(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110299991 A
(43)申请公布日 2019.10.01

(21)申请号 201910448838.X

(22)申请日 2019.05.27

(71)申请人 广东技术师范大学
地址 510665 广东省广州市天河区中山大道西293号

(72)发明人 李伟键 鹿福祥 黄娴 刘溪 李艳华

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 麦小婵 郝传鑫

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/00(2006.01)

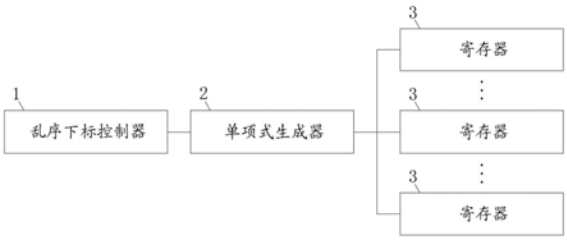
权利要求书2页 说明书6页 附图2页

(54)发明名称

抗侧信道攻击的QUAD流密码生成装置

(57)摘要

本申请公开了一种抗侧信道攻击的QUAD流密码生成装置，包括乱序下标控制器、单项式生成器和多个寄存器。乱序下标控制器用于通过乱序生成单项式下标值的方式来生成多个单项式下标值；单项式生成器用于按照单项式下标值的生成顺序，依次计算多个单项式；每个寄存器分别用于，获取属于同一所述多变量二次方程的多个单项式并依次累加，生成QUAD流密码。本申请通过打乱各个单项式的计算顺序，并对多个单项式进行累加，生成QUAD流密码，使带有该抗侧信道攻击的QUAD流密码生成装置的电子设备产生的具有相同密钥信息的侧信道信息出现在不同时刻，从而减少了寄存器存储操作的功耗曲线与密钥信息的相关性，使QUAD流密码的安全性更高，进而有效抵御侧信道攻击。



CN 110299991 A

1.一种抗侧信道攻击的QUAD流密码生成装置,其特征在于,包括:

乱序下标控制器,用于提取包括n个变量r个多变量二次方程的多变量二次方程组,并根据所述n个变量,生成大小为L的滑动窗口,根据所述滑动窗口的循环跳动,乱序生成多个单项式下标值(i,j,k)并输出;其中,1≤i≤j≤n,1≤k≤r,L=n或L=n+1,r为偶数;

单项式生成器,用于根据每个所述单项式下标值(i,j,k)的生成顺序,依次获取所述多变量二次方程组的多个单项式$\alpha_{ij}^{k}x_{i}x_{j}$;其中,$\alpha_{ij}^{k}$为明文,$x_i$为密钥,或,$\alpha_{ij}^{k}$为密钥,$x_i$为明文;

多个寄存器,每个所述寄存器分别用于,获取属于同一所述多变量二次方程的多个单项式$\alpha_{ij}^{k}x_{i}x_{j}$并依次累加,生成QUAD流密码;其中,所述多变量二次方程与所述寄存器一一对应。

2.根据权利要求1所述的抗侧信道攻击的QUAD流密码生成装置,其特征在于,所述乱序下标控制器用于根据所述滑动窗口的循环跳动,乱序生成多个单项式下标值(i,j,k),具体包括:

步骤S11、根据所述n个变量,初始化所述滑动窗口大小L,基于所述滑动窗口大小,将各单项式下标分成多个窗口;其中,若n为偶数,则长度L=n,各单项式下标分成r×(n+1)/2个窗口;若n为奇数,则长度L=n+1,各单项式下标分成r×n/2个窗口;

步骤S12、将窗口的窗口编号预设为w=1,窗口的内部迭代编号预设为l=1,随机生成初始值L_s后,随机生成单项式下标初始值$i=i_s$,$j=j_s$,$k=k_s$,并将j赋值为$j+L_s-1$,执行步骤S13;

步骤S13、判断赋值后的j是否大于n;若是,则执行步骤S14;否则,执行步骤S17;

步骤S14、将i赋值为i+1,判断赋值后的i是否大于n;若是,则执行步骤S15;否则,执行步骤S16;

步骤S15、将i赋值为i%n,判断k是否小于r;若是,将k赋值为k+1,执行步骤S16;否则,将k赋值为1,执行步骤S16;

步骤S16、将j赋值为j-(n-i+1),执行步骤S13;

步骤S17、生成一个单项式下标值,判断l是否大于L;若是,则所述多变量二次方程中单项式下标值生成完毕;否则,在w小于窗口个数时,将w赋值为w+1,将j赋值为j+L后,执行步骤S13;其中,$1\leq L_s\leq L/2$,$1\leq i_s\leq j_s\leq n$,$1\leq k_s\leq r$。

