Internet 路由级拓扑的自相似分形统计

张 君 赵 海 付大愚 张 昕
(东北大学信息科学与工程学院 沈阳 110004)

摘 要 由于多角度多度量的统计方法存在种种问题,提出了通过分形维数从整体上刻画互联网拓扑性质。以传统分形理论为基础,结合互联网拓扑所具有的自相似性质,给出网络拓扑维数的相关概念,并通过网络拓扑与欧氏空间的映射关系,对拓扑维数进行了深入的解释。分析了理想分形拓扑的迭代膨胀过程,指出简单分形方法的不足,并进一步给出加权分形的相关定义及计算方法。通过统计互联网路由级拓扑的几个主要特征量,分析了拓扑维数与传统统计度量方法的关系,说明了拓扑维数在适用于统计观察互联网宏观拓扑的整体特性方面的作用。

关键词 复杂网络,自相似性质,分形维数,拓扑维数,幂率,路由级拓扑
中图法分类号 TP301.5,TP393 **文献标识码** A

Fractal Statistic on the Self-similarity of Internet Router-level Topology

ZHANG Jun ZHAO Hai FU Da-yu ZHANG Xin
(College of Information Science and Engineering, Northeastern University, Shenyang 110004, China)

Abstract Because the statistical method with multi-angle and multi-measurement has many problems, a method to depict the overall Internet topology characteristics by using network fractal dimension was proposed in the paper. With the basement of the traditional fractal theory, combined with the self-similarity of Internet topology, the related concepts of the network topology dimension were given. By the mapping from Euclidean space to topology structure, the network topology dimension had been analyzed deeply and then the definitions of weighted network topology dimension and the computation method were given. By computing some main measurements in Internet topology such as power-law distribution and clustering, we analyzed the relationship between the network topology dimension and the traditional statistical method, described the advantage to depict network integral properties using network topology dimension.

Keywords Complex network, Self-similarity property, Fractal dimension, Topology dimension, Power law, Router-level topology

在已经获得的真实可靠的互联网拓扑数据基础之上,最重要的一项即是数据的统计整理。由海量的、分散的、不一致的、甚至近似于杂乱无章的数据中得到关键统计量,由此观察到可能存在的拓扑规律,是统计工作的重点[1],也是主要目的。在经历了初期的简单统计阶段之后,节点平均度、最大节点度、跳数等初级统计量已不能满足拓扑规律提取分析的要求。随后的网络幂律规律与聚集性质等方面的研究[2-4]指出了更深层的统计量需求和方向,诸如幂指数、聚集系数、核数等高阶统计量得到广泛关注和重点研究[5,6]。但这些统计工作基本局限于各自的网络性质范畴之内,即是说每个单独的统计量只能体现网络的某一方面性质,虽然一方面推动了网络各关键度量间的关联性研究,但终非是解决问题的根本方法。

从宏观上整体的看待网络的多方面属性,统一的表述拓扑的多种主要性质,是对网络拓扑统计研究的关键需求和重大挑战。在描述事物整体性质方面,分形几何近年来得到自然科学界的极大重视,由于传统的整数几何只能描述事物的表观现象,而分形维数可以通过简单表述来刻画事物的内在特性,因此分形理论可以用于研究复杂系统的自相似性,通过少量信息体现研究对象的本质。本文将分形理论与互联网复杂拓扑结合,给出网络拓扑分形维数的定义,并同时给出计算方法。重点分析了网络分形性质与目前已知的主要性质间的关系,论证了通过分形维数从整体上考察网络拓扑的合理性。

1 拓扑分形定义与计算方法

自相似性质的研究在几何学领域发展迅猛,通过分形理论的支持,可以定性定量的考察自然界中复杂形状物体的不规则性,从山峰与碎石的相似,河流中干流与支流的相似,到雪花结晶的自相似等等。分形理论在网络相关技术方面的拓展主要是在流量工程领域,考察时变曲线的自相似性质[7-9]。而互联网宏观拓扑结构也具有自相似的性质,无论是通过变换粒度来观察,还是由推断网络形成过程来分析,都可以发现

