ISSN 1004-9037,CODEN SCYCE4
Journal of Data Acquisition and Processing Vol. 30,No. 3,May 2015,pp. 694－702
DOI:10. 16337/j. 1004-9037. 2015. 03. 026

http://sjcj. nuaa. edu. cn
E-mail:sjcj@nuaa. edu. cn
Tel/Fax:＋86-025-84892742

N-CDMA 安全架构抗攻击性研究与改进

陈德宏　刘晓东　刘　梅

(安徽工业大学电气与信息工程学院,马鞍山,243032)

摘　要:通过分析信道结构,发现窄带码分多址(Narrow band code division multiple access, N-CDMA)移动通信系统存在固有的明文信息特征。提出一种新的唯密文攻击方法,只需截获 20 ms 的密文帧数据,即可求解密钥序列的初始相位,进一步利用密钥序列与长码产生器状态之间的线性关系,破解用户私人掩码,证明 N-CDMA 的语音加密在唯密文攻击下是不安全的。针对 N-CDMA 系统的安全缺陷与可能受到的攻击方法,提出了一种改进的 N-CDMA 安全架构措施。

关键词:信息安全;密码分析;唯密文攻击;窄带码分多址;私人掩码

中图分类号:TN918. 4　　**文献标志码**:A

Attack-Resistance and Enhancement on Security Framework of N-CDMA

Chen Dehong, Liu Xiaodong, Liu Mei

(School of Electrical and Information Engineering, Anhui University of Technology, Maanshan, 243032, China)

Abstract: Analyzed the channel structure, it is found that there is an inherent signal feature on the plaintext in N-CDMA system. A new ciphertext-only attack method is proposed to solve the initial phase of the key sequence by eavesdropping 20 ms ciphertext frame. By exploiting the linear relations between the key sequence and the state of the long code generator, an algorithm for decoding the private mask is proposed. It is proved that the voice encryption of N-CDMA system is unsecure while attacked by ciphertext-only attack. Aiming at the safety defect of IS-95 system and possible attack methods, a new enhancement scheme is proposed to improve the security framework of IS-95 system.

Key words: information security; cryptanalysis; ciphertext-only attack; N-CDMA; private mask

引　　言

当今巨大的社会需求推动着移动通信迅猛发展。由于移动通信特有的无线属性,使信号更容易被第三方在空中截获,因而移动通信的信息安全问题越来越受到关注。深入研究移动通信系统的安全架构是从第二代移动通信系统(2G)开始的。作为 2G 技术代表之一,IS-95 是一种基于窄带码分多址(Narrowband code division multiple access, N-CDMA)技术的北美数字蜂窝标准[1],也是 CDMA2000 标准的技术基础。

在 N-CDMA 系统中,用于数字话音扰乱的密钥序列是由 42 位的长码掩码和一个 42 级的线性反馈

基金项目:国家自然科学基金(61304066)资助项目。
收稿日期:2014-02-19;**修订日期**:2014-04-14

寄存器共同作用产生的长周期伪随机 m 序列。破译者要想还原明文信息需要知道密钥序列的初始相位,不同用户的 42 位掩码决定密钥序列不同的初始相位。对于某个确定的手机号码,它有唯一的用户私人掩码,这个掩码并不通过无线信道传送,而只被用户的 SIM 卡与移动交换中心(Mobile switching center, MSC)共享存储[2]。在不知道用户 42 位私人掩码的情况下,破译者不得不详尽尝试 42 位私人掩码的各种可能。采用穷举的方法理论上是可行的,搜索 42 位私人掩码的最大复杂度为 $O(2^{42})$,需要消耗巨量的时间,在实际破译中是没有意义的。因此,业内普遍认为 N-CDMA 系统提供了一种近乎完美的无线移动数字话音安全解决方案[3]。

一些研究表明,针对某些敌意的安全攻击,N-CDMA 系统可能是脆弱的[4,5]。利用信道编码过程中卷积编码和码元重复导致的信息冗余度,文献[4]提出一种唯密文攻击 N-CDMA 加密话音安全的方法。用矩阵递推方法获取密文与密钥初始相位的之间关系表达式,并通过计算一系列线性等式能够求解密钥序列的初始相位。可是,这种方法也存在它的缺陷。首先,破译者需要截获不少于 42 帧时间达 840 ms 密文数据,其次,巨大计算量和算法复杂度也限制了它的实时破译效果,除此之外,虽然密钥序列可以通过求解的初始状态和一个等效的长码产生器产生,但是,用户的私人掩码并没有得到,每次为了从截获的密文中还原明文信息,破译者不得不重新求解密钥序列的初始相位。