3.根据权利要求2所述的抗侧信道攻击的QUAD流密码生成装置,其特征在于,所述乱序下标控制器用于根据所述滑动窗口的循环跳动,乱序生成多个单项式下标值(i,j,k),还包括:

当所述步骤S17中的w大于等于窗口个数时,执行步骤S18;

步骤S18、将w赋值为1,将l赋值为l+1,判断赋值后的l是否为奇数;若是,则执行步骤S19;否则,将j赋值为j+L+L/2后,执行步骤S13;

步骤S19、判断L_s是否小于L/2;若是,则将j赋值为j+L/2+1,将L_s赋值为L_s+1后,执行步骤S13;否则,将j赋值为j+1,将L_s赋值为1后,执行步骤S13。

4.根据权利要求1所述的抗侧信道攻击的QUAD流密码生成装置,其特征在于,多个所述寄存器分别用于:

根据所述单项式下标值(i,j,k)的生成顺序,实时获取属于同一所述二次方程的多个

单项式$\alpha_{ij}^{k}x_{i}x_{j}$并依次累加，生成QUAD流密码。

5.根据权利要求1所述的抗侧信道攻击的QUAD流密码生成装置，其特征在于，每个所述多变量二次方程相应的流密码为：

$$Q(x)=\sum_{j_s\le j\le n}\alpha_{i_s j}x_{i_s}x_j+\sum_{i_s<i\le j\le n}\alpha_{ij}x_i x_j+\sum_{\substack{1\le i\le i_s,\\ i\le j\le n}}\alpha_{ij}x_i x_j+\sum_{i_s\le j<j_s}\alpha_{i_s j}x_{i_s}x_j\ 。$$

抗侧信道攻击的QUAD流密码生成装置

技术领域

[0001] 本申请涉及信息安全技术领域，尤其涉及一种抗侧信道攻击的QUAD流密码生成装置。

背景技术

[0002] QUAD是一组基于有限域上多变量二次方程组构造的可证明安全的流密码。多变量二次方程可以表示如下：

[0003] $Q(x)=\sum_{1\leqslant i\leqslant j\leqslant n}\alpha_{ij}x_ix_j+\sum_{1\leqslant i\leqslant n}\beta_{ij}x_i+\gamma$

[0004] 侧信道攻击(side channel attack简称SCA)，又称旁路攻击，是一种针对加密电子设备在运行过程中的时间消耗、功率消耗或电磁辐射之类的侧信道信息泄露而对加密设备进行攻击的方法。这种攻击方法给密码设备带来了严重的威胁。

[0005] 传统应对侧信道攻击的方法，通常在加密时直接按照相同顺序对多个多变量二次方程中的每一个单项式进行计算，再把每个单项式的计算结果累加后暂存于寄存器，生成QUAD流密码，进而抵御侧信道攻击。但若攻击者通过对每个多变量二次方程相应寄存器存储操作的功耗进行分析，即可获得密钥信息(xj的信息)，进而攻破密码算法。

[0006] 为解决上述问题，现有技术中，采用在加密时直接按照相同顺序对多个多变量二次方程中的每一个单项式进行计算，再把每个单项式的计算结果累加后暂存于寄存器从而构建QUAD流密码的方式，来抵御侧信道攻击。但在采用现有技术进行侧信道攻击抵御时发现，在选定了开始的单项式编号之后，各个多项式之间的计算仍然是固定且顺序的，攻击者通过穷举初始下标的方式，仍有可能对齐多项式计算从而获得密钥信息，进而威胁密码算法的安全性。

发明内容

[0007] 本申请实施例所要解决的技术问题在于，提供一种抗侧信道攻击的QUAD流密码生成装置，生成安全性更高的QUAD流密码，从而有效抵御侧信道攻击。

[0008] 为解决上述问题，本申请实施例提供一种抗侧信道攻击的QUAD流密码生成装置，包括：

[0009] 乱序下标控制器，用于提取包括n个变量r个多变量二次方程的多变量二次方程组，并根据所述n个变量，生成大小为L的滑动窗口，根据所述滑动窗口的循环跳动，乱序生成多个单项式下标值(i,j,k)并输出；其中，$1\leqslant i\leqslant j\leqslant n$，$1\leqslant k\leqslant r$，L＝n或L＝n+1，r为偶数；

[0010] 单项式生成器，用于根据每个所述单项式下标值(i,j,k)的生成顺序，依次获取所述多变量二次方程组的多个单项式$\alpha_{ij}^{k}x_ix_j$；其中，α_{ij}^{k}为明文，x_i为密钥，或，α_{ij}^{k}为密钥，x_i为明文；

