ANT 系列分组密码算法的 FPGA 高速实现*

王建新，刘芮安，肖超恩，张　磊
（北京电子科技学院 电子与通信工程系，北京 100070）

摘　要： ANT 系列分组密码算法是一种轻量级密码算法，针对 ANT-128/128 算法，使用 Verilog HDL 分别对密钥扩展模块、加密模块在 Quartus II 15.0 中进行工程实现，并采用 46 级全流水线结构进行高速优化。在 Cyclone V 系列 5CGXFC7D6F31C7ES 芯片中综合结果表明，工程实现结果与标准向量值一致，两模块逻辑利用率分别仅占总资源的 3%及 7%，且基于流水线优化后的加解密模块工作频率最高可达 339 MHz，数据吞吐率最高可达 43 Gb/s，能够满足大部分高速加密系统的需求。

关键词： ANT；分组密码；Verilog HDL；流水线结构
中图分类号： TP309.7　　**文献标识码：** A　　DOI：10.16157/j.issn.0258-7998.200931

中文引用格式： 王建新，刘芮安，肖超恩，等. ANT 系列分组密码算法的 FPGA 高速实现[J].电子技术应用，2021，47(4)：132-136，144.
英文引用格式： Wang Jianxin，Liu Ruian，Xiao Chaoen，et al. High-speed implementation of ANT series block cipher algorithm on FPGA[J]. Application of Electronic Technique，2021，47(4)：132-136，144.

High-speed implementation of ANT series block cipher algorithm on FPGA

Wang Jianxin，Liu Ruian，Xiao Chaoen，Zhang Lei
（Department of Electronic，Beijing Electronics Science and Technology Institute，Beijing 100070，China）

Abstract： ANT series block cipher algorithm is suitable for lightweight implementation and convenient for side channel protection. For ANT-128/128 algorithm，Verilog HDL is used to implement the key expansion module and encryption module in Quartus II 15.0，and a 46-level pipeline structure is adopted for high-speed optimization. Further，the pipeline structure was used for high-speed optimization. The comprehensive results in chip 5CGXFC7D6F31C7ES of Cyclone V show that the implementation results are consistent with the standard vector value. The logic utilization ratio of the two modules only accounts for 3% and 7% of the total resources respectively. The working frequency of the encryption and decryption module based on pipeline structure can reach up to 339 MHz and the data throughput rate can reach up to 43 Gbps.

Key words： ANT；block cipher；Verilog HDL；pipeline structure

0 引言

随着信息技术的发展，信息安全问题日益受到重视。在网络空间安全维护、发展的进程中，密码技术在公钥基础设施、GSM 鉴权、电子信封及区块链等[1]领域中起到了关键作用。分组密码算法是保障信息机密性和完整性的重要技术手段[2]，在智能终端、无线传感网络等领域广泛应用[3]。目前，所使用的分组密码多为国外设计，且传统分组密码如 AES[4]等在资源有限的情况下并不适用。我国自主设计的商用分组密码算法以 SM4 算法为主。

近年来，提升科技创新的保障效应和网络安全的动力机能[5]成为网络空间治理的重要目标。为推动密码算法技术进步，中国密码学会举办了全国密码算法设计竞赛。ANT 系列分组密码算法由山东大学网络空间安全学院王美琴[6]等提交，经公开评议、检测评估和专家评选已入选竞赛第二轮名单。

近年来，轻量级密码算法逐渐成为研究热点[7]，如 HIGHT[8]、PRESENT[9]、PICCOLO[10]、LED[11]、LBlock[12]和 Zorro[13]等。作为一款国产轻量级密码算法，ANT 系列分组密码算法具有抗侧信道攻击、适合 bit-slice 多路并行实现等优势[6]，具有一定的研究价值及应用前景。

为了适应第五代移动通信、物联网等高新技术对密码算法高速实现的需求[14]，本文采用流水线结构，对 ANT 算法进行高速、高数据吞吐率的硬件设计实现。

1 ANT 系列分组密码算法介绍

1.1 ANT-128/128 分组密码算法

ANT-128/128 分组密码算法采用 128 bit 长度主密钥 $K=k_{2n-1}||k_{2n-2}||\cdots||k_0$，并可以分为：

* 基金项目：国家自然科学基金项目(61701008)

$$\begin{cases} K_1=k_{2n-1}||k_{2n-2}||\cdots||k_n \\ K_0=k_{n-1}||k_{n-2}||\cdots||k_n \end{cases} \tag{1}$$

