2001 年 6 月
第 22 卷 第 3 期

湛江师范学院学报
JOURNAL OF ZHANJIANG NORMAL COLLEGE

Jun.,2001
Vol.22 NO.3

一种新的基于 FPGA 的加密技术

李赤松,肖道举,余祥宣
(华中科技大学 计算机学院 ,湖北 武汉 430074)

摘 要:介绍和讨论基于 FPGA 的硬件技术实现分组加密算法时所采用的 4 种结构及其性能.同时对 5 种 AES 侯选算法的软件实现和 FPGA 实现的结果和性能进行比较分析.

关键词:FPGA ;VHDL 硬件描述语言 ;数据加密标准 ;分组加密 ;密码
中图分类号:TP 309 **文献标识码**:B **文章编号**:1006 - 4702(2001)03 - 0037 - 06

随着对高速度、高容量安全通信同物理安全相结合要求的增长,利用硬件实现的加密设备将会在新世纪得到极大的发展.加密算法用硬件描述语言 VHDL 进行设计描述,然后经逻辑综合、优化,最后装配至 FPGA 器件,这种技术相当于可重配置的硬件,为将来加密设备的销售商和用户提供了极大便利.VHDL 语言使设计描述快捷方便,FPGA 技术能将大量逻辑功能集成于一个单片 IC 中,适用于各种应用环境,它的应用将产品设计的前期风险投资降至最低,利用这种技术开发的产品能在短时间上市,具有高机动性(包括可对硬件频繁修改)和低开发费用.[1]

1 密码系统基本构成

一个用硬件实现的对称分组加密算法基本系统主要由如下 5 个部分组成:

a. 加密/解密单元,用于对输入的数据加密及解密;

b. 密钥发生器,用来把一个外部密钥生成一组内部加密密钥;

c. 输入接口,用来将输入的数据块和内部密钥装入相应的电路以及储加/解密的数据;

d. 输出接口,用来暂时存储加密/解密部件的输出,并将它们送给外部存储器;

e. 控制单元,用来产生所有的控制信号.

2 算法具体操作模式

算法在实际应用中有不同的操作模式,在不同操作模式下同一个结构的性能(如速度、空间)也不同.因此,在讨论和比较如下 4 种硬件结构的性能时,必须考虑算法的具体操作模式.对称分组加密算法在具体使用时有好几种操作模式,从硬件实现的观点来看,这些模式可分为两类:

a. 非反馈模式,如电子密本(ECB),计数器模式;

b. 反馈模式,如密码分组链接模式(CBC),密文反馈模式(CFB),输出反馈模式(OFB).

在非反馈模式中,后续块的加密与前块的加密结果无关,即所有块的加密可并发执行.在反馈模式中,后续块的加密与前块的加密结果有关,后续块的加密只有在前块的加密完成后才能开始.因而,所有块的加密必须串

收稿日期:2001 - 02 - 28

作者简介:李赤松(1976 -),女,江西南丰人,华中科技大学硕士生,从事计算机信息加密技术研究.

行执行,不可能并行.[2]

根据当前的加密标准,数据的加密多采用反馈模式,如CBC、CBF;而非反馈模式,如ECB,则主要用于密钥分配时加密会话密钥.因此,使用当前的加密标准不能充分体现利用硬件实现的传统密钥算法在结构上实际上可并行处理多个数据的优势.

3 加密/解密部件采用的结构

3.1 基本结构(Basic Architecture)

在这种结构中,只有一个寄存器和多路开关,以及与算法中的一轮迭代对应的组合逻辑电路.输入的数据块(假定为128bit)通过多路开关送入电路,并被存放在寄存器中.在接下来的一个时钟内完成一轮加密计算,计算的结果又通过多路开关反馈回电路,并存放在寄存器中,如图1所示.则加密一个数据块所需的时钟数等于加密的轮数。