[0011] 多个寄存器，每个所述寄存器分别用于，获取属于同一所述多变量二次方程的多个单项式$\alpha_{ij}^{k}x_ix_j$并依次累加，生成QUAD流密码；其中，所述多变量二次方程与所述寄存器一

一对应。

[0012] 进一步的，所述乱序下标控制器用于根据所述滑动窗口的循环跳动，乱序生成多个单项式下标值(i,j,k)，具体包括：

[0013] 步骤S11、根据所述n个变量，初始化所述滑动窗口大小L，基于所述滑动窗口大小，将各单项式下标分成多个窗口；其中，若n为偶数，则长度L＝n，各单项式下标分成r×(n+1)/2个窗口；若n为奇数，则长度L＝n+1，各单项式下标分成r×n/2个窗口；

[0014] 步骤S12、将窗口的窗口编号预设为w＝1，窗口的内部迭代编号预设为l＝1，随机生成初始值L_s后，随机生成单项式下标初始值i＝i_s，j＝j_s，k＝k_s，并将j赋值为j+L_s-1，执行步骤S13；

[0015] 步骤S13、判断赋值后的j是否大于n；若是，则执行步骤S14；否则，执行步骤S17；

[0016] 步骤S14、将i赋值为i+1，判断赋值后的i是否大于n；若是，则执行步骤S15；否则，执行步骤S16；

[0017] 步骤S15、将i赋值为i％n，判断k是否小于r；若是，将k赋值为k+1，执行步骤S16；否则，将k赋值为1，执行步骤S16；

[0018] 步骤S16、将j赋值为j-(n-i+1)，执行步骤S13；

[0019] 步骤S17、生成一个单项式下标值，判断l是否大于L；若是，则所述多变量二次方程中单项式下标值生成完毕；否则，在w小于窗口个数时，将w赋值为w+1，将j赋值为j+L后，执行步骤S13；其中，1≤L_s≤L/2，1≤i_s≤j_s≤n，1≤k_s≤r。

[0020] 进一步的，所述乱序下标控制器用于根据所述滑动窗口的循环跳动，乱序生成多个单项式下标值(i,j,k)，还包括：

[0021] 当所述步骤S17中的w大于等于窗口个数时，执行步骤S18；

[0022] 步骤S18、将w赋值为1，将l赋值为l+1，判断赋值后的l是否为奇数；若是，则执行步骤S19；否则，将j赋值为j+L+L/2后，执行步骤S13；

[0023] 步骤S19、判断L_s是否小于L/2；若是，则将j赋值为j+L/2+1，将L_s赋值为L_s+1后，执行步骤S13；否则，将j赋值为j+1，将L_s赋值为1后，执行步骤S13。

[0024] 进一步的，多个所述寄存器分别用于：

[0025] 根据所述单项式下标值(i,j,k)的生成顺序，实时获取属于同一所述二次方程的多个单项式$\alpha_{ij}^{k}x_ix_j$并依次累加，生成QUAD流密码。

[0026] 进一步的，每个所述多变量二次方程相应的流密码为：

[0027] $$Q(x)=\sum_{j_s\le j\le n}\alpha_{i_sj}x_{i_s}x_j+\sum_{i_s<i\le j\le n}\alpha_{ij}x_ix_j+\sum_{\substack{1\le i\le i_s,\\ i\le j\le n}}\alpha_{ij}x_ix_j+\sum_{i_s\le j<j_s}\alpha_{i_sj}x_{i_s}x_j$$。

[0028] 实施本申请实施例，具有如下有益效果：

[0029] 本申请实施例提供的一种抗侧信道攻击的QUAD流密码生成装置，包括乱序下标控制器、单项式生成器和多个寄存器。乱序下标控制器用于通过乱序生成单项式下标值的方式来生成多个单项式下标值；单项式生成器用于按照单项式下标值的生成顺序，依次计算多个单项式；每个寄存器分别用于，获取属于同一所述多变量二次方程的多个单项式并依次累加，生成QUAD流密码。本申请通过打乱各个单项式的计算顺序，并对多个单项式进行累加，生成QUAD流密码，使带有该抗侧信道攻击的QUAD流密码生成装置的电子设备产生的具

有相同密钥信息的侧信道信息出现在不同时刻,从而减少了寄存器存储操作的功耗曲线与密钥信息的相关性,使QUAD流密码的安全性更高,进而有效抵御侧信道攻击。

附图说明

[0030] 图1是本申请的一个实施例提供的抗侧信道攻击的QUAD流密码生成装置的结构示意图;

[0031] 图2是乱序下标控制器乱序生成多个单项式下标值的一个流程示意图;

