序列密码算法安全

冯秀涛
中科院系统所

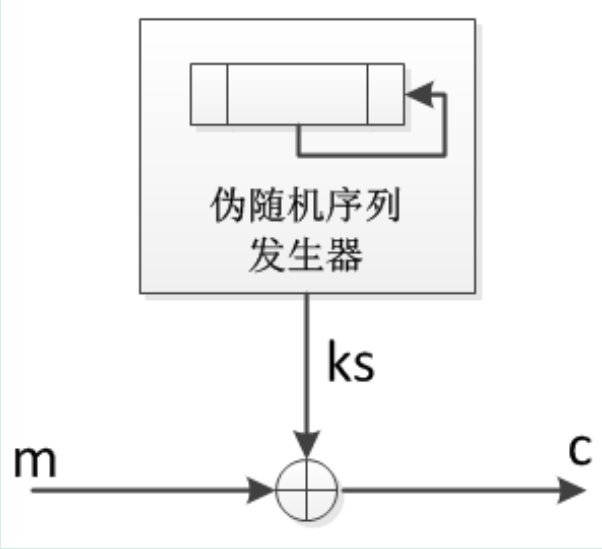
目录

序列密码

- 密码技术是信息安全的关键技术之一。序列密码是主流密码体制之一。同分组密码相比，序列密码具有实现简单，效率快，成本低等优点，被广泛用到现代网络通信中保护通信数据的安全。
- 对于网络系统，密码安全是网络安全的基石。尽管密码安全并不等于网络安全，但是如果密码不安全，其对整个网络系统安全而言将是灾难性的。因此从这个角度来看，研究密码安全对网络安全具有重要意义。

序列密码

- 序列密码是一种依赖时间而变换的对称密码函数。其通常由一个伪随机发生器和一个掩码函数组成，前者产生具有一定长度的伪随机数，后者将明文数据直接和产生的伪随机数相互作用产生对应的密文数据。这里掩码函数通常是异或操作。



序列密码

- 序列密码自提出至今已有百年历史，其属于传统密码学研究领域，已有深厚的研究积累和丰富的研究成果。当前重点关注序列密码仍具有如下一些特殊意义：
  - 近年来，移动通信网、卫星导航网、物联网得到飞速发展，这些系统中的保密通信需要用到序列密码体制，这使得序列密码的地位显著提高。
  - 欧洲NESSIE计划(2000~2004)和ECRYPT计划(2004~2008)极大推动了序列密码的发展。在序列密码领域涌现了许多新的设计思想。例如向量化序列密码的设计以及分组密码设计技巧在序列密码设计中的应用等。这些新思想同时也带来了大量的新型安全问题。然而当前国际上对这些新型思想和新型安全问题的讨论还远不够成熟。

序列密码

- 物联网和卫星导航网应用的快速发展与国家密码标准制定的滞后之间的矛盾突出。国家目前尚未制定轻量级的序列密码标准，国内已未见有成熟的轻量级序列密码算法的提出。标准制定的滞后会限制相关应用的发展，并在一定程度上影响整个行业的发展。

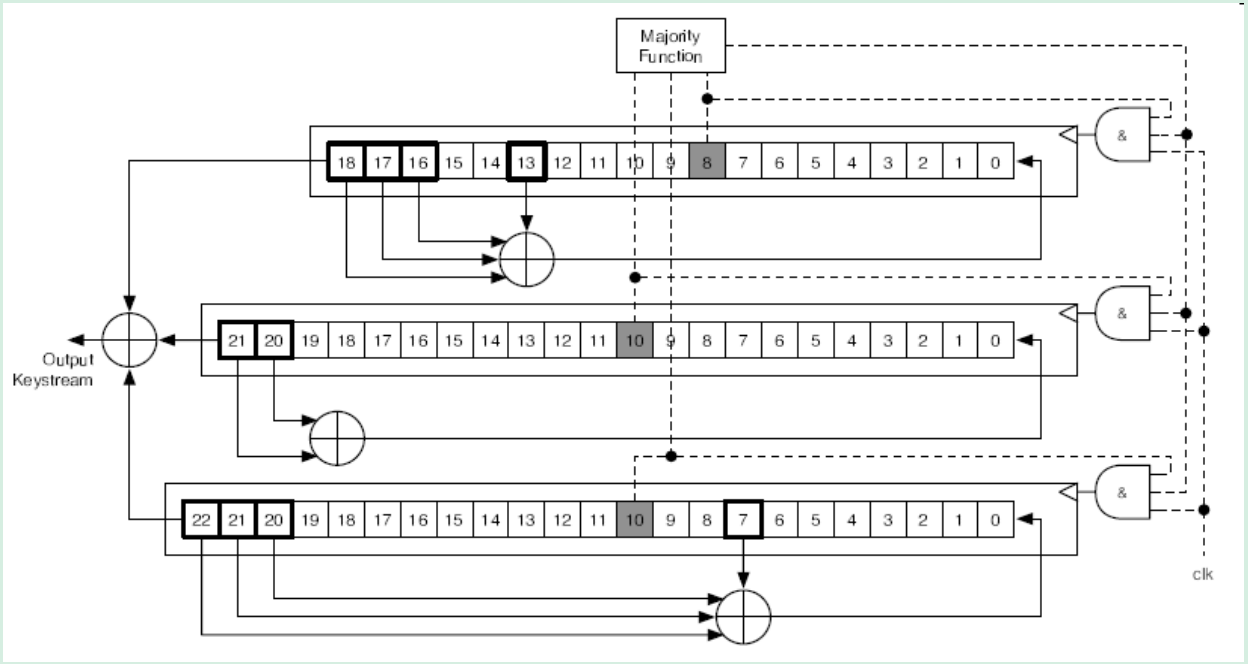
- 当前序列密码正朝着标准化、综合化方向发展。受密码理论和工业应用的双重驱动，对高安全、高效率、低功耗、低成本的新型序列密码体制的需求日益凸显。

