[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
*H04L 9/32 (2006.01)*
*G09C 1/00 (2006.01)*

# [12] 发明专利申请公布说明书

[21] 申请号 200580040976.0

[43] 公开日 2007 年 11 月 7 日

[11] 公开号 CN 101069381A

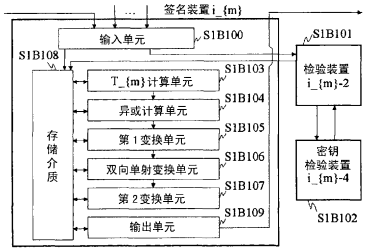
[22] 申请日 2005.11.11
[21] 申请号 200580040976.0
[30] 优先权
[32] 2004.11.29 [33] JP [31] 343703/2004
[86] 国际申请 PCT/JP2005/020729 2005.11.11
[87] 国际公布 WO2006/057171 日 2006.6.1
[85] 进入国家阶段日期 2007.5.29
[71] 申请人 日本电气株式会社
地址 日本东京都
[72] 发明人 寺西勇 佐古和惠 田口大悟 野田润
[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 李香兰
权利要求书 14 页 说明书 27 页 附图 11 页

[54] 发明名称

签名与检验方法以及签名与检验装置

[57] 摘要

本发明提供一种在多个签名装置进行签名的情况下的签名长度不依赖于签名装置的数目的 RSA 签名方法。 签名装置 i_{m}，具有：在所输入的签名句 u_{i_{m-1}}超过了模量 n_{i_{m}}的情况下，不进行任何操作，在超过了的情况下，进行以 RSA 方式为准据的签名的第 1 变换单元(SS1B105)；对该结果作用向大至模量 n_{i_{m}}的方向进行映射的函数的双向单射变换单元(S1B106)；在该操作结果超过了模量 n_{i_{m}}的情况下，不进行任何操作，在没有超过的情况下，进行以 RSA 方式为准据的签名的第 2 变换单元(S1B107)；以及将该操作结果作为签名句 u_{i_{m}}输出的输出单元(S1B109)。




i_{m} 签名装置
S1B108 存储介质
S1B100 输入单元
S1B103 T_{m} 计算单元
S1B104 异或计算单元
S1B105 第 1 变换单元
S1B106 双向单射变换单元
S1B107 第 2 变换单元
S1B109 输出单元
S1B101 检验装置
S1B102 密钥检验装置

1．一种签名方法，是一种将初始值或其他多个签名装置顺次进行签名操作所生成的签名句、消息、以及本签名装置的秘密密钥作为输入，输出与输入相同长度的签名句的签名装置的签名方法，其特征在于：

所述所输出的签名句，表示：该所述所输出的签名句的生成所述涉及的签名装置，在输入到了各个签名装置的所述消息中进行了签名。

2．如权利要求 1 所述的签名方法，其特征在于：

计算签名句的操作具有第 1 与第 2 这两个步骤，所述第 1 步骤（f^{-1}部分的操作）的计算中，使用带陷阱门的单向性置换的反函数，所述第 2 步骤（h^{-1}部分的操作）的计算中，使用与所述第 1 步骤相比相同或不同的带陷阱门的单向性置换的反函数，如果所述第 1 步骤结束，便将计算结果存储到存储介质中，在所述第 2 步骤开始时，从所述存储介质读出必要的数据，如果所述第 2 步骤结束，便将计算结果存储到所述存储介质中。

3．如权利要求 2 所述的签名方法，其特征在于：

在所述第 1 步骤中，如果针对所述第 1 步骤的输入是所述带陷阱门的单向性置换的值域的元素，便通过该所述带陷阱门的单向性置换的反函数对所述输入进行映射，如果不是则不进行任何操作，如果针对所述第 2 步骤的输入是所述带陷阱门的单向性置换的值域的元素，便通过所述带陷阱门的单向性置换的反函数对所述输入进行映射，如果不是则不进行任何操作。

4．如权利要求 3 所述的签名方法，其特征在于：

所述第 2 步骤中所使用的所述带陷阱门的单向性置换的计算进一步由第 1 与第 2 子步骤构成，所述第 1 子步骤（φ^{-1}部分的操作）中，计算签名句全体的空间上的双向单射，该双向单射能够通过多项式时间来计算，并且所述双向单射的反函数也能够通过多项式时间来计算，在所述第 2 子步骤（g^{-1}部分的操作）中使用带陷阱门的单向性置换的反函数，如果是所述带陷阱门的单向性置换的值域的元素，便通过所述带陷阱门的单向性置换的反函数对所述输入映射，如果不是则不进行任何操作，所述第 1 子步骤与所述第 2 子步骤的开始时，从所述存储介质读入必要的数据，

所述第 1 子步骤与所述第 2 子步骤的结束时，将计算结果写入到所述存储介质中。

5．如权利要求 4 所述的签名方法，其特征在于：

所述第 1 步骤中所使用的所述带陷阱门的单向性置换，与所述第 2 步骤的所述第 2 子步骤中所使用的所述带陷阱门的单向性置换，是 RSA 函数。

6．如权利要求 5 所述的签名方法，其特征在于：

所述第 2 步骤的所述第 1 子步骤中所使用的所述双向单射，使用 $\phi(x) = x - n_{i_{m}} \bmod 2^{\kappa}$，所述 $n_{i_{m}}$是作为签名装置 $i_{m}$的公开密钥的一部分的 RSA 模量，所述 $\kappa$ 是安全参数。

7．如权利要求 6 所述的签名方法，其特征在于：

所述第 1 步骤之前有 $T_{m}$计算步骤，所述 $T_{m}$计算步骤中，计算出 $T_{m} = M_{1}\|\cdots\|M_{m}\|pk_{i_{1}}\|\cdots\|pk_{i_{m}}$，对于各个 j，所述 $M_{1},\cdots, M_{j}$是输入给了第 j 个签名装置的消息，所述 $pk_{i_{j}}$是签名装置 $i_{j}$的公开密钥。

8．如权利要求 7 所述的签名方法，其特征在于：

所述第 1 步骤之前有异或计算步骤，所述异或计算步骤中，计算出 $U=H(T_{m})\bigcirc u_{i_{m-1}}$，所述 H 为散列函数，所述 $u_{i_{m-1}}$是所述所输入的签名句，○为异或。

9．如权利要求 8 所述的签名方法，其特征在于：

所述第 1 步骤之前，具有密钥合法性检验步骤，在所述密钥合法性检验步骤中，确认 $pk_{i_{1}},\cdots, pk_{i_{m-1}}$是否完全不同，但在 m＝1 的情况下，不进行任何确认。

10．如权利要求 9 所述的签名方法，其特征在于：

所述第 1 步骤之前，有对所输入的签名句进行检验的签名句检验步骤。

11．如权利要求 8 所述的签名方法，其特征在于：

所述第 1 步骤之前，具有对 $pk_{i_{1}},\cdots, pk_{i_{m-1}}$是否完全不同进行确认的密钥合法性检验步骤，以及对所输入的签名句进行检验的签名句检验步骤。

12．如权利要求 1～11 中任一项所述的签名方法，其特征在于：

具有：将所输入的初始值或签名句或他们的散列值作为辅助信息而生成并写入到所述存储介质中的步骤，并将所述辅助信息与签名句作为组输出。

13．一种签名方法，其特征在于，包括：

输入单元将初始值或其他多个签名装置顺次进行签名操作而生成的签名句 u_{i_{m-1}}、以及输入给这些签名装置的消息 M_{1},…, M_{m-1}输入并保存到存储介质中的步骤；

T_{m}计算单元从所述存储介质以及公开密钥存储装置读入必要的数据，在将 pk_{i_{j}}设为签名装置 i_{j}的公开密钥，且将||设为位列彼此的连接时，计算出 T_{m} = M_{1}||…||M_{m}||pk_{i_{1}}||…||pk_{i_{m}}，并将计算结果保存到所述存储介质中的步骤；

异或计算单元在将 H 设为散列函数，将○设为异或时，从所述存储介质读入必要的数据，并计算出 U=H(T_{m})○u_{i_{m-1}}，将计算结果保存到所述存储介质中的步骤；

第 1 变换单元从所述存储介质读入必要的数据，并在设 n_{i_{m}}为本签名装置的 RSA 模量时，如果 U＜n_{i_{m}}，便计算出 v= u^{d_{i_{m}}} mod n_{i_{m}}，此外则计算出 v=U，并将计算结果保存到所述存储介质中的步骤；

双向单射变换单元从所述存储介质读入必要的数据，在设 κ 为安全参数时，计算出 v'=v + n_{i_{m}} mod 2^{ κ }，并将计算结果保存到所述存储介质中的步骤；

第 2 变换单元从所述存储介质读入必要的数据，如果 v'＜n_{i_{m}}，便计算出 u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}，此外则计算出 u_{i_{m}} = v'，并将计算结果保存到所述存储介质中的步骤；以及

输出单元从所述存储介质读入 u_{i_{m}}并作为签名句而输出的步骤。

14．如权利要求 13 所述的签名方法，其特征在于：

具有：由 w 设置单元在 w_{i_{m}}=u_{i_{m-1}}或设 h 为散列函数时，计算 w_{i_{m}}=h(u_{i_{m-1}})，并将计算结果保存到所述存储介质中的步骤，将所述所计算出的 w_{i_{m}}作为辅助信息，与所述所生成的签名

句 u_{i_{m}}作为组而输出。

15．一种检验方法，是一种检验多个签名装置顺次进行签名操作而生成的签名句 u 是否合法的检验装置中的检验方法，其特征在于：

当且仅当签名句 u 是如下内容时通过检验：即所述所输出的签名句为，所述所输出的签名句的生成所涉及的签名装置已经在输入于各个签名装置中的所述消息中进行了签名；所述签名句 u 的位长，是不依赖于为了计算所述签名句 u 而涉及的所述签名句装置的数目的常数。

16．一种检验方法，是一种检验多个签名装置顺次进行签名操作而生成的签名句 u 是否合法的检验装置中的检验方法，其特征在于：

当且仅当生成签名句 u 的签名装置通过合法的方法生成了签名句 u 时通过检验，所述签名句 u 的位长，是不依赖于为了计算所述签名句 u 而涉及的所述签名句装置的数目的常数，且所述签名句 u 的检验，使用作为所述多个签名装置中最后 1 台执行签名操作之前的数据的辅助信息 w 来进行。

17．如权利要求 15 或 16 所述的检验方法，其特征在于：

检验签名句的操作具有第 1 与第 2 这两个步骤，所述第 1 步骤（h 部分的操作）的计算中，使用带陷阱门的单向性置换，所述第 2 步骤（f 部分的操作）的计算中，使用与所述第 1 步骤相比相同或不同的带陷阱门的单向性置换，在开始所述第 1 步骤与第 2 步骤时，从存储介质读出必要的数据，在所述第 1 步骤与第 2 步骤结束结束时，将计算结果写入到所述存储介质中。

18．如权利要求 17 所述的检验方法，其特征在于：

所述第 1 步骤中，如果针对所述第 1 步骤的输入是所述带陷阱门的单向性置换的定义域的元素，便通过所述带陷阱门的单向性置换对所述输入进行映射，如果不是则不进行任何操作，如果针对所述第 2 步骤的输入是所述带陷阱门的单向性置换的定义域的元素，便通过所述带陷阱门的单向性置换对所述输入进行映射，如果不是则不进行任何操作。

19．如权利要求 18 所述的检验方法，其特征在于：

所述第 1 步骤中所使用的所述带陷阱门的单向性置换的计算进一步由第 1 与第 2 子步骤构成，所述第 1 子步骤（g 部分的操作）中，使用带陷

阱门的单向性置换的函数，如果是所述带陷阱门的单向性置换的值域的元素，便通过所述带陷阱门的单向性置换的函数对所述输入进行映射，如果不是则不进行任何操作，所述第 2 子步骤（φ部分的操作）中，计算签名句全体的空间上的双向单射，该双向单射能够通过多项式时间来计算，并且所述双向单射的反函数也能够通过多项式时间来计算，所述第 1 子步骤与所述第 2 子步骤的开始时，从所述存储介质读入必要的数据，所述第 1 子步骤与所述第 2 子步骤的结束时，将计算结果写入到所述存储介质中。

20．如权利要求 19 所述的检验方法，其特征在于：

所述第 1 步骤的所述第 1 子步骤中所使用的所述带陷阱门的单向性置换，与所述第 2 步骤中所使用的所述带陷阱门的单向性置换，是 RSA 函数。

21．如权利要求 20 所述的检验方法，其特征在于：

所述第 1 步骤的所述第 2 子步骤中所使用的所述双向单射，采用 $\phi(x) = x + n_{i_{m}} \bmod 2^{\kappa}$，所述 $n_{i_{m}}$是作为签名装置 $i_{m}$的公开密钥的一部分的 RSA 模量，所述κ是安全参数。

22．如权利要求 21 所述的检验方法，其特征在于：

所述第 2 步骤之后有 T_{j}计算步骤，所述 T_{j}计算步骤中，计算出 $T_{j} = M_{1}\|\cdots\|M_{j}\|pk_{i_{1}}\|\cdots\|pk_{i_{j}}$，这里，对各个 j，所述 $M_{1}, \ldots, M_{j}$是输入在第 j 个签名装置的消息，所述 $pk_{i_{j}}$是签名装置 $i_{j}$的公开密钥。

23．如权利要求 22 所述的检验方法，其特征在于：

所述 T_{j}计算步骤之后，具有如下那样的 u 计算步骤：即将 H 设为散列函数，将 U 设为第 2 步骤的计算结果时，从所述存储介质读入必要的数据，而计算出 $u_{i_{j-1}}=H(T_{j})\bigcirc U$，并将计算结果存储到所述存储介质中。

24．如权利要求 23 所述的检验方法，其特征在于：

对 j=m-1,…,1，反复执行所述第 1 步骤、所述第 2 步骤、所述 T_{j}计算步骤，以及所述 u 计算步骤。

25．如权利要求 24 所述的检验方法，其特征在于：

在对 j=m-1,…,1 反复执行所述第 1 步骤、所述第 2 步骤、所述 T_{j}

计算步骤，以及所述 u 计算步骤之前，有密钥合法性检验步骤，所述密钥合法性检验步骤中，对 pk_{i_{1}},…, pk_{i_{m-1}}全部都不同进行确认，但在 m=1 的情况下，不进行任何确认。

26．如权利要求 25 所述的检验方法，其特征在于：

在对 j=m-1,…,1 反复执行所述第 1 步骤、所述第 2 步骤、所述 T_{j}计算步骤，以及所述 u 计算步骤之后，存在 u 判断步骤，其中对作为检验结果是否得到了初始值进行判断。

27．如权利要求 21 所述的检验方法，其特征在于：

所述第 1 步骤之前有 T_{m-1}计算步骤以及 v"计算步骤，所述 T_{m-1}计算步骤中，计算出 T_{m-1} =M_{1}|…||M_{m-1}||pk_{i_{1}}||…||pk_{i_{m-1}}，这里，M_{1},…, M_{m-1}是输入在第 1,…,m-1 个签名装置的消息，所述 pk_{i_{j}}是签名装置 i_{j}的公开密钥；所述 v"计算步骤中，计算出 v"=H(T_{m-1})○u_{i_{m-1}}，并且所述第 1 步骤将所述 v’’作为输入，且在所述第 2 步骤之后，存在判断所述第 2 步骤的计算结果是否与所述辅助信息相一致的 u 判断步骤。

28．一种检验方法，其特征在于，包括：

输入单元将由其他的 1 个以上的签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、输入给这些签名装置的消息 M_{1},…, M_{m-1}、以及这些签名装置的公开密钥 pk_{i_{1}},…,pk_{i_{m-1}}输入，并保存到存储介质中的步骤；

J 初始化单元将 m-1 设为变数 j 的步骤；

第 2 变换单元，从所述存储介质读入必要的数据，如果 u_{i_{j}}<n_{i_{j}}，便计算出 v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}，此外则计算出 v'=u_{i_{j}，并将计算结果保存到所述存储介质中的步骤；

双向单射计算单元从所述存储介质读入必要的数据，计算出 v=v'-n_{i_{m}} mod 2^{κ}，并将计算结果保存到所述存储介质中的步骤；

第 1 变换单元从所述存储介质读入必要的数据，如果 v<n_{i_{j}}便计算出 U=v^{e_{i_{j}}} mod n_{i_{j}}，此外则计算出 U=v，并将计算结果保存到所述存储介质中的步骤；

每当将所述变量 j 减 1 时重复基于所述第 2 变换单元、所述双向单射

计算单元、以及所述第 1 变换单元的所述步骤直到所述变量 j 变为 0 的步骤；

T_{j}计算单元从所述存储介质读入必要的数据，计算出 T_{j} = M_{1}‖…‖M_{j}‖pk_{i_{1}}‖…‖pk_{i_{j}}并将计算结果保存到所述存储介质中的步骤；

u 计算单元从所述存储介质读入必要的数据，计算出 u_{i_{j-1}}=H(T_{j})○U 并将计算结果保存到所述存储介质中的步骤；

u 判断单元从所述存储介质读入必要的数据，并判断 u 是否等于预先设定的初始值的步骤；以及

输出单元在 u 等于预先设定的初始值的情况下输出表示检验成功的通知，否则便输出表示检验失败的通知的步骤。

29．一种检验方法，其特征在于，包括：

输入单元对由其他的 1 个以上的签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、前一个签名装置所输入的签名句或其散列值即辅助信息 v_{i_{m-1}}、输入在这些签名装置中的消息 M_{1},…, M_{m-1}、以及这些签名装置的公开密钥 pk_{i_{1}},…,pk_{i_{m-1}}进行输入，并保存到存储介质中的步骤；

T_{m-1}计算单元从所述存储介质读入必要的数据，计算出 T_{m-1} = M_{1}‖…‖M_{m-1}‖pk_{i_{1}}‖…‖pk_{i_{m-1}}，并将计算结果保存到所述存储介质中的步骤；

v"计算单元从所述存储介质读入必要的数据，计算出 v"=H(T_{m-1})○u_{i_{m-1}}，并将计算结果保存到所述存储介质中的步骤；

第 2 变换单元从所述存储介质读入必要的数据，如果 v"<n_{i_{m-1}}，便计算出 v'=v"^{e_{i_{m-1}}} mod n_{i_{m-1}}，此外则计算出 v'=v"，并将计算结果保存到所述存储介质中的步骤；