[0032] 图3是乱序下标控制器乱序生成多个单项式下标值的又一个流程示意图;

[0033] 图4是本申请的再一个实施例提供的抗侧信道攻击的QUAD流密码生成装置的结构示意图。

具体实施方式

[0034] 下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0035] 参见图1,是本申请的一个实施例提供的抗侧信道攻击的QUAD流密码生成装置的结构示意图。包括:

[0036] 乱序下标控制器1,用于提取包括n个变量r个多变量二次方程的多变量二次方程组,并根据n个变量,生成大小为L的滑动窗口,根据滑动窗口的循环跳动,乱序生成多个单项式下标值(i,j,k)并输出。

[0037] 其中,1≤i≤j≤n,1≤k≤r,L=n或L=n+1,r为偶数。

[0038] 优选的,乱序生成的单项式下标值(i,j,k)的个数设定为rn(n+1)/2个。

[0039] 在本实施例中,乱序下标控制器1生成每个单项式下标值(i,j,k)后,根据生成的下标值输出变量x_i、x_i以及系数α_{ij}^k,供后续组成单项式。

[0040] 单项式生成器2,用于根据每个单项式下标值(i,j,k)的生成顺序,依次获取多变量二次方程组的多个单项式$\alpha_{ij}^k x_i x_j$。

[0041] 其中,α_{ij}^k为明文,x_i为密钥,或,α_{ij}^k为密钥,x_i为明文。

[0042] 在本实施例中,单项式生成器2将乱序下标控制器1输出的变量x_i、x_i以及系数α_{ij}^k相乘后输出,从而获得单项式$\alpha_{ij}^k x_i x_j$。

[0043] 优选的,多变量二次方程组的单项式个数设定为r×n(n+1)/2个。

[0044] 多个寄存器3,每个寄存器3分别用于,获取属于同一多变量二次方程的多个单项式$\alpha_{ij}^k x_i x_j$并依次累加,生成QUAD流密码。

[0045] 其中,多变量二次方程与寄存器3一一对应。

[0046] 在本实施例中,每个多变量二次方程相应的流密码为:

[0047] $$Q(x)=\sum_{j_s\le j\le n}\alpha_{i_s j}x_{i_s}x_j+\sum_{i_s<i\le j\le n}\alpha_{ij}x_i x_j+\sum_{\substack{1\le i\le i_s,\\ i\le j\le n}}\alpha_{ij}x_i x_j+\sum_{i_s\le j<j_s}\alpha_{i_s j}x_{i_s}x_j$$。

[0048] 其中，多变量二次方程随机生成不同的单项式下标初始值(i_s,j_s,k_s)，然后按照上述公式进行计算，从而获得每个多变量二次方程相应的流密码。

[0049] 需要说明的是，在有限域上计算具有r个方程的多变量二次方程组

$$\begin{cases} Q_1(x)=\sum_{1\le i\le j\le n} a_{ij}^1 x_i x_j+\gamma^1 \\ \cdots\cdots \\ Q_r(x)=\sum_{1\le i\le j\le n} a_{ij}^r x_i x_j+\gamma^r \end{cases}$$

来实现对密钥、明文的加密。其中，若α_{ij}^k为明文，则x_i为密钥；若α_{ij}^k为密钥，则x_i为明文。在本实施例中，在计算多变量二次方程组中的每个多变量二次方程时，随机打乱每个多变量二次方程中的各个单项式$\alpha_{ij}^k x_i x_j$的计算顺序，使不同多变量二次方程中的单项式$\alpha_{ij}^k x_i x_j$的计算顺序各不相同。

[0050] 在计算多变量二次方程组时，乱序下标控制器1乱序生成r×n(n+1)/2个单项式下标值(i,j,k)，即将多变量二次方程的单项式下标值重新进行排序，使每个多变量二次方程的单项式下标值的顺序各不相同。其中，r×n(n+1)/2个单项式下标值(i,j,k)涵盖多变量二次方程组中的所有单项式下标值。按照多变量二次方程组各自的单项式下标值生成顺序，计算各个单项式$\alpha_{ij}^k x_i x_j$。在每计算一个单项式时，将该单项式累加到寄存器中，在累加完所有单项式后，即可获得该多变量二次方程相应的流密码。多变量二次方程组中的r个方程的计算结果分别相应存储到r个寄存器中。

[0051] 每个多变量二次方程中具有n×(n+1)/2项单项式，单项式计算顺序打乱后，攻击者若想通过对r个寄存器的功耗分析来获取密钥或明文信息，则需要考虑n/2×A(n(n+1)/2,n(n+1)/2)＝n/2×(n(n+1)/2)!种可能性来进行分析，从而难以实现对侧信道的攻击。

