[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 7/72

[12] 发明专利申请公开说明书

[21] 申请号 200410032681.6

[43] 公开日 2004 年 9 月 22 日

[11] 公开号 CN 1530824A

[22] 申请日 2004.3.14
[21] 申请号 200410032681.6
[30] 优先权
[32] 2003. 3.14 [33] KR [31] 16100/2003
[71] 申请人 三星电子株式会社
地址 韩国京畿道
[72] 发明人 李炅熙 任范镇 许美淑

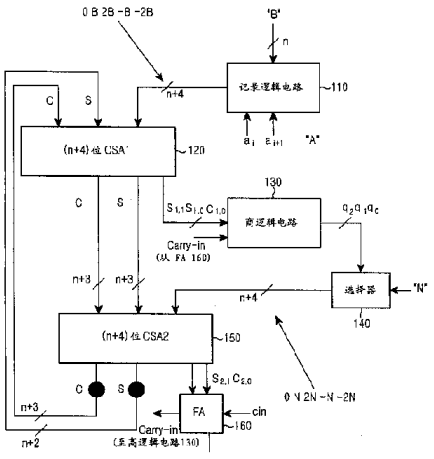
[74] 专利代理机构 北京市柳沈律师事务所
代理人 吕晓章 马 莹

权利要求书 7 页 说明书 26 页 附图 10 页

[54] 发明名称 用于执行蒙哥马利型模乘法的装置及方法

[57] 摘要

本发明公开了一种模块式乘法装置，在包括智能卡和移动终端的移动通信环境中，用于实现高速的加密/解密及电子签名。 本发明提供一种用于执行蒙哥马利型模块式乘法的装置，在 $m+2(m=n/2)$ 个时钟内利用乘数 A 和被乘数 B 计算 $A \cdot B' \cdot R^{-1} \bmod N(R=4^{m+2})$，A 和 B 具有 n 位的输入，其中顺序地移动该乘数位以生成一个移位串，且 Booth 记录该生成的移位串的两位最低有效位。 本发明提供一种具有较少逻辑门数目以及降低功耗的高速模块式乘法装置。



ISSN1008-4274

知识产权出版社出版

1、一种用于实现消息加密/解密技术的模乘装置，其中，使用第一密钥（B）和第二密钥（N）加密/解密消息（A），该模乘装置包括:

存储装置，用于存储长度都是n位的该消息、第一密钥和第二密钥;

记录逻辑电路，用于在每个时钟处使用该消息和该第一密钥生成第一n+4位信号;

第一进位存储加法器，用于使用该第一n+4位信号和两个并行的n+4位输入信号生成由一个进位值和两个和值组成的3位序列;

商逻辑电路，使用该3位序列和一个进位值生成用于确定模数简化倍数的3位限定词;

选择器，使用第二密钥和该3位限定词生成第二n+4位信号;

第二进位存储加法器，使用该第二n+4位信号和第一进位存储加法器输出的各自的和值和进位项生成一对和值和一对进位值；以及

第一全加器，用于通过对这对和值和进位值以及在先前时钟处从商逻辑电路输出的进位值（cin）执行全加操作生成进位输入值。

2、如权利要求1所述的装置，其中，该存储装置包括用于存储各自的消息、第一密钥和第二密钥的移位寄存器。

3、如权利要求1所述的装置，其中，在每个时钟处将消息右移2位。

4、如权利要求1所述的装置，其中，该第一n+4位信号是0、B、2B、-B和-2B其中之一。

5、如权利要求1所述的装置，其中，该第二n+4位信号是0、N、2N、-N和-2N其中之一。

6、如权利要求1所述的装置，其中，该记录逻辑电路包括:

Booth记录电路，用于对该消息的两位最低有效位执行Booth记录;

多路复用器，用于对该两位最低有效位和该第一密钥执行多路复用以输出0、B和2B其中之一；以及

一的补码器，依照该两位最低有效位对该多路复用器输出的该n+1位信号执行一的取补运算，以生成0、B、2B、-B和-2B其中之一。

7、如权利要求1所述的装置，其中，该第一进位存储加法器包括n+4个第二全加器，每一个全加器对该两个并行的n+4位输入信号的相应的和

值和进位以及该第一 n + 4 位输入信号的相应位执行全加操作，以生成该 3 位序列。

8、如权利要求 7 所述的装置，其中，该两个并行的 n + 4 位输入信号中的第一输入信号是按以下方式生成的：从该第二进位存储加法器的和值项中选择最高有效 n + 2 位并插入两位作为所选 n + 2 位的最高有效位。

9、如权利要求 8 所述的装置，其中，这两个最高有效位为零。

10、如权利要求 8 所述的装置，其中，该两个并行的 n + 4 位输入信号中的第二输入信号是按以下方式生成的：从该第二进位存储加法器的进位项中选择最高有效 n + 3 位并插入一位作为所选 n + 3 位的最高有效位。

11、如权利要求 10 所述的装置，其中，该最高有效位为零。

12、如权利要求 1 所述的装置，其中，该商逻辑电路包括：

D 触发器，用于临时存储来自第一全加器的进位输入值；

第三全加器，用于对该进位输入值、该第一进位存储加法器的最低有效位全加器输出的和值以及第一 n+4 位信号的符号位执行全加运算；

一个异或（XOR）逻辑门，用于对该第一进位存储加法器的最低有效位全加器输出的进位值和该第一进位存储加法器的次最低有效位全加器输出的和值以及第三全加器的进位值执行异或运算；以及

一个组合电路，用于对第三全加器和异或逻辑门的输出及第二密钥的次最低有效位进行组合，并输出该 3 位限定词信号。

13、如权利要求 1 所述的装置，其中，该第二进位存储加法器包括 n + 4 个第四全加器，每一个全加器对来自该第一进位存储加法器的除了和值的最低有效位及进位的最高有效位之外的相应的和值和进位以及该第二 n + 4 位信号的相应位执行全加操作，生成该对和值和进位值。

14、如权利要求 1 所述的装置，其中，该第一全加器对第二进位存储加法器的次低有效位全加器输出的和值和该第二进位存储加法器的最低有效位全加器输出的进位值以及在先前时钟处从商逻辑电路输出的进位值（cin）执行全加操作，并生成该进位输入值。

15、如权利要求 1 所述的装置，还包括一个进位传送加法器，在 m + 2 个时钟之后对该第二进位存储加法器输出的和值和进位项执行进位传送加法操作，其中 m = n/2。

16、如权利要求 15 所述的装置，其中，如果该进位传送加法器的值是负

的，则该进位传送加法器将第二密钥的模加到该进位传送加法运算的结果中。

17、一种用于实现消息加密/解密技术的模乘装置，其使用第一密钥（B）和第二密钥（N）对消息（A）加密/解密，该模乘装置包括：

存储装置，用于存储长度为 n 位的该消息、第一密钥和第二密钥；

记录逻辑电路，用于使用该消息和第一密钥在每个时钟处生成第一 n + 3 位信号；

第一进位存储加法器，通过对该第一 n + 3 位信号和两个并行的 n + 3 位输入信号执行第一进位存储加法操作，生成由一个进位值和两个和值组成的 3 位序列；

商逻辑电路，通过对该 3 位序列和一个进位值执行商操作，生成一个用于确定模数简化倍数的 2 位限定词；

选择器，使用该第二密钥和该 2 位限定词生成第二 n + 3 位信号；

第二进位存储加法器，通过对该第二 n + 3 位信号和第一进位加法操作输出的分别的和值项和进位项执行第二进位存储加法操作，输出一对和值和一对进位值；

与（AND）逻辑门，通过对该对和值和进位值执行与操作，输出一个进位输入值。

18、如权利要求 17 所述的装置，其中，该存储装置包括用于存储各自的消息、第一密钥和第二密钥的移位寄存器。

19、如权利要求 18 所述的装置，其中，在每个时钟将该消息移动 2 位。

20、如权利要求 17 所述的装置，其中该第一 n + 3 位信号是 0、B、2B 和 3B 其中之一。

21、如权利要求 17 所述的装置，其中，该第二 n + 3 位信号是 0、N、2N 和 3N 其中之一。

22、如权利要求 17 所述的装置，其中，该记录逻辑电路是一个多路复用器，用于对消息的两位最低有效位和 n 位的第一密钥执行多路复用，输出该第一 n + 3 位信号。

23、如权利要求 12 所述的装置，其中，该第一进位存储加法器包括 n + 3 个第一全加器，每一个全加器对两个并行的 n + 3 位输入信号的相应的和值和进位以及该第一 n + 3 位输入信号的相应位执行全加操作，输出该 3 位序列。

24、如权利要求 23 所述的装置，其中，该两个并行的 n + 3 位输入信号

中的第一输入信号是按以下方式生成的：从该第二进位存储加法器的和值项中选择最高有效位的 n + 1 位并插入两位作为所选的 n + 1 位的最高有效位。

25、如权利要求 24 所述的装置，其中，这两个最高有效位为零。

26、如权利要求 24 所述的装置，其中，该两个并行的 n + 3 位输入信号中的第二输入信号是按以下方式生成的：从该第二进位存储加法器的进位项中选择最高有效位的 n + 2 位并插入一位作为所选的 n + 2 位的最高有效位。

27、如权利要求 26 所述的装置，其中，该最高有效位为零。

28、如权利要求 17 所述的装置，其中，该商逻辑电路包括：

D 触发器，用于临时存储来自与（AND）逻辑门的该进位输入值；

半加器，用于对该进位输入值和该第一进位存储加法器的最高有效位全加器输出的和值执行半加运算；

异或（XOR）逻辑门，用于对该第一进位存储加法器的最低有效位全加器输出的进位值和次低有效位全加器输出的和值以及该半加器的输出值执行异或运算；

组合电路，用于对该半加器和异或逻辑门的输出及第二密钥的次最低有效位（n1）进行组合，并输出该 2 位限定词信号。

29、如权利要求 17 所述的装置，其中，该第二进位存储加法器包括：

n + 3 个第二全加器，每一个全加器对来自该第一进位存储加法器的除了和值的最低有效位及进位的最高有效位之外的相应的和值和进位以及该第二 n + 3 位信号的相应位执行全加操作，生成该对和值和进位。

30、如权利要求 17 所述的装置，其中，该与（AND）逻辑门对该第二进位存储加法器的次低有效位第二全加器输出的和值及该第二进位存储加法器的最低有效位第二全加器输出的进位值执行与（AND）操作，生成该进位输入值。

31、如权利要求 17 所述的装置，还包括一个进位传送加法器，在 m + 2 个时钟之后对该第二进位存储加法器输出的和值项和进位项执行进位传送加法操作，其中 m = n/2。

32、一种用于实现消息加密/解密技术的模乘方法，其中，使用第一密钥（B）和第二密钥（N）对消息（A）加密/解密，该模乘方法包括：

存储 n 位的消息、第一密钥和第二密钥；

在每个时钟使用该消息和第一密钥生成第一 n + 4 位信号；

通过对该第一 n + 4 位信号和两个并行的 n + 4 位输入信号执行第一进位存储加法操作，生成由一个进位值和两个和值组成的 3 位序列；

通过对该 3 位序列和一位输入进位值执行商操作，生成一个用于确定模数简化倍数的 3 位限定词；

使用该第二密钥和该 3 位限定词，生成第二 n + 4 位信号；

通过对该第二 n + 4 位信号和第一进位加法操作输出的分别的和值和进位项执行第二进位存储加法操作，输出一对和值和一对进位值；

通过对这对和值和进位值以及在先前时钟处从商逻辑电路输出的进位值执行全加操作输出一个进位输入值。

33、如权利要求 32 所述的方法，其中，在每个时钟处将该消息右移 2 位。

34、如权利要求 32 所述的方法，其中，生成该第一 n + 4 位信号的处理包括：

对该消息的两个最低有效位执行 Booth 记录；

根据这两个最低有效位生成 0、B、2B、 - B 和 - 2B 其中之一。

35、如权利要求 32 所述的方法，其中，该两个并行的 n + 4 位输入信号中的第一输入信号是按以下方式生成的：从该第二进位存储加法操作的和值项中选择最高有效 n + 2 位并插入两位作为所选的 n + 2 位的最高有效位。

36、如权利要求 32 所述的方法，其中，这两个最高有效位为零。

37、如权利要求 32 所述的方法，其中，该两个并行的 n + 4 位输入信号中的第二输入信号是按以下方式生成的：从该第二进位存储加法操作的进位项中选择最高有效 n + 3 位并插入一位作为所选的 n + 3 位的最高有效位。

38、如权利要求 32 所述的方法，其中，该最高有效位为零。

39、如权利要求 32 所述的方法，其中，该 3 位序列包括两个和值和一个进位值。

40、如权利要求 39 所述的方法，其中，该两个和值是第一进位存储加法操作输出的和值项中的最低有效位和次低有效位。

41、如权利要求 39 所述的方法，其中，该一位输入进位值是第一进位存储加法操作输出的进位值项中的最低有效位。

42、如权利要求 32 所述的方法，其中，该一个输入进位值是由全加操作生成的该进位输入值。

43、如权利要求 32 所述的方法，其中，根据 3 位限定词的两个最低有效位从 0、N、2N－N 和－2N 中选出该第二 n＋4 位信号。

44、如权利要求 32 所述的方法，其中，该对和值和进位值是第二进位存储加法操作输出的和值项中的次低有效位和进位值项中的最低有效位。

45、如权利要求 32 所述的方法，其中，第一进位存储加法操作输出的和值项和进位值项中的最高有效位被忽略。

46、如权利要求 32 所述的方法，还包括在 m＋2 个时钟之后对该和值项和进位项执行进位传送加法操作，其中 m＝n/2。

47、如权利要求 46 所述的方法，还包括如果该进位传送加法操作输出的值是负的，则加上模第二密钥。

48、一种用于实现消息加密/解密技术的模乘方法，其使用第一密钥（B）和第二密钥（N）对消息（A）加密/解密，该模乘方法包括:

存储长度都为 n 位的该消息、第一密钥和第二密钥;

在每个时钟使用该消息和第一密钥生成第一 n＋3 位信号;

通过对该第一 n＋3 位信号和两个并行的 n＋3 位输入信号执行第一进位存储加法操作，输出由一个进位值和两个和值组成的 3 位序列;

通过对该 3 位序列和一位输入进位值执行商操作，生成一个用于确定模数简化倍数的 2 位限定词;

使用该第二密钥和该 2 位限定词，生成第二 n＋3 位信号;

通过对该第二 n＋3 位信号和第一进位加法操作输出的各自的和值和进位项执行第二进位存储加法操作，输出一对和值和一对进位值;

通过对这对和值和进位值执行与（AND）操作输出一个进位输入值。

49、如权利要求 48 所述的方法，其中，在每个时钟处将该消息右移 2 位。

50、如权利要求 48 所述的方法，其中，通过多路复用该消息的两个最低有效位及第一密钥生成该第一 n＋3 位信号。

51、如权利要求 48 所述的方法，其中，该第一 n＋3 位信号是 0、B、2B 和 3B 其中之一。

52、如权利要求 48 所述的方法，其中，该两个并行的 n＋3 位输入信号中的第一输入信号是按以下方式生成的：从该第二进位存储加法操作的和值项中选择最高有效位的 n＋1 位并插入两位作为所选 n＋1 位的最高有效位。

53、如权利要求 52 所述的方法，其中，这两个最高有效位为零。

54、如权利要求 52 所述的方法，其中该两个并行的 n + 3 位输入信号中的第二输入信号是按以下方式生成的：从该第二进位存储加法操作的进位项中选择最高有效位的 n + 2 位并插入一位作为所选 n + 2 位的最高有效位。

55、如权利要求 54 所述的方法，其中，该最高有效位为零。

56、如权利要求 48 所述的方法，其中，该 3 位序列包括两个和值和一个进位值。

57、如权利要求 56 所述的方法，其中，该两个和值是第一进位存储加法操作输出的和值项中的最低有效位和次低有效位。

58、如权利要求 56 所述的方法，其中，该一个进位值是第一进位存储加法操作输出的进位值项中的最低有效位。

59、如权利要求 48 所述的方法，其中，该一个输入进位值是由与（AND）操作生成的该进位输入值。

60、如权利要求 48 所述的方法，其中，根据 2 位限定词从 0、N、2N 和 3N 中选出该第二 n + 3 位信号。

61、如权利要求 48 所述的方法，其中，该对和值和进位值是第二进位存储加法操作输出的和值项中的次低有效位和进位值项中的最低有效位。

62、如权利要求 48 所述的方法，其中，第一进位存储加法操作输出的和值项和进位值项中的最高有效位被忽略。

63、如权利要求 48 所述的方法，还包括在 m + 2 个时钟之后对该第二进位存储加法操作输出的和值项和进位项执行进位传送加法操作，其中，m = n/2。

用于执行蒙哥马利型模乘法的装置及方法

技术领域

本发明通常涉及加密领域，具体言之是涉及一种用在对消息加密/解密和数字签名技术中执行蒙哥马利型模乘法的装置及方法。

背景技术

在使用智能卡及电子货币的用于电子商务的通信系统中以及在使用诸如移动电话、小型计算机等移动通信装置的通信系统中，人们希望通过对消息加密/解密或进行数字签名处理来安全地传输消息（电子文本或数据）。此处术语“数字签名”是指在消息的电子交换处理中在电子正文上“签名”的技术，这类似于通常在纸上所做的签名。随着互联网用户数量以及互联网上个人消息传输频率的快速增加，极其需要在不安全的通道上能安全的传输消息。

已提出的各种算法例如，RSA（Rivest－Shamir－Adlcman）、ELGamal、Schnorr 等已经用在使用公开密钥系统的加密/解密技术中和数字签名技术中。基于 RSA 算法的 ISO（国际标准化组织）/IEC（国际电工委员会）9796 已经被采用为这些算法的国际标准，美国已经采用了 ELGamal 的一个改进版 DSA（数字签名标准），俄罗斯采用了 GOSSTANDART（通常简写为“GOST”），韩国采用了 KC－DSA。然而，目前使用的各种通信系统中已经采用了多种 PKCC（公开密钥加密标准）。上述的算法要求执行模幂运算 $m^e \bmod N$，其包括反复执行模乘法运算，$A \cdot B \bmod N$。

已经建议了诸如 RSA 的用于执行模乘法的很多算法，这些算法需要在公开密钥密码的基础上生成和验证数字签名，例如，R. L. Rivest 等人所著的于 1978 年发表在 Communication of the ACM, 21, pp. 120-126 上的“A Method For Obtaining Signatures And Public-Crytosystems”；P. L. Montgomery 所著的于 1985 年发表在 Math. of Comp., Vol. 44, No. 170, pp. 519-521 上的“Modular Multiplication With Trial Division”；S. R. Dusse 和 B. S. Kaliski Jr. 所著的于 199 年发表在 Proc. Eurocrypto' 90, pp. 230-244 上的“A Cryptographic Library For The Motorola DSP5600”以

及 Spronger-Verlag、A. Bosselaers、R. Govaerts 和 J. Vandewalle 所著的于 1993 年发表在 Advance in CrytologyCRYPTO' 93, pp. 175-186 上的 "Comparison Of Three Modular Reduction Function"。从 D. R. Stinson 所著的于 1995 年发表在 CRC Press 上的 "Cryptography" 论文中可知，在各种需要模幂的算法中，在用于模幂的模乘的计算效率上蒙哥马利算法最有效，但对于简单的模乘而言它不是有效的算法。美国专利 No. 6,185,596 中公开了一个实现蒙哥马利算法的装置的例子。

如上所述，已经提出了用于公开密钥加密/解密及电子签名的许多算法和结构。然而，由于依照大多数算法和结构的模乘装置多用于高速的公开密钥的加密/解密，所以它们存在需要大量的逻辑门及大量的功耗的缺点。

发明内容

因此，本发明已经考虑到上述问题，本发明的一个目的是提供一种具有较少逻辑门的模乘装置，用于在包括智能卡和移动终端的移动通信环境中，实现高速的加密/解密及电子签名。

本发明的另一个目的是提供一种降低了功耗的模乘装置，用于在包括智能卡和移动终端的移动通信环境中，实现高速的加密/解密及电子签名。

本发明的又一目的是提供一种模乘装置，其能在包括智能卡和移动终端的移动通信环境中，实现高速的加密/解密及电子签名。

为达到上述目的，用于实现其中使用第一密钥（B）和第二密钥（N）对消息（A）加密/解密的消息加密/解密技术的该模乘装置 消息（A），模块式乘包括：一个存储器，具有分开的区域用于存储该消息、第一密钥和第二密钥，每个区域的长度是 n 位；一个记录逻辑电路，在每个时钟处使用该消息和第一密钥生成第一 n + 4 位信号；一个第一进位存储加法器，使用该第一 n + 4 位信号和两个并行的 n + 4 位输入信号生成包括一个进位值和两个和值组成的 3 位序列；一个商逻辑电路，使用该 3 位序列和一个进位值生成一个用于确定模数简化倍数的 3 位限定词；一个选择器，用于使用第二密钥和该 3 位限定词生成一个第二 n + 4 位信号；一个第二进位存储加法器，使用该第二 n + 4 位信号和从第一进位存储加法器输出的各自的和值和进位项来输出和值和进位值；一个第一全加器，通过对该和值和进位值以及在先前时钟处从商逻辑电路输出的进位值执行全加操作输出一个进位输入值。该分开的区域是

移位寄存器，用于存储各自的消息、第一密钥和第二密钥。在每个时钟处该消息被右移 2 位。第一 n + 4 位信号是 0、B、2B、－B 和－2B 其中之一。第二 n + 4 位信号是 0、N、2N、－N 和－2N 其中之一。

该记录逻辑电路包括一个 Booth 记录电路，用于对消息的两个低阶位执行 Booth 记录；一个多路复用器，用于对该两位低位和该第一密钥执行多路复用复用以输出 0、B 和 2B 其中之一；以及一个一的补码器，用于依照两个低阶位对从该多路复用器输出的该 n + 1 位信号有选择的执行一的取补运算以生成 0、B、2B、－B 和－2B 其中之一。

该第一进位存储加法器包括 n + 4 个第二全加器，每一个全加器对两个并行的 n + 4 输入信号的相应的和值和进位以及该第一 n + 4 位输入信号的相应位执行全加操作以生成该 3 位序列。该两个并行的 n + 4 位输入信号中的第一输入信号是按以下方式生成的：从该第二进位存储加法器的和值项中选择高阶的 n + 2 位并插入两位作为所选的 n + 2 位的高阶位，且这两个高阶位为零。该两个并行的 n + 4 位输入信号中的第二输入信号是按以下方式生成的：从该第二进位存储加法器的进位项中选择较高的 n + 3 位并插入一位作为所选的 n + 3 位的较高阶高位，且这个较高阶位为零。

该商逻辑电路包括一个 D 触发器，用于临时存储来自第一全加器的进位输入值；一个第三全加器，用于对该进位输入值和该第一进位存储加法器的最低有效位全加器输出的和值执行全加运算，该运算考虑了该第一密钥的符号；一个异或（XOR）逻辑门，用于对从该第一进位存储加法器的最低有效位全加器输出的进位值和从该第一进位存储加法器的次低有效位全加器输出的和值以及在先前时钟处从商逻辑电路输出的值执行异或运算；还包括一个组合电路，用于将第三全加器和异或逻辑门的输出及第二密钥的次最低有效位（n1）进行组合以输出该 3 位限定词信号。

该第二进位存储加法器包括 n + 4 个第四全加器，每一个全加器对来自该第一进位存储加法器的除了和值的最低有效位及进位的最高有效位之外的相应的和值和进位以及该第二 n + 4 位信号的相应位执行全加操作，以生成和值及进位的一对值。该第一全加器该对从第二进位存储加法器的次低有效位全加器输出的和值及从该第二进位存储加法器的最低有效位全加器输出的进位值以及在先前时钟处商逻辑电路的进位值（cin）执行全加操作，以生成该进位输入值。

该模乘装置还包括一个进位传送加法器，用于在 m + 2 个时钟之后对该第二进位存储加法器输出的和值和进位项执行进位传送加法操作，其中 m = n/2。如果该进位传送加法器的输出是负值，则该进位传送加法器将模第二密钥加到该进位传送加法操作的结果中。

本发明的另一方面，在用于实现消息加密/解密技术的该模乘装置中，使用第一密钥（B）和第二密钥（N）对消息（A）加密/解密，该模乘装置包括：一个存储器，具有用于存储 n 位消息的独立区域、第一密钥和 n 位的第二密钥；一个记录逻辑电路，用于在每个时钟处使用该消息和第一密钥生成第一 n + 3 位信号；一个第一进位存储加法器，用于通过对该第一 n + 3 位信号和两个并行的 n + 3 位输入信号执行第一进位存储加法操作，输出由一个进位值和两个和值组成的 3 位序列；一个商逻辑电路，用于通过对该 3 位序列和一个进位值执行商操作，生成一个用于确定模数简化倍数的 2 位限定词；一个选择器，使用第二密钥和该 2 位限定词生成一个第二 n + 3 位信号；一个第二进位存储加法器，通过对该第二 n + 3 位信号和第一进位加法操作输出的分别的和值及进位项执行第二进位存储加法操作，输出一对和值和进位值；还包括一个与（AND）逻辑门，通过对该对和值及进位值执行与操作，输出一个进位输入值。该分开的区域是移位寄存器，用于存储各自的消息、第一密钥和第二密钥。在每个时钟下该消息移动 2 位。该第一 n + 3 位信号是 0、B、2B 和 3B 其中之一。该第二 n + 3 位信号是 0、N、2N 和 3N 其中之一。

该记录逻辑电路是一个多路复用器，用于对消息的两个较低位和第一密钥的 n 位执行多路复用以输出该第一 n + 3 位信号。该第一进位存储加法器包括 n + 3 个第一全加器，每一个全加器对两个并行的 n + 3 位输入信号的相应的和值及进位以及该第一 n + 3 位输入信号的相应位执行全加操作，以生成该 3 位序列。该两个并行的 n + 3 位输入信号中的第一输入信号是按以下方式生成的：从该第二进位存储加法器的和值项中选择高阶的 n + 1 位并插入两位作为所选的 n + 1 位的较高阶位，且这两个较高阶位为零。该两个并行的 n + 3 位输入信号中的第二输入信号是按以下方式生成的：从该第二进位存储加法器的进位项中选择较高阶的 n + 2 位并插入一位作为所选的 n + 2 位的较高阶位，且这一个较高阶位为零。

该商逻辑电路包括一个 D 触发器，用于临时存储来自与逻辑门的进位输入值；一个半加器，用于对该进位输入值和该第一进位存储加法器的最高有

效位全加器输出的和值执行半加运算；一个异或（XOR）逻辑门，用于对该第一进位存储加法器的最低有效位全加器输出的进位值和次低有效位全加器输出的和值以及该半加器的输出值执行异或运算；还包括一个组合电路，用于对该半加器和异或逻辑门的输出及第二密钥的次最低有效位（n1）进行组合以输出该 2 位限定词信号。

该第二进位存储加法器包括 n + 3 个第二全加器，每一个全加器对来自该第一进位存储加法器的除了和值的最低有效位及进位的最高有效位之外的相应的和值和进位以及该第二 n + 3 位信号的相应位执行全加操作，以生成该对和值和进位。该与（AND）逻辑门对该第二进位存储加法器的次低有效位第二全加器输出的和值及该第二进位存储加法器的最低有效位第二全加器输出的进位值执行与（AND）操作，以生成该进位输入值。该模乘装置还包括一个进位传送加法器，用于在 m + 2 个时钟之后对该第二进位存储加法器输出的和值和进位项执行进位传送加法操作。

