(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101753291 B
(45)授权公告日 2012.11.28

(21)申请号 200910253338.7
(22)申请日 2009.11.30
(30)优先权数据
2008-305624 2008.11.28 JP
(73)专利权人 佳能株式会社
地址 日本东京都大田区下丸子 3-30-2
(72)发明人 西川成 菊地明美 熊取谷昭彦 脇野栞
(74)专利代理机构 北京怡丰知识产权代理有限公司 11293
代理人 迟军
(51)Int.Cl.
H04L 9/06(2006.01)
(56)对比文件
JP 5108719 A,1993.04.30,
JP 4148372 A,1992.05.21,
审查员 贺利良

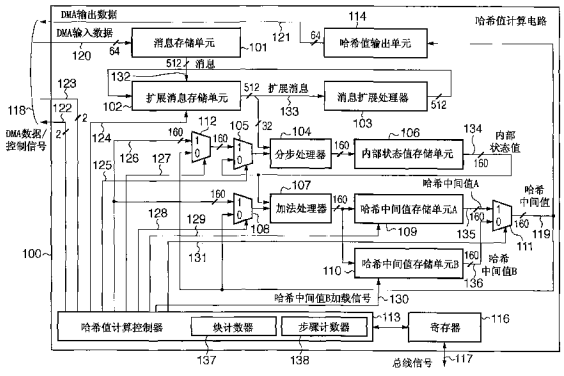
权利要求书 2 页 说明书 60 页 附图 98 页

(54)发明名称

哈希值计算装置及其方法

(57)摘要

本发明涉及一种哈希值计算装置及其方法。哈希值计算装置计算消息的哈希值，该哈希值计算装置包括：输入单元，其适于输入根据要处理的消息获得的扩展块；哈希值计算单元，其适于执行所输入的块的哈希值计算并输出哈希中间值；多个中间值存储单元，其适于针对所述要处理的消息存储由所述哈希值计算单元输出的所述哈希中间值；输出单元，其适于将与所述要处理的消息的所有块关联的哈希中间值作为所述消息的哈希值输出；以及哈希值计算控制单元，其适于通过切换用于存储从所述哈希值计算单元输出的所述哈希中间值的所述中间值存储单元来控制针对多个消息的哈希值计算。



CN 101753291 B

1. 一种哈希值计算装置，其计算消息的哈希值，该哈希值计算装置包括：

输入单元，其适于输入根据要处理的消息获得的块；

哈希值计算单元，其适于针对各块执行所输入的块的哈希值计算并输出哈希中间值；

多个中间值存储单元，其适于针对所述要处理的消息存储由所述哈希值计算单元输出的所述哈希中间值；

输出单元，其适于将与所述要处理的消息的所有块关联的哈希中间值作为所述消息的哈希值输出；以及

哈希值计算控制单元，其适于通过切换用于存储从所述哈希值计算单元输出的所述哈希中间值的所述中间值存储单元来控制针对多个消息的哈希值计算，

其中针对哈希算法规定了代表块的位数。

2. 根据权利要求 1 所述的哈希值计算装置，其中，在使用针对第一消息的第一中间值存储单元执行处理期间，输入优先级比所述第一消息高的第二消息的情况下，所述哈希值计算控制单元进行控制，以中断针对所述第一消息的处理，并使用第二中间值存储单元开始针对所述第二消息的处理，并且在针对所述第二消息的处理完成后，使用存储在所述第一中间值存储单元中的中间值重新开始针对所述第一消息的处理。

3. 根据权利要求 2 所述的哈希值计算装置，该哈希值计算装置还包括：扩展处理单元，其适于针对要处理的消息的块执行扩展处理；分步处理单元，其适于针对输入数据执行分步处理，并将经过所述分步处理的所述输入数据作为内部状态值输出，多个所述扩展处理单元和多个所述分步处理单元与不同的哈希算法对应地配置，

其中，所述输入单元输入经过所述扩展处理单元进行的所述扩展处理的块作为扩展块，

所述哈希值计算单元使用所述内部状态值执行所述哈希值计算，并且

所述哈希值计算装置还包括切换单元，该切换单元适于根据要使用的哈希算法来切换要启动的所述扩展处理单元和所述分步处理单元。

4. 根据权利要求 3 所述的哈希值计算装置，其中，所述第一中间值存储单元和所述第二中间值存储单元被配置成存储来自所述多个分步处理单元的输出数据中的具有最大位宽的输出数据。

5. 一种哈希值计算装置，其计算消息的哈希值，该哈希值计算装置包括：

输入单元，其适于输入根据要处理的消息获得的块；

多个哈希值计算单元，其适于针对各块执行所输入的块的哈希值计算并输出哈希中间值，所述多个哈希值计算单元与不同的哈希算法对应地配置；

切换单元，其适于根据要使用的哈希算法来切换要启动的所述哈希值计算单元；

中间值存储单元，其适于与要处理的消息关联地存储从所启动的哈希值计算单元输出的哈希中间值；以及

输出单元，其适于将与所述要处理的消息的所有块关联的哈希中间值作为所述消息的哈希值输出，

其中针对哈希算法规定了代表块的位数。

6. 根据权利要求 5 所述的哈希值计算装置，其中，所述中间值存储单元被配置成存储所述多个哈希值计算单元的输出数据中的具有最大位宽的输出数据。

7. 一种用于哈希值计算装置的哈希值计算方法，所述哈希值计算装置计算消息的哈希值，该哈希值计算方法包括：

输入步骤，输入根据要处理的消息获得的块；

哈希值计算步骤，针对各块执行所输入的块的哈希值计算并输出哈希中间值；

存储步骤，针对所述要处理的消息在多个中间值存储单元的一个中存储在所述哈希值计算步骤中输出的所述哈希中间值；

输出步骤，输出与所述要处理的消息的所有块关联的哈希中间值作为所述消息的哈希值；以及

哈希值计算控制步骤，通过切换用于存储在所述哈希值计算步骤中输出的所述哈希中间值的所述中间值存储单元来控制针对多个消息的哈希值计算，

其中针对哈希算法规定了代表块的位数。

8. 一种用于哈希值计算装置的哈希值计算方法，所述哈希值计算装置计算消息的哈希值，该哈希值计算方法包括：

输入步骤，输入根据要处理的消息获得的块；

哈希值计算步骤，在与不同的哈希算法对应地配置的多个哈希值计算单元的一个中，针对各块执行所输入的块的哈希值计算并输出哈希中间值；

切换步骤，根据要使用的哈希算法来切换要启动的所述哈希值计算单元；

中间值存储步骤，在存储单元中，与要处理的消息关联地存储在所启动的哈希值计算单元中输出的哈希中间值；以及

输出步骤，输出与所述要处理的消息的所有块关联的哈希中间值作为所述消息的哈希值，

其中针对哈希算法规定了代表块的位数。

哈希值计算装置及其方法

技术领域

[0001] 本发明涉及一种哈希 (hash) 值计算装置及其方法。

背景技术

[0002] （关于哈希函数）

[0003] 近年来，由于例如普通家庭用户能够以低成本连接光纤网络，因此支持因特网的基础设施投入使用，并且通信速度迅速加快。各种数字设备可以连接到网络，并且在数字设备间经由因特网频繁进行通信。

[0004] 在这种数字设备间的通信中，作为必不可少的功能，除了对要交换的消息进行加密以外，还需要对通信伙伴和消息进行认证。在这种在数字设备间对通信伙伴和消息进行认证时，通常使用称作哈希函数的算法。

[0005] 哈希函数是一种输入任意位长的消息并输出固定位长的哈希值的算法（函数）。该哈希函数通过以下处理来计算哈希值。

[0006] 1) 将预定数据附加到任意位长的输入消息的最末位置，以使该消息成为在算法中指定的块的位长的整数倍（填充 (padding) 处理）。

[0007] 2) 针对各块扩展经过填充处理的消息，以生成扩展消息（消息扩展处理）。

[0008] 3) 将使用与块对应的扩展消息（扩展块）、从初始值改变内部状态值的处理重复在算法中指定的次数。注意，作为内部状态值的初始值，针对第一个块使用在算法中指定的预定固定值（以下称作哈希初始值）。针对第二个块及随后的块，使用针对紧接在关注的块之前的块的哈希中间值（稍后描述）（分步处理）。

[0009] 4) 将进行了预定次数的分步处理后的内部状态值与针对紧接的前一个块的该加法处理结果（以下称作哈希中间值）相加，以计算新的哈希中间值。注意，针对第一个块，将进行了预定次数的分步处理后的内部状态值与哈希初始值相加，以计算哈希中间值（加法处理）。

[0010] 5) 针对所有块依次执行处理 2) 到 4)。将在完成对所有扩展消息的处理时得到的哈希中间值作为哈希值输出。

[0011] 将哈希函数的处理 1) 到 5) 的组合称作哈希值计算。注意，如果哈希初始值可用于第一个块，或者如果紧接的前一个块的哈希中间值可用于第二个块及随后的块，则能够执行针对某个块的哈希函数的处理 3) 和 4)。因此，在计算从第一个块到某个块的哈希中间值时，哈希值计算中断，可以使用该哈希中间值从下一个块重新开始处理。

[0012] 哈希函数具有以下三个主要特征。作为第一个特征，可以根据消息来计算哈希值，但是实际上不可能根据输出哈希值反过来计算输入消息（单向）。作为第二个特征，在给定某个消息的哈希值时，找出具有该哈希值的另一个消息非常困难（弱抗冲突性）。作为第三个特征，发现哈希值匹配的两个不同的消息非常困难（强抗冲突性）。

[0013] 在例如 SSL/TLS 和 IPSec 的各种通信协议中使用具有这种性质的哈希函数。针对各个通信协议，通过规格 (specification) 来确定可以使用的哈希函数算法。在数字设备

间进行通信时，从数字设备采用的通信协议可以使用的哈希算法中选择在两个数字设备中安装的哈希算法，并且在进行认证处理时使用。

[0014] 由于通信速度加快，所以在加密通信中保证通信速度的需要增加，并且所需的响应时间根据要处理的数据而不同。例如，对于进行修改检测的大容量图像数据，允许一定程度的哈希值计算的长响应时间。但是，对于进行个人认证所需的短的密码，期望非常短的哈希值计算的响应时间。因此，还要求哈希值计算加速处理并尽可能地缩短对具有高优先级的数据的响应时间。通过硬件来实现处理以加速哈希值计算是必不可少的。在硬件实现的情况下，由于电路规模直接涉及成本，因此每个系统准备一个例如实现哈希值计算的哈希值计算电路的硬件资源，并通过共享该一个硬件资源来实现针对多个消息的哈希值计算。

[0015] 如上所述，哈希值计算将任意位长的消息分割成各自具有固定位长的块，并处理这些块。在完成针对所有块的哈希值计算时，能够获得针对该消息的哈希值。

[0016] （要处理的消息的切换）

[0017] 下面，分析以下情况：在使用一个硬件资源执行针对多个消息的哈希值计算的条件下，在针对非常长的消息的哈希值计算开始后，接收针对具有高优先级的短消息的哈希处理请求。在这种情况下，针对第一个消息的哈希值计算需要很长时间，无法保证与针对具有高优先级的短消息的哈希值计算关联的给定响应时间。因此，为了保证给定响应时间，需要加速哈希值计算本身、对要处理的消息分配优先等级、并先处理具有高优先级的消息的机制。例如，需要以下机制。即，临时中断先输入的长消息的哈希值计算，先执行针对具有高优先级的短消息的哈希值计算，在完成对该短消息的处理后，重新开始对长消息的哈希值计算。

[0018] 传统上，已知一种加密处理装置，其能够与各种加密算法差异和加密处理模式差异无关地有效中断和重新开始例如哈希值计算的加密处理（日本特开 2006-39000 号公报）。在这种配置中，DMA 控制器的描述符包括指令中断和重新开始哈希值计算的格式。在传输附加有中断信息的消息时，将作为直到消息中间的某个块的哈希值计算的计算结果而存储的内部状态值写出到外部存储器中。另一方面，在传输附加有重新开始信息的消息时，读出存储在外部存储器中的内部状态值，并且从消息中的下一个块开始重新开始哈希值计算。

[0019] （多个哈希函数的支持）

[0020] 另一方面，分别规定了在加密通信协议中能够使用的哈希算法。在数字设备间的通信中，从安装在各个通信设备中的哈希算法中选择两个通信设备能够共同执行的哈希算法。对方通信设备能够执行的哈希算法经常可能不同，需要与许多通信设备进行加密通信的设备不得不执行许多不同的哈希算法。

[0021] 此外，近年来，指出了广泛用作哈希算法的标准的 SHA-1 和 MD5 的脆弱性，并且推荐转变到总称为 SHA-2 的具有更高安全性的哈希算法。即使在标准加密通信协议中，也想定在不远的将来采用例如 SHA-2 的具有多位长度的哈希算法。然而，新产品能够采用新的哈希算法，但是存在许多数字设备只支持旧的哈希算法，这些数字设备难以进行运行改变。因此，必须支持传统上用作标准的旧的哈希算法和具有高安全性的新的哈希算法两者，以与不同的数字设备进行安全的通信。日本特开 2004-53716 号公报公开了一种作为硬件来实现多个哈希函数的哈希函数处理电路。

[0022] 在哈希值计算电路依次针对各个消息执行哈希值计算的情况下，在针对某个消息的哈希值计算开始时，针对另一个消息的哈希值计算必须等待完成该哈希值计算。在当前处理的消息非常长，而另一个等待的消息非常短时，不能保证针对所有消息的在预定响应时间内的处理性能。为了解决这种问题，期望提供一种能够在一个消息的处理期间同时处理另一个消息的机制。

[0023] （关于要处理的消息的切换的问题）

[0024] 然而，在日本特开 2006-39000 号公报的配置中，作为哈希值计算的中间运算结果存储的数据是加法处理之前的内部状态值，而不存储重新开始哈希值计算所需的加法处理后的哈希中间值。因此，仅这种配置实际上不能重新开始哈希值计算。为了中断并重新开始哈希值计算，除了上述配置以外，必须另外存储紧接的前一个块的哈希中间值。作为替选方案，为了生成紧接的前一个块的哈希中间值，必须另外存储紧接的前一个块之前的块的哈希中间值，并必须将其与存储在外部存储器中的内部状态值相加。以这种方式，在传统配置的框架下，要存储的数据量增加，并且有关加法处理的时间开销也增加。

[0025] 利用通过对日本特开 2006-39000 号公报的配置添加哈希中间值存储或生成装置的配置，可以通过在处理中间切换多个消息来执行哈希值计算。但是，利用这种配置，将形成消息的多个块中的、直到中间块的哈希值计算中间值写出到外部存储器中以中断处理，并在重新开始处理时从外部存储器读出该哈希值计算中间值。由于该原因，需要额外的时间，来从存储器读取哈希值计算中间值 / 将哈希值计算中间值写入到存储器中。

[0026] 例如，哈希中间值的位长，对于 SHA-1 总计为 160 位，对于 SHA-256 总计为 256 位，对于 SHA-512 总计为 512 位。通常以 32 位或 64 位单位进行存储器读 / 写访问，并且将哈希值计算的中间运算结果写入到存储器或从存储器读出需要几到几十个循环。由于数据的存储器读 / 写访问还需要例如确保总线权所需的等待时间的额外时间，因此基于上述相关技术中断和重新开始哈希值计算，需要除了哈希值计算本身之外的大的时间开销。

[0027] 在上述配置中在处理中间切换针对多个消息的哈希值计算时，必须将作为针对一个消息的哈希值计算中的直到中间块的哈希值计算结果而获得的内部状态值写入到与总线连接的外部存储器中。但是，在哈希值计算器外部泄漏内部状态值意味着被盗的风险增加，从而引起安全问题。

[0028] 在中断和重新开始哈希值计算时，期望不仅减少哈希值计算的中间运算结果的读 / 写开销，而且减少消息本身在外部存储器上的读 / 写开销。例如，在 SHA-1 的情况下，作为消息的处理单位的块的位长为 512 位，以 32 位或 64 位单位进行存储器读 / 写访问需要 16 或 8 个循环。在对新消息的块的数据或临时放弃的消息的块应用哈希值计算时，从外部存储器读出消息的块所需的时间对哈希值计算施加大的开销。

