一种基于模运算和扩展欧几里得定理的喷泉码

朱文杰[1,2],易本顺[1,2],甘良才[1],姚渭箐[1,2]
(1. 武汉大学电子信息学院,湖北武汉 430072;2. 武汉大学深圳研究院,广东深圳 518000)

摘 要: 针对中国剩余定理在模运算喷泉码译码过程中的固有不足,本文提出一种全新的基于扩展欧几里德定理的译码算法.该算法采用合并线性同余方程组,避免分解因子非互质情况下求解乘率因子失败的问题.模运算喷泉码将信息数据编码为自然数分解因子和相对应的模余数的数据包,接收方只要获取一定数目的编码数据包就能成功解码.基于扩展欧几里得定理的译码算法扩展了模运算喷泉码的分解因子范围,提高了编译码效率.本文通过理论分析和数值仿真证实了这种编译码算法的可行性.

关键词: 喷泉码;中国剩余定理;扩展欧几里德定理;余数变换码;线性同余方程
中图分类号: TN911.2 **文献标识码:** A **文章编号:** 0372-2112 (2017)04-0855-08
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.04.013

Novel Fountain Codes Based on Modulo and Extended Euclidean

ZHU Wen-jie[1,2], YI Ben-shun[1,2], GAN Liang-cai[1], YAO Wei-qing[1,2]
(1. *School of Electronic Information, Wuhan University, Wuhan, Hubei* 430072, *China*;
2. *Shenzhen Institute of Wuhan University, Shenzhen, Guangdong* 518000, *China*)

Abstract: Aiming at the intrinsic problems of Chinese Remainder Theorem in fountain decoding process with modular arithmetic, this paper proposes a decoding algorithm based on extended Euclidean theorem. The linear congruence equations are merged in the extended Euclidean decoding algorithm, which avoids the failure of solving the rate factor when the decomposition factors are non-coprime. In the modular arithmetic fountain encoding process, the original packet is continuously decomposed by the factor, which is randomly selected from the natural number, into the encoded packets consisting of the residues and the factors. When a certain amount of packets are received, it can be achieved to decode successfully. The codec efficiency has been improved as the algorithm has extended the range of the modular arithmetic factor. Through theoretical analysis and numerical simulation, the effectiveness of this decoding algorithm of modular arithmetic fountain code has been proved.

Key words: fountain codes; Chinese remainder theorem; extended Euclidean; remainder transform codes; linear congruence equations

1 引言

基于反馈重传的传输控制协议TCP(Transmission Control Protocol)在传输距离太长的时候性能很差,因为长距离导致发送方等待反馈确认信息时的空闲时间太长.2002年,Luby提出了第一种实用数字喷泉码——LT码[1],其基本思想是,将构成原始文件的信息数据像喷泉涌水一样源源不断地转化为编码数据包,接收方只要得到编码分组流中的若干个分组就可以解码成功.LT码是第一类码率不受限的实用信道编码,即其码率不需要事先确定[2],由于具有较低的编译码时间复杂度,数字喷泉码也日益受到产业界的关注,获得了越来越多的应用.在无线移动互联网、数字电视广播网、水声通信、数字存储等领域具有广泛的应用前景[3~8].

文献[9]提出一类基于模运算的新的喷泉码并提出具体的实现方案.该方案是一种基于素数模运算分解机制的余数变换码,将信息数据编码为包含质数分解因子及对应的模余数的编码包,接收端从接受包中得到分解因子和模余数后,使用中国剩余定理(Chinese Remainder Theorem)为基础的译码算法在特定的构造比

收稿日期:2015-05-12;修回日期:2016-05-22;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61371125,No.61072041);深圳市基础研究项目(No.JCYJ20150630153917254)

率上可以以 100% 的概率恢复原始数据. 使用中国剩余定理进行译码恢复要求传输分组的分解因子为互质的素数,这限制了模运算喷泉码传输编码分解因子的选择范围. 文献[10]研究了一种基于扩展欧几里德算法改进的二进制 QR(Quick Response)编码算法,该算法主要是应用余数译码性质有效计算错误定位多项式,提升译码效率;文献[11]研究了一种能够适用于 RS(Reed-Solomon Codes)及 BCH(Bose Ray-Chaudhuri Hocquenghem)码的改进扩展欧几里德译码算法,改进算法采用固定迭代而不是进行度的计算或者比较,从而解决剩余多项式的度低于一定门限时候译码终止问题;文献[12]提出一种基于扩展欧几里德定理的可靠信息 RS 译码算法,由于可靠信息被用于标明接收码字中删除位置,该算法可以使用归一化最小距离解码,降低译码复杂度. 文献[13]通过虚拟化扩展交织 RS 码及重构多序列变长移位寄存器到等长,实现归一化欧几里得算法解码.

本文提出以扩展欧几里得算法为基础的新的模运算喷泉码译码算法,把编码分组分解因子从互质素数扩展到非互质领域,扩展其应用范围和编译码效率.

2 中国剩余定理及模运算喷泉码原理

中国剩余定理[14~17]是我国古代求解一次同余式的一般方法,是数论中一个重要定理,又称为孙子定理.

