手机银行短信息的 BCH-NAF-RSA 快速编译与加密及其安全实现①

邓从政

(凯里学院 数学科学学院, 凯里 556011)

摘 要: 智能手机的快速普及推动着通信运营商不断开发新的诸如手机银行类的增值业务以增长利润, 这些业务往往通过短信中心来完成. 为了安全快速的实现这些业务, 这里改进了信号发射台短信息的编译码算法, 引入一种优化的 BCH 迭代译码算法, 来设计和实现手机短信寻呼台译码器, 这种译码算法错码率较小, 能大大增强纠错能力, 提高了短信的发送质量. 同时对短信息的加密和解密算法进行了优化, 提出了一种优化的低存储 NAF 点压缩数乘算法, 大大地缩短了点乘运算的运行时间, 节约了存储空间, 经过 NAF 和 BCH 快速编译后, 利用安全性较高的基于圆锥曲线的 RSA 公钥密码来进行加密, 以提高手机短信寻呼台信号呼出和呼入的速度及其安全性, 保证了手机银行短消息业务的安全快捷实现.

关键词: 手机银行; 短信寻呼台; 标准二进制; 迭代译码算法; 公钥密码

Mobile Banking Short Message BCH - NAF - RSA Fast Compilation and Encryption and Security Implementation

DENG Cong-Zheng

(School of Mathematics Sciences, Kaili University, Kaili 556011, China)

Abstract: The rapid spread of the mobile communication technology promotes the communication operators continue to develop new value-added business such as mobile phone banking to increase profits. These operations are often completed by fast compiled code through the short message center. This paper improved traditional binary multiplication algorithm, and presents an optimized low storage NAF point compression multiplication algorithm. It greatly reduces the running time of point multiplication operation, and saves storage space. Here introduces an optimization of BCH iterative decoding algorithm for the design and realization of mobile phone short message paging decoder. The error rate of this decoder algorithm is small. That can greatly enhance the error correcting ability, and improve the quality of short message sending. Through twice compilation of NAF and BCH, it can use conic curve cryptography to encrypt fastly. The velocity of mobile phone SMS paging signal outgoing and incoming will get greatly improved. It can make sure the safety of mobile phone short message bank business transactions and implementation speed.

Key words: mobile banking; SMS paging; standard binary; iterative decoding algorithm; public key cryptography

手机银行是基于短信的银行业务, 由手机、GSM 短信中心和银行系统构成. 在手机银行的操作过程中, 用户通过 SIM 卡上的菜单对银行发出指令后, SIM 卡根据用户指令生成规定格式的短信并加密, 然后指示手机向 GSM 网络发出短信,GSM 短信系统收到短信后, 按相应的应用地址传给相应的银行系统,银行对短信进行预处理, 再把指令转换成主机系统格式,银行主机处理用户的请求,并把结果返回给银行接口系统, 接口

① 基金项目:贵州省科技厅科学技术基金(黔科合 J 字[2011]2218 号,黔科合 J 字[2013]2260 号);贵州省教育厅自然科学研究基金(黔教科 KY 字[2013]185 号); 凯里学院重点课题(Z1307)

收稿时间:2014-11-24;收到修改稿时间:2015-01-19

系统将处理的结果转换成短信格式, 短信中心将短信发给用户. 手机银行延长了银行的服务时间, 扩大了银行的服务业务, 是网上银行的延伸, 可以方便地开展多种银行业务, 这些业务是通过短信中心来完成. 为了保证手机银行用户业务安全快捷的完成, 需要对短信息进行快速编译码并且加密传送. 短信息的发送和接受常常收到信道噪声干扰而造成错码、乱码、乱序以及延时等现象, 严重影响了短信息发送的效率和质量, 给发送方和接收方带来了即时沟通上的不便, 影响了银行业务的顺利完成. 这里提出一种对短信 BCH 译码的优化检错算法, 在译码器中增加一个用于检错通信信号的实际错误比特的检错模块, 可以大幅减少译码的迭代次数, 提高短信息中心的编译速度和质量[1,2]. 另一方面, 短信息需要加密传送以确保用户的财产安全, 为了节约短信中心的存储资源, 这里提出了一种基于剩余类环上圆锥曲线的 RSA 公钥加密算法, 对采用的密钥进行 NAF 压缩编码, 这种低存储的点压缩算法, 大大地缩短了点乘运算的运行时间, 节约了运营商短信息中心的存储空间. 这种 BCH-NAF-RSA 快速编译与加密算法, 加快了短信息的编码和译码速度, 提高了加密和解密的安全性, 从而保证了银行业务安全快速的实现, 突显出手机银行巨大的经济应用价值.

