# 基于 Ad hoc 网的身份型广播加密方案

孙 瑾 胡予濮 张乐友
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

**摘 要** 考虑到动态 Ad hoc 网的安全性及效率难以兼顾的问题,提出一种有效的基于动态网络的广播加密方案,并给出严格的安全性证明。该方案建立在标准模型下,当用户之间通过广播方式传递信息时,采用双线性对运算对任意数量无状态用户可实现完全抗串谋攻击。在密钥提取过程中,通过引入身份随机数并利用撤销用户身份集合进行加密,使得新用户可以动态加入群却不改变加解密密钥和密文的长度,其大小不超过 O(1)。同时,所有有效操作过程在 O($r$)时间内完成,不依赖于用户总人数 $m$,从而大大提高了算法的传输及存储效率。安全性验证表明,该方案在 GDDHE 假设下是抗静态敌手 IND-IN-CPA 安全的。

**关键词** 动态 Ad hoc 网,可证明安全,标准模型,完全抗串谋攻击
**中图法分类号** TN918.1 **文献标识码** A

## Identity-based Broadcast Encryption Based on Ad hoc Networks

SUN Jin HU Yu-pu ZHANG Le-you
(Key Lab of Computer Network and Information Security, Xidian University, Xi'an 710071, China)

**Abstract** To give concurrent consideration in the security and efficiency, a novel identity-based broadcast encryption was developed for ad hoc networks. Through security analysis, the correctness and effectiveness of the above methods were verified. Based on the standard model, the bilinear maps were introduced to achieve the collusion-secure for arbitrarily large of users during the broadcast communication. In the process of extract, new users could join dynamically without modification of user decryption keys nor ciphertext size by using ID, and its size not much than O(1). Simultaneously, all efficiency measures were completed in O($r$) time but not depended on the number of user m, thus the efficiency of transmission and storage was improved. Proof of security shows that the proposed scheme is IND-IN-CPA secure against static adversaries in the standard model under the ($t$,$n$)-GDDHE intractability assumption.

**Keywords** Mobile Ad hoc networks, Provably secure, Standard model, Full collusion-secure

随着无线电通讯技术的快速发展,一种新的网络技术 Ad hoc 应运而生。它不需要有限基础设备的支持,通过移动主机可自由组网实现通信,从而推进了人们在任意环境下自由通讯的进程。但是,动态无线网络都是建立在一个公开的环境下,当成员之间传送信息时,其它接收设备也可接收广播信息,因此网络的安全性就显得尤为重要。

广播加密的核心思想是广播者将消息加密,通过广播方式发送给大量用户,其中只有拥有授权的合法用户才可以解密并获得真实信息。目前,这种加密方式在动态无线网络中的应用成为了密码学的一个新的研究热点。国内外学者纷纷涉猎于此,很多具有特殊用途的广播加密方案也相继被提出[1-6]。但这些方案存在明显的不足,比如基于的困难性问题太强,仅具有 Selective-ID 安全性或安全性依赖于随机预言机模型等。此类方法众多,正表明大家没有形成统一的认识。

最近,Y. Ching 提出一种有效的基于身份的 Ad hoc 网移动通讯协议[7],其综合了身份型加密方案[8]以及双线性对的优点。该方案采用对运算来替代以往方案中的群密钥生成运算,使得同阶段群成员不需要进行任何信息交换。但是,该方案建立在随机预言模型下,其安全性依赖于 Hash 函数的伪随机性。2009 年,Zhang 提出 Ad hoc 网中基于身份的广播加密方案[9],该方案在继承了前面方案优点的基础上,将方案建立在标准模型下,但效率还有待提高。

针对上述问题,本文提出一种基于动态 Ad hoc 网络的身份型广播加密方案,即采用双线性对运算,对任意数量的用户可实现完全抗串谋攻击,从而满足标准模型下的语义安全性。在身份嵌入过程中,通过引入身份随机数及使用被撤销用户的身份集合进行加解密,使得新用户可以动态加入群,却不改变加解密密钥及密文的长度。同时,所有有效操作过程不依赖于用户总人数 $m$,从而将算法的传输代价及存储代价控制在 O(1)和 O($r$)内。通过语义安全模式验证了本方案的正确性及安全性。