本发明的又一方面，在用于实现消息加密/解密技术的该模乘方法中，使用第一密钥（B）和第二密钥（N）对消息（A）加密/解密，该模乘方法包括：在各自的存储器中存储消息、第一密钥和 n 位的第二密钥；在每个时钟处使用该消息和第一密钥生成第一 n + 4 位信号；通过对该第一 n + 4 位信号和两个并行的 n + 4 位输入信号执行第一进位存储加法操作，生成由一个进位值和两个和值组成的 3 位序列；通过对该 3 位序列和一个输入进位值执行商操作，生成一个用于确定模数简化倍数的 3 位限定词；使用该第二密钥和该 3 位限定词，生成第二 n + 4 位信号；通过对该第二 n + 4 位信号和第一进位加法操作输出的各自和值及进位项执行第二进位存储加法操作，输出一对和值和进位值；通过对这对和值和进位值以及在先前时钟处从商逻辑电路输出的进位值执行全加操作输出一个进位输入值。在每个时钟处该消息右移 2 位。

生成该第一 n + 4 位信号的处理包括：利用该消息的两个低阶位执行 Booth 记录；根据该两个低阶位生成 0、B、2B、－B 和－2B 其中之一。该两个并行的 n + 4 位输入信号中的第一输入信号是按以下方式生成的：从该第二进位存储加法操作的和值项中选择高阶的 n + 2 位并插入两位作为所选的 n + 2 位的较高阶的位，且这两个较高阶位为零。该两个并行的 n + 4 位输入信号中的第二输入信号是按以下方式生成的：从该第二进位存储加法操作的进位项中选择较高的 n + 3 位并插入一位作为所选的 n + 3 位的较高位，且这个较

高位为零。该 3 位序列包括两个和值和一个进位值。该两个和值是第一进位存储加法操作输出的和值项中的最低有效位和次低有效位，该一个输入进位值是第一进位存储加法操作输出的进位值项中的最低有效位。该一的输入进位值是由全加操作生成的该进位输入值。根据 3 位限定词的两个较低位从 0、N、2N－N 和－2N 中选出该第二 n＋4 位信号。该对和值和进位值是第二进位存储加法操作输出的和值项中的次低有效位和进位值项中的最低有效位。第一进位存储加法操作输出的和值项和进位值项中的最高有效位被忽略。该模乘方法还包括在 m＋2 个时钟之后对该和值项和进位项执行进位传送加法操作，其中 m＝n/2。如果该进位传送加法操作的输出是负值，则该模乘方法还包括加上模第二密钥。

本发明的又一方面，在用于实现消息加密/解密技术的该模乘方法中，使用第一密钥（B）和第二密钥（N）对消息（A）加密/解密，该模乘方法包括：在各自的存储器中存储消息、第一密钥和 n 位的第二密钥；在每个时钟处使用该消息和第一密钥生成第一 n＋3 位信号；通过对该第一 n＋3 位信号和两个并行的 n＋3 位输入信号执行第一进位存储加法操作，输出由一个进位值和两个和值组成的 3 位序列；通过对该 3 位序列和一个输入进位值执行商操作，生成一个用于确定模数简化倍数的 2 位限定词；使用该第二密钥和该 2 位限定词，生成第二 n＋3 位信号；通过对该第二 n＋3 位信号和从第一进位加法操作输出的各自的和值和进位项执行第二进位存储加法操作，输出一对和值和进位值；通过对这对和值和进位值执行与（AND）操作输出一个进位输入值。在每个时钟处该消息右移 2 位。通过多路复用该消息的两个低阶位及第一密钥生成该第一 n＋3 位信号。该第一 n＋3 位信号是 0、B、2B 和 3B 其中之一。该两个并行的 n＋3 位输入信号中的第一输入信号是按以下方式生成的：从该第二进位存储加法操作的和值项中选择高阶 n＋1 位并插入两位作为所选的 n＋1 位的较高阶位，且这两个较高阶位为零。该两个并行的 n＋3 位输入信号中的第二输入信号是按以下方式生成的：从该第二进位存储加法操作的进位项中选择较高阶 n＋2 位并插入一位作为所选的 n＋2 位的较高阶位，且这个较高阶位为零。

该 3 位序列包括两个和值和一个进位值。该两个和值是第一进位存储加法操作输出的和值项中的最低有效位和次低有效位，该进位值是第一进位存储加法操作输出的进位值项中的最低有效位。该一个输入进位值是由与（AND）

操作生成的该进位输入值。根据 2 位限定词从 0、N、2N 和 3N 中选出该第二 n + 3 位信号。该对和值和进位值是第二进位存储加法操作输出的和值项中的次低有效位和进位值项中的最低有效位。从第一进位存储加法操作输出的和值项和进位项中的最高有效位被忽略。

该模乘方法还包括在 m + 2 个时钟之后对该第二进位存储加法操作输出的和值项和进位项执行进位传送加法操作。

附图说明

通过下面结合附图的详细描述可以更加清楚地理解本发明的上述和其它目的、特性和其它优点。面将参照附图详细说明本发明，从中可更清楚的理解本发明上述以及其它的目的、特点和优点，其中：

图 1 给出了依照本发明第一实施例的一个模乘装置的结构框图；

图 2 给出了图 1 中所示的记录电路的详细结构的框图；

图 3 给出了图 1 中所示的第一进位存储加法器的详细结构的框图；

图 4 给出了图 1 中所示的商逻辑电路的详细结构的框图；

图 5 给出了图 1 中所示的第二进位存储加法器的详细结构的框图；

图 6 给出了图 1 中所示的全加器的详细结构的框图；

图 7 给出了依照本发明第二实施例的一个模乘装置的结构框图；

图 8 给出了图 7 中所示的记录电路的详细结构的框图；

图 9 给出了图 7 中所示的第一进位存储加法器的详细结构的框图；

图 10 给出了图 7 中所示的商逻辑电路的详细结构的框图；

图 11 给出了图 7 中所示的第二进位存储加法器的详细结构的框图；

图 12 给出了图 7 中所示的全加器的详细结构的框图；

图 13 给出了一个依照本发明实施例的模乘装置的应用实例。

具体实施例

下面将参照附图详细说明本发明的优选实施例。即使在不同的附图中，相同或类似的元件都是由相同的参考标记表示。在下面的说明中，当所涉及的已知的功能和结构使本发明的主题不明确时，就将其省略。

A. 发明概述

在随后的说明中，本发明披露了一种使用蒙哥马利算法执行模乘 A · B mod N 的装置及方法，其中：

$A = a_{n-1} \cdot 2^{n-1} + \cdots + a_1 \cdot 2 + a_0$,

$B = b_{n-1} \cdot 2^{n-1} + \cdots + b_1 \cdot 2 + b_0$, 以及

$N = n_{n-1} \cdot 2^{n-1} + \cdots + n_1 \cdot 2 + n_0$。

此处，A 是乘数，B 是被乘数，N 是模数，每个位尺寸可以是很大的数，例如，512 或 1024。

下面将描述通过两个实施例执行模乘 A · B mod N。每个实施例都提出了一种在 m + 2 个时钟内利用 A、B 和 N（其中，$R=4^{m+2}$，$m = n/2$，$-N<=A$，以及 B<N）计算模乘 $A \cdot B \cdot R^{-1} \bmod N$ 的模乘装置和方法，A、B 和 N 中的每一个都是作为输入而接收的 n 位长度。通过使用由所提出的模乘装置得出的模乘结果可以计算模乘 A · B mod N。执行 RSA 运算所需的模幂 $m^e \bmod N$ 可由算出的 A · B mod N 导出。图 1 至 6 给出了依照本发明第一实施例的该模乘装置的元件结构框图，图 7 至 13 给出了依照本发明第二实施例的该模乘装置的元件结构框图。图 14 给出了适用于依照本发明实施例的该模乘装置的一个 IC 卡的框图。

本发明的实施例提供模乘装置，其中顺序移动乘数的位生成一个移位的位串，且该生成的位串的两个较低位被 Booth 记录。与仅记录顺序移动乘数位所生成的位串的一个单一较低位的传统模乘装置相反，本发明通过以记录两个较低位的方式处理多个位允许高速执行乘法。依照本发明实施例的模乘装置包括改进的记录逻辑电路和与该改进的用于执行蒙哥马利算法模乘操作的记录逻辑电路一致的其它的元件。

B. 第一实施例

B-1. 本发明的结构

图 1 给出了依照本发明第一实施例的一个模乘装置的结构框图。

参照图 1，该模乘装置包括记录逻辑电路 110，第一进位存储加法器（此处简写为“CSA1”）120，商逻辑电路 130，选择器 140，第二 CSA（“CSA2”）150，以及全加器（FA）160。该模乘装置是依照蒙哥马利算法，在 m + 2 个时钟内使用 A、B 和 N 计算 $A \cdot B \cdot R^{-1} \bmod N$ 的硬件装置，A、B 和 N（$R = 4^{m+2}$，$m = n/2$，$-N<=A$，以及 B<N）的每一个都具有 n 位输入。该模乘装置计算 $A \cdot B \cdot 2^{-(n+4)} \bmod N$。

CSA 120 和 150 中的每一个都由并行的（n＋4）个全加器组成，每个全加器有一个 3 位输入，输出一个进位和一个和位。记录逻辑电路 110 基于乘数 A 执行改进的 Booth 记录操作，并输出 0、±B 和±2B 值的其中一个作为该（n＋4）位的带符号的扩展位。该商逻辑电路 130 具有作为其输入的一个最低有效位(LSB)进位值 $C_{1,0}$以及来自 CSA1 120 的两个和值 LSB 位 $S_{1,1}$和 $S_{1,0}$，一个输入（carry-in），以及 B 的符号位，输出 3 位的 $q_2q_1q_0$，该值用于确定模数简化的倍数。可由多路复用器（MUX）实现的选择器 140 基于确定的值 q 选择并输出 0、±N 和±2N 的其中一个。该全加器 160 利用从 CSA2 150 输出的两位 $S_{2,1}$和 $C_{2,0}$以及作为其输入的进位值 cin 执行全加操作，并将生成的结果值提供给商逻辑电路 130 作为输入信号。

虽然图 1 中没有给出细节，但应该注意，该模乘装置包括用于将进位值以及和值存储每个时钟长度的临时存储寄存器 C 和 R，该进位值以及和值分别是 CSA1 120 与 CSA2 150 的输出，还包括一个进位传送加法器，用于将存储在该临时存储寄存器 C 和 R 中的值相加输出一个总的值作为模乘的结果。

图 2 给出了图 1 中所示的记录逻辑电路 110 的详细结构框图。

参照图 2，记录逻辑电路 110 Booth 记录由顺序移位乘数 A 所得的位串的两位较低位，用被乘数 B 多路复用该 Booth 记录结果，输出带符号的（n＋4）位二进制数。为了此目的，在记录逻辑电路 110 的前一级提供一个用于顺序移位乘数以生成一个移位串的移位寄存器 102 以及用于存储该被乘数的寄存器 104。记录逻辑电路 110 也包括一个 Booth 记录电路 112，一个多路复用器（MUX）114，以及一个一的补码器 116。Booth 记录电路 112 Booth 记录已生成的位串的两位较低位 a_{i+1}和 a_i。多路复用器 114 用被乘数多路复用该 Booth 记录的结果 z_{i+1}，输出 0、B 和 2B 作为多路复用的结果。一的补码器 116 依照该已生成的位串的两位较低位对多路复用器 114 的输出执行一的取补操作，输出带符号的（n＋4）位二进制数。根据乘数 A 实现改进 Booth 记录的记录逻辑电路 110 输出（n＋4）位的一个带符号的扩展位，其值可以是 0、±B 和±2B 其中之一。

图 3 的框图详细示出了图 1 所示 CSA1 120 的结构。

参照图 3，具有（n＋4）个全加器 121 至 125 的 CSA1 120 具有作为其输入并来自记录逻辑电路 110 的二进制的(n＋2)位的第一信号 $S_{2,2}$至 $S_{2,n+3}$、（n＋3）位的第二信号 $C_{2,1}$至 $C_{2,n+3}$、以及（n+4）位的第三信号 B_0至 B_{n+3}，并借

助（n+4）全加器 121 至 125 将所有的输入全加以输出（n+4）位的进位值 $C_{1,0}$至 $C_{1,n+3}$以及和值 $S_{1,0}$至 $S_{1,n+3}$。 此处，将该第一信号的第（n+2）个较高位 $S_{2,n+3}$输入到三个较高位全加器 123 至 125，将该第二信号的第（n+3）个较高位 $C_{2,n+3}$输入到两个较高位全加器 124 和 125。

图 4 给出了图 1 所示的商逻辑电路 130 的详细结构框图。

参照图 4，商逻辑电路 130 具有作为其输入的从两个较低全加器输出的和值 $S_{1,0}$和 $S_{1,1}$ 以及从最低全加器输出的进位值 $C_{1,0}$，这是从 CSA1 120 的（n+4）个进位值以及和值中选出的，并输出一个三位的确定值 $q_1q_2q_3$ 来确定模数简化的倍数。商逻辑电路 130 包括 D 触发器 132、全加器 134、异或（XOR）逻辑门 136 以及组合电路 138。D 触发器 132 临时存储一位来自 FA160 的进位输入值 Carry-in。全加器 134 将存储在 D 触发器 132 内的进位输入值 Carry-in 与 CSA1 120 的最低有效位全加器 121 输出的和值 $S_{1,0}$全加。异或（XOR）逻辑门 136 在 CSA1 120 的最低有效位全加器 121 输出的该进位值 $C_{1,0}$与次低位全加器 122 输出的和值 $S_{1,1}$之间执行异或运算。每一个全加器 134 和异或逻辑门 136 都具有用于修正的预置进位值 cin，全加器 134 还具有被乘数的一个符号位 B。组合电路 138 将全加器 134 的输出 S_0、异或逻辑门 136 的输出 S_1以及预置输入位 n_1 合并，输出三位的确定值 $q_1q_2q_3$。

