

基于 CDS 结构的动态安全组播密钥协商方案

永平

(南京师范大学 数学与计算机科学学院, 江苏 南京 210097)

[摘要] 提出了一个应用椭圆曲线密码体制在基于 CDS 结构的动态安全组播中进行密钥协商的方案. 首先采用 CDS 分组算法对组播组成员进行区域划分, 然后应用椭圆曲线密码体制进行各个子组及整个大的组播组的密钥协商. 采用 CDS 结构增加了灵活性, 避免了单点故障的产生, 提高了组播系统的健壮性. 应用椭圆曲线密码体制, 有效地减少了密钥程度和密码算法的计算量. 具体分析了各个子组和整个大的组播组的密钥协商过程, 以及在组成员动态变化时密钥的更新过程. 结果表明, 所提方案在降低计算和通信代价方面取得了较好的效果, 而且满足组播密钥协商的各种安全要求.

[关键词] 安全组播, 密钥协商, CDS, 椭圆曲线密码体制

[中图分类号] TP393 [文献标识码] B [文章编号] 1672-1292(2007)01-0068-04

Key Agreement Scheme for Dynamic Secure Multicast Based on Connected Dominating Set

Ding Yongping

(School of Mathematics and Computer Science, Nanjing Normal University, Nanjing 210097, China)

Abstract How to design efficient key agreement schemes is a difficult problem in dynamic secure multicast. In this paper, we propose a novel key agreement scheme using Elliptic Curve Cryptosystem for dynamic secure multicast based on CDS(Connected Dominating Set). First, we use CDS grouping arithmetic to partition the multicast group members. Then we apply Elliptic Curve Cryptosystem to the procedure of key agreement of every subgroup and the entire multicast group. Adopting the CDS structure not only increases the system agility and avoids producing hitches but also improves the system haleness. Applying Elliptic Curve Cryptosystem decreases the computation of key agreement and cryptography arithmetic. We also analyze the procedure of key agreement of every subgroup and the entire multicast group, and the procedure of updating of group keys with the dynamic change of group members in detail. The analysis shows that our scheme is not only efficient in computation and communication, but also satisfies the security requirements of multicast key agreement.

Key words secure multicast; key agreement; connected dominating set; elliptic curve cryptosystem

0 引言

组播^[1, 2]提供了一种发送者可以同时发送信息到多个接收者的高效通信机制, 可广泛地应用于多媒体远程教育、分布式系统、网络视频会议等. 与传统的单播通信方式相比, 组播需要在安全性方面作更多的考虑, 由此提出了安全组播的概念. 安全组播的一个主要难点是如何确保只有合法的组注册用户才能接收到组播通信数据. 其中, 为动态安全组播设计高效的密钥协商^[3-4]方案又是最具挑战性的问题.

已有的组播密钥协商方案主要基于将两方的 Diffie-Hellman 问题扩展到多方情形, 如 CLQUES^[5]、Hypercube 和 Octopus^[6]以及 TGDH^[7]等. 这些协议都需要固定组成员担任子组中心, 或要求组成员按照一定的次序排列. 组中心的可靠性、安全性和诚实性都可能成为组播系统的瓶颈. 而组成员按次序排列的方式显然不适合组播应用的动态特性. CDS(Connected Dominating Set)^[8-9]提出的高效且较为实用的组播体系架构方案. 其主要思想是依据分组算法将整个组播组划分为多个子组, 子组间不重叠, 且完备地覆盖组播

收稿日期: 2006-09-01

作者简介: 丁永平(1976-), 女, 助理实验员, 主要从事网络安全方面的教学与研究. E-mail: dingyongping@njnu.edu.cn

组中所有成员. 各子组中有一个组长和多个组成员, 如图 1 所示.

椭圆曲线密码体制^[3,4] (Elliptic Curve Cryptosystem, ECC)自 1987 年提出以来便引起了广泛的研究兴趣. 迄今的研究表明, 非奇异的 ECC 是安全强度最大的安全机制^[10], 可以较小的计算和通信代价达到较高的安全性要求, 特别适合对时延要求比较高的实时安全组播应用.