2.1 中国剩余定理

设 $m_1,m_2,\cdots,m_k$ 为 k 个两两互素的正整数,$m=m_1*m_2*\cdots*m_k$,$r_1,r_2,\cdots,r_k$ 为一个正整数 x 分别除以 $m_1,m_2,\cdots,m_k$ 所得的余数.

以上描述可以表达为

$$\begin{cases} x=r_1(\bmod m_1) \\ x=r_2(\bmod m_2) \\ \cdots \\ x=r_k(\bmod m_k) \end{cases} \tag{1}$$

中国剩余定理说明式(1)有多个解,其最小正整数解为

$$x=(M_1M_1'r_1+M_2M_2'r_2+\cdots+M_kM_k'r_k)\bmod m \tag{2}$$

式(2)中相关参数说明如下:

$$M_1=m/m_i,(i=1,2,\cdots,k)$$

M_i' 为 M_i 模 m_i 的逆元,即:

$$M_i'M_i=1(\bmod m_i),(i=1,2,\cdots,k) \tag{3}$$

2.2 异或运算喷泉码原理

喷泉码编码过程如图 1 所示.

(1)根据度分布函数 $\rho(d)$ 随机地选取编码分组的度数 d;

(2)从预编码之后的数据分组中随机地选取 d 个不同的输入符号;

(3)将这 d 个不同的输入符号分组进行异或和,便生成编码分组;

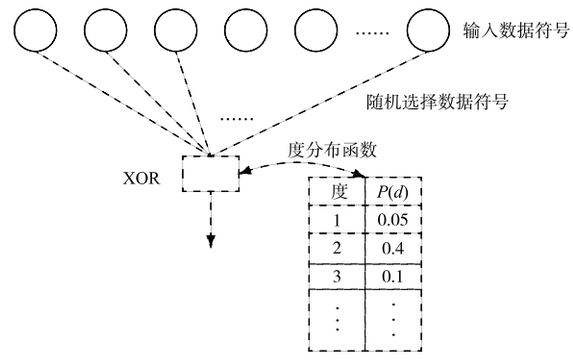


图1 喷泉码编码过程

从喷泉码编码过程可以看到,数字喷泉码是基于度分布和异或运算的构造编码而成. 解码方从发送方源源不断的编码分组中收到一定数目的接收数据就可以解码成功.

2.3 模运算喷泉码原理

为方便理解模运算喷泉码编译码过程,图 2 说明原始数据 23 如何进行模运算编译码的过程,通过互质素数 2、3、5、7、11、13、17、19 作为编码分组的分解因子,依次进行求余运算,将生成的余数和对应的分解因子作为编码分组进行发送. 接收端从收到的接收分组中提取出分解因子和对应余数,采用中国剩余定理,就可以以 100% 的概率恢复译码值 23.

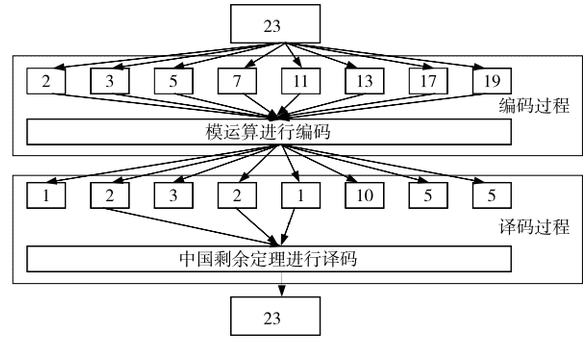


图2 基于中国剩余定理喷泉码编译码示意图

3 扩展欧几里得算法及非互质模运算喷泉码译码算法

从 2.1 节介绍中可以看到,中国剩余定理对于编码分解因子 $m_1,m_2,\cdots,m_k$ 为两两互质的要求,使得基于模运算的喷泉码分编码分解因子范围大大缩小,从而限制了模运算喷泉码编解码分解因子选择的范围,降低了其应用范围,本文提出一种在分解因子 $m_1,m_2,\cdots,m_k$ 不一定为两两互质情况下,基于扩展欧几里得定理对模运算喷泉码进行译码的新算法.

3.1 扩展欧几里得算法

扩展欧几里德算法是欧几里得算法在功能上的扩展,扩展欧几里得定理[18]可以在求得两个整数 a,b 的最大公约数 $\gcd(a,b)$ 的同时,求出存在整数对 x,y 使得它们满足贝祖等式:

$$\gcd(a,b)=a*x+b*y \tag{4}$$

运用欧几里得算法可以求出两个数 a,b 的最大公约数 $\gcd(a,b)$,进行回退运算[19]可以求出式(4)中 x,y 值,此性质为求解线性同余方程提供理论基础.

3.2 用扩展欧几里得算法求解模线性同余方程

设有线性同余方程 $a*x=b(\mathrm{mod}n)$,表示 $a*x$ 模 n,余数为 b,需要对于未知数 x 求解,当且仅当 a 与 n 的最大公约数 $\gcd(a,n)$ 能被 b 整除时候,方程有解且有 $\gcd(a,n)$ 个解.