图 5 给出了图 1 所示的 CSA2 150 的详细结构框图。

参照图 5，CSA2 150 包括（n+4）个全加器 151 至 156。CSA2 150 包括作为第一输入信号的从选择器 140 选出的（n+4）位的模数 N（N_0-N_{n+3}）、作为第二输入信号的来自 CSA1 120 的（n+4）位进位值中除了最高有效位进位值的（n+3）位的剩余进位值 $C_{1,0}$至 $C_{1,n+3}$以及作为第三输入信号的来自 CSA1 120 的（n+4）位和值中除了最低有效位进位值的（n+3）位的剩余和值 $S_{1,0}$至 $S_{1,n+3}$，用于借助全加器 151 至 156 输出（n+4）位的进位值 $C_{2,0}$ 至 $C_{2,n+3}$和（n+4）位的和值 $S_{2,0}$至 $S_{2,n+3}$。第一输入信号的（n+4）位是从最低有效位的全加器 151 开始按顺序分别输入到全加器 151 至 156，第二输入信号的（n+3）位是从次低位的全加器 152 开始按顺序分别输入到全加器 152 至 156，第三输入信号的（n+3）位是从次低位的全加器 152 开始按顺序分别输入到全加器 152 至 156。全加器 151 至 156 的最低有效位全加器 151 的输入是来自商逻辑电路 130 的全加器 134 的输出 S_0、$q_{i,2}$以及模数 N 的最低有效位 N_0。

图 6 给出了图 1 所示全加器 160 的详细结构框图。

参照图 6，全加器 160 将 CSA2 150 的最低有效位全加器 151 输出的进位值 $C_{2,0}$ 与次低位全加器 151 输出的和值 $S_{2,0}$ 全加，输出进位输入值 Carry-in。全加器 160 还具有一位用于修正全加操作的的进位值 cin，输出进位输入值 Carry-in 作为全加操作的结果。该进位输入值被提供给商逻辑电路 130。

B-2. 发明原理

本发明提供一种用于在 m + 2 个时钟内利用 A、B 和 N((R = 4^{m+2}, m = n/2, -N<=A，以及 B<N)) 计算 A · B · R^{-1} mod N 的装置，其中，A、B 和 N 都具有 n 位的输入。下面将说明可用于实现本发明的三个原理。该三个原理包括表示用于模乘的乘数 A 和被乘数 B 的第一原理，记录用于模乘的乘数 A 的第二原理以及使用本发明记录原理的蒙哥马利算法的第三原理。

B-2a. 数字表示

本发明中，用于模乘的该乘数 A 和被乘数 B 由带符号的二进制数表示。A 和 B 都具有 n 位，被分别的变换成用于带符号操作的（n + 4）位。在变换期间，任何的负值都被转换成它们的一的补码。

B-2b. Booth 记录

本发明使用一种改进的 Booth 记录系统，该系统是适于本发明的已为本领域技术人员所熟知的 Booth 记录系统的改进。本发明提高了模乘速度。依靠该改进的 Booth 记录系统将乘数 A 记录为 2 位 z_i（其中 $0 \le i \le m+1$）。此处，假设 $a_{n+4} = a_{n+3}$，$a_1 = 0$。下表给出了依照本发明的改进的 Booth 记录的规则。

表 1

a_{i+1}	a_i	a_{i-1}	Z_{i+1}
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	2
1	0	0	-2
1	0	1	-1
1	1	0	-1
1	1	1	0

B-2c. 使用 Booth 记录的基数 - 4 蒙哥马利算法

下面方程 1 中例举的算法给出了本发明对于基数－4 蒙哥马利算法采用了改进的 Booth 记录系统。最初的蒙哥马利算法将结果值与模数 N 进行比较，如果结果值大于模数 N，则执行减法运算。然而，本发明下面的算法没有示出原始蒙哥马利算法的这种比较和减法。

方程 1:

输入: N、 $-N \leqslant A、B < N$

输出: $S = A \cdot B \cdot 4^{m+2} \bmod N$, $-N \leqslant S < N$

$S = 0$ (1)

for $i = 0$ to $(n+1)/2$ (2)

$S = S + A_i \times B$ (3)

$q_{i(2,1,0)} = f(s_1, s_0, n_1, n_0)$ (4)

$S = S + q_i \times N$ (5)

$S = S/2^2$ (6)

end for (7)

在方程 1 的算法中，A_i 在处理（3）是指两个 Booth 记录位，其值为 $-2 < A_i < 2$。处理（4）是指能使处理（5）的结果值的两个最低有效位成为“0”的函数。处理（4）的结果值取决于输入位 s_1、s_0、n_1 和 n_0，并如表 2 所示被确定。用于模数简化的值 q_i 的最高有效位（MSB）q_{i2} 是一个符号位。q_i 是元素集{0、±1、2}中之一个元素，并依照方程 2 来计算。

方程 2

$$q_0 = s_0$$

$$q_1 = \overline{s_0} s_1$$

$$q_2 = s_0 \overline{\overline{s_1} n_1} + s_n s_1 n_1$$

表 2

s_0	s_1	n_1	q_2	q_1q_2
0	0	0	0	00
0	0	1	0	00
0	1	0	0	10
0	1	1	0	10
1	0	0	1	01
1	0	1	0	01

1	1	0	0	01
1	1	1	1	01

B-3. 本发明的操作

如图 1 所示的本发明的装置在 m + 2 个时钟内利用 N，A、B 和 N（$R = 4^{m+2}$，$m = n/2$，$-N \leqslant A$，以及 $B<N$）计算 $A \cdot B \cdot R^{-1} \mod N$，其中，A、B 和 N 都具有 n 位的输入。

下面将说明利用图 1 所示的装置计算 $A \cdot B \cdot R^{-1} \mod N$（其中 $R = 4^{m+2}$）的处理。在下面的说明中，步骤 a）是初始化步骤，步骤 b）至 h）是每个时钟将被执行的步骤，步骤 i）是在（m + 2）个时钟期间内在执行步骤 b）到 h）之后被执行的步骤。

a）都具有 n 位用于模乘输入的 A、B 和 N 被存储在各自的寄存器（或存储器）中。虽然本发明的装置给出了输入 A 和 B 存储在各自的寄存器 102 和 104 中，而没有给出以 N 位存储的分开的寄存器，但用在本发明中的这样分开的寄存器对于本领域技术人员来说是很清楚的。此处，存储 A 的寄存器 102 是一个移位寄存器，每个时钟 A 被向右移两位。出于方便的原因，存储 A 的寄存器表示为寄存器 A，存储 B 的寄存器表示为寄存器 B。至于存储器，则一次一个字的读出 A 和 B。用于临时存储图 1 所示的 CSA2 150 的计算值的临时寄存器（或存储器）C 和 S（都没有给出细节）被初始化为“0”。

b）当所有的数据都被输入给寄存器 102 和 104 中的每一个时，记录逻辑电路 110 的 Booth 记录电路 112 基于寄存器 102 中的两个 LSB 位执行 Booth 记录功能。记录逻辑电路 110 的 MUX 114 具有作为其输入并存储在寄存器 104 中的 B 的值，并基于寄存器 102 的两个 LSB 位生成 0、±B、±2B 值的其中一个，提供给 CSA1 120 以作为其三个输入的一个。此时，记录逻辑电路 110 的一的补码器 116 基于寄存器 102 的两个 LSB 位将 0、±B、±2B 值的其中一个变换为它的一的补码，并将该一的补码表示成 n + 4 位数，提供给 CSA1 120 以作为其三个输入的一个。

c）CSA1 120 对三个输入的 n + 4 位的带符号二进制数执行加法操作。CSA1 120 由 n + 4 个全加器 121 至 125 构成。前一级全加器生成的进位提供给后一级的全加器，而最高有效位（MSB）全加器 125 生成的进位被忽略。

d）商逻辑电路 130 具有作为其输入的来自 CSA1 120 的值 $S_{1,1}$、$C_{1,0}$ 和 $S_{1,0}$，来自全加器 160 的 Carry-in 信号，被乘数 B 的符号位 B，依靠全加器

134 和异或逻辑门 136 计算并输出 S_1和 S_0。用于修正的进位信号 cin 输入至全加器 134 和异或逻辑门 136。进位信号 cin 是用于修正使用二的补码的已有的 Booth 记录系统与使用一位补码的本发明的 Booth 记录系统之间的差异的信号。

e）商逻辑电路 130 的组合电路 138 其输入为步骤 d）所得的 S_1和 S_0，依靠表 2 的真值表确定一个三位的值 q。虽然没有给出依靠表 2 的真值表确定 q 值的电路的详细结构，但是通过一般的逻辑门电路实现用于确定 q 值的电路对本领域技术人员来讲是很明显的。

f）CSA2 150 具有作为其输入的在步骤 c）中 CSA1 120 输出的进位值以及和值，以及通过步骤 e）中所得 q 值的两位 LSB 确定的从 0、±N 和 ±2N 中选择的 n + 4 位的带符号的二进制数，其执行 n + 4 位带符号操作。CSA2 150 由 n + 4 个全加器 151 至 156 构成。步骤 e）中所得 q 值的 MSB 值 $q_{1,2}$作为全加器 151 至 156 的 LSB 全加器 151 的进位输入。

g）全加器 160 具有作为其输入的从 CSA2 150 输出的值 $S_{2,1}$ 和 $C_{2,0}$，以及用于修正的进位信号 cin，通过全加该输入以输出 Carry-in。此全加操作是用于修正使用二的补码的已有的 Booth 记录系统与使用一的补码的本发明的 Booth 记录系统之间的差异。

h）来自 CSA2 150 输出的 MSB 的（n + 2）个和值和（n + 3）个进位值被反馈到 CSA1 120 作为其输入。此时，CSA2 150 的 MSB 全加器 156 输出的和值的 MSB $S_{2,n+3}$被复制，并在其上添加两位，CSA2 150 的 MSB 全加器 156 输出的进位值的 MSB $C_{2,n+3}$被复制，并在其上添加一位。对 $S_{2,n+3}$ 和 $C_{2,n+3}$ 的复制与添加的结果被输入到 CSA1 120。CSA2 150 的全加器 156 输出的和值 $S_{2,n+3}$ 被提供给 CSA1 120 的三个全加器 123 至 125，以及进位值 $C_{2,n+3}$被提供给 CSA1 120 的两个全加器 124 和 125。

i）在（m + 2）个时钟内执行完步骤 b）和 h）之后执行下面的操作。一个进位传送加法器（CPA）（未给出）对 CSA2 150 输出的该进位值及和值执行加法操作。如果该加法的结果值为负数，则在其上加模数 N，但如果该加法的结果值为正数，则不用在其上加模数 N。

例如，如方程 3 所示，如果 A、B 和 N 每一个都有 12 位，则依照上述处理的蒙哥马利模运算结果如下面的表 3 和表 4 所示。

方程 3

N = 0000. 1010. 0101. 1001 (0xA59)　　B = 0000. 0101. 1100. 0011 (0x5C3)

N' = 1111. 0101. 1010. 0110　　B' = 1111. 1010. 0011. 1100

2N = 0001. 0100. 1011. 0010　　2B' = 1111. 0100. 0111. 1001

A = 0000. 1001. 0011. 1110 (0x93E)

5 表 3

i	A_i	CSA1 输出 S C	B 符号位	Carry-in	S_1S_0	C
i	0	0000. 0000. 0000. 0000 0. 0000. 0000. 0000. 000	0	0	00	0
0	-2	1111. 0100. 0111. 1001 0. 0000. 0000. 0000. 000	1	0	10	1
1	0	1111. 0010. 0010. 1010 0. 0001. 0000. 0010. 100	0	1	11	0
2	0	1111. 0011. 0000. 0000 0. 0001. 0000. 0010. 100	0	1	01	0
3	1	1111. 1000. 1111. 0000 0. 0000. 1011. 0000. 011	0	1	11	0
4	1	1111. 1110. 1000. 0000 0. 0000. 1010. 1101. 001	0	1	11	0
5	-2	0000. 0000. 0000. 0000 1. 1110. 1010. 1101. 001	1	1	10	1
6	1	1111. 1110. 1011. 0110 0. 0000. 1010. 1001. 001	0	1	01	0
7	0	1111. 1111. 0011. 0110 0. 0000. 0000. 0000. 000	0	1	00	1

表 4

I	A_i	S_1S_0	C	q_2q_1	CSA2 out S C	Carry-in

I	0	00	0	000	0000.0000.0000.0000 0.0000.0000.0000.000	0
0	-2	10	1	010	(11).1110.0000.1100.1010 (0)0.0010.1000.0110.000	1
1	0	11	0	001	(11). 1110.1000.0101.0010 (0)0.0010.0100.0101.001	1
2	0	01	0	101	(00).0001.0110.1000.1110 (1)1.1110.0010.0110.001	1
3	1	11	0	001	(11).1111.1001.1010.1110 (0)0.0001.0100.1010.001	1
4	1	11	0	001	(11).1111.1110.0000.1110 (0)0.0001.0101.1010.001	1
5	-2	10	1	010	(11).1111.0000.1111.0010 (0)0.0001.1101.0010.010	1
6	1	01	0	101	(00).0000.0001.1000.0010 (1).1111.1101.0110.111	1
7	0	00	1	000	1111.1111.1011.1010 0.0000.0000.0000.000	1

下面将说明通过本发明上述装置使用运算结果值计算模乘 A · B mod N 的处理。应当注意，对于本领域普通技术人员来讲，用于执行该处理的硬件结构是很明显的，因此，此处省略了详细的说明。执行下面的计算:

1）计算 $P=2^{2(n+4)} \bmod N$;