[0052] 需要说明的是，本发明实施例提供的抗侧信道攻击的QUAD流密码生成装置一般应用在ASIC集成芯片或智能卡中，密钥通过多变量二次方程的算法进行加密后存储到ASIC集成芯片或智能卡的存储器中。其中，每个多变量二次方程中各个单项式计算顺序均不相同，累加到存储器中的顺序也不相同，从而防止攻击者通过对存储器进行功耗分析而获取密钥信息。

[0053] 进一步的，参见图2，是乱序下标控制器乱序生成多个单项式下标值的一个流程示意图。在本实施例中，乱序下标控制器1乱序生成多个单项式下标值具体包括：

[0054] 步骤S11、根据n个变量，初始化滑动窗口大小L，基于滑动窗口大小，将各单项式下标分成多个窗口。

[0055] 其中，若n为偶数，则长度L＝n，各单项式下标分成r×(n+1)/2个窗口；若n为奇数，则长度L＝n+1，各单项式下标分成r×n/2个窗口。

[0056] 步骤S12、将窗口的窗口编号预设为w＝1，窗口的内部迭代编号预设为l＝1，随机生成初始值L_s后，随机生成单项式下标初始值i＝i_s，j＝j_s，k＝k_s，并将j赋值为j+L_s-1，执行步骤S13。

[0057] 步骤S13、判断赋值后的j是否大于n;若是,则执行步骤S14;否则,执行步骤S17。

[0058] 步骤S14、将i赋值为i+1,判断赋值后的i是否大于n;若是,则执行步骤S15;否则,执行步骤S16。

[0059] 步骤S15、将i赋值为i%n,判断k是否小于r;若是,将k赋值为k+1,执行步骤S16;否则,将k赋值为1,执行步骤S16。

[0060] 步骤S16、将j赋值为j-(n-i+1),执行步骤S13。

[0061] 步骤S17、生成一个单项式下标值,判断l是否大于L;若是,则所述多变量二次方程中单项式下标值生成完毕;否则,在w小于窗口个数时,将w赋值为w+1,将j赋值为j+L后,执行步骤S13。

[0062] 其中,$1\leqslant L_s\leqslant L/2$,$1\leqslant i_s\leqslant j_s\leqslant n$,$1\leqslant k_s\leqslant r$。

[0063] 进一步的,参见图3,是乱序下标控制器乱序生成多个单项式下标值的又一个流程示意图。在本实施例中,除图2所示步骤外,还包括:

[0064] 步骤S17、在w大于等于窗口个数时,执行步骤S18。

[0065] 步骤S18、将w赋值为1,将l赋值为l+1,判断赋值后的l是否为奇数;若是,则执行步骤S19;否则,将j赋值为j+L+L/2后,执行步骤S13。

[0066] 步骤S19、判断L_s是否小于L/2;若是,则将j赋值为j+L/2+1,将L_s赋值为L_s+1后,执行步骤S13;否则,将j赋值为j+1,将L_s赋值为1后,执行步骤S13。

[0067] 需要说明的是,将多变量二次方程组中的所有单项式完全打乱来抗侧信道攻击的效果最佳。同时,为了减少计算时间和存储开销,避免耗费大量的资源,采用仅打乱每个多变量二次方程中的初始计算顺序并且根据滑动窗口循环跳动,使每个多变量二次方程从不同的初始单项式开始计算,之后循环跳动计算即可。例如,需计算r个多项式方程组,单项式下标生成器2给随机生成单项式初始下标值(5,5,1),随机生成初始值$L_s=2$,则从第一个多变量二次方程的$a^2_{l1}x_1x_1$开始按步骤计算r个多变量二次方程的所有单项式等。这种抗侧信道攻击的QUAD流密码生成装置使得密钥、明文的在不同多变量二次方程中的相同操作隐藏在不同的时钟周期内,无法通过存储器的功耗曲线特征而观察得到,而且简单高效,有利于软硬件高效实现。

[0068] 进一步的,参见图4,是本申请的再一个实施例提供的抗侧信道攻击的QUAD流密码生成装置的流程示意图。

[0069] 包括乱序下标控制器31、多项式变量寄存器32、乘法器33、乘法器34、加法器35、寄存器36和判断器37。其中,多项式变量寄存器32中存储的值可以为密钥,也可以为明文。本发明实施例提供的抗侧信道攻击的QUAD流密码生成装置用于实现多变量二次方程组的加密,其中,多变量二次方程组具有r个多变量二次方程。在计算多变量二次方程时,乱序下标控制器31随机生成单项式下标值i、j和k,其中,随机生成的初始的单项式下标值为i_s、j_s和k_s。多项式变量寄存器32根据乱序下标控制器31生成的单项式下标值,输出变量x_i和x_j。乘法器33接收变量x_i和x_j并将其相乘后输出,乘法器34将乘法器33输出的值与系数α_{ij}相乘后输出,获得单项式,再将单项式通过加法器35累加到寄存器36中。判断器37在寄存器36中累加了下标为(i,j,k)的单项式后判断窗口内部迭代编号是否大于滑动窗口大小,若否,则判定为0,将寄存器36中的值与下一个单项式累加后存储到寄存器36中;若是,则判定为1,输出寄存器36中的值,即为密文。