双向单射计算单元从所述存储介质读入必要的数据，计算出 v=v'-n_{i_{m-1}} mod 2^{ κ }，并将计算结果保存到所述存储介质中的步骤；

第 1 变换单元从所述存储介质读入必要的数据，如果 v<n_{i_{m-1}}，便计算出 u_{i_{m-2}}=v^{e_{i_{m-1}}} mod n_{i_{m-1}}，此外则计算出 u_{i_{m-2}}=v，并将计算结果保存到所述存储介质中的步骤；

u 判断单元从所述存储介质读入必要的数据，并判断 u_{i_{m-2}}或其散列值是否与所述辅助信息 v_{i_{m-1}}相一致的步骤；以及

输出单元在 u_{i_{m-2}}或其散列值与所述辅助信息 v_{i_{m-1}}相一致的情况下，输出表示检验成功的通知，否则，输出表示检验失败的通知的步骤。

30．一种签名装置，其特征在于，包括：

可读写的存储介质；

输入单元，其对初始值或其他多个签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、以及输入在这些签名装置中的消息 M_{1},…,M_{m-1}进行输入，并保存到存储介质中；

T_{m}计算单元，其从所述存储介质以及公开密钥存储装置读入必要的数据，在将 pk_{i_{j}}设为签名装置 i_{j}的公开密钥，将||设为位列彼此的连接时，计算出 T_{m} = M_{1}||…||M_{m}||pk_{i_{1}}||…||pk_{i_{m}}，并将计算结果保存到所述存储介质中；

异或计算单元，其在将 H 设为散列函数，将○设为异或时，从所述存储介质读入必要的数据，并计算出 U=H(T_{m})○u_{i_{m-1}}，并将计算结果保存到所述存储介质中；

第 1 变换单元，其从所述存储介质读入必要的数据，在将 n_{i_{m}}设为本签名装置的 RSA 模量时，如果 U＜n_{i_{m}}，便计算 v=u^{d_{i_{m}}} mod n_{i_{m}}，此外则计算 v=U，并将计算结果保存到所述存储介质中；

双向单射变换单元，其从所述存储介质读入必要的数据，在将 κ 设为安全参数时，计算出 v'=v + n_{i_{m}} mod 2^{ κ }，并将计算结果保存到所述存储介质中；

第 2 变换单元，其从所述存储介质读入必要的数据，如果 v'＜n_{i_{m}}，则计算出 u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}，此外则计算出 u_{i_{m}} = v'，并将计算结果保存到所述存储介质中；以及

输出单元，其从所述存储介质读入 u_{i_{m}}，并作为签名句输出。

31．如权利要求 30 所述的签名装置，其特征在于：

具有：w 设置单元，其在 w_{i_{m}}=u_{i_{m-1}}，或者将 h 设为散

列函数时，计算 w_{i_{m}}=h(u_{i_{m-1}})，并将计算结果保存到所述存储介质中；将所述所计算出的 w_{i_{m}}作为辅助信息，与所述所生成的签名句 u_{i_{m}}作为组而输出。

32．一种检验装置，其特征在于，包括：

可读写的存储介质；

输入单元，其对由其他的 1 个以上的签名装置顺次进行了签名操作而生成的签名句 u_{i_{m-1}}、输入在些签名装置中的消息 M_{1},…,M_{m-1}、以及这些签名装置的公开密钥 pk_{i_{1}},…,pk_{i_{m-1}}进行输入，并保存到存储介质中；

J 初始化单元，其将 m-1 设置为变量 j；

第 2 变换单元，其从所述存储介质读入必要的数据，如果 u_{i_{j}}<n_{i_{j}}，计算出 v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}，此外则计算出 v'=u_{i_{j}，并将计算结果保存到所述存储介质中；

双向单射计算单元，其从所述存储介质读入必要的数据，计算出 v=v'-n_{i_{m}} mod 2^{ κ }，并将计算结果保存到所述存储介质中；

第 1 变换单元，其从所述存储介质读入必要的数据，如果 v<n_{i_{j}}，便计算出 U=v^{e_{i_{j}}} mod n_{i_{j}}，此外则计算出 U=v，并将计算结果保存到所述存储介质中；

T_{j}计算单元，其每当将所述变量 j 减 1 时，重复执行了基于所述第 2 变换单元、所述双向单射计算单元、以及所述第 1 变换单元的所述步骤之后，从所述存储介质读入必要的数据，计算出 T_{j} = M_{1}‖…‖M_{j}‖pk_{i_{1}}‖…‖pk_{i_{j}}，并将计算结果保存到所述存储介质中；

u 计算单元，其从所述存储介质读入必要的数据，计算出 u_{i_{j-1}}=H(T_{j})○U，并将计算结果保存到所述存储介质中；

u 判断单元，其从所述存储介质读入必要的数据，并判断 u 是否等于预先设定的初始值；以及

输出单元，其在 u 等于预先设定的初始值情况下，输出表示检验成功的通知，否则输出表示检验失败的通知。

33．一种检验装置，其特征在于，包括：

可读写的存储介质；

输入单元，其对由其他的 1 个以上的签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、作为前一个签名装置所输入的签名句或其散列值的辅助信息 v_{i_{m-1}}、输入在这些签名装置中的消息 M_{1},…,M_{m-1}、以及这些签名装置的公开密钥 pk_{i_{1}},…,pk_{i_{m-1}进行输入，并保存到存储介质中；

T_{m-1}计算单元，其从所述存储介质读入必要的数据，计算 T_{m-1}=M_{1}‖…‖M_{m-1}‖pk_{i_{1}}‖…‖pk_{i_{m-1}}，并将计算结果保存到所述存储介质中；

v"计算单元，其从所述存储介质读入必要的数据，计算 v"=H(T_{m-1})○u_{i_{m-1}}，并将计算结果保存到所述存储介质中；

第 2 变换单元，其从所述存储介质读入必要的数据，如果 v"<n_{i_{m-1}}，则计算 v'=v"^{e_{i_{m-1}}} mod n_{i_{m-1}}，否则计算出 v'=v"，并将计算结果保存到所述存储介质中；

双向单射计算单元，其从所述存储介质读入必要的数据，计算出 v=v'-n_{i_{m-1}} mod 2^{κ}，并将计算结果保存到所述存储介质中；

第 1 变换单元，其从所述存储介质读入必要的数据，如果 v<n_{i_{m-1}}，则计算出 u_{i_{m-2}}=v^{e_{i_{m-1}}} mod n_{i_{m-1}}，此外则计算出 u_{i_{m-2}}=v，并将计算结果保存到所述存储介质中；

u 判断单元，其从所述存储介质读入必要的数据，判断 u_{i_{m-2}}或其散列值是否与所述辅助信息 v_{i_{m-1}}相一致；以及

输出单元，其在 u_{i_{m-2}}或其散列值与所述辅助信息 v_{i_{m-1}}相一致的情况下，输出表示检验成功的通知，否则输出表示检验失败的通知。

34．一种程序，让具有可读写的存储介质的计算机起到作为以下单元而发挥功能：

输入单元，其对初始值或其他多个签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、以及输入在这些签名装置中的消息 M_{1},…,M_{m-1}进行输入，并保存到存储介质中；

T_{m}计算单元，其从所述存储介质以及公开密钥存储装置读入必要

的数据，在将 pk_{i_{j}}设为签名装置 i_{j}的公开密钥，将||设为位列彼此的连接时，计算 T_{m} = M_{1}||…||M_{m}||pk_{i_{1}}||…||pk_{i_{m}}，并将计算结果保存到所述存储介质中；

异或计算单元，其在将 H 设为散列函数，将○设为异或时，从所述存储介质读入必要的数据，并计算 U=H(T_{m})○u_{i_{m-1}}，并将计算结果保存到所述存储介质中；

第 1 变换单元，其从所述存储介质读入必要的数据，在将 n_{i_{m}}设为本签名装置的 RSA 模量时，如果 U＜n_{i_{m}}，便计算出 v= u^{d_{i_{m}}} mod n_{i_{m}}，此外则计算出 v=U，并将计算结果保存到所述存储介质中；

双向单射变换单元，其从所述存储介质读入必要的数据，在将 κ 设为安全参数时，计算 v'=v + n_{i_{m}} mod 2^{ κ }，并将计算结果保存到所述存储介质中；

第 2 变换单元，其从所述存储介质读入必要的数据，如果 v'＜n_{i_{m}}，便计算 u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}，此外则计算 u_{i_{m}} = v'，并将计算结果保存到所述存储介质中；以及

输出单元，其从所述存储介质读入 u_{i_{m}}，并作为签名句输出。

35．如权利要求 34 所述的程序，其特征在于：

让所述计算机进一步起到作为 w 设置单元而发挥功能，所述 w 设置单元在 w_{i_{m}}=u_{i_{m-1}}，或将 h 设为散列函数时，计算出 w_{i_{m}}=h(u_{i_{m-1}})，并将计算结果保存到所述存储介质中，并且将所述所计算出的 w_{i_{m}}作为辅助信息，与所述所生成的签名句 u_{i_{m}}作为组而输出。

36．一种程序，让具有可读写的存储介质的计算机作为以下单元而发挥功能：

输入单元，其对由其他的 1 个以上的签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、输入给这些签名装置的消息 M_{1},…,M_{m-1}、以及这些签名装置的公开密钥 pk_{i_{1}},…,pk_{i_{m-1}}进行输入，并保存到存储介质中；

J 初始化单元，其将 m-1 设为变量 j；

第 2 变换单元，其从所述存储介质读入必要的数据，如果 u_{i_{j}}<n_{i_{j}}，便计算出 v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}，此外则计算出 v'=u_{i_{j}，并将计算结果保存到所述存储介质中；

双向单射计算单元，其从所述存储介质读入必要的数据，计算出 v=v'-n_{i_{m}} mod 2^{ κ }，并将计算结果保存到所述存储介质中；

第 1 变换单元，其从所述存储介质读入必要的数据，如果 v<n_{i_{j}}，便计算出 U=v^{e_{i_{j}}} mod n_{i_{j}}，此外则计算出 U=v，并将计算结果保存到所述存储介质中；

T_{j}计算单元，其在每当将所述变量 j 减 1 时，重复执行了基于所述第 2 变换单元、所述双向单射计算单元、以及所述第 1 变换单元的所述步骤之后，从所述存储介质读入必要的数据，计算出 T_{j} = M_{1}‖…‖M_{j}‖pk_{i_{1}}‖…‖pk_{i_{j}}，并将计算结果保存到所述存储介质中；

u 计算单元，其从所述存储介质读入必要的数据，计算出 u_{i_{j-1}}=H(T_{j})○U，并将计算结果保存到所述存储介质中；

u 判断单元，其从所述存储介质读入必要的数据，判断 u 是否等于预先设定的初始值；以及

输出单元，其在 u＝预先设定的初始值的情况下，输出表示检验成功的通知，否则输出表示检验失败的通知。

37．一种程序，让具有可读写的存储介质的计算机起到作为以下单元的功能：

输入单元，其对由其他的 1 个以上的签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、作为前一个签名装置所输入的签名句或其散列值的辅助信息 v_{i_{m-1}}、输入在这些签名装置中的消息 M_{1},…,M_{m-1}、以及这些签名装置的公开密钥 pk_{i_{1}},…,pk_{i_{m-1}}进行输入，并保存到存储介质中；

T_{m-1}计算单元，其从所述存储介质读入必要的数据，计算出 T_{m-1} = M_{1}‖…‖M_{m-1}‖pk_{i_{1}}‖…‖pk_{i_{m-1}}，并将计算结果保存到所述存储介质中；

v"计算单元，其从所述存储介质读入必要的数据，计算出 v"=H(T_{m-1})○u_{i_{m-1}}，并将计算结果保存到所述存储介质中；

第 2 变换单元，其从所述存储介质读入必要的数据，如果 v"<n_{i_{m-1}}，则计算出 v'=v"^{e_{i_{m-1}}} mod n_{i_{m-1}}，此外则计算出 v'=v"，并将计算结果保存到所述存储介质中；

双向单射计算单元，其从所述存储介质读入必要的数据，计算出 v=v'-n_{i_{m-1}} mod 2^{κ}，并将计算结果保存到所述存储介质中；

第 1 变换单元，其从所述存储介质读入必要的数据，如果 v<n_{i_{m-1}}，便计算出 u_{i_{m-2}}=v^{e_{i_{m-1}}} mod n_{i_{m-1}}，此外则计算出 u_{i_{m-2}}=v，并将计算结果保存到所述存储介质中；

u 判断单元，其从所述存储介质读入必要的数据，判断 u_{i_{m-2}}或其散列值是否与所述辅助信息 v_{i_{m-1}}相一致；以及

输出单元，其在 u_{i_{m-2}}或其散列值与所述辅助信息 v_{i_{m-1}}相一致的情况下，输出表示检验成功的通知，否则，便输出表示检验失败的通知。

38．一种签名装置，至少包括如下那样的单元：即在输入了初始值或其他多个签名装置顺次进行签名操作所生成的签名句、以及输入在所述签名装置的消息的情况下，计算出将所述消息与本装置的公开密钥以及已经签名过的签名装置的公开密钥连接起来的结果，并导出所述连接结果的散列值与所述签名句的异或值，其特征在于，

还具有：

第 1 单元，其在所述异或值超过了所述签名装置的公开密钥的一部分即 RSA 模量的情况下，直接输出所述异或值，在没有超过的情况下，输出所述异或中进行了以 RSA 签名为准据的签名之后的结果；

第 2 单元，其对所述第 1 单元的输出，作用向大至所述 RSA 模量的方向映射的函数；以及

第 3 变换单元，其在所述第 2 单元中的运算结果超过了所述 RSA 模量的情况下，直接输出所述双向单射单元中的运算结果，在没有超过的情况下，输出在所述第 2 单元的运算结果中进行了以 RSA 签名为准据的签名之后的结果。

39．一种检验装置，是一种对多个权利要求 38 中所述的签名装置顺

次进行签名操作而生成的签名句是否合法进行检验的检验装置，包括每当检验各个签名装置中的签名时：

在所述签名句超过了对应的签名装置的 RSA 模量的情况下，直接输出，在没有超过的情况下，输出进行了以 RSA 签名为准据之后的结果的第 4 单元；

第 5 单元，其对所述第 4 单元的输出，作用向小至所述 RSA 模量的方向映射的函数；

第 6 单元，其在所述第 5 单元的输出超过了所述 RSA 模量的情况下，直接输出所述第 5 单元的输出，在没有超过的情况下，输出在所述第 5 单元的输出中进行了以 RSA 签名为准据的签名之后的结果；以及

第 7 单元，其对输入给所述签名装置的消息、连接本装置的公开密钥和已经签名过的签名装置的公开密钥的结果的散列值、以及所述第 6 单元的输出之间的异或值，进行求算；

根据对各个所述签名装置的基于所述第 7 单元的输出结果，判断检验的成功、失败。

# 签名与检验方法以及签名与检验装置

## 技术领域

本发明涉及一种签名与检验方法以及签名与检验装置，特别是一种在多个签名装置进行签名的状况下的、签名长度不依赖于签名装置数目的、签名与检验方法以及签名与检验装置。

## 背景技术

伴随着计算机与互联网环境的普及，电子发送接收消息的机会也在增加。这种情况下，为了防止在发送消息的过程中消息被篡改，希望在消息中添加电子签名。

但是在使用称作 RSA 或 DSA 的公知的签名方式，由多个签名装置进行了签名的情况下，为了表示全体都已进行了签名，需要由全签名装置分别生成签名句，并将这些签名句都保存起来。因此，签名句的数据长度的合计值与签名装置的台数成比例，在签名装置数目较多的情况下，效率不高。

作为解决这样的问题的签名方式之一，提出了非专利文献 1 中所述的签名方式。图 11 中示出了该以往的签名方式的顺序。

另外，本说明书中所使用的签名的意义，这里进行了定义。“||”表示位列彼此的连接。“〇”表示每一位的“异或”。“^”表示以右边的被算符为指数计算出左边的被算符的幂的算数算符。例如，f^{－1}为 $f^{-1}$。「_{x}」表示 x 为脚标。例如，u_{i}为 $u_i$。

参照图 11，一旦输入了成为签名对象的签名文字 u_{i_{m-1}}（S3F100），便在进行了所具有的密钥的合法性检验（S3F101）与签名句 u_{i_{m-1}}的合法性的检验（S3F102）之后，计算出将本签名装置的公开密钥与已经签名了的签名装置的公开密钥连接起来的 T_{m}（S3F103）。接下来，计算出 T_{m}的散列值与签名句 u_{i_{m-1}}的异或 U（S3F104），设 U 的位列中第一个安全参数 k 位为 a，剩下的为 s（S3F105）。接下来，

比较 a 与本签名装置的 RSA 模量 n_{i_{m}}（S3F106），在 a 小于 RSA 模量 n_{i_{m}}时，通过秘密密钥 d_{i_{m}}对 a 计算出以 RSA 方式为准据的签名句 u_{i_{m}}（S3F107），并输出（S3F109）。此时给 s 添加 1 位的信息 0 作为控制信息。另外，在 a 大于 RSA 模量 n_{i_{m}}时，对于大于模量的数，由于无法计算 RSA 签名，因此对将 a 减去了 n_{i_{m}}之后的值计算出签名句 u_{i_{m}}（S3F108）并输出（S3F109））。此时给 s 添加 1 位的信息 1 作为控制信息。

这样，在 RSA 的情况下，对于大于签名装置的 RSA 模量 n_{i_{m}}的数，由于无法计算签名，因此基于非专利文献 1 的以往技术中，在较大的情况下，减去模量 n_{i_{m}}之后再添加签名。此时，为了之后的检验能够进行，在其后添加 1bit 的控制信息（超过了模量的情况下添加 1，此外添加 0）。签名句 u_{i_{m}}的检验时，使用与签顺序与相反的顺序对签名装置的公开密钥反复进行检验，最终追溯到得到预定的初始值，通过这样，判断是正确的签名。

非专利文献 1：Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, Hovav Shacham. Sequential Aggregate Signatures from Trapdoor Permutations. In Advances in Cryptology -- EUROCRYPT 2004,vol. 3027 of LNCS, pp. 74-90. Springer-Verlag, 2004.