## 1 预备知识

### 1.1 双线性映射

设 $G_1$,$G_2$ 是两个素数 $p$ 阶的循环加法群,$G_T$ 是一个素

到稿日期:2010-03-25 返修日期:2010-06-21 本文受 973 项目(2007CB311201),国家自然科学基金项目(60970119)资助。
孙 瑾(1977—),女,博士生,讲师,主要研究方向为公钥广播加密方案的设计与分析,E-mail:oksunjin@xaut.edu.cn;胡予濮(1955—),男,教授,博士生导师。

数 $p$ 阶的循环乘法群，双线性映射 $e(\cdot,\cdot)$ 是 $G_1\times G_2\to G_T$ 并满足以下性质：

(1)双线性性：$\forall g\in G_1, h\in G_2$，及 $a,b\in Z_P$，$e([a]g,[b]h)=e(g,h)^{ab}$；

(2)非退化性：$\forall g(\neq 1)\in G_1, h(\neq 1)\in G_2$，$e(g,h)\neq 1$；

(3)可计算性：$\forall g\in G_1, h\in G_2$，存在有效算法计算 $e(g,h)$。

双线性对可以通过有限域上的超奇异椭圆曲线或超奇异超椭圆曲线中的 Weil 对或 Tate 对推导出来[10]。

### 1.2 广义判定性 Diffie-Hellman 假设(GDDHE)

**定义 1**($(t,n)-GDDHE$) 设双线性映射群系统 $S=(p,G_1,G_2,G_T,e(\cdot,\cdot))$，$f$ 和 $g$ 是两个随机的一般多项式函数：

$$f(X)=\prod_{i=1}^{t}(X+x_i)=\sum_{i=0}^{t}\mu_i X^i$$

$$g(X)=\prod_{i=t+1}^{n}(X+x_i)=\sum_{i=0}^{n-t}\upsilon_i X^i$$

其中，所有的 $x_i$ 都是 $Z_p^*$ 中随机互异的对儿元素。设 $g_0\in G_1, h_0\in G_2$ 是两个生成元，则给定 $g_0,[\alpha]g_0,\cdots,[\alpha^{t-1}]g_0,[\alpha\cdot f(\alpha)]g_0,[k\cdot\alpha\cdot f(\alpha)]g_0,h_0,[\alpha]h_0,\cdots,[\alpha^n]h_0,[k\cdot g(\alpha)]h_0,e(g_0,h_0)^{f^2(\alpha)g(\alpha)}$ 及 $T\in G_T$，判定 $T=e(g_0,h_0)^{kf(\alpha)\cdot g(\alpha)}$ 是否成立。

根据上述定义，我们用 $Adv^{gddhe}(t,n,A)$ 表示算法 $A$ 在多项式时间 $|p|$ 内成功判定 $T=e(g_0,h_0)^{kf(\alpha)\cdot g(\alpha)}$ 是否成立的优势。

**推论 1**($(t,n)-GDDHE$ 的普遍安全性) 对任意可能的算法 $A$ 总共提出 $q$ 次质询来完成 $(G_1,G_2,G_T)$ 中的群操作和对双线性映射 $e(\cdot,\cdot)$ 的评估，其优势为

$$\mathrm{Adv}^{gddhe}(t,n,A)\leqslant\frac{(q+2(n+t+4)+2)^2\cdot(t+n)}{2p}$$

### 1.3 动态广播加密的模型

在基于身份的广播加密(IBBE)中，一个公钥可以对任意多个身份构成的群进行加密。而在其基础上加入动态因素后所得到的动态广播加密体制(DBE)则更具实用性。它涉及两个权威实体[12]：群管理员和广播者。群管理员负责新成员加入时向其提供身份标签和解密密钥，而广播者负责加密消息并通过广播渠道发送给每个用户。动态广播加密方案由系统建立、密钥提取、加密和解密 4 个算法构成，详细表述如下。

系统建立：输入安全参数 $\lambda$ 及最大接收者的数目 $m$，输出群管理员密钥 $mk$ 与初始加密密钥 $ek$，其中 $ek$ 公开，而 $mk$ 仅由群管理员持有。