到稿日期:2008-11-06 返修日期:2009-01-21 本文受国家自然科学基金资助项目(69873007),国家级火炬计划项目(2002EB010154)资助。
张 君(1967—),女,博士生,讲师,主要研究方向为复杂网络,E-mail:zhangjun1@ise.neu.edu.cn;赵 海(1959—),男,教授,博士生导师,主要研究方向为复杂网络、普适计算、嵌入式系统及数据融合等;付大愚(1972—),男,博士生,主要研究方向为复杂网络;张 昕(1980—),男,博士,主要研究方向为复杂网络。

拓扑的局部与整体具有类似的特征。因此借鉴分形几何的理论，研究拓扑的自相似性质，是从整体对互联网进行统计研究的可行方法。

1.1 互联网的自相似性质

在互联网宏观拓扑结构的各个层次，都呈现出明显的度分布幂律规律，即互联网是一个无尺度网络。之所以被称为无尺度网络，是因为这样的网络局部与整体是自相似的，放大这个网络的任意部分都会发现它和整体面貌很接近，很难分辨当前的观察粒度。

不仅是幂律特性，在聚集性方面互联网也表现出各级拓扑间的相似性。在不同层级的拓扑中，均可以统计得到较高的聚集系数，且同时还可以观察到富人俱乐部现象。

这种自相似性质体现了网络拓扑一种自然的整体属性，即不依赖于局部的具体技术细节而表现出的宏观特征。可以借助这种自相似性，利用分形理论在自相似性质研究方面的先天优越性，给出一种面向互联网拓扑的整体刻画方法，从而使不借助过多统计特征量而全面考察网络特征成为可能。

1.2 拓扑分形定义

分形理论十分适合用于研究事物的自相似性质。但是经典分形几何主要针对欧几里得空间进行描述，在实际应用中多用于曲线或曲面的计算分析，而对于网络拓扑来说，直接应用经典分形理论开展研究工作有很大难度。与欧氏空间所具备的诸如长度或体积等直观度量不同，网络拓扑范畴中没有通常意义下的测度概念，因此很难直接应用以测度概念为基础的分形分析。Yook[10]直接按照物理连接的距离绘制互联网在欧氏空间平面的结构，脱离了拓扑的范畴。Song[11]为了分析细胞网络、蛋白质网络、万维网等复杂网络拓扑，将节点间连接的数目定义为传统意义上的“距离”，并按照经典分形定义所描述的，通过穷举方法搜索最小覆盖，进而计算出网络的维数。该方法虽然给出了一种计算网络维数的途径，但作为体现拓扑特征的统计度量，该定义对具有分形维数对象的诸多特性体现不足，同时其计算代价十分巨大，在实际工作中的可应用性大大降低。

借鉴经典分形相关定义方式[12]，将其主要概念映射到网络拓扑范畴，从而给出网络拓扑分形主要定义的形式化描述如下。

定义 1(拓扑集合/节点) 整个网络空间 Ω 由不可数个点构成，拓扑集合即是由其中部分点组成，下文简称集合。集合的直径为该集合包含点的多少，因为只涉及集合相对大小，故直径采用相对度量：若集合 A 可以等分为 N 个子集合 B，则集合 B 的直径为集合 A 的 $1/N$，反之同理。直径为 D 的集合也称为 D-节点。

定义 2(拓扑覆盖) 设节点 A 中的点与节点 B 中的点之间存在连接，则称节点 A 与节点 B 之间存在连接。若两个 D-节点均在集合 F 中，则这两个节点间的连接称为集合 F 的一个 D-覆盖。显然，当这两个 D-节点分裂为 $2N$ 个 D/N-节点时，该 D-覆盖可以划分为至少一个 D/N-覆盖。