$K_1||K_0$ 作为 LFSR 的初始状态。每次先取出当前低位寄存器 K_i 中的 n 比特作为当前轮的轮密钥 k_i，然后进行 LSFR 的状态更新，$(i+1)$ 作为轮常数(i 为当前轮数)，如图 1 所示。K_{i+1} 经过 A 操作迭代变换 3 次，如图2所示。

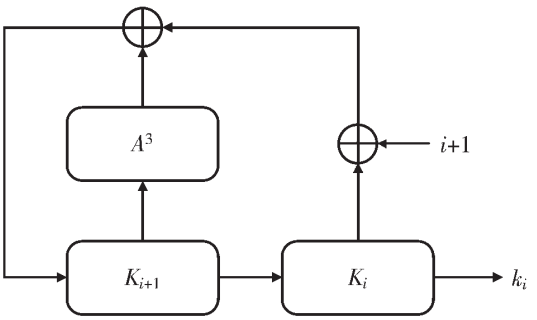

图 1 ANT-128/128 算法密钥扩展结构图

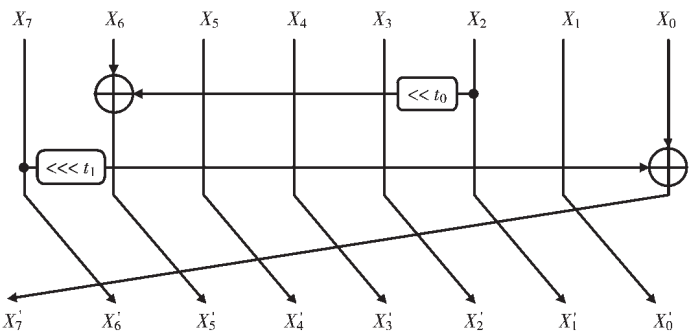

图 2 A 操作结构图

在 ANT-128/128 算法中，常数 $t_0=7$，$t_1=1$。

1.2 轮函数

ANT-128/128 分组密码算法轮函数结构如图 3 所示，其中，$(s_0,s_1)=(3,16)$。为保证加解密一致，最后一轮左支经过轮函数后不进行交换。

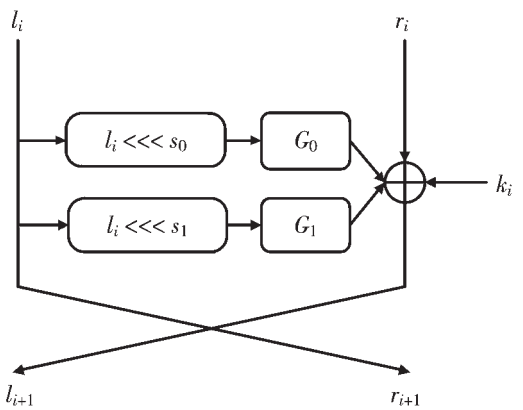

图 3 轮函数结构图

1.2.1 非线性函数 G_0、G_1

G_0、G_1 为非线性函数，包含两层，两层中间是一层比特级的置换。

(1)对于 $G_0: y^1=G_0(x^0)$

先经过第一层：

$$y_j^0=\begin{cases}(x_{j+3}^0 \otimes x_{j+2}^0)\oplus x_j^0, & j \bmod 4=0 \\ x_j^0, & \text{其他}\end{cases} \tag{2}$$

再经过比特级置换 $x_{\mathrm{PERM}(j)}^1=y_j^0$，最后经过第二层：

$$y_j^1=\begin{cases}(x_{j+3}^1 \otimes x_{j+2}^1)\oplus x_j^1, & j \bmod 4=0 \\ x_j^1, & \text{其他}\end{cases} \tag{3}$$

其中，$0\leqslant j<n$。

(2)对于 G_1，结构与 G_0 相同，仅作比特位与模数的变换，在此不作赘述。

1.2.2 比特级置换 PERM

在 ANT-128/128 算法下，比特级置换 PERM 的表达式如下：

$$\mathrm{PERM}(j)=\begin{cases}(j+58) \bmod 64, & j \bmod 4=3 \\ (j+54) \bmod 64, & j \bmod 4=2 \\ (j+30) \bmod 64, & j \bmod 4=1 \\ (j+2) \bmod 64, & j \bmod 4=0\end{cases} \tag{4}$$