[0029] 如日本特开 2006-39000 号公报所描述的，设置能够给出中断和重新开始哈希值计算的指令的 DMA 控制器的描述符格式，以消除在进行中断 / 重新开始控制时进行条件确定所需的软件的干扰，从而有效地中断和重新开始哈希值计算。但是，日本特开 2006-39000 号公报仅公开了以下技术：在数据传输到哈希值计算器之前、CPU 预先识别消息中要中断和重新开始的一部分数值之后，CPU 将该数据与表示有无中断 / 重新开始的信息一起传输给哈希值计算器。即，该参考文献没有公开针对在向哈希值计算器临时发出对消息的数据的哈希处理请求后，对消息进行中断和重新开始处理的任何技术。

[0030] （关于多个哈希函数的支持的问题）

[0031] 在用硬件实现加速哈希值计算的情况下，不仅需要哈希算法电路，还需要分别存储经过消息扩展处理的数据、经过分步处理的数据和经过加法处理的数据的存储单元。在分别配置处理许多不同的哈希算法和具有高安全性的新的哈希算法的硬件部件时，电路规模增大。尤其是，由于具有高安全性的新的哈希算法的哈希值的位长大，因此具有高安全性的新的哈希算法需要较大容量的存储单元。但是，一般需要尽量抑制硬件的电路规模以实现功率和成本节省。

[0032] 传统的哈希装置包括处理不同的哈希算法的多个专用电路以及由该多个专用电路共同使用的存储单元，并且传统的哈希装置通过选择哈希算法中的一个来执行哈希值计算。在这种情况下，由于多个哈希算法共同使用存储单元，因此不能针对多个消息同时执行哈希值计算，从而不能保证针对所有消息的在预定响应时间内的处理性能。

[0033] 如在日本特开 2004-53716 号公报中所描述的配置中，配置了处理不同的哈希算法的多个专用电路，而仅与所请求的哈希算法对应的专用电路工作。但是，在这种情况下，不仅电路规模显著增加，而且整个哈希值计算装置的功耗的变化变大。因此，在外部通过功率分析来分析电路的内部信息变得容易。由于该原因，在防篡改性（安全性）方面，也不优选这种配置。

发明内容

[0034] 首先，本发明旨在提供一种能够在处理中间切换针对多个消息的哈希值计算而不会使任何处理性能降低，并且能够确保较高安全性的哈希值计算技术。

[0035] 另外，本发明旨在提供一种允许同时执行多个哈希算法，并且能够确保小电路规模和高安全性的哈希值计算技术。

[0036] 根据本发明的一个方面，提供一种哈希值计算装置，其计算消息的哈希值，该哈希值计算装置包括：

[0037] 输入单元，其适于输入根据要处理的消息获得的扩展块；

[0038] 哈希值计算单元，其适于执行所输入的块的哈希值计算并输出哈希中间值；

[0039] 多个中间值存储单元，其适于针对所述要处理的消息存储由所述哈希值计算单元输出的所述哈希中间值；

[0040] 输出单元，其适于将与所述要处理的消息的所有块关联的哈希中间值作为所述消息的哈希值输出；以及

[0041] 哈希值计算控制单元，其适于通过切换用于存储从所述哈希值计算单元输出的所述哈希中间值的所述中间值存储单元来控制针对多个消息的哈希值计算。

[0042] 根据本发明的另一个方面，提供一种哈希值计算装置，其计算消息的哈希值，该哈希值计算装置包括：

[0043] 输入单元，其适于输入根据要处理的消息获得的扩展块；

[0044] 多个哈希值计算单元，其适于执行所输入的块的哈希值计算并输出哈希中间值，所述多个哈希值计算单元与不同的哈希算法对应地配置；

[0045] 切换单元，其适于根据要使用的哈希算法来切换要启动的所述哈希值计算单元；

[0046] 中间值存储单元，其适于与要处理的消息关联地存储从所启动的哈希值计算单元

输出的哈希中间值；以及

[0047] 输出单元，其适于将与所述要处理的消息的所有块关联的哈希中间值作为所述消息的哈希值输出。

[0048] 根据本发明的再一个方面，提供一种用于哈希值计算装置的哈希值计算方法，所述哈希值计算装置计算消息的哈希值，该哈希值计算方法包括：

[0049] 输入步骤，输入根据要处理的消息获得的扩展块；

[0050] 哈希值计算步骤，执行所输入的块的哈希值计算并输出哈希中间值；

[0051] 存储步骤，针对所述要处理的消息在多个中间值存储单元的一个中存储在所述哈希值计算步骤中输出的所述哈希中间值；

[0052] 输出步骤，输出与所述要处理的消息的所有块关联的哈希中间值作为所述消息的哈希值；以及

[0053] 哈希值计算控制步骤，通过切换用于存储在所述哈希值计算步骤中输出的所述哈希中间值的所述中间值存储单元来控制针对多个消息的哈希值计算。

[0054] 根据本发明的又一个方面，提供一种用于哈希值计算装置的哈希值计算方法，所述哈希值计算装置计算消息的哈希值，该哈希值计算方法包括：

[0055] 输入步骤，输入根据要处理的消息获得的扩展块；

[0056] 哈希值计算步骤，在与不同的哈希算法对应地配置的多个哈希值计算单元的一个中，执行所输入的块的哈希值计算并输出哈希中间值；

[0057] 切换步骤，根据要使用的哈希算法来切换要启动的所述哈希值计算单元；

[0058] 中间值存储步骤，在存储单元中，与要处理的消息关联地存储在所启动的哈希值计算单元中输出的哈希中间值；以及

[0059] 输出步骤，输出与所述要处理的消息的所有块关联的哈希中间值作为所述消息的哈希值。

[0060] 从以下参照附图对示例性实施例的描述，本发明的其它特征将变得清楚。

附图说明

[0061] 图 1 是示出哈希值计算电路的内部配置的框图；

[0062] 图 2 是示出操作哈希值计算电路所需的系统配置的主要部分的框图；

[0063] 图 3 是示出哈希值计算系统中的针对各消息的哈希值计算的操作序列的流程图；

[0064] 图 4 是示出哈希值计算电路中的寄存器的内部结构的图；

[0065] 图 5 是示出消息 A 和消息 B 的块结构的图；

[0066] 图 6 是示出消息 A 和消息 B 的块的传输顺序的图；

[0067] 图 7 是示出哈希值计算系统中的针对多个消息的哈希值计算的操作序列的流程图；

[0068] 图 8A 至图 8E 是示出针对各个步骤的哈希值计算的时序图；

[0069] 图 9A 至图 9E 是示出针对各个步骤的哈希值计算的时序图；

[0070] 图 10A 至图 10E 是示出针对各个步骤的哈希值计算的时序图；

[0071] 图 11A 和图 11B 是示出针对各个块的哈希值计算的时序图；

[0072] 图 12 是示出哈希值计算电路的内部配置的框图；

[0073] 图 13 是示出哈希值计算电路中的寄存器的内部结构的图；

[0074] 图 14A 和图 14B 是示出哈希值计算系统中的针对多个消息的哈希值计算的操作序列的流程图；

[0075] 图 15A 至图 15E 是示出针对各个步骤的哈希值计算的时序图；

[0076] 图 16A 至图 16E 是示出针对各个步骤的哈希值计算的时序图；

[0077] 图 17A 和图 17B 是示出针对各个块的哈希值计算的时序图；

[0078] 图 18 是示出哈希值计算电路的内部配置的框图；

[0079] 图 19 是示出哈希值计算电路中的寄存器的内部结构的图；

[0080] 图 20A、图 20B 和图 20C 是示出哈希值计算系统中的针对多个消息的哈希值计算的操作序列的流程图；

[0081] 图 21A 至图 21G 是示出针对各个步骤的哈希值计算的时序图；

[0082] 图 22A 至图 22F 是示出针对各个步骤的哈希值计算的时序图；

[0083] 图 23A 至图 23F 是示出针对各个步骤的哈希值计算的时序图；

[0084] 图 24A 和图 24B 是示出针对各个块的哈希值计算的时序图；

[0085] 图 25 是示出哈希值计算电路的配置的框图；

[0086] 图 26 是示出控制器的内部配置的示例的框图；

[0087] 图 27 是示出寄存器的规格的示例的图；

[0088] 图 28 是示出操作哈希值计算电路所需的系统的配置的示例的框图；

[0089] 图 29A 至图 29C 是示出哈希值计算系统中的针对各消息接收的 CPU 的操作序列的流程图；

[0090] 图 30A 和图 30B 是示出哈希值计算系统中的哈希电路的操作序列的流程图；

[0091] 图 31 是示出要进行哈希值计算的消息的示例的图；

[0092] 图 32A 至图 32H 是示出哈希值计算的详细情况的示例的时序图；

[0093] 图 33A 至图 33H 是示出哈希值计算的详细情况的示例的时序图；

[0094] 图 34A 和图 34B 是示出基于接口信号的操作的示例的时序图；

[0095] 图 35 是示出数据 ExMSG_0 和 ExMSG_1 的选择策略的示例的图；

[0096] 图 36 是示出扩展消息存储单元的内部配置的示例的图；

[0097] 图 37 是示出数据 ExMSG_N[31 :0] 和 ExMSG_N[63 :32] 的选择策略的示例的图；

[0098] 图 38 是示出数据 TEMP_0 和 TEMP_1 的选择策略的示例的图；

[0099] 图 39 是示出数据 TEMP_N[255 :0] 和 TEMP_N[511 :256] 的选择策略的示例的图；

[0100] 图 40 是示出数据 IHASH_0 和 IHASH_1 的选择策略的示例的图；以及

[0101] 图 41 是示出数据 IHASH_N[255 :0] 和 IHASH_N[511 :256] 的选择策略的示例的图。

具体实施方式

[0102] 下面，参考附图详细说明根据本发明的实施例。但是，在这些实施例中描述的部件仅是示例，其不限制本发明的范围。在这些实施例中描述的特征的所有组合对于本发明的解决手段不始终是必不可少的。

[0103] << 第一实施例 >>

[0104] 本实施例例示应用 SHA-1 作为用于计算哈希值的哈希函数的配置。在 SHA-1 中，

针对各个 512 位的块处理消息，将 160 位的哈希值作为哈希值计算的最终结果输出。SHA-1 的哈希值计算包括如下一系列处理。

[0105] • 将消息分割为 512 位的块，并将预定数据添加到消息的最末位置，以使最后的块具有 512 位（以下称作填充处理）。

[0106] • 对各 512 位的块应用稍后描述的消息扩展处理、80 个步骤的分步处理和加法处理，以生成哈希中间值。

[0107] 消息扩展处理根据 512 位的块数据生成 80 个 32 位的扩展消息（扩展块）。按原样使用源 512 位的块数据作为第 0 到第 15 个扩展消息。至于第 16 个及随后的扩展消息，对第 (n-16) 到第 (n-1) 个消息应用预定运算处理，以生成第 n 个扩展消息。

[0108] 分步处理针对包括 5 个 32 位的数据的预定内部状态值的初始值（哈希初始值），通过针对 80 个步骤中的各个步骤使用 80 个扩展消息应用预定运算操作，来依次更新内部状态值。在最初的第 0 个步骤（以下称作步骤 0）中，使用第 0 个扩展消息对哈希初始值应用预定运算处理，以更新内部状态值。在其余 79 个步骤中的各个（以下称作步骤 n）中，使用第 n 个扩展消息对步骤 (n-1) 的内部状态值应用预定运算处理，从而更新内部状态值。

[0109] 加法处理将作为关注的块的第 80 个步骤的分步处理结果的内部状态值与从第一个块到紧接的前一个块的哈希中间值相加。

[0110] 从消息的第一个块到某个块的哈希值计算结果是哈希中间值，从第一个块到最后的块的哈希中间值是整个消息的哈希值。

[0111] （哈希值计算电路的配置）

[0112] 图 1 是示出根据本发明第一实施例的哈希值计算电路的配置的框图。

[0113] 附图标记 100 表示哈希值计算电路。附图标记 101 表示临时存储由稍后描述的外部 DMA 控制器（以下称作 DMAC）从外部存储器 DMA 传输到哈希值计算电路 100 的消息的消息存储单元。

[0114] 附图标记 102 表示临时存储扩展消息的扩展消息存储单元。附图标记 103 表示输入临时存储在扩展消息存储单元 102 中的扩展消息并执行消息扩展处理的消息扩展处理器。

[0115] 附图标记 104 表示针对输入消息的各块针对各步骤依次执行步骤 0 到步骤 79 的分步处理的分步处理器。附图标记 105 表示选择要由分步处理器 104 处理的内部状态值的选择器。

[0116] 附图标记 106 表示临时存储作为来自分步处理器 104 的输出的内部状态值的内部状态值存储单元。附图标记 107 表示对完成所有步骤的处理后的内部状态值和到紧接的前一个块的哈希中间值执行加法处理的加法处理器。

[0117] 附图标记 108 表示选择要输入到加法处理器 107 的哈希中间值的选择器。附图标记 109 和 110 表示存储作为来自加法处理器 107 的输出的哈希中间值的哈希中间值存储单元（第一和第二中间值存储单元）。附图标记 111 表示选择存储在哈希中间值存储单元 109 和 110 中的哈希中间值中的一个的选择器。

[0118] 附图标记 112 表示选择作为到紧接的前一个块的哈希值计算结果的哈希中间值和哈希初始值中的一个的选择器。附图标记 113 表示生成控制外部 DMAC 和 CPU 之间的数据交换和哈希值计算所需要的各种信号的哈希值计算控制器。

[0119] 附图标记 114 表示针对消息的各分割将 32 位的假数据 (dummy data) 附加到 160 位的哈希值以获得 3 个 64 位的数据，并通过 DMA 传输将这些数据传送到哈希值计算电路 100 外部的哈希值输出单元。附图标记 116 表示存储由哈希值计算电路 100 外部的 CPU 设置的哈希值计算电路 100 的操作参数的寄存器。

[0120] 附图标记 117 表示包括用于向寄存器 116 输入数据 / 从寄存器 116 输出数据的地址信号、数据信号和控制信号的总线信号。附图标记 118 表示要与 DMAC 交换的 DMA 数据 / 控制信号，包括 DMA 输入数据、DMA 输出数据、DMA 请求信号和 DMA 确认信号（稍后描述）。

[0121] 附图标记 119 表示由选择器 111 选择的哈希中间值。附图标记 120 表示要从 DMAC 输出到哈希值计算电路 100 的 DMA 输入数据。消息存储单元 101 存储该 DMA 输入数据。

[0122] 附图标记 121 表示要从哈希值计算电路 100 输出到 DMAC 的 DMA 输出数据。哈希值输出单元 114 输出哈希值或哈希中间值作为该 DMA 输出数据。附图标记 122 表示要从哈希值计算电路 100 输出到 DMAC 的 DMA 请求信号。哈希值计算控制器 113 在发出输入数据的读取请求和输出数据的写入请求时分别断言 (assert)DMA 读取请求信号和 DMA 写入请求信号。

[0123] 附图标记 123 表示要从 DMAC 输出到哈希值计算电路 100 的 DMA 确认信号。即，DMAC 响应于输入数据的读取请求断言 DMA 读取确认信号并输出输入数据，并响应于输出数据的写入请求断言 DMA 写入确认信号并取出输出数据。注意，DMA 请求信号 122 和 DMA 确认信号 123 一起包括读 / 写信号。

[0124] 附图标记 124 表示从哈希值计算控制器 113 输出的、用于在针对各块的哈希值计算开始时将存储在消息存储单元 101 中的扩展消息加载到扩展消息存储单元 102 中的块加载信号。附图标记 125 表示从哈希值计算控制器 113 输出的作为选择器 105 的控制信号的哈希中间值选择信号。

[0125] 附图标记 126 表示在寄存器 116 中设置的表示哈希值计算的初始值的信号，即，要从哈希值计算控制器 113 输出到选择器 112 的哈希初始值。附图标记 127 表示从哈希值计算控制器 113 输出的作为选择器 112 的控制信号的哈希初始值选择信号 X。