我们定义加密执行的速度为在单位时间内能够加密的数据位(bit)数,这样定义的速度通常又称为电路的吞吐量.那么,这种结构的速度为

$$Speed_{ba} = 128bit/(KT_{ba} + Kt)$$

其中T_{ba}为时钟周期,t为多路开关延时、寄存器的时钟输出延时和信号建立时间之和,K为算法规定的加密轮数(以下同)。

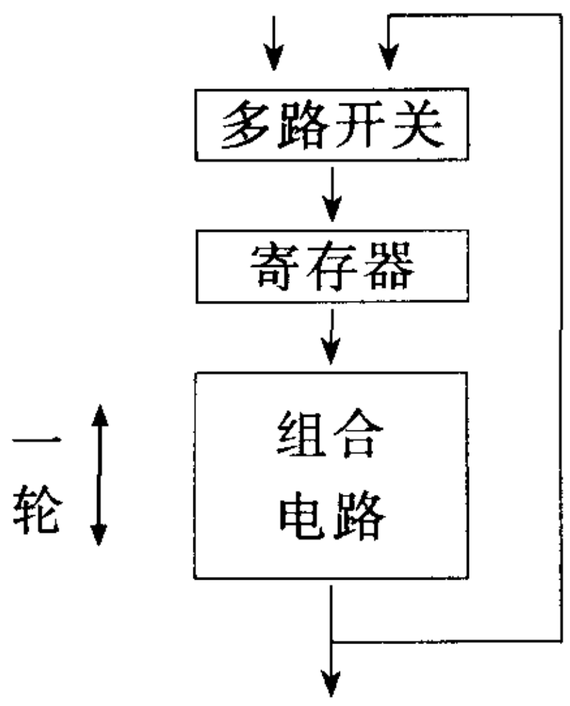

图1 基本结构

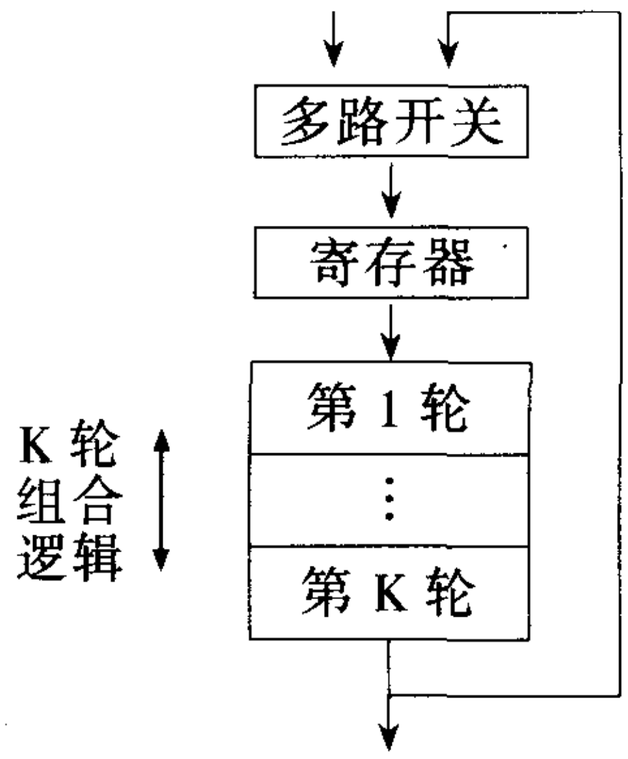

图2 循环展开结构

基本结构具有良好的速度,所需的空间也很少.

3.2 循环展开结构(Loop Unrolling Architecture)

如图2所示,循环展开结构和基本结构的唯一区别就是组合逻辑电路部分实现的是K轮加密而不是1轮.在循环展开结构中,加密一个数据块所需时钟数为1,时钟周期T_{lu}接近(略微低于)基本结构时钟周期T_{ba}的k倍,但由于每轮加密完成后数据不需经多路开关反馈回电路,加密速度有所提高.总体来讲,循环展开结构和基本结构实现的加密速度之比为:

$$Speed_{lu}/Speed_{ba} = (KT_{ba} + Kt)/(T_{lu} + t) = \frac{1 + t/T_{ba}}{1 + t/KT_{ba}}$$

在这种结构中,速度的提高是以空间的增加为代价的.加密/解密部件所用的总空间差不多与K成正比.同样,用于单个时钟的内部密钥数也增加了K倍,在采用FPGA实现时就意味着用于存储内部密钥的CLB(可配置逻辑块)数量呈K倍增加.因此,只有每轮循环占用空间小,同时每轮时延与多路开关延时、寄存器的时钟—输出延时和信号建立时间之和相比也较小的算法适合采用循环展开结构.

