SMBA 分组算法

自测报告

兴唐通信科技有限公司

2019 年 10 月

目　　次

1、 软件实现

1.1 32 位 ARM 环境下的算法速率优化 C 实现

1.1.1 平台描述

32比特ARM环境采用基于STM32 F103的开发板(主频72Mhz)：stm32f1zet6核心板6、512K片内Flash、64K片内RAM。

1.1.2 实现方法

在32位平台上，把线性变换L_{32}和S盒代替变换结合，构造4个8到32比特的大表进行快速实现，记$Y=L_{32}\circ S(X)$，$X=(x_0,x_1,x_2,x_3)$ ，则

$$Y=\begin{bmatrix}1&0&1&1\\0&1&1&1\\1&1&1&0\\1&1&0&1\end{bmatrix}\times\begin{pmatrix}S_0(x_0)\\S_1(x_1)\\S_0(x_2)\\S_1(x_3)\end{pmatrix}=\begin{bmatrix}S_0(x_0)\\0\\S_0(x_0)\\S_0(x_0)\end{bmatrix}\oplus\begin{bmatrix}0\\S_1(x_1)\\S_1(x_1)\\S_1(x_1)\end{bmatrix}\oplus\begin{bmatrix}S_0(x_2)\\S_0(x_2)\\S_0(x_2)\\0\end{bmatrix}\oplus\begin{bmatrix}S_1(x_3)\\S_1(x_3)\\0\\S_1(x_3)\end{bmatrix}$$

可按如下方式构造4个8到32比特的大表L_0、L_1、L_2、L_3进行快速实现：

$$L_0[x]=S_0(x)||0||S_0(x)||S_0(x)$$

$$L_1[x]=0||S_1(x)||S_1(x)||S_1(x)$$

$$L_2[x]=S_0(x)||S_0(x)||S_0(x)||0$$

$$L_3[x]=S_1(x)||S_1(x)||0||S_1(x)$$

则，$Y=L_{32}\circ S(X)=L_0[x_0]\oplus L_1[x_1]\oplus L_2[x_2]\oplus L_3[x_3]$。

其余变换按定义实现。

1.1.3 性能自测试结果

采用CBC模式，用256字节数据作为输入进行性能测试，每次测试变换密钥，取10^5次CBC模式运算测试结果的平均值作为速率测试的结果。具体结果见表1.1.3-1。

表1.1.3-1 32位ARM平台软件测试性能

算法软件实现类别		加密速率	解密速率
32比特ARM环境下的	SMBA-128-128	6.84Mbps	6.71Mbps
	SMBA-128-256	3.48Mbps	3.48Mbps

算法速率优化C实现	SMBA-256-256	3.91Mbps	3.90Mbps

1.2 64 位 Windows 环境下的算法速率优化 C 实现

1.2.1 平台描述

SMBA的64位软件实现平台采用Intel Core(TM) i7-9750H CPU、主频2.6GHz、Windows10、内存32G、Microsoft Visual Studio 2017编译器。

1.2.2 实现方法

在64位平台上，把线性变换L_{64}和S盒代替变换结合，构造8个8到64比特的大表进行快速实现，记$Y=L_{64}\circ S(X)$，$X=(x_0,x_1,x_2,x_3,x_4,x_5,x_6,x_7)$ ，则

$$\begin{aligned}Y=L_{64}\circ S(X)&=L_{64}(s_0(x_0),s_1(x_1),s_0(x_2),s_1(x_3),s_0(x_4),s_1(x_5),s_0(x_6),s_1(x_7))\\&=L_{64}(s_0(x_0),0,\ldots,0)\\&\oplus L_{64}(0,s_1(x_1),\ldots,0)\\&\cdots\\&\oplus L_{64}(0,\ldots,0,s_1(x_7))\end{aligned}$$