2 功能模块设计

本文采用 Verilog HDL 语言以 Quartus II 15.0 为平台进行工程实现。系统由两个主要部分组成，分别为密钥扩展模块和加解密模块。本文使用了有限状态机(FSM)[15-16]的设计思路对两个模块进行工程实现，并采用流水线结构对加解密模块进行性能优化，以提高数据吞吐率。系统整体结构框图如图 4 所示。

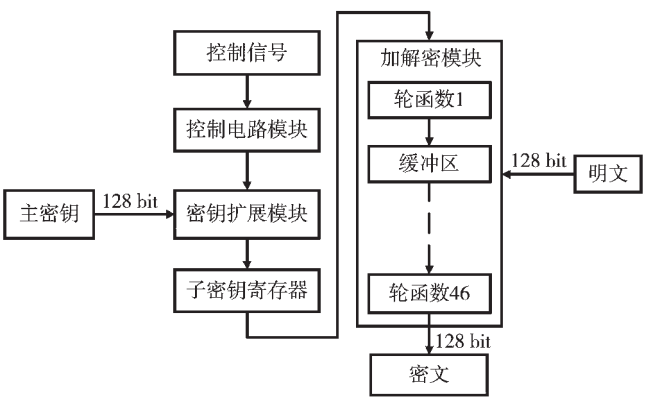

图 4 系统整体结构框图

图 4 中，在控制信号置位后，密钥扩展模块读取128 bit主密钥并进行子密钥扩展，存储于子密钥寄存器中，供加解密模块调用。加解密模块读取明文，并以流水线的形式同时开始各轮函数运算，在经历 46 轮后，生成 128 bit 密文。下面将对三个模块设计方案进行详细说明。

2.1 密钥扩展模块设计

ANT 密钥扩展模块基于 LFSR 实现，采用有限状态机结构，能够达到“状态更新一次，寄存器移位一次”的

效果。密钥扩展模块定义的输入端口有：时钟、主密钥以及复位，设置状态字寄存器。当系统检测到复位信号时，电路将从空闲状态转换为工作状态，并在每一个时钟上升沿到来时转换到下一状态。每一轮完成后，生成的子密钥将会存入相应的寄存器，供轮函数调用。经历 46 轮后，密钥扩展完毕。密钥扩展模块流程如图 5 所示。

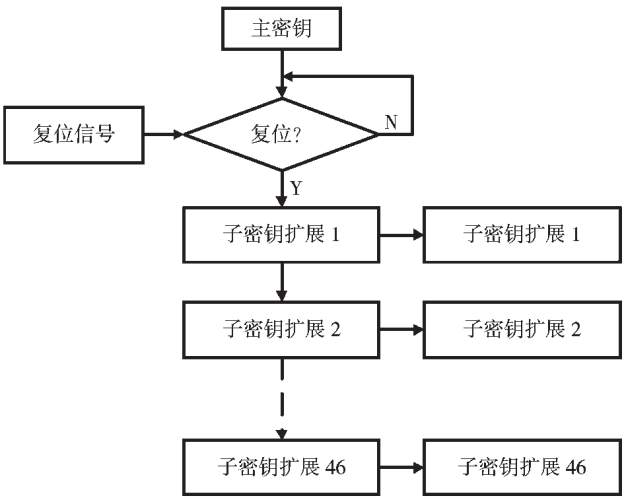

图 5　密钥扩展流程图

在密钥扩展模块中，为保证数据的扩散性，算法设计了 A 操作并对其进行三次迭代，其实质是对比特分组的移位和异或。为提升运算速度，本文经过计算得到 A 操作迭代三次后的输出表达式，并将其整体例化为元件。该设计方式无需调用三次“A 操作”，只需调用一次“A 操作三次迭代”，省去了四次异或运算与四次移位。在密钥扩展中，由于各轮中该部分功能相同，只需实现一次元件，并在各轮中依次调用，从而大大节约了硬件资源。

