文章编号：1672-2892(2010)03-0276-05

雷达系统超精简流式 AES 加密器设计和优化

周 斌，彭应宁，汤 俊

(清华大学 电子工程系，北京 100084)

摘 要：为了满足雷达系统对信息加密传输的要求，对高级加密标准(AES)的计数模式(CTR)重新设计，将其改进成流加密的工作模式。通过进行结构折叠和算法重用，有效地减小了资源占用，提高了吞吐率。在 Spartan3 型号的 FPGA 上，仅占用 728 个 slice 就可以实现 276.53 Mbps 的吞吐率。本设计实现了节省硬件资源的纯逻辑模式和速度较高的分布式内存模式，并且完成实时密钥调度和流水线设计，获得了高可靠性、高吞吐率和高安全性。通过对实际雷达数据的加密实验，验证了该设计的有效性，显示了流加密模式的 AES 在雷达系统加密传输中的强大潜力。

关键词：高级加密标准；流加密；现场可编程门阵列；精简结构

中图分类号：TN918.1 **文献标识码：**A

Design and optimization of compact AES as stream cipher in radar system

ZHOU Bin, PENG Ying-ning, TANG Jun

(Department of Electronic Engineering, Tsinghua University, Beijing 100084, China)

Abstract: In order to satisfy the encryption requirements of radar system data transfer, the Counter (CTR) mode of Advanced Encryption Standard(AES) was modified into a stream cipher. Through structure folding and module reuse, the resource utilization was reduced and the throughput was increased. In Spartan3 FPGA, 276.53 Mbps throughput could be achieved only by using 728 slices. The resource-saving pure logic mode and high-speed distributed memory mode were implemented in the design. On-the-fly key scheduling and pipeline were also performed, which led to high throughput and security level. The real-life test showed the design had satisfied the requirements of radar signal encryption, which revealed a great potential of stream mode AES in radar signal transmission.

Key words: Advanced Encryption Standard; stream cipher; FPGA; compact mode

高级加密标准(AES)是美国政府 2001 年 12 月公布并采用的最新加密标准。在美国 FIPS PUB 197[1]文献中，它被美国国家标准和技术研究局(NIST)宣布为最新的标准，并被广泛应用和深入研究。现在，AES 已经是对称加密密码学中最为流行的算法之一。通常 AES 被认为是块加密结构，其操作于独立的密钥和明文块，达到较高的吞吐率和安全性。流加密体系是另一类密码模式，其密文是所有处理过的明文和当前密钥的函数。流加密通常应用在资源受限的领域，比如手机、无线网、移动终端等。

通用的雷达信号传输系统中，数据流驱动机制要求数据的传输和处理处于一种流式的模式下。依照图 1 所示，数据从前端的高速 A/D 采样，不停地灌入到加密和处理系统中。雷达传输系统作为专用网络，传输其上的各种控制和模式指令，其安全性至关重要。信息安全传输成为必须重点考虑的内容。雷达网络具有数据传输量大，冗余数据多，安全性敏感，资源受限，实时性要求高等特点，要求加解密系统满足高效、高速和高安全性。

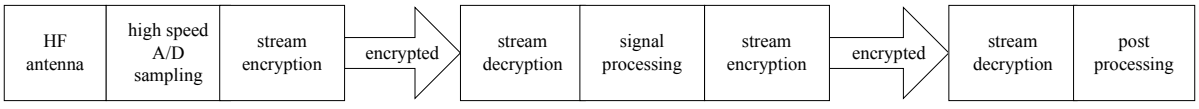

Fig.1 Encrypted data transfer in radar system
图 1 雷达系统数据加密传输结构图

收稿日期：2010-01-19；修回日期：2010-03-20

在文献[2]中，已经提出了把 AES 应用于雷达网中。而文献[3]中，则认为 AES 最为适合无线传感器网络。针对 AES 进行流加密转换，现有的研究包括：在文献[4]中，使用了特殊指令集的处理器结构来转换成流加密；在文献[5−6]中，介绍了精简结构 AES 的设计。本文不仅将探讨数据通路设计，而且会精简存储器和控制流程，提出新的超精简结构设计。设计结构通过对实际雷达图像的加密测试，验证其有效性。