私钥提取：输入群管理员密钥 $mk$ 及用户序号，输出相应用户的身份标签 $lab_i$ 及解密密钥 $dk_i$。

加密：设用户集合为 $S=(ID_1,\cdots,ID_m)$，撤销用户集合是 $R$，广播者用初始加密密钥 $ek$ 首先为 $S\backslash R$ 生成 $(Hdr,K)$，其中 $Hdr$ 称为密文头部，$K$ 称为会话密钥(实际应用中多采用对称密钥)，然后利用 $K$ 加密消息 $M$，得到广播体 $C_M$ 并将 $(Hdr,R,C_M)$ 发送给每一个用户。

解密：设用户 $ID_i$ 是诚实用户，$(Hdr,R,C_M)$ 是其接收到的密文，他首先利用 $Hdr$ 析出 $K$，然后解密 $C_M$，恢复明文 $M$。

### 1.4 动态广播加密的模型的安全性

在动态广播加密 IND-ID-CPA 安全模型中，敌手不允许解密询问。设集合 $S^*$ 表示由接收者组成的最大的集合且 $|S^*|=m$，这些信息对敌手和挑战者均是公开的，二者进行如下的交互游戏。

初始化：敌手首先输入要挑战的集合 $S'=\{ID'_1,\cdots,ID'_t\}$，其中的用户是被腐化了的。

系统建立：挑战者运行该算法得到群管理员密钥 $mk$ 与初始加密密钥 $ek$，并将 $ek$ 发送给敌手 $A$。

阶段 1 敌手 A 适应性提出质询 $q_1,\cdots,q_{n_0}$，但每次质询前先确认用户是否诚实。第 $i$ 次询问 $q_i$ 的详细描述如下：设 $ID_i$ 为用来询问的对象，若 $ID_i\notin S'$，挑战者运行密钥提取算法，得到相应于 $ID_i$ 的私钥，并将其发送给敌手 A，敌手将此私钥保留。

挑战：当敌手 $A$ 决定阶段 1 结束时，挑战者运行加密算法，得到 $(Hdr',K)=Encrypt(S',PK)$，然后随机选取 $b\in\{0,1\}$，令 $K_b=K$，$K_{1-b}$ 为 $\tilde{K}$ 中任意元素($\tilde{K}$ 为 $G_1$ 中的一个子集)，最后将 $(Hdr,K_0,K_1)$ 返回给敌手。

阶段 2 敌手继续进行询问 $q_{n_0+1},\cdots,q_n$，每一次询问类似于阶段 1。

猜测：最后，敌手要输出一个猜测 $b'\in(0,1)$。当 $b=b'$ 时，宣布敌手在游戏中获胜。

我们用符号 $\mathrm{Adv}^{ind}_{IBE}(t,n,A)$ 表示敌手赢得游戏的优势，其中 $t,n$ 是攻击参数。

## 2 身份型动态广播加密方案

### 2.1 方案构造

依据文献[9,11]，本节提出一种新的基于 Ad hoc 网络的身份型广播加密方案。此方案仅用一个实体来同时扮演广播者和群管理员两种角色。设用户集合为 $S=(ID_1,ID_2,\cdots,ID_m)$。

系统建立：给定一个公共参数 $\lambda$，$C=(p,G_1,G_2,G_T,e(\cdot,\cdot))$ 是一个双线性映射系统并满足 $|p|=\lambda$。$g\in G_1, h\in G_2$ 是两个生成元。任选 $\alpha\in Z_p^*$，可得公共参数 $PK=\{C,g,h,\alpha,W,V\}$，其中 $W=[\alpha]g, V=e(g,h)$。

密钥提取：对任意的 $ID_i\in S$，计算 $A_i=[\frac{ID_i}{\alpha+ID_i}]g, B_i=[\frac{1}{\alpha+ID_i}]h$，则相应的密钥是 $d_{ID_i}=(C,ID_i,A_i,B_i)$。

加密：设 $R=\{ID_1,\cdots ID_r\}$，随机选择一个数 $k\in Z_p^*$，并在 $Z_p^*$ 上计算 $\theta=k\alpha, \theta_i=\frac{1}{\prod_{j=1}^{i}(\alpha+ID_j)}$，其中 $i=1,2,\cdots,r$，则通过公开的 $h,W,V$，在其各自的群中就可以计算得到：