根据扩展欧几里得原理,求解方程 $a*x=b(\mathrm{mod}\ n)$ 相当于求解方程:

$$a*x+n*y=b \tag{5}$$

设 $d=\gcd(a,n)$,假如整数 x 和 y,满足式(6):

$$d=a*x+n*y \tag{6}$$

由式(4)可知用扩展欧几里德定理可以求出式(6)整数 x 与 y 的值,假设为 x_0 和 y_0,则有方程:

$$a*x_0+n*y_0=d \tag{7}$$

如果 d 可以整除 b,则方程式(7)两边乘以 b/d,得到:

$$a*x_0*b/d+n*y_0*b/d=b \tag{8}$$

所以 $x=x_0*b/d,y=y_0*b/d$ 为 $a*x+n*y=b$ 的一个解,$x=x_0*b/d$ 为 $a*x=b(\mathrm{mod}\ n)$ 的解,由此可以推出 $a*x=b(\mathrm{mod}\ n)$ 的一个解为 $x=x_0*(b/d)\bmod n$,且方程的 d 个解分别为:

$$x_i=(x+i*n/d),(i=0,1,2,\cdots,d-1) \tag{9}$$

设 $k=x_0*(b/d),t=n/d$

方程 $a*x=b(\mathrm{mod}\ n)$ 的最小非负整数解为:

$$(k+t)\%t \tag{10}$$

求解模线性方程的算法为分解因子非互质的喷泉码译码算法提供了理论基础.

3.3 编码分解因子非互质情况下模运算喷泉码解码算法

对于模运算喷泉码分解因子非互质的情况,假如原始数据为 Dat,编码分解因子为 $m_1,m_2,m_3,\cdots,m_i$,模运算对应的余数为 $r_1,r_2,r_3,\cdots,r_i$,在 $m_1,m_2,m_3,\cdots,m_i$ 不为互质情况下如何求解 Dat? 将问题可归纳为下列数学等式:

$$\begin{cases}\mathrm{Dat}=r_1(\mathrm{mod}\ m_1)\\ \mathrm{Dat}=r_2(\mathrm{mod}\ m_2)\\ \cdots\\ \mathrm{Dat}=r_k(\mathrm{mod}\ m_k)\end{cases} \tag{11}$$

问题总结为:在给出 r_i,m_i 的值,且 $m_1,m_2,m_3,\cdots,m_i$ 两两之间不一定互质,如何求 Dat 的值?

解:采用合并同余方程算法,以合并前两个方程说明此算法.

$$\begin{cases}\mathrm{Dat}=r_1+m_1*k_1\\ \mathrm{Dat}=r_2+m_2*k_2\end{cases} \tag{12}$$

即

$$r_1+m_1*k_1=r_2+m_2*k_2 \tag{13}$$

令 $d=\gcd(m_1,m_2)$,将式(12)左右两边同时除以 d 并移项得:

$$m_1*k_1/d-(r_2-r_1)/d=(m_2/d)*k_2 \tag{14}$$

由式(14)可以推出:

$$m_1*k_1/d-(r_2-r_1)/d=0(\mathrm{mod}\ m_2/d) \tag{15}$$

$$m_1*k_1=(r_2-r_1)(\mathrm{mod}\ m_2/d) \tag{16}$$

从式(9)易知式(16)中 k_1 有多个解,设 K'为所有解中的最小非负整数解,则 K'满足:

$$k_1=K'+(m_2/d)*C' \tag{17}$$

式(17)中 C'为某一整数. 将式(17)代入式(12)可以推出:

$$\mathrm{Dat}=r_1+m_1*K'+(m_1*m_2/d)*C \tag{18}$$

由式(18)可以推出:

$$\mathrm{Dat}=(r_1+m_1*K')(\mathrm{mod}(m_1*m_2/d)) \tag{19}$$

由式(13)可以推出:

$$m_1*k_1=(r_2-r_1)(\mathrm{mod}\ m_2) \tag{20}$$

根据前面 3.2 小节可知由模线性方程即可解出 k_1,得到 k_1 值后,便可通过以下运算得出 K'.

由式(17)得:

$$K'=k_1(\mathrm{mod}\ m_2/d) \tag{21}$$

令 $t=m_2/d$

所以可令

$$K'=(k_1\%t+t)\%t \tag{22}$$

即可求出最小非负数解 K'.

又式(19)与 $\mathrm{Dat}=r_1(\mathrm{mod}\ m_1)$ 对比可得:

$$r_1=r_1+\ m_1*K'$$

$$m_1=m_1*m_2/d=m_1/d*m_2 \tag{23}$$

从式(23)可以看出得到 K'后便可以求出 r_1,依次类推迭代下去,最后得到的 r_1 就是方程组的最小非负数解,即是所求的 Dat.

4 模运算喷泉码构造及性能分析

传统喷泉码概念的重要指标之一就是译码成功时所用的信息长度与原始信息长度的比值,简称为码率[20],喷泉码设计的重要指标就是要使比率尽量接近 1:1,下面的内容将从码的具体设计入手,分析模运算喷泉码的构造及性能.

