《电子技术应用》 www.ChinaAET.com

一种改进的 Montgomery 阶梯算法及其实现

袁仕继，李博章，孙慧慧，张广吉
（中国人民解放军 63888 部队，河南 济源 454650）

摘 要：提出了利用 Montgomery 阶梯算法实现快速模幂运的两种方案。第一种是将每个时钟周期内乘法和平方并行执行，且使用 2×2 正交变换器选择输出，使 Montgomery 阶梯算法简单、高效；第二种是使用循环展开技术将循环数减少一半，且只需要一半的时钟，运算效率得到更大的提高。

关键词：模幂运算；标量乘；Montgomery 阶梯算法

中图分类号：TP39 **文献标识码**：A **文章编号**：1674-7720(2013)11-0078-03

A proposed Montgomery ladder algorithm and architectures

Yuan Shiji, Li Bozhang, Sun Huihui, Zhang Guangji
(Unit 63888 of PLA, Jiyuan 454650, China)

Abstract: In this paper, two efficient architectures for modular exponentiation respectively using Montgomery ladder algorithm are proposed. The first one is a straightforward and efficient implementation of the Montgomery ladder algorithm, in which the multiplication and squaring are performed in parallel during each clock cycle. A novel designed two-by-two cross-point switch is used to select each ladder step. By parallelizing the Montgomery ladder using loop unrolling technique so that the number of loops is reduced by half, a second efficient architecture is proposed that requires only half number of clock cycles compared to the first one.

Key words: modular exponentiation; scalar multiplication; Montgomery ladder algorithm

大数模幂运算在 Diffie-Hellman 和 RSA 系统中得到了广泛应用[1]。所谓模幂运算，就是已知大数 a、x、m，求解 $a^x \pmod m$。这里的 a、x、m 一般为几百比特甚至上千比特的大整数，m 一般为素数，因此在此过程中需要做大量的乘法运算和模运算（即除法运算）。在计算机运行处理过程中，乘法运算是很耗时的运算，而除法运算更是乘法的几倍之多。因此，在计算 $a^x \pmod m$ 的过程中，如何减少乘法，尤其是模运算的次数便成为提高模幂运算速度的关键。参考文献[2]对常用算法进行了分析和总结。

经典 Montgomery[3]阶梯算法是将模运算转化为乘法运算和移位运算，从而避免计算模运算，在 RSA[4]和 ECC[5]中得到广泛应用。在该算法中执行运算的次数等于幂的二元进制长度，且平方运算是每步都要执行，仅当幂为 1 时才执行乘法运算[6]。这种在不同步中运算数量的差异导致系统易受边道攻击[7]。在 Diffie-Hellman 和 RSA 系统中的模幂运算中，幂为其密钥。一个成功的 SCA 攻击可以计算模幂运算的幂，从而导致整个系统密钥的丢失。本文利用循环展开技术，将两个循环同时进行并行处理，提高了运算速度和效率。同时，根据 Montgomery 阶梯算法原理，设计了该算法的硬件实现。

1 Montgomery 阶梯算法

1.1 经典 Montgomery 阶梯算法

算法 1 描述的过程即为经典 Montgomery 阶梯算法流程。

算法 1：

Input: M, $k=(k_{n-1}\cdots k_1\ k_0)_2$

Output: $C=M^k$

(1) Set $R_0 \leftarrow 1$, $R_1 \leftarrow M$;

(2) For $i=n-1$ to 0 Step-1

① If ($k_i=0$)

Then{Set $R_1 \leftarrow R_0 \times R_1$, $R_0 \leftarrow R_0^2$}

② If ($k_i=1$)

Then{Set $R_0 \leftarrow R_0 \times R_1$, $R_1 \leftarrow R_1^2$}

(3) Return ($C=R_0$)

由该算法可知，将一次平方运算认为是一次乘法运

《电子技术应用》 www.ChinaAET.com

算，可以完成一次求幂运算，经典 MPL 算法至少将运用 $2\log k$ 次乘法运算，而平方乘的平均运算量达到 $3/2\log k$。参考文献[8]指出 MPL 算法支持并行运算，用一个双核处理器，在同一时钟内将乘法运算和平方运算同时进行，运算速度将提高一倍。基于以上考虑，本文将设计实现一种经典 Montgomery 阶梯算法。

1.2 MPL 算法的快速实现

算法 1 的快速实现如图 1 所示，变量 R_0 和 R_1 分别初始化为 1 和 M，分别存储在存储器 R_0 和 R_1 中。设 R_0 和 R_1 可存储大数 M^k。指数 k 存储在二进制移位寄存器中，该寄存器每次循环左移一位。算法硬件实现还包括一个模乘法器、模平方单元、一个混合器和一个 2×2 正交变换器。