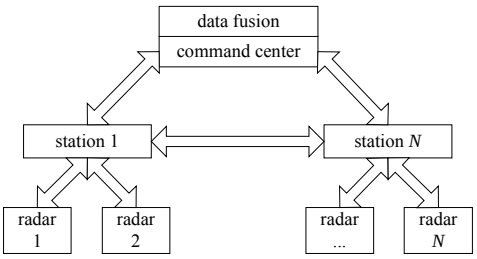

Fig.2 Architecture of radar network
图 2 组网雷达体系结构图

1　流式 AES 体系结构

1.1　标准 AES 体系结构

标准 AES[7]是基于多重循环替换和列混合密钥加操作的块加密算法。标准的 AES 具有 128 bit 的块长度和 3 个可变长度的密钥长度(128 bit,192 bit,256 bit)，各自对应 10,12,14 次的迭代操作。一轮迭代包含 4 组操作：ShiftRows,SubByte,MixColumn,AddRoundKey。图 3 展示了 AES 迭代操作的基本流程[5]。

图 4 展示了一轮加密迭代的具体操作。作用于 1 个 128 bit 的数据块，而通常该块会被组织成 16×8 的矩阵。加密结构以 1 byte 作为操作数的基本单元，所以最小的数据通路宽度为 8 bit。

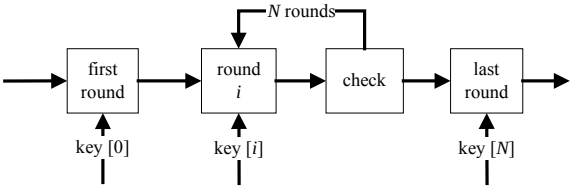

Fig.3 Basic AES processing rounds
图 3 基本迭代模式的 AES 流程图

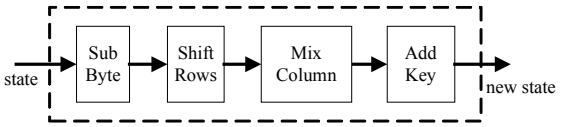

Fig.4 One round in encryption
图 4 加密的一轮操作

1.2　流加密模式设计

AES 通常被设计成块加密的模式，密钥彼此独立，明文块也彼此独立，每次加密器作用于 1 个完整的数据块。而流加密模式中，由加密器生成密钥流，通过与明文流作用而生成密文流。公式(1)表示了二者的不同。

$$\begin{aligned}&\text{block cipher:}\quad C_i = E_K(M_i)\\&\text{stream cipher: } C_i = E_K(m_i, m_{i-1}, \cdots, m_1, m_0)\end{aligned} \tag{1}$$

块加密通常吞吐率较高，安全性很高，但是资源占用多。而流加密则占用资源较少，同时具有较好的吞吐率和安全性。

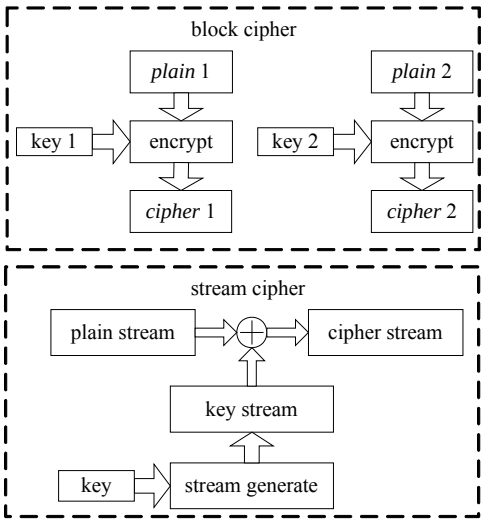

Fig.5 Block cipher and stream cipher
图 5 块加密模式和流加密模式结构图

1.3　工作模式的选择

AES的计数器模式(CTR)[6]、输出反馈(OFB)和密文反馈(CFB)模式都可以改造成流加密架构。但是流加密要求资源占用小，结构简单，可以实施流水线来提高吞吐率。这就要求加密和解密共享模块。但电文码(ECB)模式需要不同的加密解密模块，所以被排除。CTR,OFB 和 CFB 模式都可以添加流水缓冲的中间状态，CTR 模式没有反馈，故而选择 CTR 模式。流水线结构设计如图 6 所示。公式(2)表示算法流程，状态转移模式 $IS_{i+1}=IS_i+1$ 可以预测，故而流水线可连续吞吐。

$$\begin{aligned}&IS_1 = IV \qquad IS_{i+1} = IS_i + 1\\&C_i = E_K(IS_i) \oplus m_i \quad m_i = E_K(IS_i) \oplus C_i\end{aligned} \tag{2}$$