为此本文提出了一个两级分层分组组播密钥协商方案. 首先将有限域 ECC 应用到低层各子组的组密钥协商方案中, 然后在高层即所有的 dominators 间进一步协商最终的整个组播组的会话密钥. 具体的密钥协商方案由 4 部分组成, 包括组播系统初始化 P_{setup} , 组成员注册及组密钥协商过程 P_{init} , 新成员加入过程 P_{join} 以及组成员退出过程 P_{leave} .

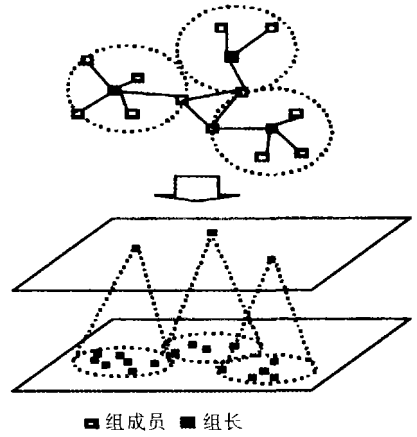


图 1 基于 CDS 的安全组播体系结构

Fig.1 Secure multicast system based on CDS

1 预备知识

1.1 $GF(p)$ 上的椭圆曲线群 $E_p(a, b)$

设 $GF(p)$ 是一个特征 $p \neq 2, 3$ 的有限域, $\exists a, b \in GF(p)$ 满足 $4a^3 + 27b^2 \neq 0, p \in (2^k, 2^{k+1})$, 且 p 为一个大素数. 取方程 $E: y^2 = x^3 + ax + b$, 则 $E_p(a, b) = \{(x, y) \mid y^2 = x^3 + ax + b \pmod{p}\} \cup \mathbf{0}$

按照如下定义组成一个 Abe 群:

- 1) 零元: 设 $\mathbf{0}$ 是 $E_p(a, b)$ 零元;
- 2) 逆元: $\forall (x, y) \in E_p(a, b), \exists (x, -y) \in E_p(a, b)$, 点 $R(x, y)$ 的逆元为 $-R(x, -y)$;
- 3) 加法: $\forall M, Q \in E_p(a, b)$, 且 $M, Q \neq \mathbf{0} \exists R \in E_p(a, b)$, 使得 $R = M + Q$, 且 $M - M = \mathbf{0}$;
- 4) 数乘: $k \in \mathbb{Z}$, 则 $k^* M = M + M + \dots + M$ (k 个 M 相加).

由上述定义, $\mathbf{0}$ 的几何意义是一条直线与椭圆曲线 EC 相交时 3 个交点的和, 从而可以推出加法的计算公式. 对于给定的 ECC 系统, 需确定一个产生器 G , 使得 $nG = \mathbf{0}$ 的最小 n 足够大. 由于 $E_p(a, b)$ 是 Abe 群, 对群内元素的加法封闭, 即 $\forall k \in \mathbb{Z}, \exists M = kG \in E_p(a, b)$, 同时 $kG = (k \bmod n)G$, 说明 $E_p(a, b)$ 是有限的 Abe 群, n 为循环周期. 记 $\#E_p(a, b)$ 为群的阶, 即群内点的总数, 确定 $\#E_p(a, b)$ 很困难, 但由 Hasse 定理可以证明 $p + 1 - \sqrt{p} \leq \#E_p(a, b) \leq p + 1 + \sqrt{p}$.

1.2 计算复杂性假设

定理 1 在 $E_p(a, b)$ 上任选一点 $M \neq \mathbf{0}$ 必有 $Q = k^* M \in E_p(a, b), k \in (0, p)$.

定义 1 椭圆曲线离散对数问题 (ECDLP): 给定点 M 和 Q , 计算 k 使得 $Q = k^* M \in E_p(a, b), k \in (0, p)$.

复杂性假设: ECDLP 是困难问题, 即不存在一个多项式时间算法能以不可忽略的概率解决 ECDLP.