根据非专利文献 1 中所述的以前的签名方式，由于即使多个签名装置顺次进行签名，签名句的数据长度的合计值也不与签名装置的台数成比例，因此在存储签名句的情况下，能够削减存储量，在进行通信的情况下，能够削减通信量。但是，存在如下问题：即签名长为固定值＋签名次数，存在如果签名次数增加，签名长度也稍有延长。

## 发明内容

本发明的目的在于，改善所述以前的签名方式所具有的问题点，使得签名长度与签名装置的数目无关，为一定值。

本发明第 1 项涉及一种签名方法，是一种将初始值或其他多个签名装置顺次进行签名操作所生成的签名句、消息、以及本签名装置的秘密密钥作为输入，输出与输入相同长度的签名句的签名装置的签名方法，其特征

在于：

所述所输出的签名句，表示：该所述所输出的签名句的生成所述涉及的签名装置，在输入到了各个签名装置的所述消息中，已经进行了签名。

本发明第 2 项所涉及的签名方法的特征在于，在本发明第 1 项所记载的签名方法中，计算签名句的操作具有第 1 与第 2 这两个步骤，所述第 1 步骤（f^{-1}部分的操作）的计算中，使用带陷阱门的单向性置换的反函数，所述第 2 步骤（h^{-1}部分的操作）的计算中，使用与所述第 1 步骤相比相同或不同的带陷阱门的单向性置换的反函数，如果所述第 1 步骤结束，便将计算结果存储到存储介质中，在所述第 2 步骤开始时，从所述存储介质读出必要的数据，如果所述第 2 步骤结束，便将计算结果存储到所述存储介质中。

本发明第 3 项所涉及的签名方法的特征在于，在本发明第 2 项所记载的签名方法中，在所述第 1 步骤中，如果针对所述第 1 步骤的输入是所述带陷阱门的单向性置换的值域的元素，便通过该所述带陷阱门的单向性置换的反函数对所述输入进行映射，如果不是则不进行任何操作，如果针对所述第 2 步骤的输入是所述带陷阱门的单向性置换的值域的元素，便通过所述带陷阱门的单向性置换的反函数对所述输入进行映射，如果不是则不进行任何操作。

本发明第 4 项所涉及的签名方法的特征在于，在本发明第 3 项所记载的签名方法中，所述第 2 步骤中所使用的所述带陷阱门的单向性置换的计算进一步由第 1 与第 2 子步骤构成，所述第 1 子步骤（Φ^{-1}部分的操作）中，计算签名句全体的空间上的双向单射，该双向单射能够通过多项式时间来计算，并且所述双向单射的反函数也能够通过多项式时间来计算，在所述第 2 子步骤（g^{-1}部分的操作）中使用带陷阱门的单向性置换的反函数，如果是所述带陷阱门的单向性置换的值域的元素，便通过所述带陷阱门的单向性置换的反函数对所述输入映射，如果不是则不进行任何操作，所述第 1 子步骤与所述第 2 子步骤的开始时，从所述存储介质读入必要的数据，所述第 1 子步骤与所述第 2 子步骤的结束时，将计算结果写入到所述存储介质中。

本发明第 5 项所涉及的签名方法的特征在于，在本发明第 4 项所记载

的签名方法中，所述第 1 步骤中所使用的所述带陷阱门的单向性置换，与所述第 2 步骤的所述第 2 子步骤中所使用的所述带陷阱门的单向性置换，是 RSA 函数。

本发明第 6 项所涉及的签名方法的特征在于，在本发明第 5 项所记载的签名方法中，所述第 2 步骤的所述第 1 子步骤中所使用的所述双向单射，采用 $\phi(x) = x - n_{i_{m}} \bmod 2^{\kappa}$，所述 $n_{i_{m}}$是作为签名装置 $i_{m}$的公开密钥的一部分的 RSA 模量，所述 $\kappa$ 是安全参数。

本发明第 7 项所涉及的签名方法的特征在于，在本发明第 6 项所记载的签名方法中，所述第 1 步骤之前有 $T_{m}$计算步骤，所述 $T_{m}$计算步骤中，计算出 $T_{m} = M_{1}\|\cdots\|M_{m}\|pk_{i_{1}}\|\cdots\|pk_{i_{m}}$，对于各个 j，所述 $M_{1},\cdots, M_{j}$是输入给了第 j 个签名装置的消息，所述 $pk_{i_{j}}$是签名装置 $i_{j}$的公开密钥。

本发明第 8 项所涉及的签名方法的特征在于，在本发明第 7 项所记载的签名方法中，所述第 1 步骤之前有异或计算步骤，在所述异或计算步骤中，计算出 $U=H(T_{m})\bigcirc u_{i_{m-1}}$，所述 H 为散列函数，所述 $u_{i_{m-1}}$是所述所输入的签名句，○为异或。

本发明第 9 项所涉及的签名方法的特征在于，在本发明第 8 项所记载的签名方法中，所述第 1 步骤之前，具有密钥合法性检验步骤，在所述密钥合法性检验步骤中，确认 $pk_{i_{1}},\cdots, pk_{i_{m-1}}$是否完全不同，但在 m＝1 的情况下，不进行任何确认。

本发明第 10 项所涉及的签名方法的特征在于，在本发明第 9 项所记载的签名方法中，所述第 1 步骤之前，有对所输入的签名句进行检验的签名句检验步骤。

本发明第 11 项所涉及的签名方法的特征在于，在本发明第 2 项所记载的签名方法中，所述第 1 步骤之前，具有对 $pk_{i_{1}},\cdots, pk_{i_{m-1}}$是否完全不同进行确认的密钥合法性检验步骤，以及对所输入的签名句进行检验的签名句检验步骤。

本发明第 12 项所涉及的签名方法的特征在于，在本发明第 1～11 的任一项所记载的签名方法中，具有：将所输入的初始值或签名句或他们的散列值作为辅助信息而生成并写入到所述存储介质中的步骤，并将所述辅

助信息与签名句作为组输出。

本发明第 13 项涉及一种签名方法，其特征在于，包括：输入单元将初始值或其他多个签名装置顺次进行签名操作而生成的签名句 u_{i_{m-1}}、以及输入给这些签名装置的消息 M_{1},…,M_{m-1}输入并保存到存储介质中的步骤；T_{m}计算单元从所述存储介质以及公开密钥存储装置读入必要的数据，在将 pk_{i_{j}}设为签名装置 i_{j}的公开密钥，且将‖设为位列彼此的连接时，计算出 T_{m} = M_{1}‖…‖M_{m}‖pk_{i_{1}}‖…‖pk_{i_{m}}，并将计算结果保存到所述存储介质中的步骤；异或计算单元在将 H 设为散列函数，将○设为异或时，从所述存储介质读入必要的数据，并计算出 U=H(T_{m})○u_{i_{m-1}}，将计算结果保存到所述存储介质中的步骤；第 1 变换单元从所述存储介质读入必要的数据，并在设 n_{i_{m}}为本签名装置的 RSA 模量时，如果 U＜n_{i_{m}}，便计算出 v= u^{d_{i_{m}}} mod n_{i_{m}}，此外则计算出 v=U，并将计算结果保存到所述存储介质中的步骤；双向单射变换单元从所述存储介质读入必要的数据，在设 κ 为安全参数时，计算出 v'=v + n_{i_{m}} mod 2^{ κ }，并将计算结果保存到所述存储介质中的步骤；第 2 变换单元从所述存储介质读入必要的数据，如果 v'＜n_{i_{m}}，便计算出 u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}，此外则计算出 u_{i_{m}} = v'，并将计算结果保存到所述存储介质中的步骤；以及输出单元从所述存储介质读入 u_{i_{m}}并作为签名句而输出的步骤。

本发明第 14 项所涉及的签名方法的特征在于，在本发明第 13 项所记载的签名方法中，具有：由 w 设置单元在 w_{i_{m}}=u_{i_{m-1}}或设 h 为散列函数时，计算 w_{i_{m}}=h(u_{i_{m-1}})，并将计算结果保存到所述存储介质中的步骤，将所述所计算出的 w_{i_{m}}作为辅助信息，与所述所生成的签名句 u_{i_{m}}作为组而输出。

本发明第 15 项涉及一种检验方法，是一种检验多个签名装置顺次进行签名操作而生成的签名句 u 是否合法的检验装置的检验方法，其特征在于：当且仅当签名句 u 为，所述所输出的签名句表示，所述所输出的签名句的生成所涉及的签名装置已经在输入在各个签名装置中的所述消息中进行了签名时，通过检验；所述签名句 u 的位长，是不依赖于为了计算所

述签名句 u 而涉及的所述签名句装置的数目的常数。

本发明第 16 项涉及一种检验方法，是一种检验多个签名装置顺次进行签名操作而生成的签名句 u 是否合法的检验装置中的检验方法，其特征在于：当且仅当生成签名句 u 的签名装置通过合法的方法生成了签名句 u 时通过检验，所述签名句 u 的位长，是不依赖于为了计算所述签名句 u 而涉及的所述签名句装置的数目的常数，且所述签名句 u 的检验，使用作为所述多个签名装置中最后 1 台执行签名操作之前的数据的辅助信息 w 来进行。

本发明第 17 项所涉及的检验方法的特征在于，在本发明第 15 或 16 项所记载的签名方法中，检验签名句的操作具有第 1 与第 2 这两个步骤，所述第 1 步骤（h 部分的操作）的计算中，使用带陷阱门的单向性置换，所述第 2 步骤（f 部分的操作）的计算中，使用与所述第 1 步骤相比相同或不同的带陷阱门的单向性置换，在开始所述第 1 步骤与第 2 步骤时，从存储介质读出必要的数据，在所述第 1 步骤与第 2 步骤结束结束时，将计算结果写入到所述存储介质中。

本发明第 18 项所涉及的检验方法的特征在于，在本发明第 17 项所记载的签名方法中，所述第 1 步骤中，如果针对所述第 1 步骤的输入是所述带陷阱门的单向性置换的定义域的元素，便通过所述带陷阱门的单向性置换对所述输入进行映射，如果不是则不进行任何操作，如果针对所述第 2 步骤的输入是所述带陷阱门的单向性置换的定义域的元素，便通过所述带陷阱门的单向性置换对所述输入进行映射，如果不是则不进行任何操作。

本发明第 19 项所涉及的检验方法的特征在于，在本发明第 18 项所记载的签名方法中，所述第 1 步骤中所使用的所述带陷阱门的单向性置换的计算进一步由第 1 与第 2 子步骤构成，所述第 1 子步骤（g 部分的操作）中，使用带陷阱门的单向性置换的函数，如果是所述带陷阱门的单向性置换的值域的元素，便通过所述带陷阱门的单向性置换的函数对所述输入进行映射，如果不是则不进行任何操作，所述第 2 子步骤（Φ 部分的操作）中，计算签名句全体的空间上的双向单射，该双向单射能够通过多项式时间来计算，并且所述双向单射的反函数也能够通过多项式时间来计算，所述第 1 子步骤与所述第 2 子步骤的开始时，从所述存储介质读入必要的数

据，所述第 1 子步骤与所述第 2 子步骤的结束时，将计算结果写入到所述存储介质中。

本发明第 20 项所涉及的检验方法的特征在于，在本发明第 19 项所记载的签名方法中，所述第 1 步骤的所述第 1 子步骤中所使用的所述带陷阱门的单向性置换，与所述第 2 步骤中所使用的所述带陷阱门的单向性置换，是 RSA 函数。

本发明第 21 项所涉及的检验方法的特征在于，在本发明第 20 项所记载的签名方法中，所述第 1 步骤的所述第 2 子步骤中所使用的所述双向单射，采用 $\phi(x) = x + n\_i\_\{m\} \bmod 2^{\{\kappa\}}$，所述 n_{i_{m}}是作为签名装置 i_{m}的公开密钥的一部分的 RSA 模量，所述 $\kappa$ 是安全参数。

本发明第 22 项所涉及的检验方法的特征在于，在本发明第 21 项所记载的签名方法中，所述第 2 步骤之后有 T_{j}计算步骤，所述 T_{j}计算步骤中，计算出 T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}，这里，对各个 j，所述 M_{1}, ..., M_{j}是输入在第 j 个签名装置的消息，所述 pk_{i_{j}}是签名装置 i_{j}的公开密钥。

本发明第 23 项所涉及的检验方法的特征在于，在本发明第 22 项所记载的签名方法中，所述 T_{j}计算步骤之后，具有如下那样的 u 计算步骤：即将 H 设为散列函数，将 U 设为第 2 步骤的计算结果时，从所述存储介质读入必要的数据，而计算出 u_{i_{j-1}}=H(T_{j})○U，并将计算结果存储到所述存储介质中。

本发明第 24 项所涉及的检验方法的特征在于，在本发明第 23 项所记载的签名方法中，对 j=m-1,…,1，反复执行所述第 1 步骤、所述第 2 步骤、所述 T_{j}计算步骤，以及所述 u 计算步骤。

本发明第 25 项所涉及的检验方法的特征在于，在本发明第 24 项所记载的签名方法中，在对 j=m-1,…,1 反复执行所述第 1 步骤、所述第 2 步骤、所述 T_{j}计算步骤，以及所述 u 计算步骤之前，有密钥合法性检验步骤，所述密钥合法性检验步骤中，对 pk_{i_{1}},…, pk_{i_{m-1}}全部都不同进行确认，但在 m=1 的情况下，不进行任何确认。

本发明第 26 项所涉及的检验方法的特征在于，在本发明第 25 项所记载的签名方法中，在对 j=m-1,…,1 反复执行所述第 1 步骤、所述第 2 步骤、

所述 T_{j}计算步骤，以及所述 u 计算步骤之后，存在 u 判断步骤，其中对作为检验结果是否得到了初始值进行判断。

本发明第 27 项所涉及的检验方法的特征在于，在本发明第 2 项所记载的签名方法中，所述第 1 步骤之前有 T_{m-1}计算步骤以及 v"计算步骤，所述 T_{m-1}计算步骤中，计算出 T_{m-1} =M_{1}‖…‖M_{m-1}‖pk_{i_{1}}‖…‖pk_{i_{m-1}}，这里，M_{1},…, M_{m-1}是输入在第 1,…,m-1 个签名装置的消息，所述 pk_{i_{j}}是签名装置 i_{j}的公开密钥；所述 v"计算步骤中，计算出 v"=H(T_{m-1})○u_{i_{m-1}}，并且所述第 1 步骤将所述 v''作为输入，在所述第 2 步骤之后，存在判断所述第 2 步骤的计算结果是否与所述辅助信息相一致的 u 判断步骤。

本发明第 28 项涉及一种检验方法，其特征在于，包括：输入单元将由其他的 1 个以上的签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、输入给这些签名装置的消息 M_{1},…, M_{m-1}、以及这些签名装置的公开密钥 pk_{i_{1}},…,pk_{i_{m-1}}输入，并保存到存储介质中的步骤；J 初始化单元将 m-1 设为变数 j 的步骤；第 2 变换单元，从所述存储介质读入必要的数据，如果 u_{i_{j}}<n_{i_{j}}，便计算出 v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}，此外则计算出 v'=u_{i_{j}，并将计算结果保存到所述存储介质中的步骤；双向单射计算单元从所述存储介质读入必要的数据，计算出 v=v'- n_{i_{m}} mod 2^{ κ }，并将计算结果保存到所述存储介质中的步骤；第 1 变换单元从所述存储介质读入必要的数据，如果 v<n_{i_{j}}便计算出 U=v^{e_{i_{j}}} mod n_{i_{j}}，此外则计算出 U=v，并将计算结果保存到所述存储介质中的步骤；每当将所述变量 j 减 1 时重复基于所述第 2 变换单元、所述双向单射计算单元、以及所述第 1 变换单元的所述步骤直到所述变量 j 变为 0 的步骤；T_{j}计算单元从所述存储介质读入必要的数据，计算出 T_{j} = M_{1}‖…‖M_{j}‖pk_{i_{1}}‖…‖pk_{i_{j}}并将计算结果保存到所述存储介质中的步骤；u 计算单元从所述存储介质读入必要的数据，计算出 u_{i_{j-1}}=H(T_{j})○U 并将计算结果保存到所述存储介质中的步骤；u 判断单元从所述存储介质读入必要的数据，并判断 u 是否等于预先设定的初始值的步骤；以及输出单元在 u 等于预先设定的初始值的情况下输出表

示检验成功的通知，否则便输出表示检验失败的通知的步骤。

本发明第 29 项涉及一种检验方法，其特征在于，包括：输入单元对由其他的 1 个以上的签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、前一个签名装置所输入的签名句或其散列值即辅助信息 v_{i_{m-1}}、输入在这些签名装置中的消息 M_{1},…, M_{m-1}、以及这些签名装置的公开密钥 pk_{i_{1}},…,pk_{i_{m-1}}进行输入，并保存到存储介质中的步骤；T_{m-1}计算单元从所述存储介质读入必要的数据，计算出 T_{m-1} = M_{1}‖…‖M_{m-1}‖pk_{i_{1}}‖…‖pk_{i_{m-1}}，并将计算结果保存到所述存储介质中的步骤；v"计算单元从所述存储介质读入必要的数据，计算出 v"=H(T_{m-1})○u_{i_{m-1}}，并将计算结果保存到所述存储介质中的步骤；第 2 变换单元从所述存储介质读入必要的数据，如果 v"<n_{i_{m-1}}，便计算出 v'=v"^{e_{i_{m-1}}} mod n_{i_{m-1}}，此外则计算出 v'=v"，并将计算结果保存到所述存储介质中的步骤；双向单射计算单元从所述存储介质读入必要的数据，计算出 v=v'- n_{i_{m-1}} mod 2^{ κ }，并将计算结果保存到所述存储介质中的步骤；

第 1 变换单元从所述存储介质读入必要的数据，如果 v<n_{i_{m-1}}，便计算出 u_{i_{m-2}}=v^{e_{i_{m-1}}} mod n_{i_{m-1}}，此外则计算出 u_{i_{m-2}}=v，并将计算结果保存到所述存储介质中的步骤；u 判断单元从所述存储介质读入必要的数据，并判断 u_{i_{m-2}}或其散列值是否与所述辅助信息 v_{i_{m-1}}相一致的步骤；以及输出单元在 u_{i_{m-2}}或其散列值与所述辅助信息 v_{i_{m-1}}相一致的情况下，输出表示检验成功的通知，否则，输出表示检验失败的通知的步骤。

