信息和通信安全——CCICS'2005

第四届中国信息和通信安全学术会议论文集

杨 波 韩 臻 编

科学出版社
www.sciencep.com

信息和通信安全——CCICS'2005

第四届中国信息和通信安全学术会议论文集

杨 波 韩 臻 编

国家自然科学基金项目(编号:60372046,60273084)
国家重点基础研究发展项目(973)(编号:G1999035801)

科学出版社
北 京

内 容 简 介

本书为第四届中国信息和通信安全学术会议论文集，收录论文73篇，内容涉及信息和通信安全的各个领域，包括密码学、网络安全、信息隐藏与数字水印、电子商务安全等。

本书可供从事信息安全、密码学、计算机、通信、数学等专业的科技人员和高等院校相关专业的师生阅读、参考。

图书在版编目(CIP)数据

信息和通信安全：CCICS'2005 第四届中国信息和通信安全学术会议论文集/杨波，韩臻编. —北京：科学出版社，2005

ISBN 7-03-015244-1

Ⅰ.信… Ⅱ.①杨…②韩… Ⅲ.①计算机网络-安全技术-学术会议-文集②计算机通信-安全技术-学术会议-文集 Ⅳ.①TP393.08-53②TN915.08-53

中国版本图书馆 CIP 数据核字(2005)第 024548 号

责任编辑：鞠丽娜 韩 洁 / 责任校对：柏连海

责任印制：吕春珉 / 封面设计：高海英

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2005 年 4 月第 一 版 开本：787×1092 1/16

2005 年 4 月第一次印刷 印张：25 1/2

印数：1 2 000 字数：587 000

定价：56.00 元

（如有印装质量问题，我社负责调换<双青>）

销售部电话 010-62136131 编辑部电话 010-62138978-8002(BI06)

第四届中国信息和通信安全学术会议
程序委员会

主　席：杨　波（北京交通大学）

副主席：胡予濮（西安电子科技大学）

祝世雄（中国电子科技集团第三十研究所）

委　员：（以姓氏笔画为序）

方　勇（北京电子科技学院）

王丽娜（武汉大学）

王育民（西安电子科技大学）

冯登国（中国科学院信息安全国家重点实验室）

何大可（西南交通大学）

吴文玲（中国科学院软件研究所）

张文政（中国电子科技集团第三十研究所）

张玉清（国家计算机网络入侵防范中心）

张焕国（武汉大学）

李　超（国防科技大学）

李大兴（山东大学）

杨义先（北京邮电大学）

肖德琴（华南农业大学）

陈克非（上海交通大学）

祝跃飞（郑州信息工程大学）

徐茂智（北京大学）

贾春福（南开大学）

郭宝安（清华大学）

曹珍富（上海交通大学）

黄继武（中山大学）

温巧燕（北京邮电大学）

覃中平（华中科技大学）

韩　臻（北京交通大学）

第四届中国信息和通信安全学术会议
组织委员会

主　席：胡予濮

成　员：尹伟谊　杨波　李晖　马华
展文娟　权义宁

此为试读，需要完整PDF请访问：www.ertongbook.com

前　言

第四届中国信息和通信安全学术会议由西安电子科技大学综合业务网关键技术国家重点实验室和信息安全与保密研究所主办，北京电子科技学院、中国电子科技集团第三十研究所国防科技保密通信重点实验室、北京交通大学信息安全体系结构研究中心协办，于2005年5月在西安召开。本书收集了在这次会议上报告的73篇论文，内容涉及密码学、网络安全、信息隐藏与数字水印、电子商务安全等研究课题。这些论文反映了我国当前在信息安全领域的研究动态，也展现出我国信息安全研究与应用的学术水平。