[0126] 附图标记 128 表示从哈希值计算控制器 113 输出的作为选择器 108 的控制信号的哈希初始值选择信号 Y。附图标记 129 表示从哈希值计算控制器 113 输出的作为哈希中间值存储单元 A 109 中的哈希中间值 A 135 的加载信号的哈希中间值 A 加载信号。

[0127] 附图标记 130 表示从哈希值计算控制器 113 输出的作为哈希中间值存储单元 B 110 中的哈希中间值 B 136 的加载信号的哈希中间值 B 加载信号。附图标记 131 表示从哈希值计算控制器 113 输出的作为选择器 111 的控制信号的消息 A 选择信号。

[0128] 附图标记 132 表示从消息存储单元 101 输出到扩展消息存储单元 102 的消息。附图标记 133 表示从扩展消息存储单元 102 输出到消息扩展处理器 103 的扩展消息。

[0129] 附图标记 134 表示作为来自内部状态值存储单元 106 的输出的内部状态值。附图标记 135 表示作为来自哈希中间值存储单元 A 109 的输出的哈希中间值 A。附图标记 136 表示作为来自哈希中间值存储单元 B 110 的输出的哈希中间值 B。

[0130] 附图标记 137 表示对要针对各消息处理的块的数量进行计数的块计数器，其在针对形成消息的预定数量的块的哈希值计算完成时清零。附图标记 138 表示对要针对消息的各块处理的步骤的数量进行计数的步骤计数器，其在对预定数量的步骤进行计数后清零。

[0131] 注意，在本实施例中，块计数器 137 的计数器值针对第 n(n = 0、…) 个块处理指示值 (n+1)。步骤计数器 138 的计数器值针对第 n(n = 0、…、79) 个分步处理指示值 (n+1)。

[0132] 在本实施例中，哈希值计算电路 100 执行除填充处理外的哈希值计算的消息扩展处理、分步处理和加法处理。稍后描述的哈希值计算系统 200 中的除哈希值计算电路 100 以外的部件、即稍后描述的 CPU 201 和存储器 202 执行填充处理。

[0133] （哈希值计算系统的配置）

[0134] 图 2 是示出操作哈希值计算电路 100 所需的系统的配置的示例的框图。附图标记 200 表示哈希值计算系统。附图标记 201 表示控制哈希值计算系统 200 的操作的 CPU。附图标记 202 表示用于存储要进行哈希值计算的消息和哈希值等的存储器。

[0135] 附图标记 203 表示将消息从存储器 202 传输到哈希值计算电路 100 以及将哈希值从哈希值计算电路 100 传输到存储器 202 的直接存储存取控制器 (DMAC，direct memory access controller)。附图标记 204 表示控制哈希值计算系统 200 的中断信号的中断控制器。附图标记 205 表示连接哈希值计算电路 100、CPU 201、存储器 202、DMAC 203 和中断控制器 204 的总线，其包括地址信号、数据信号和控制信号。

[0136] 附图标记 206 表示从 DMAC 203 到中断控制器 204 的中断信号。在本实施例中，在 DMAC 203 将哈希值从哈希值计算电路 100 传输到存储器 202 后，DMAC 203 使用中断信号 206 将来自 DMAC 203 的中断通知给中断控制器 204。中断控制器 204 使用中断信号（未示出）将哈希值的存储通知给 CPU 201。

[0137] （哈希值计算的概要）

[0138] 图 3 是示出本实施例的哈希值计算系统中的针对各消息的哈希值计算的操作序列的流程图。

[0139] 在 ST001 中，CPU 201 经由总线信号 117 在哈希值计算电路 100 的寄存器 116 中设置针对关注的消息的哈希值计算的操作参数。

[0140] 在 ST002 中，哈希值计算电路 100 通过 DMA 读传输来读取消息的数据，针对各块执行哈希值计算，并生成直到最后的块的哈希值。

[0141] 在 ST003 中，哈希值计算电路 100 通过 DMA 写传输来输出关注的消息的哈希值。

[0142] （寄存器的存储内容）

[0143] 图 4 是示出本实施例的哈希值计算电路 100 中的寄存器 116 存储的信息的图。

[0144] 寄存器 116 具有作业开始信息、消息标识符信息、块的数量信息、哈希初始值信息和处理继续信息的存储区域。“作业开始”区域中的信息表示是否根据在“消息标识符”、“块的数量”、“哈希初始值”和“处理继续”区域中设置的信息“开始哈希值计算”或者“不开始哈希值计算”。可以通过相应区域中的预定位的“1”或“0”来表示是否开始哈希值计算。以下将在预定位中设置“1”或“0”称作“设置标志”或“清除标志”。

[0145] CPU 201 在哈希值计算电路 100 的寄存器 116 中的“作业开始”区域中设置预定标志，以针对与一个消息对应的各个哈希处理请求指示“开始哈希值计算”。当在对应的区域中设置预定标志、并完成针对紧接的前一个消息的哈希值计算时，哈希值计算电路 100 开始哈希值计算。接着，在针对要处理的消息的哈希值计算完成时，哈希值计算电路 100 清除标志以指示“不开始哈希值计算”。

[0146] “消息标识符”区域中的信息是用于通过区域中的多个预定位来识别处理请求中

的目标消息的标识符。例如，在消息的类型的数量为 2 时，如果预定位是“1”，则其指示“处理消息 A”；如果预定位是“0”，则其指示“处理消息 B”。

[0147] “块的数量”区域中的信息通过预定位来指示处理请求中的块的数量。例如，在预定位指示的值指示要处理的块的数量时，如果预定位的值是“0x004”，则要处理的块的数量为 4。

[0148] “哈希初始值”区域中的信息指示处理请求中的内部状态值的初始值（哈希初始值）。在 SHA-1 的情况下，由于内部状态值包括 5 个 32 位的数据，因此该区域中的预定 160 位指示哈希初始值。注意，CPU 201 可以将 SHA-1 算法的内部状态值的初始值写入到“哈希初始值”区域，或者可以写入与哈希中间值对应的值，以重新开始并处理中断的哈希值计算。

[0149] “处理继续”区域中的信息通过该区域中的预定位的“1”或“0”指示将使用哪个值作为处理请求中的在哈希值计算中所使用的内部状态值的初始值：

[0150] • 存储在“哈希初始值”区域中的“使用内部状态值的初始值”；或

[0151] • 存储在哈希值计算电路 100 的哈希中间值存储单元中的“使用哈希中间值”。

[0152] 注意，CPU 201 针对与一个消息对应的各个哈希处理请求在“消息标识符”、“块的数量”、“哈希初始值”和“处理继续”区域中写入预定值。

[0153] （消息示例）

[0154] 图 5 示出了在本实施例中进行哈希值计算的两个消息，即消息 A（第一消息）和消息 B（第二消息）。在 SHA-1 中，针对各个 512 位的块进行哈希值计算。在这种情况下，将消息 A 从其头位置开始分割为 512 位的块 A0、A1、A2、…、A51、A52、A53、A54、…、A93、A94 和 A95。对于最后的块 A95，对少于 512 位的部分附加填充数据。同样地，将消息 B 从其头位置开始分割为 512 位的块 B0、B1、B2 和 B3，并将填充数据附加到块 B3。这些消息存储在存储器 202 中。

[0155] （消息传输的概要）

[0156] 图 6 示出在本实施例中进行哈希值计算的消息 A 和消息 B 从存储器 202 传输到哈希值计算电路 100 时的传输顺序。本实施例将例示 CPU 201 控制哈希值计算电路 100 在消息 A 的中间优先处理消息 B 的情况。即，DMAC 203 将形成消息 A 的块 A0、A1、A2、…、A51 和 A52 依次传输到哈希值计算电路 100，接着将形成消息 B 的块 B0、B1、B2 和 B3 依次传输到哈希值计算电路 100。之后，DMAC 203 将形成消息 A 的块 A53、A54、…、A93、A94 和 A95 传输到哈希值计算电路 100。

[0157] 在本实施例中，预先决定 CPU 201 发出中断消息 A 的哈希值计算并开始消息 B 的哈希值计算的处理请求。此外，CPU 201 向哈希值计算电路 100 发出作为两个消息、即包括块 A0 到 A52 的消息和包括块 A53 到 A95 的消息的消息 A 的处理请求。

[0158] （哈希值计算）

[0159] 在本实施例中，哈希值计算电路 100 根据图 3 所示的序列，针对具有在 ST001 中由 CPU 201 在寄存器 116 中设置的块的数量的消息，在 ST002 中执行块的数量的哈希值计算，而不中断这些哈希值计算。在 ST003 中，哈希值计算电路 100 输出哈希值计算结果的哈希值。在完成针对该消息的哈希值计算时，在 CPU 201 在哈希值计算电路 100 的寄存器 116 中设置了针对下一个消息的处理请求时，哈希值计算电路 100 执行针对下一个消息的在寄

存器 116 中设置的块的数量的哈希值计算。

[0160] 图 7 是示出在以图 6 所示的顺序输入三个消息 (A0 到 A52、B0 到 B3 以及 A53 到 A95) 时，本实施例的哈希值计算的操作序列的流程图。根据图 3 中的 ST001 和 ST002 中的操作序列，依次针对各消息执行哈希值计算。

[0161] 在 ST101 中，CPU 201 在哈希值计算电路 100 的寄存器 116 中设置针对第一消息 (A0 到 A52) 的处理请求。

[0162] 在 ST102 中，哈希值计算电路 100 通过向 DMAC 203 发出读取请求来读取第一消息 (A0 到 A52) 的数据，并执行针对该消息的哈希值计算。

[0163] 在 ST103 中，哈希值计算电路 100 通过向 DMAC 203 发出写入请求来输出针对第一消息 (A0 到 A52) 的哈希值。

[0164] 在 ST104 中，CPU 201 在哈希值计算电路 100 的寄存器 116 中设置针对第二消息 (B0 到 B3) 的处理请求。

[0165] 在 ST105 中，哈希值计算电路 100 通过向 DMAC 203 发出读取请求来读取第二消息 (B0 到 B3) 的数据，并执行针对该消息的哈希值计算。

[0166] 在 ST106 中，哈希值计算电路 100 通过向 DMAC 203 发出写入请求来输出针对第二消息 (B0 到 B3) 的哈希值。

[0167] 在 ST107 中，CPU 201 在哈希值计算电路 100 的寄存器 116 中设置针对第三消息 (A53 到 A95) 的处理请求。

[0168] 在 ST108 中，哈希值计算电路 100 通过向 DMAC 203 发出读取请求来读取第三消息 (A53 到 A95) 的数据，并执行针对该消息的哈希值计算。

[0169] 在 ST109 中，哈希值计算电路 100 通过向 DMAC 203 发出写入请求来输出针对第三消息 (A53 到 A95) 的哈希值。

[0170] (哈希值计算的详细情况)

[0171] 图 8A 至图 10E 是示出针对各个步骤的哈希值计算的操作的时序图。注意，TXXX 代表基于作为分步处理和 DMA 传输处理的基本单位的操作时钟周期 T 的时间段。在本实施例中，根据具有周期 T 的操作时钟同步设计哈希值计算电路 100。例如，消息 A 的每个 512 位的块的数据对应于 16 个、即第 0 到第 15 个 32 位的扩展消息 W0 到 W15。例如，将消息 A 的第 0 个块描述为 A0，将块 A0 的第 0 个和第 1 个 32 位的数据描述为 A0_W00-W01，将块 A0 的最初的 16 个扩展消息描述为 EA0_W00-W15。同样地，将块 A0 的第 0 个步骤的内部状态值描述为 SA_000，将块 A0 的哈希中间值描述为 HA0。以下将描述针对各个单位时间段的各个单元的操作。

[0172] 在 T000 中，哈希值计算控制器 113 将 DMA 写入请求信号 122 断言到 DMAC 203 以写入数据。在 T001 中，DMAC 203 返回 DMA 写入确认信号 123，并将从哈希值输出单元 114 作为 DMA 输出数据 116 输出的哈希值 (在这种情况下为 HAX) 的最初的 64 位传输到存储器 202。之后，从 T002 到 T005，DMAC 203 将哈希值 HAX 传输到存储器 202。在该区间期间，哈希值计算控制器 113 对 DMAC 203 断言 DMA 写入确认信号 123 的次数进行计数。在这种情况下，哈希值计算控制器 113 确认在 T005 以前断言了 DMA 写入确认信号 123 三次，并在 T006 中取消断言 (deassert)DMA 写入请求信号 122。

[0173] 在 T006 和 T007 中，CPU 201 经由总线 205 和总线信号 117 设置寄存器 116。在这

种情况下，CPU 201 在图 4 中的寄存器 116 的“作业开始”区域中设置“开始哈希值计算”的标志，并且在“处理继续”区域中设置“使用内部状态值的初始值”的标志。另外，CPU 201 在“消息标识符”区域中设置“处理消息 A”的标志，在“块的数量”区域中设置“针对 53 个块进行处理”的标志，并且在“哈希初始值”区域中设置“SHA-1 算法的初始值”。

[0174] 在 T008 中，响应于在寄存器 116 的“作业开始”区域中设置“开始哈希值计算”的标志，哈希值计算控制器 113 将 DMA 读取请求信号 122 断言到 DMAC 203 以读取数据。在 T009 中，DMAC 203 返回 DMA 读取确认信号 123。同时，DMAC 203 将存储在存储器 202 中的消息 A 的第一个块 A0 的最初的 64 位 (A0_W00-W01) 传输到哈希值计算电路 100。

[0175] 在 T010 中，消息存储单元 101 存储 64 位的数据 A0_W00-W01。之后，从 T011 到 T023，DMAC 203 将块 A0 从存储器 202 传输到哈希值计算电路 100。在该区间期间，哈希值计算控制器 113 对 DMAC 203 断言 DMA 确认信号 123 的次数进行计数。哈希值计算控制器 113 确认在 T023 以前断言了 DMA 确认信号 123 八次，并在 T024 中取消断言 DMA 读取请求信号 122。在寄存器 116 的“作业开始”区域中设置了“开始哈希值计算”的标志的状态下，块计数器 137 根据 DMA 读取请求信号 122 的取消断言的次数对要处理的块的数量进行计数。设块计数器 137 的计数器值为 BC，在这种情况下 BC ＝ 1。此外，在 T024 中，消息存储单元 101 存储块 A0。

[0176] 在 T025 中，哈希值计算控制器 113 断言块加载信号 124。

[0177] 在 T026 中，扩展消息存储单元 102 检测块加载信号 124 的断言，并加载存储在消息存储单元 101 中的块 A0。此时，扩展消息存储单元 102 通过将块 A0 分割为 16 个 32 位的数据 EA0_W00 到 EA0_W15 来存储块 A0。在块加载信号 124 的断言后，步骤计数器 138 使用针对各个基本处理时间段 T 的时钟（未示出）来对步骤的数量进行计数。设步骤计数器 138 的计数器值为 SC，在这种情况下 SC ＝ 1。之后，步骤计数器 138 针对作为一个分步处理的单位的基本处理时间段 T 的各时钟进行向上计数，直到计数器值 SC 达到 80。响应于将存储在消息存储单元 101 中的数据加载到扩展消息存储单元 102，哈希值计算控制器 113 断言 DMA 读取请求信号 122 以读取下一个块的数据。

[0178] 在 T026 中，消息扩展处理器 103 输入存储在扩展消息存储单元 102 中的扩展消息 133(EA0_W00 到 EA0_W15)，并计算 32 位的数据 EA0_W16。

[0179] 在 T026 中，哈希值计算控制器 113 响应于在寄存器 116 的“处理继续”区域中设置的“使用内部状态值的初始值”的标志和步骤计数器 138 的计数器值＝ 1，断言哈希初始值选择信号 X 127。在 T026 中，哈希值计算控制器 113 响应于步骤计数器 138 的计数器值＝ 1 来断言哈希中间值选择信号 125。