定义 3(拓扑测度) 将集合 F 划分为若干 D-节点，则当 D 趋近于 0 时，D 的 S 次幂与集合 F 的 D-覆盖总数的乘积，称为集合 F 的 S-拓扑测度，记作 $HS(F)$，并简称为 S-测度：

$$H^s(F)=\lim_{D\to 0}\sum D^s \tag{1}$$

定义 4(拓扑维数) 若存在 S_0，使得集合 F 的测度 $HS(F)$ 为正的有限值，即：

$$0<H^S(F)<+\infty,(S=S_0)$$

则集合 F 的拓扑维数为 S_0，简称维数。

在分形的研究范畴内，通常所关心的是一种相对的尺度，即研究对象“膨胀”后其测度的变化率，而且这种膨胀可以是双向的：一种是放大观察集合，体现观察集合内更多的细节；另一种是观察集合的增长，更多相同结构的集合与原集合合并，表现出更为复杂的结构。在研究网络分形性质时，前一种膨胀对应的是由粗到细的观察粒度，如 AS 级拓扑与路由级拓扑对比，后一种膨胀则对应网络的迭代增长，如局域网互联构成城域网。

网络拓扑与欧氏空间的映射可以用一种简洁、直观的方法表述。将拓扑中的点给出一个任意序，对应欧氏空间 2 维平面的坐标区间，拓扑中的连接则是对应的坐标区间对所标示的区域，一个拓扑可看作 2 维欧氏空间内的一个对象，即一个平面图形。当网络拓扑放大膨胀时，坐标区间划分为小区间，则连接所对应的区域也划分为更小的多个区域，拓扑对应的图形也发生变化。同样，拓扑进行增长膨胀时，则是多个图形拼接，在坐标为相对刻度时，两类膨胀对图形产生的变化是一致的。通过观察拓扑膨胀过程中对应图形的测度变化，就可以得到所需的拓扑维数。

通过与欧氏空间对象的映射分析，可以看出在拓扑分形概念中节点数目与连接数目的关系确定了拓扑的维数。分形定义的给出完成了分形基本理论基础由欧式空间到网络拓扑的映射关系，同理类比于欧式空间上的相似维数[12]，可以得到拓扑维数的一种简便计算方法：网络拓扑膨胀后，节点数为原节点数的 N 倍，连接数为原连接数的 N' 倍，则该拓扑的维数为 $\log N'/\log N$。这种相似维数计算方式更好地体现了考察对象的自相似性，同时也体现了分形分析的双向性：不考虑膨胀的方向性，而仅考察节点数与连接数。这种定义与计算方式可以很好地刻画网络拓扑的维数，同时与欧氏空间下的分形相关定义与计算方式一样，具有直观上的含义：维数可以表征该对象的膨胀速度，维数越高的对象，其测度随集合增大而膨胀得越快。欧氏空间中曲线测度为 1 维的“长度”，其膨胀率为线性；曲面测度为 2 维的“面积”，其膨胀率为平方级；球体测度为 3 维的“体积”，其膨胀率为立方级；分数维对象相关性质则居于相应整数维对象之间。同样，拓扑维数也可以刻画网络拓扑的类似性质，1 维的规则网络随节点数增加，其连接数目呈线性增长，相对的 2 维全连接网络则呈平方级增长。

1.3 加权扩展定义

拓扑维数说明网络拓扑的复杂程度，当其具有介于 1 和 2 之间的分数维时，维数越大说明该网络拓扑越倾向于全连接的 2 维网络。按照上节给出的计算方法来看，当拓扑维数明显大于 1 时，随着拓扑膨胀，节点数目增加，网络拓扑中连接数目呈指数增长，若节点数目接近实际互联网拓扑，则连接数目将会十分巨大，远大于互联网中统计得到的数值。因此，按照该计算方法得出的互联网拓扑维数应该接近于 1，这对互联网拓扑的分形特征体现比较不利。因此需要对上述的分形相关定义进行扩展。前述定义说明了网络拓扑中连接数量的迭代增长可以体现网络的复杂程度，但不同连接的重要程度实际上也有所区别，这一点在复杂程度的衡量时应该有所