已有的研究表明, 除超奇异椭圆曲线和异常曲线外, ECC 的求解算法都是指数时间算法^[3,5], 与其它一些加密算法如 RSA 相比, 在同等安全强度下只需小得多的密钥长度, 例如 139 位 ECC 相当于 1024 位 RSA. 安全强度越大, ECC 的优点越突出. 在选择椭圆曲线时, 对于 $\forall B \in (1, \log_2 p)$, 只要生成元 G 的阶满足 $(p^B - 1) \bmod n \neq 0$ 就可以避免针对超奇异椭圆曲线的 MOV 攻击. 而通过检查 $\#E_p(a, b) \neq p$ 可判断是否为异常曲线, 若不是则可避免 Smart-Satoh-Araki 攻击. 目前最有效的攻击算法是文献 [11] 提出的并行算法 Pollard rho, 但其为指数时间算法.

2 基于 CDS 结构的动态安全组播密钥协商方案

2.1 变量标记说明及系统初始化过程 P_{setup}

本方案涉及到如下一些变量标记:

$E_p(a, b)$ 的系统公共参数 $\text{params} = \{p, a, b, n, G\}$. 其中, n 为阶数, G 为基点. N : 整个组播组的成员数; m : 划分的子组个数; n_i : 第 i 个子组的成员数; U_i : 整个组播组的第 i 个成员, $i \in [1, N]$; $U = \{U_1, U_2, \dots$,

U_N 为整个组播组成员的集合; U_{ij} : 第 i 个子组中的第 j 个成员, $j \in [1, n_i]$, 假定 U_{i1} 为第 i 个子组的 dominator ; $U_i = \{U_{i1}, U_{i2}, \dots, U_{in_i}\}$ 为第 i 个子组成员的集合; α_{ij} : U_{ij} 选择的秘密随机整数, 作为私钥, $\alpha_{ij} < n_i$; K_i : 第 i 个子组的组内共享秘密; s_i : 第 i 个子组的子组私钥, $s_i < n_i$; Q_i : 第 i 个子组的子组公钥, $Q_i = s_i G$; K : 最终协商出的整个组播组的会话密钥.

2.2 组播成员注册及组密钥协商过程 P_{init}

按照文献 [8-9] 中的分组算法对注册成功的合法组播组成员进行子组划分, 构建 CDS 为保证一定的计算和通信效率, 子组规模应控制在 $n_i < N/m$ 以内.

各子组成员首先选择一个秘密的随机整数作为私钥. 组播组的初始会话密钥协商按步骤分为两大部分, 即各个子组成员协商子组秘密和高层 dominators 组会话密钥协商.

(1) 各个子组成员协商子组秘密, 以第 i 个子组 $U_i = \{U_{i1}, U_{i2}, \dots, U_{in_i}\}$ 为例, 具体过程如下:

Step 1 U_{i2} 将 $(\alpha_{i2})G$ 通过秘密信道传送给 U_{i3} ;

Step 2 U_{ij} 将 $(\alpha_{i2}\alpha_{i3}\dots\alpha_{ij})G$ 通过秘密信道传送给 $U_{i(j+1 \pmod{n_i})}$, $j \in [3, n_i-1]$, 即从第 3 个子组成员开始, 依次在接收到的信息中嵌入自己的私钥信息, 并传送给下一个成员;

Step 3 最后一个成员 U_{in_i} 将 $(\alpha_{i2}\alpha_{i3}\dots\alpha_{in_i})G$ 广播给除 dominator 之外的各个子组成员, $j \in [2, n_i-1]$;

Step 4 各成员 U_{ij} 将 $((\alpha_{i2}\alpha_{i3}\dots\alpha_{in_i})/\alpha_{ij})G$ 通过秘密信道传送给 $\text{dominator } U_{i1}$, $j \in [2, n_i]$;

Step 5 $\text{dominator } U_{i1}$ 将接收到的所有信息中嵌入自己的私钥, 然后将 $\{((\alpha_{i1}\alpha_{i2}\dots\alpha_{in_i})/\alpha_{ij})G \mid j \in [2, n_i]\}$ 在子组中广播, 各成员计算协商出的子组共享秘密 $K_i = (\alpha_{i2}\alpha_{i3}\dots\alpha_{in_i})G = (x_i, y_i)$, 并进一步计算出子组私钥 $s_i = x_i \pmod{n}$, $Q_i = s_i G$.