本发明第 30 项涉及一种签名装置，其特征在于，包括：可读写的存储介质；输入单元，其对初始值或其他多个签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、以及输入在这些签名装置中的消息 M_{1},…, M_{m-1}进行输入，并保存到存储介质中；T_{m}计算单元，其从所述存储介质以及公开密钥存储装置读入必要的数据，在将 pk_{i_{j}}设为签名装置 i_{j}的公开密钥，将‖设为位列彼此的连接时，计算出 T_{m} = M_{1}‖…‖M_{m}‖pk_{i_{1}}‖…‖pk_{i_{m}}，并将计算结果保存到所述存储介质中；异或计算单元，其在将 H 设为散列函数，将○设为异或时，

从所述存储介质读入必要的数据，并计算出 U=H(T_{m})○u_{i_{m-1}}，并将计算结果保存到所述存储介质中；第 1 变换单元，其从所述存储介质读入必要的数据，在将 n_{i_{m}}设为本签名装置的 RSA 模量时，如果 U＜n_{i_{m}}，便计算 v= u^{d_{i_{m}}} mod n_{i_{m}}，此外则计算 v=U，并将计算结果保存到所述存储介质中；双向单射变换单元，其从所述存储介质读入必要的数据，在将 κ 设为安全参数时，计算出 v'=v + n_{i_{m}} mod 2^{ κ }，并将计算结果保存到所述存储介质中；第 2 变换单元，其从所述存储介质读入必要的数据，如果 v'＜n_{i_{m}}，则计算出 u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}，此外则计算出 u_{i_{m}} = v'，并将计算结果保存到所述存储介质中；以及输出单元，其从所述存储介质读入 u_{i_{m}}，并作为签名句输出。

本发明第 31 项所涉及的签名装置的特征在于，在本发明第 30 项所记载的签名方法中，具有 w 设置单元，其在 w_{i_{m}}=u_{i_{m-1}}，或者将 h 设为散列函数时，计算 w_{i_{m}}=h(u_{i_{m-1}})，并将计算结果保存到所述存储介质中；将所述所计算出的 w_{i_{m}}作为辅助信息，与所述所生成的签名句 u_{i_{m}}作为组而输出。

本发明第 32 项涉及一种检验装置，其特征在于，包括：可读写的存储介质；输入单元，其对由其他的 1 个以上的签名装置顺次进行了签名操作而生成的签名句 u_{i_{m-1}}、输入在些签名装置中的消息 M_{1},…,M_{m-1}、以及这些签名装置的公开密钥 pk_{i_{1}},…,pk_{i_{m-1}}进行输入，并保存到存储介质中；J 初始化单元，其将 m-1 设置为变量 j；第 2 变换单元，其从所述存储介质读入必要的数据，如果 u_{i_{j}}<n_{i_{j}}，计算出 v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}，此外则计算出 v'=u_{i_{j}}，并将计算结果保存到所述存储介质中；双向单射计算单元，其从所述存储介质读入必要的数据，计算出 v=v'- n_{i_{m}} mod 2^{ κ }，并将计算结果保存到所述存储介质中；第 1 变换单元，其从所述存储介质读入必要的数据，如果 v<n_{i_{j}}，便计算出 U=v^{e_{i_{j}}} mod n_{i_{j}}，此外则计算出 U=v，并将计算结果保存到所述存储介质中；T_{j}计算单元，其每当将所述变量 j 减 1 时，重复执行了基于所述第 2 变换单元、所述双向单射计算单元、以及所述第 1 变换单元的所述步骤之后，从所述存储介质

读入必要的数据，计算出 T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}，并将计算结果保存到所述存储介质中；

u 计算单元，其从所述存储介质读入必要的数据，计算出 u_{i_{j-1}}=H(T_{j})○U，并将计算结果保存到所述存储介质中；u 判断单元，其从所述存储介质读入必要的数据，并判断 u 是否等于预先设定的初始值；以及输出单元，其在 u 等于预先设定的初始值情况下，输出表示检验成功的通知，否则输出表示检验失败的通知。

本发明第 33 项涉及一种检验装置，其特征在于，包括：可读写的存储介质；输入单元，其对由其他的 1 个以上的签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、作为前一个签名装置所输入的签名句或其散列值的辅助信息 v_{i_{m-1}}、输入在这些签名装置中的消息 M_{1},…,M_{m-1}、以及这些签名装置的公开密钥 pk_{i_{1}},…,pk_{i_{m-1}进行输入，并保存到存储介质中；T_{m-1}计算单元，其从所述存储介质读入必要的数据，计算 T_{m-1} = M_{1}||…||M_{m-1}||pk_{i_{1}}||…||pk_{i_{m-1}}，并将计算结果保存到所述存储介质中；v"计算单元，其从所述存储介质读入必要的数据，计算 v"=H(T_{m-1})○u_{i_{m-1}}，并将计算结果保存到所述存储介质中；第 2 变换单元，其从所述存储介质读入必要的数据，如果 v"<n_{i_{m-1}}，则计算 v'=v"^{e_{i_{m-1}}} mod n_{i_{m-1}}，否则计算出 v'=v"，并将计算结果保存到所述存储介质中；双向单射计算单元，其从所述存储介质读入必要的数据，计算出 v=v'-n_{i_{m-1}} mod 2^{κ}，并将计算结果保存到所述存储介质中；第 1 变换单元，其从所述存储介质读入必要的数据，如果 v<n_{i_{m-1}}，则计算出 u_{i_{m-2}}=v^{e_{i_{m-1}}} mod n_{i_{m-1}}，此外则计算出 u_{i_{m-2}}=v，并将计算结果保存到所述存储介质中；u 判断单元，其从所述存储介质读入必要的数据，判断 u_{i_{m-2}}或其散列值是否与所述辅助信息 v_{i_{m-1}}相一致；以及输出单元，其在 u_{i_{m-2}}或其散列值与所述辅助信息 v_{i_{m-1}}相一致的情况下，输出表示检验成功的通知，否则输出表示检验失败的通知。

本发明第 34 项涉及一种程序，让具有可读写的存储介质的计算机起到作为以下单元而发挥功能：输入单元，其对初始值或其他多个签名装置

顺次进行签名操作所生成的签名句 u_{i_{m-1}}、以及输入在这些签名装置中的消息 M_{1},…, M_{m-1}进行输入，并保存到存储介质中；T_{m}计算单元，其从所述存储介质以及公开密钥存储装置读入必要的数据，在将 pk_{i_{j}}设为签名装置 i_{j}的公开密钥，将||设为位列彼此的连接时，计算 T_{m} = M_{1}||…||M_{m}||pk_{i_{1}}||…||pk_{i_{m}}，并将计算结果保存到所述存储介质中；异或计算单元，其在将 H 设为散列函数，将○设为异或时，从所述存储介质读入必要的数据，并计算 U=H(T_{m})○u_{i_{m-1}}，并将计算结果保存到所述存储介质中；第 1 变换单元，其从所述存储介质读入必要的数据，在将 n_{i_{m}}设为本签名装置的 RSA 模量时，如果 U＜n_{i_{m}}，便计算出 v= u^{d_{i_{m}}} mod n_{i_{m}}，此外则计算出 v=U，并将计算结果保存到所述存储介质中；双向单射变换单元，其从所述存储介质读入必要的数据，在将 κ 设为安全参数时，计算 v'=v + n_{i_{m}} mod 2^{ κ }，并将计算结果保存到所述存储介质中；第 2 变换单元，其从所述存储介质读入必要的数据，如果 v'＜n_{i_{m}}，便计算 u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}，此外则计算 u_{i_{m}} = v'，并将计算结果保存到所述存储介质中；以及输出单元，其从所述存储介质读入 u_{i_{m}}，并作为签名句输出。

本发明第 35 项所涉及的程序的特征在于，在本发明第 34 项所记载的签名方法中，让所述计算机进一步起到作为 w 设置单元而发挥功能，所述 w 设置单元在 w_{i_{m}}=u_{i_{m-1}}，或将 h 设为散列函数时，计算出 w_{i_{m}}=h(u_{i_{m-1}})，并将计算结果保存到所述存储介质中，并且将所述所计算出的 w_{i_{m}}作为辅助信息，与所述所生成的签名句 u_{i_{m}}作为组而输出。

本发明第 36 项涉及一种程序，让具有可写入的存储介质的计算机作为以下单元而发挥功能：输入单元，其对由其他的 1 个以上的签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、输入给这些签名装置的消息 M_{1},…, M_{m-1}、以及这些签名装置的公开密钥 pk_{i_{1}},…,pk_{i_{m-1}}进行输入，并保存到存储介质中；J 初始化单元，其将 m-1 设为变量 j；第 2 变换单元，其从所述存储介质读入必要的数据，如果 u_{i_{j}}<n_{i_{j}}，便计算出 v'=u_{i_{j}}^{e_{i_{j}}} mod

n_{i_{j}}，此外则计算出 v'=u_{i_{j}，并将计算结果保存到所述存储介质中；双向单射计算单元，其从所述存储介质读入必要的数据，计算出 v=v'-n_{i_{m}} mod 2^{κ}，并将计算结果保存到所述存储介质中；第 1 变换单元，其从所述存储介质读入必要的数据，如果 v<n_{i_{j}}，便计算出 U=v^{e_{i_{j}}} mod n_{i_{j}}，此外则计算出 U=v，并将计算结果保存到所述存储介质中；T_{j}计算单元，其在每当将所述变量 j 减 1 时，重复执行了基于所述第 2 变换单元、所述双向单射计算单元、以及所述第 1 变换单元的所述步骤之后，从所述存储介质读入必要的数据，计算出 T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}，并将计算结果保存到所述存储介质中；

u 计算单元，其从所述存储介质读入必要的数据，计算出 u_{i_{j-1}}=H(T_{j})○U，并将计算结果保存到所述存储介质中；u 判断单元，其从所述存储介质读入必要的数据，判断 u 是否等于预先设定的初始值；以及输出单元，其在 u＝预先设定的初始值的情况下，输出表示检验成功的通知，否则输出表示检验失败的通知。

本发明第 37 项涉及一种程序，让具有可读写的存储介质的计算机起到作为以下单元的功能：输入单元，其对由其他的 1 个以上的签名装置顺次进行签名操作所生成的签名句 u_{i_{m-1}}、作为前一个签名装置所输入的签名句或其散列值的辅助信息 v_{i_{m-1}}、输入在这些签名装置中的消息 M_{1},…, M_{m-1}、以及这些签名装置的公开密钥 pk_{i_{1}},…,pk_{i_{m-1}}进行输入，并保存到存储介质中；T_{m-1}计算单元，其从所述存储介质读入必要的数据，计算出 T_{m-1} = M_{1}||…||M_{m-1}||pk_{i_{1}}||…||pk_{i_{m-1}}，并将计算结果保存到所述存储介质中；v"计算单元，其从所述存储介质读入必要的数据，计算出 v"=H(T_{m-1})○u_{i_{m-1}}，并将计算结果保存到所述存储介质中；第 2 变换单元，其从所述存储介质读入必要的数据，如果 v"<n_{i_{m-1}}，则计算出 v'=v"^{e_{i_{m-1}}} mod n_{i_{m-1}}，此外则计算出 v'=v"，并将计算结果保存到所述存储介质中；双向单射计算单元，其从所述存储介质读入必要的数据，计算出 v=v'- n_{i_{m-1}} mod 2^{κ}，并将计算结果保存到所述存储介质中；第 1 变换单元，其从所述存储介质读入必要的数

据，如果 v<n_{i_{m-1}}，便计算出 u_{i_{m-2}}=v^{e_{i_{m-1}}} mod n_{i_{m-1}}，此外则计算出 u_{i_{m-2}}=v，并将计算结果保存到所述存储介质中；u 判断单元，其从所述存储介质读入必要的数据，判断 u_{i_{m-2}}或其散列值是否与所述辅助信息 v_{i_{m-1}}相一致；以及输出单元，其在 u_{i_{m-2}}或其散列值与所述辅助信息 v_{i_{m-1}}相一致的情况下，输出表示检验成功的通知，否则，便输出表示检验失败的通知。

本发明中，在签名装置 i_{m}中进行：在所输入的签名句 u_{i_{m-1}}超过了模量 n_{i_{m}}的情况下，不进行任何操作，在没有超过的情况下，进行以 RSA 签名为准据的签名的第 1 操作；对第 1 操作的结果，作用向大至模量 n_{i_{m}}的方向映射的函数的第 2 操作；以及在该第 2 操作的结果超过了模量 n_{i_{m}}的情况下，不进行任何操作，在没有超过的情况下，进行以 RSA 签名为准据的签名的第 3 操作。这里，如果设各个签名装置的 RSA 模量的位长与安全参数 κ 相等，签名句 u_{i_{m-1}}以及签名装置 i_{m}的模量 n_{i_{m}}就变为小于 2^{κ}的数。第 1 操作中，对取 0～n_{i_{m}}的值的签名句 u_{i_{m-1}}，进行以 RSA 签名为准据的签名，因此第 1 操作之后的值变为 0～n_{i_{m}}，另外，对于取 n_{i_{m}}～2^{κ}的值的签名句 u_{i_{m-1}}，不进行任何操作，因此第 1 操作之后的值变为 n_{i_{m}}～2^{κ}。另外，第 2 操作中，进行从第 1 操作之后的值向以 2^{κ}为模量的 n_{i_{m}}的加法，因此第 2 操作之后的值也变为小于 2^{κ}的数，但第 1 操作之后的值为 n_{i_{m}}～2^{κ}者，在第 2 操作之后变为 0～n_{i_{m}}。因此，第 3 操作中，对第 2 操作之后的值变为 0～n_{i_{m}}者进行以 RSA 签名为准据的签名，由此对任意值的签名句 u_{i_{m-1}}，至少都进行 1 次 RSA 签名。另外，第 3 操作之后的值，也即签名值 u_{i_{m}}的值与所输入的签名句 u_{i_{m-1}}的值一一对应，因此根据签名值 u_{i_{m}}的值，能够唯一决定所实施的签名操作，从而不需要添加非专利文献 1 中那样的控制位。

第 1 效果是，签名长度不依赖于签名装置的数目。其原因是，签名前的数据与签名后所生成的数据位数不变。

第 2 效果是，能够在每次签名时变更签名装置的顺序。其原因与第 1 效果的情况下相同，签名前的数据与签名后所生成的数据位数不变。因此，

对各个签名装置的输入是一定的，跟该签名装置是第几个进行签名的无关，因此不管是第几个，都能够通过相同的操作来签名。

第 3 效果是，与签名装置勾结的攻击者，无法伪造出从线路中的“诚实 honest”的签名装置中通过的签名句。其原因在于，不管对签名装置的输入 u 是什么，签名时最多进行两次的 RSA 计算中的至少一方的 u 不变。

第 4 效果是，在系统使用的开始阶段，不需要知道签名装置的数目 m，即使签名装置的数目 m 在使用中动态变化，也能够正常使用。其原因是，签名装置的数目为 m+1 台时的签名顺序，是在进行了签名装置的数目为 m 台时的签名顺序之后再进行一次同样的签名操作，签名的操作方法不依赖于签名装置的数目 m。

## 附图说明

图 1 为本发明的第 1 实施方式的方框图。

图 2 为表示本发明的第 1 实施方式中的签名装置之构成的方框图。

图 3 为表示本发明的第 1 实施方式中的签名装置之动作的流程图。

图 4 为表示本发明的第 1 实施方式中的检验装置之构成的方框图。

图 5 为表示本发明的第 1 实施方式中的检验装置之动作的流程图。

图 6 为本发明的第 2 实施方式的方框图。

图 7 为表示本发明的第 2 实施方式中的签名装置之构成的方框图。

图 8 为表示本发明的第 2 实施方式中的签名装置之动作的流程图。

图 9 为表示本发明的第 2 实施方式中的检验装置之构成的方框图。

图 10 为表示本发明的第 2 实施方式中的检验装置之动作的流程图。

图 11 为表示以前的签名装置之动作的流程图。

图中：

i_{1},…,i_{m-1}－签名装置，

i_{1}-2,…,i_{m-1}-2－检验装置，

i_{1}-3,…,i_{m-1}-3－密钥存储装置，

i_{1}-4,…,i_{m-1}-4－密钥合法性检验装置，

i_{1}-5,…,i_{m-1}-5－密钥生成装置，

M_{1},…, M_{m}－消息，

u_ {i_{0}},…, u_ {i_{m-1}}－签名句，

w_ {i_{0}},…, w_ {i_{m-1}}－辅助信息。

## 具体实施方式

<第 1 实施方式>

对照图 1，本发明的第 1 实施方式，由签名装置 i_{1},…,i_{m}、检验装置 i_{1}-2,…,i_{m-1}-2、公开密钥存储装置 i_{1}-3,…,i_{m-1}-3、密钥合法性检验装置 i_{1}-4,…,i_{m}-4、以及秘密密钥存储装置 i_{1}-5,…,i_{m-1}-5 构成。

参照图 2，签名装置 i_{m}由输入单元 S1B100、T_{m}计算单元 S1B103、异或计算单元 S1B104、第一变换单元 S1B105、双向单射变换单元 S1B106、第二变换单元 S1B107、存储介质 S1B108、以及输出单元 S1B109 构成，其他的签名装置也具有与签名装置 i_{m}相同的构成。

参照图 4，检验装置 i_{m}-2 由输入单元 V1B100、j 初始化单元 V1B102、j 判断单元 V1B103、第二变换单元 V1B104、双向单射变换单元 V1B105、第一变换单元 V1B106、T_{j}计算单元 V1B107、u 计算单元 V1B108、j 减少单元 V1B109、存储介质 V1B1010、u 判断单元 V1B1011、accept 输出单元 V1B1012、以及 reject 输出单元 V1B1013 构成。其他检验装置也具有与检验装置 i_{m}-2 相同的构成。