本次会议共收到投稿论文230篇，每篇论文至少由两位专家评审，录用论文73篇，其中55篇全文录用，18篇为短文录用。

我们衷心感谢所有向本次会议投稿的作者对会议的关心与支持。由于受文集篇幅所限，向论文未能被收录的作者表示歉意；感谢程序委员会的所有成员，他们为从众多的稿件中选出更具代表性的论文参加会议交流而做了大量的工作。我们还要感谢会议的主办单位——综合业务网关键技术国家重点实验室和西安电子科技大学信息安全与保密研究所，感谢协办单位——北京电子科技学院、中国电子科技集团第三十研究所国防科技保密通信重点实验室以及北京交通大学信息安全体系结构研究中心，他们在本次会议的筹备和组织中做了很多工作。感谢陕西省委保密委员会办公室、陕西省国家保密局、陕西省密码管理办公室对会议的支持。正是由于各方的共同努力，使本次会议得以顺利进行。最后还要感谢崔海燕硕士和科学出版社责任编辑鞠丽娜女士，他们为会议论文集的出版做了大量细致而繁琐的工作。本论文集的出版得到了科学出版社的大力支持，在此向他们表示衷心的感谢。

目　录

密 码 学

(短文)

网络安全

(短文)

信息隐藏与数字水印

电子商务安全

一种完整的非对称公钥叛逆者追踪方案*

王青龙[1] 杨 波[1,2]

(1 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,中国西安,710071)

(2 北京交通大学信息安全体系结构研究中心,中国北京,100044)

摘 要 利用不经意多项式估值协议,本文提出了一种新的非对称公钥叛逆者追踪方案。与现有的非对称公钥追踪方案相比,本方案能够以完全的黑盒子追踪方式准确地确定出全部叛逆者;具有完善的撤销性,能够撤销任意数量的叛逆者。此外,与已有方案相比本方案显著降低了追踪时的计算量并且有更高的传输效率。

关键词 黑盒子追踪性 可撤销性 不经意多项式估值 追踪叛逆者 非对称性

目前利用网络提供服务的行业越来越多。当这种服务是以广播发送的方式提供时,为了保护数据提供者 DS(Data Supplier)的合法权益,数据需要以加密方式传送,以保证只有授权用户才能使用解密钥获得所需的信息。这里 DS 面临的主要问题是某些授权用户(叛逆者)非法复制自己的或共谋的解密钥给非授权用户(非法者),使得这些非授权用户能够非法获得 DS 提供的信息。为了指控叛逆者,DS 须确定出叛逆者并且能够提出令人信服的证据。由此导致叛逆者追踪方案的出现(当共谋者数量不超过某个预定值时要能确定出至少一个叛逆者)。应用场合包括付费电视系统、网上娱乐服务、网上金融信息的发布、CDROM 的在线发布、软件保护等。

自 Chor 的文章[1]发表后,各种叛逆者方案相继被提出来。文献[5]提出的公钥叛逆者追踪方案解决了文献[1,2]的分组长度随着用户数量的增长而增加的缺点。文献[3,4]进一步提出了具有非对称性的公钥叛逆者追踪方案,即只有用户自己知道解密钥,从而使 DS 可以提供不可否认证据。但文献[3,4]的两个方案的不足之处是都不具备完全的黑盒子追踪能力(不需要打开盗版解码器,而是通过输入输出之间的关系来确定其中包含的解密钥),也没有提到如何撤销叛逆者(使叛逆者拥有的解密钥失去作用,不能再用来解密

* 国家自然科学基金资助项目(60372046);现代通信国家重点实验室基金资助项目(51436040204DZ0102)。

DS 发送的加密数据，但合法用户不受影响）。

本文在文献[3,4]的基础上，提出了一种具备完全黑盒子追踪并且能够撤销任意个叛逆者的非对称公钥叛逆者追踪方案。方案的执行不需要第三方的参与，也不需要使用陷门离散对数。完备的撤销性使得 DS 不仅可撤销叛逆者，也可撤销服务到期的用户，从而可更好地保护数据提供者的利益。

