第 19 卷第 4 期　　广西科学院学报　　Vol. 19, No. 4
2003 年 11 月　　Journal of Guangxi Academy of Sciences　　November 2003

一种基于椭圆曲线密码体制的组密钥约定方案

A Group Key Agreement Scheme Based on Elliptic Curve Cryptosystems

石润华　　钟　诚*

Shi Runhua　Zhong Cheng

（广西大学计算机与信息工程学院　南宁　530004）

(Coll. of Comp. & Info. Engi., Guangxi Univ., Nanning, 530004)

摘要　在分析基于 Diffie-Hellman 的组密钥约定协议 BD 和 TGDH 的基础上，提出一种新的基于椭圆曲线密码体制的组密钥约定方案 TGDH-BD。由于该方案建立在椭圆曲线离散对数计算难题之上，最大可能地减少了通信开销与计算工作量，因而更安全有效，适合分布式网络环境的组应用.

关键词　动态组　密钥约定　密钥管理　椭圆曲线密码体制　离散对数

中图法分类号　TP393.08

Abstract　The group key agreement and its new characteristic are introduced, and current group key agreement protocols BD and TGDH are also analyzed. A new group key agreement scheme based on Elliptic Curve Cryptosystems is presented. The scheme is secure and effective, and fit for the group application on distributed network.

Key words　dynamic group, key agreement, key management, elliptic curve cryptosystems, discrete logarithm.

随着网络计算技术的迅速发展，出现了诸如多个用户参加的视频/声频会议、网络娱乐游戏等基于组的应用. 安全可靠的组通信也因此成为研究的热点. 寻找安全、有效的密钥管理机制是其最大的挑战. 从传统的中心服务到分布式服务的改变是当前基于组应用的发展趋势. 这种基于组的分布式、协作应用同样需要安全服务. 而实现这些安全服务，建立一个共享的组密钥是其关键. 于是，人们提出了组密钥约定协议[1~6]. 组密钥约定协议与传统的多播组密钥管理机制不同，它没有中心密钥服务器，组共享的密钥由所有组用户通过对等协商约定，具有分布式、协作、动态等新特性.

椭圆曲线密码体制最早于1985年由 Miller[7] 和 Koblitz[8] 分别独立地提出. 它的思想是利用有限域上的椭圆曲线有限群，代替基于离散对数问题密码体制中的有限循环群所得到的一

2003-03-06 收稿，2003-04-18修回。

* 中国科学技术大学在读博士。

类密码体制,它是目前已知的所有公钥密码体制中能够提供最高比特强度的一种公钥体制. 本文将提出一种基于椭圆曲线密码体制的组密钥约定方案.

1 组密钥约定协议

Diffie 与 Hellman 于1976年第一次提出了两方参加的密钥交换协议——Diffie－Hellman 密钥交换协议[9]. 后来发展到多方参加的密钥交换协议,也即组密钥约定协议. 与仅有两方参加的密钥交换协议不同,组密钥约定协议需要遵循组密钥秘密性、后向安全性、前向安全性、密钥独立性等安全性要求.

1.1 BD 协议[1,2]

p 是一个大素数,g 是 Z_p^* 上的生成元,设定组大小为 n,即有 n 个成员:$p_1, p_2, \cdots, p_n$.

1) 每个参加者 p_i 随机选取整数 $r_i \in Z_p^*$,计算并广播 $z_i = g^{r_i}$.

2) 每个参加者 p_i 计算并广播 $X_i = (z_{i+1}/z_{i-1})^{r_i}$.

3) 每个参加者 p_i 计算 $K_i = (z_{i-1})^{nr_i} \cdot X_i^{n-1} \cdot X_{i+1}^{n-2} \cdots X_{i-2}$

$= (z_{i-1})^{nr_i} \cdot (z_{i+1}/z_{i-1})^{r_i(n-1)} \cdot (z_{i+2}/z_i)^{r_{i+1}(n-2)} \cdots (z_{i-1}/z_{i-3})^{r_{i-2}}$

$= (g^{r_{i-1}})^{nr_i} \cdot (g^{(r_{i+1}-r_{i-1})n})^{n-1} \cdot (g^{(r_{i+2}-r_i)r_{r+1}})^{n-2} \cdots (g^{(r_{i-1}-r_{i-3})r_{i-2}})$

$= g^{r_1r_2+r_2r_3+\cdots+r_nr_1}$,

这样得到组密钥 $K = K_i = g^{r_1r_2+r_2r_3+\cdots r_nr_1}, i = 1 \sim n$.