本文通过对 N-CDMA 系统的前向业务信道结构的详细分析,发现在低速率帧时,块交织器会导致帧内明文周期反复。利用密钥序列是 m 序列以及明文数据周期反复的特性,采用一种新的唯密文攻击法来讨论 N-CDMA 系统的话音安全性。这种方法只需要 20 ms 一个密文帧数据,就可以恢复出明文帧。为了彻底破译 N-CDMA 系统的安全架构,基于密钥序列与长码产生器状态之间的线性关系,提出了一种求解私人掩码的方法。

1 前向业务信道分析

N-CDMA 信道包括控制信道和业务信道两类。其中控制信道传送信令信息,而业务信道传送数字压缩语音。业务信道又分为前向业务信道和反向业务信道。由于前向业务信道中采用 Walsh 码作为扩频码对信息进行扩频传输,与反向业务信道相比,破译者更容易从前向业务信道截取密文信息。图 1 是 CDMA 前向业务信道基带信号编码结构框图。

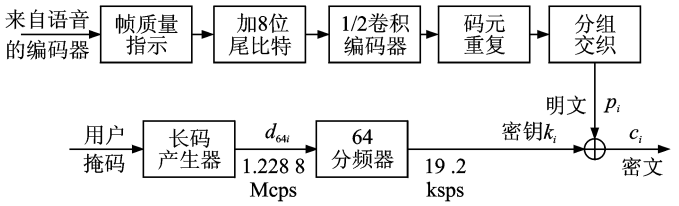

图 1 前向业务信道基带信号编码结构

Fig. 1 Baseband signal encoding of forward traffic channel

图 1 中基站对语音压缩编码构成每帧 20 ms 的数据流,为了提高容量和减少同道干扰,在 N-CDMA 中采用变速率语音编码器。速率分别为 8.6,4.0,2.0 和 0.8 kbps,也被称为速率 1,1/2,1/4 和 1/8 四种速率帧,对应每种速率,20 ms 信息帧比特为 172/80/40/16 比特。不同的帧速率取决于背景噪音的功率,在通话时数据以较高的速率传送,而停顿时选择较低速率。帧质量指示对 8.6 kbps 和 4.0 kbps 数据帧进行循环冗余度编码,每帧分别增加 12 比特和 8 比特用于帧质量指示。编码器尾比特的作用是使每帧数据卷积编码时编码器末尾状态复位至"0",这样,4 种速率帧到达卷积编码器输入端,速率分别为 9.6,4.8,2.4 和 1.2 kbps,再经过 1/2 卷积编码器,输出时速率分为 19.2,9.6,4.8 和 2.4 kbps。为了

统一交织器的输入速率,4 种数率帧要先进行符号重复,以保证交织符号率均为 19.2 ksps,不同速率的帧符号重复的次数也不相同。这 4 种速率在交织之前均变为 19.2 ksps 的符号速率,即每 20 ms 帧有 384 个符号。块交织的作用就是将突发性误码分散开来,便于卷积纠错。

块交织具体操作:

(1)对每帧码元重复后的 384 个符号,按行写入一个 6×64 输入矩阵。表 1 以前向业务速率 1/8 帧为例,交织器输入矩阵数据排列示意。表中 C_n 表示矩阵中符号的列地址为 n,R_n 表示行地址为 n。阵列中的数字表示输入交织器符号在码元重复之前的序号,由于码元重复,表中同一序号连续出现 8 次。

(2)将输入矩阵的每行数据按位翻转地址交织打乱,送入输出矩阵并按列输出,见表 2。所谓位翻转地址,即若交织前列二进制地址为:$X_1X_2X_3X_4X_5X_6$,则交织后列地址为:$X_6X_5X_4X_3X_2X_1$。

表 1 速率 1/8 帧交织器输入矩阵数据排列示意

Table 1 Interleaver input of rate 1/8

	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}	…	C_{48}	C_{49}	C_{50}	C_{51}	C_{52}	C_{53}	C_{54}	C_{55}	C_{56}	C_{57}	C_{58}	C_{59}	C_{60}	C_{61}	C_{62}	C_{63}
R_1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	…	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	8
R_2	9	9	9	9	9	9	9	9	10	10	10	10	10	10	10	10	…	15	15	15	15	15	15	15	15	16	16	16	16	16	16	16	16
R_3	17	17	17	17	17	17	17	17	18	18	18	18	18	18	18	18	…	23	23	23	23	23	23	23	23	24	24	24	24	24	24	24	24
R_4	25	25	25	25	25	25	25	25	26	26	26	26	26	26	26	26	…	31	31	31	31	31	31	31	31	32	32	32	32	32	32	32	32
R_5	33	33	33	33	33	33	33	33	34	34	34	34	34	34	34	34	…	39	39	39	39	39	39	39	39	40	40	40	40	40	40	40	40
R_6	41	41	41	41	41	41	41	41	42	42	42	42	42	42	42	42	…	47	47	47	47	47	47	47	47	48	48	48	48	48	48	48	48