$P_i=[\theta_i]h(i=1,2,\cdots,r)$，$T_1=[k]W$，

$T_2=[k\theta_r]h=[k]P_r$，$K=V^{k\alpha_r}$

以上计算均可在 $O(r)$ 时间内完成[8]，从而加密头部为 $Hdr=\{T_1,T_2,(ID_1,P_1),\cdots,(ID_r,P_r)\}$，输出为 $(Hdr,K)$。

解密：为了重新获得封装在 $Hdr$ 中的消息密钥 $K$，用户 $ID_i'$ 用 $\{ID_j,P_j\}_{j=1}^{r}\in Hdr$ 和 $d_{ID_i'}=(C,ID_i',A_i',B_i')$ 计算 $K=e(T_1,B_{i,R})\cdot e(A_i',T_2)$，其中：

$$B_{i,R}=[\frac{1}{\prod_{j=1}^{r}(\alpha+ID_j)}]B_{ID_i'}=[\frac{1}{(\alpha+ID_i')\prod_{j=1}^{r}(\alpha+ID_j)}]h$$

且 $B_{i,R}$ 是在时间 $O(r)$ 中计算出来。但注意 $ID_i'\neq ID_j$ 或 $i\notin R$，否则将会出错，且当 $R=\Phi$ 时，结构不为动态。

### 2.2 正确性

设 $Hdr$ 是合法的密文，则有

$$K=e(T_1,B_{i,R})\cdot e(A_i',T_2)$$
$$=e([k]W,[\frac{1}{(\alpha+ID_i')\prod_{j=1}^{r}(\alpha+ID_j)}]h)\cdot e([\frac{ID_i'}{\alpha+ID_i'}]g,[\frac{k}{(\alpha+ID_1)\cdots(\alpha+ID_r)}]h)$$
$$=e(g,h)^{\frac{kr}{(\alpha+ID_i')\prod_{j=1}^{r}(\alpha+ID_j)}+\frac{kID_i'}{(\alpha+ID_i')(\alpha+ID_1)\cdots(\alpha+ID_r)}}$$
$$=e(g,h)^{kq_r}=V^{kq_r}$$

### 2.3 有效性

在动态 Ad hoc 网络中，所有用户的加入和撤离均是动态的。该结构直接将用户身份嵌入算法，无需再给用户分配标签，从而可以用一个实体同时分担群管理员和广播者两个角色，同时用户的动态加入不需要改变原有的信息，尤其是用户的解密密钥不需要再重新计算，这使得方案更加精炼。另外，广播者的加解密密钥及密文的尺寸不随动态用户的数量而改变，只在解密过程中使用一个对运算，且所有手段不依赖用户总数 $m$。因此，本方案能将传输代价和存储代价控制在 $O(r)$ 及 $O(1)$之内。

考虑到密文与密钥的尺寸、时间复杂度及是否动态等因素，表 1 特将本文的身份型动态广播加密方案与以往的广播加密方案 $BGW_2$[12] 和 $NNL_2$[13] 进行了比较，具体如表 1 所列。

表 1 广播加密方案的效率对比

| | 密钥/密文尺寸 | | | 时间复杂度 | | 动态 |
|---|---|---|---|---|---|---|
| | $l_{ek}$ | $l_{dk}$ | $l_C$ | $\tau_{ek}$ | $\tau_{dk}$ | |
| $BGW_2$ | $O(\sqrt{n})$ | $O(\sqrt{n})$ | $O(\sqrt{n})$ | $O(\sqrt{n})$ | $O(\sqrt{n})$ | 否 |
| $NNL_2$ | $O(1)$ | $O(\log^2 n)$ | $O(r)$ | $O(r)$ | $O(\log n)$ | 否 |
| 该方案 | $O(1)$ | $O(1)$ | $O(r)$ | $O(r)$ | $O(r)$ | 是 |