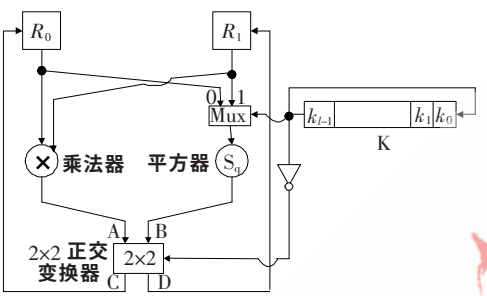

图 1 MPL 快速实现(算法 1)

假设模数 M 有 m 比特，存储器 R_0 和 R_1 可存储至少 m 比特。模乘法器和模平方单元输入、输出都为 m 比特。移位寄存器的输出值 k_i 决定混合器的输出，输出值为混合器输入两个 m 比特值中的一个。

图 2 是图 1 中 2×2 正交变换器的实现示意图。它利用两个混合器实现如下变换：

If E=0, then C=A, D=B

If E=1, then D=A, C=B

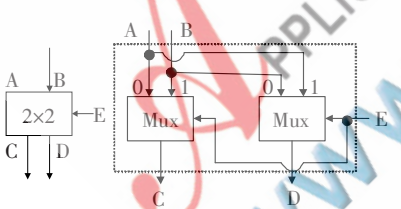

图 2 2×2 正交变换器

设计工作原理如下：首先，将 R_0 和 R_1 分别初始化为 1 和 M。在第 j (j=0, 1, 2, …, n−1) 轮循环，指数中比特 k_{n-1-j} 是移位寄存器最左边的比特，由它控制混合器运算和 2×2 正交变换。如果 k_{n-1-j}=0，则由 R_0 输出 R_0，并作乘法运算和平方运算，其中，平方运算生成 R_0；如果 k_{n-1-j}=1，则由 R_1 输出 R_1，并作乘法运算和平方运算，其中，平方运算生成 R_1。

2×2 正交变换器工作原理：在第 j (j=0, 1, 2, … n−1) 轮循环，如果 k_{n-1-j}=0，即控制端输入 E=1，变换表现为交叉关系，这时乘法器和平方单元的输出分别输入 R_0 和 R_1 中；如果 k_{n-1-j}=1，即控制端的输入为 E=0，变换表现为平行关系，这时乘法器和平方单元的输出分别为 R_0 和 R_1 中。

在第 j (j=0, 1, 2 … , n−1) 轮循环中，运行算法 1 中 i=j 的步骤。进行 n 轮循环后，存储器 R_0 中的值即为 $C=M^k$。

设计包含了一个模乘法运算，一个模平方运算，3 个混合运算和 2 个存储器过程。算法时间复杂度为：

$$T=\max\{\text{Tmultiplier}, \text{Tsquarer}+\text{Tmux}\}+T_{2\times2}$$
$$=\max\{\text{Tmultiplier}+\text{Tmux}, \text{Tsquarer}+2\text{Tmux}\}$$

从图 2 中可以看出，2×2 正交变换等价于一个混合器。由于是对大数的运算，可以认为 Tmultiplier >> Tsquarer，则一次循环耗时 T=Tmultiplier+Tmux。整个模幂运算耗时 $nT=n$(Tmultiplier+Tmux)。

2 一种改进的 MPL 算法及实现

2.1 一种改进的 MPL 算法

经典 MPL 算法是从 k_2 的最高位循环到最低位，而且是单位循环。为了提高运算速度，需对经典 MPL 算法进行改进。将循环展开技术应用于 MPL 算法，并将两个循环合并，得到如下改进算法：

算法 2：

Input: M, k=$(k_{n-1}\cdots k_1\ k_0)_2$

Output: C=M^k

(1)Set m←(n−2)/2 if n is even

otherwise set m←(n−1)/2 and kn←0

(2)Set R_0←1, R_1←M;

(3)For i=m to 0 step−1

①If($k2i+1k2i$=00)

Then{Set R_1←R_0×R_1, R_0←R_0^2,

R_1←R_0×R_1, R_0←R_0^2 }

②If($k2i+1k2i$=01)

Then{Set R_1←R_0×R_1, R_0←R_0^2,

R_0←R_0×R_1, R_1←R_1^2 }

③If($k2i+1k2i$=10)

Then{Set R_0←R_0×R_1, R_1←R_1^2,

R_1←R_0×R_1, R_0←R_0^2 }

④If($k2i+1k2i$=11)

Then{Set R_0←R_0×R_1, R_1←R_1^2,

R_0←R_0×R_1, R_1←R_1^2 }

(4)Return(C=R_0)