2）计算 $C=A \cdot B \cdot 2^{-2(n+4)} \bmod N$; 以及

3）计算 $P \cdot C \cdot 2^{-2(n+4)} \bmod N = A \cdot B \bmod N$。

下面将说明使用本发明上述装置运算的结果值来计算 RSA 运算所需的模幂 $m^e \bmod N$ 的处理。执行下面的运算:

1） 在寄存器（或存储器）中存储指数 e;

2） 在临时寄存器 C 中存储模数 N;

3） 将寄存器 C 和 S 初始化为 “0”;

4） 执行蒙哥马利模乘 $m' = f_m(m, P, N) = m \cdot P \cdot R^{-1} \bmod N$, 其中 P 在模幂中是上述处理定义的预先计算的值，以及 $R = 4^{n+2}$;

5） 将 m' 载入该寄存器 B;

6） 使用载入寄存器 B 的值执行模平方运算，此处，将蒙哥马利模乘所需的乘数 A 从寄存器 B 中读出，该值是通过使用改进的 Booth 记录电路获得的;

7） 向左移位该指数 e;

8） 忽略指数 e 的 MSB 1，在下一位之后执行后面的步骤 9）和 10);

9） 忽略指数 e 的一位（0 或 1）执行用于模平方运算的步骤 4）和 5），其中该平方运算所需的乘数和被乘数分别存储在寄存器 A 和寄存器 B 中;

10） 如果指数 e 的当前位是 1，在步骤 9）之后执行用于模乘的步骤 4）和 5），其中该被乘数是寄存器 B 中的内容，乘数是在求幂中的底数 m'；以及

11） 在对指数 e 的所有位执行步骤 8）至 10）之后，再一次使用步骤 4）执行该模乘，其中被乘数是寄存器 B 的内容，乘数是 1。

如果在执行完上述的步骤 1）至 11）之后对保留在寄存器 C 和 S 内的值执行 CPA 运算的结果值是负数，则将模数 N 添加到其上。反之，如果该结果值是正数，这就是求幂 m^e mod N 的最终值，不需加模数 N。

B-4. 本发明的效果

从上述说明可见，本发明提供一种用于计算 $A \cdot B \cdot 2^{-2(n+4)} \text{mod} N$ 的电路，依靠此电路可以计算一般的模乘 $A \cdot B \text{mod} N$。依照本发明计算的 $A \cdot B \text{mod} N$ 适用于硬件装置，该装置用于生成和验证数字签名的装置中。此外，本发明适用于基于 IC 卡的用于生成电子签名、验证身份以及加密/解密的硬件装置中。此外，本发明依靠执行模乘运算的电子签名装置，能提供用于加密和解密数据或消息的装置。另外，本发明能够实现现有的基于电子签名装置公开密钥密码系统，例如 NIST-DSS, RSA, ELGamal 以及 Schnorr 电子签名。

C. 第二实施例

C-1. 本发明的结构

图 7 给出了依照本发明第二实施例的一个模乘装置的结构框图。

参照图 7，该模乘装置包括记录逻辑电路 210，第一进位存储加法器（此处简写为 “CSA1”）220，商逻辑电路 230，选择器 240，第二进位存储加法器（CSA2）250，以及与（AND）逻辑门 260。 该模乘装置是一个硬件装置，用于根据蒙哥马利算法在 m + 2 个时钟内使用 A、B 和 N（$R = 4^{m+2}$，$m = n/2$，$-N \leqslant A$，以及 $B<N$）计算 $A \cdot B \cdot R^{-1} \text{mod} N$，其中， A、B 和 N 每一个都具有

n 位输入。 即，该模乘装置具有用于计算 $A \cdot B \cdot 2^{-(n+4)} \bmod N$ 的结构。

每一个 CSA 220 和 250 的都由（n+4）个并行的全加器构成，每个全加器有一个 3 位输入，输出一位进位和一位和值。逻辑电路 210 基于乘数 A 执行改进的 Booth 记录操作，并输出（n+3）位的 0、B、2B 和 3B 值的其中一个。商逻辑电路 230 其输入有一个最低有效位（LSB）进位值 $C_{1,0}$以及两位来自 CSA1 220 和值的 LSB 位 $S_{1,1}$和 $S_{1,0}$、一个 carry-in、以及 B 的符号位，输出 2 位的 q_1q_0，该值用于确定模数简化的倍数。选择器 240 可由多路复用器（MUX）实现，基于确定的 q 值来选择并输出 0、N、2N 和 3N 的其中一个。AND 逻辑门 260 执行与操作，CSA2 250 输出的两位 $S_{2,1}$和 $C_{2,0}$作为其输入，并将与操作的结果值提供给商逻辑电路 230 作为 carry-in 信号。

虽然图 7 中没有给出细节，但应该注意该模乘装置包括用于将进位值以及和值存储长达每个时钟的临时存储寄存器 C 和 R，该进位值以及和值来自 CSA2 250 的输出，还包括一个进位传送加法器，用于将存储在该临时存储寄存器 C 和 R 中的值相加输出一个总的值作为模乘的结果。

图 8 给出了图 7 中所示的记录逻辑电路 210 的详细结构框图。

参照图 8，记录逻辑电路 210 Booth 记录由顺序移位乘数 A 所得的位串的两位较低位，多路复用具有被乘数 B 的 Booth 记录结果，输出（n+3）位二进制数。为了此目的，在记录逻辑电路 210 的前一级提供一个用于顺序移位乘数以生成一个移位串的移位寄存器 202 以及用于存储该被乘数的寄存器 204。记录逻辑电路 210 也包括一个多路复用器（MUX）212。多路复用器 212 多路复用所生成的具有被乘数的位串的两个较低位 a_{i+1}和 a_i，并输出 0、B、2B 和 3B 作为多路复用的结果。记录逻辑电路 210 是基于乘数 A 实现改进的 Booth 记录的电路，其选择并输出（n+3）位 0、B、2B 和 3B 值的其中之一。

图 9 给出了图 7 所示的 CSA1 的详细结构框图。

参照图 9，具有（n+4）个全加器 221 至 225 的 CSA1 220 具有作为其输入的（n+1）位的第一信号 $S_{2,2}$至 $S_{2,n+2}$、（n+2）位的第二信号 $C_{2,1}$至 $C_{2,n+2}$、以及来自记录逻辑电路 210 的（n+3）位二进制数的第三输入信号 B_0至 B_{n+2}，依靠（n+3）个全加器 221 至 225 将所有的输入全加输出（n+3）位的进位值 $C_{1,0}$至 $C_{1,n+2}$以及和值 $S_{1,0}$至 $S_{1,n+2}$。该第一和第二信号是 CSA2 250 提供的信号，第三信号是记录逻辑电路 210 提供的。该第一信号的最高有效位 $S_{2,n+2}$被输入到全加器的第三高位全加器 223 中，该第二信号的最高有效位 $C_{2,n}$

$_{+2}$被输入到全加器的第二高位全加器 224 中。全加器的最高有效位全加器 225 具有“0”作为第一和第二信号，以及第二高位全加器 224 具有“0”作为第三信号。即，（n+1）位的第一信号 $S_{2,2}$至 $S_{2,n+2}$分别顺序的输入至 CSA1 220 的最低有效位全加器 221 和第（n+1）位全加器 223，“0”作为第一信号被输入至第（n+2）位全加器 224 和第（n+3）位全加器 225。此外，（n+2）位的第二信号 $C_{2,1}$至 $C_{2,n+2}$分别顺序的输入至 CSA1 220 的最低有效位全加器 221 和第（n+2）位全加器 224，“0”作为第二信号分别顺序的输入至 CSA1 220 的最低有效位全加器 221 和第（n+1）位全加器 223。

图 10 给出了图 7 所示的商逻辑电路 230 的详细结构框图。

参照图 10，商逻辑电路 230 具有作为其输入的两个较低位全加器输出的和值 $S_{1,0}$和 $S_{1,1}$ 以及最低有效位全加器输出的进位值 $C_{1,0}$，这是从 CSA1 120 的（n+4）位进位值以及和值中选出的，并输出一个 2 位的确定值 q_1q_0来确定模数简化的倍数。商逻辑电路 230 包括 D 触发器 232、半加器 234、异或（XOR）逻辑门 126 以及组合电路 238。D 触发器 232 临时存储一位来自与逻辑门 260 的进位输入值 Carry-in。半加器 234 将存储在 D 触发器 232 内的进位输入值 Carry-in 与 CSA1 220 的最低有效位全加器 221 输出的和值 $S_{1,0}$半加。异或（XOR）逻辑门 236 在 CSA1 220 的最低有效位全加器 221 输出的该进位值 $C_{1,0}$与次低全加器 222 输出的和值 $S_{1,1}$之间执行异或运算。组合电路 238 将半加器 234 的输出 S_0、异或逻辑门 236 的输出 S_1以及预置输入位 n_1 合并，输出 2 位的确定值 q_1q_0。

图 11 给出了图 7 所示的 CSA2 250 的详细结构框图。

参照图 11，CSA2 250 包括（n+3）个全加器 251 至 256。CSA2 250 包括从选择器 240 选出的（n+3）位的模数 N（N_0 - N_{n+2}）作为第一输入信号，和来自 CSA1 220 的（n+3）位进位值中除了最高有效位进位值的（n+3）位的剩余进位值 $C_{1,0}$ 至 $C_{1,n+2}$作为第二输入信号，以及来自 CSA1 220 的（n+3）位和值中除了最低有效位和值的（n+2）位的剩余和值 $S_{1,1}$ 至 $S_{1,n+2}$作为第三输入信号，通过（n+3）个全加器 251 至 256 输出（n+3）位的进位值 $C_{2,0}$至 $C_{2,n+2}$和（n+3）位的和值 $S_{2,0}$至 $S_{2,n+2}$。第一输入信号的（n+3）位是从最低有效位的全加器 251 开始到全加器 251 至 256 分别依顺序输入的，第二输入信号的（n+2）位是从次低有效位的全加器 252 开始到全加器 252 至 256 分别依顺序输入的，第三输入信号的（n+2）位是从次低有效位的全加器 252

开始到全加器 252 至 256 分别依顺序输入的。全加器 251 至 256 的最低有效位全加器 251 的输入是来自商逻辑电路 230 的全加器 234 的输出 S_0以及来自与（AND）逻辑门 260 的进位输入值。

图 12 给出了图 7 所示的 AND 逻辑门的详细结构框图。

参照图 12， AND 逻辑门 260 将 CSA2 250 的最低有效位全加器 251 输出的进位值 $C_{2,0}$与次低位全加器 251 输出的和值 $S_{2,1}$全加，输出进位输入值 Carry-in。该进位输入值 Carry-in 被提供给商逻辑电路 230。

C-2.发明原理

本发明提供一种用于在 m + 2 个时钟内使用 A、B 和 N（$R = 4^{m+2}$，$m = n/2$，$-N \leqslant A$，以及 $B<N$）计算 $A \cdot B \cdot R^{-1} \mod N$ 的装置，群众，A、B 和 N 具有 n 位的输入。下面将说明可用于实现本发明的两个原理。该两个原理包括表示用于模乘的乘数 A 和被乘数 B 的第一原理以及使用本发明记录原理的蒙哥马利算法的第二原理。

C-2a.2 位扫描

本发明中，在每个时钟从 LSB 以两位扫描（或移位）该乘数 A，然后将其与被乘数 B 相乘，该乘的结果用于蒙哥马利算法。因此，每个循环生成的 a_i是元素集{0、1、2、3}中的一个元素，该 a_i与被乘数 B 相乘，相乘的结果被输入至 CSA1 220。

C-2b.基数－4 蒙哥马利算法

下面方程 4 中例举的算法给出了本发明采用基数－4 蒙哥马利模乘。原始的蒙哥马利算法将结果值与模数 N 进行比较，如果结果值大于模数 N，则执行减法运算。然而，本发明下面的算法并没有示出原始蒙哥马利算法的这种比较和操作。

方程 4

输入：N、$-N<=A$、$B<N$

输出：$S = A \cdot B \cdot 4^{m+2} \mod N$，$0 \leqslant S<N$

$S = 0$ （1）

for $i = 0$ to $(n+1)/2$ （2）

$S = S + A_i \times B$ （3）

$q_{i(1,0)} = f(s_1, s_0, n_1, n_0)$ （4）

$S = S + q_i \times N$ （5）

$S = S/2^2$ （6）

end for （7）

在方程 4 的算法中，A_i 在处理（3）是指两个被扫描的位。处理（4）是指能使处理（5）的结果值的两个最低有效位为“0”的函数。由于 N 是奇数且 n_0 一直是 1，所以处理（4）的结果值取决于输入位 s_1、s_0、n_1 和 n_0，且对于蒙哥马利模乘来说，该值事实上如下面的表 5 所示的被确定。用于模数简化的值 q_i 是元素集{0、1、2、3}中的一个元素，并依照方程 5 来计算。

方程 5

$$q_0 = s_0$$

$$q_1 = s_0\overline{s_1 n_1} + s_0 s_1 + s_1 n_1$$

表 5

s_0	s_1	n_1	q_1	q0
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	0
1	0	0	1	1
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

C-3. 本发明的操作

如图 7 所示本发明的装置在 m + 2 个时钟内使用 A、B 和 N（$R = 4^{m+2}$，$m = n/2$，$-N \leqslant A$，以及 $B<N$）计算 $A \cdot B \cdot R^{-1} \bmod N$，作为其输入的 A、B 和 N 都具有 n 位。

下面将说明利用图 7 所示的装置计算 $A \cdot B \cdot R^{-1} \bmod N$（其中 $R = 4^{m+2}$）的处理。在下面的说明中，步骤 a）是初始化步骤，步骤 b）至 h）是每个时钟执行的步骤，和步骤 i）是在（m + 2）个时钟期间执行步骤 b）至 h）后将被执行的步骤。

a）每一个都由 n 位组成并用于模乘的 A、B 和 N 被存储在各自的寄存器（或存储器）中。此外，n + 2 位的 2B 和 3B 存储在各自的寄存器（或存储器）中。虽然本发明的装置显示了在各自的寄存器 202 和 204 中存储输入 A 和 B，