考虑。通常，连接的重要性可以由几个方面来体现，如流量、介数、端点度等等。考虑到相关定义的合理性以及计算的便利，选用端点度对连接进行加权处理。另一方面，由于膨胀连接对于拓扑维数具有重要意义，膨胀后的连接可能会选择不同的端点，以端点度进行相应加权可以区分此类不同，如核心节点和边缘节点就存在节点度的差别，这样即使膨胀连接数目不多，也可能通过加权获得非线性的增长，从而使拓扑维数不再限于1附近。

定义5(拓扑加权覆盖) 设两个 D-节点 A 和 B 均在集合 F 中，节点 A 的度为 d_A，节点 B 的度为 d_B，则节点 A 与节点 B 之间的连接即为集合 F 的 $\frac{d_A+d_B}{2}$ 个 D-加权覆盖。

定义6(拓扑加权测度) 依拓扑加权覆盖得出的拓扑测度即为拓扑加权测度，简称加权测度。

定义7(拓扑加权维数) 依拓扑加权测度得出的拓扑维数即为拓扑加权维数，简称加权维数。

由加权定义可以看出，连接加权是指每条连接按其两个端点的度均值计数。拓扑维数的简便计算方法也同样适用于加权维数：网络拓扑膨胀后，节点数为原节点数的 N 倍，连接加权数为原连接加权数的 N' 倍，则该拓扑的加权维数为 $\log N'/\log N$。其中连接加权数是指所有连接加权后的计数总和。

由于规则网络在细化的过程中，节点度保持不变，因此连接的加权为常数，这样网络在膨胀时加权连接数目变化速度与未加权时一样，仍是线性变化，所以规则网络的加权维数仍然为1。但全连接网络的维数在加权定义下会发生变化，由于在膨胀时节点度会有所增长，导致连接加权增加，而全连接网络节点度与连接数目相等，因此加权幅度也就是节点度增长的幅度。由连接数目的平方增长乘以加权的线性增长，全连接网络拓扑的加权膨胀速度提升至立方级，因此全连接网络的加权维数为3。

另一个在加权维数定义下维数明显变化的是星型网络，这种网络在膨胀时连接都集中到中心节点。非加权时，星型网络维数为1，但加权时由于中心节点度猛增，且连接都集中于一点，所有连接均获得加权且量级与连接数目相同，因此连接的加权膨胀速度为平方级，拓扑维数也相应的为2。

实际互联网的拓扑维数计算，可以通过缩放观察粒度来考察拓扑节点数目变化与连接加权数目变化的关系。但是如何将拓扑中的节点划分为不同集合，并将节点集合看作是一个节点，以实现粗粒度观察互联网拓扑，是一个需要考虑的问题。不同的划分方法会导致不同的观察结果，最终会影响拓扑维数的计算。由于传统分形理论对于计算几何体的维数有很多有效的方法，因此结合欧氏空间与网络拓扑的映射关系给出解决方案，是一个较为理想的做法。理想的自相似网络拓扑映射到欧氏空间，也应形成理想的平面分形图形，显然，问题的重点在于如何确定拓扑中节点在欧氏坐标中的位置。合理的拓扑映射后，粗粒度时拓扑中的核心节点对应图形中的突出特征，在观察粒度变细时，图形特征散列开，此时拓扑中的细粒度核心节点也应随之散开。因此，本文采用如下方法安置拓扑中的节点：选取一区间，大小为拓扑中节点数目，将节点按度降序排列，度最高的节点位于区间正中，将原区间分为两半，次高的两个节点分列两个子区间的正中，依此类推。划分节点集的时候，按所需节点集大小将区间等分即可。图1给出互联网路由级拓扑膨胀的具体情况，即在不同粒度下节点数目与连接数目的对比，包括非加权与加权两种情况，且均取对数值。由于现实中的事物不可能具有绝对理想的分形性质，通常仅考察其一定缩放范围内的自相似性质，因此拓扑的最粗粒度取为100个节点为一个集团。