目录

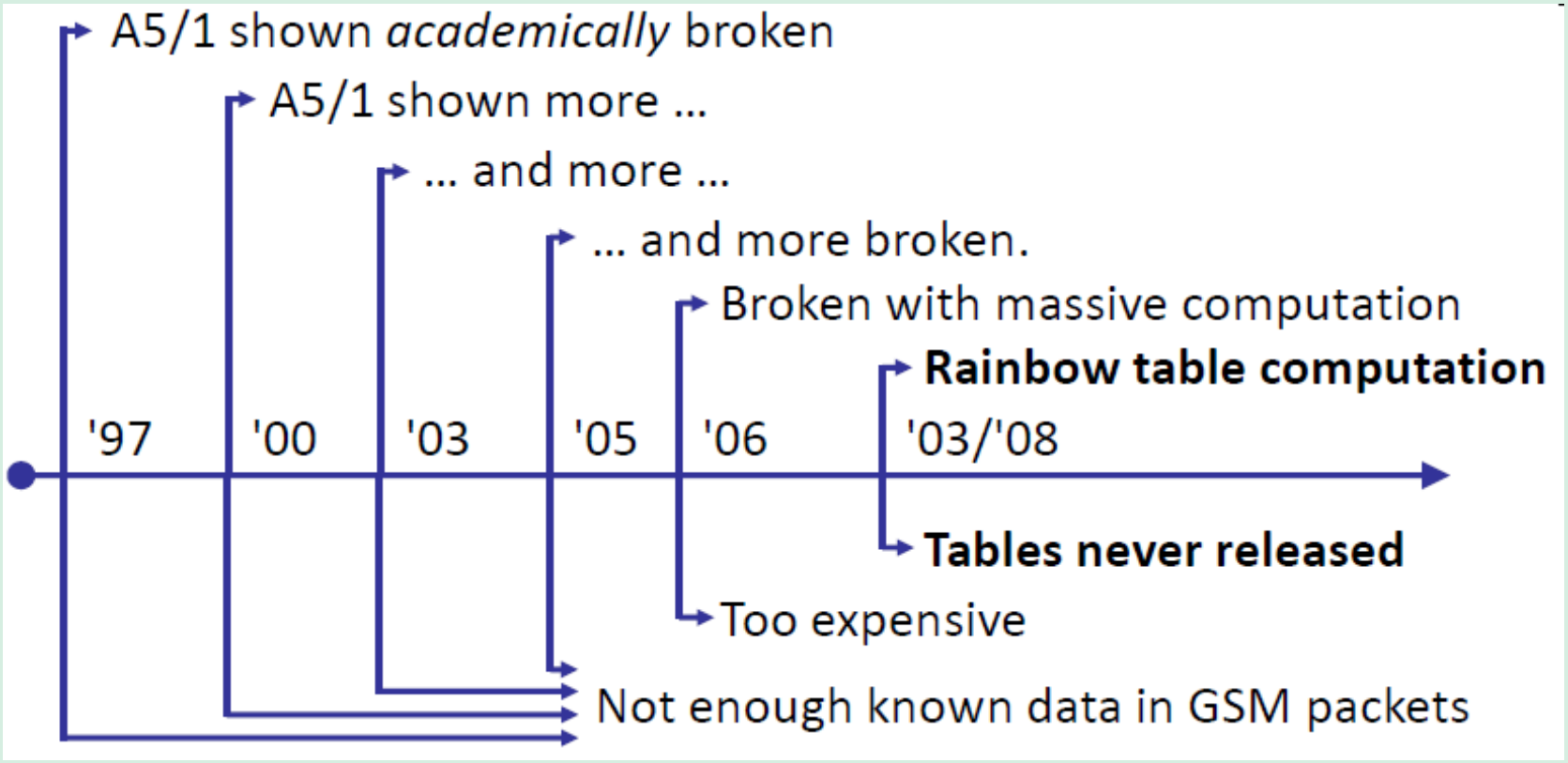
- 相关背景
- 典型序列密码算法
- 已取得的阶段性成果

GSM加密标准A5/1

- A5/1是由3个LFSR（19级、22级、23级）组成的钟控生成器，其密钥长度为64比特，初始向量为22比特。



A5/1 安全现状


A5/1 shown *academically* broken
A5/1 shown more ...
... and more ...
... and more broken.
Broken with massive computation
Rainbow table computation
'97
'00
'03
'05
'06
'03/'08
Tables never released
Too expensive
Not enough known data in GSM packets