设原始信息二进制比特流的长度为 L bit,将原始信息比特流按照长度 k bit 进行等长分段,分别对每一

段进行模运算喷泉编码,即每段原始信息比特流能表达的最大十进制整数为 2^k;令编码分组因子的长度为 l bit,即编码分组能表达的最大十进制整数为 2^l,显然 $l<k$. 则原始信息可以被划分为 L/k 个原始分组,在此令原始分组的集合为 $P\in(p_1,p_2,\cdots,p_t\mid t=L/k)$.

任意一个原始分组 p_i 都应该在 $(0,2^k)$ 内,令 $M\in(m_1,m_2,\cdots,m_t\mid m_t<2^l)$ 为用于编码分组的正整数集,模运算喷泉码能够成功译码的概率为:

$$\begin{aligned}P_d &= \sum_{j=1}^{k}\binom{k}{j}P_r\left[\prod_{t=1}^{j}m_t > m\right]\\ &= \sum_{j=1}^{k}C_k^jP_r\left[\prod_{t=1}^{j}m_t > 2^k\right]\\ &= \sum_{j=1}^{k}\frac{k!}{j!(k-j)!}P_r\left[\prod_{t=1}^{j}m_t > 2^k\right]\end{aligned}\tag{24}$$

其中 $P_r[\ ]$ 表示[ ]内条件满足的概率,经过编码分组之后,由于原始分组长度为 k bit,其所能表示最大数是 2^k,编码分组长度为 l bit,其所能表示最大数是 2^l,用 m_t 表示,在进行模运算喷泉码译码时候,可以选用进行译码的编码分组数目理论上是原始信息分组长度,即为 k 个,所以可以从 k 个编码分组中选出 j 个用于恢复原始数据,即译码,这是一个组合 C_k^j,根据文献[9],要使模运算喷泉码能译码成功,则要求接收的编码分组累乘的乘积大于原始被分解的数据,所以假设用于译码的分组数为 j,$P_r[\prod_{t=1}^{j}m_t>m]$ 为分组编码累乘大于原始分组的概率,j 为可变值,其范围为 $1\leqslant j\leqslant k$.

在式(24)中,j 为参与一次译码的分组数目,则译码成功所需的编码分组的平均数量为:

$$N_d = \sum_{j=1}^{k}j*P_r\left[\prod_{t=1}^{j}m_t > 2^k\right]\tag{25}$$

由于原始信息分组长度为 k bit,每个编码分组的长度为 l bit,则译码成功时所用的编码分组的 bit 数与原始分组的 bit 数的比率为:

$$R_d = \frac{1}{k}\sum_{j=1}^{k}j*P_r\left[\prod_{t=1}^{j}m_t > 2^k\right]\tag{26}$$

从式(24)~(26)可以看出,如果对模运算喷泉码的构造结构不加考虑,则上述三个指标的实际值一定是随机变化的,不能够保证译码成功的代价为固定值,这一点与 LT 码较为类似,即在某一个比率值上译码成功的概率并非 100%[21],在模运算喷泉码中,我们通过下述的构造分析,在不引入外部级联码的前提下实现了模运算喷泉码译码空时代价的稳定,即在某一个比率上,实现 100% 的译码成功.

按照之前的假设,原始信息的长度为 L bit,单个原始分组的长度为 k bit,编码分组因子的长度为 l bit,随机使用 n 个接收分组成功解码的要求为用于解码的分解因子乘积值大于原始数据值,即要求:

$$\prod_{t=1}^{n}(2^{\lfloor k/l\rfloor+1}+t) > 2^k\tag{27}$$

不等式左边属于较为宽泛的近似,要保证从生成的编码分组中任意选取 n 个时都能译码成功[22],所以必须满足 $n\geqslant\lfloor k/l\rfloor+1$,才能使编码分组累乘积要大于原始分组数据,显然上式成立.

5 模运算喷泉码编译码算法

根据前述分析,假设原始信息长度为 L bit,原始信息分组长度为 k,编码分组的长度为 l,很明显 $l\leqslant k$,则基于扩展欧几里得算法编译码步骤如下.

5.1 编码算法

新型喷泉码编码过程如图 3 所示,步骤如下:

(1)将原始信息 bit 顺次按照长度 k 进行分组,有 $\lfloor L/k\rfloor+1$ 组;

(2)计算原始信息分组长度 k 与编码分组长度 l 的比值,根据编码构造分析式(27)可知,至少使用 $\lfloor k/l\rfloor+1$ 个编码分组对原始分组进行分解;

(3)从已知的编码分组中随机选取至少 $\lfloor k/l\rfloor+1$ 个编码分组进行模运算;

(4)将模运算得到的余数作为信息和相应的编码分组序号作为开销生成一个编码分组;

(5)重复(3)、(4)步不断生成新编码分组,直到满足编码分组的最低个数.