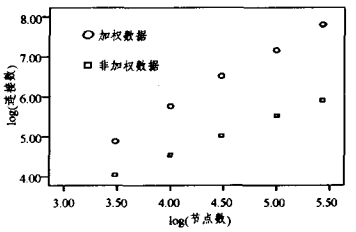

图1 路由级拓扑膨胀情况

图1显示拓扑膨胀过程中，节点与连接的变化规律在对数坐标下呈近似直线，其斜率即为网络的拓扑维数。计算得互联网路由级拓扑非加权维数约为1.02，加权维数约为1.38，显然加权维数具有更好的体现网络拓扑深层次性质的能力。下面主要考察加权拓扑维数。

2 自相似性质分析

互联网呈现多种多样的特性，这些特性又极其自然的融合在实际的拓扑当中。而网络的自相似性质虽然具有从整体上考察宏观拓扑的潜力，但对于网络现有主要特性的涵盖仍需进一步论证，拓扑维数与现有统计度量的一致性也需要考证。因此通过统计互联网路由级拓扑的具体特征，结合对自相似性质的分析，深入展示网络拓扑的多种主要性质在自相似性质下的融合情况是十分必要的。

2.1 与度分布关系

由数据统计可知，互联网路由级拓扑节点度分布十分不均匀，度小于等于3的节点约占节点总数的1/3。图2描述了拓扑中节点度的degree-rank幂律分布与CCDF(d)-degree幂律分布情况及各自的拟合曲线，图中横纵坐标均取自然对数值，拟合得到秩幂指数为0.831，补累计幂指数为1.256，表现出显著的幂律规律。图中显示，在叶子节点部分以及节点度较高时拟合曲线偏差较大，但整体拟合效果较好，尤其是CCDF(d)-degree幂律分布，符合其对数据偏差鲁棒性较好的特点。

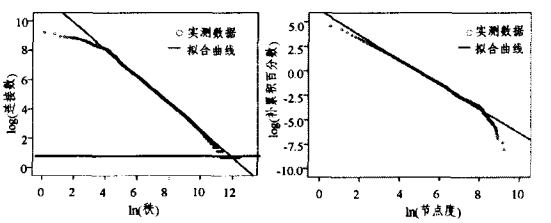

图2 路由级拓扑节点度幂律分布

补累积幂律分布与秩幂律分布均显示出互联网的度分布扭曲性，这种扭曲性质通常认为是由节点连接的度优先倾向产生的。但从自相似拓扑膨胀的观点出发，可以得到另一种解释。在粗粒度观察下，网络已具有不均匀的度分布，如在国家级别上，美国拥有绝对的高连接率，几乎任何一个国家的互联网均与美国相连。在AS级别上，也可以看到不同节点度

的巨大差异，上游的服务提供商拥有大量的客户。同样，在细粒度下，拓扑也具有度分布的扭曲，核心路由器具有更大的转发能力，从而获得更多的连接。这种层层迭代的自相似性形成了拓扑整体的度分布结构：由少数核心节点与部分边缘节点组成原始结构，其中核心节点拥有较高的度，膨胀过程中，原单一节点转变为与原结构相似的一组节点集，且各集合之间仍具有一定数量的连接，这些连接则主要由各组的核心节点来维持。随着迭代次数的增加，最初的少数核心节点获得了大量的连接，相应的次一级核心节点数目相对增加，但其拥有的连接数目则比上一级核心节点有所下降。依此类推，形成了少数高度节点伴随大量低度节点的现象，并且这种现象是一种普遍的、多层级的存在。

