GF(2)域上FSR+NLF类序列密码可重构处理结构设计

王志远[1,3]，黄建华[1]，管子铭[2]
(1. 解放军信息工程学院 信息技术研究所，河南 郑州 450002；
2. 解放军电子技术学院，河南 郑州 450004；
3. 空军电子技术研究所，北京 100195)

摘 要：讨论了FSR+NLF类序列密码的可重构处理结构设计，包括总体结构设计、可重构FSR结构设计、可重构NLF结构设计以及互连网络结构设计。采用该结构的密码运算单元可以根据需要实现多种此类序列密码，具有结构简单、可扩展、运行速度高等特点。

关键词：序列密码；可重构计算；线性反馈移位寄存器；非线性反馈移位寄存器；非线性函数
中图分类号：TN918.4　　**文献标识码**：A

The reconfigurable processing architecture design of the FSR+NLF type sequence cipher over GF(2)

WANG Zhi Yuan[1,3], HUANG Jian Hua[1], GUAN Zi Ming[2]
(1. Research Institute of Information Technology, PLA Information Engineering College, Zhengzhou 450002, China;
2. PLA Electronic Technology College, Zhengzhou 450004, China;
3. Research Institute of Electronic Technology, Air Force, Beijing 100195, China)

Abstract: This paper introduces the reconfigurable processing architecture design of the FSR+NLF type sequence cipher, including the whole architecture design, the reconfigurable FSR architecture design, the reconfigurable NLF architecture design and the interconnection network architecture design. The reconfigurable processing architecture's characters are simple, extensible and high-speed.

Key words: sequence cipher; reconfigurable computing; LFSR; NLFSR; NLF

可重构计算的思想最早由加利福尼亚大学洛杉矶分校的Estrin教授[1]提出来的。可重构计算没有严格的定义，目前学术界普遍接受的定义是：使用集成了可编程硬件的系统进行计算，该可编程硬件的功能可由一系列定时变化的物理可控点来定义[2]。从这个定义可以看出，可重构计算是通过对结构可变的硬件进行软件配置，以适应不同算法的处理，故其既具有软件的灵活性，又具备了ASIC硬件的高速性，是解决资源受限类算法，如多媒体处理算法、DSP、加解密算法的一种理想选择。

明文数据流与密钥流逐位地加密成密文数据流的密码体制称为序列密码(Sequence Cipher)。当密钥流满足离散无记忆二元均匀分布，即完全随机时，则该体制就是"一次一密"密码体制，香农证明该体制是不可破译的[3]。实际应用中，序列密码的密钥流是用确定的算法产生的，即密钥流是伪随机的，但可以通过数学的手段尽可能地提高密钥流的随机性，最大程度地逼近"一次一密"，因此序列密码的保密性较高。此外，由于序列密码具有容易实现、实时性好、错误传播有限等优点，被广泛应用于政府、军事等重要部门。

根据序列密码设计所采用的理论不同，可将序列密码分为4类：基于信息论设计、基于系统论设计、基于复杂度理论设计和基于随机化理论设计的序列密码[4]。其中第1、3、4类序列密码涉及的数学理论多样，适于用软件的方法实现，不适于专用硬件或可重构硬件来实现。而第2类基于系统论设计的序列密码是目前最为实用的序列密码，这类序列密码的密钥流生成器大多由1个或多个线性或非线性反馈移位寄存器LFSR/NLFSR(Linear/Non-linear Feedback Shift Register)和1个非线性函数NLF(Non-linear Function)构成，本文把符合该特点的序列密码简称为FSR+NLF类序列密码。这类密码由

于具有相似的运算单元，很适合采用可重构硬件实现。FSR+NLF 类序列密码又分为 2 个子类：(1)若序列密码中 1 个或多个 FSR 状态位参与 NLF 运算，则称为非线性滤波型序列密码，相应的 NLF 称为非线性滤波函数，其结构如图 1 所示，Grain[5]就属于这类序列密码；(2)若序列密码中只有各个 FSR 的最低状态位参与 NLF 运算，则称为非线性组合型序列密码，相应的 NLF 称为非线性组合函数，其结构如图 2 所示，Achterbahn[6]就属于这类序列密码。根据 FSR 运算域的不同，FSR+NLF 类序列密码又有 GF(2)域上和 $GF(2^n)$域上之分，本文将详细讨论 GF(2)域上该类序列密码的可重构处理结构设计，非线性滤波型和非线性组合型序列密码均可以在该可重构处理结构上实现。