而没有示出分别存储 2B 和 3B 的独立的寄存器，但对于本领域技术人员来说很明显，这种独立的寄存器可以被用在本发明的装置中。存储 A 的寄存器 202 是一个移位寄存器，每个时钟将 A 右移两位。存储 A 的寄存器表示为寄存器 A，存储 B 的寄存器表示为寄存器 B。在使用存储器的情况下，一次一个字的读出 A 和 B。临时存储图 7 所示的 CSA2 250 计算结果的临时寄存器（或存储器）C 和 S（没有给出细节）被初始化为“0”。

b）当所有的数据被输入至寄存器 202 和 204 中的每一个时，记录逻辑电路 210 基于寄存器 A 202 中的两个 LSB 位执行 Booth 记录功能。记录逻辑电路 210 的 MUX 212 具有作为其输入的存储在寄存器 204 中的 B 的值，并基于寄存器 A 202 中的两个 LSB 位选择 0、B、2B 和 3B 值的其中一个，提供给 CSA1 220 作为其三个输入的一个。

c）CSA1 220 对三个输入的 n + 3 位的带符号二进制数执行加法操作。CSA1 220 由 n + 3 个全加器 121 至 125 构成。

d）商逻辑电路 230 具有作为其输入的来自 CSA1 220 的值 $S_{1,1}$ 、$C_{1,0}$ 和 $S_{1,0}$、及来自与（AND）逻辑门 260 的 Carry-in 信号，依靠半加器 234 和异或逻辑门 236 计算并输出 S_1 和 S_0。

e）商逻辑电路 230 的组合电路 238 其输入为步骤 d）所得的 S_1 和 S_0，依靠表 5 的真值表确定一个 2 位的值 q。虽然没有给出依靠表 5 的真值表确定 q 值的电路的详细结构，但是通过一般的逻辑门电路实现用于确定 q 值的电路对本领域技术人员来讲是很明显的。

f）CSA2 250 具有作为其输入的在步骤 c）中 CSA1 220 输出的进位值及和值，以及通过步骤 e）中所得 q 值的两个 LSB 位确定的从 0、N、2N 和 3N 中选择的 n + 3 位的二进制数，以执行 n + 3 位的无符号操作。CSA2 250 由 n + 3 个全加器 251 至 256 构成，类似于 CSA1 220。应当注意，全加器 251 至 256 的 LSB 全加器 251 具有作为其进位输入的前一级生成的 Carry-in 信号。

g）与逻辑门 260 具有作为其输入的 CSA2 250 的输出值 $S_{2,1}$ 和 $C_{2,0}$，通过对该输入执行与操作输出 Carry-in 位。

h）来自 CSA2 250 输出的 MSB 的（n + 2）个和值和（n + 3）个进位值被反馈到 CSA1 220 作为其输入。该和值的两个较高位和进位值的一个较高位是“0”，且在 CSA2 250 中两个位被右移以用于到 CSA1 220 的反馈。从 CSA2 250 的全加器 256 输出的和值 $S_{2,n+2}$ 被提供给 CSA1 220 的第三最高全加器 223，

和值“0” 被提供给MSB全加器225和第二最高全加器224。CSA2 250的全加器256输出的进位值$C_{2,n+2}$被提供给CSA1 220的第二最高全加器224，进位值“0” 被提供给MSB全加器225。

i）在（m+2）个时钟内执行完步骤b）和h）之后执行下面的操作。一个进位传送加法器（CPA）（未示出）对CSA2 250输出的该进位值及和值执行加法操作。

例如，如方程6所示，如果A、B和N中的每一个都有12位，则依照上述处理的蒙哥马利模运算结果如下面的表6和表7所示。此时，最终的运算结果如下所示：最终结果：

0111.1100.0111(0x7C7)+0010.1000.0000(0x280)+1=1010.0100.1000(0xA48)

方程6

N=000.1010.0101.1001(0xA59)　　B = 000.0101.1100.0011(0x5C3)

2N=001.0100.1011.0010((0x13B2)　　2B=000.1011.1000.0110(0xB86)

3N=001.1111.0000.1011(0x1F0B)　　3B= 001.0001.0100.1001(0x1149)

A=000.1001.0011.1110(0x93E)

表6

I	A_i	CSA1输出 S C	Carry-in	S_1S_0
I	0	0000.0000.0000.0000 0000.0000.0000.000	0	00
0	2	000.1011.1000.0110 0000.0000.0000.000	0	10
1	3	001.0110.1100.0101 0000.0010.1001.001	0	11
2	3	001.0111.0000.0000 0000.0010.1001.001	1	01
3	0	000.1001.1010.0010 0000.0101.0000.000	1	00
4	1	000.0110.0101.0000	1	11

		0000.0011.0000.011		
5	2	000.1001.0110.1101 1.1110.1010.1101.001	1	10
6	0	000.0100.0010.0100 0000.0101.0010.010	1	01
7	0	000.0101.0001.0000 0000.0101.0000.010	1	01

表 7

I	A_i	S_1S_0	q_2q_1	CSA2 输出 S C	Carry-in
I	0	00	00	0000.0000.0000.0000 0.0000.0000.0000.000	0
0	2	10	01	(0.0).010.1111.0011.0100 (0).0000.0001.0000.010	0
1	3	11	01	(0.0)001.1110.0000.1110 (0).0000.0101.1010.001	1
2	3	01	11	(0.0).000.1010.0011.1010 (0).0010.1111.0000.011	1
3	0	00	00	(0.0)000.1100.0100.1110 (0).0000.0010.0000.001	1
4	1	11	01	(0.0)000.1111.0000.1110 (0).0000.0100.1010.001	1
5	2	10	10	(0.0)001.1010.1101.1010 (0).0000.1010.0100.101	1
6	0	01	11	(0.0)001.1110.0000.1010 (0).0000.1010.0100.101	1
7	0	01	11	(0.0)001.1111.0001.1110 0.0000.1010.0000.001	1

下面将说明使用本发明上述装置运算的结果值来计算模乘 A · B mod N

的处理。应当注意，对于本领域普通技术人员来讲，用于执行该处理的硬件结构是很明显的，因此，此处省略了详细的说明。执下面的计算:

1）计算 $P = 2^{2(n+4)} \bmod N$;

2）计算 $C = A \cdot B \cdot 2^{-2(n+4)} \bmod N$; 以及

3）计算 $P \cdot C \cdot 2^{-2(n+4)} \bmod N = A \cdot B \bmod N$。

下面将说明使用本发明上述装置运算的结果值来计算RSA运算所需的模幂 $m^e \bmod N$ 的处理。执行下面的处理:

1） 将指数 e 存储在寄存器（或存储器）中;

2） 将模数 N 存储在临时寄存器 C 中;

3） 将寄存器 C 和 S 初始化为 “0”;

4） 执行蒙哥马利模乘 $m' = f_m(m, P, N) = m \cdot P \cdot R^{-1} \bmod N$，其中，P 在模幂中是上述处理定义的预先计算的值，以及 $R = 4^{n+2}$;

5） 将 m’ 载入该寄存器 B;

6） 使用载入寄存器 B 的值执行模平方运算，此处，将蒙哥马利模乘所需的乘数 A 从寄存器 B 中读出，该值是通过使用基数－4 记录电路获得的;

7） 向左移位该指数 e;

8） 忽略指数 e 的 MSB 1，在接下来的位之后执行后面的步骤 9)和 10);

9） 忽略指数 e 的一位（0 或 1）执行用于模平方运算的步骤 4）和 5），其中该平方运算所需的乘数和被乘数分别存储在寄存器 A 和寄存器 B 中;

10） 如果指数 e 的当前位是 1，在步骤 9）之后执行用于模乘的步骤 4）和 5），其中该被乘数是寄存器 B 中的内容，乘数是在求幂中的底数 m’; 以及

11） 在对指数 e 的所有位执行步骤 8）至 10）之后，再一次使用步骤 4）执行该模乘，其中被乘数是寄存器 B 的内容，乘数是 1。

在执行完上述的步骤 1）至 11）之后，对留在寄存器 C 和 S 内的值执行 CPA 运算所得的值是求幂 $m^e \bmod N$ 的最终值。

C-4. 本发明的效果

从上述说明可见，本发明提供一种用于计算 $A \cdot B \cdot 2^{-2(n+4)} \bmod N$ 的电路，依靠此电路可能计算一般的模乘 $A \cdot B \bmod N$。依照本发明计算的 $A \cdot B \bmod N$ 适用于硬件装置，该装置用于生成和验证数字签名的装置中。此外，本发明适用于基于 IC 卡的用于生成电子签名、验证身份以及加密/解密的硬件装置中。此外，本发明依靠执行模乘运算的电子签名装置，能提供用于加密

和解密数据或消息的装置。另外，本发明能够实现现有的基于电子签名装置的公开密钥密码系统，例如 NIST-DSS, RSA, ELGamal 以及 Schnorr 电子签名。

D. 本发明的应用实例

图 13 给出了一个 IC 卡的框图，通过使用本发明公开的蒙哥马利型模乘装置其能够执行加密和电子签名。

在图 13 中，一个中央处理单元（CPU）310 译出指令来执行加密、验证和电子签名，并为协同处理器 330 提供模运算所需的控制信号和数据。只读存储器（ROM）350 包括一个用于使数据安全的安全模块，例如，加密和电子签名所需的密钥。还给出了控制逻辑电路 320 和随机存取存储器（RAM）340，为执行上述操作提供逻辑电路和存储器。

虽然出于举例的目的给出了本发明的优选实施例，但本领域技术人员应理解，在没有脱离后附权利要求所公开的本发明的范围与精神的情况下，可能进行不同的修改、添加及删减。

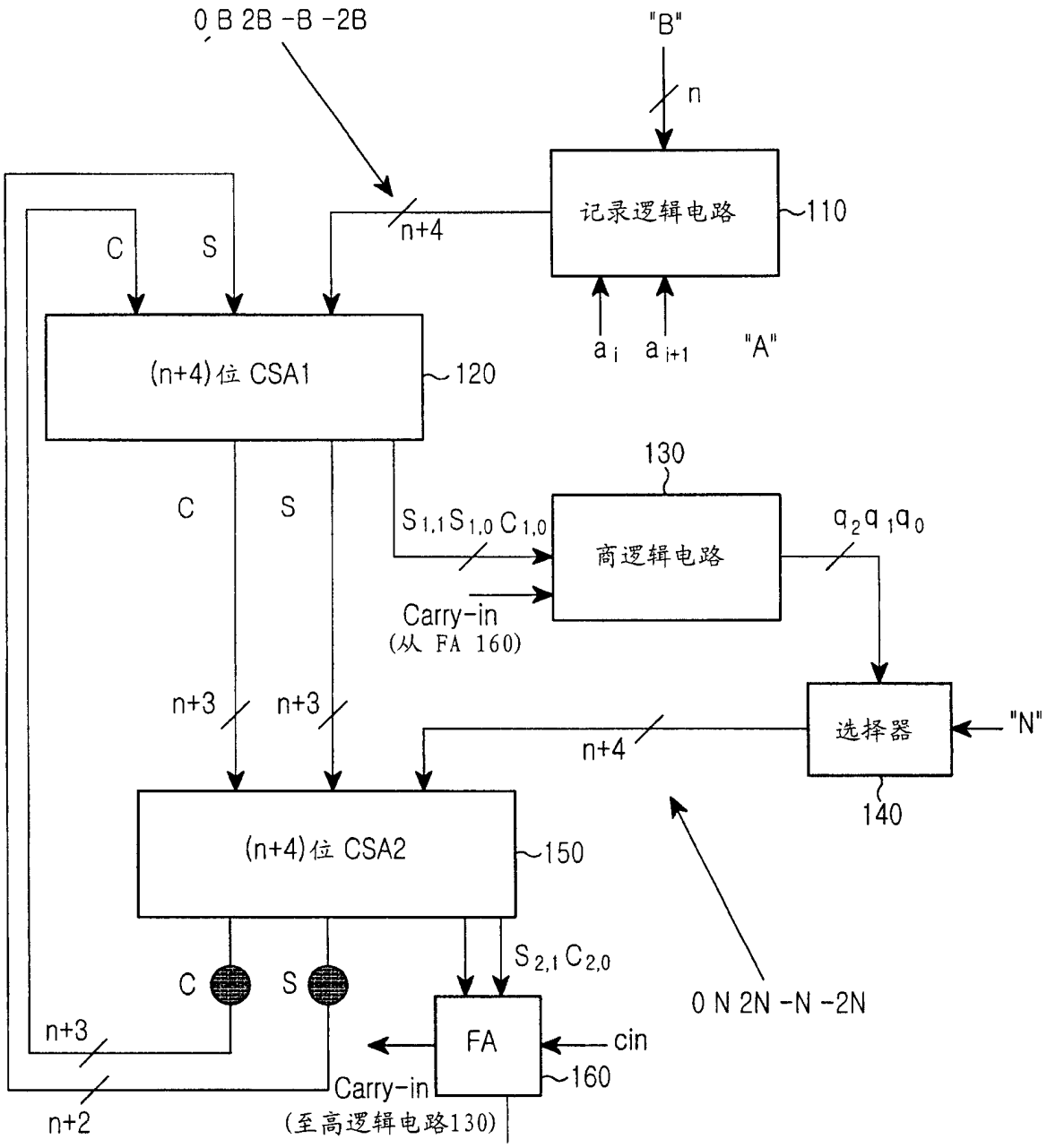

0 B 2B -B -2B
"B"
n
记录逻辑电路
110
n+4
C
S
(n+4)位 CSA1
120
a_i a_{i+1}
"A"
130
C
S
$S_{1,1}S_{1,0}C_{1,0}$
商逻辑电路
$q_2q_1q_0$
Carry-in
(从 FA 160)
n+3
n+3
选择器
"N"
n+4
140
(n+4)位 CSA2
150
$S_{2,1}C_{2,0}$
C
S
0 N 2N -N -2N
n+3
FA
cin
160
Carry-in
(至高逻辑电路130)
n+2