(2) 高层 dominators 组会话密钥协商, 具体过程如下:

Step 1 各个 $\text{dominator } U_{i1}$ 将各自子组的公钥 $Q_i = s_i G$ 在整个组播组中广播, $i \in [1, m]$;

Step 2 各个 $\text{dominator } U_{i1}$ 各自计算 $X_i = s_i(Q_{i+1} - Q_{i-1})$, 并在整个组播组中广播, $i \in [1, m]$;

Step 3 整个组播组中各成员 U_i 计算出组会话密钥 $K = m s_i \pmod{n} Q_{i-1 \pmod{m}} + (m-2)X_{i \pmod{m}} + (m-1)X_{(i+1) \pmod{m}} + \dots + X_{(i-2) \pmod{m}} = (s_1 s_2 + s_2 s_3 + \dots + s_{m-1} s_m + s_m s_1)G$, $i \in [1, N]$.

关于组会话密钥协商过程的几点说明:

1) 此处处在 (1) Step 1 中由 U_{i2} 发起子组秘密协商过程, 实际运行时是所有当前子组用户排列成一个环, 任何一个合法子组都可以发起协商过程.

2) 为防止多个 dominators 发起合谋攻击, 在 (2) Step 1 中, 当某个子组的 dominator 广播该子组公钥时, 子组内任一成员广播自己所计算出的子组公钥, 所有成员通过比较接收到的两个子组公钥从而判断 dominator 是否存在欺骗行为; 同样, 对于 X_i , 所有成员都可自由地选择检验某一个 dominator 广播的 X_i 是否正确. 这两种验证机制可以使任一成员及时发现任一不诚实的 dominator 从而可以防止合谋攻击的发生.

3) 各子组 dominator 的角色可以由子组中任何一个合法成员担任, 当前担任 dominator 的成员退出组播组后, 不会影响后续组播应用的进行, 充分体现了组播的动态特性, 并提高了组播应用的健壮性.

2.3 新成员加入过程 P_{join}

设有新成员 U_{N+1} 要加入组播组. U_{N+1} 首先查找与之距离最近的子组, 若其已有子组成员数 $n_i < N/m$, 则加入该子组; 否则, U_{N+1} 将独立形成新的第 $m+1$ 个子组, 并作为该新子组的 dominator . 因此 U_{N+1} 加入后的组会话密钥的更新分以下两种情况:

(1) U_{N+1} 作为第 n_i+1 个成员 U_{in_i+1} 加入第 i 个子组, 具体过程为:

Step 1 $\text{dominator } U_{i1}$ 重新选择其私钥 α'_{i1} 在子组内更新子组秘密, 并将信息 $\{((\alpha'_{i1}\alpha_{i2}\dots\alpha_{in_i})/\alpha_{ij})G \mid j \in [2, n_i], (\alpha'_{i1}\alpha_{i2}\dots\alpha_{in_i})G\}$ 通过秘密信道传送给 U_{in_i+1} ;

Step 2 U_{in_i+1} 将 $\{((\alpha'_{i1}\alpha_{i2}\dots\alpha_{in_i})/\alpha_{ij})G \mid j \in [1, n_i]\}$ 在子组中广播;

Step 3 $\text{dominator } U_{i1}$ 在整个组播组中广播新的第 i 个子组的公钥 $Q'_i = s'_i G$;

Step 4 第 k 个子组的 $\text{dominator } U_{k1}$ 在整个组播组中广播 $X_k = s_k(Q_{k+1} - Q_{k-1})$, $k \in [i-1, i+1]$;

Step 5 和 P_{init} (2) 的 Step 3 类似, 组播组中各成员 U_i 重新计算组会话密钥 K' , $i \in [1, N+1]$.

(2) U_{N+1} 将独立形成新的第 $m+1$ 个子组加入组播组, 则组会话密钥的更新过程为上一种情形的 Step 3 ~ Step 5

2.4 组成员退出过程 P_{leave}

设有成员 $U_i (i \in [1, N])$ 要退出组播组, 则需要考虑该成员是为某子组的组成员 $dominatee$ 还是组长 $dominator$ 因此 U_i 退出后的组会话密钥的更新也要分以下两种情况:

(1) U_i 为第 i 个子组的组成员 $dominatee$ $U_{i,l}$ 退出组播组, 具体过程为:

Step 1 $dominator U_{i,1}$ 重新选择其私钥 $\alpha_{i,b}^*$ 在子组内更新子组秘密, 并将信息 $\{(\alpha_{i,1}\alpha_{i,2}\cdots\alpha_{i,n_i})/\alpha_{i,j}\}G \mid j \in [2, n_i], j \neq l\}$ 在子组中广播;

Step 2 $dominator U_{i,1}$ 在整个组播组中广播新的第 i 个子组的公钥 $Q_i^* = s_i^* G$;

Step 3 第 k 个子组的 $dominator U_{k,1}$ 在整个组播组中广播 $X_k = s_k(Q_{k+1} - Q_{k-1})$, $k \in [i-1, i+1]$;

Step 4 和 $P_{init}(2)$ 的 Step 3 类似, 组播组中各成员 U_i 重新计算组会话密钥 K^* , $i \in [1, N+1]$.

(2) U_i 作为第 i 个子组的组长 $dominator U_{i,1}$ 退出组播组, 则第 i 个子组首先重新确定新的 $dominator$ 然后更新子组秘密, 类似于上一种情形的 Step 1; 接着高层 $dominators$ 广播更新后的信息, 最后所有组成员重新计算组会话密钥, 与上一种情形的 Step 2 ~ Step 4 类似.

3 安全性及计算与通信代价分析

3.1 安全性分析

由 2.3 的分析可知, 本密钥协商方案是安全的, 能够抵抗子组内用户的合谋攻击, 即任意 $(t-1)$ 个用户不能恢复出子组会话密钥 K , 也无法获得某个组成员的私钥信息 α_i .

从密钥协商安全性要求的角度来看, 本方案同样满足其要求:

(1) 机密性. 方案基于椭圆曲线密码体制, 攻击者无法获得私钥, 也就无法计算出组会话密钥. P_{init} 中提供的验证机制可以防止不诚实的 $dominators$ 发起合谋攻击.

(2) 前向安全. 对于新加入组播组的成员, 由于有一个子组成员更新了私钥, 故其即使得到上一轮所有的公钥, 也无法得知任一成员的私钥, 自然也无法计算出其加入前的组会话密钥, 从而保证了前向安全.

(3) 后向安全. 对于已经退出组播组的成员, 由于有一个子组成员更新了私钥, 故其同样也无法计算出退出后的组会话密钥, 从而保证了后向安全.

(4) 共同协商. 密钥协商过程结合了每个成员的私钥, 缺少了任何一个成员的私钥都无法计算出最终的组会话密钥, 体现了密钥共同协商的原则.

3.2 计算与通信代价分析

密钥协商的两个主要性能指标, 即计算量和通信量是一对矛盾联合体, 很难兼顾, 常常需要在两者间寻求一个平衡点或折衷 (trade-off). 在低层各子组成员密钥协商时, 考虑到一个子组的成员通常地理位置上也比较靠近, 相互间通信消耗较小且可靠, 适合用通信量较大的方案以换取计算量的减少, 故采用了类似 GDH. 3 的方案. 而高层的 $dominators$ 相互间较分散, 通信开销大且不完全可靠, 因此需要牺牲计算量以降低通信量, 减少通信开销.

本密钥协商方案的计算量为 $6N - 5m$ 次指数运算, 通信量分别为 $2(N+m) - 1$

4 结语

本文提出了基于 CDS 结构的动态安全密钥协商方案. 首先采用 CDS 分组算法对组播组成员进行区域划分, 然后应用椭圆曲线密码体制进行各个子组及整个大的组播组的密钥协商. 虚拟中枢结构的设计具有较高的灵活性, 避免了单点故障的产生, 提高了组播系统的健壮性. ECC 是一种高效的密码体制, 在同等安全强度下需要的密钥长度比其它密码体制要小得多, 计算代价较小, 特别适合对时延要求比较高的实时动态安全组播应用, 如视频点播. 本方案满足密钥协商的前向安全和后向安全要求, 且能抵抗不诚实组成员的合谋攻击. 下一步的工作将考虑如何平衡子组各成员在密钥协商的计算负担, 以期构造一个更高效、更安全的密钥协商方案.