表 2 速率 1/8 帧交织器输出矩阵数据排列示意

Table 2 Interleaver output of rate 1/8

	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}	…	C_{48}	C_{49}	C_{50}	C_{51}	C_{52}	C_{53}	C_{54}	C_{55}	C_{56}	C_{57}	C_{58}	C_{59}	C_{60}	C_{61}	C_{62}	C_{63}
	C_0	C_{32}	C_{16}	C_{48}	C_8	C_{40}	C_{24}	C_{56}	C_1	C_{36}	C_{20}	C_{52}	C_{12}	C_{44}	C_{28}	C_{60}	…	C_3	C_{35}	C_{19}	C_{51}	C_{11}	C_{43}	C_{27}	C_{59}	C_7	C_{39}	C_{23}	C_{55}	C_{15}	C_{47}	C_{31}	C_{63}
R_1	1	5	3	7	2	6	4	8	1	5	3	7	2	6	4	8	…	1	5	3	7	2	6	4	8	1	5	3	7	2	6	4	8
R_2	9	13	11	15	10	14	12	16	9	13	11	15	10	14	12	16	…	9	13	11	15	10	14	12	16	9	13	11	15	10	14	12	16
R_3	17	21	19	23	18	22	20	24	17	21	19	23	18	22	20	24	…	17	21	19	23	18	22	20	24	17	21	19	23	18	22	20	24
R_4	25	29	27	31	26	30	28	32	25	29	27	31	26	30	28	32	…	25	29	27	31	26	30	28	32	25	29	27	31	26	30	28	32
R_5	33	37	35	39	34	38	36	40	33	37	35	39	34	38	36	40	…	33	37	35	39	34	38	36	40	33	37	35	39	34	38	36	40
R_6	41	45	43	47	42	46	44	48	41	45	43	47	42	46	44	48	…	41	45	43	47	42	46	44	48	41	45	43	47	42	46	44	48

下面分析地址位翻转交织后,交织前连续出现的同一序号的分布特性。表 3 给出了除速率 1 之外的 3 种速率帧在位翻转前后相邻重复符号的变化规律。表 3 最后一列为一帧内连续出现的重复符号在位翻转后分布的位置间隔。

如表 3 所示,对于速率 1/2 的数据帧中的任意两个相邻的重复符号,其位比特翻转后列地址的唯一区别是列地址的最高位,而低 5 位($X_5X_4X_3X_2X_1$)是相同的,故地址的位置间隔是一个固定值 32。对于速率 1/4 的数据帧中的任意 4 个相邻的重复符号,位翻转后列地址的前 2 位是不同的,而低 4 位($X_4X_3X_2X_1$)是相同的,相同的符号其地址的位置间隔是定值 16。同理,对于速率 1/8 的数据帧中的任意 8 个相邻的重复符号,位比特翻转后列地址前 3 位是不同的,而低 3 位($X_3X_2X_1$)是相同的,其地址的位置间隔是定值为 8。因此,对于速率为 1/2,1/4 和 1/8 的数据帧,其交织输出矩阵中的每一行分别以 32,16 和 8 为周期排列。当 6×64 的交织矩阵按列输出后,每个数据帧中的 384 个符号分别变成以 192(32×6),96(16×6)和 48(8×6)为周期重复的数据流。表 2 中每间隔 8 列出现序号相同码元,显示了速率 1/8 时,数据帧呈现 48 反复的周期特征。

数据加扰的过程见图 1 所示。长码产生器以 1.228 8 Mcps 速率产生长码序列,通过一个 64 分频器得到一个速率为 19.2 ksps 密钥序列,密钥序列与交织后的明文模 2 加产生密文。图 2 是长码产生器的结构。