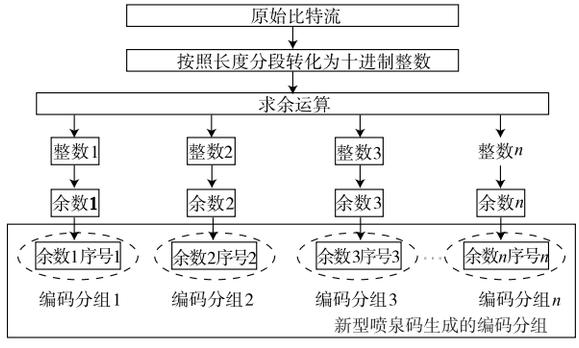


图3 新型喷泉码编码示意图

5.2 译码算法

如果解码方接收 i 个分组,i 一般大于等于 2,本文所提出的解码流程如图 4 所示,具体如下:

(1)从接收的编码分组中开销部分提取出序号,得到用于编码的分组;

(2)从接收的编码分组中信息部分提取出信息序列,得到与之对应的余数;

(3)计算接 i 个分组中分解因子构成的累乘值 m_i,如果 $m_i>2^k$,则根据 3.3 小节进行解码;

(4)若 $m_i\leqslant 2^k$,继续接收一个新分组,重复进行步

骤(1)~(3);

(5)根据3.3节内容,使用扩展欧几里得算法求出原始信息序列.

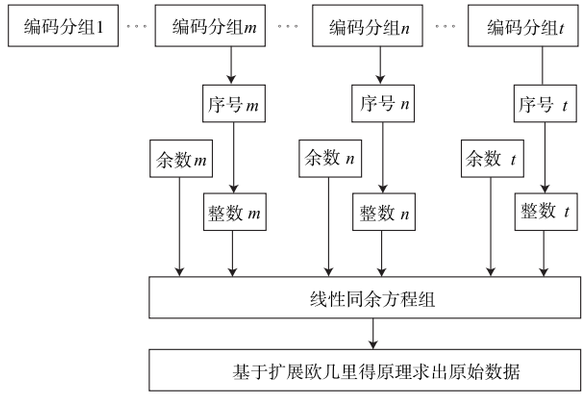


图4　新型喷泉码译码示意图

5.3　编译码时间复杂度分析

模运算喷泉码在编码时只有求余运算即可得到模余数,而分解因子是已知的,其编码复杂度为 $O(1)$,就编码而言,中国剩余定理与扩展欧几里得算法一样的,但扩展欧几里得算法可以使用的编码分解因子更多,应用范围更广.

同理,从2.1小节可以看出,对于中国剩余定理码译码核心部分大衍求一术而言,需要求 M_i 及其逆元 $M_i^{'}$,其算法复杂度应该为 $O(2k^2)$,基于扩展欧几里得算法译码,每次合并调用一次扩展欧几里得算法,假设 $n=\max\{r_i\}$,其中 $n<k$,合并 n 次,所以最坏时间复杂度为 $O(k\log n)$,小于中国剩余定理的译码复杂度. 因此,就编译码的效率而言,扩展欧几里得算法要优于中国剩余定理.

6　仿真实验及结果

为了验证基于扩展欧几里得定理的模运算喷泉码构造算法的有效性,及编译码算法的可行性,本文通过Matlab实验来仿真验证其实际性能.

实验1　模运算喷泉码译码成功率随接收分组数目变化分析

本实验验证接收分组数目变化对于译码成功率影响. 设 k 表示原始数据分组的长度,本次仿真中设置 $k=32$,l 表示编码分组分解因子的平均长度,仿真中设置为可变长度3、4、5,仿真10000次,然后计算相应译码成功次数测试值,观察不同分组长度情况下译码成功率随接收分组数目的变化,译码结果如图5所示. 图5中横轴表示接收编码分组的数目 n,纵轴表示译码成功率. 从图中可以看出:与常规异或运算喷泉码性质类似,各种不同长度 l 的编码,都随着接收分组数量不断增加,模运算喷泉码译码成功率次数不断增加,当满足式(27)构造后,译码成功率为100%.

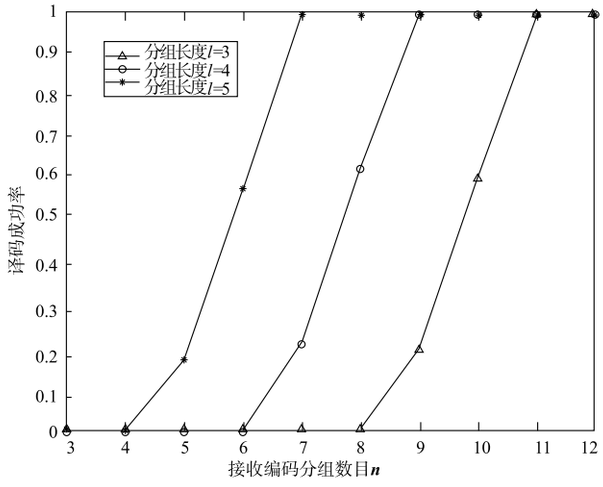


图5　不同译码分组数目情况下模运算喷泉码性能对比

实验2　模运算喷泉码确定100%译码成功时构造参数性能分析

本文第4节分析和推导了模运算喷泉码成功译码概率计算公式,本实验构造了确保基于模运算喷泉码译码成功的相关参数,表1中 n 表示用于恢复译码的接收的编码分组的个数,k 表示原始数据分组的长度,l 表示编码分组的长度,m 表示分解因子累积乘积,2^k 是原始分组能够表示的十进制最大值,R 表示取这种参数构造条件时译码成功时,接收的编码分组中总共参与译码的比特数与原始信息比特数的比率,即为码率. 从表中可以看到,依照式(27)参数构造出来的模运算喷泉码满足编译码确定成功的构造条件,表1中确保译码成功所需要的码率 R 从1.142到1.200不等,即能够以概率1恢复译码成功.

