DOI:10.3969/j.issn.1006-6403.2012.12.016

LTE系统中SNOW 3G算法的原理分析与实现

[李小文 刘芳]

摘要 介绍了从2G系统到4G系统加密算法设计的不断改进和完善的过程，重点对SNOW 3G保密性和完整性算法的原理与实现过程进行了阐述，分析了算法的性能，最后在VC环境下仿真出了该保密性和完整性算法的测试结果。

关键词： 长期演进 加密算法 完整性保护算法 SNOW3G

李小文
重庆邮电大学 计算机科学与技术学院。
刘芳
重庆邮电大学 计算机科学与技术学院。

技术交流

引言

通信技术日益普及，人们对通信过程的机密性和完整性的不断提出更高的要求，安全性算法的的设计逐步完善，经历了KASUMI算法、SNOW 2.0算法到SNOW 3G算法的演进过程。SNOW 3G算法作为LTE系统的加密算法，其安全性更优于SNOW 2.0，且能够适应高速率通信。

1 加密算法的演进

1.1 功能演进简述

从2G到3G，在安全特征与安全服务方面逐步完善，2G系统身份认证和加密算法等方面存在着很多隐患，比如没有考虑到数据完整性保护问题，这样数据在传输中很容易被篡改。3G系统中保留了2G系统的安全优点，并且提出保证空中接口数据传输保密性和完整性的要求，使数据不被窃听和篡改。LTE系统更多是沿用了第三代移动通信系统的安全策略，另外提供了一种更高速率的服务，这就对网络的安全性也提出了更高的要求，不仅要有强大的抗攻击能力，还要适应高速率通信的特点。

为了实现安全需求，3GPP提出了加密算法f8和完整性保护算法f9，f8和f9（UEA2和UIA2）核心部件有两种KASUMI算法和SNOW 3G。目前在LTE系统中则采用了SNOW3G加密算法，它是SNOW 2.0的升级版本。

1.2 UEA2设计演进[1]

对于3GPP这第二套密码算法SNOW 3G具有与前一套同样的功能和安全需求，并且是从基于KASUMI的f8/f9中分离出来的，唯一的修改是它支持10 Mbit/s的输出。SNOW 3G 源于SNOW 2.0而设计的，SNOW 2.0的很多有效的安全性能被直接继承下来，然而SNOW 2.0的时间复杂度是2^{50}，并且输出不多于1000字节，因此很容易受到代数攻击，为了弥补这一缺点增加了寄存器R3，S-Box S2的设置和增加的寄存器S3改善了系统对抗攻击的能力。如图1，FSM函数循环图增加了寄存器R3:

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

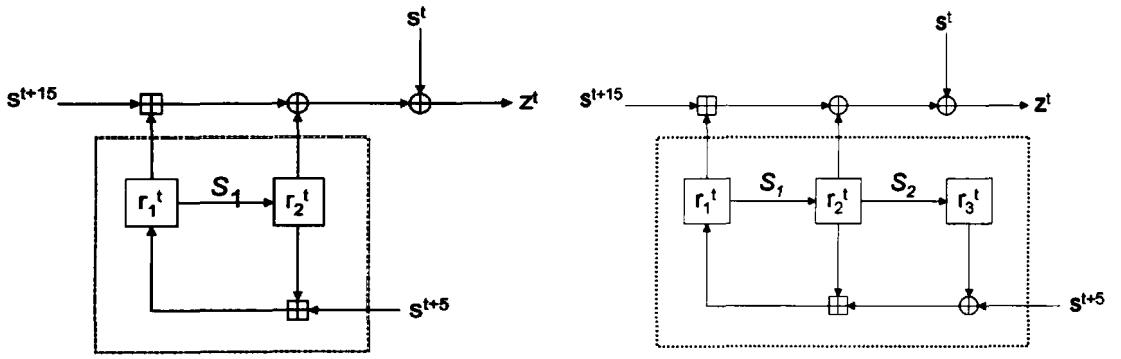

图1 FSM函数循环图

2 SNOW 3G加密算法设计

2.1 SNOW 3G操作说明[2]

运算符注释:

= 赋值

⊕ 异或

+ 整数和模2^{32}

|| 连接符

<<nt 在n-bit寄存器中左移t-bit

2.1.1 基本函数

(1) MULx函数

这是一个将16bits数据转换为8bits数据的函数。

设：V是一个16bits数据的高8位，c是该16bits数据的低8位。

当V最高位为1，MULx(V,c) = （V $<<_8$1）+c，否则，MULx(V,c) = V $<<_8$1

(2) MULxPOW函数

该函数的输入为一个16bits数据与一个正整数，经过转换，输出为一个8bits数据。

设：V是一个16bits数据的高8位，c是该16bits数据的低8位，i为正整数。

当i=0时，MULxPOW(V,i,c) = V

否则，MULxPOW(V,i,c) = MULx(MULxPOW(V, i - 1, c), c)（其中i>1时该函数递归）

(3) MUL函数

该函数将192bits映射成为64bits。另V、P、c均为64-bit输入。

计算过程：首先另result=0,

再for i= 0 to 63

if((P>>64 i)& 640x01)

result=result+ MULxPOW(V, i, c)

(4) 线性反馈移位寄存器（LFSR）

LFSR包括16部分s_0,s_1,s_2 ……s_{15}每部分32bits。

(5) 有限状态机（FSM）

有限状态机包含三个32bits寄存器，R1,R2和R3。S-boxes S_1和S_2更新寄存器R2和R3:

a.32x32-bit S-BoxS_1:

S-BoxS_1将一个32-bit输入转化为32-bit输出。

令w = w_0 || w_1 || w_2 || w_3（本处为R1），32-bit输入以w_0开头以w_3结尾。

令$S_1(w)$= r_0 || r_1 || r_2 || r_3，以r_0开头r_3结尾。

b.32x32-bit S-BoxS_2:

S-BoxS_2将一个32-bit输入转化成32-bit输出。

令w = w_0 || w_1 || w_2 || w_3（本处为R2），32-bit输入以w_0开头以w_3结尾。

令$S_2(w)$= r_0 || r_1 || r_2 || r_3，以r_0开头r_3结尾。

2.1.2 计时操作

(1) LFSR时钟

LFSR计时有两种不同的模式，初始模式和密钥流模式。在初始化模式中，LFSR 接收一个32-bit输入字F,它是FSM的输出；而密钥流模下，LFSR不接收任何输入。这里用到两种函数MUL_α和DIV_α

函数MUL_α:

函数MUL_α映射8 bits成为32 bits。

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

设C为8-bit输入,则 MUL 定义为:

$MUL_{\alpha}(c)$ =(MULxPOW(c, 23, 0xA9) || MULxPOW(c, 245, 0xA9) || MULxPOW(c, 48, 0xA9) || MULxPOW(c, 239, 0xA9))

函数DIV_{α}:

函数DIV_{α}映射8 bits成为32 bits。

设c为8-bit输入,则DIV_{α}定义为:

$DIV_{\alpha}(c)$ =(MULxPOW(c, 16, 0xA9) || MULxPOW(c, 39, 0xA9) || MULxPOW(c, 6, 0xA9) || MULxPOW(c, 64, 0xA9))

(2) FSM时钟

FSM有两个输入字s_{15} 和s_5、其来自LFSR。它产生一个32-bit输入字。

F: F = (s_{15} R1) +R2, 然后寄存器更新数据。

计算中间值r如下: r = R2 (R3 +s_5),

令: R3 = S2(R2),

R2 = S1(R1),

R1 = r

2.2 SNOW 3G运算

SNOW 3G是一种面向字的流加密算法、输入为128bits的密钥Key和128bits的矢量IV, 产生以32位字为单位的密钥流、该密钥流与明文异或后得到密文。下面介绍SNOW 3G的核心算法UEA2和UIA2[3]。