一、不经意多项式估值协议 OPE (oblivious polynominal evaluation)[7]简介

Bob 知道一个多项式 $p(x)$，Alice 知道一个值 a。协议执行结束后，Alice 获得 $p(a)$，但是不能得到 p 的任何信息，同时 Bob 也不能得到有关 a 的信息。协议过程如下：Bob 随机选一个二元多项式 $Q(x,y)$，满足 $Q(0,y)=p(y)$，用来隐藏 $p(y)$；Alice 随机选一元多项式 $s(x)$，满足 $s(0)=a$，用来隐藏 a。最后 Alice 可以通过插值恢复出多项式 $R(x)=Q(x,s(x))$，显然有 $R(0)=Q(0,s(0))=p(s(0))=p(a)$。设 $R(x)$的次数为 z，当 Alice 获得 $R(x)$上 $z+1$ 个点上的值$\{(x_i,R(x_i)),i=1,2,\cdots,z+1\}$后，就能利用 Lagrange 插值求出 $R(x)$。而每对$(x_i,R(x_i))$可通过不经意传输协议[7]OT_n^1(oblivious transfer)的方式来获取。OPE 协议的安全性在文献[7]中已给出了详细说明。

二、方 案 叙 述

1. 系统参数

q 和 p 为两个大素数，且 $q|p-1$。g 是 Z_p 上阶为 q 的本原元。

DS 在 Z_q 上秘密选一个 k 次多项式 $f_1(x)=\sum_{i=0}^{k}a_ix^i$。DS 再任选 $x_0\in Z_q^*$，$\{h_1,h_2,\cdots,h_k\}\subset Z_q\backslash\{0\}$，$\Omega=\{m_1,m_2,\cdots,m_k\}\subset Z_q\backslash(\{x_0\}\cup\{0\})$。设 $f(x,y)=f_1(x)+by,b\in Z_q^*$ 由 DS 秘密选取。又设 Φ 为已注册用户的集合，$\Phi\subseteq Z_q\backslash(\{x_0\}\cup\{0\}\cup\Omega)$。令

$$\Delta=\{(m_1,g^{h_1}),(m_2,g^{h_2}),\cdots,(m_k,g^{h_k})\}$$

DS 公开 g、p、q、Δ 和公开钥

$$e=(g,g^{f_1(x_0)},g^b,x_0,(x_1,g^{f_1(x_1)}),\cdots,(x_k,g^{f_1(x_k)}))$$

其中$\{x_1,x_2,\cdots,x_k\}\subset Z_q\backslash(\{0\}\cup\{x_0\}\cup\Phi)$。除非特别说明，本方案的所有算术运算都在 Z_p 上。

2. 注册过程

1）当用户 $i[i\in Z_q\backslash(\{0\}\cup\{x_0\}\cup\Omega\cup\Phi)]$注册时，$i$ 秘密选一个数 $\alpha_i\in Z_q^*$，DS 秘密选一个数 $v\in Z_q^*$。使用 OPE 协议，用户得到

$$d=v(f_1(i)+b\cdot\alpha_i)$$

2）用户发送 $pk_i\parallel sign_{sk_i}(g^d\parallel g^{\alpha_i})$给 DS($pk_i$、$sk_i$ 为用户的公开钥和秘密钥，$sign$ 为可恢复消息的签字）。

此为试读，需要完整PDF请访问：www.ertongbook.com

3) DS 恢复出 $g^d \| g^{\alpha_i}$，并验证 $g^d=(g^{\alpha_i})^{vb} \cdot g^{vf_1(i)}$，若相等将 v 发给用户，将 Φ 更新为 $\Phi \cup \{i\}$。

4) 令 $m_0=i, h_0=f_1(i)$，DS 计算 $B_i=\prod_{j=0}^{k}(g^{h_j})^{\lambda_j}, \lambda_j=\prod_{0\leqslant l\neq j\leqslant k}\frac{m_l}{m_l-m_j}$，并记录购单

$$text = i \| B_i \| pk_i \| sign_{sk_i}(g^d \| g^{\alpha_i})$$

5) 用户 i 的解密钥为

$$d_i = (i, \alpha_i, d/v) = (i, \alpha_i, f_1(i) + \alpha_i b) = (i, \alpha_i, f(i, \alpha_i))$$

3. 加密算法

设 M 为待加密消息，DS 任选 $r \in Z_q^*$，$s \in Z_q^*$，则 DS 发送的数据分组为 $(g^r, s \cdot g^{rf_1(x_0)}, g^{rb}, x_0, (x_1, g^{rf_1(x_1)}), \cdots, (x_k, g^{rf_1(x_k)}), E_s(M)) = (H, E_s(M))$（其中 H 称为分组头，E 为对称加密算法）。