图 1

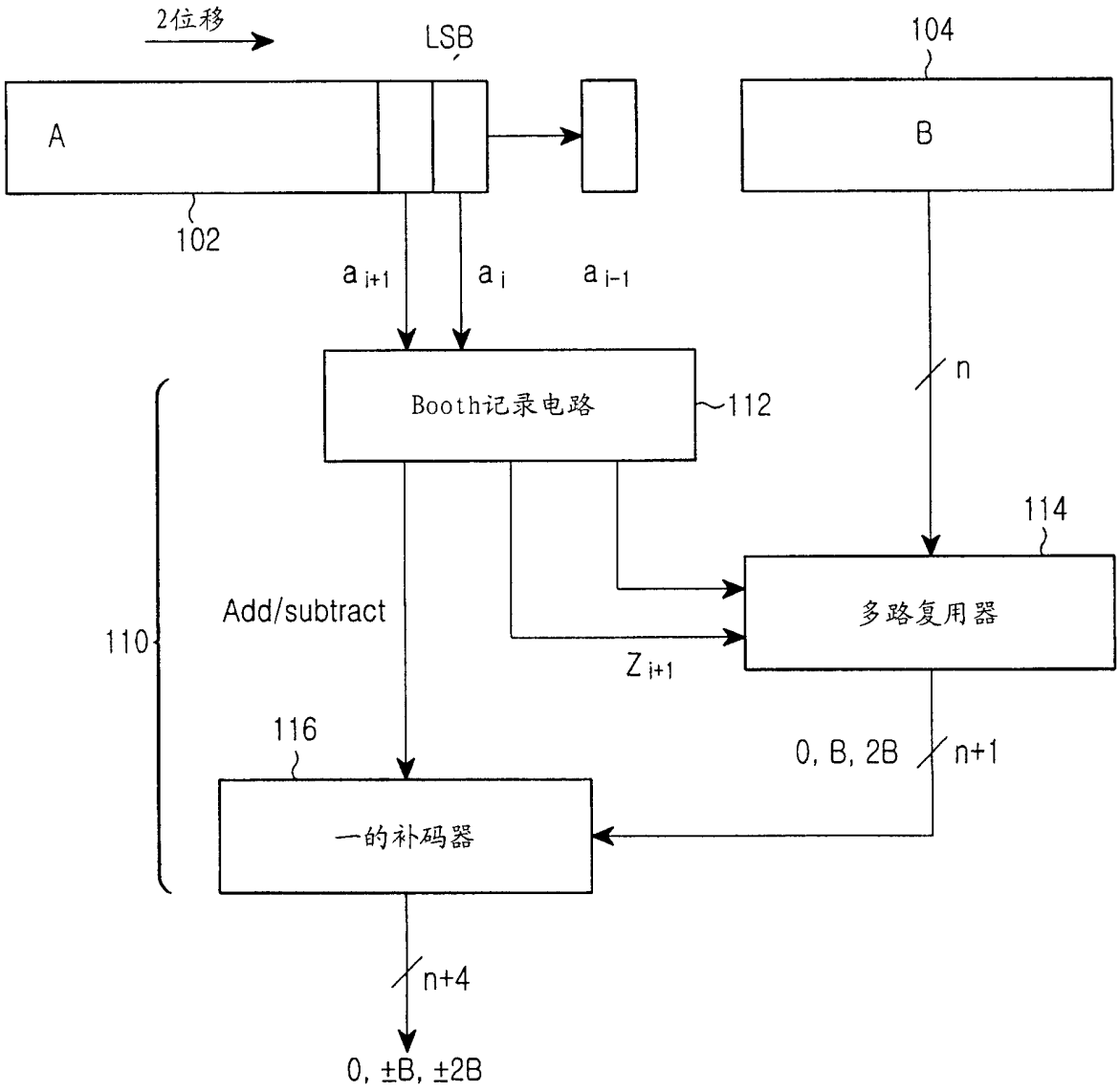

2位移
LSB
104
A
B
102
a_{i+1}
a_i
a_{i-1}
Booth记录电路
112
n
114
110
Add/subtract
多路复用器
Z_{i+1}
116
0, B, 2B
n+1
一的补码器
n+4
0, ±B, ±2B

图 2

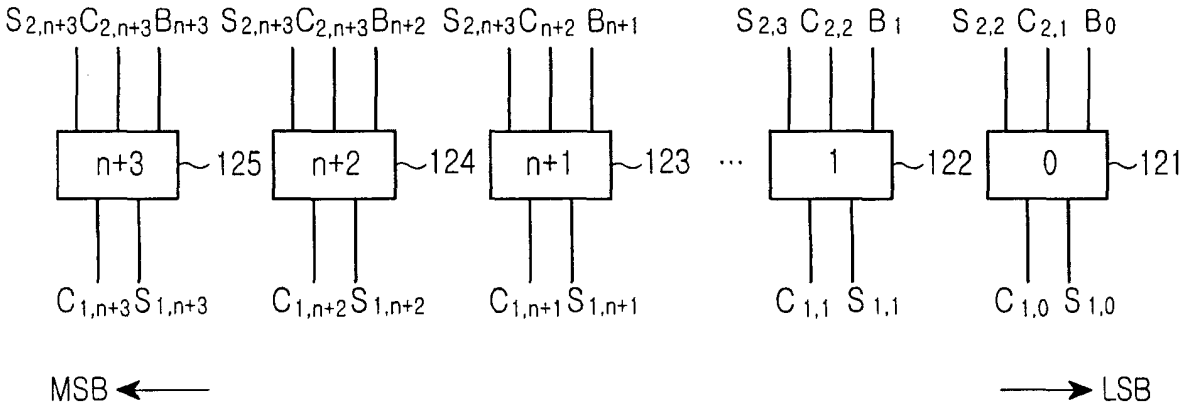

S2,n+3C2,n+3Bn+3
S2,n+3C2,n+3Bn+2
S2,n+3Cn+2 Bn+1
S2,3 C2,2 B1
S2,2 C2,1 B0
n+3
125
n+2
124
n+1
123
1
122
0
121
C1,n+3S1,n+3
C1,n+2S1,n+2
C1,n+1S1,n+1
C1,1 S1,1
C1,0 S1,0
MSB
LSB

图 3

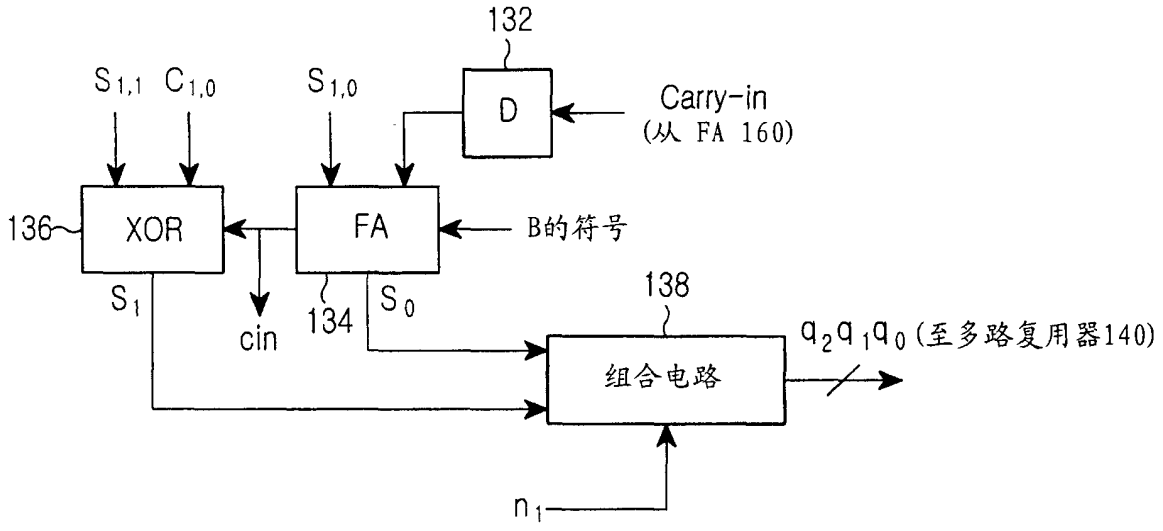

132
S1,1 C1,0
S1,0
D
Carry-in
(从 FA 160)
136
XOR
FA
B的符号
S1
cin
134
S0
138
q2q1q0 (至多路复用器140)
组合电路
n1

图 4

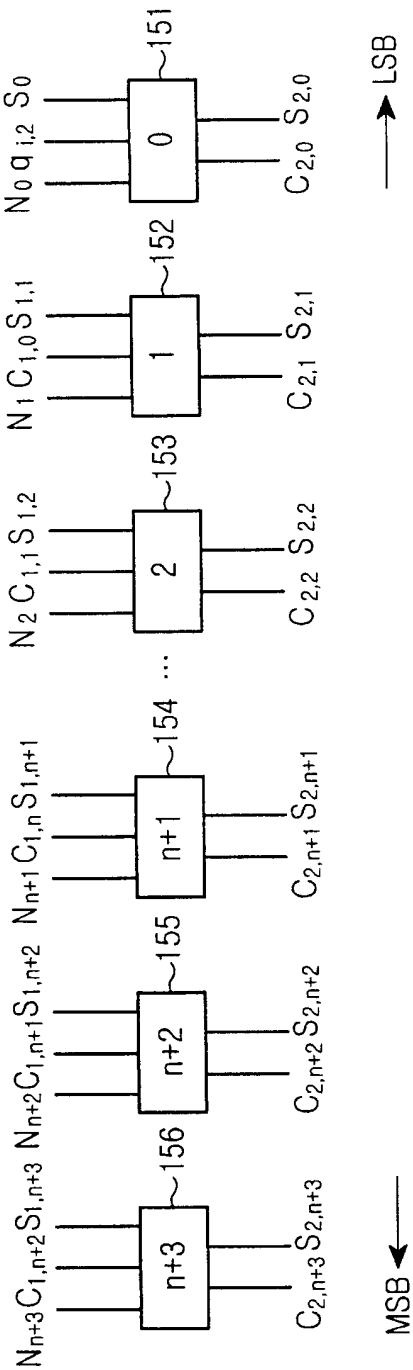


图 5

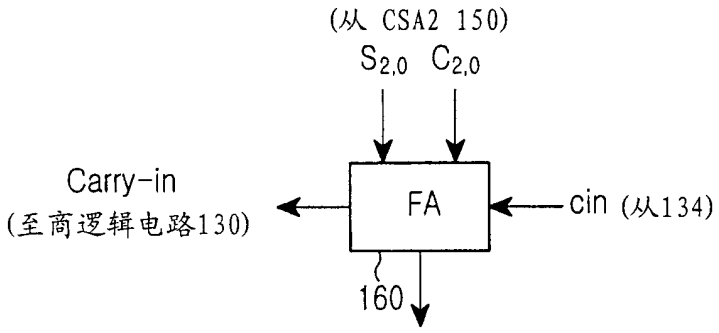


图 6

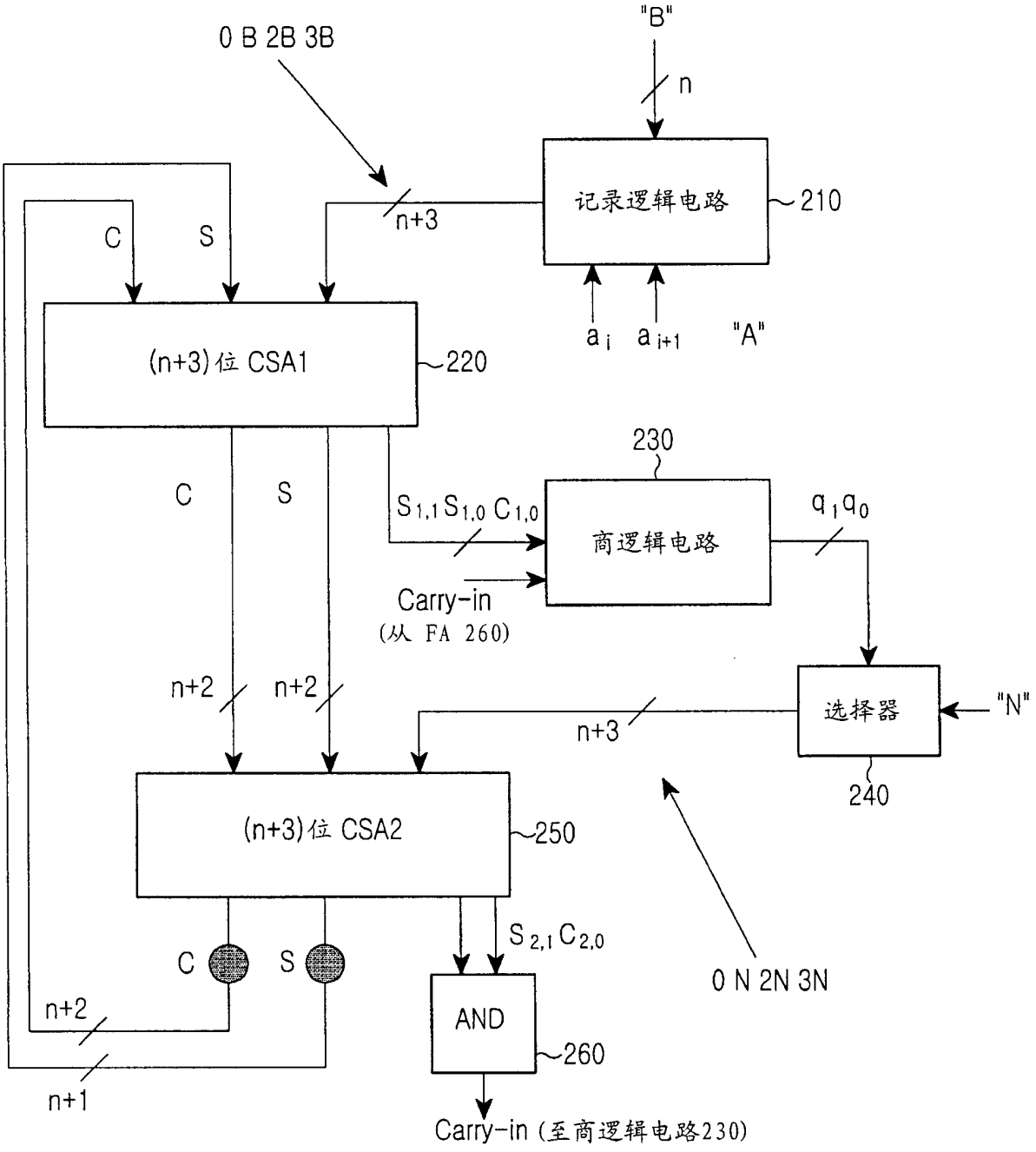

0 B 2B 3B
"B"
n
记录逻辑电路
210
n+3
C
S
(n+3)位 CSA1
220
a_i a_{i+1}
"A"
230
C
S
$S_{1,1}S_{1,0}C_{1,0}$
商逻辑电路
q_1q_0
Carry-in
(从 FA 260)
n+2
n+2
选择器
"N"
n+3
240
(n+3)位 CSA2
250
$S_{2,1}C_{2,0}$
C
S
0 N 2N 3N
n+2
AND
260
n+1
Carry-in (至商逻辑电路230)