1.2 TGDH 协议[3,4]

在 TGDH (Tree-Based Group Diffie-Hellman Protocol) 协议中,需要建立密钥树[10],密钥以分层二叉树结构排列,如图1. 每个成员拥有一个密钥集合. 结点标识 ID 为序号 v. 对于一个给定结点 v,规定拥有一个私钥 K_x 和一公钥 $BK_x = g^{K_x} \bmod p$,其中 g 为生成元,p 为群的阶. 在密钥树中的每个叶子结点连着组用户,他的私钥由组用户定义. 每个用户拥有从他所连接的叶子结点到根结点的密钥路径上的所有私钥. 因此,根结点的私钥被所有的组用户共享,故可作为组通信密钥. 图 1 列出了一个可能的密钥树,有 6 个用户 M_1 到 M_6. 例如,用户 M_1 知道结点 7,3,1,0 的私钥. 结点 0 的私钥是整个组秘密约定的组密钥,负责对整个组的秘密通信. 这里根结点的 ID 设定为 0. 每个非叶子结点 v 包含 2 个子结点,一个子结点的 ID 为 $2v+1$,另一个 ID 为 $2v+2$,基于 Diffie-Hellman 协议,非叶子结点 v 的私钥由一个孩子结点的私钥和另一个孩子结点的公钥生成:

$$K_v = (BK_{2v+1})^{K_{2v+2}} \bmod p = (BK_{2v+2})^{K_{2v+1}} \bmod p = g^{k_{2v+1}k_{2v+2}} \bmod p, \quad (1)$$

因为每个结点的公钥是公开的,所以每个用户能沿着他的密钥路径计算路径上所有结点的密钥. 例如图 1 中用户 M_1 随机产生密钥 K_7,并且他能通过用户 M_2 得到结点 8 的公钥 BK_8,从用户 M_3 得到结点 4 的公钥 BK_4,从用户 M_4,M_5 或者 M_6 处得到结点 2 的公钥 BK_2. 给出 M_1 的私钥 K_7 和公钥 BK_8,根据(1)式,M_1 能生成私钥 K_3. 由公钥 BK_4 及新生成的密钥 K_3,同样 M_1 能生成私钥 K_1. 由 K_1, BK_2, M_1 就可计算出根结点 0 的私钥 K_0.

为了保证后向安全性、前向安全性,当组成员有任何变化(用户加入、离开)时,均需要重新生成组密钥. 在组成员变化前,选取一个特殊的组成员称为发起者(sponsor). 这个发起者负责更新密钥,向其他用户多播密钥信息[3,4].

2　椭圆曲线公钥密码体制的 TGDH-BD 方案

上述2个协议的安全性均是建立在 CDH（Computational Diffie-Hellman Assumption）以及一般有限域上离散对数问题 DLP（Discrete Logarithm Problem）计算难题之上. 为了增强协议安全性，我们选择更安全的椭圆曲线公钥密码体制. 因为有限域上的椭圆曲线离散对数问题 ECDLP 是比一般有限域上的离散对数问题要困难得多的一个困难问题，至今没有亚指数算法求解 ECDLP，而有限域上的 DLP 已有亚指数算法了. 所以基于 ECDLP 的密码系统具有更高的安全性. 确定有限域 F_q，选择安全有效的椭圆曲线 $E(F_q)$，固定基点 G，确定椭圆曲线域参数[11]，建立椭圆曲线公钥密码体制. 这样上述协议中的一般有限域上对生成元 g 的幂运算均换成椭圆曲线上对固定基点 G 的点乘运算[12].

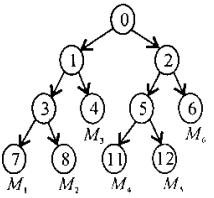

图1　密钥树

在组密钥约定协议中，通信量与计算量是衡量协议是否有效的最关键的两个因素. 基于分布式系统及 Internet 网络资源特点，分散较远的用户之间的密钥约定协议应该尽量减少通信量，因为这时通信开销比计算开销大. 分布在拥挤的局域网内的用户之间的密钥约定协议应该尽量减少计算量，因为此时计算花销比通信花销大. 一般地，节省通信量可能要增加计算量，节省计算量就要增加通信量. 目前很难有一种协议做到两全其美. 上面两种方案的通信量和计算量比较（主要是求幂运算）如表1所示. 权衡通信量和计算量的开销，我们提出一种基于椭圆曲线密码体制的 TGDH-BD 协议. 由于 BD 协议的计算量相对较少，而通信量相对较多，适宜于短距离的局域网内部的密钥约定；而 TGDH 协议通信量相对较少，计算量相对较多，适宜于长距离的分散的用户之间的密钥协商. 基于实际使用资源分布的不确定性，既有分散较远的又有相对较拥挤的用户，所以我们提出了基于椭圆曲线密码体制的 TGDH-BD 方案.