自相似膨胀可以产生扭曲的度分布，而拓扑维数则可以对扭曲程度进行定量的描述。从整数维网络拓扑来看，1 维的规则网络度分布均匀，其扭曲程度最弱，而 2 维的星型网络扭曲程度则显然最强。实际互联网路由级拓扑的扭曲程度显然在这两者之间，同时其拓扑维数也是大于 1 并小于 2 的分数维。由星型网络的拓扑维数分析可以看到，维数小于 2 的网络拓扑，在随膨胀过程发生节点数目的变化时，连接的数目变化是线性的，其维数提升的重点并不在于连接数目的增长，而是在于连接加权的增长，而这种加权的增长正是度分布不均匀造成的。当核心节点随膨胀迭代而获得更多连接时，这些连接的加权也在随之增加。度分布的扭曲程度越厉害，就表示核心节点的连接聚集力越强，则连接加权的增长越快，拓扑维数也就越大。

2.2 与聚集性质关系

聚集性质通常由聚集系数、富人俱乐部连通性与同配性系数来表示，而且这几个重要度量之间具有十分密切的关联。统计互联网路由级拓扑的平均聚集系数为 0.302，但单凭平均聚集系数不能判别网络拓扑内节点的具体聚集情况，因此对部分节点的局部聚集系数进行了统计，同时为考察富人俱乐部性质，统计了拓扑的富人俱乐部连通性。表 1 给出了二者的统计结果，表中显示，低度节点依靠高度节点作为邻居而获得较高的局部聚集系数，但低度节点之间的连通性极差，而高度节点之间的联系则相对紧密，不过连接比例并不十分高。这主要是由于路由级拓扑节点数量巨大，即使是高度节点之间的互联也比较有限。

表 1 路由级拓扑的局部聚集系数与富人俱乐部连通性

节点度	局部聚集系数(均值)	富人俱乐部连通性
2	0.41	约为 0
3	0.40	约为 0
4	0.32	约为 0
Top1%	约为 0	0.005
Top0.5%	约为 0	0.011
Top0.2%	约为 0	0.133

考察拓扑中低度节点向高度节点的连接倾向，图 3 给出度为 2 节点的邻居作为高度节点的累积分布。可以看出，超过 60%的邻居是度靠前的 20%的节点，这体现了互联网的异配性质。这种异配性质使得低度节点更倾向于与高度节点相连，从而获得较高的局部聚集系数，反之高度节点的低局部聚集系数则是由于邻居度普遍较低而造成的。但同时路由级拓扑的富人俱乐部连通性并不是很高，所以整体聚集性也并非十分突出。

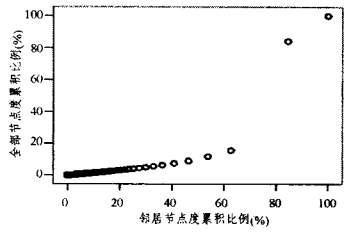

图 3 路由级拓扑的异配性质

从自相似性质的角度看来，核心节点在迭代膨胀过程中保持了相互间的连接。但核心节点数量有限，这种互联并不能使大量高度节点之间形成高比例的联通。而且迭代过程所增加的连接数目为线性，次一级核心节点之间增加连接的机会不多，达到较高富人俱乐部连通性的可能性也就不大。而低度节点主要在迭代过程的末期出现，其连接主要围绕各自迭代体的核心节点，自然的形成异配结果。异配性质与富人俱乐部性质共同造就了互联网路由级拓扑的聚集性分布。

考察整数维网络拓扑，可发现维数为 2 的星型网络聚集系数极高，其拓扑中除中心节点外，其余所有节点均只有一个邻居，因此非中心节点的局部聚集系数均为 1，从而网络的平均聚集系数随节点数上升而无限接近于 1。同时，拓扑中心节点的局部聚集系数为 0，整个拓扑的局部聚集系数关于节点度的分布呈现极不均匀的特征。且由于星型网络中心节点的唯一性，使得其富人俱乐部连通性也极高，并且所有非中心节点均只与中心节点连接，形成了十分突出的网络异配性质。相对地，维数为 1 的规则网络则由于网络中节点度均等，从而不具有富人俱乐部性质，也不涉及是否为同配网络的问题。规则网络的局部聚集系数有可能很高，但其关于节点度的分布均匀。具有分数维的实际拓扑的聚集性质介于二者之间，其富人俱乐部连通性与异配性质明显强于规则网络，并弱于星型网络，且局部聚集系数也呈不均匀分布，但不均匀程度弱于星型网络。