可按如下方式构造8个8到64比特的大表L_0、L_1、L_2、L_3、L_4、L_5、L_6、L_7：

$$L_0[x]= L_{64}(s_0(x),0,0,0,0,0,0,0)$$

$$L_1[x]= L_{64}(0,s_1(x),0,0,0,0,0,0)$$

$$L_2[x]= L_{64}(0,0,s_0(x),0,0,0,0,0)$$

$$L_3[x]= L_{64}(0,0,0,s_1(x),0,0,0,0)$$

$$L_4[x]= L_{64}(0,0,0,0,s_0(x),0,0,0)$$

$$L_5[x]= L_{64}(0,0,0,0,0,s_1(x),0,0)$$

$$L_6[x]= L_{64}(0,0,0,0,0,\ 0,s_0(x),0)$$

$$L_7[x]= L_{64}(0,0,0,0,0,0,0,s_1(x))$$

则，$Y=L_{64}\circ S(X)=L_0[x_0]\oplus L_1[x_1]\oplus L_2[x_2]\oplus L_3[x_3]\oplus L_4[x_4]\oplus L_5[x_5]\oplus L_6[x_6]\oplus L_7[x_7]$。

其余变换按定义实现。

1.2.3 性能测试结果

采用CBC模式，用256字节数据作为输入进行性能测试，每次测试变换密钥，取10^5次CBC模式运算测试结果的平均值作为速率测试的结果。具体结果见表1.2.4-1。

表1.2.4-1 64比特Windows平台软件测试性能

算法软件实现类别		加密速率	解密速率
64比特Windows环境下的算法速率优化C实现	SMBA-128-128	1405Mbps	1438Mbps
	SMBA-128-256	1110Mbps	1134Mbps
	SMBA-256-256	1655Mbps	1611Mbps

2、 硬件实现

2.1 Verilog 硬件仿真实现

算法的 ASIC 实现环境，采用的设计库为 HJTC0.11um 工艺库，采用的综合工具为 Synopsys Design Vision(F-2011.09-SP1 Version)。仿真环境为 Modelsim SE 10.1a。测试结果如下：

表 1.3-1 Verilog 硬件仿真测试性能

	自测试结果		
	SMBA-128-128	SMBA-128-256	SMBA-256-256
运算周期	627	825	825
时钟约束	11ns	11ns	11ns
加密速率	566.37Mbps	430.44Mbps	860.88Mbps
解密速率	566.37Mbps	430.44Mbps	860.88Mbps
面积	69065um^2	87851um^2	164683um^2
加密吞面比	0.00820	0.00490	0.00523
解密吞面比	0.00820	0.00490	0.00523

2.2 FPGA 评估结果

算法的 FPGA 实现环境，采用 Xilinx 的 4vfx100ff1152-12，采用的综合工具为 ISE14.7。仿真环境为 Modelsim SE 10.2c。

（1）SMBA-128-128 算法的评估结果

表 2.2-1 SMBA-128-128 算法 FPGA 实现的资源占用情况

Number of Slices	1517
Number of Slice Flip Flops	1488
Number of 4 input LUTs	2813

表 2.2-2 SMBA-128-128 算法 FPGA 实现的性能情况

性能指标	性能值
最大时钟频率	153.312MHz
最小时钟周期	6.523ns
加密/解密时钟数	18
密钥扩展时钟数	19
吞吐量	1.09Gbps
加密/解密延时	117.414ns

（2）SMBA-128-256 算法的评估结果

表 2.2-3 SMBA-128-256 算法 FPGA 实现的资源占用情况

Number of Slices	1809
Number of Slice Flip Flops	2000
Number of 4 input LUTs	3321

表 2.2-4 SMBA-128-256 算法 FPGA 实现的性能情况

性能指标	性能值
最大时钟频率	153.312MHZ
最小时钟周期	6.523ns
加密/解密时钟数	24
密钥扩展时钟数	25
吞吐量	0.82Gbps
加密/解密延时	156.552ns

（3）SMBA-256-256 算法的评估结果

表 2.2-5 SMBA-256-256 算法 FPGA 实现的资源占用情况

Number of Slices	3296
Number of Slice Flip Flops	3728
Number of 4 input LUTs	6041

表 2.2-6 SMBA-256-256 算法 FPGA 实现的性能情况

性能指标	性能值
最大时钟频率	143.542MHz
最小时钟周期	6.967ns
加密/解密时钟数	24

密钥扩展时钟数	25
吞吐量	1.53Gbps
加密/解密延时	167.208ns