3GPP LTE 国际加密标准 ZUC 算法

冯秀涛
（中国科学院软件研究所信息安全国家重点实验室，北京 100190）

[摘　要] ZUC 算法是中国自主设计的流密码算法，现已被 3GPP LTE 采纳为国际加密标准，即第四代移动通信加密标准。ZUC 算法是中国第一个成为国际密码标准的密码算法，其标准化的成功，是中国在商用密码算法领域取得的一次重大突破，体现了中国商用密码应用的开放性和商用密码设计的高能力，必将增大中国在国际通信安全应用领域的影响力。文中简单介绍了 ZUC 算法及其特点。

[关键词] ZUC 算法；3GPP LTE 加密标准；4G 移动通信
[中图分类号] TN918.4　　[文献标识码] A　　[文章编号] 1009-8054(2011)12-0045-02

ZUC Algorithm: 3GPP LTE International Encryption Standard

FENG Xiu-tao
(State Key Laboratory of Information Security, Institute of Software, China Academy of Sciences, Beijing 100190, China)

[Abstract] The ZUC algorithm, a stream cipher designed by Chinese cryptogists, is accepted by the 3GPP LTE as the international encryption standard for the 4G mobile communication. The ZUC algorithm is the first crypto algorithm designed by Chinese cryptologists and accepted as an international standard. The success of its standardization is an important breakthrough in the field of commercial crypto algorithm, and reflects China's opening in commercial crypto application and high capability in the design of commercial crypto algorithms, and these would inevitably raise the impact of China in the field of international communication security applications. This paper gives a brief description of ZUC and its properties.

[Keywords] ZUC; 3GPP LTE Encryption Standard; 4G mobile communication

0　引言

3GPP，即第三代合作伙伴计划，是由欧洲电信标准协会(ETSI)、日本无线工业及商贸委员会(ARIB)和电信技术委员会(TTC)、韩国电信技术协会(TTA)，以及美国电信标准委员会 T1 于 1998 年底发起成立的，是一个专门负责制定全球 3G 通信标准的计划。中国的通信标准协会(CCSA)于 1999 年加入该计划。目前 3GPP 已经囊括了全球最主要的电信标准化协会以及电信运营商和设备提供商，是电信领域全球最具影响力的计划之一。

2004 年 3GPP 开始启动长期演进 LTE(Long Term Evolution)，旨在确保 3GPP 未来在电信领域的持续竞争力。该计划已于 2010 年底被指定为第四代移动通信标准，简称 4G 通信标准。LTE 是下一代无线通信的主要技术之一，安全技术是 LTE 的关键技术。在安全算法方面，LTE 空中接口预留了 16 个机密性算法和 16 个完整性算法的接口。目前 3GPP 已经选择了两套加密算法，即美国的高级加密标准 AES 和欧洲的 SNOW 3G。为了适应中国商业密码政策的需要，同时谋求在下一代无线通信领域更大的话语权，因此向 3GPP 提交申请具有国内自主知识产权的密码算法显得尤为紧迫。

ZUC 算法[1-2]，即祖冲之算法，是 3GPP 机密性算法 EEA3 和完整性算法 EIA3[2-3] 的核心，是中国自主设计的加密算法。2009 年 5 月 ZUC 算法获得 3GPP 安全算法组 SA 立项，正式申请参加 3GPP LTE 第三套机密性和完整性算法标准的竞选工作。历时两年多的时间，ZUC 算法经过包括 3GPP SAGE 内部评估，两个邀请付费的学术团体的外部评估以及公开评估等在内的 3 个阶段的安全评估工作后，于 2011 年 9 月正式被 3GPP SA 全会通过，成为 3GPP LTE 第三套加密标准核心算法。

ZUC 算法是中国第一个成为国际密码标准的密码算法。其标准化的成功，是中国在商用密码算法领域取得的一次重大突破，体现了中国商用密码应用的开放性和商用密码设计的高能力，其必将增大中国在国际通信安全应用领域的影响力，且今后无论是对中国在国际商用密码标准化方面的工作还是商用密码的密码设计来说都有深远的影响。

1　ZUC 算法

ZUC 是一个同步流密码算法，其以中国古代著名数学家祖

收稿日期：2011-11-24
作者简介：冯秀涛，1978 年生，男，博士，研究方向：流密码的设计与分析。

冲之的拼音 (ZU Chongzhi) 首字母命名，中文称作祖冲之算法。该算法在设计之初就面临着高的挑战。美国高级加密标准 AES 和欧洲 SNOW 3G 已经被选为 LTE 加密标准，它们是两个设计非常优秀的密码算法，具有非常高的安全强度。ZUC 算法的设计必须做到不能比 AES 或 SNOW 3G 差，才有可能在 3GPP LTE 有立脚之处。面对挑战，ZUC 算法的设计必须具有高安全、高效率以及新颖性等特点。其中高安全和高效率要求设计的新算法在安全和效率上不能比 AES 或 SNOW 3G 低，而新颖性要求设计的密码算法在结构和部件上都有创新。然而密码算法设计发展到今天，许多经典结构和部件的设计都基本定型，要同时达到上述目标，无疑是一项非常艰巨的任务。