1 基于BCH编译码的手机银行短信息迭代译码算法的优化

现代数字通信中,短信息的发送和接受常常收到信道噪声干扰而造成错码、乱码、乱序以及延时等现象, 严重影响了影响了手机银行业务的顺利完成. 为了提高短信息中心信息传输的正确率和传送速度, 提高短信息的发送质量, 需要进行检错和纠错. 在实际通信的过程中, 由于不知道信号在传递的信道中会产生多少个实际错误比特, 因此使用二元 BCH 码译码时, 必须对每个接受码字逐个比特加以检错然后迭代. 但是信道中信号产生的实际错误个数比译码器预先设计的最大纠错能力往往要少一些, 如果能判断出接受码字中的实际错误个数, 每一个码字的迭代次数就会得以减少, 这样对于一段消息来说, 迭代次数的大幅降低就会减少译码器的计算量, 从而较快地得到错位多项式并送入搜根器, 达到提高译码器的译码速度[1-3]. 这里通过对二元 BCH 译码器伴随式矩阵检错算法的优化, 在译码器中增加一个用于检错通信中信号的实际错误比特的检错模块, 可以大幅减少译码的迭代次数, 提高译码速度, 提高通信效率和质量. 如果由接受码字的伴随式来构造矩阵, 根据伴随式矩阵的可逆性来判断接受码字的实际错误个数 λ, 使得实际中当接受码字有 λ $(\lambda \le t)$比特出错时, 只需迭代 2λ 次就可以得到错位多项式, 这样对于每一个码字可以减少迭代次数 $2(t-\lambda)$, 而对于一段消息来说, 大大地减少了迭代次数, 加快译码速度, 另一方面, 当 i 为奇数时, $d_i=0$, 为此在 BM 迭代算法流程中增加一个对迭代次数 i 的模 2 逻辑判断模块, 以判断 i 的奇偶性, 当 i 为奇数时, 无需计算修正差值 d_i, 直接进入下一次迭代, 这样减少了流程中的迭代次数和计算量, 通过这个模块的优化, 整个迭代次数可以减少一半, 大大的减少了译码器的计算量, 从而加快了整个二元 BCH 码的译码进程. 对传统的迭代算法加以改进, 可以节约译码器的硬件资源, 提高译码速度, 因此具有很大的实际意义[1,4].

2 低存储的NAF压缩编码与基于剩余类环 Z_n 上圆锥曲线的快速倍点算法

手机银行业务的完成是通过用户向银行发送指令, 银行根据指令进行转账、划拨等业务操作. 现代信息技术发展迅猛, 滋生了很多不安全因素, 要保证这些业务的安全完成, 短信息的安全发送和接受至关重要, 因此需要对指令性的短信息进行加密和解密, 另一方面, 通信运营商希望短信息中心资源耗费低且实现速度快, 而 NAF 压缩编码算法在加密和解密过程中计算倍点时, 可以节约存储空间, 提高加解密速度. 基于剩余类环 Z_n 上圆锥曲线 $(C_n(a,b),\oplus)$ 密码系统中的加法就是点乘运算, 为了节约存储空间, 传统算法采用“倍和” 来计算圆锥曲线上的加密倍点 kP, 也就是乘法群中的幂运算转换为加法群的数乘运算: $\alpha^n \to n\alpha$, 乘法群的积运算转换为加法群中和运算: $\alpha\beta=\alpha\oplus\beta$, 这样圆锥曲线 $(C_n(a,b),\oplus)$ 上只有和运算和倍点运算了. 群中加法逆非常容易计算, 这样倍和运算可以转换为倍差运算了, 也就是说 $(C_n(a,b),\oplus)$ 上的点乘法可以转换成加法和减法两种运算, 为了实现倍差算法, 需要把传统的二进制改进为标准二进制 NAF, 这种进制中 0 的个数比传统二进制要多, 计算倍点时可以大大减少运算次数以提高

运算速度，且能大大的节约存储空间，从而提高整个密码系统的加解密速度[5, 6]，现在描述 NAF 如下.