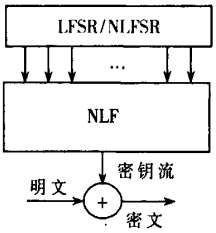

图 1 非线性滤波型序列密码

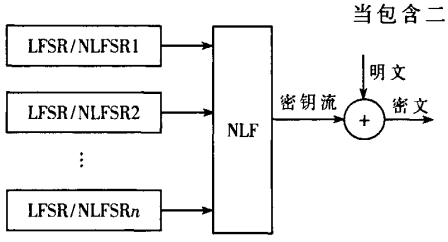

图 2 非线性组合型序列密码

1 总体结构设计

对现有的 GF(2)域上 FSR+NLF 类序列密码分析发现，绝大多数此类密码的 FSR 个数不超过 8 个，长度不超过 256 bit，因此其可重构处理总体结构设计如图 3 所示。从图中可以看出，此类密码的可重构处理结构主要由 8 个可重构 FSR 和 1 个可重构 NLF 通过互连网络连接而成。其中，8 个可重构 FSR 分成完全相同的两组，每组中的 4 个可重构 FSR 的最大长度分别为32 bit、64 bit、128 bit 和 256 bit，以满足不同算法的需要，又可以减少互连资源。该可重构处理结构采用了特殊的互连网络结构，外部送入的配置指令经译码电路译码后存入配置寄存器组，再由配置寄存器组对各可重构 FSR、可重构 NLF和互连网络进行配置，从而构成相应的序列密码算法处理结构。

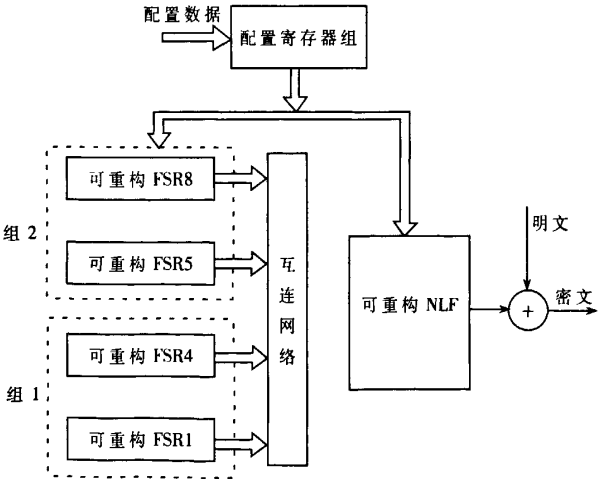

图 3 FSR+NLF 类序列密码可重构处理总体结构

2 可重构 FSR 结构设计

FSR 由 1 个移位寄存器 SR 和 1 个反馈函数 F 组成，设 n 级移位寄存器 SR 的状态为 $x_0, x_1, \cdots, x_{n-1}$，则函数 F 表示为：

$$F(x_0,x_1,\cdots,x_{n-1})=a_0x_0+a_1x_1+\cdots+a_{n-1}x_{n-1}+a_{01}x_0x_1+\cdots+a_{n-2n-1}x_{n-2}x_{n-1}+\cdots+a_{01\cdots n}x_0x_1\cdots x_{n-1} \quad (1)$$

式中，$a_i, x_i \in GF(2)$，“+”表示“异或”运算，每一项中各数间的运算为“与”运算。当 F 中只包含 1 次项时，称 F 是线性的，对应的 FSR 称为线性反馈移位寄存器(LFSR)；当包含二次及二次以上项时，称 F 是非线性的，对应的 FSR 称为非线性反馈移位寄存器(NLFSR)。

基于以上基本理论，1 个最长级数为 n 的可重构 FSR 结构设计如图 4 所示。其结构总体上分为 3 部分：中间是 1 个级数为 n 的移位寄存器 SR，其移动方向为从 $n-1$ 级到 0 级；SR 以上的部分为反馈函数部分；SR 以下部分为前馈函数部分，因为有的序列密码的 FSR 带有前馈输出(例如 Achterbahn)。