表 3　3 种速率帧位翻转交织后重复符号的位置关系

Table 3　Position relations of repeating symbols of rate 1/2,1/4 and 1/8

速率	重复次数	原列地址	位翻转列地址	重复符号位置间隔
1/2	2	$X_1X_2X_3X_4X_50$	$0\ X_5X_4X_3X_2X_1$	32
		$X_1X_2X_3X_4X_51$	$1\ X_5X_4X_3X_2X_1$	
1/4	4	$X_1X_2X_3X_400$	$0\ 0\ X_4X_3X_2X_1$	16
		$X_1X_2X_3X_401$	$0\ 1\ X_4X_3X_2X_1$	
		$X_1X_2X_3X_410$	$1\ 0\ X_4X_3X_2X_1$	
		$X_1X_2X_3X_411$	$1\ 1\ X_4X_3X_2X_1$	
1/8	8	$X_1X_2X_3\ 000$	$0\ 0\ 0\ X_3X_2X_1$	8
		$X_1X_2X_3\ 001$	$0\ 0\ 1\ X_3X_2X_1$	
		$X_1X_2X_3\ 010$	$0\ 1\ 0\ X_3X_2X_1$	
		$X_1X_2X_30\ 11$	$0\ 1\ 1\ X_3X_2X_1$	
		$X_1X_2X_3\ 100$	$1\ 0\ 0\ X_3X_2X_1$	
		$X_1X_2X_3\ 101$	$1\ 0\ 1\ X_3X_2X_1$	
		$X_1X_2X_3\ 110$	$1\ 1\ 0\ X_3X_2X_1$	
		$X_1X_2X_3111$	$1\ 1\ 1\ X_3X_2X_1$	

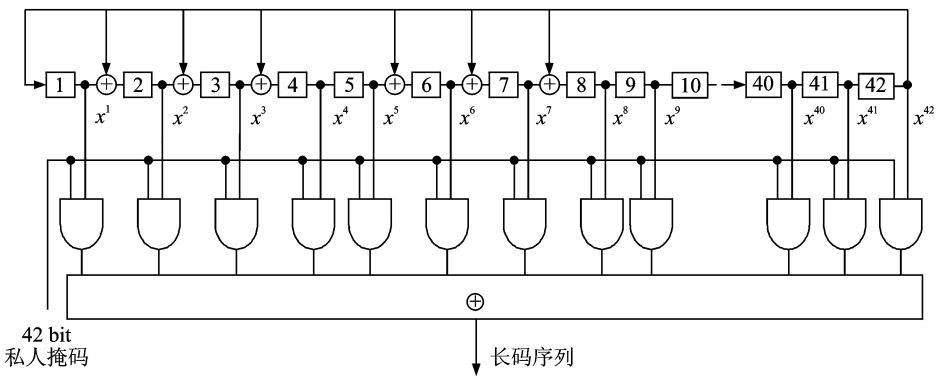

图 2　长码产生器结构图

Fig. 2　Long code generator

图 2 可分为上下两部分,上半部分为一个按多反馈移位寄存器(Multi-return shift regiter generator, MSRG) 结构和式(1)为特征多项式的 42 级 m 序列产生器。

$$f(x)=x^{42}+x^{35}+x^{33}+x^{31}+x^{27}+x^{26}+x^{25}+x^{22}+x^{21}+x^{19}+x^{18}+x^{17}+x^{16}+x^{10}+x^7+x^6+x^5+x^3+x^2+x+1 \tag{1}$$

下半部分为 42 级移存器状态输出与用户掩码相与再模 2 加产生长码序列。令 $M=[m_1,m_2,\cdots,m_{42}]$表示用户私人掩码,$S_l=[s_i(1),s_i(2),\cdots,s_i(42)]$表示第 i 时刻线性反馈移位寄存器(Linear feedback shift registers, LFSR)的状态,则第 i 时刻长码输出 d_i 可以表示为

$$d_i = m_1 s_i(1) \oplus m_2 s_i(2) \oplus \cdots \oplus m_{42} s_i(42) \tag{2}$$

由于式(1)是一个本原多项式,因此 LFSR 各级输出都是同一平移等价 m 序列,根据 m 序列的线性组合特性,得到的长码也是同一平移等价 m 序列。由于不同移动用户的 42 位用户掩码是不同的,决定了各个移动用户长码产生器输出的长码序列在同一时刻具有不同的相位。长码产生器速率为1.228 8 Mcps,而要加密的明文信息的速率为 19.2 ksps。因此,用于加密的密钥序列是通过长码序列 64 分频得到的。第 i 时刻密钥码元 k_i 可表示为

$$k_i = d_{64i} \tag{3}$$

根据 m 序列的抽样特性可知,密钥序列与长码序列是同一平移等价 m 序列。结论:在序列是同一个 m 序列,唯一的区别是它们的相位是不同的且是由用户私人掩码决定的,N-CDMA 安全保密的核心是用户 42 位私人掩码的安全。