结束语 目前统计技术常采用多角度全面统计，为避免众多统计度量所产生的各自的片面性、多余的复杂性以及不必要的计算代价，本文提出通过分形维数刻画网络整体性质，并以性质丰富且具有足够数据量级的路由级拓扑为分析对象。通过欧氏空间与拓扑结构的映射，给出网络拓扑维数的相关概念与计算方法，并将互联网拓扑的自相似性质与分形理论中的迭代概念结合起来。根据互联网的实际情况分析，进一步给出加权拓扑维数的定义，并将其作为刻画互联网整体性质的重点度量，统计了互联网拓扑中幂律性质、聚集性质等几个主要代表性特征，结合规则网络、星型网络等整数维网络的性质分析，论述了网络拓扑维数与主要拓扑性质之间的联系，说明了自相似特性与对应的网络拓扑维数度量在体现网络拓扑整体特性方面的优势。

参 考 文 献

[1] Boccaletti S, Latora V, Moreno Y, et al. Complex networks: structure and dynamics[J]. Physics Reports, 2006, 424: 175-308

[2] Chen Q, Chang H, Govindan R, et al. The origin of power laws in Internet topologies revisited[C]// Proc. IEEE INFOCOM. 2002, 2: 608-617

(下转第 67 页)

$$\Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A^*]=\Pr[A^*]\Pr[\bigwedge_{i=1}^{q_I} A_i \mid A^*]=\Pr[A^*](1-\Pr[\bigvee_{i=1}^{q_I} \neg A_i \mid A^*])\geqslant \Pr[A^*](1-\sum_{i=1}^{q_I}\Pr[\neg A_i \mid A^*])=\frac{1}{(l_1(n+1))}\cdot(1-\frac{q_I}{l_1})\geqslant \frac{1}{(l_1(n+1))}\cdot(1-\frac{(q_e+q_d)}{l_1})=\frac{1}{(4(q_e+q_d)(n+1))}$$

同理，有：

$$\Pr[\bigwedge_{j=1}^{q_M} B_j \wedge B^*]=\Pr[B^*]\Pr[\bigwedge_{j=1}^{q_M} B_j \mid B^*]\geqslant \frac{1}{(l_2(m+1))}\cdot(1-\frac{q_d}{l_2})=\frac{1}{(4q_d(m+1))}$$

所以有：

$$\Pr[\neg abort]\geqslant \Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A^* \wedge \bigwedge_{j=1}^{q_M} B_j \wedge B^*]=\Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A^*]\Pr[\bigwedge_{j=1}^{q_M} B_j \wedge B^*]=\frac{1}{(16q_d(q_e+q_d)(n+1)(m+1))}$$

若 $Z=e(g,g)^{abc}$，则敌手 $\mathcal{A}$ 将以 $\varepsilon+1/2$ 的概率猜对比特 γ；否则，若 Z 是随机的，$\mathcal{A}$ 没有任何优势猜对比特 γ，即它猜对 γ 的概率是 1/2。从而 $\mathcal{C}$ 解决 DBDH 问题的优势至少为 $\varepsilon/(32q_d(q_e+q_d)(n+1)(m+1))$。

时间复杂度分析：对 C 的运行时间的估算主要来自于应答询问需要的指数、乘法和双线性对运算。每次 Extract 询问至多需要 $\mathcal{O}(1)$次指数运算和 $\mathcal{O}(n)$次乘法运算。每次 Decrypt 询问至多需要 $\mathcal{O}(1)$次指数运算，$\mathcal{O}(n+m)$次乘法运算和 $\mathcal{O}(1)$次双线性对运算。所以 $\mathcal{C}$ 的时间复杂度为 $t'=t+\mathcal{O}((q_e+q_d)t_e+(nq_e+(n+m)q_d)t_m+q_dt_p)$。