## 3 方案的安全性证明

本节将证明新的身份型广播加密方案在 GDDHE 假设下是抗静态敌手 IND-IN-CPA 安全的。

**定理 1** 对任意的 $n,t$，满足 $0\leqslant t\leqslant n$。若 $(t,n)$-GDDHE 假设成立，则方案是抗静态敌手 IND-IN-CPA 安全的。

证明：假设存在一个动态敌手 $A$ 能攻破 DBE 方案，将表明存在一个算法 $B$ 能解决 $(t,n)$-GDDHE 问题。

设 $B$ 已经获得的双线性映射系统 $C=(p,G_1,G_2,G_T,e(\cdot,\cdot))$及下列元素：

$f(X)=\prod_{i=1}^{t}(X+ID_i^*)$和 $g(X)=\prod_{i=1}^{n-t}(X+ID'_i)$是两个具有非零对儿式异根的 $t$ 阶及 $n-t$ 阶随机多项式，$g_0\in G_1$，$h_0\in G_2$ 是两个生成元，以及 $g_0,[\alpha]g_0,\cdots,[\alpha^{t-1}]g_0,[\alpha\cdot f(\alpha)]g_0,[k\cdot\alpha\cdot f(\alpha)]g_0,h_0,[\alpha]h_0,\cdots,[\alpha^n]h_0,[k\cdot g(\alpha)]h_0,e(g_0,h_0)^{f^2(\alpha)g(\alpha)}$和 $T\in G_T$。若 $T=e(g_0,h_0)^{kf(\alpha)\cdot g(\alpha)}$，则 $B$ 输出 0，否则输出 1。二者的交互游戏运行如下。

初始化：敌手 $A$ 首先输出要挑战的身份集合 $S^*=(ID_1^*,ID_2^*,\cdots,ID_t^*)$，其中收纳了准备挑战的身份。

系统建立：设 $g=[f(\alpha)]g_0$，算法 $B$ 计算下列值 $h=[f(\alpha)\cdot g(\alpha)]h_0$，$W=[a]g=[a\cdot f(\alpha)Ig_0]$，$V=e(g_0,h_0)^{f^2(\alpha)\cdot g(\alpha)}=e(g,h)$，于是 $B$ 能得到公共参数 $ek=(C,h,W,V)$并将其发送给 $A$。

阶段 1 $A$ 进行适应性密钥提取质询 $q_1,\cdots,q_{n_0}$。每一次询问详细如下：

设第 $i$ 次讯问的身份是 $ID_i$，并满足 $ID_i\notin S^*$，$B$ 运行密钥提取算法，计算对应私钥 $d_{ID_i}=(C,ID_i,A_i,B_i)$并回应给 $A$；若 $ID_i\in S^*$，暗示此用户被腐化了，则定义

$$f_i(X)=f(X)/(X+ID_i),i\in(1,\cdots,t)$$
$$A_i'=[ID_i\cdot f_i(\alpha)]g_0=[\frac{ID_i}{\alpha+ID_i}]g\text{ 及}$$
$$B_i'=[f_i(\alpha)\cdot g(\alpha)]h_0=[\frac{1}{\alpha+ID_i}]h$$

而后得到用户私钥 $d_{ID'_i}=(C,ID_i,A_i',B_i')$并发送给 $A$，敌手 $A$ 保留 $d_{ID'_i}$。

挑战：$B$ 运行加密算法得到可以被诚实用户解密的合法头部 $Hdr=(C_1,C_2,\{ID_i,B_i\}_{i=1}^{s})$，其中的 $ID_i\in S^*$ 指被撤销的用户。在给定的 $(t,n)$-GDDHE 状态下，$B$ 计算 $C_1=[k\cdot\alpha\cdot f(\alpha)]g_0=[k]W$ 和 $C_2=[k\cdot g(\alpha)]h_0=[\frac{k}{f(\alpha)}]h=[\frac{k}{(\alpha+ID_1)\cdots(\alpha+ID_t)}]h$。

这样 $B$ 就可以得到

$$K=e(g,h)^{\frac{k}{(\alpha+ID_1)\cdots(\alpha+ID_t)}}=e(g_0,h_0)^{\frac{k\cdot f^2(\alpha)\cdot g(\alpha)}{f(\alpha)}}$$
$$=e(g_0,h_0)^{k\cdot f(\alpha)\cdot g(\alpha)}$$

最后 $B$ 随机选择 $b\in\{0,1\}$。设 $K_b=K$ 而 $K_{1-b}$ 是 $G_T$ 中的随机元素，然后将 $(Hdr,K_0,K_1)$发送给 $A$。