对现有的 FSR+NLF 类序列密码反馈函数分析发现：反馈函数 F 中二次及二次以上项的总数不超过 20 项。为此，该结构中为一次项设计了 1 个配置寄存器 CR_1；为二次及二次以上项设计了 30 个配置寄存器 CR_2~CR_{31}，共计 31 个配置寄存器。这 31 个配置寄存器的位数均与 SR 的级数相同，为 n bit。

该结构中反馈函数部分工作原理：假设反馈函数 $F=x_0+x_3+x_{n-2}+x_1x_2+x_5x_{n-1}+x_6x_9x_{12}+x_1x_3x_7x_{10}x_{n-3}x_{n-2}$，配置时，将 CR_1 的第 0、3、$n-2$ 位配置为“1”，其余位配置为“0”；将 CR_2 的第 1、2 位配置为“0”，其余位配置为“1”；将 CR_3 的第 5、$n-1$ 位配置为“0”，其余位配置为“1”；将 CR_4 的第 6、9、12 位配置为“0”，其余位配置为“1”；将 CR_5 的第 1、3、7、10、$n-3$、$n-2$ 位配置为“0”，其余位配置为“1”；其余的配置寄存器各位均配置为“1”。配置完成后，SR 的各级状态与 CR_1 的对应位相“与”，得到的各位结果相“异或”即得到 F 的所有一次项模 2 加的和，即 $x_0+x_3+x_{n-2}$ 的结果；SR 的各级状态与 CR_2 的对应位相“或”，得到的各位结果再一起相“与”即得到 x_1x_2 的结果；CR_3、CR_4、CR_5 进行与 CR_2 相同的运算后可分别得到 x_5x_{n-1}、$x_6x_9x_{12}$、$x_1x_3x_7x_{10}x_{n-3}x_{n-2}$ 的结果，其余各配置寄存器运算与 CR_{21} 也相同，得到的结果为“1”。然后，通过 1 个 32 bit 的组合配置寄存器 CRcom 将各项结果组合运算后即得到 F，F 反馈给 SR 的最后一级，CRcom 的配置方式和运算过程与 CR_1 相同。CRcom 在进行组合运算时，还有 1 个外部反馈值 FV_ext 参与了运算，这是因为一些