A5/1存在的安全缺陷

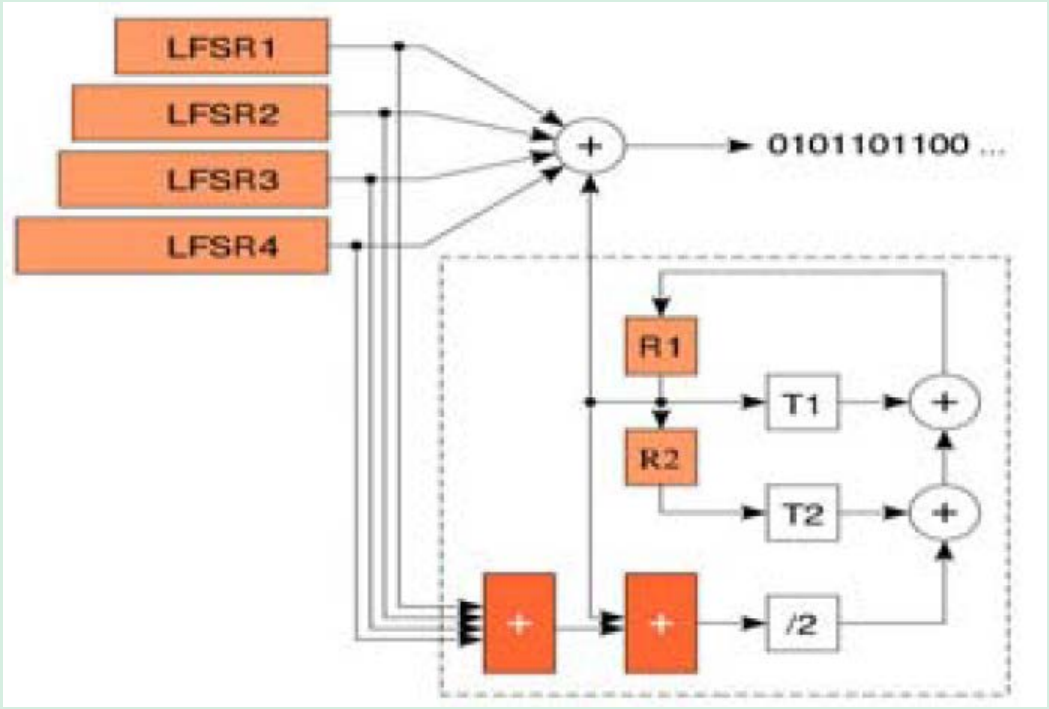
- A5/1属于钟控设计，其主要攻击手段有：
  - 相关攻击
  - 猜测确定攻击
  - 存储数据时间折衷攻击

- A5/1的主要设计缺陷在于：记忆单元规模较小，不能提供与种子密钥长度等级的安全强度，容易受到猜测确定攻击和时间存储数据折衷攻击。

1. J. Golic. Cryptanalysis of Alleged A5 Stream Cipher. Eurocrypt’ 97, LNCS 1233, pp.239–255, 1997.
2. E. Biham and O. Dunkelman. Cryptanalysis of the A5/1 GSM Stream Cipher. Indocrypt’ 00, LNCS 1977, 2000.
3. A. Biryukov, A. Shamir, and D. Wagner. Real Time Cryptanalysis of A5/1 on a PC. FSE’ 00, LNCS 1978, pp.1–18, 2001.
4. A. Maximov, T. Johansson, and S. Babbage. An Improved Correlation Attack on A5/1. SAC’ 04, LNCS 3357, pp.239–255, 2005.

蓝牙加密标准E0

- E0有4个LFSR，分别为25级、31级、33级和39级，种子密钥长度为128比特。



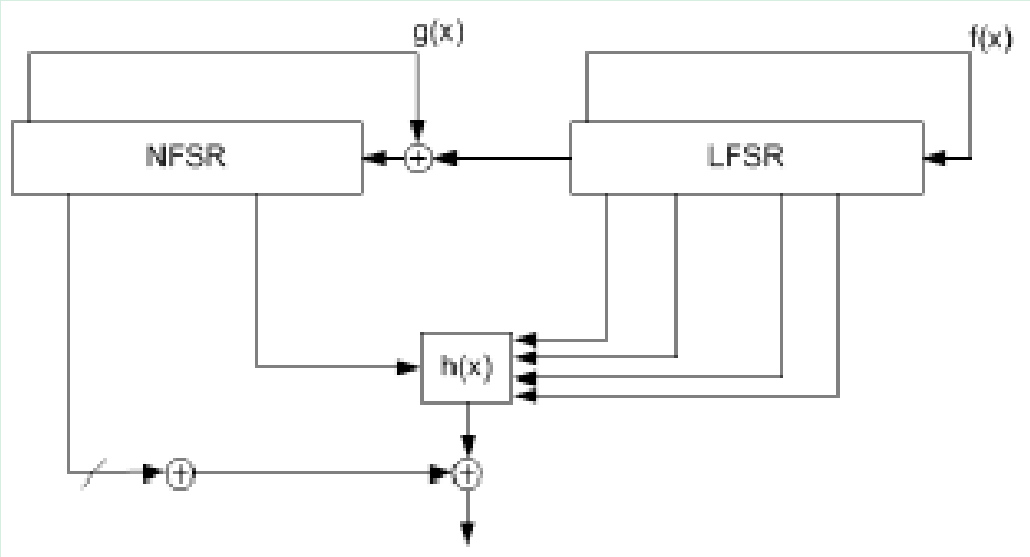
E0 存在的安全缺陷

- E0属于带少量记忆比特的过滤生成器结构，容易受到相关攻击和代数攻击。
- E0中非线性部件仅含2比特记忆单元，很容易通过联立多个方程消去上述2比特记忆单元变量，从而转化成经典的过滤生成器。
- 非线性部件设计过于简单，容易受到区分攻击、相关攻击、代数攻击等方法的攻击。

1. Scott R. Fluhrer, Stefan Lucks, Analysis of the E0 encryption System, SAC 2001, LNCS 2259, pp.38-48, 2001.
2. Frederik Armknecht, A linearization attack on the bluetooth key stream generator.
3. Lu Yi, Serge Vaudenay, Cryptanalysis of Bluetooth Keystream Generator Two-Level E0, Asiacrypt2004, pp.483–499, 2004.
4. Lu Yi, Serge Vaudenay, Faster Correlation Attack on Bluetooth Keystream Generator E0, CRYPTO2004, pp.407–425, 2004.
5. Lu Yi, Willi Meier, Serge Vaudenay, The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption, CRYPTO 2005, LNCS 3621, pp. 97–117, 2005.