总之,对于反馈模式和非反馈模式,循环展开结构都能有效地提高电路速度,虽然提高不是很多,并导致空间的大量增加.

3.3 内部循环流水线结构(Inner - round Pipelining Architecture)

内部循环流水线结构由基本结构发展而来.流水线是提高数字电路在单位时间内处理数据量的常用方法,

它的概念是把在一个时钟周期内执行的逻辑操作分成几步较小的操作,并在多个较高速的时钟内完成.如图 3 所示,在这种结构中,与一轮加密对应的组合逻辑被均分为 n 个部分,并在各个部分之间添加一个额外的寄存器,其余部件与基本结构相同.这些分割得到的组合逻辑电路部分称为流水线站,每个流水线站执行不同的处理步骤.用这种方法,电路可以同时处理多个数据块,提高系统在单位时间内处理的的数据量,也就是速度.在每一个时钟周期,被部分处理过的数据块移入下一个流水线站,后续块则紧跟其上,占据它原来的位置.也就是说,一个流水线电路可以同时加密与它所含有的流水线站数量相等的数据块.

那么,这种结构的速度为 $Spead_{ip} = \frac{128bit}{KT_{ip}}$,其中 T_{ip}为通过流水线的最小时钟周期.理想情况下,T_{ip}接近(略微高于)基本结构时钟周期 T_{ba}的 1/n.

以一个具有 3 个流水线站的流水线为例,在理想情况下每个流水线站的时延相同,为分割前时钟周期的 1/3(当然我们并没有计算寄存器的时钟—输出延时和信号建立时间,因此实际的时延应该稍大)则该流水线的时钟频率为分割前的 3 倍.在头 3 个时钟周期内,3 个数据块循序进入流水线,接下来的时钟内,这些数据块在流水线内循环,每 3 个时钟对应一轮加密.在第 3K + 1 个时钟,第 1 个数据块,B1,离开流水线,第 4 个数据块,B4,进入轮空的流水线站.紧接着的 2 个时钟内,数据块 B2、B3 离开流水线,它们的空位由 B5、B6 代入.