A 操作经计算后的表达式为：

$$\begin{aligned}
&x[7]'=x[2]\oplus\{\{x[1]\oplus\{[x[0]\oplus\\
&\qquad(x[7]<<<1)]<<<1\}\}<<<1\}\\
&x[6]'=x[1]\oplus\{[x[0]\oplus(x[7]<<<1)]<<<1\}\\
&x[5]'=[x[0]\oplus(x[7]<<<1)]\oplus(x[4]<<7)\\
&x[4]'=x[7]\oplus(x[3]<<7)\\
&x[3]'=x[6]\oplus(x[2]<<7)\\
&x[2]'=x[5]\\
&x[1]'=x[4]\\
&x[0]'=x[3]\oplus i
\end{aligned}\tag{5}$$

其中，i 为轮数，$x[7]$、$x[6]\cdots x[0]$为 A 操作输入均分成的 8 个 32 比特的分组。

2.2 轮函数设计

ANT 轮函数采用 Feistel 结构，在每一轮中，左侧输出涉及两个循环左移、两次 G 操作和三个异或运算，右侧输出等于左侧输入，不参与运算。对于循环左移，由于各次移动位数相同，本文直接采用位拼接的方式改变输入信号，省去了移位运算。

G_0、G_1 操作是比特级非线性函数，仅采用比特级的与操作、异或操作和 PERM 置换操作[6]。由于各轮中比特置换 PERM 完全一致，本文则直接对相应比特位进行线网型赋值，不进行单独例化，从而减少不必要的运算和资源占用。G_0、G_1 操作功能一致但各轮输入输出信号不同，例化为元件，供各轮调用。G_0 实现流程如图 6 所示，G_1 与 G_0 操作类似，仅模数不同，故此处不再赘述。

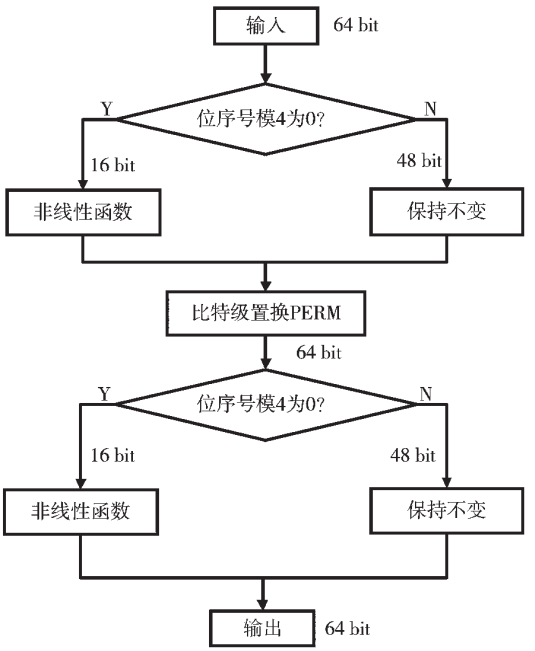

图 6　G_0 操作流程图

2.3 加解密模块设计

ANT 加(解)密模块中各轮相同功能模块只需实现一次并对其重复调用。由于轮函数每一轮的左输出即为下一轮的右输入；每一轮的右输出即为下一轮的左输入；又因为每轮右输入的值与上一轮左输入的值相同，采用有限状态机方式，定义了左右两组寄存器，实现数据在状态跳变时的依次传递。当系统检测到密钥扩展完成后，状态机跳转至工作状态，读取明(密)文数据。当状态依次更新时，各轮进行左右数据交换，并进行加(解)密运算，以此类推。ANT 算法加解密结构一致，本文仅以加密过程为例。具体流程如图 7 所示。

2.4 流水线设计优化

本文采用流水线结构[16-19]对算法进行速度优化。流水线是一种通过增加空间的利用来减少时间消耗的时空映射技术[20]，对电路逻辑进行系统分割，在各部分之间插入寄存器暂存中间数据，将大操作分解成若干个小操作。每一个小操作的时间短且支持并行计算。

ANT-128/128 算法包含 46 轮加解密运算，采用流水线结构可以实现轮运算的并行操作，大大提升加解密效率。在具体实现中，本文采用 46 级全级流水线结构，每