4. 解密算法

用户 i 收到分组数据后，利用自己的解密钥 d_i 执行以下几步：

1) $$\frac{(g^r)^{f(i,\alpha_i)}}{(g^{rb})^{\alpha_i}}=\frac{g^{rf_1(i)} \cdot g^{rb\alpha_i}}{g^{\alpha_i rb}}=g^{rf_1(i)}$$

2) 令 $x_{k+1}=i$，利用 Lagrange 插值法计算

$$g^{rf_1(x_0)} = \prod_{t=1}^{k+1}(g^{rf_1(x_t)})^{\lambda_t}, t \in \{x_1, x_2, \cdots, x_{k+1}\}$$

其中 $\lambda_t=\prod_{1\leqslant j\neq t\leqslant k+1}\frac{x_j-x_0}{x_j-x_t}$ 为 Lagrange 插值系数。

3) 计算

$$s = \frac{s \cdot g^{rf_1(x_0)}}{g^{rf_1(x_0)}}$$

4) 计算 $D_s(E_s(M))=M$，得到明文。

5. 追踪算法

设盗版解码器中包含 $l(\leqslant k)$ 个解密钥 $\{d_{i_1}, d_{i_2}, \cdots, d_{i_l}\}=\Lambda$。叛逆者的策略是每次解密时随机选用 Λ 中的一个解密钥 $d_i, i \in \{i_1, i_2, \cdots, i_l\}$（由于本方案的公开钥中用 $g^{f_1(x_0)}$ 而不是用 $g^{\alpha_0}=g^{f_1(0)}$ 隐藏 s，所以文献[4]中 Claim 1 提到的共谋方式在这里不适用），为了确定解密钥，DS 执行以下步骤：

1) 往盗版解码器中输入数据

$$(g, A, g^b, 0, (m_1, g^{h_1}), (m_2, g^{h_2}), \cdots, (m_k, g^{h_k}))$$

2) 设解码器使用的解密钥为

$$d_i = (i, \alpha_i, f(i, \alpha_i)), i \in \{i_1, i_2, \cdots, i_l\}$$

按照解密算法解码器输出 $C_i=A/B_i$。详细过程如下：

$$\frac{(g)^{f(i,\alpha_i)}}{(g^b)^{\alpha_i}} = \frac{g^{f_1(i)} \cdot g^{b\alpha_i}}{g^{\alpha_i b}} = g^{f_1(i)}$$

令 $m_0=i, h_0=f_1(i)$，解码器计算

$$\prod_{j=0}^{k}(g^{h_j})^{\lambda_j}=B_i,\lambda_j=\prod_{0\leqslant l\neq j\leqslant k}\frac{m_l}{m_l-m_j}$$

解码器输出

$$\frac{A}{B_i}=C_i$$

由此可得 $B_i=A/C_i$。通过与保存的 *text* 相比较，找到与 B_i 相对应的 *text*，即可确定叛逆者。由于一次输入就能确定出一个叛逆者，所以经过有限次输入输出后即可确定出全部的叛逆者。

6. 撤销算法

设 $\Lambda_\gamma=\{i_1,i_2,\cdots,i_\gamma\},\gamma\leqslant k$，是由叛逆者组成的集合。DS 用 $\{(i_1,g^{f_1(i_1)}),\cdots,(i_\gamma,g^{f_1(i_\gamma)})\}$ 替换公开钥 e 中的任意 γ 个 $\{(x_{j_1},g^{f_1(x_{j_1})}),\cdots,(x_{j_\gamma},g^{f_1(j_\gamma)})\},\{j_1,j_2,\cdots,j_\gamma\}\subseteq\{1,2,\cdots,k\}$，这时对合法用户而言不会受到任何影响，但对叛逆者而言因其持有的份额被包含在发送的分组中，所以不能获得解密所需的 $k+1$ 个份额，即达到撤销叛逆者的目的。