经典的密钥生成是预先计算密钥，然后存放在存储器，当加密时读入，这会浪费很多计算周期并且增加资源占用。实时的密钥生成会在每一个加密轮自动生成需要的密钥，从而克服这些缺点[8]。

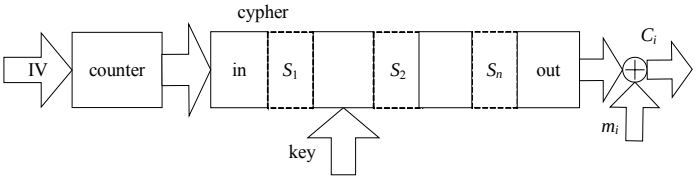

Fig.6 CTR mode and pipeline design
图 6 CTR 模式以及流水线设计

2 精简模式的 AES 体系结构

通过对 AES 的细致研究，可以发现它的体系结构中蕴含着大量的并行性和流水线空间。可以逐步精简数据通路，设计极其精简的模式，而且具有较好的吞吐率。

2.1 完全 128-bit 模式

图 7 表示了完全模式的 128-bitAES 加密架构。其包含 16 个 SubByte 单元，4 个 MixColumn 和 128 bit 的 AddRoundKey 操作。

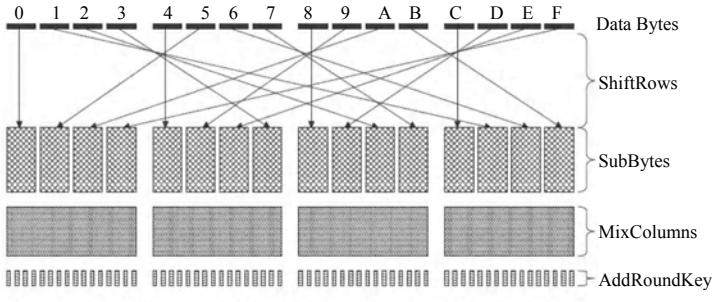

Fig.7 Complete 128-bit mode
图 7 完全 128-bit 模式结构

2.2 精简 32-bit 模式

分析图 7 的完全架构，其 SubByte, MixColumn 和 AddRoundKey 操作是作用于独立的 32 bit 的状态空间，只有 ShiftRows 作用于所有的字节。该结构可以存储中间状态，设法重复利用子字节、列混合和密钥加模块。所以通过折叠操作，可以设计如图 8 的 32-bit 精简结构。

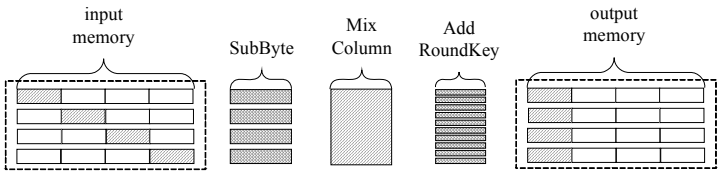

Fig.8 Compact 32-bit mode
图 8 精简 32-bit 架构

通过如下的 4 步操作，可以将一轮加密操作通过 4 个周期完成：

1) 读入输入的位置：0,5,A,F；执行 SubByte,MixColumn 和 AddRoundKey 操作，输出结果存放到 0,1,2,3 位置。这步操作在图 10 中用阴影表示。

2) 重复上面操作，作用于输入位置的 4,9,E,3 字节；并且将输出结果保存于 4,5,6,7 位置。

3) 重复操作，作用输入位置的 8,D,2,7；输出结果到 8,9,A,B。

4) 重复操作，作用输入位置的 C,1,6,B；输出结果到 C,D,E,F。此时输出存储器保存的就是最终一轮结果。

然后交换输入输出存储空间，进行下一轮的操作，直到达到需要操作的轮数，最终的输出就会作为加密输出。以上精简结构完成完整的 128-bit 加密需要 4 倍于完整结构的时钟周期。