[0180] 在 T026 中，由于断言了哈希初始值选择信号 X 127，因此选择器 112 输出作为其自身的输入的哈希中间值 119 和哈希初始值 126 中的哈希初始值 126。选择器 105 响应于哈希中间值选择信号 125 的断言，输出作为其自身的输入的来自选择器 112 的输出和内部状态值 134 中的来自选择器 112 的输出。结果，选择器 105 输出哈希初始值 126。

[0181] 在 T026 中，分步处理器 104 输入存储在扩展消息存储单元 102 中的数据 EA0_W00 和哈希初始值 126，并通过对它们应用 SHA-1 的步骤 0 的处理来计算内部状态值 SA0_00。

[0182] 在 T027 中，步骤计数器 138 将其计数器值 SC 向上计数到 2。

[0183] 在 T027 中，扩展消息存储单元 102 存储数据 EA0_W01 到 EA0_W15，和在 T026 中消

息扩展处理器 103 计算的数据 EA0_W16。

[0184] 在 T027 中，内部状态值存储单元 106 存储在 T026 中计算的内部状态值 SA0_00。

[0185] 在 T027 中，消息扩展处理器 103 输入存储在扩展消息存储单元 102 中的扩展消息 133(EA0_W01 到 EA0_W16)，并计算 32 位的数据 EA0_W17。

[0186] 在 T027 中，哈希值计算控制器 113 响应于步骤计数器 138 的计数器值≠ 1，取消断言哈希初始值选择信号 X 127 和哈希中间值选择信号 125。

[0187] 在 T027 中，选择器 105 响应于哈希中间值选择信号 125 的取消断言，输出作为其自身的输入的来自选择器 112 的输出和内部状态值 134 中的内部状态值 134。结果，选择器 105 输出内部状态值 SA000。

[0188] 在 T027 中，分步处理器 104 输入扩展消息 EA0_W01 和内部状态值 SA0_00，并通过对它们应用 SHA-1 的步骤 1 的处理来计算内部状态值 SA0_01。

[0189] 在 T027 中，DMAC 203 返回 DMA 读取确认信号 123，并将 64 位的数据 A1_W00-W01 从存储器 202 传输到哈希值计算电路 100。

[0190] 在 T028 中，步骤计数器 138 将其计数器值 SC 向上计数到 3。

[0191] 在 T028 中，扩展消息存储单元 102 存储数据 EA0_W02 到 EA0_W16 和在 T027 中消息扩展处理器 103 计算的数据 EA0_W17。

[0192] 在 T028 中，内部状态值存储单元 106 存储在 T027 中计算的内部状态值 SA0_01。

[0193] 在 T028 中，消息扩展处理器 103 输入存储在扩展消息存储单元 102 中的扩展消息 133(EA0_W02 到 EA0_W17)，并计算 32 位的数据 EA0_W18。

[0194] 在 T028 中，选择器 105 响应于哈希中间值选择信号 125 的取消断言，输出作为其自身的输入的来自选择器 112 的输出和内部状态值 134 中的内部状态值 134。结果，选择器 105 输出内部状态值 SA0_01。

[0195] 在 T028 中，分步处理器 104 输入存储在扩展消息存储单元 102 中的数据 EA0_W02 和内部状态值 SA0_01，并通过对它们应用 SHA-1 的步骤 2 的处理来计算内部状态值 SA0_02。

[0196] 在 T028 中，消息存储单元 101 存储 64 位的数据 A1_W00-W01。

[0197] 之后，从 T029 到 T041，DMAC 203 将块 A1 从存储器 202 DMA 传输到哈希值计算电路 100。在该区间期间，哈希值计算控制器 113 对 DMAC203 断言 DMA 读取确认信号 123 的次数进行计数。哈希值计算控制器 113 确认在 T041 以前 DMAC 203 断言了 DMA 确认信号 123 八次，并在 T042 中取消断言 DMA 读取请求信号 122。在 T042 中，消息存储单元 101 存储块 A1。响应于 DMA 读取请求信号 122 的取消断言，块计数器 137 将其计数器值 BC 向上计数到 2。

[0198] 在从 T029 到 T105 的区间期间，哈希值计算电路 100 执行 SHA-1 的步骤 2 到步骤 79 的处理。在该区间期间，步骤计数器 138 将计数器值 SC 从 3 向上计数到 80。结果，在 T106 中，内部状态值存储单元 106 存储内部状态值 SA0_79 作为 SHA-1 的步骤 79 的处理结果。

[0199] 由于在 T105 之前计数了预定 80 个步骤，因此在 T106 中步骤计数器 138 将计数器值 SC 清空为 0。

[0200] 在 T106 中，哈希值计算控制器 113 响应于以下内容，来断言哈希初始值选择信号

Y 128：

[0201] •在寄存器 116 的“处理继续”区域中设置“使用内部状态值的初始值”的标志；以及

[0202] • 在 T105 中，步骤计数器 138 的计数器值 SC = 80。

[0203] 在 T106 中，选择器 108 响应于哈希初始值选择信号 Y 128 的断言，输出作为其自身的输入的哈希初始值 126 和哈希中间值 119 中的哈希初始值 126。

[0204] 在 T106 中，加法处理器 107 输入内部状态值 134(SA0_79) 和哈希初始值 126，并计算哈希中间值 HA0。

[0205] 在 T106 中，由于寄存器 116 的“消息标识符”区域指示“处理消息 A”，因此哈希值计算控制器 113 断言哈希中间值 A 加载信号 129。此外，哈希值计算控制器 113 断言块加载信号 124。

[0206] 哈希中间值存储单元 A 109 检测哈希中间值 A 加载信号 129 的断言，并在 T107 中存储哈希中间值 HA0。在 T107 中，由于寄存器 116 的“消息标识符”区域指示“处理消息 A”，因此哈希值计算控制器 113 断言消息 A 选择信号 131。接着，选择器 111 将来自哈希中间值存储单元 A 109 的输出和来自哈希中间值存储单元 B 110 的输出中的来自哈希中间值存储单元 A 109 的输出 (HA0) 输出到哈希值输出单元 114。

[0207] 扩展消息存储单元 102 检测块加载信号 124 的断言，并在 T107 中加载存储在消息存储单元 101 中的块 A1。此时，扩展消息存储单元 102 通过将块 A1 分割为 16 个 32 位的数据 EA1_W00 到 EA1_W15 来存储块 A1。哈希值计算控制器 113 响应于扩展消息存储单元 102 对存储在消息存储单元 101 中的数据的存储，断言 DMA 读取请求信号 122 以读取下一个块的数据。

[0208] 在 T107 中，哈希值计算控制器 113 响应于块 A0 的哈希值计算的完成，取消断言哈希初始值选择信号 Y 128。

[0209] 在 T107 中，步骤计数器 138 响应于块加载信号 124 的断言，开始将其计数器值 SC 向上计数到 1。

[0210] 在 T107 中，消息扩展处理器 103 输入存储在扩展消息存储单元 102 中的扩展消息 133(EA1_W00 到 EA1_W15)，并计算 32 位的数据 EA1_W16。

[0211] 由于正在进行块 A1 的处理，因此在 T107 中哈希值计算控制器 113 不断言哈希初始值选择信号 X 127。

[0212] 在 T107 中，选择器 112 响应于哈希初始值选择信号 X 127 的取消断言，输出作为其自身的输入的哈希中间值 119 和哈希初始值 126 中的哈希中间值 119(HA0)。此外，选择器 105 响应于哈希中间值选择信号 125 的断言，输出作为其自身的输入的来自选择器 112 的输出和内部状态值 134 中的来自选择器 112 的输出。结果，选择器 105 输出哈希中间值 119(HA0)。

[0213] 在 T107 中，分步处理器 104 输入存储在扩展消息存储单元 102 中的数据 EA1_W00 和哈希中间值 119(HA0)，并通过对它们应用 SHA-1 的步骤 0 的处理来计算内部状态值 SA1_00。

[0214] 之后，与从 T027 到 T041 的块 A1 的 DMA 传输相同，从 T108 到 T122，DMA 传输块 A2。在 T123 中，哈希值计算控制器 113 取消断言针对块 A1 的 DMA 读取请求信号 122。响应于

DMA 读取请求信号 122 的取消断言，块计数器 137 将其计数器值 BC 向上计数到 3。与从 T027 到 T105 的针对块 A0 的 SHA-1 的步骤 1 到步骤 79 的处理相同，从 T108 到 T186，对块 A1 应用 SHA-1 的步骤 1 到步骤 79 的处理。在该区间期间，步骤计数器 138 将计数器值 SC 从 2 向上计数到 80。结果，在 T187 中，内部状态值存储单元 106 存储内部状态值 SA1_79 作为 SHA-1 的步骤 79 的处理结果。

[0215] 在 T187 中，由于正在进行块 A1 的处理，因此哈希值计算控制器 113 不断言哈希初始值选择信号 Y 128。

[0216] 在 T187 中，选择器 108 响应于哈希初始值选择信号 Y 128 的取消断言，输出作为其自身的输入的哈希初始值 126 和哈希中间值 119(HA0) 中的哈希中间值 119(HA0)。

[0217] 在 T187 中，加法处理器 107 输入内部状态值 134(SA1_79) 和哈希中间值 119(HA0)，并计算哈希中间值 HA1。

[0218] 在 T187 中，由于寄存器 116 的“消息标识符”区域指示“处理消息 A”，因此哈希值计算控制器 113 断言哈希中间值 A 加载信号 129。哈希中间值存储单元 A 109 检测哈希中间值 A 加载信号 129 的断言，并在 T188 中存储哈希中间值 HA1。在这种情况下，由于寄存器 116 的“消息标识符”区域指示“处理消息 A”，因此哈希值计算控制器 113 断言消息 A 选择信号 131。接着，选择器 111 将来自哈希中间值存储单元 A 109 的输出和来自哈希中间值存储单元 B 110 的输出中的来自哈希中间值存储单元 A 109 的输出 (HA1) 输出到哈希值输出单元 114。

[0219] 之后，响应于寄存器 116 的“消息标识符”区域指示“处理消息 A”并且“块的数量”区域指示“针对 53 个块进行处理”，DMA 传输块 A3 到 A52。此外，针对块 A2 到 A52 执行哈希值计算。

[0220] （以块为单位的操作）

[0221] 图 11A 和图 11B（以下总称为图 11）是示出根据本实施例的针对各个块的哈希值计算的操作的时序图。注意，TBXXX 代表针对 81 个时间段 T 的时间段，每个时间段用作块处理的基本单位。上述 T026 到 T106 与 TB0 对应，T107 到 T187 与 TB1 对应。但是，与执行针对各消息的哈希值计算的完成时的 DMA 写传输和下一个消息的最初的块的 DMA 读传输的时间段对应的 TB53 和 TB58 中的各个与针对 26 个时间段 T 的时间段对应。A0(t) 表示输入消息 A0_W00 至 A0_W15，EA0(t) 表示扩展消息 EA0_W00 到 EA0_W79，SA0(t) 表示内部状态值 SA0_00 到 SA0_79。注意，t 代表步骤的数量，XX(t) 的值根据步骤的数量 t 而变化。

[0222] 以下将描述各个块处理时间段的各个单元的操作。注意，还将描述一些分步处理时间段的详细操作。

[0223] 如上所述，在 TB0 中，DMAC 203 将块 A1 从存储器 202 DMA 传输到哈希值计算电路 100。在块 A1 的 DMA 传输完成时，块计数器 137 将其计数器值 BC 向上计数到 2。在 TB1 中，DMAC 203 将块 A2 从存储器 202DMA 传输到哈希值计算电路 100。在块 A2 的 DMA 传输完成时，块计数器 137 将其计数器值 BC 向上计数到 3。

[0224] 如上所述，在 TB0 中，哈希值计算电路 100 输入块 A0 作为消息 A 的第一个块，并计算扩展消息 EA0(t) 和内部状态值 SA0(t)。在更新 SA(t) 的分步处理中，针对各步骤 t 使用第 t 个扩展消息和第 (t-1) 个内部状态值来更新内部状态值，并在步骤 79 中计算内部状态值 SA0_79。最终，将内部状态值 SA0_79 与哈希初始值相加，以计算哈希中间值 HA0。在 TB1

中，哈希中间值存储单元 A 109 存储哈希中间值 HA0。哈希值计算电路 100 输入块 A1，计算扩展消息 EA1(t) 和内部状态值 SA1(t)，并在步骤 79 中计算内部状态值 SA1_79。最终，将内部状态值 SA1_79 与哈希中间值 HA0 相加，以计算哈希中间值 HA1。

[0225] 之后，在 TB2 到 TB51 中，DMAC 203 将块 A3 到 A52 从存储器 202DMA 传输到哈希值计算电路 100。此时，将块计数器 137 的值从 4 向上计数到 53。在 TB2 到 TB52 中，哈希值计算电路 100 执行块 A2 到 A52 的哈希值计算。结果，在 TB53 中，哈希中间值存储单元 A 109 保持哈希中间值 HA52，并且哈希值输出单元 114 输出哈希中间值 HA52。

[0226] 在这种情况下，满足存储在寄存器 116 的“消息标识符”区域和“块的数量”区域中的“处理消息 A”和“针对 53 个块进行处理”的要求。因此，在 TB53 中，哈希值计算控制器 113 清除存储在寄存器 116 的“作业开始”区域中的“开始哈希值计算”的标志和存储在“处理继续”区域中的“使用内部状态值的初始值”的标志。此外，在 TB53 中，哈希值计算控制器 113 将 DMA 写入请求信号 122 断言到 DMAC 203。DMAC 203 返回 DMA 写入确认信号 123，并将从哈希值输出单元 114 输出的哈希中间值 HA52 传输到存储器 202。哈希值计算控制器 113 对 DMAC 203 断言 DMA 写入确认信号 123 的次数进行计数。哈希值计算控制器 113 确认 DMAC 203 断言了 DMA 写入确认信号 123 三次，并取消断言 DMA 写入请求信号 122。

[0227] 在 TB53 中，DMAC 203 检测来自哈希值计算电路 100 的 DMA 写入请求信号 122 的取消断言，并断言中断信号 206，以将中断通知给中断控制器 204。中断控制器 204 使用中断信号（未示出）将哈希中间值 HA52 在存储器 202 中的存储通知给 CPU 201。

[0228] 在 TB53 中，CPU 201 根据来自 DMAC 203 的中断，检测到“从消息的头开始”“针对 53 个块”对“消息 A”的处理完成。接着，CPU 201 经由总线 205 和总线信号 117 设置寄存器 116。在这种情况下，CPU 201 在图 4 所示的寄存器 116 的“作业开始”区域中设置“开始哈希值计算”的标志，还在“处理继续”区域中设置“使用内部状态值的初始值”的标志。另外，CPU 201 在“消息标识符”区域中设置“处理消息 B”的标志，在“块的数量”区域中设置“针对 4 个块进行处理”的标志，并且在“哈希初始值”区域中设置“SHA-1 算法的初始值”。

[0229] 响应于在寄存器 116 的“作业开始”区域中设置的“开始哈希值计算”的标志，在 TB53 中哈希值计算控制器 113 将 DMA 读取请求信号 122 断言到 DMAC 203，以读取数据。DMAC 203 返回 DMA 读取确认信号 123，并将消息 B 的第一个块 B0 DMA 传输到哈希值计算电路 100。接着，消息存储单元 101 存储块 B0。块计数器 137 将其计数器值 BC 向上计数到 1。

[0230] 在 TB54 中，DMA 传输块 B1，并针对块 B0 执行哈希值计算。以下将描述详细情况。

[0231] 在 T4344 中，哈希值计算控制器 113 断言块加载信号 124。在 T4345 中，扩展消息存储单元 102 检测块加载信号 124 的断言，并加载存储在消息存储单元 101 中的块 B0。此时，扩展消息存储单元 102 通过将块 B0 分割为 16 个 32 位的数据 EB0_W00 到 EB0_W15 来存储块 B0。步骤计数器 138 开始将其计数器值 SC 向上计数到 1。哈希值计算控制器 113 响应于扩展消息存储单元 102 对存储在消息存储单元 101 中的数据的存储，断言 DMA 读取请求信号 122，以读取下一个块的数据。