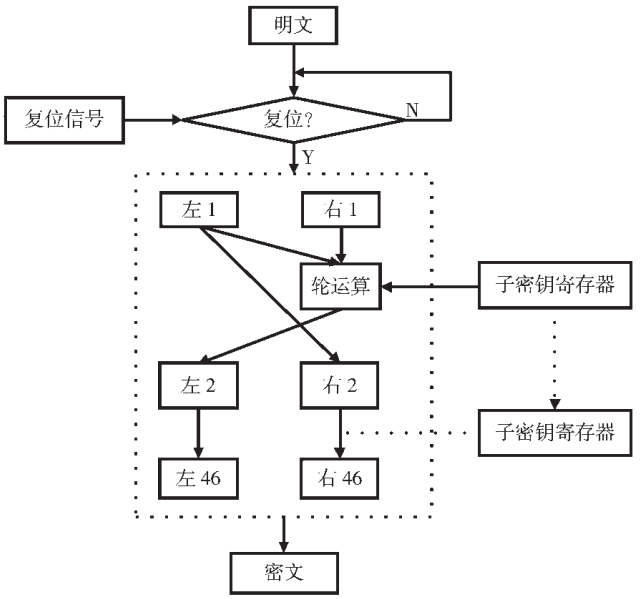

图 7 加密模块流程图

一轮函数运算结束后，其结果存入缓冲区中，供下一轮函数运算调用。同时，其本身也将从上一轮运算的缓冲区中提取数据，开始下一轮运算。与非流水线结构相比，该方法能够使效率显著提升。基于流水线的加密模块流程如图 8 所示。

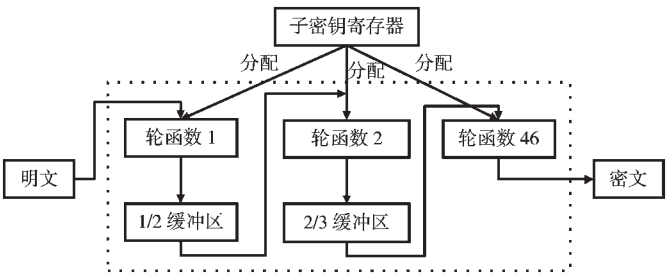

图 8 基于流水线的加密模块流程图

图 8 中，轮函数 1 使用第一组明文开始运算，将结果存入 1/2 轮缓冲区，同时读取下一组明文。轮函数 2 读取 1/2 轮缓冲区中的数据，将结果存入 2/3 缓冲区，并再次从 1/2 缓冲区中读取新的数据，以此类推。

3 仿真验证与性能分析

本文采用 Altera 公司 Cyclone V 系列的 5CGXFC7D6-F31C7ES 芯片，以 Quartus II 15.0 为开发环境对算法进行系统仿真验证与性能分析。

3.1 密钥扩展模块结果与性能分析

密钥扩展模块仿真波形如图 9 所示。为方便观察，图中仅列出了 00 轮至 05 轮、10 轮至 15 轮以及最后一轮的数据。算法作者给出的部分子密钥标准向量值如表 1 所示，可以得出：仿真结果与标准向量值一致。

表 1 部分轮次子密钥标准向量值

密钥类别	值(十六进制)
子密钥 10	5368192F9AD7E664
子密钥 20	3D97C746E490ACCB
子密钥 40	F1C52C0CD0D9405F
子密钥 46	157DCF6ADD035253