eSTREAM计划胜选算法Grain

- Grain由瑞典学者Martin Hell、Thomas Johansson和瑞士学者Willi Meier共同设计，其密钥长度为80比特、初始向量长度为64比特，包含NFSR(80级)和LFSR(80级)。



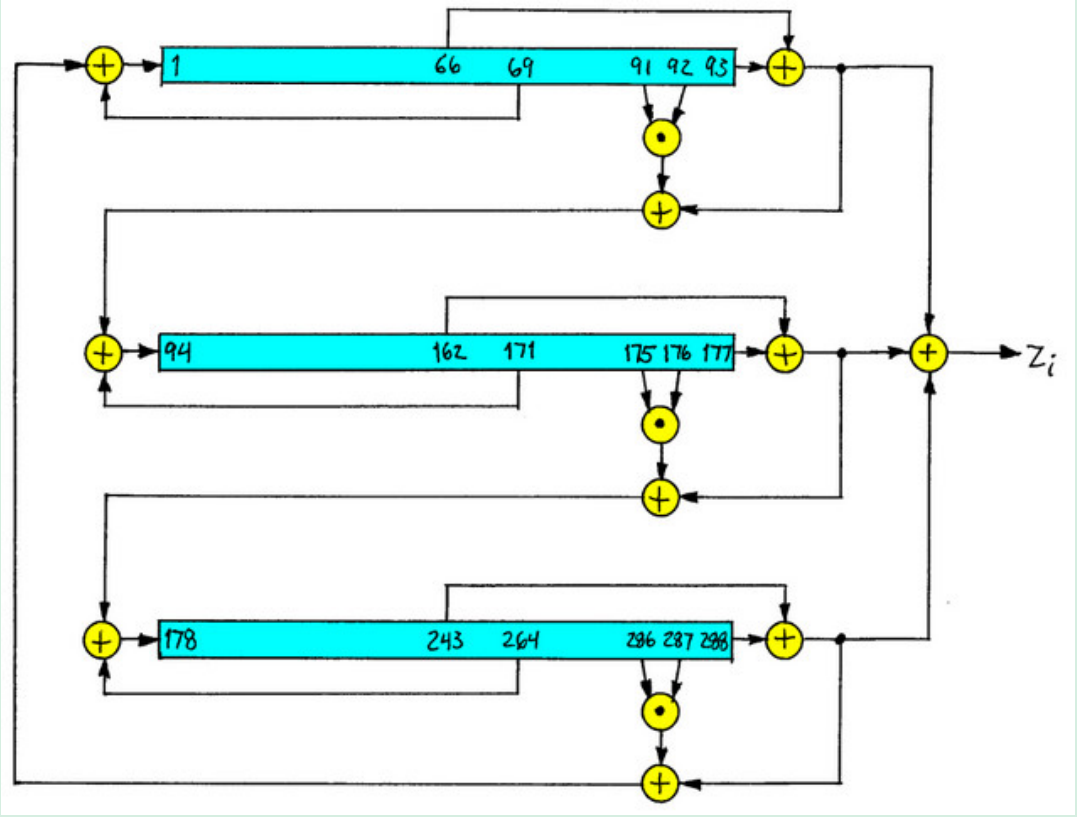
Grain 安全现状

- Grain为eSTREAM计划最后胜选的7个算法之一，具有较高的安全性。
- Grain的前身Grain v0由于函数g(x)和h(x)的选择存在缺陷，容易受到相关攻击。
- Grain结构没有明显的安全缺陷，但是各子部件仍需精心挑选。(非线性反馈函数g(x)和非线性导出函数h(x)需具备高非线性度、高相关免疫阶)。

1. Honggang Hu, Guang Gong: Periods on Two Kinds of nonlinear Feedback Shift Registers with Time Varying Feedback Functions. Int. J. Found. Comput. Sci. 22(6): 1317-1329 (2011)
2. O. Kucuk, "Slide Resynchronization Attack on the Initialization of Grain 1.0", http://www.ecrypt.eu.org/stream/grainp3.html
3. T. Bjorstad, "Cryptanalysis of Grain using Time/Memory/Date Tradeoffs", http://www.ecrypt.eu.org/stream/grainp3.html
4. S. Khazaei, M. Hassanzadeh and M. Kiaei, "Distinguishing Attack on Grain", http://www.ecrypt.eu.org/stream/grain.html
5. C. Berbain, H. Gilbert and A. Maximov, "Cryptanalysis of Grain", http://www.ecrypt.eu.org/stream/grain.html
6. Itai Dinur and Adi Shamir, Breaking Grain-128 with Dynamic Cube Attacks, http://eprint.iacr.org/2010/570.pdf.

eSTREAM计划胜选算法Trivium

- Trivium由比利时学者Christophe De Canniere和Bart Preneel设计。其包含3个NFSR（93级、84级、111级），密钥和初始向量长度均为80比特。