表1　不同参数下的若干模运算喷泉码构造示例

N	k	l	m	2^k	R
2	10	6	1122	1024	1.200
2	12	7	4290	4096	1.167
2	14	8	16770	16384	1.142
3	15	6	39270	32768	1.200
3	18	7	287430	262144	1.167
3	21	8	2196870	2097152	1.142
4	20	6	1413720	1048576	1.200
4	24	7	19545240	16777216	1.167
4	28	8	289986840	268435456	1.142

图6仿真给出可100%译码成功的原始分组长度 k 与不同编码分组长度 l 及不同接收分组数目 n 关系三维图;x 轴表示接收分组数量 n,仿真中接收分组数量取

1 ~30 的整数值,y 轴表示编码分组长度 l,仿真中编码分组长度设为 1 ~30 整数值,z 轴表示在对应(l,n)情况下可 100% 译码成功的原始分组长度 k. 从图中可以看出,编码长度固定时,接收编码数目越多可以成功译码的信息数据越长,当接收编码数目固定时,编码长度越长可以成功译码的信息数据越长.

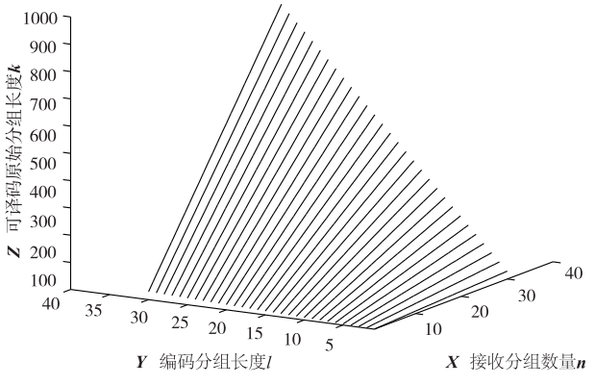


图6 可译码成功的原始分组长度k与不同编码分组长度l及不同接收分组数目n关系

实验 3 中国剩余定理及扩展欧几里得定理等不同译码算法误码率对比分析

仿真中模运算喷泉码参数选取为 $k=15$,$l=6$,编码信息长度与原始信息的比率为 1.2,分解因子选定为 1 ~10000 范围的正整数,设定参数 r 为分解因子中互质数所占的比率,在 r 等于 0.8 及 0.1 两种情况下对比误码率性能,10000 次仿真. 从仿真图 7 可以看出,扩展欧几里得定理算法几乎不受分解因子中互质参数影响,在 $r=0.1$ 及 $r=0.8$ 两种情况下误码率性能相近,当接收到足够的编码分组 $n=4$ 时候,误码率达到 10^{-4},之后当接收分组继续增多,能够全部译码成功. 中国剩余定理由于只能使用互质因子译码,所以在 $r=0.1$ 及 $r=0.8$ 两种情况下误码率性能差异较大,当 $r=0.1$ 时候互质因子较少,所以要达到相同的误码率需要接收的编码分组较 $r=0.8$ 更多,两种互质参数情况相对于扩展欧几里得定理都需要更多分组才能达到相同性能. 从图 7 中也可以看出,中国剩余定理算法互质的限制,限制了分解因子选取范围,需要接收更多编码分组才能达到相同译码性能,降低编码效率.

采用满足式(27)条件构造模运算喷泉码,用于一幅图像的编解码仿真以验证其实际性能. 模运算喷泉码参数选取为 $k=15$,$l=6$,编码信息长度与原始信息的比率为 1.2 对原始图像信息进行编码后,再分别用中国剩余定理与扩展欧几里得定进行译码恢复,对比图像如图 8 所示. 从图 8 中可以看出通过扩展欧几里得算法译码得到图像清晰图明显好于中国剩余定理,因为编码分解因子在自然数范围内随机选取,采用中国剩余

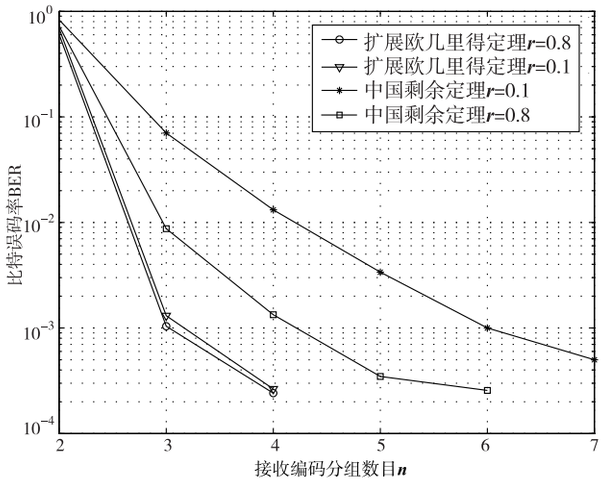
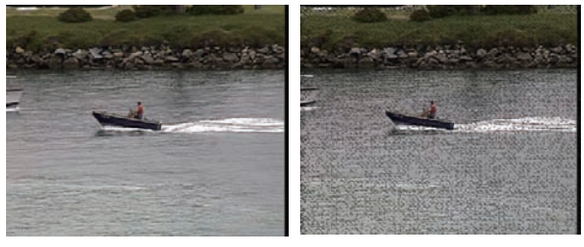