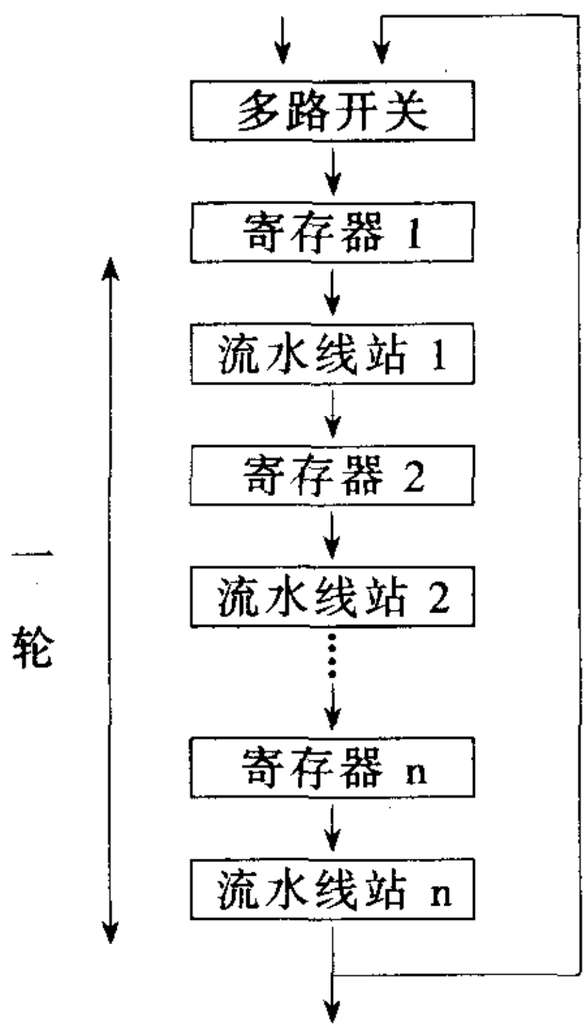

图 3　内部循环流水线结构

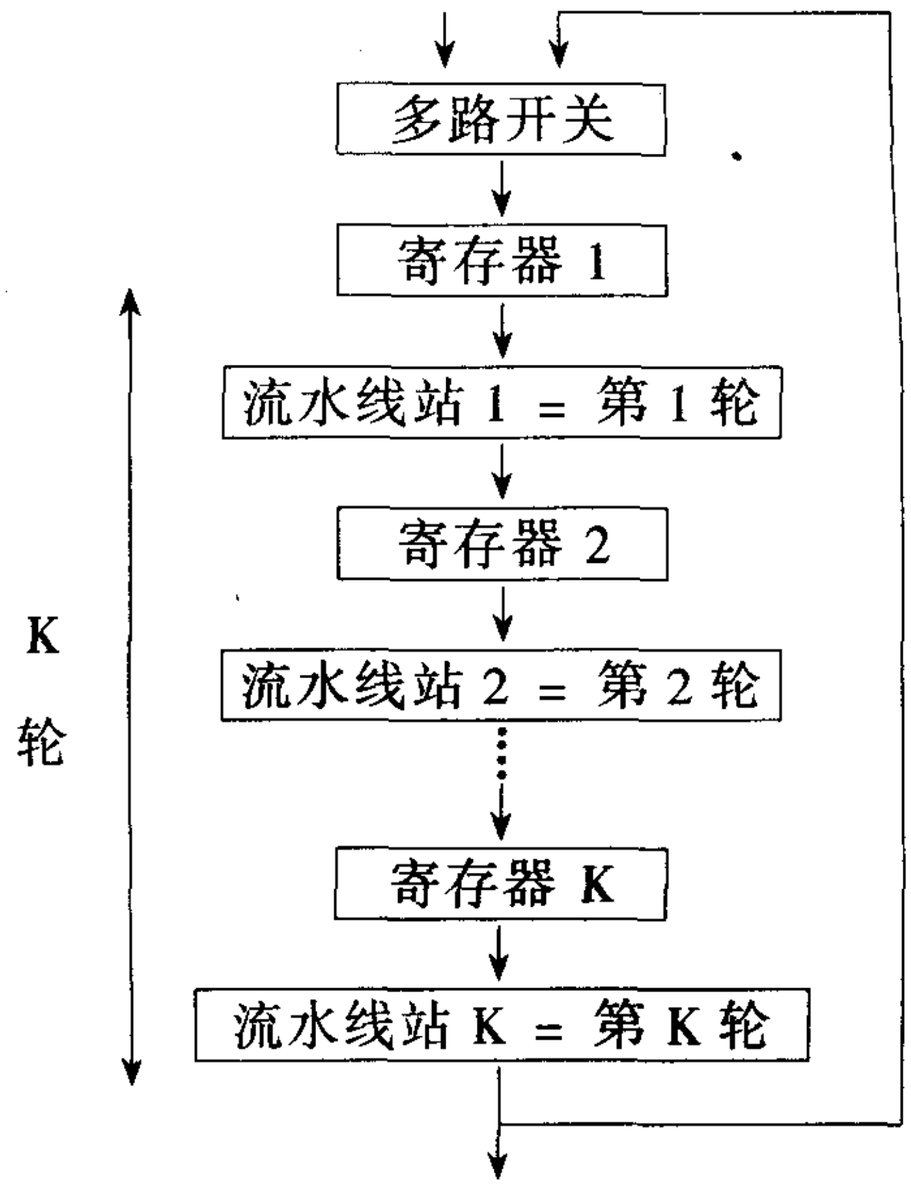

图 4　外部循环流水线结构

在内部循环流水线结构中,附加的寄存器并不影响电路吞吐量,算法速度随流水线站数的增加而增大.但由于算法本身的结构,流水线站的划分不是随意的,存在一个上限.流水线站数的最大值由组合电路中最大功能部件的时延决定.对算法而言,很难将实现它一轮加密的组合电路划分成几个具有相同时延的部件,尤其是当电路是用高性能的硬件描述语言,如用 VHDL 来描述时,算法速度的提高就受到限制.因此,适合采用这种结构的算法应具有下面两个特性:

1) 算法的一轮循环由许多层构成,并且每一层的时延相差不大,在同一个量级上.

2) 算法的一轮循环中不包含大的、难以分割的功能模块.

在内部循环流水线结构中,电路空间虽然也随流水段数的增加而增加,但比例很小,增加的部分主要是 128bit 寄存器的空间,对 FPGA 电路而言就更是这样了,因为 FPGA 的 CLB 本身就含有寄存器,在用于非流水线结构时,这些寄存器没有得到充分利用.

3.4　外部循环流水线结构(Outer - round pipelining architecture)

外部循环流水线结构由循环展开结构发展而来.具体方法是在组合电路中与每一轮加密对应的部件之间都插入额外的寄存器,其结构示意图如图 4 所示.因此,它的流水线站数为加密的轮数 K.

用外部循环结构实现的加密部件的空间与流水线站数 K 成正比.在非反馈模式中,如 ECB,算法的速度与流

水线站数 K 成正比,因此,外部循环结构可以直接以空间换速度.而在反馈模式中,算法的速度不依赖于流水线站数 k,所以这种流水线结构不适合于反馈模式的算法.

3.5 资源共享结构

对于某一些算法,可以通过分时共享一些资源来进一步减小电路空间,即,在不同的时钟周期内可以使用相同的功能部件对数据块的两个或更多的部分进行处理.例如,一个数据块分为 L、R 两部分,L、R 用两个完全相同的功能部件并行进行相同的处理,采用资源共享结构后,两个功能部件保留一个, L、R 的处理由并行变为串行,所需的时钟数为原来的 2 倍.

资源共享结构不适用实时响应要求高的设备,因为它所节约的空间与电路速度的损失相比很小,而且对称算法在用基本结构实现时所占用的空间本身就很小.

4 各种结构的比较

在比较各种结构时,我们重点考虑 3 个方面的性能:最大速度(吞吐量),所需的最小空间,以及最大的速度/空间之比.

4.1 非反馈模式

非反馈模式中,后继块的加密与前块无关,理论上所有块的加密可以并发执行,这样无论是内部循环流水线结构还是外部循环流水线结构,在进行数据块加密时都不存在块与块处理的优先问题,也就是说在流水线站划分时只需要考虑算法本身的结构和算法中各个模块的时延.

对非反馈模式而言,采用外部循环流水线结构实现的算法速度与流水线站数 K 成正比,而在外部循环流水线结构中流水线站数 K 等于算法要求的加密轮数,但由于外部循环流水线结构所占用的空间也和流水线站数 K 成正比,即速度的提高是以空间的成比例增加为代价的,所以这种结构的速度/空间比最低.由于内部循环流水线结构是通过提高电路时钟频率的方式来提高处理速度的,当流水线站数 n 增加时,速度的增长虽然与 n 的增长不成正比,但空间的相应增长极小,因而它具有最高的速度/空间比.由于内部循环流水线结构的流水线站的划分受算法中一轮加密的结构控制,流水线站数 n 不能任意增加,而且当 n 等值增加时,速度的增加量逐渐减少.而结合了资源共享的基本结构所占用的空间是最小的.