NAF 的描述：设 $n\in Z$，n 表为：$n=\sum_{i=0}^{l}c_i2^i, c_i\in\{1,0,-1\}$，$0\le i<l$，其中 $c_ic_{i+1}=0$，则称这种带有符号的二进制为整数 n 的标准二进制表示，记为 $NAF(n)=(c_lc_{l-1}...c_1c_0)$.

下面给出一个对于任意整数的快速 NAF 编码算法.

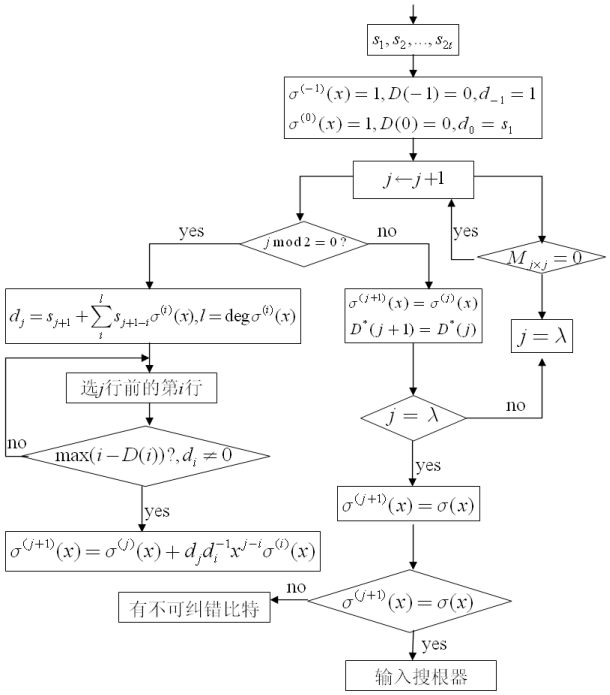

图 1 短信息 BCH 迭代译码算法的优化流程

任何一个非负整数有惟一的一个 NAF 表示，NAF 表法比传统的二进制表示中有更多的零，例如素数 5659 传统二进制编码为：(1010100011010)，压缩编码为 $NAF(5659)=(0-10-1000100-10-1)$. 可以证明，一个 l 比特整数的二进制表示中含有 $l/2$ 个零，它的 NAF 表示中含有 $2l/3$ 个零，可以非常容易地比较两种算法的计算速度：两种算法需要 l 次倍乘运算，但在倍和算中需要 $l/2$ 次加法运算，在倍差算法中需要 $l/3$ 次. 假设倍乘运算与加法或减法花费大致相同的时间，那么两个算法花费的时间的比率约为：$(l+l/2)/(l+l/3)=9/8$，利用倍差运算大约提高 11% 的速度[7, 8]. 利用 NAF 压缩编码算法可以快速计算圆锥曲线 $(C_n(a,b),\oplus)$ 上的倍点，压缩编码后 0 的个数较多且将传统二进制的倍加算法转换成倍差算法，减少了加法次数并且不用存储，这样大大节约了存储空间、提高了加密的计算速度.

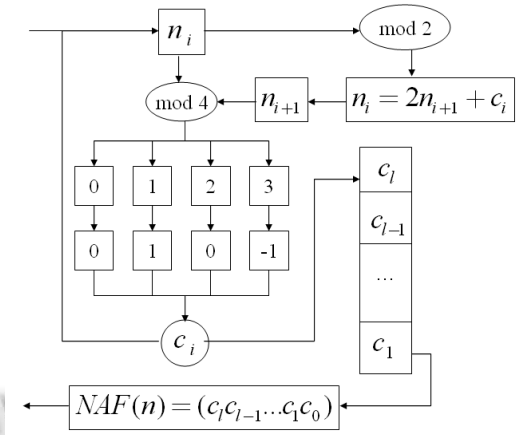

图 2 $NAF(n)$压缩编码算法流程

倍点($Q=cP$)的快速倍差算法:

(1) 设 $P\in(C_n(a,b),\oplus)$，给定整数 $c\in Z, 0\le c<n$;

(2) 用 NAF 对 c 压缩编码：$NAF(c)=(c_lc_{l-1}...c_1c_0)$;

(3)赋值 $Q\leftarrow O$ (O 为 $(C_n(a,b),\oplus)$ 的零元);

(4) $for\ i\leftarrow l-1 downto 0;$

$else$

$Q\leftarrow 2Q;$

$if\ c_i=1;$

$then\ Q\leftarrow Q+P;$

$else\ if\ c_i=-1;$

$then\ Q\leftarrow Q-P$

(5) $return(Q)$.

3 基于圆锥曲线的手机银行短信息 BCH-NAF-RSA 快速编译和加密算法

基于剩余类环 Z_n 上圆锥曲线的 *RSA* 公钥密码系统极大地提高了传统 *RSA* 算法的安全性，对于手机银行来说，一方面要保证用户的财产安全，另一方面还要保证通信运营商资源消耗不能过高，也就是短信息中心的存储成本要低，这样就要求短信寻呼台发送的信息速度要快、存储成本要低、发送和接收要安全. 这里结合 *BCH* 快速编码和 *NAF* 压缩编码，利用安全性较高的基于圆锥曲线的 *RSA* 公钥密码来进行加密，提出一种基于圆锥曲线的 *BCH-NAF-RSA* 编译和加密的算

法, 来安全快捷的实现手机银行业务[9, 10].

手机银行短信息 *BCH-NAF-RSA* 快速编译和加密的算法:

(1) 生产大素数: $n=pq, p\neq q$为奇素数;

(2) 生产参数 (a,b) : $(\frac{a}{p})=(\frac{a}{q})$=-1, $n=pq$, $(a,b)=(b,n)=1$;

(3) 生成圆锥曲线 $(C_n(a,b),\oplus)$:
$y^2\equiv ax^2-bx(\mathrm{mod}\,n),(a,b\in Z_n)$;

(4) 任意选取$1<e<2rs$, $p+1=2r, q+1=2s$, r,s 也为素数;

(5) 设计密钥: $ed\equiv 1\mathrm{mod}(2rs)$;

(6) 密码参数系统生成: 公钥 (n,a,b,e), 私钥 (d,p,q,r,s);

(7) 对短信息 s 源码进行 BCH 编码: $BCH(S)=m$

(8) 将编码 $BCH(S)$ 进行嵌入 $(C_n(a,b),\oplus)$:
$x_m=b/(m^2-a)(\mathrm{mod}n), y_m=bm/(m^2-a)(\mathrm{mod}n)$, 得到 $P(m)=(x_m,y_m)$;

(10) 将公钥参数 e 进行 NAF 编码得到 $NAF(e)=k$;

(11) 快速计算倍点 $kP(m)=P(t)$, 得到密文 t;

(12) 计算私钥 $d\equiv e^{-1}\mathrm{mod}(2rs)$;

(13) 解密密文: $P(m)$ =dP(t);

(14) 将密文进行 BCH 译码得到短信息 s 源码: $BCH(m)=s$

参数 (p,q,a) 生成参见文献 [11], 整个 *BCH-NAF-RSA* 实现流程如图 3

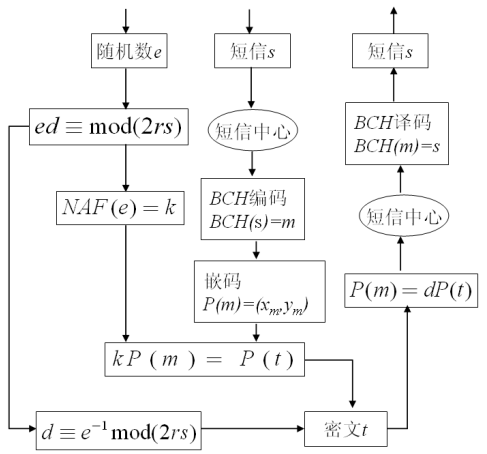

图3 短信息 *BCH-NAF-RSA* 快速编译与加密算法的实现流程

下面我们根据上述算法来模拟实现一个特殊的案例,假设我们向银行下达的一段短信息指令即源码经过短信中心编译为 $S=10010110$, 采用手机短信寻呼台 $BCH(15,5,7)$ 来实现编译码[12], 则 $C++$ 实现算法如下:

(1) 选取圆锥曲线 $(C_{5809}(2,1,b),\oplus)$:
$y^2\equiv 2x^2-x(\mathrm{mod}\,5809)$;

(2) 使用 $BCH(15,5,7)$ 编码:
$BCH(10010110)=(1000110111010100)$;

(3)将编码 $BCH(10010110)=(1000110111010100)$ 进行嵌入 $(C_{5809}(2,1,b),\oplus)$:

$P(1000110111010100)$=((1010110101010111), (1011100001010100))

(4) 公钥参数 35 进行 NAF 压缩编码得到 $k=NAF(35)=(10010-1)$;

(5) *RSA* 生产密钥, 计算
$35d\equiv \mathrm{mod}(2\times 19\times 79)$ 得到 $d=1887$;

(6) $(C_{5809}(2,1,b),\oplus)$ 上 *RSA* 倍点加密得到密文:
(010100101011101);
$kP(m)$ =35P(1000110111010100)
=P(5013) = P(010100101011101)

(7) 送达短信息中心后, 进行 *RSA* 解密:
1887P(010100101011101)=P(1000110111010100);

(8) 短信中心解码:
$BCH(1000110111010100)=(10010110)$;

(9) 短信中心反编译生产源码指令 (10010110) 送达银行接收并处理.

4 结语

为了保证手机银行业务快速、安全、便捷的完成, 对短信息的传统编码算法进行了优化, 使用二元 *BCH* 检错编码算法, 对其迭代译码算法进行了优化, 大幅减少迭代次数从而导致译码器的计算量降低, 大大降低了译码器的翻译计算时间, 节约了硬件资源, 大大提高了译码器的译码速度, 提高了短信息的准确性和稳定性; 另一方面, 为了短信息传送的安全性, 在使用安全性高的 *RSA* 加密过程中, 对加密参数进行了快速的 *NAF* 压缩编码, 大大提高了短信息的加密速度, 通过 *BCH-NAF-RSA* 快速编译与加密, 短信息可以快速、安全、稳定的在信道上传送, 保证了手机银行用户的信息安全和便捷使用, 有助于电信运营商拓展手机银行业务, 适应电信市场经济的快速发展, 具有巨

大的经济价值和应用前景.

参考文献

1 邓从政.二元 BCH 码译码算法的优化与应用[硕士学位论文].广州:广州大学,2007.

2 王新梅,肖国镇.纠错码—原理与方法(修订版).西安:西安电子科技大学出版社,2001.

3 于月华.Berlekamp 迭代算法的改进.信号处理,1994,10(3):53–58.

4 唐建军,纪越峰.超高速 BCH 码解码改进算法研究.通信学报,2004.28(9):23–25.

5 陈熹,祝跃飞.一种高效安全的椭圆曲线标量乘算法.计算机工程,2012,38(18):103–106.

6 李忠,彭代渊.低存储需求的快速标量乘法算法.计算机工程,2012,38(4):137–139.

7 沈学利,张龙华,姜丽.NAF 标量乘算法的改进.计算机仿真,2010,2(27):316–319.

8 蒋洪波,尚春雨,冯新宇.NAF 算法的改进.科学技术与工程.2012; 12(19) :63–66.

9 曹珍富.RSA 与改进的 RSA 的圆锥曲线模拟.黑龙江大学自然科学学报,1999,16(4):15–18.

10 徐旭东,靳岩岩,赵磊.圆锥曲线公钥密码算法的参数选择.计算机工程,2007,15(8):158–159.

11 孙琦,朱文余,王标.环 ZN 上圆锥曲线和公钥密码协议.四川大学学报,2005,42(3):471–475.

12 邓从政.二元捕错译码器的译码算法与设计.凯里学院学报,2010,28(6):75–77.