对本实施方式进行概述。首先，给签名装置 i_{1}输入签名装置 i_{1}的公开密钥秘密密钥对、初始值 u_{i_{0}}、以及消息 M_{1}。签名装置 i_{1}使用 u_{i_{0}}生成对消息 M_{1}的签名句 u_{i_{1}}。之后，顺次给签名装置 i_{j}输入签名装置 i_{j}的公开密钥秘密密钥对、前一个签名装置所输出的签名句 u_{i_{j-1}}、以及消息 M_{j}，签名装置 i_{j}使用这些生成签名句 u_{i_{j}}。签名句 u_{i_{j}}是表示签名装置 i_{1}在消息 M_{1}中进行了签名，签名装置 i_{2}在消息 M_{2}中进行了签名，…、签名装置 i_{j}在消息 M_{j}中进行了签名的数据。

对各个 j，给检验装置 i_{j}输入签名装置 i_{1},…,i_{j}的公开密钥与消息 M_{1},…,M_{j-1}，以及签名句 u_{i_{j-1}}。于是，检验装置 i_{j}对签名句 u_{i_{j-1}}是否是使用签名装置 i_{1},…,i_{j-1}的秘密密钥，且

针对消息 M_{1},…,M_{j-1}所生成的签名句进行检验。

本实施方式的系统目标是，生成签名句 u_{i_{m}}即对签名装置 i_{1}在消息 M_{1}中进行了签名，签名装置 i_{2}在消息 M_{2}中进行了签名，…，签名装置 i_{m}在消息 M_{m}中进行了签名进行表示的数据。

另外，本实施方式系统的应用开始阶段，不需要知道签名装置的数目 m。签名装置的数目 m 可以在应用中动态变化。另外，签名装置 i_{1},…,i_{m}的动作完全相同。检验装置、公开密钥存储装置、密钥合法性检验装置、秘密密钥存储装置也基本都进行相同的动作。

接下来对本实施方式进行详细说明。

签名装置 i_{j}的公开密钥 pk_{i}、秘密密钥 sk_{i}分别为(n_{i},e_{i}）、（p_{i_{j}}，q_{i_{j}},d_{i_{j}}），满足下面的 5 个性质。

1. p_{i_{j}}，q_{i_{j}}为质数。

2. n_{i_{j}} =p_{i_{j}}q_{i_{j}}

3. n_{i_{j}}的位长等于安全参数 κ 。

4. p_{i_{j}}，q_{i_{j}}的位长为相同程度。

5. e_{i_{j}}与Φ(n_{i}）互为质数。

6. d_{i_{j}}=e_{i_{j}} -1 mod Φ(n_{i}）

其中，这里Φ(n_{i}）为 1 以上不满 n_{i}且与 n_{i}互为质数的整数的个数。生成满足该性质(pk_{i},(sk_{i}）的方法，例如记载在非专利文献 2「Alfred J. Menezes Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press.」（http://www.cacr.math. uwaterloo. ca/hac/）中。

从安全性的观点来说，最好能够均对 e_{i_{j}}是否与Φ(n_{i}）互为质数进行确认。作为能够进行该确认的方法，有使 e_{i_{j}}为比 n_{i}大的质数的方法。但 e_{i_{j}}不一定必须满足该性质。

对各个 j=1,…,m,秘密密钥存储装置 i_{j}-5 存储秘密密钥 sk_{i_{j}}，公开密钥存储装置 i_{j}-3 存储公开密钥 pk_{1},…,pk_{m}。

对密钥合法性检验装置 i_{m}-4 的动作进行说明。密钥合法性检验装置 i_{m}-4 是确认公开密钥 pk_{i_{1}},…, pk_{i_{m-1}}的合法性的装置。

为了确认合法性，首先，从密钥存储装置 i_{m}-3 读入 pk_{i_{1}},…, pk_{i_{m-1}}，确认 pk_{i_{1}},…, pk_{i_{m-1}}全部都不同。但在 m=1 的情况下，不进行确认。

从安全性的观点出发，希望也对 e_{i_{j}}与Φ(n_{i}）互为质数进行确认，但也可以省略该确认。

对签名装置 i_{m}的动作进行说明。对照图 2、图 3，对如下方法进行说明：将消息 M_{1},…, M_{m}以及由签名装置 i_{1} ,…,i_{m-1}使用公开密钥 pk_{i_{1}},…, pk_{i_{m-1}}所生成的针对消息 M_{1},…, M_{m-1}的签名句 u_{i_{m-1}}，输入给了签名装置 i_{m}时，签名装置 i_{m}在消息 M_{m}中进行签名。

签名装置 i_{m}首先通过输入单元 S1B101，读入 M_{1},…, M_{m}、pk_{i_{1}},…, pk_{i_{m}}、sk_{i_{m}}、u_{i_{m-1}}，并存储到存储介质 S1B108 中(S1F100）。其中，在 m=1 的情况下，满足 u_{i_{0}}=0。

接下来，签名装置 i_{m}将 u_{i_{m-1}}、M_{1},…, M_{m-1}、pk_{i_{1}},…, pk_{i_{m-1}}发送给检验装置 i_{m}-2。检验装置 i_{m}-2 检验签名句 u_{i_{m-1}}的合法性 （S1B101,S1F102）。此时，检验装置 i_{m}-2 将 pk_{i_{1}},…, pk_{i_{m-1}}发送给密钥合法性检验装置 i_{m}-4。密钥合法性检验装置 i_{m}-4 对密钥的合法性进行检验（S1B102,S1F101）。设在 m=1 的情况下，只确认出 u_{i_{0}}=0。

从安全性的观点来说，希望进行所述 u_{i_{m-1}}的检验与密钥合法性检验，但为了实现高效化，可以省略其中一方或双方的操作。

接下来，签名装置 i_{m}通过 T_{m}计算单元 S1B103，从存储介质 S1B108 读入必要的数据，计算出 T_{m} = M_{1}‖…‖M_{m}‖pk_{i_{1}}‖…‖pk_{i_{m}} （S1F103）。一旦计算结束，T_{m}计算单元 S1B103 便在存储介质 S1B108 中写入 T_{m}。

接下来，签名装置 i_{m}通过异或单元 S1B104，从存储介质 S1B108 读入必要的数据，计算 U=H（T_{m}）○u_{i_{m-1}}，并将计算结果存储到存储介质 S1B108 中（S1F104）。这里，H 为输出与所输入的位数相同的散列（hash）值的散列函数。

接下来，签名装置 i_{m}通过第一变换单元 S1B105，从存储介质

S1B108 读入输入给签名装置 i_{m}的数据，首先判断 U 是否小于 n_{i_{m}}（S1F105）。如果 U＜n_{i_{m}}，签名装置 i_{m}便通过第一变换单元 S1B105 计算出 v= u^{d_{i_{m}}} mod n_{i_{m}}，并将计算结果写入到存储介质 S1B108 中（S1F106）。反之，如果 U≧n_{i_{m}}，签名装置 i_{m}便通过第一变换单元 S1B105，设为 v=u，将计算结果写入到存储介质 S1B108 中（S1F107）。

接下来，签名装置 i_{m}通过双向单射变换单元 S1B106，从存储介质 S1B108 读入必要的数据，计算出 v'=v + n_{i_{m}} mod 2^{ κ }，并将计算结果写入到存储介质 S1B108 中（S1F108）。

接下来，签名装置 i_{m}通过第二变换单元 S1B107，从存储介质 S1B108 读入必要的数据，判断 v'是否小于 n_{i_{m}}（S1F109）。如果 v'＜n_{i_{m}}，签名装置 i_{m}便通过第二变换单元 S1B107，计算出 u_{i_{m}} = v'^{d_{i_{m}}} mod n_{i_{m}}，并将计算结果写入到存储介质 S1B108 中（S1F1010）。反之，如果 v'≧n_{i_{m}}，签名装置 i_{m}便通过第二变换单元 S1B107 计算出 u_{i_{m}} = v'，将计算结果写入到存储介质 S1B108 中（S1F1011）。

最后，签名装置 i_{m}通过输出单元 S1B109，从存储介质 S1B108 读入 u_{i_{m}}并输出（S1F1012）。

这样，签名装置 i_{m}判断所输入的签名句 u_{i_{m-1}}是否超过了模量 n_{i_{m}}，在超过了的情况下，不进行操作，在没有超过的情况下，执行进行以 RSA 方式为准据的签名的第 1 操作，对该第 1 操作的结果执行对其作用向大至模量 n_{i_{m}}的方向映射的函数的第 2 操作，判断该第 2 操作的结果是否超过了模量 n_{i_{m}}，在超过了的情况下，不进行操作，在没有超过的情况下，执行进行以 RSA 方式为准据的签名的第 3 操作。根据签名句 u_{i_{m-1}}的值，存在 RSA 签名被实施两次的的冗长，但是也能够根据签名值 u_{i_{m}}的值来唯一决定所实施的签名操作，因此不需要附加非专利文献 1 中那样的控制位。

接下来，参照图 4、图 5，对检验装置 i_{m}-2 检验签名句 u_{m-1}的方法进行说明。

检验装置 i_{m}-2，首先通过输入单元 V1B100 从公开密钥存储装置

i_{m}-3 读入 pk_{i_{1}},…,pk_{i_{m-1}}，进而读入消息 M_{1},…,M_{m-1} （V1F100）。所读入的数据由输入单元 V1B100 写入到存储介质 V1B1010 中。

接下来，检验装置 i_{m}-2 通过输入单元 V1B100 将 pk_{i_{1}},…,pk_{i_{m-1}}发送给密钥检验装置 i_{m}-4，请求其检验公开密钥 pk_{i_{1}},…,pk_{i_{m-1}}的合法性 （V1B101, V1F101）。

接下来，检验装置 i_{m}-2 为了从前一个签名装置追溯到第一个签名装置而顺次进行检验处理，首先，通过 j 初始化单元 V1B102，将 m-1 设置为对正在检验哪个签名装置的签名进行管理的变量 j（V1F102）。

接下来，检验装置 i_{m}-2 通过 j 判断单元 V1B103，判断是否为 j>0 (V1F103）。

下面，对 j>0 的情况下的检验装置 i_{m}-2 的动作进行说明。关于不是 j>0 的情况下的动作，将在后面说明。

接下来，检验装置 i_{m}-2 通过第二变换单元 V1B104，首先从存储介质 V1B1010 读入必要的数据，判断是否为 u_{i_{j}}<n_{i_{j}} （V1F104）。

之后，如果是 u_{i_{j}}<n_{i_{j}}，检验装置 i_{m}-2 便通过第二变换单元 V1B104，计算出 v'=u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}，并将计算结果写入到存储介质 V1B1010 中（V1F105）。

反之，如果不是 u_{i_{j}}<n_{i_{j}}，检验装置 i_{m}-2 便通过第二变换单元 V1B104，将 v'=u_{i_{j}作为计算结果，写入到存储介质 V1B1010 中（V1F106）。

接下来，检验装置 i_{m}-2 通过双向单射计算单元 V1B105，从存储介质 V1B1010 读入必要的数据，计算出 v=v'- n_{i_{m}} mod 2^{ κ }，将计算结果写入到存储介质 V1B1010 中（V1F107）。

接下来，检验装置 i_{m}-2 通过第一变换单元 V1B106，从存储介质 V1B1010 读入必要的数据，首先判断是否为 v<n_{i_{j}} （V1F108）。

于是，如果是 v<n_{i_{j}}，检验装置 i_{m}-2 便通过第一变换单元 V1B106 计算出 U=v^{e_{i_{j}}} mod n_{i_{j}}，并将计算结果写入到存储介质 V1B1010 中（V1F109）。

另一方面，如果 v<n_{i_{j}}，检验装置 i_{m}-2 便通过第一变换单元 V1B106，将 U=v 作为计算结果写入到存储介质 V1B1010 中（V1F1010）。

接下来，检验装置 i_{m}-2 通过 T_{j}计算单元 V1B107，从存储介质 V1B1010 读入必要的数据，并计算出 T_{j} = M_{1}||…||M_{j}||pk_{i_{1}}||…||pk_{i_{j}}，将计算结果写入到存储介质 V1B1010 中（V1F1011）。

检验装置 i_{m}-2 接着通过 u 计算单元 V1B108，从存储介质 V1B1010 读入必要的数据，计算出 u_{i_{j-1}}=H(T_{j}）○U，并将计算结果写入到存储介质 V1B1010 中（V1F1012）。

接下来，检验装置 i_{m}-2 通过 j 减少单元 V1B109，使得 j=j-1（V1F1013）。

之后，检验装置 i_{m}-2 再次通过 j 判断单元 V1B103，判断是否为 j>0（V1F103）。

如果 j>0，检验装置 i_{m}-2 便进行步骤 V1F104 之后的处理。

如果 j=0，检验装置 i_{m}-2 便通过 u 判断单元 V1B1011，从存储介质 V1B1010 读入必要的数据，调查是否为 u=0 （V1F1014）。

之后，如果 u=0，检验装置 i_{m}-2 便通过 accept 输出单元 V1B1012，输出表示检验成功的 accept （V1F1015），如果不是这样，便通过 reject 输出单元 V1B1013，输出表示检验失败的 reject （V1F1016）。

另外，设图 5 的虚线所包围的部分的操作为 f(x), g(x), h(x), Φ(x)。

也即：

f（x）= x^{e_{i_{j}}} mod n_{i_{j}}　　if x < n_{i_{j}}

= x　　otherwise.

g（x）= x^{e_{i_{j}}} mod n_{i_{j}}　　if x < n_{i_{j}}

= x　　otherwise.

Φ(x)= x + n_{i_{j}} mod 2^{κ}

h(x)= g(Φ(x))。

于是，图 3 的虚线所包围的部分的操作 f^{-1}(x), g^{-1} (x), h^{-1} (x), Φ^{-1} (x)，分别是 f(x), g(x), h(x), Φ(x)的反函数。

因此，本实施方式中的签名装置 i_{m}，通过计算公式：u_{i_{m}}

=(g_{m}^{-1}(φ^{-1}(f_{m}^{-1}(H(T_{m})○u_{i_{m-1}}))))，生成签名句。另外，本实施方式中的检验装置 i_{m}-2，通过计算公式 u_{i_{m-2}}=H(T_{m-1})○(f_{m-1}(φ(g_{m-1}(u_{i_{m-1}})))))，求出成为前一个签名装置的输入的签名句，之后重复进行同样的处理，直到达到最初的签名装置，求出输入的初始值，并调查所求出的初始值是否与预先设定的初始值（本实施方式的情况下为值 0）相一致。

接下来，对本实施方式的效果进行说明。

第 1 效果是，签名长度不依赖于签名装置的数目。其原因是，签名前的数据与签名后所生成的数据位数不变。

第 2 效果是，能够在每次签名时变更签名装置的顺序。其原因与第 1 效果的情况下相同，签名前的数据与签名后所生成的数据位数不变。因此，对各个签名装置的输入是一定的，跟该签名装置是第几个进行签名的无关，因此不管是第几个，都能够通过相同的操作来签名。但需要通过某种形式，将按照什么样的顺序进行了签名通知给检验装置。

第 3 效果是：与签名装置勾结的攻击者，无法伪造出从线路中途的“诚实（honest）”的签名装置中通过的签名句。其原因在于，不管对签名装置的输入 u 是什么，签名时进行两次的 RSA 计算中的至少一方的 u 变化。

第 4 效果是，在开始系统的使用的阶段，不需要知道签名装置的数目 m，这是由于，即使签名装置的数目 m 在使用中动态变化，也能够正常使用。其原因是，签名装置的数目为 m+1 台时的签名顺序，是在进行了签名装置的数目为 m 台时的签名顺序之后再进行一次同样的签名操作，签名的操作方法不依赖于签名装置的数目 m。

另外，以上的第 1 实施方式中，使用很典型的例子即 RSA 函数进行了说明，但更普通的是，只要有存在于{0,1}^{κ}中的部分集合 X，并且满足以下条件(1)、(2)，就跟第 1 实施方式一样，能够实现一种签名长度不依赖于签名者的人数且安全的签名方式。

（1）f，g 是带陷阱门的单向性置换，且 X 既包括在 f 的定义区中又包括在 g 的定义区中。

（2）φ、φ、φ^{-1}都是在多项式时间中能够计算的{0,1}^{κ}上的双向单射，将{0,1}^{κ}\X 映射到 X 中。

这里，带陷阱门的单向性置换，是满足以下 4 个性质的函数。

1）计算 f 较为容易。

2)对于不知道陷阱门(也称作秘密密钥)的人来说,很难计算出 f^{-1}。

3）对于知道陷阱门的人来说，计算 f^{-1}很容易。

4）是双向单射（全单射）。

进而，一般来说存在位于{0,1}^{κ}中的部分集合 X，如果满足以下条件（1）、（2），就与第 1 实施方式一样，能够实现签名长度不依赖于签名者的人数且安全的签名方式。

（1） f 是带陷阱门的单向性置换，且 X 包括在 f 的定义区中。

（2） h 是带陷阱门的单向性置换，且{0,1}^{κ}＼X 包括在 h 的定义区中。

第 2 实施方式

参照图 6，本发明的第 2 实施方式，由签名装置 i_{1},…,i_{m}、检验装置 i_{1}-2,…,i_{m}-2、公开密钥存储装置 i_{1}-3,…,i_{m}-3、密钥合法性检验装置 i_{1}-4,…,i_{m}-4、以及秘密密钥存储装置 i_{1}-5,…,i_{m}-5 构成。

参照图 7，签名装置 i_{m}由输入单元 S1B100、T_{m}计算单元 S1B103、异或计算单元 S1B104、第一变换单元 S1B105、双向单射变换单元 S1B106、第二变换单元 S1B107、存储介质 S1B108、输出单元 S1B109 以及 w 设置单元 S2B100 构成。其他的签名装置也具有与签名装置 i_{m}相同的构成。

参照图 9，检验装置 i_{m}-2 由输入单元 V2B200、T_{m-1}计算单元 V2B202、v"计算单元 V2B203、第二变换单元 V2B204、双向单射变换单元 V2B205、第一变换单元 V2B206、u 判断单元 V2B207、accept 输出单元 V2B208、reject 输出单元 V2B209 以及存储介质 V2B2010 构成。其他的检验装置也具有与检验装置 i_{m}-2 相同的构成。