[0070] 本申请实施例提供一种抗侧信道攻击的QUAD流密码生成装置，包括乱序下标控制器、单项式生成器和多个寄存器。乱序下标控制器用于通过乱序生成单项式下标值的方式来生成r×n(n+1)/2个单项式下标值(i,j,k)；单项式生成器用于按照单项式下标值(i,j,k)的生成顺序，依次计算r×n(n+1)/2个单项式$a^k_{ij}x_ix_j$，使不同多变量二次方程中单项式的计算顺序各不相同；每个寄存器分别用于，获取属于同一所述多变量二次方程的多个单项式$\alpha_{ij}^k x_i x_j$并依次累加，生成QUAD流密码。本申请通过打乱各个单项式的计算顺序，并对多个单项式进行累加，生成QUAD流密码，使带有该抗侧信道攻击的QUAD流密码生成装置的电子设备产生的具有相同密钥信息的侧信道信息出现在不同时刻，从而减少了寄存器存储操作的功耗曲线与密钥信息的相关性，使QUAD流密码的安全性更高，进而有效抵御侧信道攻击。

[0071] 以上所述是本申请的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本申请原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也视为本申请的保护范围。

[0072] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)或随机存储记忆体(Random Access Memory，RAM)等。

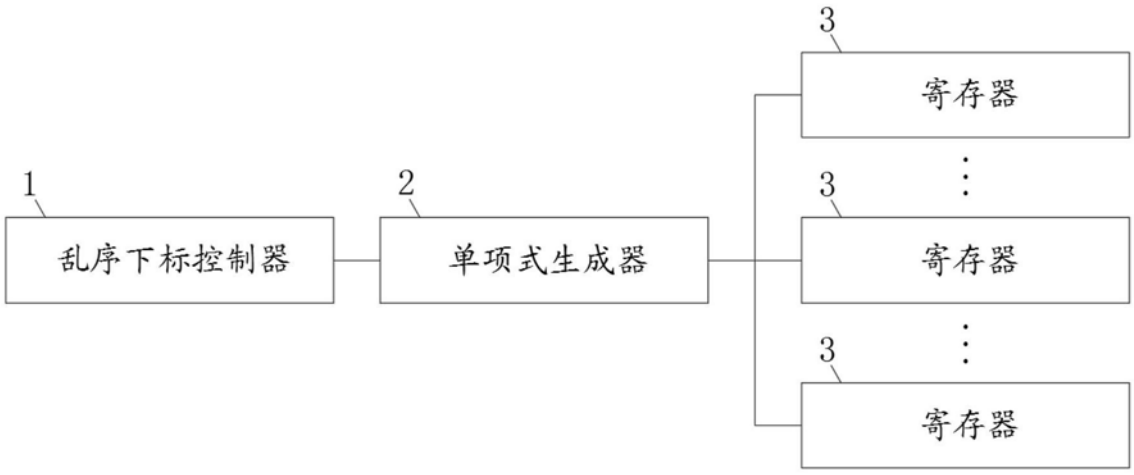

1
乱序下标控制器
2
单项式生成器
3
寄存器
3
寄存器
3
寄存器

图1

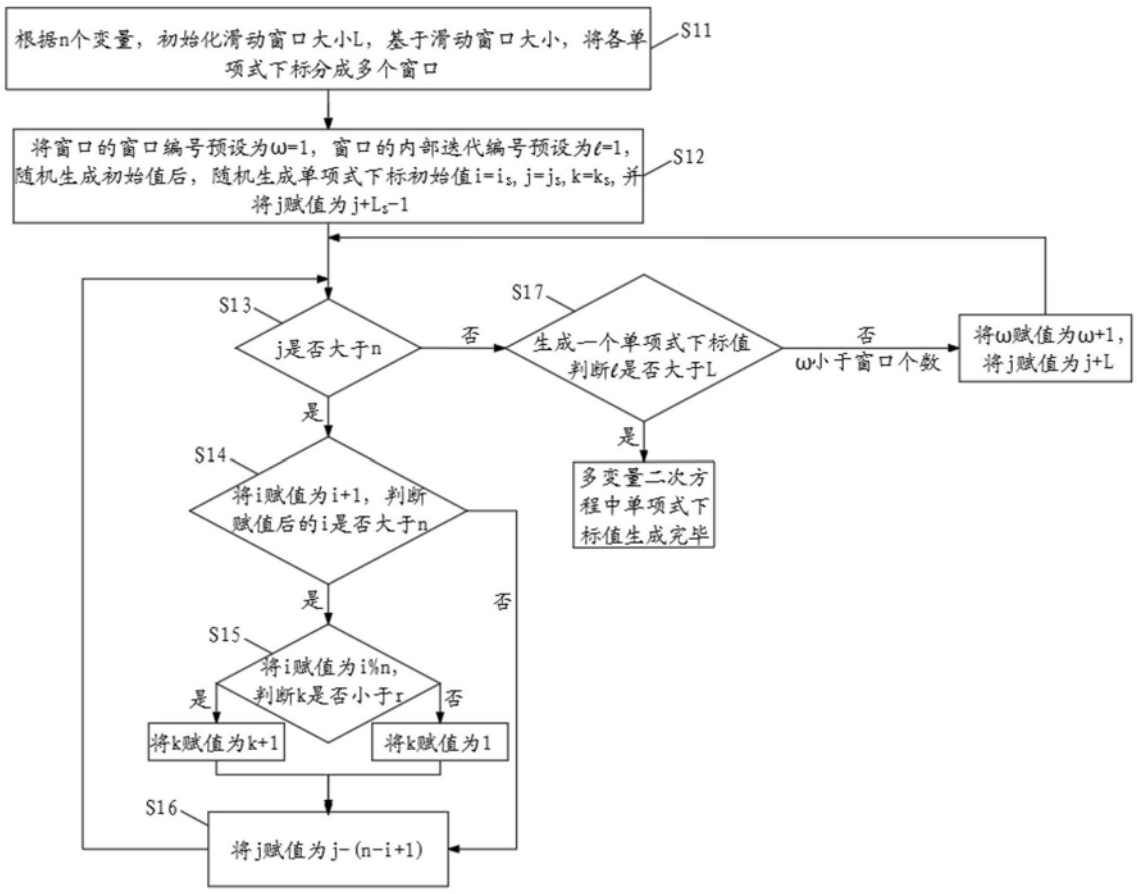

根据n个变量，初始化滑动窗口大小L，基于滑动窗口大小，将各单项式下标分成多个窗口
S11
将窗口的窗口编号预设为ω=1，窗口的内部迭代编号预设为ℓ=1，随机生成初始值后，随机生成单项式下标初始值i=is, j=js, k=ks, 并将j赋值为j+Ls-1
S12
S13
j是否大于n
否
是
S17
生成一个单项式下标值
判断ℓ是否大于L
否
ω小于窗口个数
将ω赋值为ω+1，将j赋值为j+L
是
多变量二次方程中单项式下标值生成完毕
S14
将i赋值为i+1，判断赋值后的i是否大于n
是
否
S15
将i赋值为i%n，判断k是否小于r
是
否
将k赋值为k+1
将k赋值为1
S16
将j赋值为j-(n-i+1)