2.2.1 UEA2

该加密算法将参数COUNT、BEARER、DIRECTION跟CK一同作为输入来初始化, 设 $L=\lceil LENGTH/32 \rceil$, 产生的密钥流由32比特的$Z_1$……$Z_L$组成, 其中$Z_1$由KS[0]…KS[LENGTH-1]构成, 例如KS[0]是Z_1最高位KS[31]是其最低位。

加密过程: 设整数i、0<=i<=LENGTH-1, OBS[i]=IBS[i] +KS[i] (OBS为输出流, IBS为输入流)

(1) 初始化

SNOW 3G被初始化通过一个128-bit密钥包含4个32-bit字k_0, k_1, k_2, k_3和一个128-bit的初始变量包含4个32-bit字IV_0, IV_1, IV_2, IV_3如下:

① 置LFSR

s15 = k3 +IV0 s14= k2 s13 = k1 s12 = k0 +IV1 s11 = k3 +1

s10= k2 +1 +IV2 s9 = k1 +1 +IV3

s8 = k0 +1 s7 = k3 s6= k2 s5 = k1 s4 = k0s3 = k3 +1 s2= k2+1 s1 = k1 +1 s0 = k0 +1

② FSM被初始化为R1 = R2 = R3 = 0

③ 加密在没有输出的特殊模式下运行:

重复32-times{STEP 1: FSM 被计时产生32-bit字F

STEP 2: LFSR 被计时在初始模式,消耗F}

初始化过程如图2所示:

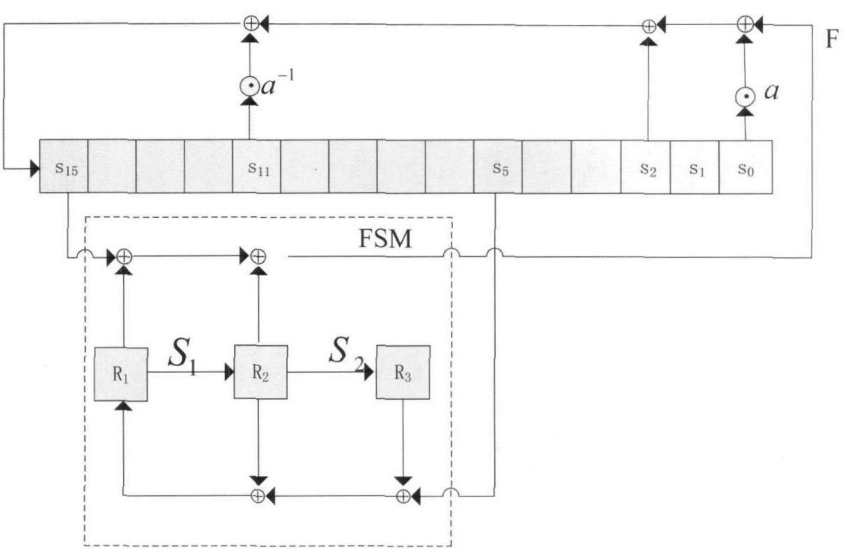

图2 初始化过程

(2) Keystream的产生

①计时FSM一次, FSM的输出字被丢弃

②FSM在密钥流模式被计时一次

2-bit 字的密钥流被产生:

for t = 1 to n{

STEP 1: 计时FSM, 并产生一个32-bit的输出字F

STEP 2: 下一个密钥流进行一次计算: zt = F+s_0

STEP 3: LFSR 被计时, 采用密钥流模式}

密钥流产生过程如图3所示:

©1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

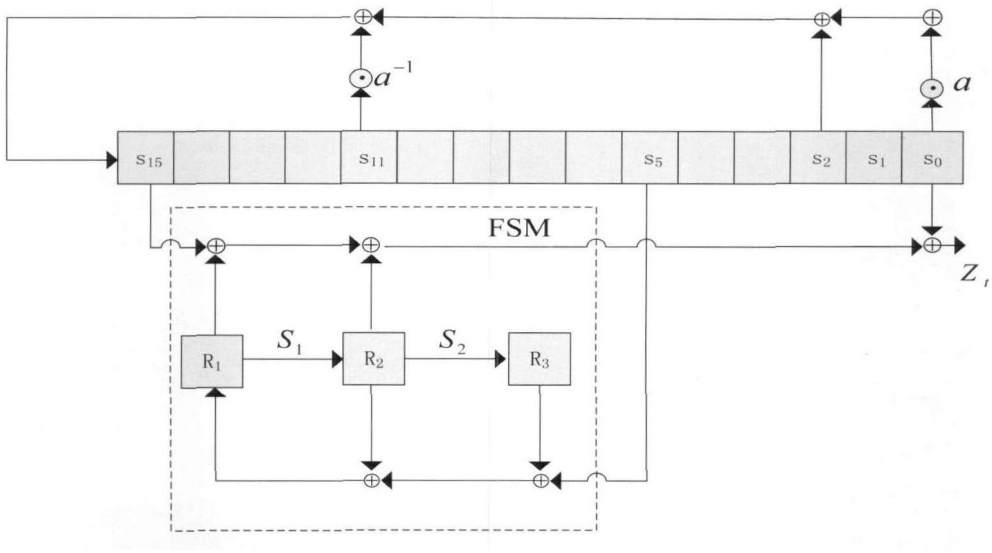

图3 KeyStream产生过程

2.2.2 UIA2

该完整性保护算法用于产生32-bit的MAC-I值，其输入信息有完整性密钥IK和矢量IV，产生$Z_1Z_2Z_3Z_4Z_5$、组成三个随机值64-bit的P、Q和32-bit的OPT、被完整性保护的信息长度可在1bit到2000bits之间。

完整性保护过程[1]：

设 $D=\lceil LENGTH/64\rceil+1$

设P=$Z_1||Z_2$、Q =$Z_3||Z_4$

再另Z_5=OPT[0]||OPT[1]||…||OPT[31]

当0<=i<=D-3时:

设：M_i=MESSAGE[64i]||MESSAGE[64i+1]||… ||MESSAGE[64i+63]

故 M_{D-2}= MESSAGE[64i（D-2）]||…||MESSAGE[LENGTH-1]|| 0…0

M_{D-1}=LENGTH[0]||LENGTH[1]||… || LENGTH[63] (LENGTH[0]LENGTH[1]…LENGTH[63]代表LENGTH的64bits)

EVAL_M过程:

设64-bit的EVAL值为0。

当0<=i<=D-2时：EVAL=MUL（EVAL+M_i、P、0x0000000000000001b）

置EVAL=EVAL+MD-1

又另EVAL=MUL（EVAL、Q、0x0000000000000001b）

将EVAL写成EVAL=$e_0e_1\cdots e_{63}$形式。

当0<=i<=31时：MAC-I［i］=ei+OPT[i]($e_{32}\cdots e_{63}$被丢弃)

完整性保护过程如图4所示:

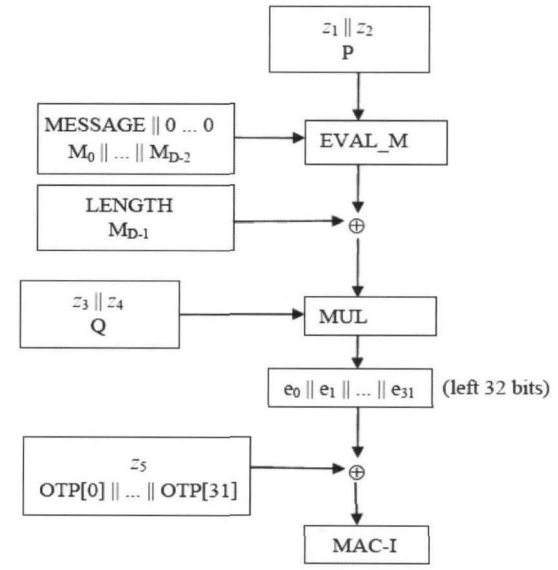

图4 完整性保护算法

2.3 加密算法性能[4]