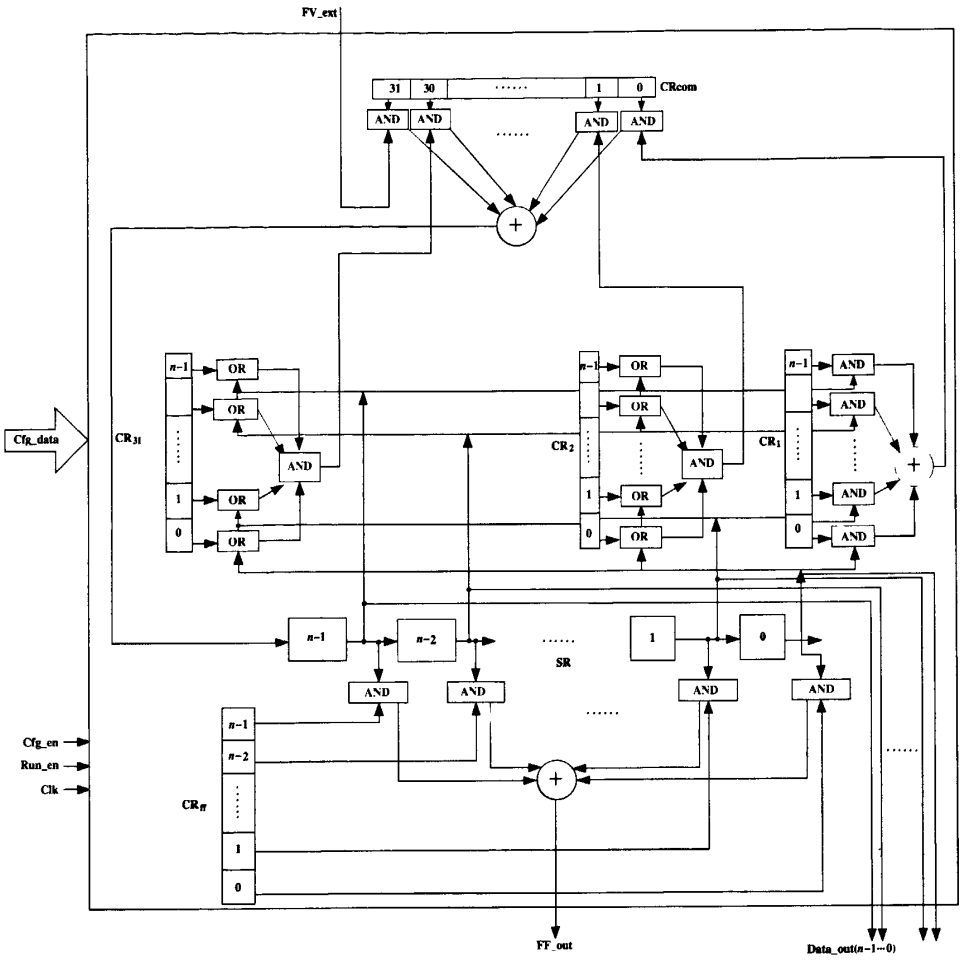

图 4 最长级数为 n 的可重构 FSR 结构

序列密码中，有外部数据参与了 FSR 的反馈（例如 Grain）。

该可重构 FSR 结构中，SR 以下是 1 个前馈函数部分，因为在有些序列密码中，FSR 带有前馈输出（例如 Achterbahn）。前馈函数 F' 是 FSR 某些级状态的 1 个线形函数，其中必定包含 FSR 的最低一级状态。该结构设计中，采用 1 个 n bit 的前馈函数配置寄存器 CR_{ff} 和 SR 的各级状态进行组合运算即得到前馈输出 FF_out，CR_{ff} 的配置方式和运算过程与 CR_{11} 相同。当 CR_{ff} 中只有某一位被配置为“1”时，则 FF_out 输出即为 FSR 对应一级的状态，特别是这样可以得到 FSR 最低一级的状态输出，用于另一个 FSR 的 FV_ext 输入或 NLF 的输入。

该可重构 FSR 的最长级数为 n，通过对其各个寄存器的配置，可以将其配置为级数小于等于 n 的任意 FSR。例如，当 n=32 时，要得到一个级数为 30 的 FSR，则将配置寄存器 CR_1 的第 0 位和第 1 位都配置为“0”，将 CR_2~CR_{31} 的第 0 位和第 1 位都配置为“1”，则 SR 的第 0 级和第 1 级没有参与反馈运算，相应的 FSR 退化为 30 级，其有效级为第 2~31 级。

n 位输出信号线 Data_out 输出 FSR 的 n 级状态，当 NLF 为滤波函数时作为其输入。外部输入信号线有配置使能信号线 Cfg_en、运行使能信号线 Run _en、时钟 Clk 以及 32 bit 宽的配置数据线 Cfg_data。配置使能信号 Cfg_en 有效后，外部配置寄存器组通过 Cfg_data 对 FSR 内部各寄存器进行配置，配置完成后运行使能信号 Run_en 变为有效，FSR 在时钟控制下开始运行。

3 可重构 NLF 结构

FSR+NLF 类序列密码中的 NLF 单元对输入的信号进行非线性变换后输出密钥，其定义与(1)式相同，故可重构 NLF 的结构与可重构 FSR 结构中的反馈函数部分相似。与可重构 FSR 结构不同的是，在可重构 NLF 中设计了 32 个配置寄存器 NCR_1~NCR_{32}，而且由于输入数据线 Data_in 宽度固定为 32 bit，因此 32 个配置寄存器 NCR_1~NCR_{32} 均为 32 bit。输入数据 Data_in 分别与各配置寄存器进行组合运算后得到 NLF 各项结果，各项结果通过 NCR_{com} 组合运算后输出 NLF 值，即密钥 Key。