对本实施方式进行概述。首先，给签名装置 i_{1}输入签名装置 i_{1}的公开密钥秘密密钥对、初始值 u_{i_{0}}、以及消息 M_{1}。签名装置 i_{1}使用 u_{i_{0}}生成针对消息 M_{1}的签名句 u_{i_{1}}。并且将初始值 u_{i_{0}}作为辅助信息 w_{i_{1}}而生成，输出 u_{i_{1}}与 w_{i_{1}}

之组。接下来，给签名装置 i_{2}输入签名装置 i_{2}的公开密钥秘密密钥对、u_{i_{1}}与 w_{i_{1}}之组、以及消息 M_{2}。签名装置 i_{2}使用 u_{i_{1}}，生成针对消息 M_{2}的签名句 u_{i_{2}}，并且将 u_{i_{1}}作为辅助信息 w_{i_{2}}而生成，输出 u_{i_{2}}与 w_{i_{2}}之组。之后，顺次给签名装置 i_{j}输入签名装置 i_{j}的公开密钥秘密密钥对、前一个签名装置所输出的签名句 u_{i_{j-1}}、辅助信息 w_{i_{j-1}}、以及消息 M_{j}，签名装置 i_{j}使用这些生成签名句 u_{i_{j}}与辅助信息 w_{i_{j}}之组。u_{i_{j}}是与第 1 实施方式相同的签名句，是表示签名装置 i_{1}在消息 M_{1}中进行了签名，签名装置 i_{2}在消息 M_{2}中进行了签名，…、签名装置 i_{j}在消息 M_{j}中进行了签名的数据。

另外，w_{i_{j}}是用来让签名句 u_{i_{j}}的检验能够简单地进行的辅助信息，本实施方式的情况下，是成为签名装置 i_{j}的输入的签名句 u_{i_{j-1}}本身。对各个 j，若给检验装置 i_{j}输入签名装置 i_{1},…,i_{j}的公开密钥与消息 M_{1},…,M_{j-1}，以及签名句 u_{i_{j-1}}，w_{i_{j-1}}，则检验装置 i_{j}运用辅助信息 w_{i_{j-1}}，对 u_{i_{j-1}}是否是使用签名装置 i_{1},…,i_{j-1}的公开密钥生成了针对消息 M_{1},…,M_{j-1}的签名句进行检验。

本实施方式的系统目标与第 1 实施方式一样，是生成签名句 u_{i_{m}}，也即表示签名装置 i_{1}在消息 M_{1}中进行了签名，签名装置 i_{2}在消息 M_{2}中进行了签名，…，签名装置 i_{m}在消息 M_{m}中进行了签名的数据。

另外，与第 1 实施方式一样，另外，本实施方式系统的应用开始阶段，也不需要知道签名装置的数目 m。签名装置的数目 m 可以在应用中动态变化。另外，签名装置 i_{1},…,i_{m}的动作完全相同。检验装置、公开密钥存储装置、密钥合法性检验装置、秘密密钥存储装置也基本都进行相同的动作。

接下来以与第 1 实施方式的不同的为中心，对本实施方式进行详细说明。

签名装置 i_{ j }的公开密钥 pk_{i}、秘密密钥 sk_{i}，与第 1 实施方式一样被生成，对各个 j=1,…,m，秘密密钥存储装置 i_{j}-5 存储秘密密钥

sk_{i_{j}}，且公开密钥存储装置 i_{j}-3 存储公开密钥 pk_{1},…,pk_{m}。

密钥合法性检验装置的动作与第 1 实施方式相同。

在将消息 M_{1},…, M_{m}、签名装置 i_{1} ,…,i_{m-1}使用公开密钥 pk_{i_{1}},…, pk_{i_{m-1}}所生成的针对消息 M_{1},…, M_{m-1}的签名句 u_{i_{m-1}}、以及辅助信息 w_{i_{m-1}}输入给了签名装置 i_{m}时的、签名装置 i_{m}在消息 M_{m}中进行签名的方法中，添加了生成辅助信息的顺序这一点，与第 1 实施方式不同，此外均与第 1 实施方式相同。对照图 7、图 8 进行说明，本实施方式的情况下，签名装置 i_{m}接着步骤 S1F102 的处理，通过 w 设置单元 S2B100，计算出 w_{i_{m}}=u_{i_{m-1}}，并将计算结果写入到存储介质 S1B108 中（S2F100）。写入到了存储介质 S1B108 中的辅助信息 w_{i_{m}}，与由输出单元 S1B109 通过与第 1 实施方式相同的顺序所生成并写入在存储介质 S1B108 中的签名句 u_{i_{m}}一起被读出、输出（S1F1012'）。

接下来，对照图 9、图 10，对检验装置 i_{m}-2 检验签名句 u_{m-1}的方法进行说明。

检验装置 i_{m}-2，首先通过输入单元 V1B200 从公开密钥存储装置 i_{m}-3 读入 pk_{i_{1}},…,pk_{i_{m-1}}，进而读入消息 M_{1},…, M_{m-1}，并写入到存储介质 V1B2010 中。（V1F200）。

接下来，检验装置 i_{m}-2 通过输入单元 V2B200，将 pk_{i_{1}},…,pk_{i_{m-1}}发送给密钥检验装置 i_{m}-4，请求其检验公开密钥 pk_{i_{1}},…,pk_{i_{m-1}}的合法性 （V2F201)。

接下来，检验装置 i_{m}-2 通过 T_{m-1}计算单元 V2B202，从存储介质 V2B2010 读入必要的数据，计算出 T_{m-1} = M_{1}‖…‖M_{m-1}‖pk_{i_{1}}‖…‖pk_{i_{m-1}}，并将计算结果 T_{m-1}保存到存储介质 V2B2010 中（V2F202）。

接下来，检验装置 i_{m}-2 通过 v"计算单元 V2B203，从存储介质 V2B2010 读入必要的数据，计算出 v"=H（T_{m-1}）○u_{i_{m-1}}，并将计算结果 v"保存到存储介质 V2B2010 中（V2F203）。

接下来，检验装置 i_{m}-2 通过第二变换单元 V2B204，从存储介质 V2B2010 读入必要的数据，判断是否为 v"<n_{i_{m-1}} （V2F204）。如

果是 v"<n_{i_{m-1}}，检验装置 i_{m}-2 便通过第二变换单元 V2B204 计算出 v'=v"^{e_{i_{m-1}}} mod n_{i_{m-1}}，并将计算结果 v'保存到存储介质 V2B2010 中（V2F205）。另外，如果不是 v"<n_{i_{m-1}}，检验装置 i_{m}-2 便设为 v'=v"，并将计算结果 v'保存到存储介质 V2B2010 中（V2F206）。

接下来，检验装置 i_{m}-2 通过双向单射变换单元 V2B205，从存储介质 V2B2010 读入必要的数据，计算出 v=v' - n_{i_{m-1}} mod 2^{ κ }，并将计算结果 v 保存到存储介质 V2B2010 中（V2F207）。

接下来，检验装置 i_{m}-2 通过第一变换单元 V2B206，从存储介质 V2B2010 读入必要的数据，判断是否是 v<n_{i_{m-1}} （V2F208）。如果 v<n_{i_{m-1}}，检验装置 i_{m}-2 便通过第一变换单元 V2B206，计算出 u _{i_{m-2}} = v^{e_{i_{m-1}}} mod n_{i_{m-1}}}，并将计算结果 u _{i_{m-2}}保存到存储介质 V2B2010 中（V2F209）。另外，如果不是 u_{i_{m-2}}<n_{i_{m-1}}，检验装置 i_{m}-2 便设 u _{i_{m-1}}）=v，将计算结果 u _{i_{m-2}}保存到存储介质 V2B2010 中（V2F2010）。

接下来，检验装置 i_{m}-2 通过 u 判断单元 V2B2011，从存储介质 V2B2010 读入必要的数据，调查是否为 u_{i_{m-2}}} =w_{i_{m-1}}（V2F2011）。如果是 u_{i_{m-2}}} =w _{i_{m-1}}，检验装置 i_{m}-2 便通过 accept 输出单元 V2B208 输出 accept （V2F2012），如果不是，便通过 reject 输出单元 V2B209 输出 reject （V2F2013）。

接下来，对本实施方式的效果进行说明。

第 1 效果是，签名长度不依赖于签名装置的数目。其原因是，签名前的数据与签名后所生成的数据位数不变。但与第 1 实施方式相比，数据长度增加了辅助信息的部分。

第 2 效果是，与第 1 实施方式相比，能够削减检验计算的计算量。其原因是，第 1 实施方式中，最终需要求出初始值，因此需要与已进行过签名签名的签名装置的数目成正比的检验计算，与此相对，本实施方式中，成为前一个签名装置的输入的签名句被作为辅助信息传送过来，因此只需要进行 1 签名装置份量的检验计算。但本实施方式需要以前一个签名装置能够信赖为前提，与不需要这样的前提就能够证明安全性的第 1 实施方式

相比，安全性降低。

此外，还起到了与第 1 实施方式相同的效果。

另外，本实施方式中，作为与签名句 u_{i_{j}}成组的辅助信息 w_{i_{j}}，采用成为签名装置 i_{j}的输入的签名句 u_{i_{j-1}}本身，但也可以将 h 作为输出与输入位数相同的散列值的的给定的散列函数，并将 u_{i_{j-1}}的散列值 h（u_{i_{j-1}}）作为辅助信息 w_{i_{j}}。另外，对本实施方式也能够进行与第 1 实施方式相同的附加变更。

以上对本发明的实施方式进行了说明，但本发明并不仅限于以上实施方式，还可以进行其他各种附加变更。另外，本发明的签名装置与检验装置，其所具有的功能当然能够硬件实现，还可以通过计算机与程序来实现。程序在磁盘或半导体存储器等计算机可读存储介质中进行记录并被提供，在计算机的启动等时读入到计算机中，控制该计算机的动作，通由此使该计算机起到上述各个实施方式中的签名装置以及检验装置的功能。

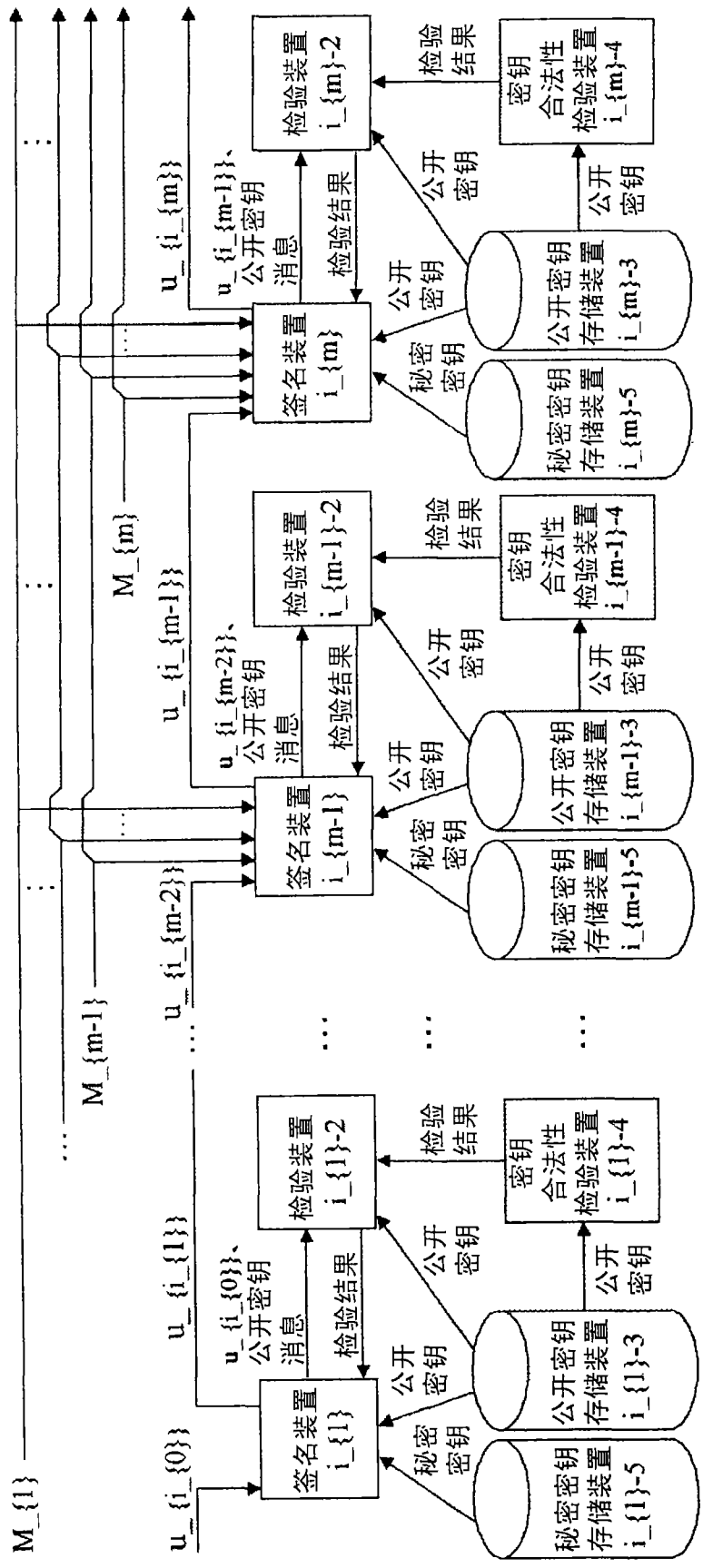

M_{1}
M_{m-1}
M_{m}
u_i_{0}
u_i_{1}
u_i_{m-2}
u_i_{m-1}
u_i_{m}
签名装置 i_{1}
检验装置 i_{1}-2
密钥合法性检验装置 i_{1}-4
公开密钥存储装置 i_{1}-3
秘密密钥存储装置 i_{1}-5
签名装置 i_{m-1}
检验装置 i_{m-1}-2
密钥合法性检验装置 i_{m-1}-4
公开密钥存储装置 i_{m-1}-3
秘密密钥存储装置 i_{m-1}-5
签名装置 i_{m}
检验装置 i_{m}-2
密钥合法性检验装置 i_{m}-4
公开密钥存储装置 i_{m}-3
秘密密钥存储装置 i_{m}-5
u_i_{0}、公开密钥消息
u_i_{m-2}、公开密钥消息
u_i_{m-1}、公开密钥消息
检验结果
公开密钥
秘密密钥

图 1

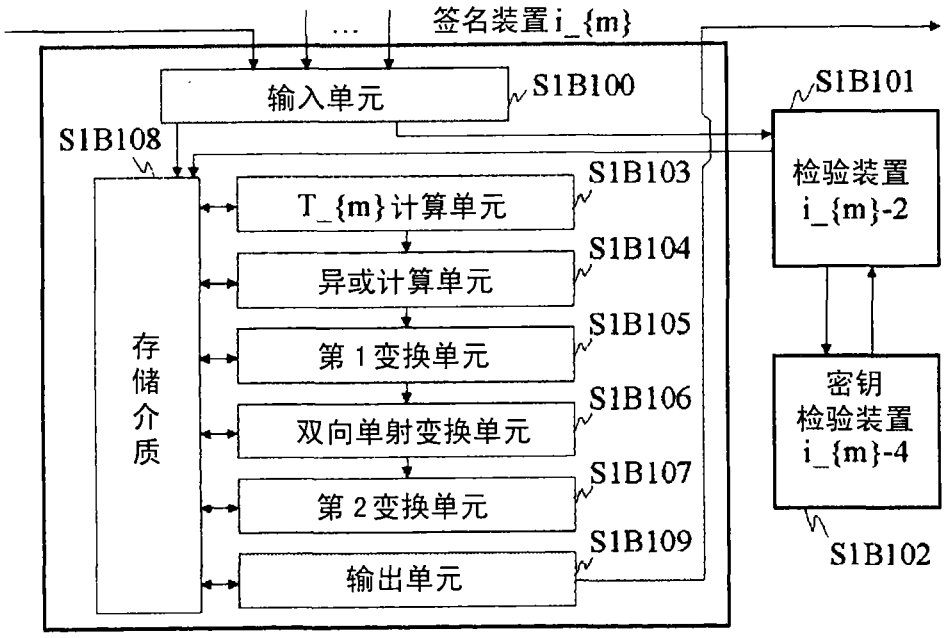

签名装置i_{m}
...
输入单元
S1B100
S1B101
S1B108
检验装置
i_{m}-2
T_{m}计算单元
S1B103
异或计算单元
S1B104
第1变换单元
S1B105
双向单射变换单元
S1B106
第2变换单元
S1B107
输出单元
S1B109
存储介质
密钥
检验装置
i_{m}-4
S1B102