2.3 精简 8-bit 模式

继续探索 AES 精简结构的并行性，发现其中的 SubByte 和 AddRoundKey 操作依然独立地操作于 1 个 8 bit 的字节上，所以可以继续重复利用这 2 个模块。图 9 展示了一种更加精简的 AES 轮操作。此种结构充分挖掘了并行性，但是每周期只能操作 1 byte 的操作数。通过将 4 byte 的数据缓冲之后，发射到列混合操作单元，其他操作和 32-bit 操作一致，但资源占用大幅减少，性能将减弱为 1/4 左右。

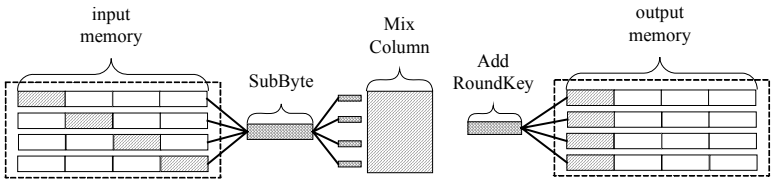

Fig.9 Compact 8-bit mode
图 9 精简 8-bit 的架构

2.4 纯逻辑运算的 S-Box

S-Box 单元基本实现是一个简单的查找表，但是其包含了在 GF(2^8)域上的倒数运算和仿射变换，用于扩散不同的位。其基本数学表达[5]为：

$$s' = \boldsymbol{MX}(\boldsymbol{X}^{-1}s)^{-1} \qquad (3)$$

其中 $\boldsymbol{MX}$ 是仿射变换矩阵，$\boldsymbol{X}^{-1}$ 是用于向 GF(2^8)域转换的转移矩阵，如图 10 所示。所有的乘操作都是在 GF(2^8)域上进行。

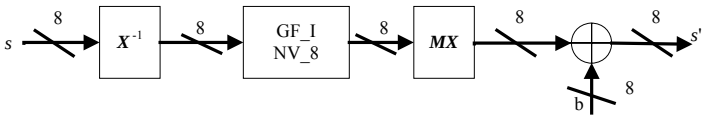

Fig.10 Logic expression of SubByte operation
图 10 SubByte 操作的具体逻辑表达

GF(2^8)域的乘法、加法和求逆运算可以通过分解到 GF(2^4)域上解决，依次类推，GF(2^4)域操作可以到 GF(2^2)域，最终转化到 GF(2)域，此时的操作将非常简单，仅包含“与非”和“与”操作[5]。纯逻辑运算的子字节操作仅由最基本的逻辑门运算组成，所以将大大地节省资源，并且有利于流水线设计。经过实际测试，其可以比分布式内存的查找表实现节省一半以上的资源。

3　超级精简结构设计

仔细研究和分析 AES 加密轮和密钥生成的过程，所有操作都可以分解为最基本的运算，包括 MixColumn,SubByte 和异或操作。操作运作于不同的内存空间，配合完成整个加密、解密和密钥生成过程。图 11 展示了整体架构设计，控制逻辑负责管理对内存地址的生成，而数据通路则通过 1 个多路选择器分时接入到存储单元。整个 AES 加密迭代操作可以通过 1 个 2 层循环完成，所以其控制指令代码也相对较少，可以放入较小的器件中，节省资源。

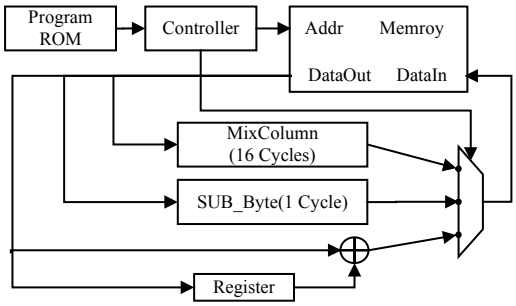

Fig.11 Extreme compact mode
图 11　超级精简结构设计

图 12 展示了精简结构 MixColumn 设计。MixColumn 主要包括乘和异或操作，通常的 MixColumn 作用域是一个 8×4 bit 的多字节模块。但是通过分解操作，可以得到如公式(4)的流式操作算法流程。建立如图 13 的流程控制，可以使用 16 个时钟周期来完成 32 bit 的 MixColumn 操作。

超级精简结构设计会大大减少资源占用，但是吞吐率在相同时钟周期的情况下变为原来的 1/16[9]。

$$b_0 = a_3 \oplus a_2 \oplus 2a_0 \oplus 3a_1 \quad b_1 = a_0 \oplus a_3 \oplus 2a_2 \oplus 3a_1$$
$$b_2 = a_0 \oplus a_1 \oplus 2a_2 \oplus 3a_3 \quad b_3 = a_1 \oplus a_2 \oplus 2a_3 \oplus 3a_0 \tag{4}$$