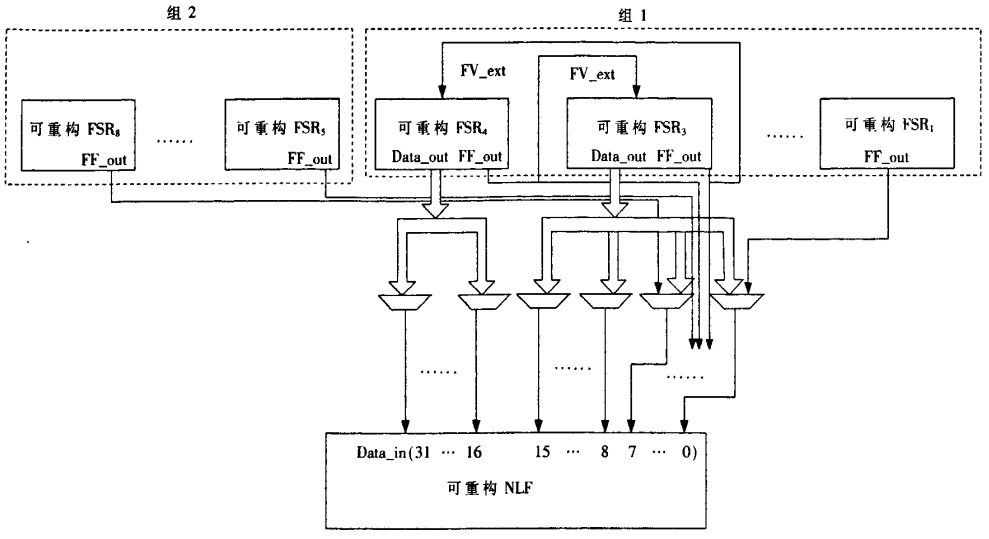

图 5 互连网络结构

4 互连网络结构

本文讨论的序列密码可重构处理结构可以实现滤波型和非线性组合型两类序列密码，因此，其互连网络结构应能满足这两类序列密码的连接需要，基于此要求设计的互连网络结构如图 5 所示。

该互连网络结构总的设计思路：当实现非线性组合型序列密码时，可重构 FSR_1~FSR_8 的前馈输出信号 FF_out 与可重构 NLF 单元的数据输入信号 Data_in(0~7)分别相连；当实现滤波型序列密码时，由于此类密码中 FSR 一般为 1 个，个别为 2 个，因此选择组 1 中级数最长的 2 个可重构 FSR_3 和 FSR_4 参与互连，组 2 中的 4 个和组 1 中的其他 2 个可重构 FSR 这种情况下不参与互连。

具体连接规则是：可重构 FSR_3 的 128 bit 状态输出信号 Data_out 分别与可重构 FSR_1~FSR_8 的前馈输出信号 FF_out 通过 8 个 129 选 1 选路器 MUX_0~MUX_7 与可重构 NLF 的数据输入信号 Data_in(0~7)相连；可重构 FSR_3 的 128 bit 状态输出信号 Data_out 再通过8 个 128 选 1 选路器 MUX_8~MUX_{15} 与可重构 NLF 的数据输入信号 Data_in(8~15)相连；可重构 FSR_4 的 128 bit 状态输出信号 Data_out 通过 16 个 128 选 1 选路器 MUX_{16}~MUX_{31} 与可重构 NLF 的数据输入信号 Data_in(16~31)相连；同时，为了满足有些序列密码算法中某一个 FSR 的最低一级输出要参与另一个 FSR 的反馈的情况，将可重构 FSR_3、FSR_4 的 FF_out 分别与对方的 FV_ext 相连。

本文论述的 FSR+NLF 类序列密码可重构处理结构的配置寄存器都是 32 bit 的整数倍，故规定其重构粒度为 32 bit，配置数据线 Cfg_data 宽度为 32 bit。从功能上来看，该可重构处理结构除可以满足 FSR+NLF 类序列密码的处理需求外，还可以和自收缩式发生器、有限状态机等单元结合使用来处理一些该类衍生的序列密码。

此外，该可重构处理结构具有可扩展性，可重构 FSR 的个数、各可重构 FSR 的最大长度、各可重构 FSR 的反馈函数部分与可重构 NLF 中二次以上项的项数都可以根据需要进行扩展。

本文论述的 FSR+NLF 类序列密码可重构处理结构的原型已经在 Altera 公司生产的 EP2S60F1020C5 型 FPGA 上实现，所需资源约为 2.2 万门，最高工作频率为 200 MHz。由此可见，该可重构处理结构简单，实现时占用资源较少，运行速度较高。

参考文献

[1] ESTRIN G, BUSSEL B. Parallel processing in a restructurable computer system[J]. IEEE Trans. Elect comput, 1963. 747-755.