结束语 针对 Waters 基于身份的基本加密方案仅达到选择明文安全的问题，提出了一个自适应选择密文安全的基于身份的加密扩展方案。与 Waters 加密方案相比，扩展方案增加了 1/3 密文长度，更重要的是提高了安全级别，适合应用于安全性要求较高的环境。在标准模型下，扩展方案的语义安全性归约为判定性双线性 Diffie-Hellman 困难假设。本文的结果为进一步具体的安全实施提供了有力的理论依据。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proc. Crypto 1984. LNCS 196. Berlin: Springer-Verlag, 1984:47-53

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairings[C]// Proc. Crypto 2001. LNCS 2139. Berlin: Springer-Verlag, 2001:213-229

[3] Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols[C]// Proc. of the first ACM conference on computer and communications security. New-York: ACM Press, 1993:62-73

[4] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited[J]. Journal of the ACM, 2004, 51(4):557-594

[5] Nishioka M, Komatsu N. A note on the random oracle methodology[J]. IEICE Transaction Fundamentals, 2008, E91-A(2): 650-663

[6] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报, 2005, 16(10):1743-1756

[7] Waters R. Efficient identity based encryption without random oracles[C]// Proc. Eurocrypt 2005. LNCS 3494. Berlin: Springer-Verlag, 2005:114-127

[8] Dent A W, Libert B, Paterson K G. Certificateless encryption schemes strongly secure in the standard model[C]// Proc. of the 11th International Workshop on Practice and Theory in Public Key Cryptography 2008. LNCS 4939. Berlin: Springer-Verlag, 2008:344-359

[9] Bellare M, et al. Relations among notions of security for public-key encryption schemes[C]// Proc. Crypto 1998. LNCS 1462. Berlin: Springer-Verlag, 1998:26-45

[10] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack[C]// Proc. Crypto 1998. LNCS 1462. Berlin: Springer-Verlag, 1998: 13-25

[11] Gentry C. Practical Identity - based encryption without random oracles[C]// Proc. Eurocrypt 2006. LNCS 4004. Berlin: Springer-Verlag, 2006:445-464

[12] Paterson K G, Schuldt J C. Efficient identity based signatures secure in the standard model[C]// Proc. of the 11th Australasian Conference Information Security and Privacy 2006. LNCS 4058. Berlin: Springer-Verlag, 2006:207-222

(上接第 58 页)

[3] Siganos G, Faloutsos M, Faloutsos P, et al. Power laws and the AS-level Internet topology[J]. IEEE/ACM Trans. on Networking, 2003, 11(4):514-524

[4] Zhou S, Mondragon R J. The rich-club phenomenon in the Internet topology [J]. IEEE Communication Letters, 2004, 8(3): 180-182

[5] 赵海，徐野，苏威积，等. Internet 网络效能及其物理特征量分析[J]. 东北大学学报：自然科学版，2006，27(11)：1216-1219

[6] 张君，赵海，周艳. Internet 路由级节点的度与核数的关系[J]. 东北大学学报：自然科学版，2008，29(5)：653-656

[7] Gao J B, Rubin I. Statistical properties of multiplicative multifractal processes in modeling telecommunications traffic streams [J]. Electronics Letter, 2000, 36:101-102

[8] 魏进武，邹江兴，陈庶樵. 网络流量的联合多重分形模型及特性分析[J]. 电子学报，2004，32(9)：1459-1463

[9] 罗恒端，吴诗其. 数据分组网中自相似业务模型的研究进展[J]. 通信学报，2002，23(7)：107-115

[10] Yook S H, Jeong H, Barabasi A L. Modeling the Internet's large-scale topology [J]. Applied Physical Sciences, 2002, 99(21):13382-13386

[11] Song C, Havlin S, Makse H A. Self-similarity of complex networks [J]. Nature, 2005, 433:392-395

[12] 肯尼斯·法尔科内. 分形几何[M]. 沈阳：东北大学出版社，2003