图2

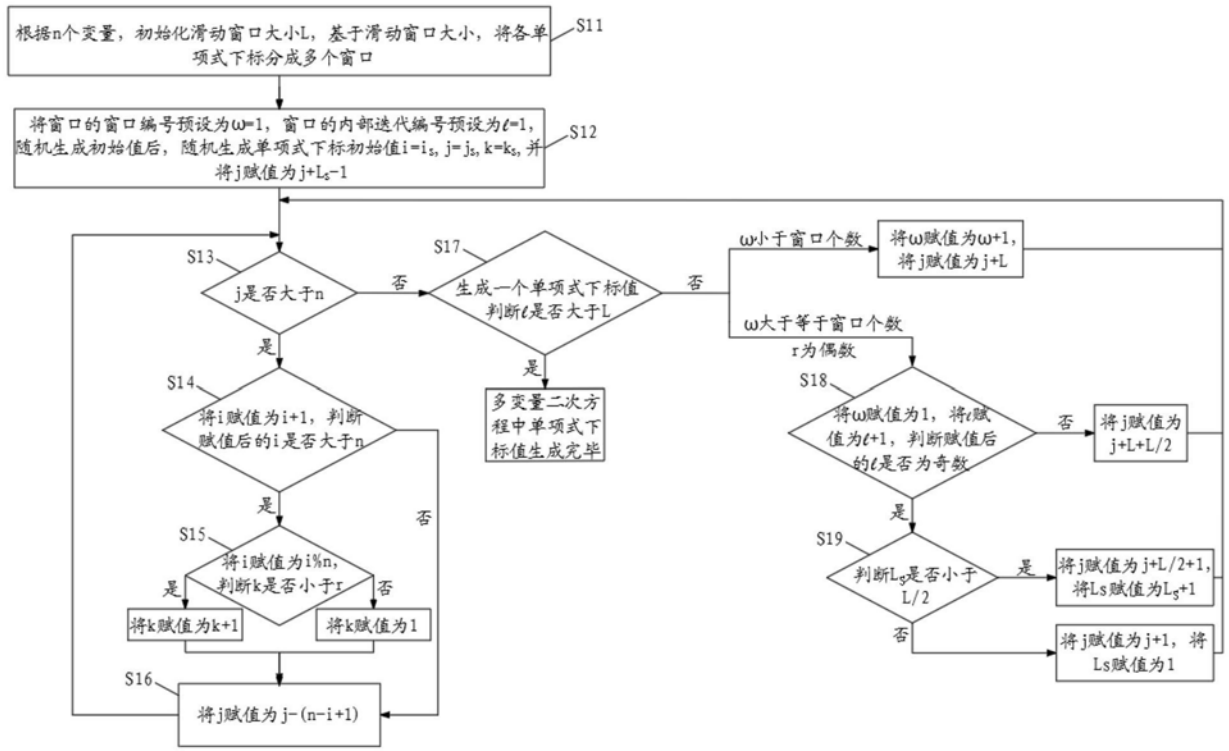

根据n个变量，初始化滑动窗口大小L，基于滑动窗口大小，将各单项式下标分成多个窗口
S11
将窗口的窗口编号预设为ω=1，窗口的内部迭代编号预设为ℓ=1，随机生成初始值后，随机生成单项式下标初始值i=is，j=js，k=ks，并将j赋值为j+Ls-1
S12
S13
j是否大于n
否
是
S14
将i赋值为i+1，判断赋值后的i是否大于n
是
否
S15
将i赋值为i%n，判断k是否小于r
是
否
将k赋值为k+1
将k赋值为1
S16
将j赋值为j-(n-i+1)
S17
生成一个单项式下标值判断ℓ是否大于L
否
是
多变量二次方程中单项式下标值生成完毕
ω小于窗口个数
将ω赋值为ω+1，将j赋值为j+L
ω大于等于窗口个数
r为偶数
S18
将ω赋值为1，将ℓ赋值为ℓ+1，判断赋值后的ℓ是否为奇数
否
将j赋值为j+L+L/2
是
S19
判断Ls是否小于L/2
是
将j赋值为j+L/2+1，将Ls赋值为Ls+1
否
将j赋值为j+1，将Ls赋值为1

图3

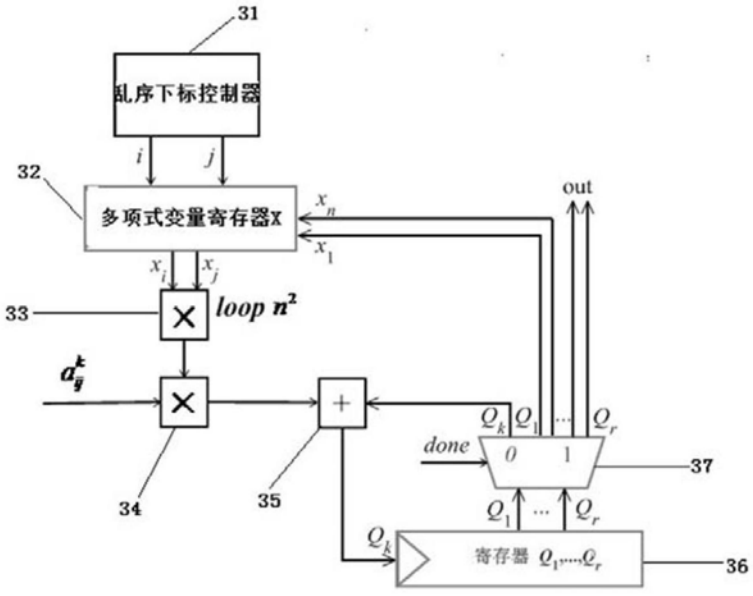

31
乱序下标控制器
i
j
32
多项式变量寄存器X
x_n
x_1
x_i
x_j
out
33
loop n^2
a_{ij}^k
34
35
Q_k Q_1 ... Q_r
done
0
1
37
Q_1 ... Q_r
Q_k
寄存器 Q_1,...,Q_r
36

图4