2 一种有效的唯密文攻击方法

在图 1 中,密文是由明文信息和密钥序列模 2 加产生的,设第 i 时刻的明文为 p_i,密文为 c_i,则有

$$c_i = p_i \oplus k_i \tag{4}$$

对于 N-CDMA,密钥序列是一个 m 序列,并且产生该 m 序列的特征多项式是已知的。虽然破译者不知道用户的私人掩码,但是,只要能知道密钥序列的 42 比特的初始相位,就可以通过已知的特征多项式,产生后续的密钥序列,进而恢复用户的明文信息。一种有效的唯密文攻击方法就是消除明文的影响,试图从密文中得到密钥的初始相位。攻击的突破口就是选择具有特殊特征明文底码的密文作为攻击的素材。由第 1 节可知,对于速率 1/2,1/4,1/8 的数据帧,在块交织后每帧码元具有周期反复现象。对于 1/2 帧 192 码元周期反复一次,对于 1/4 帧有 96 码元周期反复 3 次,对于 1/4 帧有 48 码元周期反复 7 次,因此,可以认为对于这 3 种速率帧每帧 384 个码元均是 192 个周期反复一次发送。则有

$$p_i = p_{i+192} \tag{5}$$

由式(4,5),可得

$$c_i \oplus c_{i+192} = p_i \oplus k_i \oplus p_{i+192} \oplus k_{i+192} = k_i \oplus k_{i+192} \tag{6}$$

根据 m 序列的移位相加特性:平移等价 m 序列的模 2 加,得到的序列仍然是平移等价 m 序列[6],即

$$k_i \oplus k_{i+r} = k_{i+j} \tag{7}$$

令 $r=192$,由式(6,7)转换为

$$c_i \oplus c_{i+192} = k_i \oplus k_{i+192} = k_{i+j} \tag{8}$$

从式(8)可知:利用密文帧前 192 码元与后 192 码元之间模 2 加,可以抵消明文的影响,可得到 i 时刻密文帧的密钥序列的平移了 j 个相位的等价 m 序列。如果知道了 j,就可以利用 k_{i+j} 序列反推出该帧的密钥序列 k_i。因此,问题的关键是如何求出相移 j。对于某个特定特征多项式产生的 m 序列,式(8)中的 r 和 j 存在固定一一对应关系且与初始相位 i 无关。令 $i=0$,则由式(8)得

$$k_0 \oplus k_{192} = k_j \tag{9}$$

密钥序列可以式(1)为特征多项式,用 MSRG 结构的移位寄存器产生器产生,也可由式(1)的对偶多项式,用简单移位寄存器(Simple shift register generator, SSRG)结构的移位寄存器产生器产生[7,8]。设第 i 时刻 SSRG 结构的移存器的输出码元为 k_i,则 $k_{i-41}, k_{i-40}, \cdots, k_{i-1}, k_i$ 是移存器此刻的状态。求解 j 的具体步骤如下:

步骤 1:设计一个 SSRG 结构的 m 序列产生器,其特征多项式为式(1)的对偶多项式。以任意 42 位码元 $k_{-41}, k_{-40}, \cdots, k_{-1}, k_0$ 作为第 0 时刻移存器的初始状态,由初始状态和特征多项式通过简单计算可

以得到第 192 时刻的移存器状态 $k_{151},k_{152},\cdots,k_{191},k_{192}$。

步骤 2:根据式(9),计算第 j 时刻,SSRG 结构移存器的状态:$k_{j-41},k_{j-40},\cdots,k_{j-1},k_j$。

$$\begin{array}{cccccc} & k_{-41} & k_{-40} & \cdots & k_{-1} & k_0 \\ \oplus & k_{151} & k_{152} & \cdots & k_{191} & k_{192} \\ \hline & k_{j-41} & k_{j-40} & \cdots & k_{j-1} & k_j \end{array}$$

步骤 3:计算 SSRG 结构的 m 序列产生器由状态 $k_{-41},k_{-40},\cdots,k_{-1},k_0$ 到状态 $k_{j-41},k_{j-40},\cdots,k_{j-1},k_j$ 之间的状态转移次数,即 j 的值。需要指出的是:在后续求解密钥序列初始状态的工作中,实际需要计算的是由 $k_{j-41},k_{j-40},\cdots,k_{j-1},k_j$ 到 $k_{-41},k_{-40},\cdots,k_{-1},k_0$ 的状态转移次数(记为 j')。由于该移存器的状态是以 $2^{42}-1$ 周期构成状态转移圈,因此,$j'=2^{42}-1-j$。

42 级 m 序列的周期长达 $2^{42}-1$,若编写软件用微型计算机在一个周期内计算两个状态转移的次数,可能需要数百小时。因而,基于 FPGA 设计了一个数字逻辑电路硬件电路,用于快速求解 j'。这个数字逻辑电路工作主频为 150 MHz,内部包括一个 SSRG 结构的 m 序列产生器并能记录移存器的任意两种状态的转移次数。利用此高速硬件逻辑电路花费约 90 m 求出 j'值,j'值为 28 483 522 265。

下面提出一种针对 N-CDMA 的唯密文攻击方法:

(1)破译者从前向业务信道截获无线电波,解调并用沃尔什码解扩频接收的信号,得到密文帧数据。设已知一个密文帧的 384 个码元:$c_{i-41},c_{i-40},\cdots,c_{i-1},c_i,\cdots,c_{i+342}$。