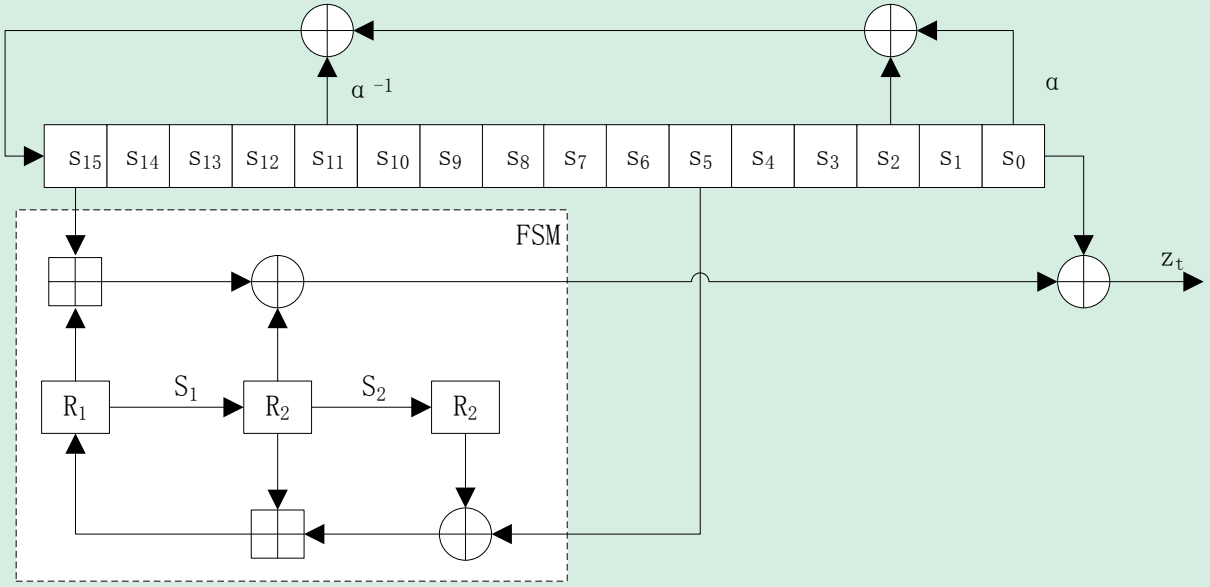
Trivium安全现状

- Trivium为eSTREAM计划最后胜选的7个算法之一，具有较高的安全性。
- 当前攻击Trivium最有效的方法为Cube Attack，其由Itai Dinur和Adi Shamir提出。
- Trivium结构没有明显安全缺陷。

1. Honggang Hu, Guang Gong: Periods on Two Kinds of nonlinear Feedback Shift Registers with Time Varying Feedback Functions. Int. J. Found. Comput. Sci. 22(6): 1317-1329 (2011)
2. Itai Dinur and Adi Shamir, Cube Attacks on Tweakable Black Box Polynomials, http://eprint.iacr.org/2008/385.

LTE加密标准SNOW 3G

- SNOW 3G是在SNOW 2.0的基础上改进而来的，现已是LTE通信加密标准。SNOW 3G主要由1个LFSR和1个FSM组成，如图所示。



SNOW 3G安全现状

- SNOW 3G针对SNOW 2.0在代数攻击方面可能存在的缺陷改进而来，具有非常高的安全特性，能够抵抗目前常见的序列密码攻击方法的攻击。

- 当前国际上有关SNOW 3G的安全性分析的结果很少。

1. ETSI/SAGE. Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 5: Design and Evaluation Report, version 1.1 (September 2006), http://www.3gpp.org/ftp/

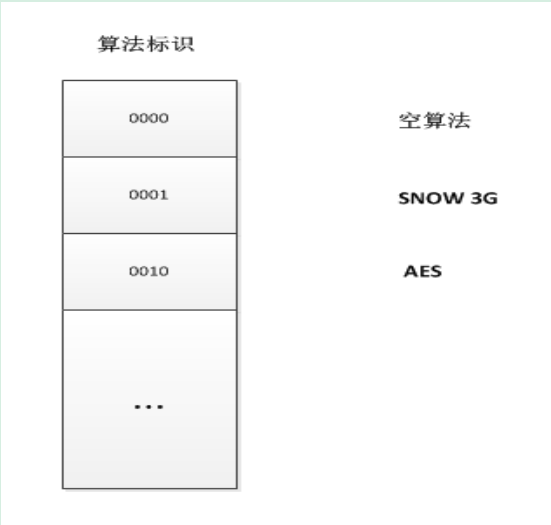
2. Alex Biryukov，Deike Priemuth-Schmid and Bin Zhang, Multiset collision attacks on reduced-round SNOW 3G and SNOW 3G, ACNS’ 2010, LNCS 6123, pp.139-153, 2010.

目录

- 相关背景
- 典型序列密码算法
- 已取得的阶段性成果

祖冲之算法(ZUC)

- 3GPP，即第3代合作伙伴计划，1998年由欧洲电信标准协会等启动，是一个专门负责制定全球3G通信标准的计划，2004年开始制定4G通信标准LTE。3GPP是电信领域全球最具影响力的计划之一。
- 在密码算法方面，我们关注到LTE标准中预留了16个密码算法接口，并已采用了两个标准算法，即美国高级加密标准AES和欧洲SNOW 3G。