[0232] 在 T4345 中，消息扩展处理器 103 输入存储在扩展消息存储单元 102 中的扩展消息 133(EB0_W00 到 EB0_W15)，并计算 32 位的数据 EB0_W16。

[0233] 在 T4345 中，哈希值计算控制器 113 响应于以下内容，断言哈希初始值选择信号 X 127 和哈希中间值选择信号 125：

[0234] • 在寄存器 116 的“处理继续”区域中设置的“使用内部状态值的初始值”的标志；和

[0235] • 步骤计数器 138 的计数器值 SC = 1。

[0236] 在 T4345 中，选择器 112 响应于哈希初始值选择信号 X 127 的断言，输出作为其自身的输入的哈希中间值 119 和哈希初始值 126 中的哈希初始值 126。此外，选择器 105 响应于哈希中间值选择信号 125 的断言，输出作为其自身的输入的来自选择器 112 的输出和内部状态值 134 中的来自选择器 112 的输出。结果，选择器 105 输出哈希初始值 126。

[0237] 在 T4345 中，分步处理器 104 输入存储在扩展消息存储单元 102 中的数据 EB0_W00 和哈希初始值 126，并通过对它们应用 SHA-1 的步骤 0 的处理来计算内部状态值 SB0_00。

[0238] 在 T4346 中，步骤计数器 138 将其计数器值 SC 向上计数到 2。

[0239] 在 T4346 中，扩展消息存储单元 102 存储数据 EB0_W01 到 EB0_W15，和消息扩展处理器 103 计算的数据 EB0_W16。

[0240] 在 T4346 中，内部状态值存储单元 106 存储内部状态值 SB0_00。

[0241] 在 T4346 中，消息扩展处理器 103 输入存储在扩展消息存储单元 102 中的扩展消息 133(EB0_W01 到 EB0_W16)，并计算 32 位的数据 EB0_W17。

[0242] 在 T4346 中，哈希值计算控制器 113 响应于步骤计数器 138 的计数器值 SC ≠ 1，取消断言哈希初始值选择信号 X 127 和哈希中间值选择信号 125。

[0243] 在 T4346 中，选择器 105 响应于哈希中间值选择信号 125 的取消断言，输出作为其自身的输入的来自选择器 112 的输出和内部状态值 134 中的内部状态值 134。结果，选择器 105 输出内部状态值 SB000。

[0244] 在 T4346 中，分步处理器 104 输入扩展消息 EB0_W01 和内部状态值 SB0_00，并通过对它们应用 SHA-1 的步骤 1 的处理来计算内部状态值 SB0_01。接着，哈希值计算控制器 113 将步骤计数器 138 向上计数。此时，步骤计数器 138 的值为 2。

[0245] 在 T4346 中，DMAC 203 返回 DMA 读取确认信号 123，并将 64 位的数据 B1_W00-W01 从存储器 202 传输到哈希值计算电路 100。

[0246] 在 T4347 中，步骤计数器 138 将其计数器值 SC 向上计数到 3。

[0247] 在 T4347 中，扩展消息存储单元 102 存储数据 EB0_W02 到 EB0_W16 和消息扩展处理器 103 计算的数据 EB0_W17。

[0248] 在 T4347 中，内部状态值存储单元 106 存储内部状态值 SB0_01。

[0249] 在 T4347 中，消息扩展处理器 103 输入存储在扩展消息存储单元 102 中的扩展消息 133(EB0_W02 到 EB0_W17)，并计算 32 位的数据 EB0_W18。

[0250] 在 T4347 中，选择器 105 响应于哈希中间值选择信号 125 的取消断言，输出作为其自身的输入的来自选择器 112 的输出和内部状态值 134 中的内部状态值 134。结果，选择器 105 输出内部状态值 SB0_01。

[0251] 在 T4347 中，分步处理器 104 输入扩展消息 EB0_W02 和内部状态值 SB0_01，并通过对它们应用 SHA-1 的步骤 2 的处理来计算内部状态值 SB0_02。

[0252] 在 T4347 中，消息存储单元 101 存储 DMAC 203 DMA 传输的 64 位的数据 B1_W00-W01。

[0253] 之后，从 T4348 到 T4360，DMAC 203 连续执行块 B1 的从存储器 202 到哈希值计算

电路 100 的 DMA 传输。在该区间期间，哈希值计算控制器 113 对 DMAC 203 断言 DMA 读取确认信号 123 的次数进行计数。在哈希值计算控制器 113 确认 DMAC 203 断言了 DMA 确认信号 123 八次后，其取消断言 DMA 读取请求信号 122。接着，消息存储单元 101 存储块 B1。块计数器 137 将其计数器值 BC 向上计数到 2。

[0254] 从 T4348 到 T4424，哈希值计算电路 100 执行 SHA-1 的步骤 3 到步骤 79 的处理。在该区间期间，步骤计数器 138 在各个分步处理的开始从 4 向上计数到 80。结果，在 T4425 中，内部状态值存储单元 106 存储内部状态值 SB0_79 作为 SHA-1 的步骤 79 的处理结果。

[0255] 在 T4425 中，哈希值计算控制器 113 响应于以下内容，断言哈希初始值选择信号 Y 128：

[0256] •在寄存器 116 的“处理继续”区域中设置的“使用内部状态值的初始值”的标志；和

[0257] •在 T4424 中，步骤计数器 138 的计数器值 SC ＝ 80。

[0258] 在 T4425 中，选择器 108 响应于哈希初始值选择信号 Y 128 的断言，输出作为其自身的输入的哈希初始值 126 和哈希中间值 119 中的哈希初始值 126。

[0259] 在 T4425 中，加法处理器 107 输入内部状态值 134(SB0_79) 和哈希初始值 126，并计算哈希中间值 HB0。

[0260] 在 T4425 中，由于寄存器 116 的“消息标识符”区域指示“处理消息 B”，因此哈希值计算控制器 113 断言哈希中间值 B 加载信号 130。哈希值计算控制器 113 还断言块加载信号 124。在 TB55 时间段期间的 T4426 中，哈希中间值存储单元 B 110 存储哈希中间值 HB0。此外，由于寄存器 116 的“消息标识符”区域指示“处理消息 B”，因此哈希值计算控制器 113 不断言消息 A 选择信号 131。接着，选择器 111 将来自哈希中间值存储单元 A 109 的输出和来自哈希中间值存储单元 B 110 的输出中的来自哈希中间值存储单元 B 110 的输出 (HB0) 输出到哈希值输出单元 114。

[0261] 在 T4426 中，扩展消息存储单元 102 检测块加载信号 124 的断言，并加载存储在消息存储单元 101 中的块 B1。此时，扩展消息存储单元 102 通过将块 B1 分割为 16 个 32 位的数据 EB1_W00 到 EB1_W15 来存储块 B1。哈希值计算控制器 113 响应于扩展消息存储单元 102 对存储在消息存储单元 101 中的数据的存储，断言 DMA 读取请求信号 122，以读取下一个块的数据。

[0262] 在 T4426 中，哈希值计算控制器 113 响应于块 B0 的哈希值计算的完成，取消断言哈希初始值选择信号 Y 128。

[0263] 如上所述，在 TB55 中，哈希中间值存储单元 A 109 存储哈希中间值 HA52，并且哈希中间值存储单元 B 110 存储哈希中间值 HB0。

[0264] 使用在 TB55 中存储在哈希中间值存储单元 B 110 中的哈希中间值 HB0 来进行针对块 B1 的哈希值计算。

[0265] 之后，在 TB55 和 TB56 中，DMAC 203 将块 B2 和 B3 从存储器 202DMA 传输到哈希值计算电路 100。此时，块计数器 137 将计数器值 BC 从 3 向上计数到 4。在 TB55 到 TB57 中，哈希值计算电路 100 执行针对块 B1 到 B3 的哈希值计算。在该区间期间，由于寄存器 116 的“消息标识符”区域指示“处理消息 B”，因此哈希值计算控制器 113 不断言哈希中间值 A 加载信号 129，而根据需要断言哈希中间值 B 加载信号 130。由于该原因，哈希中间值存储

单元 A 109 不存储消息 B 的任何哈希中间值，而哈希中间值存储单元 B 110 存储消息 B 的哈希中间值。由于寄存器 116 的“消息标识符”区域指示“处理消息 B”，因此哈希值计算控制器 113 不断言消息 A 选择信号 131。由于该原因，选择器 111 输出来自哈希中间值存储单元 A 109 的输出和来自哈希中间值存储单元 B 110 的输出中的来自哈希中间值存储单元 B 110 的输出。其它处理与针对块 A1 到 A3 的处理相同。

[0266] 结果，在 TB55 到 TB57 中，计算哈希中间值 HB1 到 HB3。在 TB58 中，哈希中间值存储单元 A 109 存储针对消息 A 的块 A0 到 A52 的哈希中间值 HA52，并且哈希中间值存储单元 B 110 存储针对消息 B 的块 B0 到 B3 的哈希中间值 HB3。如图 5 所示，由于消息 B 包括块 B0 到 B3，因此输出哈希中间值 HB3 作为消息 B 的哈希值 HB。在 TB58 中，由于寄存器 116 的“消息标识符”区域指示“处理消息 B”，因此哈希值计算控制器 113 不断言消息 A 选择信号 131。由于该原因，选择器 111 将作为其自身的输入的来自哈希中间值存储单元 A 109 的输出 (HA52) 和来自哈希中间值存储单元 B 110 的输出 (HB) 中的来自哈希中间值存储单元 B 110 的输出 (HB) 输出到哈希值输出单元 114。

[0267] 在这种状态下，满足存储在寄存器 116 的“消息标识符”和“块的数量”区域中的“处理消息 B”和“针对 4 个块进行处理”的要求。接着，在 TB58 中，哈希值计算控制器 113 清除存储在寄存器 116 的“作业开始”区域中的“开始哈希值计算”的标志和存储在“处理继续”区域中的“使用内部状态值的初始值”的标志。此外，在 TB58 中，哈希值计算控制器 113 将 DMA 写入请求信号 122 断言到 DMAC 203。DMAC 203 返回 DMA 写入确认信号 123，并将来自哈希值输出单元 114 的哈希值 HB 传输到存储器 202。哈希值计算控制器 113 对 DMAC 203 断言 DMA 写入确认信号 123 的次数进行计数。哈希值计算控制器 113 确认 DMAC 203 断言了 DMA 写入确认信号 123 三次，并取消断言 DMA 写入请求信号 122。

[0268] 在 TB58 中，DMAC 203 检测哈希值计算电路 100 对 DMA 写入请求信号 122 的取消断言，断言中断信号 206，并将中断通知给中断控制器 204。接着，中断控制器 204 使用中断信号（未示出）将哈希值 HB 在存储器 202 中的存储通知给 CPU 201。

[0269] 在 TB58 中，CPU 201 根据来自 DMAC 203 的中断，检测到“使用内部状态值的初始值”“针对 4 个块”对“消息 B”对处理完成。接着，CPU201 经由总线 205 和总线信号 117 设置寄存器 116。在这种情况下，CPU 201 在图 4 所示的寄存器 116 的“作业开始”区域中设置“开始哈希值计算”的标志，并且在“处理继续”区域中设置“使用哈希中间值”的标志。另外，CPU 201 在“消息标识符”区域中设置“处理消息 A”的标志，并且在“块的数量”区域中设置“针对 43 个块进行处理”的标志。此时，哈希值计算控制器 113 将块计数器 137 清零。

[0270] 响应于在寄存器 116 的“作业开始”区域中设置的“开始哈希值计算”的标志，在 TB58 中，哈希值计算控制器 113 将 DMA 读取请求信号 122 断言到 DMAC 203，以读取数据。DMAC 203 返回 DMA 读取确认信号 123，并将消息 A 的块 A53 DMA 传输到哈希值计算电路 100。消息存储单元 101 存储块 A53。接着，块计数器 137 将其计数器值 BC 向上计数到 1。

[0271] 在 TB59 中，DMA 传输块 A54，并针对块 A53 执行哈希值计算。以下将描述详细情况。

[0272] 在 T4694 中，哈希值计算控制器 113 断言块加载信号 124。在 T4695 中，扩展消息存储单元 102 检测块加载信号 124 的断言，并加载存储在消息存储单元 101 中的块 A53。此

时，扩展消息存储单元 102 通过将块 A53 分割为 16 个 32 位的数据 EA53_W00 到 EA53_W15 来存储块 A53。哈希值计算控制器 113 响应于扩展消息存储单元 102 对存储在消息存储单元 101 中的数据的存储，断言 DMA 读取请求信号 122，以读取下一个块的数据。

[0273] 在 T4695 中，步骤计数器 138 将其计数器值 SC 向上计数到 1。

[0274] 在 T4695 中，消息扩展处理器 103 输入存储在扩展消息存储单元 102 中的扩展消息 133(EA53_W00 到 EA53_W15)，并计算 32 位的数据 EA53_W16。

[0275] 哈希值计算控制器 113 响应于在寄存器 116 的“处理继续”区域中设置的“使用哈希中间值”的标志，取消断言哈希初始值选择信号 X 127。

[0276] 在 T4695 中，由于寄存器 116 的“消息标识符”区域指示“处理消息 A”，因此哈希值计算控制器 113 断言消息 A 选择信号 131。由此，选择器 111 输出作为其自身的输入的来自哈希中间值存储单元 A 109 的输出 (HA52) 和来自哈希中间值存储单元 B 110 的输出 (HB) 中的来自哈希中间值存储单元 A 109 的输出 (HA52)。选择器 112 响应于哈希初始值选择信号 X 127 的取消断言，输出作为其自身的输入的哈希中间值 119(HA52) 和哈希初始值 126 中的哈希中间值 119(HA52)。选择器 105 响应于哈希中间值选择信号 125 的断言，输出作为其自身的输入的来自选择器 112 的输出和内部状态值 134 中的来自选择器 112 的输出。结果，选择器 105 输出哈希中间值 119(HA52)。

[0277] 在 T4695 中，分步处理器 104 输入存储在扩展消息存储单元 102 中的数据 EA53_W00 和哈希中间值 HA52，并通过对它们应用 SHA-1 的步骤 0 的处理来计算内部状态值 SA53_00。

[0278] 在 T4696 中，步骤计数器 138 将其计数器值 SC 向上计数到 2。

[0279] 在 T4696 中，扩展消息存储单元 102 存储数据 EA53_W01 到 EA53_W15，和消息扩展处理器 103 计算的数据 EA53_W16。

[0280] 在 T4696 中，内部状态值存储单元 106 存储内部状态值 SA53_00。

[0281] 在 T4696 中，消息扩展处理器 103 输入存储在扩展消息存储单元 102 中的扩展消息 133(EA53_W01 到 EA53_W16)，并计算 32 位的数据 EA53_W17。

[0282] 在 T4696 中，由于正在进行 SHA-1 的步骤 1 的处理，因此哈希值计算控制器 113 取消断言哈希初始值选择信号 X 127。

[0283] 在 T4696 中，选择器 105 响应于哈希中间值选择信号 125 的取消断言，输出作为其自身的输入的来自选择器 112 的输出和内部状态值 134 中的内部状态值 134。结果，选择器 105 输出内部状态值 SA53_00。

[0284] 在 T4696 中，分步处理器 104 输入扩展消息 EA53_W01 和内部状态值 SA53_00，并通过对它们应用 SHA-1 的步骤 1 的处理来计算内部状态值 SA53_01。

[0285] 在 T4696 中，DMAC 203 返回 DMA 读取确认信号 123，并将 64 位的数据 A54_W00-W01 从存储器 202 传输到哈希值计算电路 100。在 T4697 中，步骤计数器 138 将其计数器值 SC 向上计数到 3。

[0286] 在 T4697 中，扩展消息存储单元 102 存储数据 EA53_W02 到 EA53_W16 和消息扩展处理器 103 计算的数据 EA53_W17。