表1　TGDH 与 BD 模型的通信量和计算量比较

模型		通信量			计算量
		Rounds	Msgs	Broad	Exp
TGDH	Jion，Merge	2	3	3	$2\log n$
	Leave	1	1	1	$\log n$
	Partition	$\log n/2$	$\log n$	$\log n$	$\log n$
BD		2	$2n$	$2n$	3

该方案首先把相对较近的同在一个局域网内的所有用户组成一子组，如图3的子组7中有用户 M_1、M_2、M_3. 在子组7中，应用基于椭圆曲线密码体制的 BD 协议求出其子组密钥 K_7. 其计算过程如下：①M_1，M_2，M_3 分别随机选取整数 r_1，r_2，r_3 作为私钥，计算公钥 $P_i = r_iG$ 并广播（在子组内）；②计算并广播 $Q_i = r_iP_{i+1} - r_iP_{i-1}$；③ 计算子组密钥 $K_7 = 3r_iP_{i-1} + 2Q_i + Q_{i+1} = 3r_iP_{i-1} + 2r_iP_{i+1} - 2r_iP_{i-1} + r_{i+1}P_{i+2} - r_{i+1}P_i = (r_1r_2 + r_2r_3 + r_3r_1)G$（其中 $i - 1 = (i + 2)\bmod 3$）. 而各个这样的子组（如图 2 中的子组 7，11，12），与其他分散的用户（如 M_4、M_5、M_{12}）一样，作为 TGDH 密钥树中的叶子结点. 各子组与分散的单个用户之间应用基于椭圆曲线密码体制的 TGDH 协议生成共享的组密钥 K_0. 例如子组 7 计算组密钥过程如下：知道自己的私钥 K_7，从用户 M_4 处得到结点 8 的公钥 P_8，可以计算结点 3 的私钥 $K_3 = K_7P_8 = K_7K_8G$；从用户 M_5 处得到结点 4 的公钥 P_4，可以计算 $K_1 = K_3P_4 = K_3K_4G$；从子组 11，子组 12

或用户 M_{12} 处得到结点 2 的公钥 P_2，可以计算根结点私钥，即组共享密钥 $K_0 = K_1P_2 = K_1K_2G$.

为了保证组通信的前向安全性、后向安全性，当有组成员变化（加入、离开）时，需要更新组密钥. 在我们的方案中，当有新用户加入时，首先选择将要插入的地方（结点）. 插入原则是选择加入在同一局域网内的子组，如没有这样的子组，就根据 TGDH 协议选定插入点[3,4]. 用户插入后需要调用 BD 协议更新插入后的子组密钥，再根据 TGDH 协议更新密钥树，重新生成新的组密钥. 当有组成员离开时，同样需要更新变化了的子组和整个密钥树，重新生成组密钥.

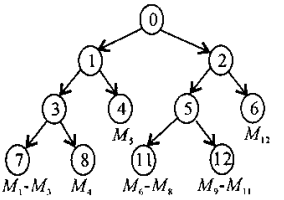

图2 BD-TGDH 模型

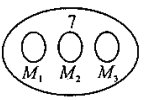

图3 BD 模型

该方案的安全性建立在椭圆曲线离散对数计算难题之上. 由于有限域上的椭圆曲线离散对数问题是比一般有限域上的离散对数问题要困难得多的一个问题，所以该方案更安全. 与 TGDH 协议相比，TGDH-BD 方案中的密钥树级数大大减少，所以计算量相应减少. 另外子组内采用 BD 协议，虽然通信次数增加，但因为通信距离短，所以通信开销并不大，相反计算量大大减少. 权衡通信量与计算量，选择 TGDH-BD 结合的最佳方案最大可能地减少了通信开销与计算工作量，相比单个 TGDH、BD 方案，该方案更有效.

3 结束语

随着网络计算技术的发展，出现了大量分布式、动态的协作组应用. 相应地产生了一种新的密钥管理方案——组密钥约定. 本文分析了两种流行的组密钥约定协议——BD 和 TGDH 协议，并就基于 Internet 资源的分布特点，提出一种基于椭圆曲线密码体制的 TGDH-BD 组密钥约定方案. 该方案的安全性建立在计算有限域上椭圆曲线离散对数难题之上，同时考虑了实际资源分布的不确性，最大可能地减少了通信和计算开销. 因此，该方案更安全、有效，适合分布式网络环境下的组应用.

参考文献

1 Burmester M, Desmedt Y. A secure and efficient conference key distribution system. Advances in Cryptology-Eurocrypt, 1994, 275～287.