4.2 反馈模式

反馈模式中,后续块的加密与前块的加密结果有关,因而所有块的加密必须串行执行,不可能并行.在这种情况下,由于外部循环流水线结构的每个流水线站完成的是一轮加密而不是一轮加密中一个步骤,而对称分组加密算法的每一轮加密执行的操作都是相同的,因此,这种结构在反馈模式下不存在任何并行性,即算法的速度不依赖于流水线站数 K.K 增大时速度保持不变,而空间却与 K 成正比例增长,毫无效率可言.同样的,虽然内部循环流水线结构的每个流水线站完成的是一轮加密中一个步骤,但由于流水线站划分时不但要考虑各个步骤的时延,还要考虑前块与后继块加密的时间间隔,这意味着最大时延的值与加密一个数据块的时延相同.对依靠提高电路时钟频率来增加运算速度的内部循环流水线结构而言,经由划分流水线站而得到的时钟频率与划分前相比不但没有增加,反而减小,所以速度随流水线站数 n 的增加而减小.综上所述,流水线结构不能在反馈模式中使用.

基本结构在两种模式中的速度相同,所以反馈模式中,最大的速度/空间比可以经由这种结构得到,最大的速度在循环展开结构中获得,但是以空间的显著增加为代价的.可以得到最小空间的结构是资源共享结构,同样是以速度的锐减为代价的.

5 AES 侯选算法软/硬件执行结果比较

5.1 硬件执行结果介绍

算法采用基本结构,用 Xilinx 公司生产的 FPGA 器件 XCV100BG560 - 6 实现.硬件实现不包括密钥发生器部件,每轮加密所需的内部密钥预先计算生成,并存放在寄存器中,电路在执行加密时只需将它们取出送入加密/解密部件即可.表 1 是采用基本结构时 AES 5 种侯选算法的执行参数,表 2 给出了执行结果.[3, 4]

表 1　采用基本结构时的具体参数

	密钥/分组长度(bit)	时钟周期(ns)	循环轮数
Serpent	(128,128)	94.3	4
Rijndael	(128,128)	38.6	10
Twofish	(128,128)	45.1	*16*
RC6	(128,128)	61.6	20
Mars	(128,128)	100.6	32

表 2　用 XCV100BG560 - 6 实现的代价

	速度(Mbit/s)	空间(CLB 片)	速度/空间(Kbit/s·CLB 片)
Serpent	339.4	4438	76.5
Rijndael	331.5	2902	114.2
Twofish	177.3	1076	164.8
RC6	103.9	1139	91.2
Mars	39.8	2737	14.5

5.2　软件执行结果介绍

表 3 给出了采用软件技术实现 AES 侯选算法的最好结果.[5]

表 3　软件实现的代价

	密钥/分组长度(bit)	加密时钟周期	实现方式
Rijndael	(128,128)	363	32 位处理机,Visual C++
Twofish	(128,128)	285	Pentium Pro/II 处理机,汇编语言
RC6	(128,128)	254	200MHz 主频,汇编语言
Mars	(128,128)	300	PowPC 604e,C set ++ 3.1.1

5.3　硬件执行结果与软件执行结果的比较

比较表 1 和表 2 可以看出,循环轮数越小的算法速度越快.原因在于,基本结构中,$Speed_{ba} = \frac{128bit}{KT_{ba} + Kt}$,所以 Serpent 的时钟周期虽然仅次于 Mars,但它的循环轮数只有 4,因而速度最快,与采用软件实现时比其他侯选者慢 1.5 ~ 6 倍的结果完全相反.Rijndael 依托的理论伽罗瓦域 $GF(2^n)$ 中的计算能用线性反馈移位寄存器用硬件快速实现,因此它的时钟周期最小,加上只需循环 10 轮,所以速度极快.同等条件下,在 32 位处理机上用 Visual C++ 实现 Rijndael 加密/解密最少需 363 个时钟周期,假设 32 位处理机的主频为 500MHz,则软件实现的速度为 176.3Mbit/s,远小于硬件.与 Twofish 和 RC6 相比,Serpent 与 Rijndael 都是以大量的空间为代价实现的高速算法.在不增大占用空间和采用非反馈模式为前提的条件下,提高它们速度的最好方法是内部循环流水线结构.在基本结构中,Serpent 的一轮加密由 8 个不同的循环顺序构成,把这 8 个循环作为 8 个流水线站就可以构成一条内部循环流水线,因此 Serpent 是 5 种算法中最适合用内部循环流水线结构实现的.