[0287] 在 T4697 中，内部状态值存储单元 106 存储内部状态值 SA53_01。

[0288] 在 T4697 中，消息扩展处理器 103 输入存储在扩展消息存储单元 102 中的扩展消

息 133(EA53_W02 到 EA53_W17)，并计算 32 位的数据 EA53_W18。

[0289] 在 T4697 中，选择器 105 响应于哈希中间值选择信号 125 的取消断言，输出作为其自身的输入的来自选择器 112 的输出和内部状态值 134 中的内部状态值 134。结果，选择器 105 输出内部状态值 SA53_01。

[0290] 在 T4697 中，分步处理器 104 输入扩展消息 EA53_W02 和内部状态值 SA53_01，并通过对它们应用 SHA-1 的步骤 2 的处理来计算内部状态值 SA53_02。

[0291] 在 T4697 中，消息存储单元 101 存储 64 位的数据 A54_W00-W01。

[0292] 之后，从 T4698 到 T4710，DMAC 203 连续执行块 A54 的从存储器 202 到哈希值计算电路 100 的 DMA 传输。在该区间期间，哈希值计算控制器 113 对 DMAC 203 断言 DMA 读取确认信号 123 的次数进行计数。在 T4711 中，在哈希值计算控制器 113 确认 DMAC 203 断言了 DMA 确认信号 123 八次后，其取消断言 DMA 读取请求信号 122。接着，消息存储单元 101 存储块 A54。块计数器 137 将其计数器值 BC 向上计数到 2。

[0293] 从 T4697 到 T4774，哈希值计算电路 100 执行 SHA-1 的步骤 2 到步骤 79 的处理。在该区间期间，在各个分步处理开始时，步骤计数器 138 将其计数器值 SC 从 3 向上计数到 80。结果，在 T4775 中，内部状态值存储单元 106 存储内部状态值 SA53_79 作为 SHA-1 的步骤 79 的处理结果。

[0294] 在 T4775 中，哈希值计算控制器 113 响应于在寄存器 116 的“处理继续”区域中设置的“使用哈希中间值”的标志，取消断言哈希初始值选择信号 Y 128。

[0295] 在 T4775 中，选择器 108 响应于哈希初始值选择信号 Y 128 的取消断言，输出作为其自身的输入的哈希初始值 126 和哈希中间值 119 中的哈希中间值 119。

[0296] 在 T4775 中，加法处理器 107 输入内部状态值 134(SA53_79) 和哈希中间值 119(HA52)，并计算哈希中间值 HA53。

[0297] 在 T4775 中，哈希值计算控制器 113 断言块加载信号 124。

[0298] 在 T4775 中，由于寄存器 116 的“消息标识符”区域指示“处理消息 A”，因此哈希值计算控制器 113 断言哈希中间值 A 加载信号 129。在 TB60 时间段期间的 T4776 中，哈希中间值存储单元 A 109 存储哈希中间值 HA53。此外，由于寄存器 116 的“消息标识符”区域指示“处理消息 A”，因此哈希值计算控制器 113 断言消息 A 选择信号 131。接着，选择器 111 将来自哈希中间值存储单元 A 109 的输出和来自哈希中间值存储单元 B110 的输出中的来自哈希中间值存储单元 A 109 的输出 (HA53) 输出到哈希值输出单元 114。

[0299] 在 T4776 中，扩展消息存储单元 102 检测到块加载信号 124 的断言，并加载存储在消息存储单元 101 中的块 A54。此时，扩展消息存储单元 102 通过将块 A54 分割为 16 个 32 位的数据 EA54_W00 到 EA54_W15 来存储块 A54。哈希值计算控制器 113 响应于扩展消息存储单元 102 对存储在消息存储单元 101 中的数据的存储，断言 DMA 读取请求信号 122，以读取下一个块的数据。

[0300] 在 T4776 中，哈希值计算控制器 113 响应于块 A53 的哈希值计算的完成，取消断言哈希初始值选择信号 Y 128。

[0301] 如上所述，在 TB60 中，哈希中间值存储单元 A 109 存储哈希中间值 HA53，并且哈希中间值存储单元 B 110 存储哈希值 HB。

[0302] 之后，从 TB60 到 TB100，DMAC 203 将块 A55 到 A95 从存储器 202DMA 传输到哈希值

计算电路 100。此时，块计数器 137 将计数器值 BC 从 3 向上计数到 43。从 TB60 到 TB101，哈希值计算电路 100 执行针对块 A54 到 A95 的哈希值计算。在该区间期间，由于寄存器 116 的“消息标识符”区域指示“处理消息 A”，因此哈希值计算控制器 113 不断言哈希中间值 B 加载信号 130，而根据需要断言哈希中间值 A 加载信号 129。由于该原因，哈希中间值存储单元 B 110 不存储消息 A 的任何哈希中间值，而哈希中间值存储单元 A 109 存储消息 A 的哈希中间值。由于寄存器 116 的“消息标识符”区域指示“处理消息 A”，因此哈希值计算控制器 113 断言消息 A 选择信号 131。由于该原因，选择器 111 输出来自哈希中间值存储单元 A 109 的输出和来自哈希中间值存储单元 B 110 的输出中的来自哈希中间值存储单元 A 109 的输出。其它处理与针对其它块的处理相同。

[0303] 结果，在 TB102 中，哈希中间值存储单元 A 109 针对消息 A 的块 A0 到 A95 存储哈希中间值 HA95。如图 5 所示，由于消息 A 包括块 A0 到 A95，因此输出哈希中间值 HA95 作为消息 A 的哈希值 HA。在 TB 102 中，哈希值计算控制器 113 断言消息 A 选择信号 131。由此，选择器 111 将作为其自身的输入的来自哈希中间值存储单元 A 109 的输出 (HA) 和来自哈希中间值存储单元 B 110 的输出 (HB) 中的来自哈希中间值存储单元 A 109 的输出 (HA) 输出到哈希值输出单元 114。

[0304] 在这种状态下，满足存储在寄存器 116 的“消息标识符”和“块的数量”区域中的“处理消息 A”和“针对 43 个块进行处理”的要求。因此，在 TB102 中，哈希值计算控制器 113 清除存储在寄存器 116 的“作业开始”区域中的“开始哈希值计算”的标志和存储在“处理继续”区域中的“使用哈希中间值”的标志。此外，在 TB102 中，哈希值计算控制器 113 将 DMA 写入请求信号 122 断言到 DMAC 203。DMAC 203 返回 DMA 写入确认信号 123，并将哈希值 HA 从哈希值输出单元 114 传输到存储器 202。哈希值计算控制器 113 对 DMAC 203 断言 DMA 写入确认信号 123 的次数进行计数。哈希值计算控制器 113 确认 DMAC 203 断言了 DMA 写入确认信号 123 三次，并取消断言 DMA 写入请求信号 122。

[0305] 在 TB102 中，DMAC 203 检测到哈希值计算电路 100 进行的 DMA 写入请求信号 122 的取消断言，断言中断信号 206，并将中断通知给中断控制器 204。接着，中断控制器 204 使用中断信号（未示出）将哈希值 HA 在存储器 202 中的存储通知给 CPU 201。

[0306] 如上所述，根据本实施例，CPU 依次请求哈希值计算电路执行针对第一、第二和第三消息的哈希值计算，使得在消息 A 的中间先处理消息 B。注意，第一消息包括块 A0 到 A52，第二消息包括块 B0 到 B3，第三消息包括块 A53 到 A95。接着，将作为针对第一消息的哈希值计算结果的哈希中间值存储到哈希值计算电路中。在第二消息的哈希值计算完成后，使用所存储的第一消息的哈希中间值来执行针对第三消息的哈希值计算。结果，与将哈希中间值临时写出到外部存储器并重新加载的传统配置相比，能够减少与外部存储器交换哈希中间值所需的时间开销，并能够实现以高响应速度进行高效率的哈希值计算。

[0307] 在本实施例中，由于将消息的一个块的数据存储在哈希值计算电路中，因此能够消除从外部存储器传输消息的各块数据所需的开销时间的需要。由于该原因，能够实现更高效率的哈希值计算。

[0308] 在本实施例中，在完成针对紧接的前一个块的哈希值计算时，将存储在电路中的一个块的数据加载到扩展处理器，接着发出从外部存储器传输下一个块的数据传输请求。但是，本发明不限于此。例如，在完成针对该块的哈希值计算之前将加载的该块的数据存储

在存储单元中，接着可以发出针对下一个块的数据传输请求。即使在处理中间针对关注的块的哈希值计算异常中断时，由于在电路中存储了关注的块的数据，因此也能够获得减少从外部存储器重新加载该数据所需的开销的效果。

[0309] 本实施例例示了将 SHA-1 用作哈希函数。但是，哈希函数可以使用例如 MD5 和 SHA-256 的其它算法。

[0310] 在本实施例中，针对各步骤依次生成扩展消息。但是，可以在最初同时生成扩展消息。

[0311] 在本实施例的配置中，能够存储针对两个不同的消息的哈希中间值。通过配置三个或更多个哈希中间值存储单元，能够中断和重新开始针对三个或更多个不同的消息的哈希值计算。

[0312] 在本实施例的配置中，配置了各自具有能够存储一个哈希中间值的哈希中间值存储区域的多个哈希中间值存储单元。但是，本发明不限于这种特定配置。例如，可以配置各自具有能够存储多个哈希中间值的哈希中间值存储区域的一个或多个哈希中间值存储单元。

[0313] 在本实施例中，各个消息的哈希中间值和哈希中间值存储单元之间的对应关系是固定的，如消息 A 的哈希中间值存储在哈希中间值存储单元 A 中，消息 B 的哈希中间值存储在哈希中间值存储单元 B 中。但是，例如，可以配置存储表示哈希中间值存储区域和消息的哈希中间值之间的对应关系的对应关系信息的对应关系信息存储单元，可以根据存储在对应关系信息存储单元中的对应关系信息来决定哈希中间值存储区域。

[0314] 在本实施例中，CPU 在哈希电路外部对哈希值计算的填充处理进行处理。但是，也可以在哈希电路内部对填充处理进行处理。

[0315] 在本实施例中，DMAC 用作用于在哈希值计算电路和外部存储器之间交换消息和哈希值的设备。但是，可以使用其它传输设备。

[0316] 在本实施例的示例中，DMA 输入 / 输出数据的位宽 (bit width) 为 64 位。但是，可以使用其它位数。

[0317] 在本实施例中，哈希值计算的各步骤的处理的基本处理时间段 T 等于 DMA 传输处理的基本处理时间段 T。但是，分步处理和 DMA 传输处理的基本处理时间段可以不同。

[0318] 在本实施例的示例中，CPU 在哈希值计算电路的寄存器中设置消息的块的数量，哈希值计算电路通过对 DMA 确认信号进行计数来检测具有 CPU 设置的块的数量的消息的供应。但是，可以使用其它方法。例如，CPU 可以通过在寄存器中设置消息传输完成，来通知完成消息传输。

[0319] 注意，本发明的实施例不限于上述配置，可以进行各种变型。

[0320] << 第二实施例 >>

[0321] 在第一实施例中，CPU 201 针对各消息在哈希值计算电路 100 的寄存器中设置处理继续信息和消息标识符信息等。第二实施例将说明作为与消息的数据同步的边带信号的输入数据属性信号包括处理继续信息和消息标识符信息等的情况。

[0322] (哈希值计算电路的配置)

[0323] 图 12 是示出根据第二实施例的哈希值计算电路的配置的框图。下面，参照图 12 仅描述与第一实施例的不同之处。

[0324] 附图标记 137 表示对哈希值计算电路 100 接收的第一消息（以下称作消息 A）的块的数量进行计数的块计数器。附图标记 140 表示对哈希值计算电路 100 接收的第二消息（以下称作消息 B）的块的数量进行计数的块计数器 X。在针对形成消息的给定数量的块的哈希值计算完成时，哈希值计算控制器 113 将块计数器 137 或块计数器 X 140 的计数器值清零。附图标记 139 表示与 DMA 输入数据 120 同步地从 DMAC 203 输出到哈希值计算电路 100 的输入数据属性信号。输入数据属性信号的内容包括消息标识符信息和处理继续信息。

[0325] （寄存器的存储内容）

[0326] 图 13 是示出存储在本实施例的哈希值计算电路 100 内的寄存器 116 中的信息的图。以下仅描述与第一实施例的不同之处。

[0327] 寄存器 116 具有针对各个消息类型的作业开始信息、块的数量信息和哈希初始值信息的存储区域。

[0328] 在本实施例中，在哈希值计算电路 100 开始作业之前，CPU 201 将针对要处理的多个消息的作业开始信息、块的数量信息和哈希初始值信息的设置写入寄存器 116 中。

[0329] 在第一实施例中，CPU 201 预先决定发出处理请求以中断针对消息 A 的哈希值计算，并执行针对消息 B 的哈希值计算。即，CPU 201 决定向哈希值计算电路 100 发出针对作为两个消息、即包括块 A0 到 A52 的消息和包括块 A53 到 A95 的消息的消息 A 的处理请求。在本实施例中，CPU 201 首先在哈希值计算电路 100 的寄存器中设置针对要进行哈希值计算的多个消息的信息。即，CPU 201 在寄存器 116 的预定区域中设置包括 96 个块的消息 A 的信息和包括 4 个块的消息 B 的信息。在 CPU 201 设置寄存器并且哈希值计算电路 100 开始针对对应的处理请求的哈希值计算后，CPU 201 决定中断消息 A 的哈希值计算。此外，CPU 201 控制 DMAC 203，从消息 A 的块 A52 开始，从块 B0 开始将消息 B 的数据依次传输到哈希值计算电路。

[0330] 哈希值计算电路 100 针对在寄存器中设置的多个消息，根据包括在输入数据属性信号 139 中的消息标识符信息和处理继续信息，确定各消息类型和处理继续的存在 / 不存在。此外，哈希值计算电路 100 针对各消息，根据需要执行哈希值计算。

[0331] 哈希值计算电路 100 根据以下内容，检测到在接收到消息 A 的在寄存器中设置的 96 个块的数据之前，接收到消息 B 的块数据：

[0332] • 对传输的各消息的块的数量进行计数的块计数器 137 的计数器值 BC；和

[0333] • 包括在属性信息中的消息标识符。

[0334] 接着，哈希值计算电路 100 确定中断消息 A 的哈希值计算。

[0335] （哈希值计算）

[0336] 图 14A 和图 14B 是示出在以图 6 所示的顺序输入两个消息（块 A0 到 A95 及块 B0 到 B3）时，本实施例的哈希值计算的操作序列的流程图。

[0337] 在 ST201 中，CPU 201 在哈希值计算电路 100 的寄存器 116 中设置针对第一消息 (A0 到 A95) 的处理请求。

[0338] 在 ST202 中，CPU 201 在哈希值计算电路 100 的寄存器 116 中设置针对第二消息 (B0 到 B3) 的处理请求。

[0339] 在 ST203 中，哈希值计算电路 100 向 DMAC 203 发出读取请求，以读取消息的一个块的数据。

[0340] 在ST204中，哈希值计算电路100根据属性信号的消息标识符，确定读取块数据的消息。如果消息标识符指示消息A，则处理进行到ST205；如果消息标识符指示消息B，则处理进行到ST209。

[0341] 在ST205中，哈希值计算电路100确定是否正在进行针对紧接的前一个块的哈希值计算。如果正在进行哈希值计算，则处理等待，直到完成该块的哈希值计算为止；如果哈希值计算完成，则处理进行到ST206。

[0342] 在ST206中，哈希值计算电路100执行针对第一消息(A0到A95)的一个块的哈希值计算。

[0343] 在ST207中，哈希值计算电路100确定针对包括总数＝96的块的第一消息(A0到A95)的哈希值计算是否完成。如果哈希值计算完成，则处理进行到ST208；否则，处理返回到ST203。

[0344] 在ST208中，哈希值计算电路100向DMAC 203发出写入请求，以输出针对第一消息(A0到A95)的哈希值。

[0345] 在ST209中，哈希值计算电路100确定是否正在进行针对紧接的前一个块的哈希值计算。如果正在进行哈希值计算，则处理等待，直到完成该块的哈希值计算为止；如果哈希值计算完成，则处理进行到ST210。