密钥扩展模块性能参数如表 2 所示。其中，逻辑单元 1 663 Slices，占总逻辑资源的 3%；寄存器 3 185 Slices；

表 2 密钥扩展模块性能参数

性能参数	综合结果
逻辑利用率	1 663/56 480(3%)
寄存器	3 185
接口	202
最大工作频率/MHz	247.52

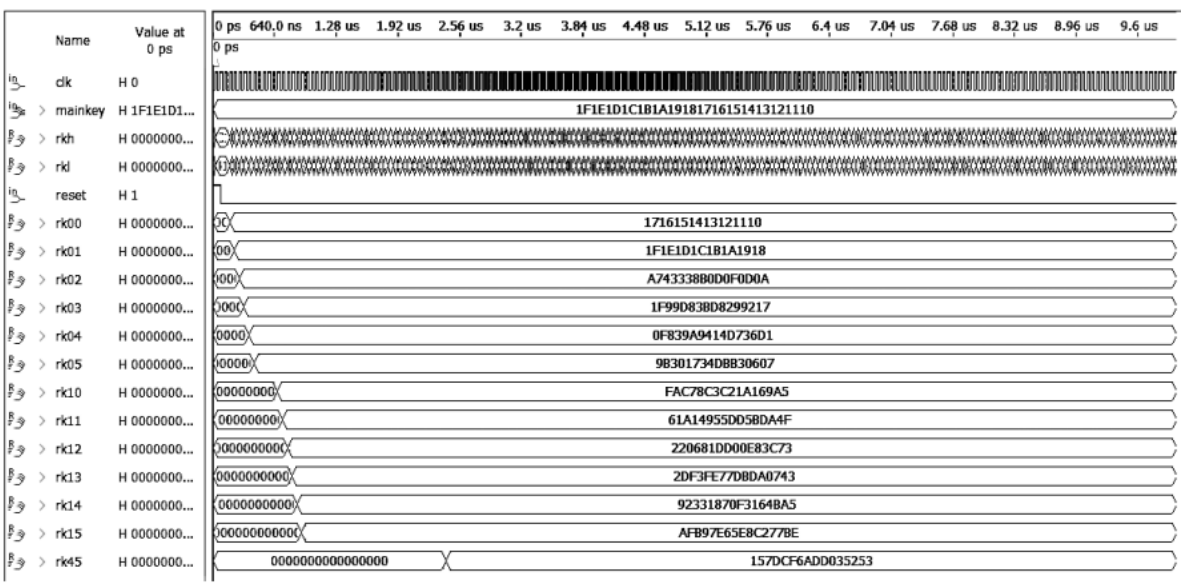

图 9 密钥扩展模块仿真波形图

综合最大工作频率 247.52 MHz。

3.2 加解密模块结果与性能分析

本文利用 Verilog HDL 语言进行了基于单轮单个分组数据的加密，并已将各轮子密钥存储于寄存器中。其中，采用有限状态机设计的仿真波形如图 10 所示，采用流水线设计的仿真波形如图 11 所示。算法作者给出的密文标准向量值如图 12 所示，仿真结果与标准向量值一致。

由表 3 可知，采用有限状态机设计的加解密模块占用资源较少，但运算速度不高，其吞吐率 v_1 为：

表 3 加解密模块性能参数对比

	有限状态机设计	高速流水线设计
逻辑利用率	521/56 480(<1%)	4 081/56 480(7%)
寄存器	305	13 455
接口	258	257
最大工作频率/MHz	241.2	338.52

$$v_1=(128\ \text{bit}\times 241.2\ \text{MHz})/46=669.6\ \text{Mb/s} \tag{6}$$

采用流水线设计进行优化后，虽然占用资源较多，但可以获得更高的工作频率，使得数据吞吐率得到极大提升。流水线设计的最大工作频率为 338.52 MHz，其吞吐率 v_2 为：

$$v_2=128\ \text{bit}\times 338.5\ \text{MHz}=43\ \text{Gb/s} \tag{7}$$

算法作者给出的硬件仿真(基于 HJTC110nm 标准元件库)数据中，加密吞吐率约为 1.3 Gb/s，而本文所得加密吞吐率为 43 Gb/s，约为其吞吐率的 33 倍。可见，ANT 分组密码算法的加密吞吐率在经流水线结构优化后显著提升。

4 结论

本文对 ANT-128/128 分组密码算法进行了相关研究，在用有限状态机结构对算法进行硬件实现后，采用流水线设计对加解密模块进行效率优化，并对二者进行了性能对比。其中，面向速度优化的流水线设计大大提高了加解密速率，在工作频率 339 MHz 下，生成一组 128 bit 的密文，速度达到 43 Gb/s。后续将会对其面积、速度进行更深入优化，进一步提升算法运行效率。

参考文献

[1] 王保仓，贾文娟，陈艳格.密码学现状、应用及发展趋势[J].无线电通信技术，2019，45(1)：1-8.
[2] 吕述望，苏波展，王鹏，等.SM4 分组密码算法综述[J].信息安全研究，2016，2(11)：995-1007.
[3] 张利华，吴松，蒋腾飞，等.基于 FPGA 的 SMS4 算法实现及在线验证[J].华东交通大学学报，2018，35(5)：111-116.
[4] DAEMEN J，RIJMEN V.AES proposal：Rijndael[OL].1999.