图 7 编码因子不同互质情况下扩展欧几里得算法与中国剩余定理译码误码率对比

定理译码时候若遇到分解因子非互质情况下,大衍求一术译码算法就会失败,导致图像信息恢复不完整,清晰度下降. 而扩展欧几里得译码算法在分解因子非互质情况下也能译码成功,适应分解因子自然数的范围选取要求,可以完全恢复图像信息.



扩展欧几里得算法 中国剩余定理

图8 不同模运算喷泉码译码算法恢复图像对比

实验 4 中国剩余定理及扩展欧几里得定理等不同译码算法耗时统计分析

采用实验 2 表 1 中模运算喷泉码构造参数,在确定译码成功情况下,在 Matlab R2008b 环境中统计两种不同译码算法分别耗时,PC 硬件配置为 2.6GHz E5300 Dual-Core 处理器,2G 内存. 由图 9 可以看出,基于扩展欧几里得定理译码算法耗时明显少于中国剩余定理,由此可以说明扩展欧几里得算法能够提高基于模运算喷泉码译码效率.

7 结束语

本文提出一种全新的基于扩展欧几里德定理的新的模运算喷泉码译码算法,模运算分解机制实现了喷泉码概念要求的相关特性,利用扩展欧几里德定理合并线性同余方程组实现了模运算喷泉码译码,从而将模运算喷泉码分解因子选择范围从互质素数扩展到一般自然数,扩大其应用范围. 提出了模运算喷泉码能够

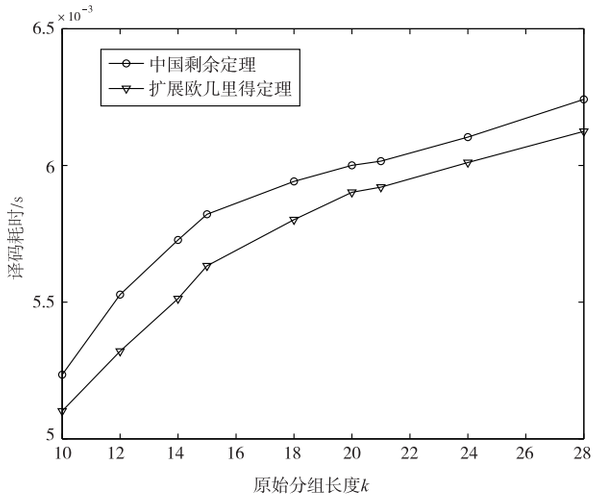


图9　不同参数下模运算喷泉码时间复杂度

成功解码的构造不等式,通过将扩展欧几里德算法与中国剩余定理算法进行对比仿真实验,验证了基于扩展欧几里德算法喷泉码的可行性和可用性.

参考文献

[1] LUBY M, WATSON M, GASIBA T, STOCKHAMMER T. Mobile data broadcasting over MBMS trade offs in forward error correction[A]. ACM International Conference Proceeding Series[C]. New York:ACM,2006. 10 – 20.

[2] MIRREZAEI S M,FAEZ K,YOUSEFI S. Analysis and design of a new fountain codec under belief propagation[J]. IET Communications,2014,8(1):27 – 40.

[3] NESSA A,KADOCH M,BO Rong. Joint network channel fountain scheme for reliable communication in wireless networks[A]. International Conference on Computing, Networking and Communications[C]. Iguazu Falls: IEEE, 2014. 206 – 210.

[4] HAO Niu,IWAI M,SEZAKI K. Exploiting fountain codes for secure wireless delivery[J]. IEEE Communications Letters,2014,18(5):777 – 780.

[5] HUANG Wei,LU Zhufei,DING Lianghui. Television broadcast using unequal fountain codes[A]. IEEE International Symposium on Broadband Multimedia Systems and Broadcasting[C]. Beijing:IEEE,2014. 1 – 6.

[6] SHIRVANIMOGHADDAM,LI Yonghui,VUCETIC B. Sparse event detection in wireless sensor networks using analog fountain codes[A]. IEEE Global Communications Conference [C]. Austin:IEEE,2014. 3520 – 3525.

[7] ALEXANDRE P, VIEIRA J, NAVARRO A. Data broadcasting over DAB/DMB with Fountain codes and auxilliary mobile data channels[A]. The 16th International Telecommunications Network Strategy and Planning Symposium [C]. Funchal:IEEE,2014. 1 – 6.