[0346] 在ST210中，哈希值计算电路100执行针对第二消息(B0到B3)的一个块的哈希值计算。

[0347] 在ST211中，哈希值计算电路100确定针对包括总数＝4的块的第二消息(B0到B3)的哈希值计算是否完成。如果哈希值计算完成，则处理进行到ST212；否则，处理返回到ST203。

[0348] 在ST212中，哈希值计算电路100向DMAC 203发出写入请求，以输出针对第二消息(B0到B3)的哈希值。

[0349] 在ST213中，哈希值计算电路100确定其它消息的处理是否完成。如果处理完成，则结束处理；否则，处理返回到ST203。

[0350] 在本实施例中，与在第一实施例中相同，在T006和T007(未示出)中，CPU 201经由总线205和总线信号117设置寄存器116。在这种情况下，CPU 201在图12所示的寄存器116的用于消息A的“作业开始”区域中设置“开始哈希值计算”的标志。另外，CPU 201在“块的数量”区域中设置“针对96个块进行处理”的标志，并且在“哈希初始值”区域中设置“SHA-1算法的初始值”。同样地，CPU 201在用于消息B的“作业开始”区域中设置“开始哈希值计算”的标志，在“块的数量”区域中设置“针对4个块进行处理”的标志，并且在“哈希初始值”区域中设置“SHA-1算法的初始值”。

[0351] 之后，哈希值计算电路100接收DMAC 203从存储器传输的消息的DMA输入数据120和输入数据属性信号139。哈希值计算电路100根据包括在输入数据属性信号139中的消息标识符和处理继续信息，以及针对各消息存储在寄存器中的块的总数和DMA传输块的数量，执行针对各消息的哈希值计算。

[0352] (哈希值计算的详细情况)

[0353] 图15A至图16E是示出针对各个步骤的哈希值计算的操作的时序图。图15A至图16E分别示出将消息A切换到消息B时的操作以及将消息B切换到消息A时的操作。以下

仅描述与第一实施例的不同之处。

[0354] 从T000到T4237的处理与第一实施例中的处理相同。在T4237中，加法处理器107输入内部状态值SA51_79和哈希中间值HA50以执行加法处理，并输出哈希中间值HA51。在T4238中，哈希中间值存储单元A 109存储哈希中间值HA51。

[0355] 在T4237中，哈希值计算控制器113断言块加载信号124。在T4238中，扩展消息存储单元102检测到块加载信号124的断言，并加载存储在消息存储单元101中的块A52。

[0356] 假定CPU 201控制DMAC 203，以在块A52的传输完成后，开始从存储器202向哈希值计算电路100传输消息B。在T4238中，哈希值计算控制器113响应于扩展消息存储单元102对存储在消息存储单元101中的块A52的数据的存储，断言DMA读取请求信号122，以读取下一个块的数据。

[0357] 从T4238到T4318，执行针对块A52的哈希值计算。

[0358] 另一方面，从T4239到T4253，DMAC 203返回DMA数据读取确认信号123，同时将块B0从存储器202传输到哈希值计算电路100。在T4254中，消息存储单元101存储块B0。哈希值计算控制器113与块B0的加载同时地，加载输入数据属性信号139，以识别指示“消息B”的信息和指示“使用内部状态值的初始值”的信息。设块计数器X 140的计数器值为BCX，块计数器X 140将与消息B的块B0对应的计数器值BCX向上计数到1。块计数器137存储“53”作为与消息A的块A52对应的计数器值BC。

[0359] 在T4319中，哈希中间值存储单元A 109存储哈希中间值HA52。由于仅完成了针对包括总数＝96的块的消息A中的从第一个块开始的53个块的哈希值计算，因此在T4319中，哈希值计算控制器113不断言DMA写入请求信号122。此外，DMAC 203不将哈希中间值HA52从哈希值计算电路100 DMA传输到存储器202。

[0360] （以块为单位的操作）

[0361] 图17A和图17B（以下总称为图17）是示出根据本实施例的针对各个块的哈希值计算的操作的时序图。注意，还描述一些分步处理时间段的详细操作。

[0362] 在TB52中，哈希值计算控制器113将DMA读取请求信号122断言到DMAC 203以读取数据。DMAC 203返回DMA读取确认信号123，并将消息B的第一个块B0 DMA传输到哈希值计算电路100。消息存储单元101存储块B0。

[0363] 在TB53中，DMA传输块B1，并执行针对块B0的哈希值计算。在TB54中，由于哈希值计算控制器113断言哈希中间值B加载信号130，因此哈希中间值存储单元B 110存储在TB53中计算的哈希中间值HB0。哈希值计算控制器113取消断言消息A选择信号131。接着，选择器111将来自哈希中间值存储单元A 109的输出和来自哈希中间值存储单元B 110的输出中的来自哈希中间值存储单元B 110的输出（HB0）输出到哈希值输出单元114。

[0364] 以这种方式，在TB54中，哈希中间值存储单元A 109存储哈希中间值HA52，并且哈希中间值存储单元B 110存储哈希中间值HB0。

[0365] 在TB54中，使用存储在哈希中间值存储单元B 110中的哈希中间值HB0来执行针对块B1的哈希值计算。

[0366] 之后，在TB54和TB55中，DMAC 203将块B2和B3从存储器202DMA传输到哈希值计算电路100。

[0367] 假定CPU 201控制DMAC 203，在块B3的传输完成后，重新开始将消息A的其余数

据从存储器 202 传输到哈希值计算电路 100。接着，在 TB56 中，DMAC 203 将形成消息 A 的块 A53 从存储器 202 DMA 传输到哈希值计算电路 100。此时，DMAC 203 传送指示“使用哈希中间值”的值作为针对消息 A 的输入数据属性信号 139 中的处理继续信息。在 DMAC 203 完成块 A53 的传输并且哈希值计算电路 100 存储块 A53 的数据后，哈希值计算控制器 113 加载输入数据属性信号 139。接着，哈希值计算控制器 113 识别指示“消息 A”的信息和指示“使用哈希中间值”的信息。块计数器 X 140 存储“4”作为计数器值 BCX。块计数器 139 与消息 A 的块 A53 对应地将计数器值 BC 向上计数到 54。注意，在第一实施例中，在消息 B 的哈希值计算完成时进行针对消息 A 的块 A53 到 A95 的寄存器设置后，传输块 A53。对比而言，在本实施例中，能够在消息 B 的哈希值计算完成前，传输块 A53。

[0368] 在 TB54 到 TB56 中，哈希值计算电路 100 执行针对块 B1 到 B3 的哈希值计算。在该区间期间，哈希值计算控制器 113 不断言哈希中间值 A 加载信号 129，而根据需要断言哈希中间值 B 加载信号 130。由于该原因，哈希中间值存储单元 A 109 不存储消息 B 的任何哈希中间值，而哈希中间值存储单元 B 110 存储消息 B 的哈希中间值。此外，哈希值计算控制器 113 取消断言消息 A 选择信号 131。因此，选择器 111 输出来自哈希中间值存储单元 A 109 的输出和来自哈希中间值存储单元 B 110 的输出中的来自哈希中间值存储单元 B 110 的输出。其它处理与针对块 A1 到 A3 的处理相同。

[0369] 结果，在 TB54 到 TB56 中，哈希值计算电路 100 计算哈希中间值 HB1 到 HB3。

[0370] 在 TB57 中，哈希中间值存储单元 A 109 存储针对消息 A 的块 A0 到 A52 的哈希中间值 HA52，并且哈希中间值存储单元 B 110 存储针对消息 B 的块 B0 到 B3 的哈希中间值 HB3。如图 5 所示，由于消息 B 包括块 B0 到 B3，因此输出哈希中间值 HB3 作为消息 B 的哈希值 HB。在 TB57 中，哈希值计算控制器 113 取消断言消息 A 选择信号 131。由于该原因，选择器 111 将作为其自身的输入的来自哈希中间值存储单元 A 109 的输出 (HA52) 和来自哈希中间值存储单元 B 110 的输出 (HB) 中的来自哈希中间值存储单元 B 110 的输出 (HB) 输出到哈希值输出单元 114。

[0371] 此时，满足存储在寄存器 116 的用于消息 B 的“块的数量”区域中的“针对 4 个块进行处理”的要求。由此，在 TB57 中，哈希值计算控制器 113 清除存储在寄存器 116 的“作业开始”区域中的“开始哈希值计算”的标志。此外，哈希值计算控制器 113 清除块计数器 X 140 的计数器值 BCX。在 TB57 中，哈希值计算控制器 113 将 DMA 写入请求信号 122 断言到 DMAC 203。DMAC 203 返回 DMA 写入确认信号 123，并将来自哈希值输出单元 114 的哈希值 HB 传输到存储器 202。哈希值计算控制器 113 对 DMAC 203 断言 DMA 写入确认信号 123 的次数进行计数。哈希值计算控制器 113 确认 DMAC 203 断言了 DMA 写入确认信号 123 三次，接着取消断言 DMA 写入请求信号 122。

[0372] 在 TB57 中，DMAC 203 检测到哈希值计算电路 100 进行的 DMA 写入请求信号 122 的取消断言，断言中断信号 206，并将中断通知给中断控制器 204。接着，中断控制器 204 使用中断信号（未示出）将哈希值 HB 在存储器 202 中的存储通知给 CPU 201。

[0373] 在 TB57 中，CPU 201 根据来自 DMAC 203 的中断，检测到“使用内部状态值的初始值”“针对 4 个块”对“消息 B”的处理完成。

[0374] 在 TB57 中，DMA 传输块 A54，并执行针对块 A53 的哈希值计算。之后，在 TB58 到 TB98 中，DMAC 203 将块 A55 到 A95 从存储器 202DMA 传输到哈希值计算电路 100。在 TB58

到 TB99 中，哈希值计算电路 100 执行针对块 A54 到 A95 的哈希值计算。在该区间期间，哈希值计算控制器 113 不断言哈希中间值 B 加载信号 130，而根据需要断言哈希中间值 A 加载信号 129。由于该原因，哈希中间值存储单元 B 110 不存储消息 A 的任何哈希中间值，而哈希中间值存储单元 A 109 存储消息 A 的哈希中间值。哈希值计算控制器 113 断言消息 A 选择信号 131。由于该原因，选择器 111 输出来自哈希中间值存储单元 A 109 的输出和来自哈希中间值存储单元 B110 的输出中的来自哈希中间值存储单元 A 109 的输出。其它处理与针对其它块的处理相同。

[0375] 结果，在 TB100 中，哈希中间值存储单元 A 109 存储针对块 A0 到 A95 的哈希中间值 HA95。如图 5 所示，由于消息 A 包括块 A0 到 A95，因此输出哈希中间值 HA95 作为消息 A 的哈希值 HA。在 TB100 中，哈希值计算控制器 113 断言消息 A 选择信号 131。由于该原因，选择器 111 将作为其自身的输入的来自哈希中间值存储单元 A 109 的输出 (HA) 和来自哈希中间值存储单元 B 110 的输出 (HB) 中的来自哈希中间值存储单元 A109 的输出 (HA) 输出到哈希值输出单元 114。

[0376] 此时，满足存储在寄存器 116 的用于消息 A 的“块的数量”区域中的“针对 96 个块进行处理”的要求。接着，在 TB100 中，哈希值计算控制器 113 清除存储在寄存器 116 的“作业开始”区域中的“开始哈希值计算”的标志。此外，哈希值计算控制器 113 清除块计数器 137 的计数器值 BC。

[0377] 在 TB100 中，哈希值计算控制器 113 将 DMA 写入请求信号 122 断言到 DMAC 203。DMAC 203 返回 DMA 写入确认信号 123，并将来自哈希值输出单元 114 的哈希值 HA 传输到存储器 202。哈希值计算控制器 113 对 DMAC 203 断言 DMA 写入确认信号 123 的次数进行计数。哈希值计算控制器 113 确认 DMAC 203 断言了 DMA 写入确认信号 123 三次，接着取消断言 DMA 写入请求信号 122。

[0378] 在 TB100 中，DMAC 203 检测到哈希值计算电路 100 进行的 DMA 写入请求信号 122 的取消断言，断言中断信号 206，并将中断通知给中断控制器 204。接着，中断控制器 204 使用中断信号（未示出）将哈希值 HA 在存储器 202 中的存储通知给 CPU 201。

[0379] 在 TB 100 中，CPU 201 根据来自 DMAC 203 的中断检测到“使用内部状态值的初始值”“针对 96 个块”对“消息 A”的处理完成。

[0380] 如上所述，根据本实施例，从附加到消息的数据的输入数据属性信号中提取消息标识符和处理继续信息，并进行识别。接着，在处理中间中断针对第一消息的哈希值计算，并且首先执行针对另外的第二消息的哈希值计算时，与第一实施例相比，能够进一步缩短哈希值计算时间段。即，能够减少在直到第一消息的中间块的哈希值计算之后将哈希值计算结果（哈希中间值）DMA 传输到存储器所需的时间，和在针对各消息的哈希值计算开始时进行针对消息的寄存器设置所需的时间。此外，能够更早完成针对第二消息的哈希值计算。

[0381] 更具体而言，在示出第一实施例中的各个步骤的哈希值计算的时序图的图 9A 至图 9E 中，在 TB58 内的 T4669 的定时，输出消息 B 的哈希值。对比而言，在示出第二实施例中的各个步骤的哈希值计算的时序图的图 16A 至图 16E 中，在 TB57 内的 T4643 的定时，输出消息 B 的哈希值 HB。

[0382] 在第二实施例中，与第一实施例相比，哈希值计算时间段缩短了与第一实施例中的 TB53 的时间段对应的 26 个基本处理时间段。能够将第一消息的未处理部分的第一个块

的 DMA 传输时间段隐藏在第二消息的哈希值计算时间段中，并且能够比第一实施例更早地重新开始第一消息的哈希值计算。更具体而言，在图 11A 和图 11B 中，在 TB60 内的 T4776 的定时，输出第一实施例中的针对消息 A 的第一个块到块 A53 的哈希中间值 HA53。相比而言，在图 16A 到图 16E 中，在 TB58 内的 T4724 的定时，输出第二实施例中的针对消息 A 的第一个块到块 A53 的哈希中间值 HA53。与第一实施例相比，在第二实施例中，哈希值计算时间段缩短了与第一实施例的 TB53 和 TB58 的时间段的和对应的 52 个基本处理时间段。

[0383] 在本实施例中，在完成针对紧接的前一个块的哈希值计算时，将存储在电路中的一个块的数据加载到扩展处理器，并且在加载后发出从外部存储器传输下一个块的数据传输请求。虽然处理时间段延长，但是可以在完成针对一个加载的块的哈希值计算之前将该块的数据存储在存储单元中，之后，可以发出针对下一个块的数据传输请求。此时，即使在处理中间针对关注的块的哈希值计算异常中断，由于关注的块的数据存储在电路中，因此也能够获得减少从外部存储器重新加载该数据所需的开销的效果。

[0384] 本实施例例示了 SHA-1 用作哈希函数。但是，哈希函数可以使用例如 MD5 和 SHA-256 的其它算法。

[0385] 在本实施例中，针对各步骤依次生成扩展消息。但是，可以在最初同时生成扩展消息。

[0386] 在本实施例的配置中，能够存储针对两个不同的消息的哈希中间值。但是，本发明不限于这种特定配置。例如，通过配置三个或者更多个哈希中间值存储单元、块计数器和寄存器设置区域等，能够中断和重新开始针对三个或者更多个不同的消息的哈希值计算。

[0387] 在本实施例的配置中，配置了各自具有能够存储一个哈希中间值的哈希中间值存储区域的多个哈希中间值存储单元。但是，本发明不限于这种特定配置。例如，可以配置各自具有能够存储多个哈希中间值的哈希中间值存储区域的一个或多个哈希中间值存储单元。

[0388] 在本实施例中，各个消息的哈希中间值和哈希中间值存储单元之间的对应关系是固定的，如消息 A 的哈希中间值存储在哈希中间值存储单元 A 中，消息 B 的哈希中间值存储在哈希中间值存储单元 B 中。但是，例如，可以配置存储表示哈希中间值存储区域和消息的哈希中间值之间的对应关系的对应关系信息的哈希中间值存储信息存储单元，可以根据存储在哈希中间值存储信息存储单元中的对应关系信息来决定哈希中间值存储区域。