图 2

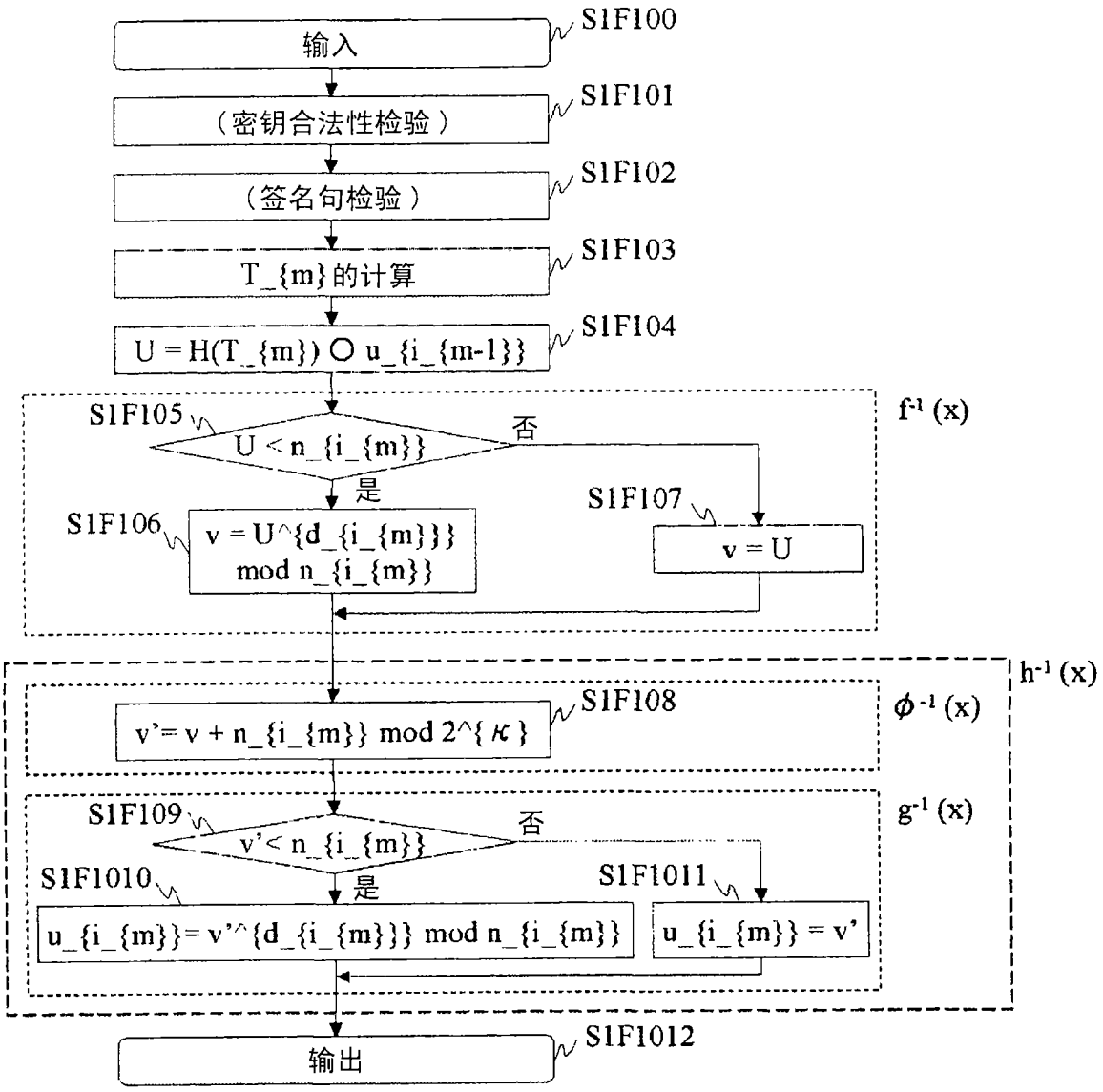

输入
S1F100
（密钥合法性检验）
S1F101
（签名句检验）
S1F102
T_{m}的计算
S1F103
U = H(T_{m}) ○ u_{i_{m-1}}
S1F104
S1F105
U < n_{i_{m}}
否
是
S1F106
v = U^{d_{i_{m}}} mod n_{i_{m}}
S1F107
v = U
f-1 (x)
h-1 (x)
S1F108
v'= v + n_{i_{m}} mod 2^{κ}
φ-1 (x)
S1F109
v' < n_{i_{m}}
否
是
S1F1010
u_{i_{m}}= v'^{d_{i_{m}}} mod n_{i_{m}}
S1F1011
u_{i_{m}} = v'
g-1 (x)
输出
S1F1012

图 3

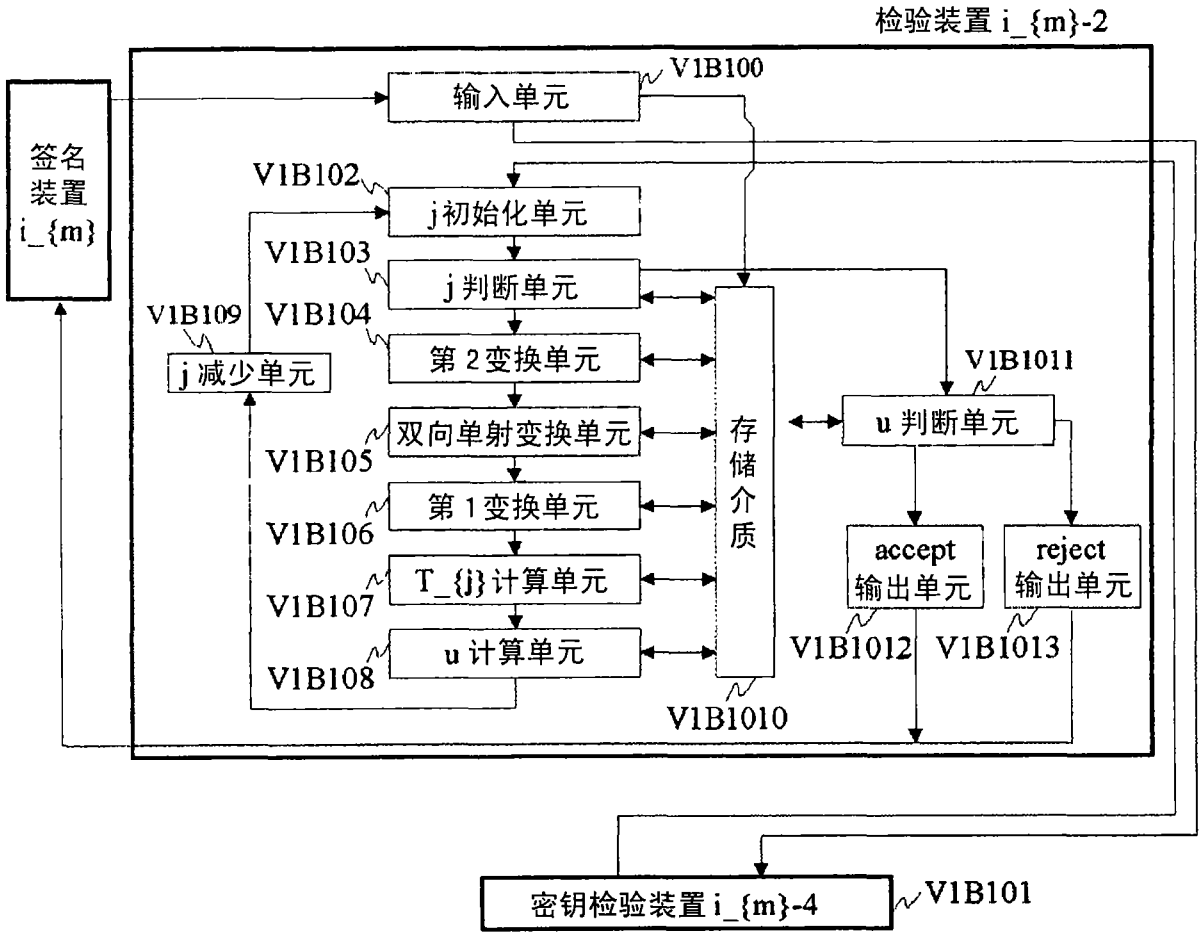

检验装置 i_{m}-2
签名装置 i_{m}
输入单元
V1B100
V1B102
j初始化单元
V1B103
j 判断单元
V1B109
V1B104
j 减少单元
第 2 变换单元
双向单射变换单元
V1B105
第 1 变换单元
V1B106
T_{j}计算单元
V1B107
u 计算单元
V1B108
存储介质
V1B1010
V1B1011
u 判断单元
accept 输出单元
reject 输出单元
V1B1012
V1B1013
密钥检验装置 i_{m}-4
V1B101

图 4

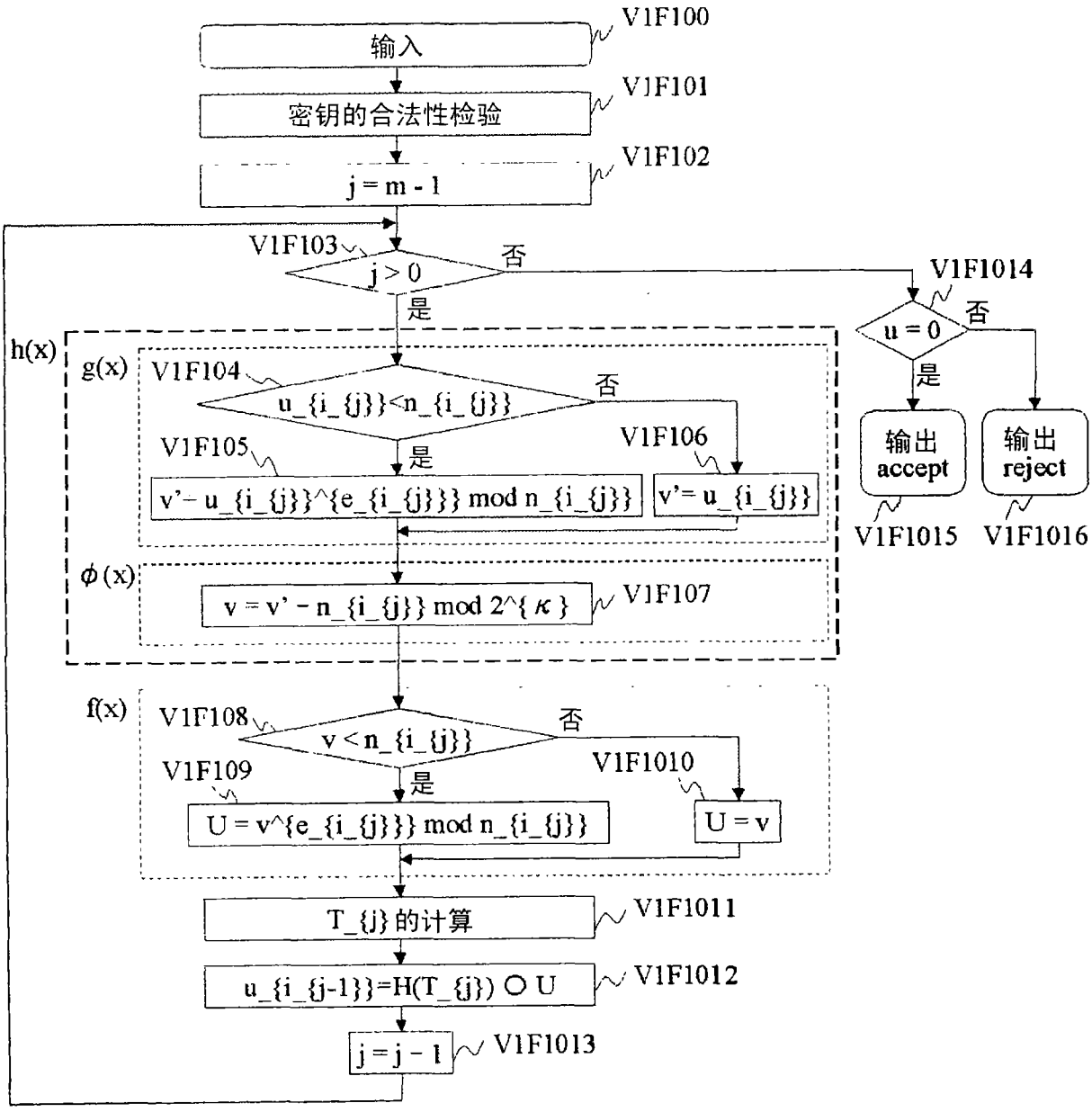

输入
V1F100
密钥的合法性检验
V1F101
j = m - 1
V1F102
V1F103
j > 0
否
是
V1F1014
u = 0
否
是
输出 accept
输出 reject
V1F1015
V1F1016
h(x)
g(x)
V1F104
u_{i_{j}}<n_{i_{j}}
否
是
V1F105
V1F106
v'= u_{i_{j}}^{e_{i_{j}}} mod n_{i_{j}}
v'= u_{i_{j}}
φ(x)
v = v' - n_{i_{j}} mod 2^{κ}
V1F107
f(x)
V1F108
v < n_{i_{j}}
否
是
V1F109
V1F1010
U = v^{e_{i_{j}}} mod n_{i_{j}}
U = v
T_{j} 的计算
V1F1011
u_{i_{j-1}}=H(T_{j}) ○ U
V1F1012
j = j - 1
V1F1013

图 5

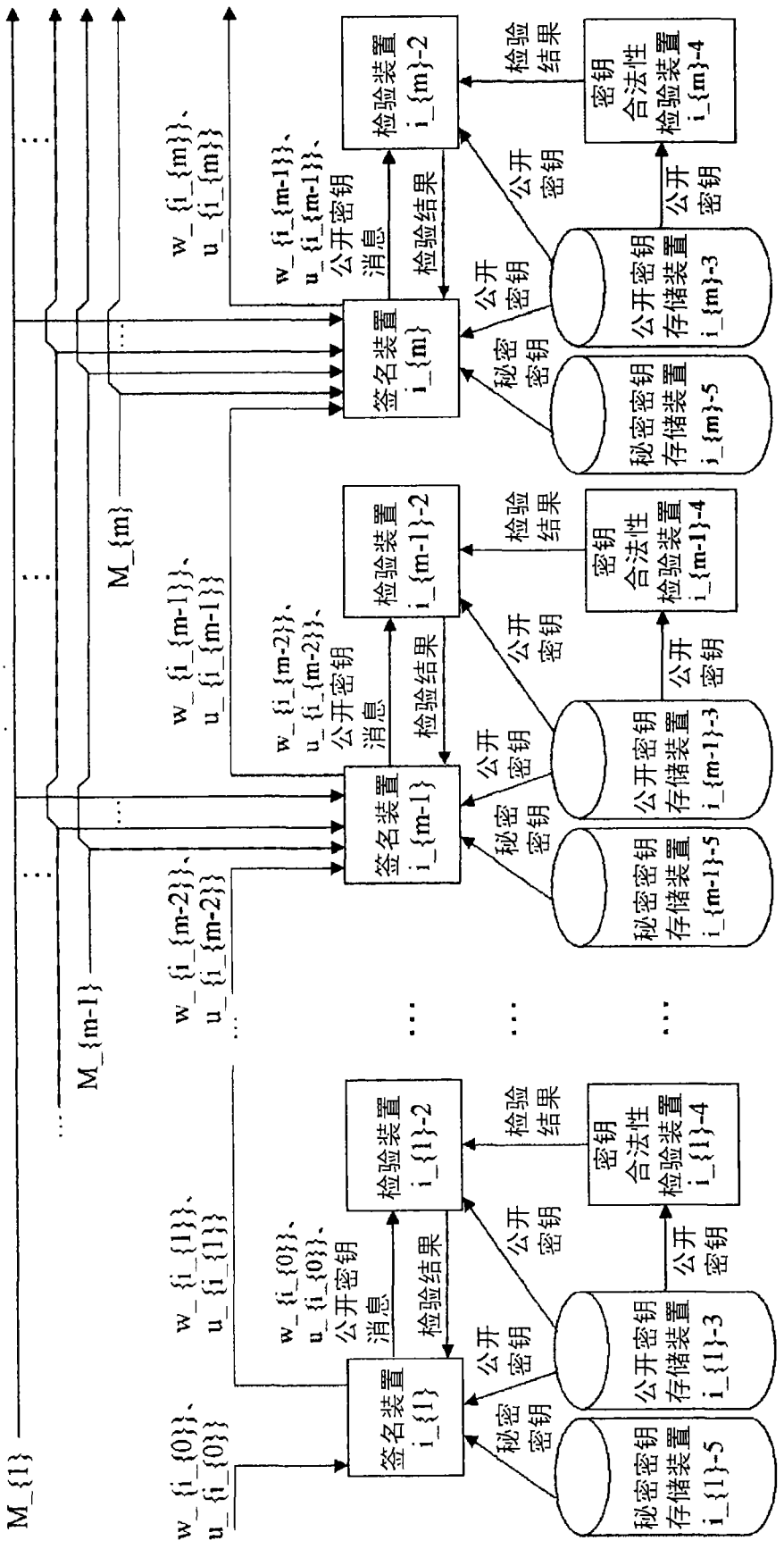

M_{1}
M_{m-1}
M_{m}
w_{i_{0}}、u_{i_{0}}
w_{i_{1}}、u_{i_{1}}
w_{i_{m-2}}、u_{i_{m-2}}
w_{i_{m-1}}、u_{i_{m-1}}
w_{i_{m}}、u_{i_{m}}
签名装置 i_{1}
签名装置 i_{m-1}
签名装置 i_{m}
检验装置 i_{1}-2
检验装置 i_{m-1}-2
检验装置 i_{m}-2
w_{i_{0}}、u_{i_{0}}、公开密钥消息
w_{i_{m-2}}、u_{i_{m-2}}、公开密钥消息
w_{i_{m-1}}、u_{i_{m-1}}、公开密钥消息
检验结果
秘密密钥存储装置 i_{1}-5
公开密钥存储装置 i_{1}-3
密钥合法性检验装置 i_{1}-4
秘密密钥存储装置 i_{m-1}-5
公开密钥存储装置 i_{m-1}-3
密钥合法性检验装置 i_{m-1}-4
秘密密钥存储装置 i_{m}-5
公开密钥存储装置 i_{m}-3
密钥合法性检验装置 i_{m}-4
秘密密钥
公开密钥
检验结果

图 6

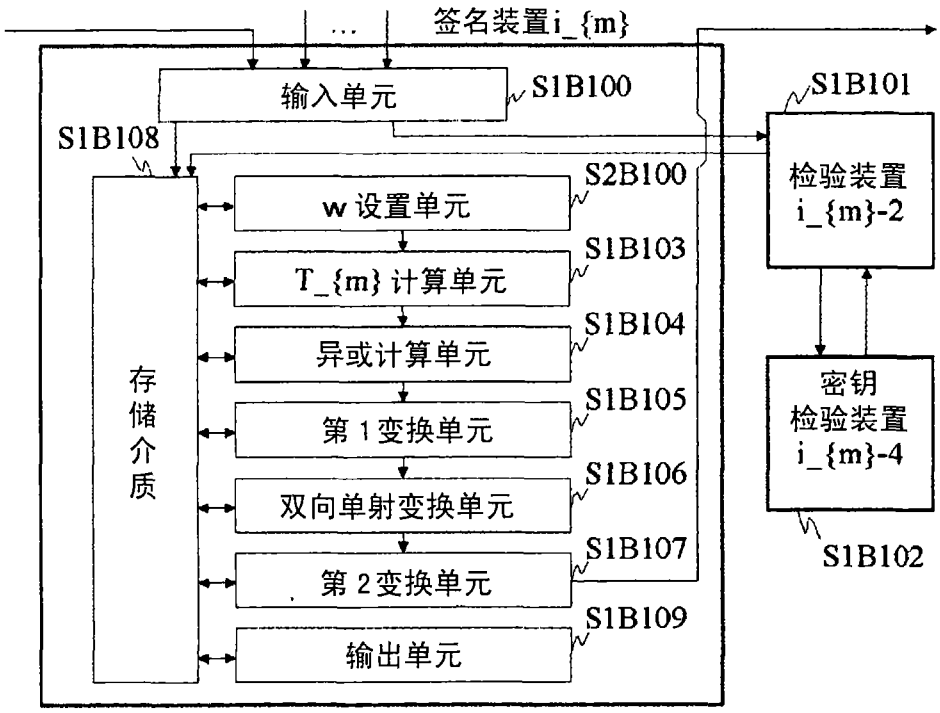

签名装置i_{m}
输入单元
S1B100
S1B101
S1B108
检验装置
i_{m}-2
S2B100
w 设置单元
S1B103
T_{m} 计算单元
S1B104
异或计算单元
S1B105
第 1 变换单元
S1B106
双向单射变换单元
S1B107
第 2 变换单元
S1B109
输出单元
存储介质
密钥
检验装置
i_{m}-4
S1B102