Twofish 与 RC6 占用的空间远小于其他 3 种算法,硬件测试的综合结果与软件相近.同等条件下,Twofish 在 Pentium Pro/II 处理机上用汇编语言实现最少需 285 个时钟周期,RC6 在主频 200M 的处理机上用汇编语言实现最少需 254 个时钟周期,即 100.8Mbit/s.同时,Twofish 算法由于自身的结构,十分适合用内部循环流水线结构实现,从而可以得到很高的速度/空间比.在速度为第一考量的条件下,外部循环流水线结构(非反馈模式)或者循环展开结构(反馈模式)可以充分提高 Twofish 与 RC6 的速度,在非反馈模式时采用外部循环流水线结构,最大的吞吐量可以超过 1Gbit/s.

Mars 综合使用了多种加密手段,层次结构很多,大量使用循环移位和乘法,所以它执行一轮加密的时钟周期

最大.同时,它又是一种安全余量较高的算法,这意味着它主循环的循环轮数很高,两者综合,采用基本结构实现时它的速度最慢.

6 总结

随着计算机网络的发展和电子商务的日趋频繁,对加密技术提出了更高的要求.从整体发展趋势来看,密码装置应该作为外接在主机串口或并口的一个硬件设备或是一块插卡,具有速度快,低时延的特点.基于 FPGA 实现的加密技术与以往的主流硬件实现方式(如 DSP 芯片、单片机等)相比,具有低成本、高速度、微功耗、微小封装尺寸以及保密性强等优点.美国国家标准与技术协会(NIST)在对高级加密标准 AES 的侯选算法进行评判时就将能否在智能卡上实现作为一个很重要的标准.[6]另一个明显的优点在于:在对时间代价和空间代价的取舍上,基于 FPGA 实现的加密技术提供了多种实现方案,分别对时间代价和空间代价有不同的偏重,有利于在各种应用环境中进行优化.

此外,采用 FPGA 器件实现加密算法还为算法的评测提供了一条新的途径.算法采用软件实现时的效率受编译平台和操作平台的影响很大,而且不同平台上的效率往往不成线性关系,差距很大,而采用 FPGA 器件实现的加密算法效率虽然也受开发工具和 FPGA 器件电气性能的影响,但影响不大.在对 AES 侯选算法的密码分析和软件评估没有决定性结果的情况下,也许会为新的标准的最终决定提供一个重要的指标.

参考文献:

[1] [美]Kevin Skahill. 可编程逻辑系统的 VHDL 设计技术[M].朱明程,孙普译,南京: 东南大学出版社, 1998.

[2] [美]Bruce Schneier.应用密码学[M]. 吴世忠等译 . 北京:机械工业出版社, 2000.

[3] Kris Gaj, Pawel Chodowiec. Comparison of the hardware performance of the AES candidates using reconfigurable hardware[EB/OL]. http://www.counterpane.com,2000,12.

[4] Kris Gaj, Pawel Chodowiec. Implementation of the Twofish cipher of using FPGA Device[EB/OL]. http://www.counterpane.com, 2000,12.

[5] 崔劲松,张焕国. 高级加密标准 AES 侯选算法的比较[J]. 通讯保密, 2000, (1): 50 - 56.

[6] 崔劲松,张焕国. 高级加密标准 AES 评判规则[J].通讯保密, 2000, (3): 30 - 34.

A New Encryption Techniques Based on Field Programmable Gate Arrays (FPGA)

LI Chi - song, XIAO Dao - ju, YU Xiang - xuan

(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan Hubei 430074, China)

Abstract: Performance of four alternative hardware architectures of the symmetric block cipher using an alternative hardware technology based on Field Programmable Gate Arrays (FPGA) is discussed and compared. The results of hardware implementation of all AES finalists using Field Programmable Gate Arrays (FPGA) are analyzed and compared with the results of software implementation.

Key words: FPGA; VHDL; AES; Block Cipher; Cryptography