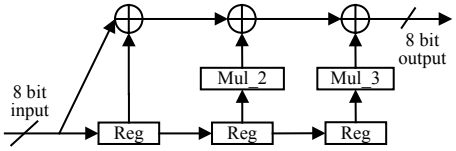

Fig.12 Folded MixColumn
图 12　精简的 MixColumn 结构设计

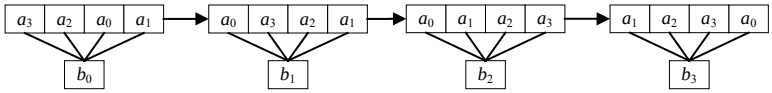

Fig.13 Processing of MixColumn in extreme compact mode
图 13　超精简结构的 MixColumn 处理流程图

4　实际测试结果和分析

通过使用 Xilinx 的 ISE 开发工具包，并且针对其低端器件 Spartan 3 来实现。所有的源代码是可综合的 VHDL 代码，作为主要的对比指标，笔者侧重吞吐率和吞吐率/面积比这 2 个指标。表 1 展示了不同的结构模式的具体性能[10]。结果显示使用纯逻辑结构的子字节，8 bit 的数据通路具有最小的资源占用，但是吞吐率较低；32 bit 的数据通路具有较好的吞吐率，资源占用较高。

表 1　在 Spartan3 上的测试结果
Table1 Test results on Spartan 3

S-Box	data path	bank #	area (slices)	max clock/MHz	max throughput/Mbps	throughput/area(×10^3)
RAM	8	2	689	117.60	85.84	124.59
RAM	32	2	728	95.026	276.53	363.85
logic	8	2	437	75.622	55.20	126.33
logic	32	2	669	58.367	169.85	253.88

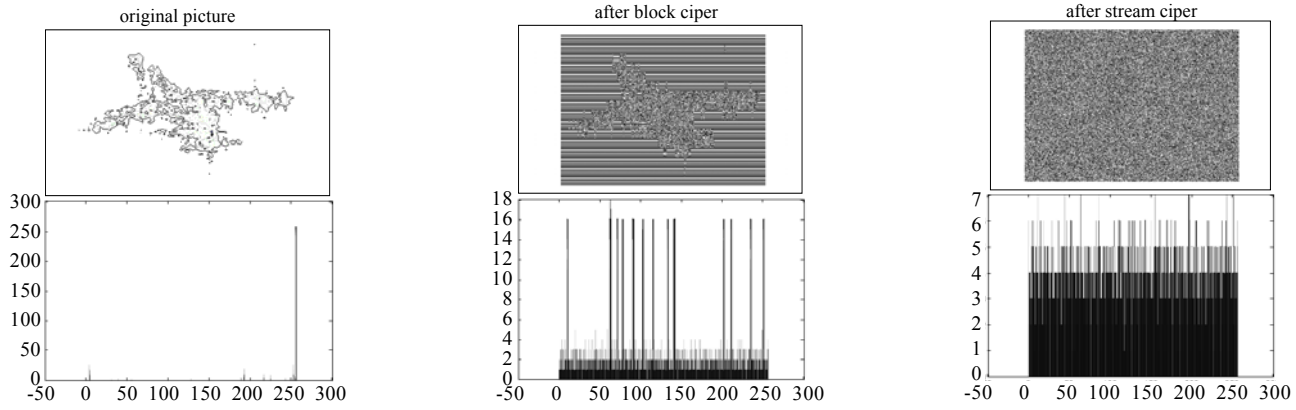

Fig.14 Histogram of real-life radar data
图 14　实际加密测试和图像的灰度直方图

图 14 展示了原始图像、块加密图像和流加密图像的结果和各自的灰度直方图。由于该图像本身灰度比较集中，可以看出经过块加密，纹理部分依然存在。而改用流加密处理之后，纹理消失，数据的随机性加强，其灰度

