in
 $(i = 1, 2, \dots, n)$ 
let  $D_i = f(s, Q_i)$  in
 $\text{key}_i < D_i >.$ 
 $(! I_1) | (! I_2) | \dots | (! I_m)$ 

```

通道 key_i 是用来建模 PKG 与各组成员之间传递信息的私有、安全信道,攻击者得不到通道内的内容。文中采用形式化的方法证明协议的安全性,部分形式化分析工作是在 ProVerif 自动化分析工具的辅助下完成的。

3.2 私密性分析

当环境无法区分组密钥协商过程中传递的身份信息 ID_i 和随机数 r_i^{-1} 时,则实现了对内容的保护,即满足私密性。由

于身份信息 ID_i 是在消息中加密传送的,因此,该协议还具有身份主动保护功能。对保密性和身份保护的验证只需在自动化工具 ProVerif 下查询(query)以下事实是否成立:

```

query attacker:  $ID_i. (* i = 1, \dots, m *)$ 
query attacker:  $r_i^{-1}. (* i = 1, \dots, m *)$ 

```

文中验证 4 个组成员参加密钥协商的过程,其中具有 4 个组成员时的验证输出结果如图 1 所示。

由图 1 可知,输出结果为 true,表明即使在主动攻击模式下,攻击者也无法获得组密钥协商各方传递消息中的内容 ID_i 和 $r_i^{-1} (i = 1, 2, 3, 4)$,该协议能够满足私密性,同时具备对组成员的身份保护。

3.3 认证性分析

如果组中任意成员成功协商了组会话密钥,则其他组成员所声称的身份一定是真实的。具体查询语句如下:

```

query ev: U1finished(k1) ==> ev: U1Verified(ID4, ID3, ID2)
& (ev: U2finished(k2) ==> ev: U2Verified(ID4, ID3, ID1))
& (ev: U3finished(k3) ==> ev: U3Verified(ID4, ID2, ID1))
& (ev: U4finished(k4) ==> ev: U4Verified(ID3, ID2, ID1))

```

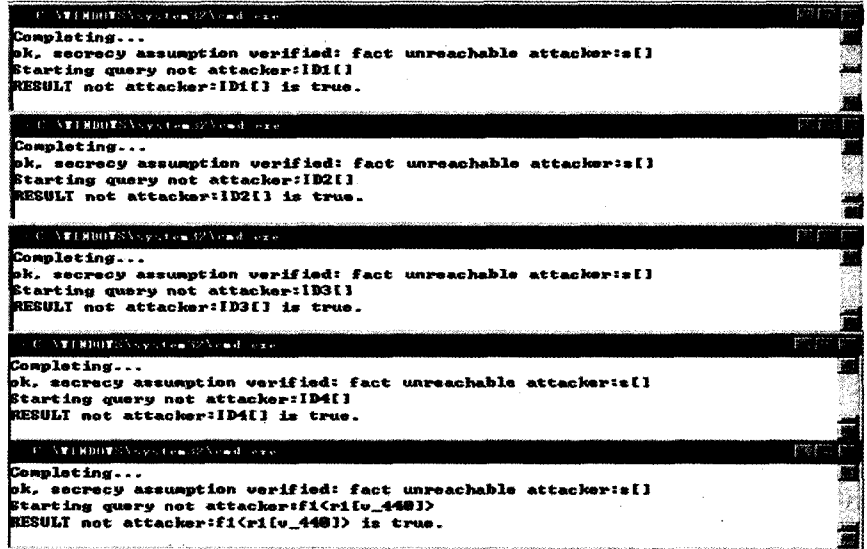


图 1 协议的保密性与身份保护验证结果

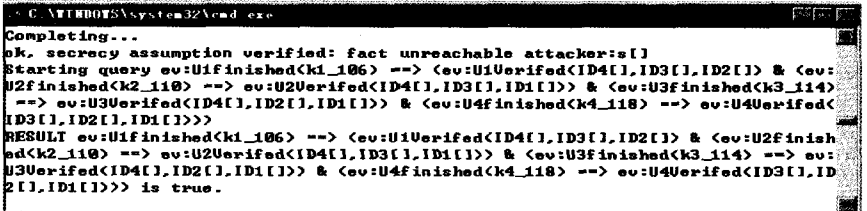


图 2 协议的认证性验证结果

验证结果如图 2 所示。

由图 2 可知,输出结果为 true,说明组成员各方能相互确认身份,该协议满足认证性。

4 结束语

文中在文献[11,14]基础上通过应用椭圆曲线上离散对数问题和多线性表的性质,提出了一种基于无证书的认证组密钥协商方案,并采用形式化分析方法证明了协议的安全性。综合分析表明,该方案不但实现了组内成员身份的认证,而且还能主动保护组成员身份信息,更重要的是解决了密钥托管问题。密钥协商过程中每个成员只需多增加一次椭圆曲线上点乘运算即可换取更强的安全性,每个成员只需广播传输 2 条较短的消息,通信开销较小,协议的实用性和可扩展性更强。

参考文献:

- [1] Steiner M, Tsudik G, Waidner M. Key agreement in dynamic peer groups[J]. IEEE Transactions on Parallel and Distributed Systems, 2000, 11(8): 769-780.
- [2] Burmester M, Desmedt Y. A secure and efficient conference key distribution system [C]//Advance in Cryptology EURO2CRYPT'94. Berlin: Springer-Verlag, 1994: 275-286.
- [3] Becker K, Wille U. Communication complexity of group key distribution[C]//ACM Conference on Computer and Communication Security. New York: ACM Press, 1998: 1-6.
- [4] Ateniese G, Steiner M, Tsudik G. New multiparty authentication services and key agreement protocols[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 628-640.
- [5] Boneh D, Franklin M. Identity-based encryption from the weil pairing[C]//Proceedings of Crypto'2001. Berlin: Springer-Verlag, 2001: 213-229.
- [6] Joux A. One round protocol for tripartite Diffie-Hellman [C]//Proceedings of Algorithmic Number Theory Symposium. Berlin: Springer-Verlag, 2000: 385-394.
- [7] Smart N P. An identity based authenticated key agreement protocol based on the weil pairing cryptography [R/OL]. 2001. <http://eprint.iacr.org/2001/111>.
- [8] 赵 婷, 王晓峰, 王尚平, 等. 基于身份的认证多方密钥协商方案[J]. 计算机工程, 2008, 34(6): 164-166.
- [9] 宋 震, 周贤伟, 窦文华. 一种基于身份标识的 MANET 组密钥协商协议[J]. 电子学报, 2008, 36(10): 1862-1863.
- [10] Lee H M, Ha K J, Ku K M. ID-based Multi-party Authenticated Key Agreement Protocols from Multilinear Forms [C]//8th International Conference on Information Security, ISC 2005. Berlin: Springer-Verlag, 2005: 104-117.
- [11] 钟 欢, 许春香. 基于身份的多方认证组密钥协商协议[J]. 电子学报, 2008, 36(10): 1869-1871.
- [12] Boneh D, Silverberg A. Application of Multilinear forms to Cryptography[EB/OL]. 2002. <http://eprint.iacr.org/2002/080>.
- [13] Lee H K, Lee H S, Lee Y R. Multi-party Authenticated Key Agreement Protocols from Multilinear Forms [R/OL]. 2002. <http://eprint.iacr.org/2002/166>.
- [14] 陈安林, 潘 进, 徐邢启, 等. MANET 中可认证组密钥协商协议及验证[J]. 电脑知识与技术, 2010, 32(6): 8966-8969.

(上接第 228 页)

可成为完整的报警系统;上述种种优点及其所具有的功能提升空间,使它具有市场推广的价值与潜力。

参考文献:

- [1] 王海向, 党瑞荣. 基于 AT89S51 的新型家庭语音报警系统设计[J]. 世界电子元器件, 2008(11): 64-68.
- [2] 周 正, 陆 阳. 新型联动报警系统[J]. 计算机技术与发展, 2006, 16(3): 200-205.
- [3] 熊慧萍, 陈发堂, 陈东生, 等. 家居安防系统监控主机的设计与实现[J]. 现代电子技术, 2007(24): 40-42.
- [4] 马兆远, 王 勇, 马志峰. 基于 AT89S52 的智能报警系统的设计与实现[J]. 计算机技术与发展, 2009, 19(12): 181-184.
- [5] 孙 媛, 王水清. 基于以太网嵌入式家庭监控网络系统的设计[J]. 江南大学学报, 2003(3): 40-42.
- [6] 王 汀. 微处理器原理与接口技术[M]. 杭州: 浙江大学出版社, 2008.
- [7] 王 春, 秦付军. 智能门监控系统的开发与设计[J]. 机电工程技术, 2009, 38(6): 52-53.
- [8] Rialle V, Cand F D, Noury N, et al. Health "Smart" Home: Information Technology for Patients at Home [J]. Telemedicine Journal and e-Health, 2002, 8(4): 395-409.
- [9] 求是科技. 单片机典型模块设计实例导航[M]. 第 2 版. 北京: 人民邮电出版社, 2008.
- [10] 张元敏. 基于 AT89C52 的远程智能语音防盗报警系统设计[J]. 现代电子技术, 2008(13): 38-41.
- [11] Peeters P H F. Design criteria for an automatic safety-alarm system for elderly[J]. Technology and Health Care, 2000(8): 81-91.
- [12] Tamura T, Togawa T, Ogawa M, et al. Fully automated health monitoring system in the home [J]. Medical Engineering & Physics, 1998, 20(8): 573-579.