以上算法与 M−ary 算法中为 m=4 的情况类似。

2.2 改进 MPL 算法的实现

实现算法 2 的设计如图 3 所示。变量 R_0 和 R_1 分别初始化为 1 和 M，存储在存储器 R_0 和 R_l 中。设 R_0 和 $R1$ 可存储大数 N−1 (N 为模数)。

如图 4 所示，二进制指数 k 存储在移位寄存器中。n 为偶数时，寄存器 K 有 n 比特，$k_{2m+1}=k_{n-1}$，即 $m=n/2-1$；n 为奇数时，寄存器 K 有 n+1 比特，$k_{2m}=k_{n-1}$，即 $m=(n-1)/2$。

《电子技术应用》 www.ChinaAET.com

《电子技术应用》 www.ChinaAET.com

寄存器 K 每循环一次，有两个比特输出。一个比特用来控制图 3 上方的混合器和 2×2 的正交变换；另一个比特用来控制图 3 下方的混合器和 2×2 正交变换。除寄存器外，改进 MPL 设计还包括两个乘法器，两个平方单元，两个混合器和两个 2×2 正交变换。

这种设计可以分成上下两部分。两部分结构都与图 1 结构类似。不同之处在于，上方部分 2×2 正交变换的输出分别为下方部分乘法器和平方单元的输入。

分析该算法的实现，算法时间复杂度为：

$T=\max\{2TMultiplier+2T_{2\times2}, Tmultiplier+Tsquarer+2T_{2\times2}+Tmux, 2Tsquarer+2T_{2\times2}+2Tmux\}$

完成模幂运算需要 $m+1=(n+1)/2$ 个循环，则整个运算耗时 $(M+1)T$。

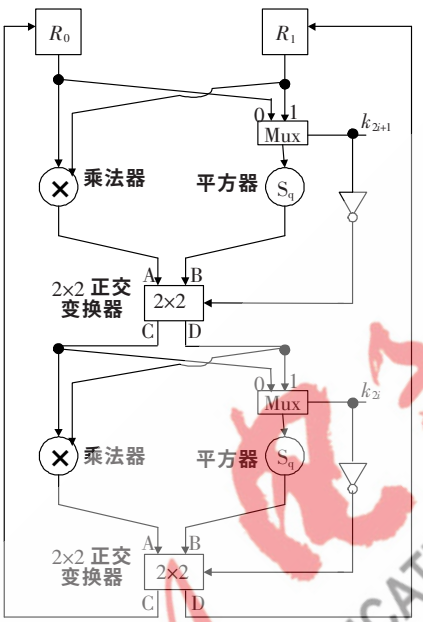

图 3 改进 MPL 快速实现(算法 2)

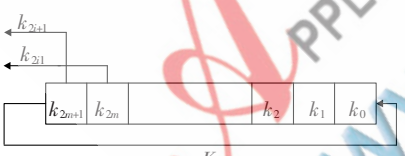

图 4 移位寄存器

大数模幂运算是公约密码体质研究的热点内容之一。本文结合经典 Montgomery 阶梯算法能并行处理的特点，首先设计实现出经典 Montgomery 阶梯算法；然后结合循环展开技术，提出了一种改进 Montgomery 阶梯算法，设计并实现了该算法。分析表明，该方法能将经典 Montgomery 阶梯算法的循环次数降低一半，使得该算法能在 ECC 和其他领域得到广泛应用。

参考文献

[1] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE tans. Inform. Theory, 1976(22):644-654.

[2] 朱兆国，任忠保，桂祚勤.大数模幂运算的快速算法[J].高性能计算技术，2006(2):45-48.

[3] MONTGOMERY P L. Modular multiplication without trial division[J]. Mathmatics of Computation, 1985,44(170):519-521.

[4] 王平水.公钥密码体制及其安全性分析研究[D].合肥：合肥工业大学，2006.

[5] 左平，庞世春，华宏图，等.安全的并行椭圆曲线 Montgomery 阶梯算法[J].吉林大学学报(物理版)，2011，49(4):690-692.

[6] GORDON D M. A survey of fast exponentiation methods[J]. Algorithms, 1998,27(1):129-146.

[7] MESSERGES T S, DABBISH E A, SLOAN R H. Power analysis attacks of modular exponentiation in Smartcards[C]. CHES'99, 1999: 144-157.

[8] WELSCHENBACH M. 密码编码学-加密方法的 C 与 C++实现[M].赵振江，等译.北京：电子工业出版社，2003.

(收稿日期：2013-03-09)

作者简介：

袁仕继，男，1981 年生，硕士，工程师，主要研究方向：网络安全体系构建。

李博章，男，1979 年生，硕士，工程师，主要研究方向：身份认证技术研究。

孙慧慧，女，1983 年生，硕士，工程师，主要研究方向：身份认证技术。

《电子技术应用》 www.ChinaAET.com