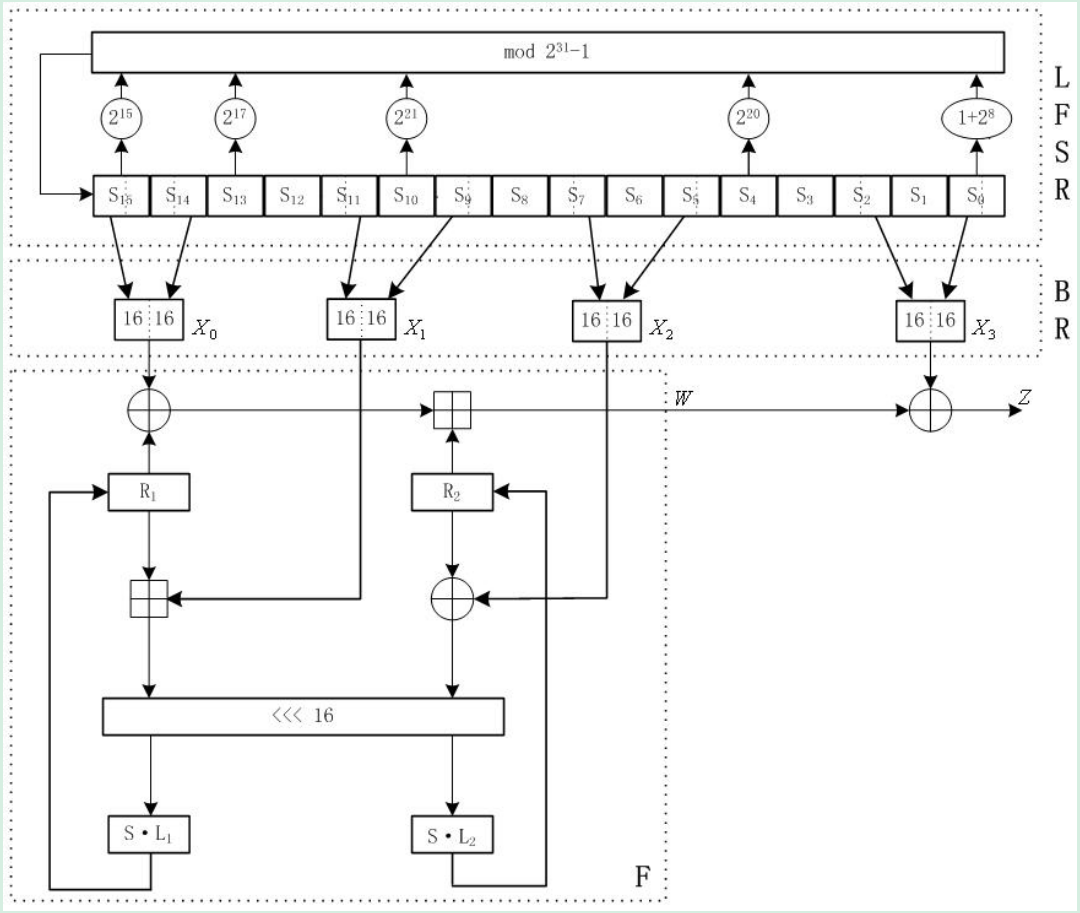
LTE算法标识示意图

祖冲之算法研制与国际标准化推进

- 针对LTE，我们研制了祖冲之算法(ZUC)，其已于2011年9月被3GPP选为第三个LTE国际加密标准(算法标识0011_2)，2012年3月被选为国家行业加密标准。
- 祖冲之算法的研制填补了**我国在国际商业密码标准领域中的空白**。2011年11月**工信部副部长杨学山**在祖冲之算法工业化部署大会上发言，高度肯定了祖冲之算法的设计和国际标准化推进工作，认为：

"祖冲之算法是我国第一个成为国际密码标准的密码算法。其标准化成功，是我国在国际密码领域的一次重大突破，可以增强我国在4G通信领域中的话语权。"

祖冲之算法结构图


mod $2^{31}-1$
2^{15}
2^{17}
2^{21}
2^{20}
$1+2^8$
S_{15} S_{14} S_{13} S_{12} S_{11} S_{10} S_9 S_8 S_7 S_6 S_5 S_4 S_3 S_2 S_1 S_0
L F S R
16 16 X_0
16 16 X_1
16 16 X_2
16 16 X_3
B R
W
Z
R_1
R_2
<<< 16
$S \cdot L_1$
$S \cdot L_2$
F

面向字节的猜测确定分析

- eSTREAM是欧洲提出的一个面向全球征集流密码算法的计划(2004~2008)，**是流密码领域最具影响力的计划**。该计划挑选了7个算法作为最终的**胜选算法**。这些算法：
  - **代表现代商用序列密码设计的最高水平**；
  - **具有非常高的安全性，能够很好抵抗现有常规攻击方法**。

Profile 1 (SW)	Profile 2 (HW)
HC-128	Grain v1
Rabbit	MICKEY 2.0
Salsa20/12	Trivium
SOSEMANUK	

针对SOSEMANUK的猜测确定分析

- SOSEMANUK是eSTREAM七个胜选算法之一，由法国12位密码学家共同设计，其中包括著名密码学专家H.Gilbert和N.Courtois。针对SOSEMANUK算法，我们给出了有效的攻击，将其复杂度由2^{226}大幅降到2^{176}。该工作发表在亚密会。

匿名审稿者给出的评价：

"To my knowledge, this is the first attack considering SOSEMANUK fro m the point of view of bytes. This new approach leads to a significant red uction of the time complexity in comparison to all other published guess a nd determine attacks on this cipher. "

（中文翻译：据我所知，这是第一个从字节角度考虑SOSEMANUK的攻击。同针对该密码已经发表的其它猜测确定分析方法相比，该新方法带来时间复杂度上的大幅度的降低。）

Xiutao Feng, **Jun Liu, Zhaocun Zhou, Chuankun Wu, and Dengguo Feng, A Byte-Based Guess and Determine Attack on SOSEMANUK, ASIACRYPT 2010, LNCS 6477, pp.146-157, 2010.**