阶段 2 敌手 $A$ 继续进行询问 $q_{s_0+1},\cdots,q_s$，每一次询问类似于阶段 1。

猜测：敌手 $A$ 要输出一个猜测 $b'\in(0,1)$。当 $b=b'$时，宣布敌手在游戏中获胜。

如果 $A$ 能够赢得游戏，则说明算法 $B$ 可以成功地解决 $(t,n)$-GDDHE 问题[11]，故有

$$\mathrm{Adv}_{DBE}^{ind}(t,n,B)\leqslant 2\mathrm{Adv}^{gddhe}(t,n,B)\leqslant\frac{(q+2(n+t+4)+2)^2\cdot(t+n)}{p}$$

**结束语** 本文所提出的基于 Ad hoc 网络的身份型广播加密方案，通过直接引入身份指标，避免了给每个用户分配身份标签的过程，从而可以将群管理员和广播者两个角色用一个实体来扮演，仅需计算一个公共密钥 $ek$，而群管理员密钥 $mk$ 被废除，从而大大缩减了算法结构，提高了运算效率。本方案加解密运算简单，加密阶段不需要对运算，只在解密阶段使用了一个对运算，且利用被撤销用户的身份集合进行加解密运算，使得加解密密钥和密文尺寸不随用户数量而改变，从而进一步将方案的传输代价和存储代价提高至 $O(r)$及 $O(1)$。通过对方案进行严格的安全性证明及正确性和有效性分析，证实了本方案在标准模型下对任意数量无状态用户抗完全的串谋攻击是 IND-IN-CPA 安全的，满足“紧”的安全性。

## 参 考 文 献


[1] Baek J, Safavi-Naini R, Susilo W. Efficient multireceiver identity-based encryption and its application to broadcast encryption [C]// PKC 2005, Lecture Notes in Computer Science 3386. 2005: 380-397

[2] Frodigh M, et al. Wireless ad hoc networking: The art of networking without a network [J]. Ericsson Review, 2000, 4: 248-263

[3] Barbosa M, Farshim P. Efficient identity-based key encapsulation to multiple parties [C]// Crytography and Coding, LEC-

TURE NOTES IN COMPUTER SCIENCE 3796. 2005:428-441
[4] Anton E R, Duarte O C M B. Group key establishment in wireless ad hoc networks [C]// Proc. Workshop en Qualidade de Servicoe Mobilidade. 2002:1-8
[5] Delerablée C. Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys [C]// Advances in Cryptology-ASIA CRYPT. Lecture Notes in Computer Science 4833. 2007:200-215
[6] Asokan N, Ginzboorg P. Key-agreement in ad hoc networks [J]. Compute Communication, 2000, 23(17):1627-1637
[7] Ching Y N, Mu Y, Susilo W. An identity-based broadcast encryption scheme for mobile ad hoc networks [J]. Communications and Information Technology, 2006, 1(01):24-29
[8] Boneh D, Franklin M. Identity Based Encryption from the Weil Pairing [C]//CRYPTO, LNCS 2139. 2001:213-229
[9] Zhang L Y, Hu Y P, Mu N B. Identity-based Broadcast Encryption Protocol for Ad Hoc Networks [J]. IEEE Computer Society, 2009:1619-1623
[10] Boneh D, Franklin M. Identity-based encryption form the weil pairing[C]// Advances in Cryptology-CRYPTO 2001, LNCS 2139. Berlin: Springer-Verlag, 2001:213-229
[11] Delerablée C, Paillier P, David P. Fully Collusion Secure Dynamic Broadcast Encryption with Constant-size Ciphertexts or Decryption Keys [C]// Lecture Notes in Computer Science 4575. Berlin Heidelberg: Springer-Verlag, 2007:39-59
[12] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys [C]//CRYPTO 2005. Lecture Notes in Computer Science 3621. Heidelberg: Springer, 2005:258-275
[13] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers[C]// Kilian J, ed. CRYPTO 2001. LNCS, vol. 2139. Heidelberg: Springer, 2001:41-62

(上接第 45 页)

为信道利用率；$a_{10}$ 为硬件缺陷；$a_{11}$ 为软件漏洞；$a_{12}$ 为信息恢复。

在一个具体网络通信系统风险域中，由 12 个脆性因子组成的信源，在崩溃系数相等时，当这 12 个脆性因子相互统计独立、互不相关，而且等概分布时，达到脆性信源的最大熵值。