(2)用密文帧前 192 位码元 $c_{i-41},c_{i-40},\cdots,c_{i-1},c_i,\cdots,c_{i+150}$ 与后 192 码元 $c_{i+151},c_{i+152},\cdots,c_{i+342}$ 模 2 加得到 192 个新码元 $k_{i+j-41},k_{i+j-40},\cdots,k_{i+j-1},k_{i+j},\cdots,k_{i+j+150}$。

$$\begin{array}{cccccccc} & c_{i-41} & c_{i-40} & \cdots & c_{i-1} & c_i & \cdots & c_{i+150} \\ \oplus & c_{i+151} & c_{i+152} & \cdots & c_{i+191} & c_{i+192} & \cdots & c_{i+342} \\ \hline & k_{i+j-41} & k_{i+j-40} & \cdots & k_{i+j-1} & k_{i+j} & \cdots & k_{i+j+150} \end{array}$$

(3)根据 Berlekamp-Massey 算法[9]求解 192 个新码元 $k_{i+j-41},k_{i+j-40},\cdots,k_{i+j-1},k_{i+j},\cdots,k_{i+j+150}$ 的特征多项式。若得到的特征多项式不是式(1)的对偶多项式,则说明截获的素材密文帧是速率为 1 即底码明文不具备 192 周期反复特性,返回到步骤(1)重新选取一个新的密文帧,直到求解出的特征多项式为式(1)的对偶多项式。

(4)取 42 个码元 $k_{i+j-41},k_{i+j-40},\cdots,k_{i+j-1},k_{i+j}$ 做为 SSRG 结构的 m 序列产生器的初始状态,以式(1)的对偶多项式为特征多项式,使该序列产生器状态转移 284 835 222 265 次得到一个新的移存器状态 $k_{i-41},k_{i-40},\cdots,k_{i-1},k_i$。这个状态就是该密文帧的密钥初始状态。这一步的状态转移仍然可以采用 FPGA 硬件电路进行快速求解。

(5)利用求出密钥序列的初始状态 $k_{i-41},k_{i-40},\cdots,k_{i-1},k_i$ 和设计的以式(1)的对偶多项式为特征多项式的 SSRG 结构 m 序列产生器,密钥序列可以等效重构 $k_{i-41},k_{i-40},\cdots,k_{i-1},k_i,\cdots,k_{i+342}\cdots$。将重构的密钥序列与截获的密文帧模 2 加,即可破译出明文信息。

$$\begin{array}{cccccccc} & c_{i-41} & c_{i-40} & \cdots & c_{i-1} & c_i & \cdots & c_{i+342} & \cdots \\ \oplus & k_{i-41} & k_{i-40} & \cdots & k_{i-1} & k_i & \cdots & k_{i+342} & \cdots \\ \hline & p_{i-41} & p_{i-40} & \cdots & p_{i-1} & p_i & \cdots & p_{i+342} & \cdots \end{array}$$

3 用户私人掩码的破解

第 2 节提出的唯密文攻击方法由于不知用户私人掩码,对于每次截获的密文需要花费一定时间重新求解等效密钥序列的初始相位,因此,它并不是一个实时破译系统。等效密钥序列的初始相位是由固

化在用户移动电话的 SIM 卡的用户私人掩码唯一决定的，因此，只有彻底破解用户私人掩码，才能完全实时还原用户的加密信息。在文献[10]中，提出一种利用移存器的状态和长码密钥之间的线性关系，通过 2 元域的方程组求解用户掩码的方法。

从式(2)和(3)可知

$$k_i = d_{64i} = m_1 s_{64i}(1) \oplus m_2 s_{64i}(2) \oplus \cdots \oplus m_{42} s_{64i}(42) \tag{10}$$

式(10)也可以写成向量直积形式

$$k_i = \boldsymbol{S}_{64i} \cdot [m_1 \quad m_2 \quad m_3 \quad \cdots \quad m_{42}]^{\mathrm{T}} = [s_{64i}(1) \quad s_{64i}(2) \quad s_{64i}(3) \quad \cdots \quad s_{64i}(42)] \cdot \begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ \vdots \\ m_{42} \end{bmatrix} \tag{11}$$