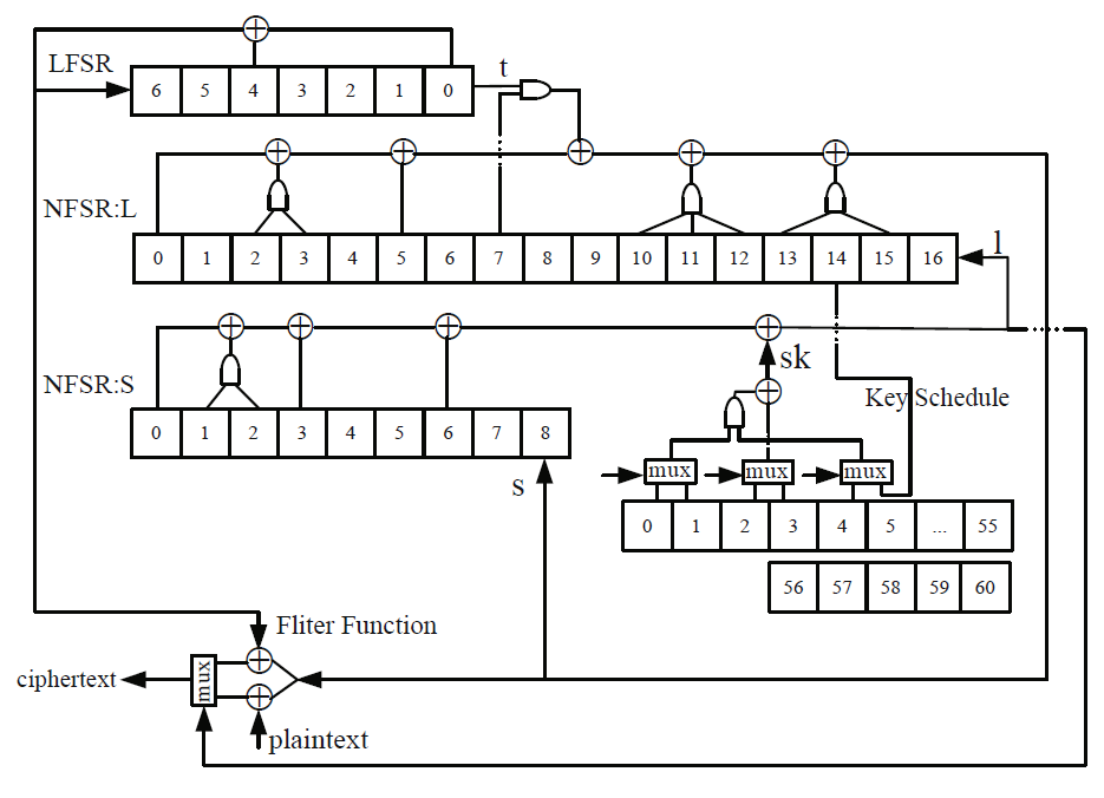
针对Rabbit的猜测确定分析

- 我们**针对状态函数反向求逆给出了目前最好的求解方法，**并基于该方法给出了一个针对Rabbit的面向字节的猜测确定攻击，其将猜测确定分析的复杂度由2^{303}大幅降到2^{242}。该工作发表在SCI刊源Foundations of Computer Science。

Xiutao Feng, Zhenqin Shi, Chuankun Wu and Dengguo Feng, On Guess and Determine Analysis of Rabbit, International Journal of Foundations of Computer Science**, Vol. 22, No. 6, pp.1283–1296, 2011.**

针对A2U2的实时密钥恢复攻击

- A2U2是由丹麦学者D.Mathieu、C.Damith和L.Torben提出的一个轻量级序列密码，拟用于RFID电子标签加密，该算法发表在RFID专业的国际顶级会议IEEE RFID。



针对A2U2的实时密钥恢复攻击

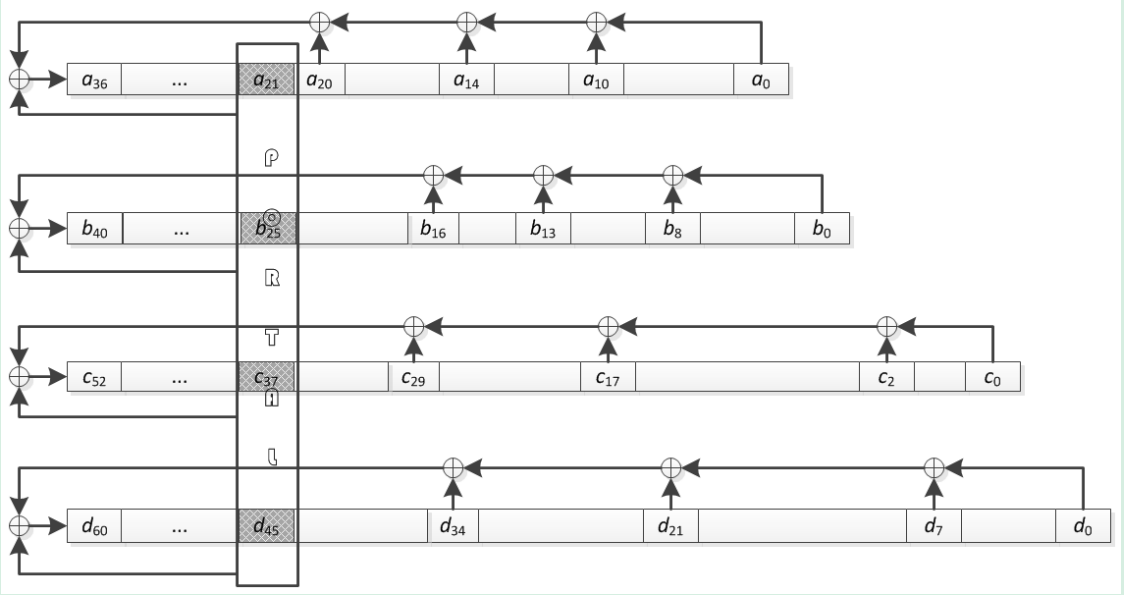
- 针对A2U2，在已知明文攻击模型下，我们给出了**一种实时的密钥恢复攻击方法**，在**个人PC**上只需**数秒钟**便可以**恢复**出**全部种子密钥**，从而**彻底攻破了该算法**。