7. 更新过程

当撤销的叛逆者数量达到 k 时，执行密钥更新过程。DS 任选一 $u\in Z_q\backslash\{0\}$，发送 $(g^r,u\cdot g^{rf_1(x_0)},g^{rb},(i_1,g^{rf_1(i_1)}),\cdots,(i_\gamma,g^{rf_1(i_\gamma)}))$，属于 $\Phi\backslash\Lambda_\gamma$ 中的合法用户按照解密算法得到 u，把自己的解密钥 $(i,\alpha_i,f(i,\alpha_i))$ 更新为 $(i,u\alpha_i,uf(i,\alpha_i))$，而叛逆者不能得到 u，所以不能更新其解密钥。相应地，DS 将发送的分组数据更新为

$$e'=(g^r,s\cdot(g^{rf_1(x_0)})^u,g^{rb},(x_1,(g^{rf_1(x_1)})^u),\cdots,(x_k,(g^{rf_1(x_k)})^u),E_s(M))=(H,E_s(M))$$

就可以保证用户在密钥更新后按照解密算法仍能正确解密。经过这样更新后，DS 可继续撤销另外 k 个叛逆者。根据需要 DS 可无限次重复更新过程。

(1) 更新后的追踪

如果盗版解码器中包含的是更新后的解密钥，DS 在追踪时只需将输入盗版解码器的数据更新为

$$(g,A,g^b,0,(m_1,(g^{h(m_1)})^u),(m_2,(g^{h(m_2)})^u),\cdots,(m_k,(g^{h(m_k)})^u))$$

假定盗版解码器中的解密钥为 $(i,u\alpha_i,uf(i,\alpha_i))$，则按照上述追踪算法其输出数据 $C=A/B_i^u$，由此可得 $B_i=(A/C)^{u^{-1}}$，经过与 text 比较确定出叛逆者。

(2) 更新后的撤销

设 $\Lambda'_\gamma=\{i_1,i_2,\cdots,i_\gamma\},\gamma\leqslant k$ 为更新密钥后的叛逆者集合，DS 用 $\{(i_1,g^{uf_1(i_1)}),\cdots,(i_\gamma,g^{uf_1(i_\gamma)})\}$ 取代 e' 中的任意 γ 个 $\{(x_{j_1},g^{uf_1(x_{j_1})},\cdots,(x_{j_\gamma},g^{uf_1(x_{j_\gamma})})\},\{j_1,j_2,\cdots,j_\gamma\}\subseteq\{1,2,\cdots,k\}$，即可撤销叛逆者。

三、安全分析

设用户拥有的信息为：公开钥 e，足够多的已发送的分组头

$$H_i=(g^{r_i},s_i\cdot g^{r_if_1(x_0)},g^{r_ib},x_0,(x_1,g^{r_if_1(x_1)}),\cdots,(x_k,g^{r_if_1(x_k)}))$$

及对应的 s_i，则用户从一个新的分组头

$$H = (g^r, s \cdot g^{rf_1(x_0)}, g^{rb}, x_0, (x_1, g^{rf_1(x_1)}), \cdots, (x_k, g^{rf_1(x_k)}))$$

中求 s 的计算复杂度相当于破译 ElGamal 加密体制下的密文(证明参见文献[6]定理14)。

k 个用户 $I=\{i_1, i_2, \cdots, i_k\}$ 利用他们的解密钥 $(l, \alpha_l, f(l, \alpha_l)), l \in I$ 和公开钥 e 构造出另外一个满足 $j \notin I, \alpha_j \in Z_q^*$ 的解密钥 $(j, \alpha_j, f(j, \alpha_j))$,它的计算复杂性相等于求解离散对数困难问题(证明参见文献[3]中的引理4)。

由 OPE 协议的性质可知:

1) 若用户在执行 OPE 时使用一个与其所选 α 不同的 α',则用户不能通过 DS 的验证。

2) DS 不能陷害一个诚实的用户(证明略)。

如果 DDH 问题是困难的,则盗版解码器不能识别输入数据是正常数据还是用来进行追踪的数据(证明参见文献[3]中的引理5)。

四、性能比较

为了更好地说明本方案的性能,表1列出了文中方案与现有非对称公钥叛逆者追踪方案的对比结果。

表1 文中方案与文献[3,4]的比较

	OPE 使用次数	分组长度	撤销性	追踪方式	确定一个叛逆者所需的计算量	解密密钥长度
文献[3]	2	$2k+2$	不具备	直接打开*		3
文献[4]	1	$2k+2$	不具备	部分黑盒子	$2k$ 次输入输出	3
本方案	1	$k+4$	能撤销任意叛逆者	完全黑盒子	一次输入输出	3

* 文献[3]中提出的黑盒子追踪实际上是黑盒子确认方式。k 为共谋门限值。

五、结　论

本文提出的非对称公钥叛逆者追踪方案有效地解决了现有方案中存在的追踪性和撤销性不足的问题,以完全黑盒子追踪的方式快速、准确地确定出全部的叛逆者。完备的撤销性为数据提供者提供了更好的保护,同时传输效率得到显著改善。

附　录

当解密过程中要用到 Lagrange 插值法时,对于叛逆者能否通过共谋构造出与其所持有的解密钥不同的新的解密钥,Yuji Watanabe 在其文献[3]的 3.3 节中写到:"On the other hand, it seems not to be applicable to the threshold-decryption-based scheme such as…, since a session key can be computed by combining $k+1$ shares using the Lagrange interpolation, and simple convex combination of the personal keys of k traitors does not lead to the pirate key."。

但是文献[4]中的 Claim 1 提到一种破解方式(详细过程参见文献[4])。分析其破解成功的原因,主要因为文献[3]中使用了所选多项式在零点的函数值来隐藏会话密钥,由于函数在零点的值等于函数的常数项值,在使用共谋构造的解密钥时,可通过常数项求得解密时所需的 Lagrange 插值系数,所以只要不用常数项来隐藏会话密钥,这种破解方式就失去了作用。

参 考 文 献

1 Chor B, Fiat A, Naor M. Tracing Traitors Advances in Cryptology. In: Proc. of CRYPTO'94. Berlin:Springer-Verlag, 1994, 257～270

2 Pfitzmann B. Trails of Traced Traitors. In: Proc. of Information Hiding'96. Berlin : Springer-Verlag, 1996, 49～64

3 Yuji Watanabe, Goichiro Hanaoka, Hideki. Efficient Asymmetric Public-key Traitor Tracing without Trusted Agents. In: Proc. of CT-RSA 2001. Berlin: Springer-Verlag, 2001, 392～407

4 Aggelos Kiayias, Moti Yung. Breaking and Repairing Asymmetric Public-key Traitor Tracing. In: ACM. Digital Rights Management: revised papers, 2002. Berlin: Springer-Verlag, 2003,32～50

5 Boneh D, Franklin M. An Efficient Public Key Traitor Tracing Scheme. In: Proc. of CRYPTO'99. Berlin : Springer-Verlag, 1999,338～353

6 Kurosawa K, Desmedt Y. Optimum Traitor Tracing and Asymmetric Scheme. In: Proc. of EUROCRYPTO'98. Berlin : Springer-Verlag, 1998,145～157

7 Naor M and Pinkas B. Oblivious Transfer and Polynomial Evaluation. In: Proc. of STOC'99. 1999, 245～254

A Complete Asymmetric Public-key Traitor Tracing Scheme

Qinglong Wang[1] Bo Yang[1,2]

(1 The Ministry of Edu. Key Lab. of Computer Network and Info. Security, Xidian Univ, Xi'an,PRC,710071)

(2 Research Center of Information Security Architecture, Beijing Jiaotong University, Beijing,PRC,100044)

Abstract Based on oblivious polynomial evaluation, this paper presents a new asymmetric public-key traitor tracing scheme. Compared with the previous schemes, our scheme can accurately determine a or all traitor(s) from an illegal decoder by full black-box tracing; and revocate unlimited traitors. Moreover, our scheme greatly decreases the computational cost of tracing a traitor and has a higher transmission efficiency compared with those of available.