(下转第 77 页)

- [4] 包昌火, 黄英, 赵刚. 发展中的竞争情报系统 [J]. 企业信息管理技术, 2004(1): 76-80
Bao Changhuo Research on developing competitive intelligence system [J]. New Technology of Library and Information Service, 2004(1): 76-80 (in Chinese)
- [5] Leonard M. Fuhl. Intelligence Software Report 2003 — A Review of Twelve Software Offerings in the Competitive Intelligence Arena [R]. Fuhl & Company, 2003
- [6] France Bouthillier. CI professionals and their interactions with CI technology a research agenda [J]. Journal of Competitive Intelligence Management, 2005, 4(1): 41-53
- [7] Werther G. Building an “analysis age” for competitive intelligence in the twenty-first century [J]. Competitive Intelligence Review, 2001, 12(1): 41-47.
- [8] 刘玉照, 刘建准, 范志雯. 基于 C/S 与 B/S 集成模式的企业竞争情报系统构建研究 [J]. 情报科学, 2005, 23(3): 411-413
Liu Yuzhao, Liu Jianzhun, Fan Zhiwen. Research on constructing enterprise competitive intelligence system based on integrated pattern of C/S and B/S [J]. Information Science, 2005, 23(3): 411-413 (in Chinese)
- [9] 吴晓伟, 徐福缘. 基于“综合集成研讨厅”的企业竞争情报系统研究 [J]. 情报学报, 2004, 23(6): 746-754
Wu Xiaowei, Xu Fuyuan. Research of competitive intelligence system based on hall for workshop of meta-synthetic engineering [J]. Journal of the Society for Scientific and Technical Information, 2004, 23(6): 746-754 (in Chinese)
- [10] 郭丽芳, 张义兰. 充分发挥高校科技查新咨询的情报评价作用 [J]. 科技情报开发与经济, 2006, 16(2): 250-251.
Guo L Fang, Zhang Yilan. Giving full play to the information evaluation function of university in the sci-tech novelty searching and consulting [J]. Sci-tech Information Development and Economy, 2006, 16(2): 250-251 (in Chinese)

[责任编辑: 严海琳]

(上接第 71 页)

[参考文献] (References)

- [1] Berkovits S. How to broadcast a secret [C] // Advances in Cryptology — EUROCRYPT 91. Berlin: Springer-Verlag, 1991. LNCS 547: 535-541.
- [2] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys [C] // Advances in Cryptology-CRYPTO 05. Berlin: Springer-Verlag, 2005. LNCS 3621: 258-275.
- [3] Hankerson D, Menezes A, Vanstone S. Guide to Elliptic Curve Cryptography [M]. New York: Springer-Verlag, 2004: 75-198.
- [4] Menezes A, Oorschot P, Vanstone S. Handbook of Applied Cryptography [M]. New York: CRC Press, 1997: 425-488.
- [5] Steiner M, Tsudik G, Waidner M. CLQUES: A new approach to group key agreement [C] // Proceedings of 18th International Conference on Distributed Computing Systems. Amsterdam, New York: IEEE Computer Society Press, 1998: 380-387.
- [6] Becker K. Communication complexity of group key distribution [C] // Proceedings of 5th ACM Conference on Computer and Communications Security. New York: ACM Press, 1998: 1-6.
- [7] Kim Y, Perrig A, Tsudik G. Tree-based group key agreement [J]. ACM Transactions on Information and System Security (TISSEC), 2004, 7(1): 60-96.
- [8] Wan P, Alzoubi K, Frieder O. Distributed construction of connected dominating set in wireless ad hoc networks [J]. Mobile Networks and Applications, 2004, 9(2): 141-149.
- [9] Alzoubi K, Wan P, Frieder O. Message-optimal connected-dominating-set construction for routing in mobile ad hoc networks [C] // Proceedings of 3rd ACM International Symposium Mobile Ad Hoc Networking and Computing. New York: ACM Press, 2002: 157-164.
- [10] Zhang F, Wang Y. Study and advance of hyper-elliptic curves cryptosystems [J]. Acta Electronica Sinica, 2002, 30(1): 126-131.
- [11] Oorschot P, Wiener M. Parallel collision search with cryptanalytic applications [J]. Journal of Cryptology, 1999, 12(1): 1-28.

[责任编辑: 严海琳]