2 Burmester M, Desmedt Y. Efficient and secure conference-key distribution. Security Protocols Workshop, 1996, 119～129.

3 Kim Y, Perrig A, Tsudik G. Simple and fault-tolerant key agreement for dynamic collaborative groups. In: Proceedings of the 7th ACM Conference on Computer and Communications Security (ACM CCS 2000), ACM Press, 2000.

4 Kim Y, Perrig A, Tsudik G. Communication-efficient group key agreement. Information Systems Security, In: Proceedings of the 17th International Information Security Conference, 2001.

5 Steiner M, Tsudik G, Waidner M. Cliques: A new approach to group key agreement. Proceedings of the 18th International Conference on Distributed Computing Systems, 1998. 380～387.

6 Patrick P, Lee C, John C et al.. Distributed collaborative key agreement protocols for dynamic peer groups. 10th IEEE International Conference on Network Protocols, 2002.

7 Miller V. Uses of elliptic curves in cryptography. Advances in Cryptology-CRYPTO'85, Lecture Notes in Computer Science, Springer-Verlag, 1986, 218: 417～426.

8 Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation, 1987, 48: 203～209.
9 Diffie W, Hellman E W. New directions in cryptography. IEEE Trans Inform Theory, 1976, 6: 644～654.
10 Wallner D, Harder E, Agee R. Key management for multicast: Issues and architecture. Internet-Draft draftwallner-key-arch-00. txt, 1997.
11 Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security, 2001, 1(1): 36～63.
12 López J, Dahab R. An Overview of Elliptic Curve Cryptography. Http://citeseer. nj. nec. com/333066. html. 2002-12-06.

（责任编辑：黎贞崇）

星载 SAR 分布杂波的计算机模拟

高　飞[1]　玉振明[2]

（1. 北京航空航天大学203教研室　北京　100083；2. 广西大学梧州分校　梧州　543002）

摘要　星载雷达是适应各种军用和民用的目的而提出来的，美国和加拿大都在研究包含 SAR（合成孔径雷达）-GMTI（地面运动目标指示）模式的星载雷达，由于星载雷达在地面轨迹较大，卫星速度快，运动目标信号淹没在强大的地杂波中。为了完成 GMTI 功能，只有首先对 SAR-GMTI 系统中地杂波精确建模，分析和掌握其在 SAR 机制下空间分布情况和功率谱特性，才能有效去除杂波。地杂波建模困难，具有很多随机性的环境因素，没有现成的算法，跟具体雷达设备、系统参数也有关系。因此杂波仿真是很复杂的，大量仿真和实验数据表明 K 分布较能精确描述杂波，而且引入了空间的相关性。本文用 K 分布来描述雷达截面积的空间起伏。K 分布的混合模型包含了杂波起伏的两个分量。一、快变化分量也称为斑点分量，其幅度服从负指数分布的方根即瑞利分布，源于雷达从随机相位散射点反射回波的相干求和；二、慢变化分量也称为纹理分量，它服从平方根伽马分布，纹理变量表征观测面特性，受成像场景物理特性的影响，决定了场景空间变化的雷达横截面。因此 K 分布杂波模型等同于用伽马分布去调制平方律检测（负指数分布）的功率调制过程。本文通过无记忆非线性变换产生相关高斯序列，多个独立的相关高斯序列分别组成相应纹理分量和斑点分量，最后产生相关 K 分布序列，并且对它进行统计检验和相关性检验，验证其正确性。

本文基于 SAR（合成孔径雷达）机制，主要针对复杂的星载几何关系和坐标变换关系，给出了分布杂波仿真的详细步骤，通过公式推导，假设一定尺寸的目标位于地面，分辨单元的数据是产生的 K 分布序列，经过卫星几何关系投影到斜距方向，由几何关系和星历表计算多谱勒中心频率和调频率，每个等效点反射体被发射信号展宽，循环所有点，相干叠加可求得回波信号，最后给出仿真结果。仿真过程同样适用于分布目标的仿真。

本文对生成的杂波经过成像处理并且将它应用于一种杂波抑制技术 DPCA（天线相位中心偏移法）的研究。DPCA 利用两个独立的沿载机飞行方向放置的接收通道，使前向天线的相位中心与延迟一段时间后拖尾天线的相位中心保持一致，从而补偿由于平台运动带来的杂波谱展宽，实现杂波抑制。利用本文的分布杂波仿真方法，验证 DPCA 杂波抑制结果，结果表明该方法行之有效，对工程问题有一定的指导意义。用本文的模拟技术为今后深入研究星载 SAR-GMTI 技术提供了仿真数据。

关键词　星载 SAR（合成孔径雷达）　GMTI（地面运动目标指示）　杂波仿真　DPCA（天线相位中心偏移法）