图 7

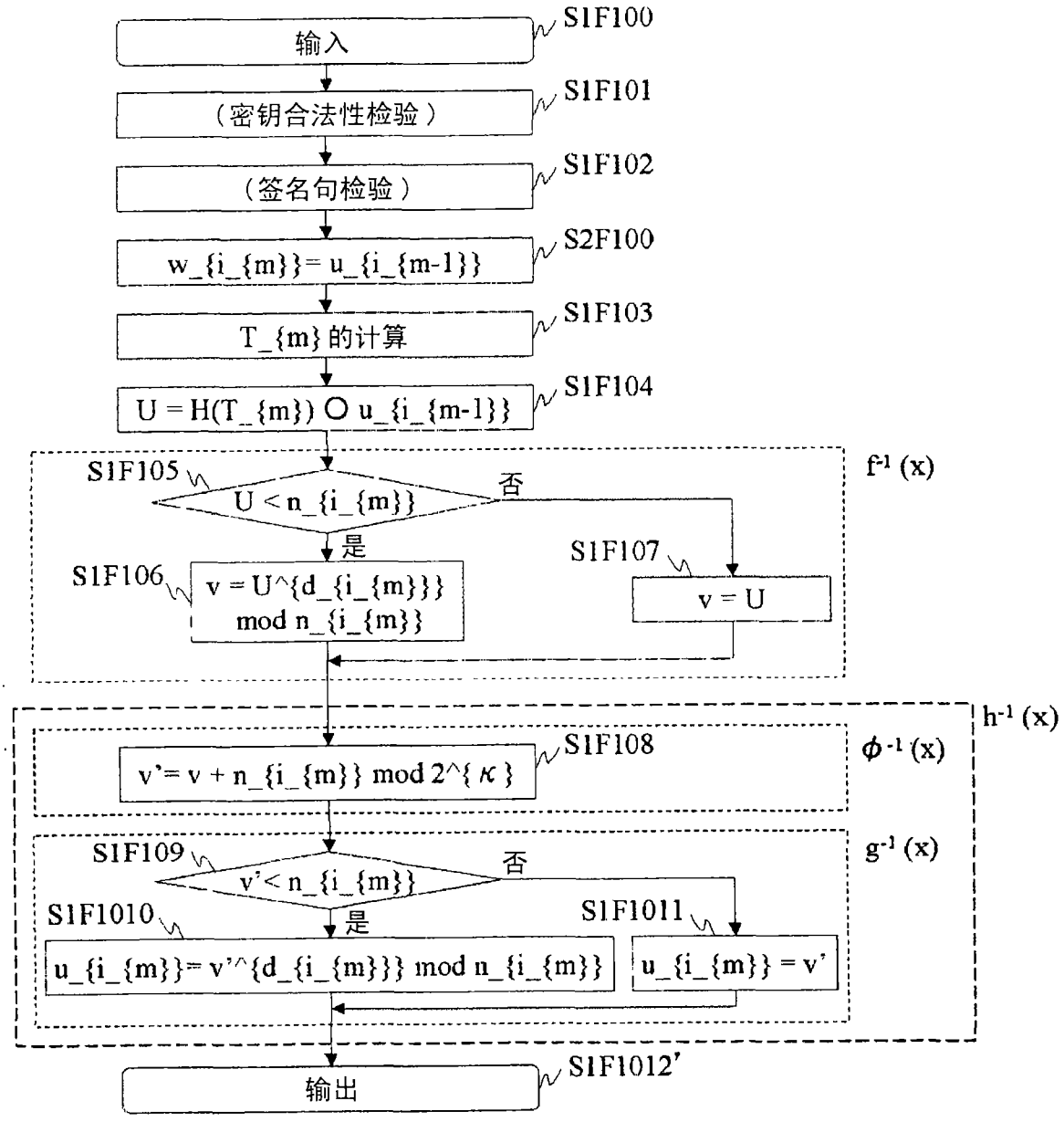

输入
S1F100
（密钥合法性检验）
S1F101
（签名句检验）
S1F102
w_{i_{m}}= u_{i_{m-1}}
S2F100
T_{m}的计算
S1F103
U = H(T_{m}) ○ u_{i_{m-1}}
S1F104
f-1 (x)
S1F105
U < n_{i_{m}}
否
是
S1F106
v = U^{d_{i_{m}}} mod n_{i_{m}}
S1F107
v = U
h-1 (x)
φ-1 (x)
S1F108
v'= v + n_{i_{m}} mod 2^{κ}
g-1 (x)
S1F109
v'< n_{i_{m}}
否
是
S1F1010
S1F1011
u_{i_{m}}= v'^{d_{i_{m}}} mod n_{i_{m}}
u_{i_{m}} = v'
输出
S1F1012'

图 8

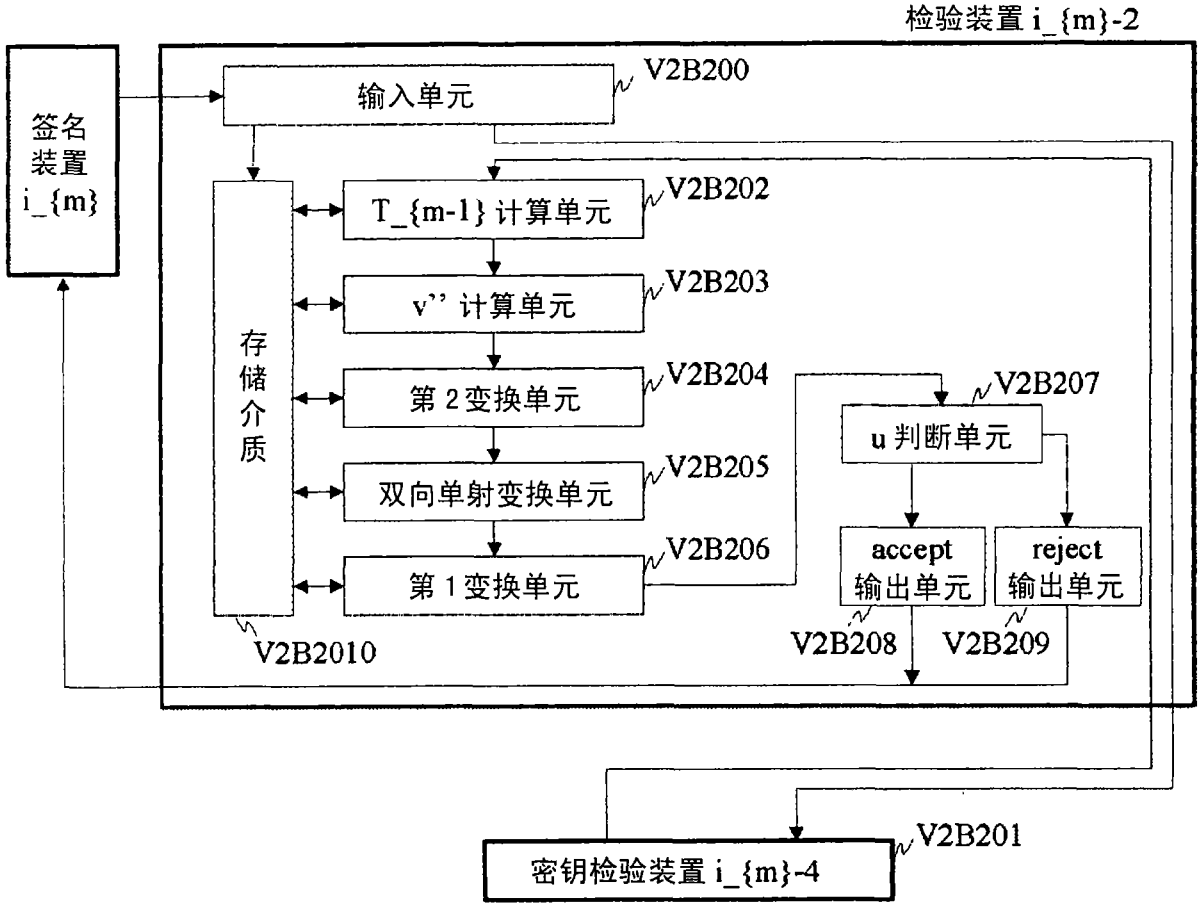

检验装置 i_{m}-2
签名装置 i_{m}
输入单元
V2B200
存储介质
T_{m-1} 计算单元
V2B202
v'' 计算单元
V2B203
第 2 变换单元
V2B204
双向单射变换单元
V2B205
第 1 变换单元
V2B206
V2B2010
u 判断单元
V2B207
accept 输出单元
reject 输出单元
V2B208
V2B209
密钥检验装置 i_{m}-4
V2B201

图 9

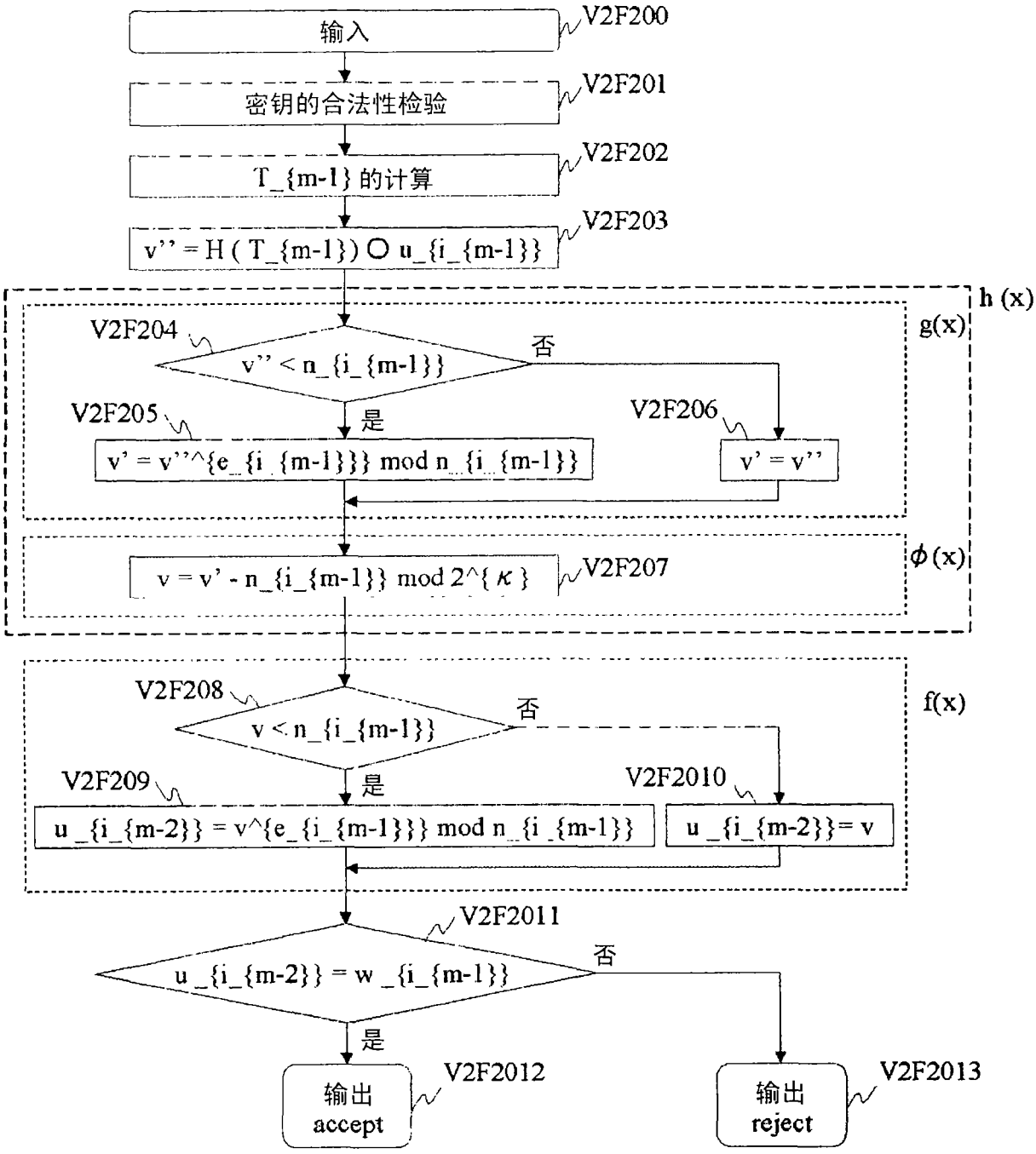

输入
V2F200
密钥的合法性检验
V2F201
T_{m-1} 的计算
V2F202
v'' = H ( T_{m-1}) ○ u_{i_{m-1}}
V2F203
h (x)
g(x)
V2F204
v'' < n_{i_{m-1}}
否
是
V2F205
v' = v''^{e_{i_{m-1}}} mod n_{i_{m-1}}
V2F206
v' = v''
φ(x)
v = v' - n_{i_{m-1}} mod 2^{κ}
V2F207
f(x)
V2F208
v < n_{i_{m-1}}
否
是
V2F209
u_{i_{m-2}} = v^{e_{i_{m-1}}} mod n_{i_{m-1}}
V2F2010
u_{i_{m-2}}= v
V2F2011
u_{i_{m-2}} = w_{i_{m-1}}
否
是
输出 accept
V2F2012
输出 reject
V2F2013

图 10

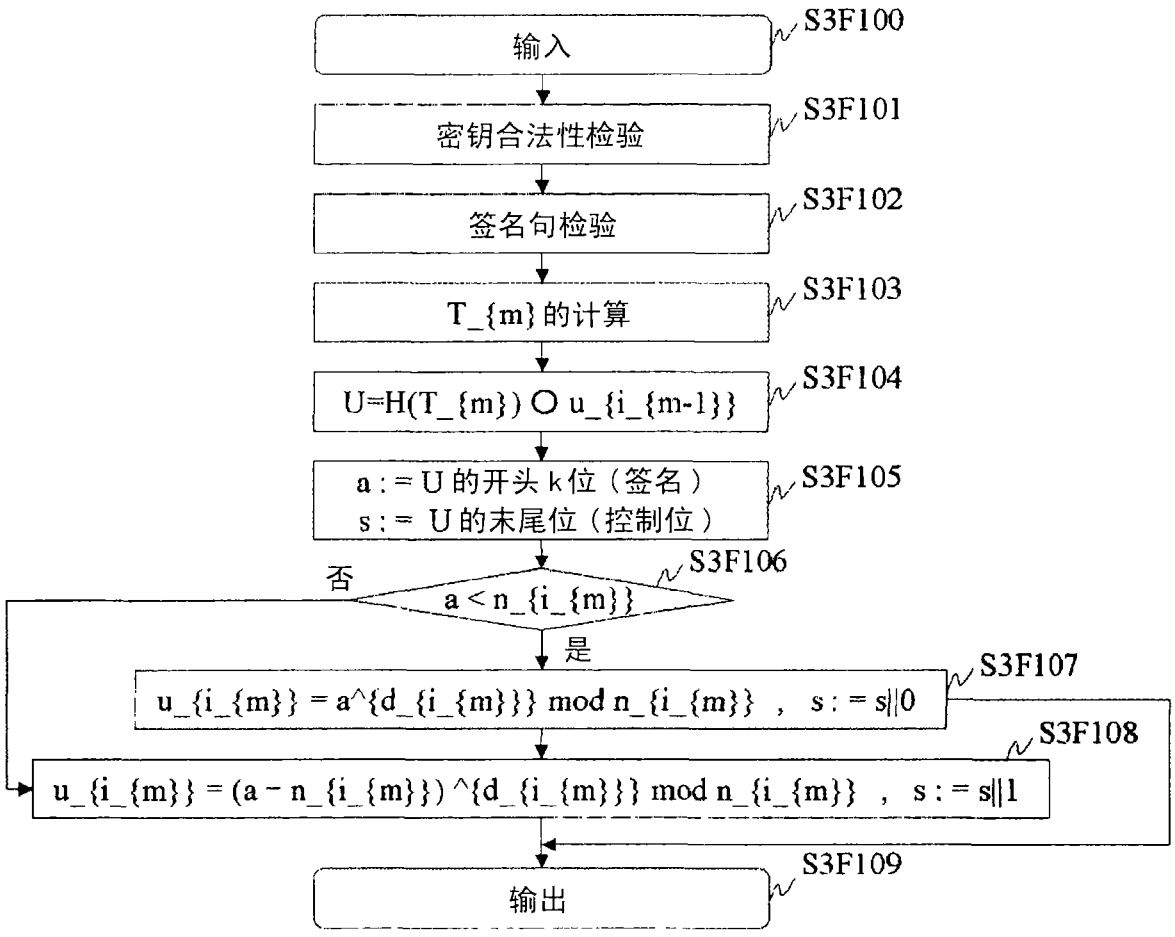

输入
S3F100
密钥合法性检验
S3F101
签名句检验
S3F102
T_{m}的计算
S3F103
U=H(T_{m})○u_{i_{m-1}}
S3F104
a:=U的开头k位（签名）
s:=U的末尾位（控制位）
S3F105
a<n_{i_{m}}
S3F106
否
是
u_{i_{m}}=a^{d_{i_{m}}} mod n_{i_{m}} , s:=s||0
S3F107
u_{i_{m}}=(a-n_{i_{m}})^{d_{i_{m}}} mod n_{i_{m}} , s:=s||1
S3F108
输出
S3F109

图 11