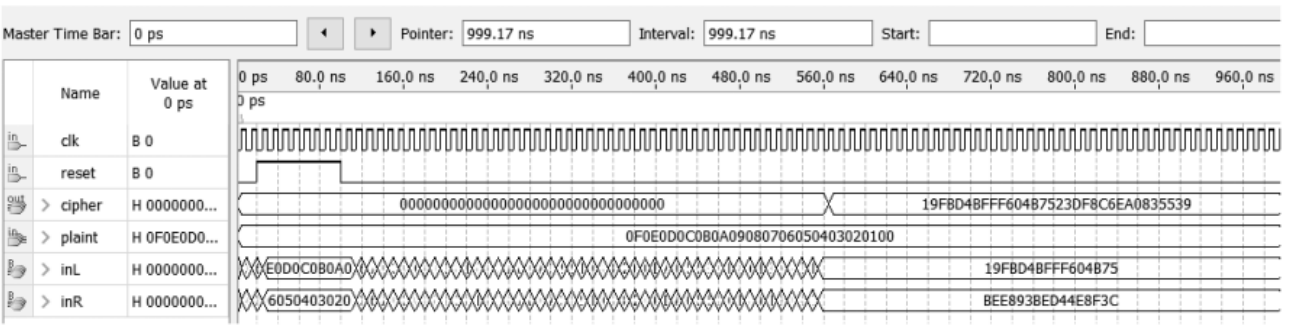

图 10 采用有限状态机设计的仿真波形图

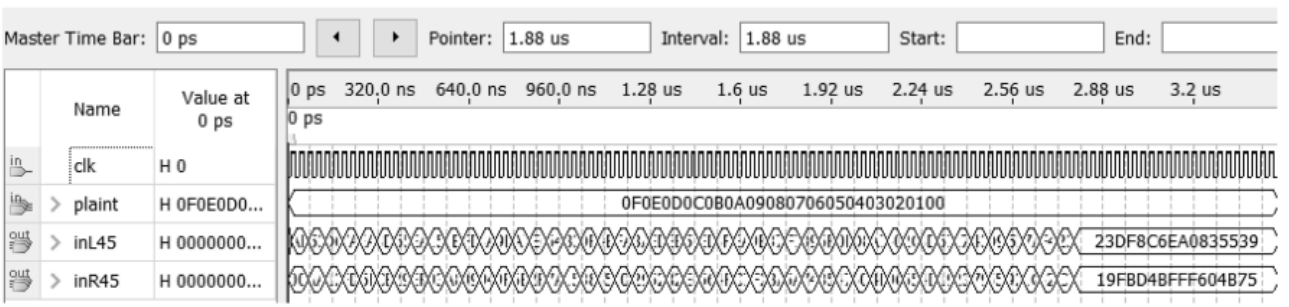

图 11 采用流水线设计的仿真波形图

```
round   045 : BEE893BED44E8F3C 19FBD4BFFF604B75 rk045 : F050611AA168DF4F
round   046 : 19FBD4BFFF604B75 23DF8C6EA0835539 rk046 : 157DCF6ADD035253
ciphertext is:
cy    19 FB D4 BF FF 60 4B 75 23 DF 8C 6E A0 83 55 39
```

图 12 算法作者给出的密文标准向量值

(下转第 144 页)

参考文献
[1] 谭铭,王春阳,李欣,等.对步进频雷达灵巧干扰的建模方法与仿真[J].传感器与微系统,2016,35(7):26-29.
[2] 金胜,朱天林,王海波.步进频雷达成像技术研究进展[J].飞行器测控学报,2013,32(6):490-495.
[3] 刘春生,鲍燕飞,伍波.难以干扰的几种新体制雷达[J].航天电子对抗,2001(2):28-30.
[4] 胡体玲,李兴国.毫米波步进频率单脉冲雷达及其信号处理[J].雷达科学与技术,2006,4(4):193-196.
[5] 刘柳.不断发展的毫米波对抗技术[J].飞机工程,2006(3):11-13,58.
[6] 凌永顺,同武勤,张鑫,等.毫米波对抗技术[J].光电工程,2004,31(7):1-4,41.
[7] 张宏伟,冯振,俞静一,等.对频率步进毫米波导引头的干扰研究[J].电子信息对抗技术,2010,25(4):35-38.
[8] 周政,唐宏,张永顺,等.基于时域采样的灵巧噪声干扰研究[J].现代雷达,2010,32(5):53-55.
[9] 徐晓阳,包亚先,周宏宇.基于卷积调制的灵巧噪声干扰技术[J].现代雷达,2007,29(5):28-31.
[10] 张智,赵健,李帅.针对频率步进雷达的一种灵巧噪声干扰方法[J].舰船电子对抗,2010,33(2):5-8.
[11] 尚志刚,白渭雄,董会旭.对PD雷达进行综合欺骗干扰研究[J].火力与指挥控制,2013,38(1):91-93.
[12] 邬诚,颜振亚.噪声调制灵巧噪声对雷达干扰性能研究与实现[J].现代雷达,2014,36(7):77-80.
[13] 向敬成,张明友.毫米波雷达及应用[M].北京:国防工业出版社,2016.
[14] 张江华,梁培康,刘逸平,等.毫米波导引头系统设计与工程实现[M].北京:国防工业出版社,2016.
[15] 张东坡,刘兴钊.基于NDFT的步进频率雷达信号处理[J].雷达科学与技术,2004,,2(5):289-292,314.
[16] 梁潇,袁业术.频率步进雷达信号的二维处理[C].2005年中国电子学会第十一届青年学术年会论文集,2005:709-712.