图 7

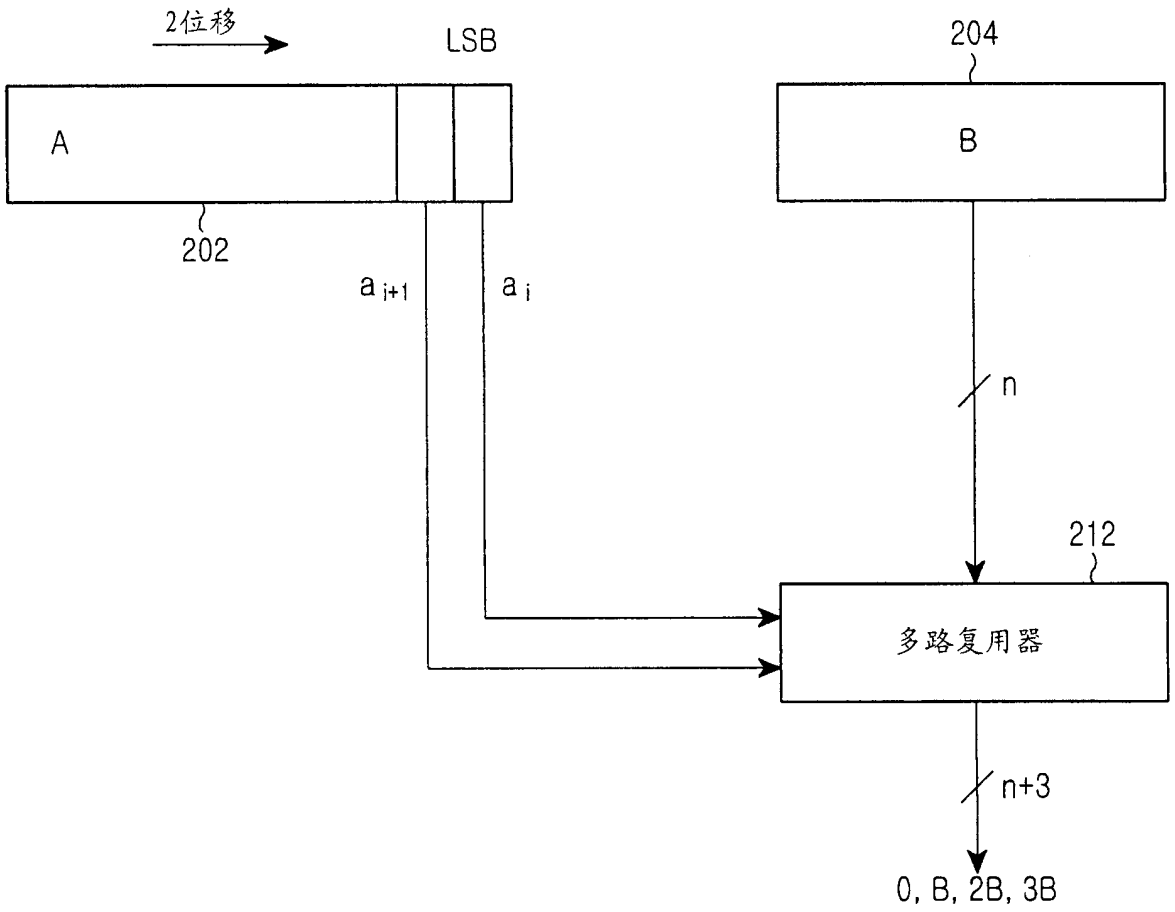


图 8

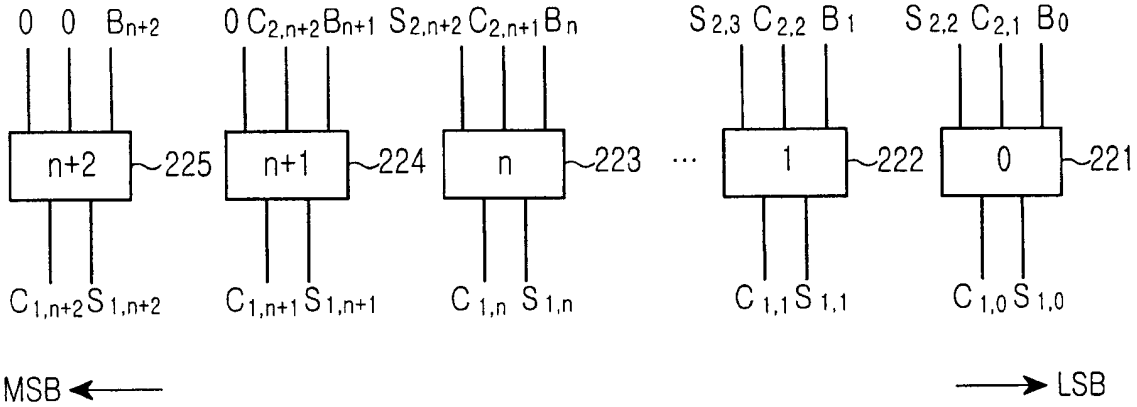

0 0 Bn+2
0 C2,n+2 Bn+1
S2,n+2 C2,n+1 Bn
S2,3 C2,2 B1
S2,2 C2,1 B0
n+2
225
n+1
224
n
223
1
222
0
221
C1,n+2 S1,n+2
C1,n+1 S1,n+1
C1,n S1,n
C1,1 S1,1
C1,0 S1,0
MSB
LSB

图 9

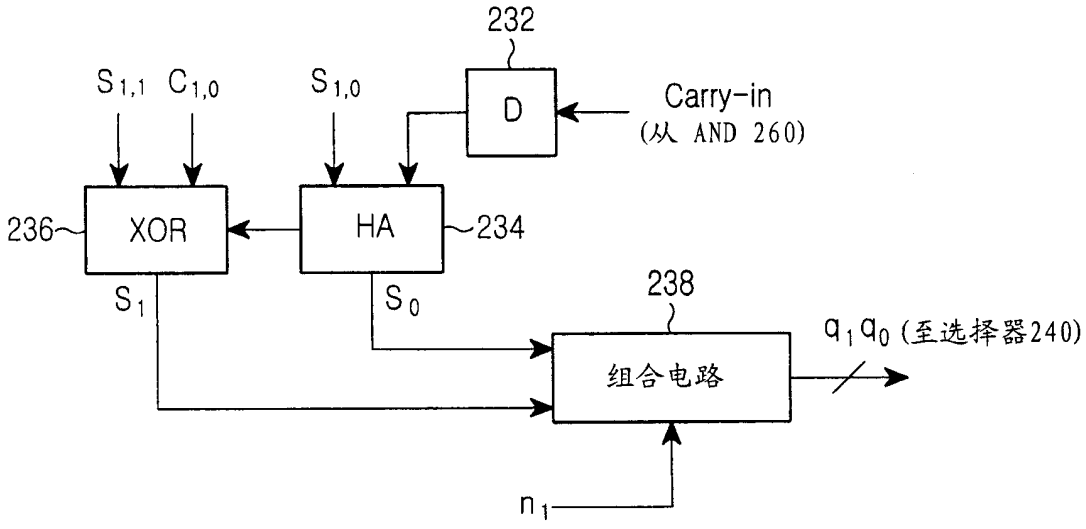

232
S1,1 C1,0
S1,0
D
Carry-in
(从 AND 260)
236
XOR
HA
234
S1
S0
238
q1 q0 (至选择器240)
组合电路
n1

图 10

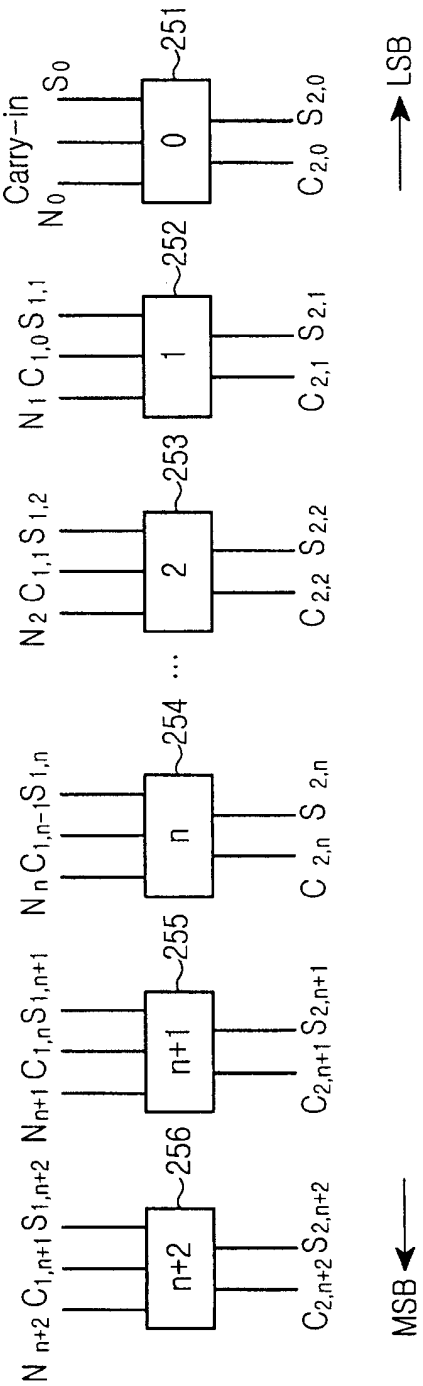

Carry-in
N0
S0
251
0
C2,0 S2,0
LSB
N1 C1,0 S1,1
252
1
C2,1 S2,1
N2 C1,1 S1,2
253
2
C2,2 S2,2
...
Nn C1,n-1 S1,n
254
n
C 2,n S 2,n
Nn+1 C1,n S1,n+1
255
n+1
C2,n+1 S2,n+1
N n+2 C1,n+1 S1,n+2
256
n+2
C2,n+2 S2,n+2
MSB

图 11

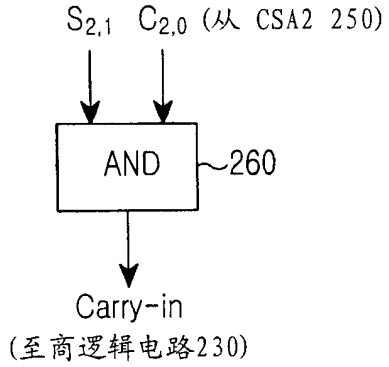

$S_{2,1}$ $C_{2,0}$ (从 CSA2 250)
AND
260
Carry-in
(至商逻辑电路230)

图 12

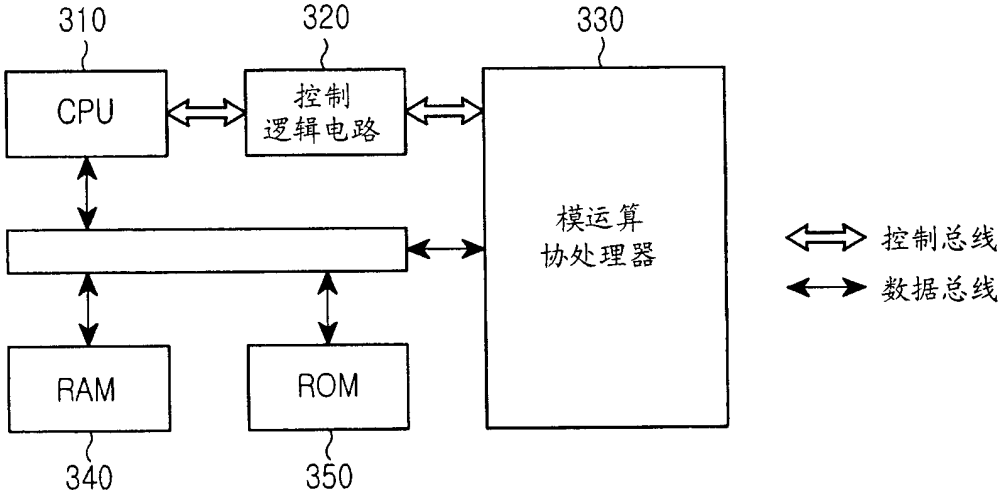

310
320
330
CPU
控制
逻辑电路
模运算
协处理器
控制总线
数据总线
RAM
ROM
340
350

图 13