式中：$(m1, m2, m3, \cdots, m42)$表示用户 42 位私人掩码，$k_i$ 表示第 i 时刻的密钥码元，向量 $\boldsymbol{S}_{64i}$ 表示第 $64i$ 时刻长码产生器的 42 位状态。为了求解 42 私人掩码，取 42 个时刻的密钥码元，根据式(11)，可以列出一个 42 元一次方程组

$$\begin{bmatrix} s_{64}(1) & s_{64}(2) & s_{64}(3) & \cdots & s_{64}(42) \\ s_{128}(1) & s_{128}(2) & s_{128}(3) & \cdots & s_{128}(42) \\ s_{192}(1) & s_{192}(2) & s_{192}(3) & \cdots & s_{192}(42) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{64\times42}(1) & s_{64\times42}(2) & s_{64\times42}(3) & \cdots & s_{64\times42}(42) \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ \vdots \\ m_{42} \end{bmatrix} = \begin{bmatrix} k_1 \\ k_2 \\ k_3 \\ \vdots \\ k_{42} \end{bmatrix} \tag{12}$$

在 N-CDMA 系统的同步信道总是不断地广播系统特定时刻的长码产生器的状态[11]，因此，破译者可以设计一个长码产生器与基站的长码产生器的状态严格同步。换句话说，破译者在从密文中求解出 42 位密钥码元的同时，可以已知长码产生器对应时刻的状态信息。

用增广矩阵法解这个方程组，用 $\boldsymbol{AX}=b$ 表示等式(12)，若矩阵 $\boldsymbol{A}$ 是可逆的，则 $\boldsymbol{AX}=b$ 的增广矩阵 $(\boldsymbol{A}, b)$可通过行变换转换成$(\boldsymbol{E}, \boldsymbol{A}^{-1}b)$形式，这里 $\boldsymbol{E}$ 是一个单位阵，$\boldsymbol{A}^{-1}b$ 就是方程组的解

$$\begin{bmatrix} s_{64}(1) & s_{64}(2) & s_{64}(3) & \cdots & s_{64}(42) \\ s_{128}(1) & s_{128}(2) & s_{128}(3) & \cdots & s_{128}(42) \\ s_{192}(1) & s_{192}(2) & s_{192}(3) & \cdots & s_{192}(42) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{64\times42}(1) & s_{64\times42}(2) & s_{64\times42}(3) & \cdots & s_{64\times42}(42) \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \\ k_3 \\ \vdots \\ k_{42} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & m_1 \\ 0 & 1 & 0 & \cdots & 0 & m_2 \\ 0 & 0 & 1 & \cdots & 0 & m_3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & m_{42} \end{bmatrix} \tag{13}$$

注意这里的行变换是在伽罗华域 GF(2)做模 2 加变换。式(13)右边矩阵最后一列即求解出的用户私人掩码。

4 N-CDMA 安全架构的改进

以上的分析表明，针对敌意的安全攻击，N-CDMA 给用户提供的话音保密非常脆弱。导致系统安全脆弱的原因，不是长码产生器的复杂度不够，而是长码产生器与前向业务信道之间不匹配造成。在图 1 中，信息被加密是在信道编码之后，而卷积编码、码元重复和块交织会导致明文信息出现冗余度和周期反复。已知的唯密文攻击方法均是利用 N-CDMA 系统的明文存在冗余度这个缺陷进行攻击的。文献[3,12,13]讨论了 CDMA 系统的几种新的加密方法。本文在不改变 IS-95 标准长码产生器结构的基础上，提出一种既加强了系统的安全性又兼顾了系统的兼容与可实施性的改进 N-CDMA 系统安全架