	攻击模型	时间复杂度	数据复杂度
我们的攻击	已知明文攻击	$\leq 2^{25}$	≤210
丹麦学者Zenner等人给出的攻击	已知明文攻击	$2^{49}*C$	≈200
加拿大G. Gong等人给出的攻击	选择明文攻击	-	638

Zhenqing Shi, Xiutao Feng, Dengguo Feng and Chuankun Wu, A real-time key recovery attack on the lightweight stream cipher A2U2, CANS 2012, LNCS 7712, pp.12-22, 2012.

Portal：一个轻量级序列密码算法

- Portal是一个面向比特设计的轻量级序列密码。其种子密钥长度为80比特，初始向量为80比特，在同一个种子密钥和初始向量控制下生成长度不超过2^{50}比特的密钥流。
- Portal包含192比特的记忆单元，逻辑上由4个反馈移位寄存器、1个混合器S和1个密钥导出算子D组成，整体结构如图所示。



算法描述

- 4个反馈移位寄存器FSR的反馈多项式均为有限域F2上的本原多项式：
  - $f_1=x^{37}+x^{20}+x^{14}+x^{10}+1$
  - $f_2=x^{41}+x^{16}+x^{13}+x^{8}+1$
  - $f_3=x^{53}+x^{29}+x^{17}+x^{2}+1$
  - $f_4=x^{61}+x^{34}+x^{21}+x^{7}+1$

- 混合器是一个4*4的S盒：

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$S(x)$	10	9	15	2	13	14	3	4	5	12	8	1	0	7	6	11

- 密钥导出算子D是线性的：

$$z = a_4+b_5+c_{11}+d_{12}$$

初始化过程

- 将80比特的种子密钥和80比特的初始向量顺序填入4个FSR的记忆单元中，对最后一个FSR的剩余32比特记忆单元(即第4个FSR的最右边32个记忆单元)置常数串：

  0000 0100 1011 0011 1110 0011 0111 0101

- 重复执行下述过程160次完成算法初始化过程：
  - $z = a_4+b_5+c_{11}+d_{12}$;
  - $t_1\ t_2\ t_3\ t_4 = S(a_{21}\ b_{25}\ c_{37}\ d_{45})$;
  - $a_{37}=a_0+a_{10}+a_{14}+a_{20}$;
  - $b_{41}=b_0+b_8+b_{13}+b_{16}$;
  - $c_{53}=c_0+c_2+c_{17}+c_{29}$;
  - $d_{61}=d_0+d_7+d_{21}+d_{34}$;
  - $(a_1,a_2,\ldots,a_{36},a_{37}+t_1+z)\rightarrow(a_0,a_1,\ldots,a_{36})$;
  - $(b_1,b_2,\ldots,b_{40},b_{41}+t_2+z)\rightarrow(b_0,b_1,\ldots,b_{40})$;
  - $(c_1,c_2,\ldots,c_{52},c_{53}+t_3+z)\rightarrow(c_0,c_1,\ldots,c_{52})$;
  - $(d_1,d_2,\ldots,d_{60},d_{61}+t_4+z)\rightarrow(d_0,d_1,\ldots,d_{60})$.

密钥流生成过程

- 算法完成初始化过程后，重复执行下述过程，产生长度不超过2^{50}比特的密钥流：
  - $z = a_4+b_5+c_{11}+d_{12}$;
  - $t_1\ t_2\ t_3\ t_4 = S(a_{21}\ b_{25}\ c_{37}\ d_{45})$;
  - $a_{37}=a_0+a_{10}+a_{14}+a_{20}$;
  - $b_{41}=b_0+b_8+b_{13}+b_{16}$;
  - $c_{53}=c_0+c_2+c_{17}+c_{29}$;
  - $d_{61}=d_0+d_7+d_{21}+d_{34}$;
  - $(a_1,a_2,\ldots,a_{36},a_{37}+t_1)\rightarrow(a_0,a_1,\ldots,a_{36})$;
  - $(b_1,b_2,\ldots,b_{40},b_{41}+t_2)\rightarrow(b_0,b_1,\ldots,b_{40})$;
  - $(c_1,c_2,\ldots,c_{52},c_{53}+t_3)\rightarrow(c_0,c_1,\ldots,c_{52})$;
  - $(d_1,d_2,\ldots,d_{60},d_{61}+t_4)\rightarrow(d_0,d_1,\ldots,d_{60})$.

Portal算法设计小结

- Portal算法结构简单，易于理解，便于硬件实现。
- Portal算法能抵抗常见的序列密码分析方法的攻击，具有较高的安全性。
- Portal算法可以用大约1400门电路便可以硬件实现，具有成本低，功耗小，时延短等特性。
- Portal算法具有高度并行特征，可以轻松硬件实现1次吐多个比特，譬如8比特、16比特等。

谢谢大家！

欢迎批评指正！