直方图的分布也可以直接体现这一点。通过公式(5)计算不同图像的信息熵[11]

$$H(P)=-\sum_{i=0}^{255}p(x_i)\log_2(p(x_i)) \tag{5}$$

可以得到如表 2 的结果。经过 AES 加密之后的信息熵得到了极大的增加，逼近理论极限值 8。当系统越接近均匀分布，其熵越大，从直方图中可以明显看出，流加密的图像分布已经比较均匀。从信息论原理可知[11]，信息熵越大，系统混乱程度越高，从而可以有效对抗统计攻击等模式的密码分析手段。

表 2 与其他的实现性能对比

Table2 Comparison among different modes

dataset	original	block cipher	stream cipher
entropy	0.513 5	5.590 1	7.966 0

5 结论

在本文中，通过 CTR 模式，将 AES 改进成为流加密模式，并且设计了不同长度的数据通路。本研究实验了实时密钥调度、纯逻辑运算 S-Box、分布式共享内存与超级精简结构设计等。通过在 FPGA 上进行验证，可以得到较小的资源占用和较高的吞吐率，并且安全性得到了有效保证。更进一步，通过对实际雷达数据进行加密和解密实验，发现流式 AES 可以有效地对数据进行离散化，提高信息熵，增加了破解和攻击的困难。后续的研究工作包括设计更加精简的特殊指令集和更加高性能的数据通路设计，以及进行大规模的应用测试和应对各种攻击模式的压力测试等。

参考文献：

[1] NIST. Specification for the ADVANCED ENCRYPTION STANDARD (AES)[S/OL]. Springfield: National Institute of Standards and Technology. (2001-11-26)[2010-04-29]. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[2] 吴瑕,韩德红,谷京朝. Rijndael算法的改进及其在雷达网数据加密中的应用[J]. 空军雷达学院学报, 2005,19(4):43-45.

[3] 焦四辈,黄波,左朝树,等. 无线传感器网络中的分组加密算法评测与分析[J]. 信息与电子工程, 2008,6(4):258-261.

[4] Good T,Benaissa M. AES as Stream Cipher on a Small FPGA[C/OL]// International Symposium on Circuits and Systems (ISCAS 2006), Island of Kos, Greece. (2006-09-11)[2010-04-29]. http://ieeexplore.ieee.org/search/freesearchresult.jsp?newsearch=true&queryText=AES+as+Stream+Cipher+on+a+Small+FPGA&filter=&x=51&y=22.

[5] Pawe l Chodowiec,Kris Gaj. Very Compact FPGA Implementation of the AES Algorithm[G]// Cryptographic Hardware and Embedded Systems-CHES 2003, New York:Springer, 2003.

[6] Kris Gaj,Pawel Chodowiec.FPGA and ASIC Implementations of AES[M]. New York:Springer, 2009.

[7] Housley R. Using Advanced Encryption Standard(AES) Counter Mode With IPsec Encapsulating Security Payload(ESP)[EB/OL]. (2004-04-01)[2010-04-29]. http://tools.ietf.org/html/rfc3686.

[8] Lipmaa H,Rogaway P,Wagner D. CTR-Mode Encryption, Comments to NIST concerning AES Modes of Operations[R]. Baltimore, Maryland:Symmetric Key Block Cipher Modes of Operation Workshop, 2000.

[9] Good T,Benaissa M. AES on FPGA from the Fastest to the Smallest[G]// Cryptographic Hardware and Embedded Systems CHES 2005. New York:Springer, 2005.

[10] Zhou B, Peng Y N, Gaj K,et al, Implementation and comparative analysis of AES as a stream cipher[C/OL]// ICCSIT 2009, Beijing, China. [2010-04-29]. http://www.computer.org/portal/web/csdl/doi/10.1109/ICCSIT.2009.5234770.

[11] Zeghid M,Machhout M,Khriji L Baganne A,et al. A modified AES based algorithm for image encryption[J]. International Journal of Computer Science and Engineering, 2007,1(1):70-75.

作者简介：

周 斌(1980-)，男，山东省烟台市人，在读博士研究生，主要从事加密系统、高性能嵌入式计算、高速信号处理研究.email: zhoubin06@mails.tsinghua.edu.cn.

彭应宁(1939-)，男，成都市人，教授，博士生导师，从事高速实时数字信号处理和自适应信号处理研究多年，现在的研究方向是谱估计、自适应滤波、阵列信号处理、雷达信号处理等.

汤 俊(1973-)，男，南京市人，博士，副教授，博士生导师，主要研究方向为高速数字信号处理、自适应信号处理等.