(收稿日期:2020-10-13)

作者简介:
项正山(1979-),男,硕士,高级工程师,主要研究方向:雷达对抗及信号处理。

(上接第136页)

[5] 习近平.在网络安全和信息化工作座谈会上的讲话[N].人民日报,2016-04-26(002).
[6] 陈师尧,樊燕红,付勇,等.ANT系列分组密码算法[J].密码学报,2019,6(6):748-759.
[7] 邹祎,李浪,贺位位,等.轻量级密码算法LBlock的FPGA优化实现[J].计算机系统应用,2015,24(7):240-243.
[8] HONG D,SUNG J,HONG S,et al.HIGHT:a new block cipher suitable for low-resource device[C].International Workshop on Cryptographic Hardware and Embedded Systems.Springer,Berlin,Heidelberg,2006.
[9] BOGDANOV A,KNUDSEN L R,LEANDER G,et al.PRESENT:an ultra-lightweight block cipher[C].Proceedings of Cryptographic Hardware and Embedded Systems,2007:450-466.
[10] SHIBUTANI K,ISOBE T,HIWATARI H,et al.Piccolo:an ultra-lightweight block cipher[C].Proceeding of the CHES 2011.Nara,Japan.LNCS 6917,2011:342-357.
[11] GUO J,PEYRIN T,POSCHMANN A,et al.The LED block cipher[C].Cryptographic Hardware and Embedded Systems-CHES 2011.Springer Berlin Heidelberg,2011:326-341.
[12] WU W L,ZHANG L.LBlock:a lightweight block cipher[C].Applied Cryptography and Network Security—ACNS 2011.Springer Berlin Heidelberg,2011:327-344.
[13] GÉRARD B,GROSSO V,NAYA-PLASENCIA M,et al.Block ciphers that are easier to mask:How far can we go?[C].Cryptographic Hardware and Embedded Systems—CHES 2013.Springer Berlin Heidelberg,2013:383-399.
[14] 高志权.高性能高安全的密码机研究[J].信息安全与通信保密,2019(11):28-35.
[15] 刘小平,何云斌,董怀国.基于Verilog HDL的有限状态机设计与描述[J].计算机工程与设计,2008(4):958-960.
[16] 孔昕,吴武臣,侯立刚,等.基于Verilog的有限状态机设计与优化[J].微电子学与计算机,2010,27(2):180-183.
[17] 蔡冰清,白国强.SM3杂凑算法的流水线结构硬件实现[J].微电子学与计算机,2015,32(1):15-18.
[18] 李磊,韩文报.FPGA上SHA-1算法的流水线结构实现[J].计算机科学,2011,38(7):58-60.
[19] 何星,张铁军,侯朝焕.流水线结构FFT/IFFT处理器的设计与实现[J].微电子学与计算机,2007(4):141-143,147.
[20] 周雍浩,董婉莹,李斌,等.可重构的SHA-3算法流水线结构优化及实现[J].现代计算机,2020(12):15-20.

(收稿日期:2020-09-23)

作者简介:
王建新(1977-),男,博士,副教授,主要研究方向:电子信息工程。
刘芮安(1997-),通信作者,男,硕士研究生,主要研究方向:密码算法的FPGA设计与实现,E-mail:ryenliu@sina.cn。
肖超恩(1982-),男,博士,讲师,主要研究方向:人工智能。

版权声明