[2] COMPTON K, HAUCK S. Reconfigurable computing: a survey of systems and software[J]. ACM Computing Surveys. 2002, 34(2): 171-210.

[3] SHANNON C E. Communication theory of secrecy systems [EB/OL]. http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf. 2009-01.

[4] 冯登国，裴定一.密码学导引[M]. 北京：科学出版社，1999:486-100.

[5] GAMMEL B, GOTTFERT R. The achterbahn stream cipher [EB/OL]. http://www.ecrypt.eu.org/stream/papers.html. 2009-02.

[6] HELL M, JOHANSSON T, MEIER W. Grain-a stream cipher for constrained environments[EB/OL]. http://www.it.lth.se/grain/grainV1.pdf. 2009.02.

(收稿日期:2009-06-16)

GF(2)域上FSR+NLF类序列密码可重构处理结构设计

作者： 王志远， 黄建华， 管子铭， WANG Zhi Yuan， HUANG Jian Hua， GUAN Zi Ming
作者单位： 王志远,WANG Zhi Yuan(解放军信息工程学,院信息技术研究所,河南,郑州,450002;空军电子技术研究所,北京,100195)， 黄建华,HUANG Jian Hua(解放军信息工程学,院信息技术研究所,河南,郑州,450002)， 管子铭,GUAN Zi Ming(解放军电子技术学院,河南,郑州,450004)
刊名： 电子技术应用 ISTIC PKU
英文刊名： APPLICATION OF ELECTRONIC TECHNIQUE
年，卷(期)： 2009,35(11)

参考文献(6条)

1. ESTRIN G;BUSSEL B Parallel processing in a restructurable computer system 1963

2. COMPTON K;HAUCK S Reconfigurable computing:a survey of systems and software[外文期刊] 2002(02)

3. SHANNON C E Communication theory of secrecy systems 2009

4. 冯登国;裴定一 密码学导引 1999

5. GAMMEL B;GOTFFERT R The achterbahn stream cipher 2009

6. HELL M;JOHANSSON T;MEIER W Grain-a stream cipher for constrained environments 2009

本文读者也读过(10条)

1. 孙国华.李芳芳 一类广义自缩序列的伪随机性[期刊论文]-计算机技术与发展2010,20(3)

2. 徐望.奚刚.Xu Wang.Xi Gang 基于Simulink的序列密码仿真建模与分析[期刊论文]-计算机应用与软件2008,25(11)

3. 曾光.韩文报.范淑琴.Zeng Guang.Han Wen-bao.Fan Shu-qin σ-LFSR在序列密码算法ABC中的应用[期刊论文]-电子与信息学报2009,31(3)

4. 伍文君.唐贵林.黄芝平.WU Wen-jun.TANG Gui-lin.HUANG Zhi-ping 一种快速相关攻击算法[期刊论文]-计算机工程2009,35(17)

5. 马卫局.冯登国.MA Wei-ju.FENG Deng-guo 钟控密钥流生成器及其密码性能[期刊论文]-通信学报2007,28(7)

6. 祁传达.陈越奋.王丽娜.QI Chuan-da.CHEN Yue-fen.WANG Li-na 序列密码采样攻击的改进方法[期刊论文]-计算机工程2009,35(8)

7. 岳鸿鹏.王和明.Yue Hongpeng.Wang Heming 基于DSP Builder的改进型序列生成器设计[期刊论文]-计算机测量与控制2010,18(11)

8. 金晨辉.张斌.张远洋.Jin Chen-hui.Zhang Bin.Zhang Yuan-yang Whitenoise密码Wu破译方法的分析与改进[期刊论文]-电子与信息学报2006,28(8)

9. 盖光.Gai Guang 自然价值之于生态审美价值:作用和意义[期刊论文]-山东理工大学学报（社会科学版）2007,23(2)

10. 刘强.汪斌强.潘冬存.于婧.LIU Qiang.WANG Bin-qiang.PAN Dong-cun.YU Jing 可重构路由单元软件体系结构的研究与实现[期刊论文]-计算机应用研究2009,26(9)