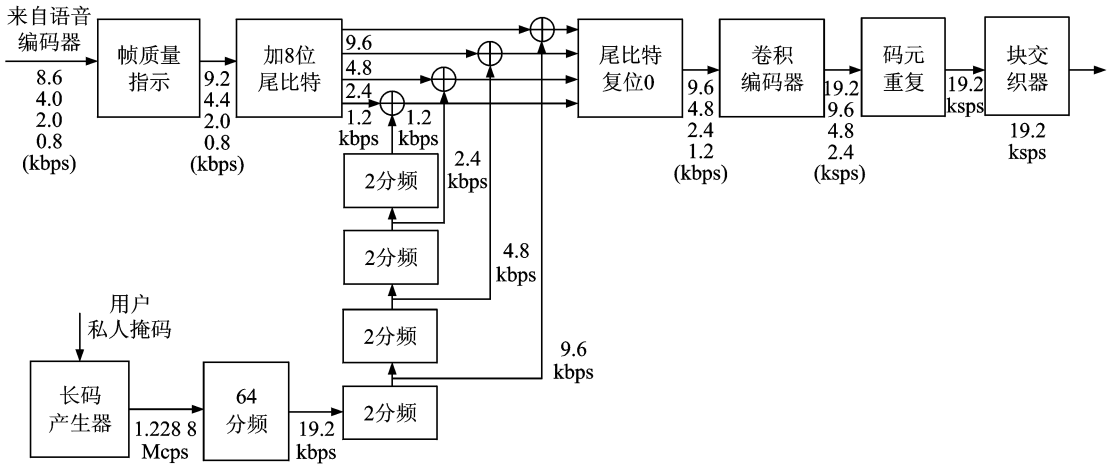

图 3 改进后的前向业务信道基带编码结构

Fig. 3 Proposed enhancement scheme of scrambling

构,见图 3。在图 3 中,为了抵御针对明文冗余度的唯密文攻击,明文信息在信道编码之前被长码序列扰乱加密,这样,就很好地消除了明文信息帧的冗余及周期反复特性。由于卷积编码之前,信息帧有 4 种速率分别为:9.6,4.8,2.4,1.2 kbps,因此,19.2 kbps 长码需要经过四次二分频与信息帧适配。在加扰之前进行加尾比特,目的是使 4 种信息帧的速率呈倍数关系。由于加扰后每帧尾比特不再为 0,需要对每帧尾 8 位重新复位为 0。

5 结束语

本文证明了 N-CDMA 移动通信系统是不安全的。需要指出的是:本文并没有用提出的唯密文攻击方法去攻击符合 IS-95 标准的真实通信系统,也无意破坏对现有的商业移动通信系统的安全架构。同时 N-CDMA 系统已经由 IS-95 标准演进为 CDMA 2000 1x 标准,在下一代移动通信系统中改进的加密算法已经提出[14]。本文的目的是以 N-CDMA 的安全架构为背景探讨新的密码分析方法,为 3G 乃至更新的移动通信系统的设计提供经验。

参考文献:

[1] TIA/EIA-95-B. Mobile station-base station compatibility standard for dual-mode spread spectrum systems[M]. Washington, America: ANSI Publication Version, 1998.

[2] Gray V K. IS-95 CDMA and CDMA2000[M]. Upper Saddle River, NJ: Prentice Hall, 2000.

[3] Li Tongtong, Ling Qi, Ren Jian. Physical layer built-in security analysis and enhancement algorithms for CDMA systems [J]. Eurasip Journal on Wireless Communications and Networking, 2007, 2007:1-8.

[4] Zhang Muxiang, Carroll C, Chan A H. Analysis of IS-95 CDMA voice privacy[C]// Seventh Annual Workshop on Selected Areas in Cryptography. Ontario, Canada: Springer, 2000:1-13.

[5] Ryu D H, Jang S J. A security weakness of the CDMA(code division multiple access)cellular service[J]. International Journal of Computer Science and Network Security, 2006,6(5B):218-225.

[6] 万哲先. 代数与编码[M]. 3 版. 北京:高等教育出版社,2007:220-220.
Wan Zhexian. Algebra and coding[M]. 3Ed. Beijing: Higher Education Press, 2007:220-220.

[7] Kim S C, Lee B G. Parallel scrambling techniques for multibit-interleaved multiplexing environments[C]// PROC ICC'93. Geneva: [s. n.], 1993:1526-1530.

[8] Lee B G, Byoung-Hoon Kim. Scrambling techniques for CDMA communications[M]. New York: Springer International Series in Engineering and Computer Science, Kluwer Academic Publishers, 2001.

[9] Massey J. Shift-register synthesis and BCH decoding[J]. IEEE Transactions on Information Theory, 1969, 15(1): 122-127.

[10] 陈德宏,刘梅. 一种求解延迟型 m 序列线性组合的新算法[J]. 数据采集与处理, 2014, 29(3): 339-444.
Chen Dehong, Liu Mei. A new algorithm of multiplex problem for delayedm-sequence[J]. Journal of Data Acquisition and Processing, 2014, 29(3): 339-444.

[11] He Jiaming, Zeng Xingbin, Xu Bensong. A new CDMA long code fast computing method[C]// The IEEE-Siberian Conference on Control and Communications. [S. l.]: IEEE, 2003: 146-151.

[12] Falahati A, Tafaroji M, Mashreghi M. Security enhancement in CDMA with a hidden direct sequence spread spectrum system[J]. IEEE Trans Magn Japan, 2006, 2: 2524-2529.

[13] Krishna Bharathi L, Sudha G F. Security enhancement using mutual authentication in existing CDMA systems[J]. International Journal on Computer Science and Engineering, 2010, 2(2): 237-245.

[14] Mohammed A M, Mohamed M. Abd E, et al. Security analysis and enhancement of authentication in CDMA based on elliptic curve cryptography[J]. Research Journal of Information Technology, 2012, 4(3): 106-123.

作者简介:

陈德宏(1965-),男,副教授,研究方向:通信系统总体设计、数字语音编码、密码分析,E-mail: cdh@ahut.edu.cn。

刘晓东(1971-),男,博士,教授,研究方向:电力电子自动化、新能源开发与应用、DC-DC 功率变换器及其控制技术、功率变换技术。

刘梅(1987-),女,硕士研究生,研究方向:信息安全。