Keywords Black-box tracing Revocation Oblivious polynomial evaluation Tracing traitors Asymmetry

Jacobi 序列的 pattern 分布*

王劲松　戚文峰

（解放军信息工程大学信息工程学院应用数学系，中国郑州，450002）

（E-mail：wenfeng.qi@263.net）

摘　要　Jacobi 序列是一类重要的伪随机序列，本文研究 Jacobi 序列的 pattern 分布，较精确刻画了 3-pattern 和 4-pattern 分布，并分析了一般的 s-pattern 分布性质，给出了一个可以用来估计其 pattern 分布的算法。利用此算法得到的结果表明在绝大多数情况下，当 s 相对于 $\log_2 pq$ 较小时，Jacobi 序列的 pattern 分布是相当理想的。

关键词　Jacobi 序列　pattern 分布　孪生素数序列

一、引　　言

Jacobi 序列是一类重要的伪随机序列，它具有良好的自相关性质和较大的线性复杂度[1~3]。下面给出 Jacobi 序列的定义。

定义 1[1]　设 p 和 q 是两个不同的奇素数，则 pq 型 Jacobi 序列 $\boldsymbol{J}_{p,q}=(J_{p,q}(0),J_{p,q}(1),\cdots)$ 定义为

$$J_{p,q}(i)=\begin{cases}0, & \text{若 } i=0 \bmod pq\\ 1, & \text{若 } i=0 \bmod p \text{ 且 } i\neq 0 \bmod q\\ 0, & \text{若 } i\neq 0 \bmod p \text{ 且 } i=0 \bmod q\\ \sigma\left(\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\right), & \text{若 } (i,pq)=1\end{cases}$$

其中 $\left(\frac{i}{p}\right)$ 是 Legendre 符号，$\sigma(1)=0,\sigma(-1)=1$。

注 1　pq 型 Jacobi 序列的周期为 pq。

定义 2　设 $\boldsymbol{a}=(a_0,a_1,\cdots)$ 是周期为 T 的二元序列，$r_0,r_1,\cdots,r_{s-1}$ 是 s 个两两不同的非负整数，称 $(a_{r_0},a_{r_1},\cdots,a_{r_{s-1}})$ 为序列 $\boldsymbol{a}$ 的一个 pattern[4]。

对任意 $(b_0,b_1,\cdots,b_{s-1})\in F_2^s$，定义 $WH(b_0,b_1,\cdots,b_{s-1})$ 为向量 $(b_0,b_1,\cdots,b_{s-1})$ 的重量，即 $b_0,b_1,\cdots,b_{s-1}$ 中“1”的个数。

若 $\boldsymbol{a}=(a_0,a_1,\cdots)$ 为 Jacobi 序列，设

$$C_0=\{j\mid a_j=0,0\leqslant j\leqslant pq-1\},\ C_1=\{j\mid a_j=1,0\leqslant j\leqslant pq-1\}$$

对 $b_0,b_1,\cdots,b_{s-1}\in\{0,1\}$ 和两两不同的 $r_0,r_1,\cdots,r_{s-1}\in Z_{pq}=\{0,1,\cdots,pq-1\}$，记

$$C_{b_k}+r_k=\{j+r_k\mid j\in C_{b_k}\},\ k=0,1,\cdots,s-1$$

* 全国优秀博士学位论文专项基金项目（200060）和国家自然科学基金项目（60373092）。

又设

$$D_{b_0,b_1,\cdots,b_{s-1}}(r_0,r_1,\cdots,r_{s-1})=\bigcap_{k=0}^{s-1}(C_{b_k}+r_k)$$

即

$$D_{b_0,b_1,\cdots,b_{s-1}}(r_0,r_1,\cdots,r_{s-1})=\{k\mid(a_{r_0+k},a_{r_1+k},\cdots,a_{r_{s-1}+k})=(b_0,b_1,\cdots,b_{s-1})\}$$