ZUC 算法在逻辑上采用三层结构设计，如图 1 所示。上层为定义在素域 GF($2^{31}-1$) 上的线性反馈移位寄存器 (LFSR)，这是 ZUC 算法设计的一大创新。目前常见流密码体制的 LFSR 均采用二元域或二元域的某个扩域上的 m 序列。这种序列具有明显的多重线性关系，这使得以其为序列源的密码算法容易受到相关攻击。ZUC 算法的 LFSR 设计首次采用素域 GF($2^{31}-1$) 的 m 序列。该类序列周期长、统计特性好，且在特征为 2 的有限域上是非线性的，其具有线性结构弱、比特关系符合率低等优点。因而采用 GF($2^{31}-1$) 上的 LFSR 设计的 ZUC 算法具有天然的强抵抗二元域上密码攻击方法的能力，譬如二元域上的代数攻击、区分分析和相关攻击等。此外，由于素域 GF($2^{31}-1$) 上的乘法可以快速实现，ZUC 算法 LFSR 在设计时充分考虑到安全和效率两方面的问题，在达到高安全目标的同时可以非常高效地软硬件实现[4]。

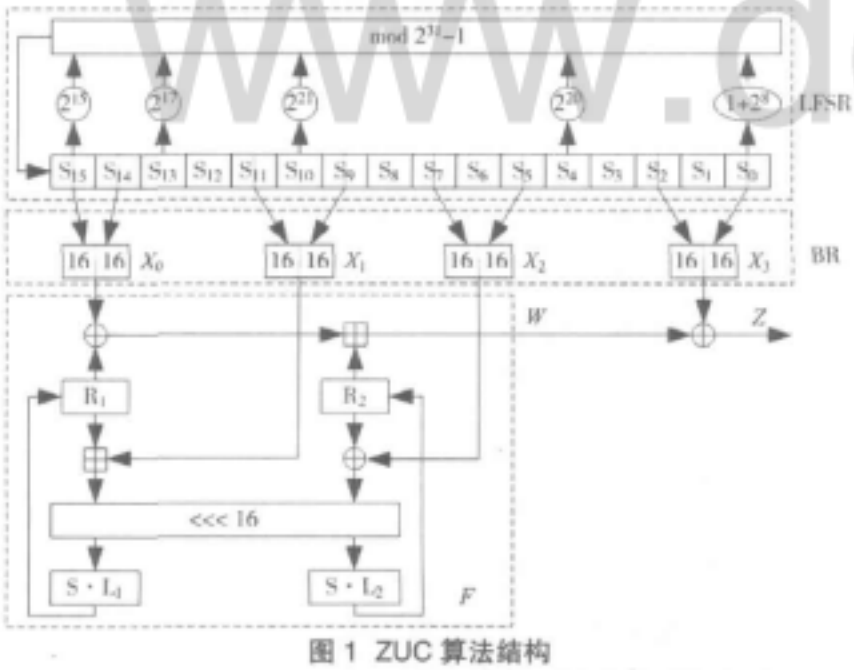

图 1 ZUC 算法结构

ZUC 算法中间层为比特重组。比特重组采用取半合并技术，实现 LFSR 数据单元到非线性函数 F 和密钥输出的数据转换，其主要目的是破坏 LFSR 在素域 GF($2^{31}-1$) 上的线性结构。结合下层的非线性函数 F，比特重组可使得一些在素域 GF($2^{31}-1$) 上的密码攻击方法变得非常困难。

ZUC 算法下层为非线性函数 F。在非线性函数 F 的设计上，ZUC 算法设计充分借鉴了分组密码的设计技巧，采用 S 盒和高扩散特性的线性变换 L，非线性函数 F 具有高的抵抗区分分析、快速相关攻击和猜测确定攻击等方法的能力。此外，非线性函数 F 的 S 盒采用结构化设计方法，在具有好的密码学性质的同时降低了硬件实现代价，具有实现面积小、功耗低等特点[5]。

经过上述三层结构的综合运用，ZUC 算法具有非常高的安全强度，能够抵抗目前常见的各种流密码攻击方法。其设计已得到国内外著名密码学家的认可，他们对其安全强度给予了很高的评价。

2 结语

有志者，事竟成。ZUC 算法已通过层层考验，最终证明其完全达到了 ZUC 算法设计当初拟定的目标，是一个高安全、高效率的新颖的密码算法。ZUC 算法标准化的成功，必将对中国在商用密码标准化领域的工作以及商用密码算法设计等方面产生深远的影响。2011 年 11 月，ZUC 算法国内产业化促进会在工业和信息化部电信研究院召开，大会高度肯定了 ZUC 算法的设计和标准化工作，其将开启 ZUC 算法产业化应用新的篇章。

参考文献

[1] ETSI/SAGE TS 35.221-2011, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3; Document 1: 128-EEA3 and 128-EIA3 Specification[S].

[2] ETSI/SAGE TS 35.222-2011, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3; Document 2: ZUC Specification[S].

[3] ETSI/SAGE TS 35.223-2011, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3; Document 3: Implementors'test data[S].

[4] 冯登国，金晨辉，戚文峰，等．一种序列密码实现方法及装置：国际专利，PCT/CN2009/072257[P]. 2009-06.

[5] 吴文玲，冯秀涛，周春芳．一种 S 盒构造方法及 S 盒：国际专利，PCT/CN2010/001048[P]. 2010-07.