2.3.1 LFSR

在SNOW 3G算法中，LFSR存储s_0，s_1，…，s_{15}这16个数据，均为32bits、共512bits。其反馈多项式为:

$$f(x)=\alpha x^{16}+x^{14}+\alpha^{-1}x^5+1$$

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

而

$$\alpha = \sqrt{x^4 + \beta^{23}x^3 + \beta^{245}x^2 + \beta^{48}x + \beta^{239}}$$

其中

$$\beta = \sqrt{x^8 + x^7 + x^5 + x^3 + 1}$$

该反馈多项式在尽量保证性能的同时也能保证相对高的安全性。

2.3.2 非线性函数

非线性组合函数可使密钥流具有高线性复杂度和良好的统计性、从而保证了密钥流的安全强度和密码性质。

FSM：FSM是由3个32bits的寄存器和两个S-Box以及相关操作组成的。其运算过程大致是：FSM的输入来自LFSR中两个寄存器、S-Box S_1和S_2进行运算、得到一个32-bit字、再与LFSR中的s_0异或、输出密钥流。S-Box S_2的设置和增加的非线性寄存器S_3使攻击无法消除方程中的中间变量，因此算法的健壮性更好。

2.3.3 S-Box

S-Box都经过特别设计的，密码算法中的地位相当重要、整个算法的密码强度由它决定。S-Box S_1是基于8*8的RijndaelS_R、S-Box S_2是基于8*8的DicksonxS_Q、都是为了减小数据的线性相关性而做了特殊的设计。

3 算法实现与测试

3.1 保密性的实现

该程序由头文件、保密性函数和主函数组成。保密性函数是整个程序的核心、定义了自定义函数的函数体、完成了算法的密钥流的产生，密钥流与明文异或产生了密文[5]。

依测试规范[1] [6] [7]：

COUNT-C = 72A4F20F,

Bearer = 0C , Direction = 1,

CK = 2B D6 45 9F 82 C5 B3 00 95 2C 49 10 48 81 FF 48,

Length = 798bits,

Keystream: F22DB45B 37E71C5B

4EB6F404 CD886C15

9DCA27BA F062AF46

F8E2F587 8976E8B8

33E2B848 E798968D

85E5961A 057983F1

10F55076 71185285

D53CED16 FD580500

7BEE12BE 1C5C52EC

78C12E8A C5B1B9D5

3BF90900 DF06DF63

3C3C15D5 C270DE52

FB4D09C0

VC中的实现如图5所示：

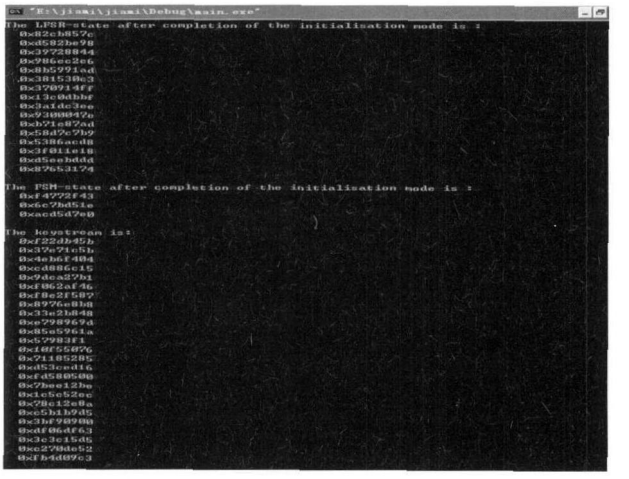

图5 保密性测试结果

3.2 完整性的实现

该程序依然由头文件、完整性函数和主函数组成。完整性函数的整个程序的核心、定义了自定义函数的函数体、最后产生MAC-I值。

依测试规范[1] [6] [7]：

COUNT-C = 3EDC87E2,

FRESH = A4F2D8E2 , Direction = 1,

IK = D4 2F 68 24 28 20 1C AF CD 9F 97 94 5E 6D E7 B7,

Length = 254bits,

MESSAGE: B5924384328A4AE00B737109F8B6C8DD 2B4DB63DD533981CEB19AAD52A5B2BC0,

EVAL: E7354091 E1B57157

655CA81A A179F483

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

E6E0FD58 B1B4BA89

9BC353AA 5FE30866

9BC353AA 5FE30898,

Multiply by Q: EVAL= DC8378CD FD41FE17,

MAC-I:: FC7B18BD

VC中的实现如图6所示:

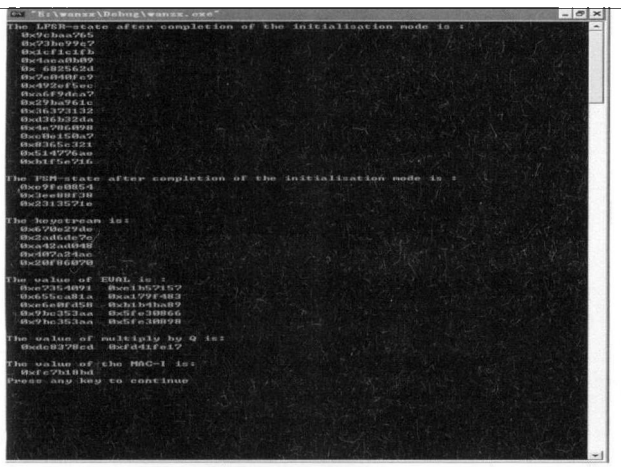

图6 安全性测试结果

4 结论

本文介绍了加密算法设计的改进过程，重点对SNOW 3G加密算法的实现原理进行了详细的分析，并通过了基于TTCN标准[8] [9]的测试。SNOW 3G作为LTE的核心算法，为系统的空中接口数据传输提供了保密性和完整性保障，促进了移动通信领域各项业务的发展，因此得到了广泛的应用。当然对于这个复杂的系统还有很多可提高和完善的空间，对其各功能模块还需要进行不断地改进。

参考文献

1 Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2.Document 5: Document and Evaluation Report(V1.1)2006-09-06.

2 Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2.Document 2: SNOW 3G Specification（V 1.1）2006-09-06

3 Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2.Document 1: UEA2 and UIA2 Specification(V1.1)2006-09-06.

4 张玉安，冯登国. 浅论序列密码算法中的几个亮点[J]. 信息安全与通信保密，2002，（1）：32-34

5 张洪铭，何登平. 基于LTE系统的SNOW 3G加密算法研究[J]. 电视技术，2010,34(12)：91-93.

6 Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2 Document 3: Implementors' Test Data(V1.0)2006-01-10.

7 Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2&UIA2 Document 4: Design Conformance Test Data.V(1.0)2006-01-10

8 3GPP TS 36.523. Protocol conformance specification(Release8)2009-09

9 3GPP TS 33.401.3GPP System Architecture Evolution(SAE): "Security architect" (V8.50)[EB/OL]. E2009-09.

(收稿日期：2012-11-13)

（上接第39页）

部署CSFB及MTRF功能，在部署MSC Pool的情况下，每个MSC Pool内可以选择1个或2个MSC改造支持CSFB功能，其他MSC仅改造支持 MTRF功能用以处理TA跨越MSC Pool时的被叫业务。不建议采用限制无线区域划分以及IWF方式。

4 小结

电路域回落是目前被广泛接受的一种为LTE用户提供话音业务的方式。CSFB方式话音业务需要EPC、电路域、分组域、HLR/HSS及无线网的共同支持，其中MSC的改造范围主要取决于CSFB被叫业务需求，重点在于解决TA内LA归属不同MSC造成被叫失败的问题。通过对各种方案进行分析，得出MTRF是相对较佳的方式，设备改动范围小同时时延相对较短，建议进行部署。

参考文献

1 周彦，武欣. TD-LTE CSFB话音解决方案研究.移动通信 2011年19期

1 冯征，刘蕾，牛晓丹.LTE语音解决方案跟踪研究，院内课题KY2001JI08

3 李侠宇. EPS网络CS FallBack技术研究，电信网技术. 2009年6期

4 3GPP TS 23.272, Circuit Switched Fallback in Evolved Packet System

5 3GPP TS 23.018, Basic Call Handling

（收稿日期：2012-11-21）

技术交流

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net