$H_0=\log 12=3.12$ 比特/脆性因子

但实际上，由脆性因子组成脆性事件时，脆性因子并非等概出现。设脆性因子之间不是统计独立的，相互之间是有一定的统计依赖关系的。把由这些脆性因子构成的脆性事件近似地看作 $m(m=1,2,3,\cdots)$ 阶 $M$ 信源来处理，分别求出 $m(m=1,2,3,\cdots)$ 阶 $M$ 信源的极限熵

$H_1=2.18$ 比特/脆性因子

$H_2=1.98$ 比特/脆性因子

…

$H_\infty=1.08$ 比特/脆性因子

由此可见：$H_0\geqslant H_1\geqslant H_2\cdots\geqslant H_m$。这表明，脆性信源的极限熵随着记忆长度 $m$ 的增大而减小。脆性事件中脆性因子的脆性联系程度越紧密，每一个脆性因子提供的平均信息量就越小。这就是说，由脆性因子组成的时间序列中，脆性因子之间的脆性联系程度越紧密，脆性信源每发出一个脆性因子提供的平均信息量就越小。此脆性信源的信息剩余度为

$\xi=65.4\%$。

这说明，用这 12 个脆性因子组成的系统脆性事件的脆性风险分析时，在满足概率跟随性的特性时，有 65.4% 的脆性因子是由于必须遵循系统脆性结构而不得不有的，只有 34.6% 的脆性因子是影响系统脆性风险需要加以选择的。由此可知，系统信息剩余度 $\xi$ 越大，脆性因子间的脆性联系程度越紧密，脆性事件就具有较强的抗扰能力。反之，信息剩余度 $\xi$ 越小，脆性因子间的脆性联系程度越小，脆性事件就越容易发生。

如果系统信息剩余度随时间变化不断增加，当干扰要使脆性事件发生时，则可以从系统脆性结构的关联中调整。否则，如果信息剩余度随时间变化不断减小，就可能造成系统脆性事件发生，增加网络通信系统的脆性风险。因此增加或保留必要的、有用的信息剩余度，可以降低网络通信系统的信息脆性风险，实现系统脆性风险的有效控制。

**结束语** 系统脆性模型结构实际上是关于脆性环境结构的，而系统的脆性环境结构主要由脆性事件和脆性因子构成，其中脆性因子又是脆性环境的本质因素。本文在建立的系统脆性结构模型的基础上，应用信息脆性熵给出了系统在整个连续时间域上的信息脆性风险过程，结合极限熵和信息剩余度的概念分析了该方法的可行性。最后将这套分析方法应用到一个具体网络通信系统，对其主脆性因子建立分析模型，分析该系统的脆性状态，并取得了比较满意的结果，从而为下一阶段系统信息脆性风险预测提供了理论依据。

## 参 考 文 献

[1] 韦琦，金鸿章，郭健，等. 基于脆性的复杂系统研究[J]. 系统工程学报，2004，19(3)：326-328
[2] Wei Qi, Jin Hongzhang, Ji Ming. The Research on Brittle Catastrophe of Complex Giant System[C]// IEEE Region 10 Technical Conference on Computers, Communications, Control and Power Engineering(TENCON'02). Beijing, China, October 2002
[3] 张义荣，鲜明，王国玉. 一种基于网络熵的计算机网络攻击效果定量评估方法[J]. 通信学报，2004，25(11)：158-165
[4] 赵冬梅，赵玉清，马建峰. 熵权系数法应用于网络安全的模糊风险评估[J]. 计算机工程，2004，30(18)：21-23
[5] 金鸿章，郭健，韦琦. 基于尖点突变模型对复杂系统脆性问题的研究[J]. 船舶电子工程，2004，24(2)：3-8
[6] 李琦，金鸿章，林德明. 复杂系统的脆性模型及分析方法[J]. 系统工程，2005，23(1)：9-12
[7] 陈为化，江全元，曹一家. 基于风险理论和模糊推理的电压脆弱性评估[J]. 中国电机工程学报，2005，25(24)：20-25
[8] 周勇，刘三阳，杨曙光. 基于交叉熵的通讯网的优化算法[J]. 系统工程与电子技术，2004，26(10)：1471-1475
[9] 姜丹. 信息论与编码[M]. 合肥：中国科学技术大学出版社，2004：89-117
[10] 张连明，陈志刚，邓晓衡. 一种基于信息熵的 Internet 宏观行为模型研究[J]. 计算机工程与应用，2004，19：33-37