设 $d_{b_0,b_1,\cdots,b_{s-1}}(r_0,r_1,\cdots,r_{s-1})=|D_{b_0,b_1,\cdots,b_{s-1}}(r_0,r_1,\cdots,r_{s-1})|$，显然 $d_{b_0,b_1,\cdots,b_{s-1}}(r_0,r_1,\cdots,r_{s-1})$就是数组$(b_0,b_1,\cdots,b_{s-1})$在序列 $\boldsymbol{a}$ 的一个周期中出现的次数。Golomb[5]分析了 m-序列一些特殊 pattern 的分布，如游程和子序列的分布。丁存生[4]研究了 Legendre 序列的 s-pattern 分布，得到了当 s 相对 $\log_2 p$ 较小时，Legendre 序列的 s-pattern 分布是相当理想的。

不妨假设 $p<q,l=q-p>0$，那么 Jacobi 序列的一个周期中“0”出现$(pq+1-l)/2$次，“1”出现$(pq-1+l)/2$次。文献[2]指出当 $l\equiv 2 \bmod 4$ 时，Jacobi 序列的自相关值为 $pq,l-3,1-l,-1$；而当 $l\equiv 0 \bmod 4$ 时 Jacobi 序列的自相关值为 pq、$l-3$、$1-l$、-3、1。由此可见，l 越小 Jacobi 序列的自相关性质越好，特别地，$l=2$ 的 Jacobi 序列又叫做孪生素数序列，它具有理想自相关性质。Jacobi 序列的线性复杂度很高，Dai，Gong 和 Song[1]证明了 Jacobi 序列的线性复杂度大于等于$(p-1)\cdot(q-1)/2$，并给出了 Jacobi 序列的迹表示。

二、两个引理

周期为 pq 的 Jacobi 序列是由两条周期分别为 p 和 q 的 Legendre 序列进行模 2 加后并对某些特殊位置上的值修改后得到的[2]。由于 Z_{pq}中两两不等的数 $r_0,r_1,\cdots,r_{s-1} \bmod p$ 或 $\bmod q$ 可能相等，所以必须对 $r_0,r_1,\cdots,r_{s-1} \bmod p$ 和 $\bmod q$ 的不同情况讨论。

设 $r_0,r_1,\cdots,r_{s-1}\in Z_{pq}$且两两不同，$(b_0,b_1,\cdots,b_{s-1})\in F_2^s$。为了刻画 Jacobi 序列的 s-pattern 分布，使用下面的函数：

$$G(x)=\frac{1}{2^s}\prod_{j=0}^{s-1}\left[1+(-1)^{b_j}\left(\frac{x+r_j}{p}\right)\left(\frac{x+r_j}{q}\right)+(-1)^{b_j}\left(\left(\frac{x+r_j}{p}\right)^2-\left(\frac{x+r_j}{q}\right)^2\right)\right]$$

由 $G(x)$的定义可知，

1）若 $x\notin\{-r_0,-r_1,\cdots,-r_{s-1}\}$，则 $G(x)\neq 0$ 当且仅当 $x\in D_{b_0,b_1,\cdots,b_{s-1}}(r_0,r_1,\cdots,r_{s-1})$。

2）若 $x\in\{-r_0,-r_1,\cdots,-r_{s-1}\}$，则 $|G(x)|\leqslant 1/2$。

因此，

$$|d_{b_0,b_1,\cdots,b_{s-1}}(r_0,r_1,\cdots,r_{s-1})-\sum_{x=0}^{pq-1}G(x)|\leqslant s/2$$

下面通过计算$\sum_{x=0}^{pq-1}G(x)$来估计 Jacobi 序列的 pattern 分布。

又因为

$$G(x)=\frac{1}{2^s}\prod_{j=0}^{s-1}\left[1+(-1)^{b_j}\left(\frac{x+r_j}{p}\right)\left(\frac{x+r_j}{q}\right)+(-1)^{b_j}\left(\left(\frac{x+r_j}{p}\right)^2-\left(\frac{x+r_j}{q}\right)^2\right)\right]$$

$$=\sum_{(\beta_0,\beta_1,\cdots,\beta_{s-1})\in F_2^s}f(\beta_0,\beta_1,\cdots,\beta_{s-1},x)$$

此为试读，需要完整PDF请访问：www.ertongbook.com