[8] 慕建君,焦晓鹏,曹训志. 数字喷泉码及其应用的研究进展与展望[J]. 电子学报,2009,37(7):1571 – 1577.
MU Jian-jun,JIAO Xiao-peng,CAO Xun-zhi. A survey of digital fountain codes and its application[J]. Acta Ecectronica Sinica,2009,37(7):1571 – 1577. (in Chinese)

[9] CHANG Shih-Ying,CHIAO Hsin-Ta,HUNG Yu-Hsiang. Ideal forward error correction codes for high-speed rail multimedia communications[J]. IEEE Transactions on Vehicular Technology,2014,63(8):3517 – 3529.

[10] SHIH Pei-Yu, SU Wen-Ku, LIN Tsung-Ching, TRUONG Trieu-Kien. Modified decoding of binary quadratic residue codes by using euclidean algorithm[A]. Proceedings of the 11th International Conference on Advanced Communication Technology[C]. Gangwon-Do: IEEE, 2009. 1398 – 1402.

[11] DILIP V, YAN Sarwate Zhiyuan. Modified euclidean algorithms for decoding reed-solomon codes[J]. Proceedings of IEEE International Symposium on Information Theory, Seoul, Korea: IEEE, 2009. 1398 – 1402.

[12] KAMPF Sabine, WACHTER Antonia, BOSSERT Martin. A method for soft-decision decoding of reed-solomon codes based on the extended Euclidean algorithm[A]. Proceedings of International ITG Conference on Source and Channel Coding[C]. Ulm: IEEE, 2010. 1 – 6.

[13] ZEH Alexander, LI Wenhui. Decoding reed-solomon codes up to the sudan radius with the euclidean algorithm[A]. Proceedings of International Symposium on Information Theory and its Applications[C]. Austin: IEEE, 2010. 986 – 990.

[14] 陈代梅,范希辉,朱静,汪玉美. 基于同余方程和中国剩余定理的混淆算法[J]. 计算机应用研究,2015,32(2):485 – 488.
CHEN Dai-mei, FAN Xi-hui, ZHU Jing, WANG Yu-mei. Obfuscation algorithms based on congruence equation and Chinese remainder theorem[J]. Application Research of Computers,2015,32(2):485 – 488. (in Chinese)

[15] LUO Xiaofeng, XU Qiaozhi, ZHANG Junxing. A digital watermarking algorithm based on Chinese remainder theorem[A]. The 10th International Conference on Communications[C]. Bucharest: IEEE, 2014. 1 – 4.

[16] 杨阳,朱晓玲,丁凉. 基于中国剩余定理的无可信中心可验证秘密共享研究[J]. 计算机工程,2015,41(2):122 – 128.
YANG Yang, ZHU Xiaoling, DING Liang. Research on verifiable secret sharing without trusted center based on chinese remainder theorem[J]. Computer Engineering, 2015,41(2):122 – 128. (in Chinese)

[17] 陈泽文,张龙军,王育民,黄继武,黄达人. 一种基于中国

剩余定理的群签名方案[J]. 电子学报,2004,32(7):1062 – 1065.
CHEN Ze-wen, ZHANG Long-jun, WANG Yu-min, HUANG Ji-wu, HUANG Da-ren. A group signature scheme based on chinese remainder theorem [J]. Acta Ecectronica Sinica, 2004, 32(7): 1062 – 1065. (in Chinese)

[18] MOSTAFA Mohamed, MARTIN H Bossert. A chase-like decoding algorithm for reed-solomon codes based on the extended euclidean algorithm[A]. Proceedings of the 10th International ITG Conference on Systems, Communications and Coding[C]. Hamburg: IEEE, 2015. 1 – 4.

[19] YANG Jun-jian, WANG Yun. An extended euclid algorithm for rational reconstruction[A]. IEEE Symposium on Electrical & Electronics Engineering[C]. Kuala Lumpur: IEEE, 2012. 422 – 424.

[20] ZENG Meng, CALDERBANK Robert, CUI Shuguang. On design of rateless codes over dying binary erasure channel [J]. IEEE Transactions on Communications, 2012, 60(4): 889 – 894.

[21] CHEN Guo-tai, CAO Lei, ZHAO Fei-long. Analysis of robust soliton distribution for LT code[A]. Proceedings of the IEEE 11th International Conference on Signal Processing[C]. Beijing: IEEE, 2012. 1546 – 1549.

[22] 祝开艳,王洪玉,孙文珠,牛芳琳. 一种分布式喷泉码在协作通信中的应用[J]. 电子学报,2014,42(7):1249 – 1255.
ZHU Kai-yan, WANG Hong-yu, SUN Wen-zhu, NIU Fang-lin. A distributed fountain code for cooperative Communications[J]. Acta Ecectronica Sinica, 2014, 42(7): 1249 – 1255. (in Chinese)

作者简介

朱文杰 男,1984 年出生于湖北孝昌县,武汉大学博士研究生,研究方向为无线通信,信道编码.
E-mail: wenjie8408@163.com

易本顺 男,1965 出生于湖北武汉,武汉大学教授,博士生导师,主要研究方向为多媒体通信,无线网络.
E-mail: yibs@whu.edu.cn