[0389] 在本实施例中，CPU 在哈希电路的外部对哈希值计算的填充处理进行处理。但是，也可以在哈希电路内部对填充处理进行处理。

[0390] 在本实施例中，DMAC 用作用于在哈希值计算电路和外部存储器之间交换消息和哈希值的设备。但是，也可以使用其它传输设备。

[0391] 在本实施例的示例中，DMA 输入 / 输出数据的位宽为 64 位。但是，可以使用其它位数。

[0392] 在本实施例中，哈希值计算的各步骤的处理的基本处理时间段 T 等于 DMA 传输处理的基本处理时间段 T。但是，分步处理和 DMA 传输处理的基本处理时间段可以不同。

[0393] 在本实施例中，输入数据属性信号包括消息标识符信息和处理继续信息，并且将其数据宽度定义为 8 位。但是，输入数据属性信号还可以包括例如消息优先级信息的其它信息，并可以根据信息来改变信号的数据宽度。

[0394] 在本实施例中，哈希值计算电路通过对各消息的输入块的数量进行计数来识别输入消息的块编号。可替换地，输入数据属性信号还可以包括块编号。

[0395] 在本实施例中，CPU 在哈希值计算电路的寄存器中设置消息的块的数量，哈希值计算电路通过对 DMA 确认信号进行计数，来检测具有 CPU 设置的块的数量的消息的供应。但是，可以使用其它方法。例如，CPU 可以通过在寄存器中设置消息传输完成来通知消息传输的完成。

[0396] 在本实施例中，最初在寄存器中设置关于进行哈希值计算的消息 A 和 B 的设置，并根据输入消息针对消息 A 或 B 执行哈希值计算。但是，在需要在针对消息 A 或 B 的哈希值计算中间开始针对消息 C 的哈希值计算时，可以在处理中间增加针对消息 C 的哈希处理请求的寄存器设置。在这种情况下，能够根据输入消息来执行针对消息 A、B 和 C 的哈希值计算。

[0397] 注意，本发明的实施例不限于上述配置，可以进行各种变型。

[0398] << 第三实施例 >>

[0399] 在第二实施例中，CPU 预先在哈希值计算电路内的寄存器中设置作业开始信息、块的数量信息和哈希初始值信息，来作为与各消息关联的处理请求的信息。在第三实施例中，除了上述信息之外，CPU 还预先在哈希值计算电路内的寄存器中设置消息优先级信息。

[0400] （哈希值计算电路的配置）

[0401] 图 18 是示出根据本实施例的哈希值计算电路的配置的框图。下面，参照图 18 仅描述与第二实施例的不同。

[0402] 附图标记 141 表示存储块数据的消息存储单元 X。在满足以下所有条件的情况下，消息存储单元 X 141 在哈希值计算完成时对存储在消息存储单元 101 中的数据进行存储。

[0403] • 存储在消息存储单元 101 中的块数据的消息的优先级低。

[0404] • 正在进行哈希值计算的块的消息的优先级低。

[0405] • 正在进行哈希值计算的块存储在其自身中。

[0406] 附图标记 142 表示块加载信号 X，该块加载信号 X 从哈希值计算控制器 113 输出，以将存储在消息存储单元 101 中的消息的数据加载到消息存储单元 X。附图标记 143 表示从消息存储单元 X 141 输出到稍后描述的选择器 144 的消息 X。附图标记 144 表示选择消息 132 和消息 X 143 中的一个、并将所选择的信息输出到扩展消息存储单元 102 的选择器。附图标记 145 表示作为选择器 144 的控制信号而从哈希值计算控制器 113 输出的消息 X 选择信号。

[0407] （寄存器的存储内容）

[0408] 图 19 是示出存储在哈希值计算电路 100 内的寄存器 116 中的信息的图。以下仅描述与第二实施例的不同之处。

[0409] 寄存器 116 具有针对各个消息类型的作业开始信息、块的数量信息、哈希初始值信息和消息优先级信息的存储区域。

[0410] 在本实施例中，在 T006 和 T007 中，与在第二实施例中相同，CPU 201 经由总线 205 和总线信号 117 设置寄存器 116。在这种情况下，CPU 201 在图 19 所示的寄存器 116 的用于消息 A 的“作业开始”区域中设置“开始哈希值计算”的标志。此外，CPU 201 在“块的数量”区域中设置“针对 96 个块进行处理”的标志，在“哈希初始值”区域中设置“SHA-1 算法

的初始值”，并且在“消息优先级”区域中设置“低优先级”的标志。同样地，CPU 201 在用于消息 B 的“作业开始”区域中设置“开始哈希值计算”的标志。此外，CPU 201 在“块的数量”区域中设置“针对 4 个块进行处理”的标志，在“哈希初始值”区域中设置“SHA-1 算法的初始值”，并且在“消息优先级”区域中设置“高优先级”的标志。

[0411] 之后，哈希值计算电路 100 接收 DMAC 203 从存储器传输的消息的 DMA 输入数据 120 和输入数据属性信号 139。哈希值计算电路 100 根据包括在输入数据属性信号 139 中的消息标识符信息和处理继续信息，以及针对各消息存储在寄存器中的预定区域中的块的总数和 DMA 传输块的数量，执行针对各消息的哈希值计算。

[0412] （哈希值计算）

[0413] 图 20A、图 20B 和图 20C 是示出在以图 6 所示的顺序输入两个消息（块 A0 到 A95 及块 B0 到 B3）时，根据本实施例的哈希值计算的操作序列的流程图。

[0414] 在 ST301 中，CPU 201 在哈希值计算电路 100 的寄存器 116 中设置针对第一消息 (A0 到 A95) 的处理请求。

[0415] 在 ST302 中，CPU 201 在哈希值计算电路 100 的寄存器 116 中设置针对第二消息 (B0 到 B3) 的处理请求。

[0416] 在 ST303 中，哈希值计算电路 100 向 DMAC 203 发出读取请求，以读取消息的一个块的数据。

[0417] 在 ST304 中，哈希值计算电路 100 根据属性信号的消息标识符来确定读取的块数据的消息。如果消息标识符信息指示消息 A，则处理进行到 ST305 ；如果消息标识符信息指示消息 B，则处理进行到 ST312。

[0418] 在 ST305 中，哈希值计算电路 100 确定是否正在进行针对紧接的前一个块的哈希值计算。如果正在进行哈希值计算，则处理等待，直到完成该块的哈希值计算为止 ；如果哈希值计算完成，则处理进行到 ST306。

[0419] 在 ST306 中，哈希值计算电路 100 确定消息存储单元 X 141 是否存储具有低优先级的第一消息的放弃块。如果消息存储单元 X 存储第一消息的放弃块的数据，则处理进行到 ST307 ；否则，处理跳至 ST309。

[0420] 在 ST307 中，哈希值计算电路 100 执行针对具有低优先级的第一消息的放弃的块的哈希值计算。

[0421] 在 ST308 中，哈希值计算电路 100 确定针对包括总数＝ 96 的块的第一消息 (A0 到 A95) 的哈希值计算是否完成。如果哈希值计算完成，则处理跳至 ST311 ；否则，处理进行到 ST309。

[0422] 在 ST309 中，哈希值计算电路 100 执行针对第一消息 (A0 到 A95) 的一个块的哈希值计算。

[0423] 在 ST310 中，哈希值计算电路 100 确定针对包括总数＝ 96 的块的第一消息 (A0 到 A95) 的哈希值计算是否完成。如果哈希值计算完成，则处理进行到 ST311 ；否则，处理返回到 ST303。

[0424] 在 ST311 中，哈希值计算电路 100 向 DMAC 203 发出写入请求，以输出针对第一消息 (A0 到 A95) 的哈希值。

[0425] 在 ST312 中，哈希值计算电路 100 确定紧接的前一个块是否为具有高优先级的第

二消息的块。如果紧接的前一个块是具有高优先级的第二消息的块，则处理进行到 ST313；如果紧接的前一个块是具有低优先级的第一消息的块，则处理跳至 ST314。

[0426] 在 ST313 中，哈希值计算电路 100 确定是否正在进行针对紧接的前一个块的哈希值计算。如果正在进行哈希值计算，则处理等待，直到完成该块的哈希值计算为止；如果哈希值计算完成，则处理进行到 ST314。

[0427] 在 ST314 中，哈希值计算电路 100 执行针对第二消息 (B0 到 B3) 的一个块的哈希值计算。

[0428] 在 ST315 中，哈希值计算电路 100 确定针对包括总数＝ 4 的块的第二消息 (B0 到 B3) 的哈希值计算是否完成。如果哈希值计算完成，则处理进行到 ST316；否则，处理返回到 ST303。

[0429] 在 ST316 中，哈希值计算电路 100 向 DMAC 203 发出写入请求，以输出针对第二消息 (B0 到 B3) 的哈希值。

[0430] 在 ST317 中，哈希值计算电路 100 确定其它消息的处理是否完成。如果处理完成，则结束处理；否则，处理返回到 ST303。

[0431] （哈希值计算的详细情况）

[0432] 图 21A 至图 23F 是示出根据本实施例的各个步骤的哈希值计算的操作的时序图。图 21A 至图 23F 分别示出消息 A 的开始步骤的操作、将消息 A 切换到消息 B 时的操作、和将消息 B 切换到消息 A 时的操作。以下仅描述与第二实施例的不同之处。

[0433] 从 T000 到 T024 的处理与第二实施例中的处理相同。在 T025 中，哈希值计算控制器 113 断言块加载信号 124。由于存储在消息存储单元中的消息 A 具有低优先级，因此哈希值计算控制器 113 断言块加载信号 124 和块加载信号 X 142。消息存储单元 X 141 检测到块加载信号 X 142 的断言，并在 T026 中加载存储在消息存储单元 101 中的块 A0。此外，扩展消息存储单元 102 检测到块加载信号 124 的断言，并在 T026 中加载来自选择器 144 的输出。此时，由于哈希值计算控制器 113 不断言消息 X 选择信号 145，因此选择器 144 输出消息 132 和消息 X 143 中的消息 132。

[0434] 从 T000 到 T4237，执行与第二实施例基本相同的处理。但是，在本实施例中，消息存储单元 X 141 根据消息的优先级来存储消息 132，并且选择器 144 选择来自消息存储单元 101 的输出和来自消息存储单元 X 141 的输出中的一个，并将所选择的消息输出到扩展消息存储单元 102。

[0435] 在 T4237 中，哈希值计算控制器 113 断言块加载信号 124。扩展消息存储单元 102 检测到块加载信号 124 的断言，并在 T4238 中加载存储在消息存储单元 101 中的块 A52 作为从选择器 144 的输出。此时，扩展消息存储单元 102 通过将块 A52 分割为 16 个 32 位的数据 EA52_W00 到 EA52_W15 来存储块 A52。在从 T4238 到 T4255 中，哈希值计算电路 100 执行针对消息 A 的块 A52 的步骤 0 到步骤 17 的处理。

[0436] 在 T4238 中，哈希值计算控制器 113 响应于扩展消息存储单元 102 对存储在消息存储单元 101 中的数据的存储，断言 DMA 读取请求信号 122，以读取下一个块的数据。从 T4238 到 T4253，哈希值计算电路 100 经由 DMA 传输来加载块 B0，并且在 T4254 中，消息存储单元 101 存储块 B0。

[0437] 在 T4255 中，哈希值计算控制器 113 根据输入数据属性信号 139 中的消息标识符

信息，检测到消息 B。此外，哈希值计算控制器 113 根据寄存器 116 的“消息优先级”区域中的信息，检测到消息 B 具有“高优先级”。接着，哈希值计算控制器 113 断言块加载信号 124，以放弃针对在 T4255 以前处理的消息 A 的块 A52 的分步处理，并先执行具有高优先级的消息 B 的哈希值计算。扩展消息存储单元 102 检测到块加载信号 124 的断言，并在 T4256 中加载作为来自选择器 144 的输出的存储在消息存储单元 101 中的块 B0。此时，由于在 T4255 中，哈希值计算控制器 113 不断言块加载信号 X 142，因此消息存储单元 X 141 不加载作为来自消息存储单元 101 的输出的消息 132（块 B0）。

[0438] 之后，从 T4256 到 T4579，哈希值计算电路 100 执行针对消息 B 的哈希值计算，从 T4580 到 T4585，DMAC 203 输出消息 B 的哈希值 HB。

[0439] 在 T4499 中，哈希值计算控制器 113 响应于将存储在消息存储单元 101 中的消息 B 的最后的块 B3 加载到扩展消息存储单元 102，断言 DMA 读取请求信号 122。接着，读取下一个消息的数据。从 T4500 到 T4514，DMAC 203 DMA 传输消息 A 的块 A53。在 T4515 中，消息存储单元 101 存储块 A53。此时，虽然存储在消息存储单元 101 中的消息 A 具有低优先级，但由于存储在消息存储单元 X 141 中的数据的哈希值计算尚未完成，因此哈希值计算控制器 113 不断言块加载信号 X 142。因此，消息存储单元 X 141 不加载作为来自消息存储单元 101 的输出的消息 132（块 A53）。

[0440] 在 T4500 中，哈希值计算控制器 113 加载输入数据属性信号 139 并检测到重新开始了消息 A 的加载。因此，在 T4501 中，哈希值计算控制器 113 断言消息 X 选择信号 145。接着，选择器 144 输出消息 132 和消息 X 143 中的消息 X 143。在 T4579 中，哈希值计算控制器 113 断言块加载信号 124。在 T4580 中，扩展消息存储单元 102 检测到块加载信号 124 的断言，并加载作为选择器 144 的输出的消息 X 143(A52)。哈希值计算控制器 113 在 T4580 中取消断言消息 X 选择信号 145。从 T4580 开始，重新开始之前在处理中间放弃的块 A52 的处理。

[0441] （以块为单位的操作）

[0442] 图 24A 和图 24B（以下总称为图 24）是示出根据本实施例的针对各个块的哈希值计算的操作的时序图。

[0443] 与第二实施例中相同，在 TB52 中，DMAC 203 将块 B0 DMA 传输到哈希值计算电路 100。但是，在 TB56 内的 T4580 的定时，DMAC 203 从哈希值计算电路 100 传输消息 B 的哈希值 HB。在第二实施例中，在 TB57 内的 T4643 的定时，哈希值计算电路 100 输出哈希值 HB。因此，在第三实施例中，与第二实施例相比，消息 B 的哈希值的输出开始定时缩短了 63 个基本处理时间段。注意，通过从一个块的 81 个基本处理时间段中减去存储消息 B 的块 B0 的数据所需的 18 个基本处理时间段，来计算 63 个基本处理时间段。这 18 个基本处理时间段也是执行在处理中间放弃的哈希中间值 A52 的哈希值计算的时间段。

[0444] 另一方面，在本实施例中，在 TB58 内的 T4742 的定时，哈希值计算单元 100 输出哈希中间值 HA53。在第二实施例中，在 TB58 内的 T4724 定时，哈希值计算单元 100 输出哈希中间值 HA53。因此，在第三实施例中，与第二实施例相比，消息 A 的哈希值的输出开始定时延迟了 18 个基本处理时间段。

[0445] 在本实施例中，消息 B 的消息优先级高，但是本发明并不限于此。当消息 B 的消息优先级与消息 A 同样低时，与在第二实施例中相同，哈希值计算单元 100 不在处理中间放弃

块 52 的哈希值计算。换言之，在块 A52 的哈希中间值的生成之后，哈希值计算单元 100 执行针对块 B0 的哈希值计算。

[0446] 如上所述，根据本实施例，通过从附加到该消息的数据的输入数据属性信号中提取目标消息来识别目标消息，并且增加了进一步对存储在消息存储单元中的消息进行存储的第二消息存储单元。例如，下面分析在处理中间中断针对第一消息的哈希值计算，并首先执行针对另外的第二消息的哈希值计算的情况。根据本实施例的配置，在存储第二消息的数据之前，放弃针对正在处理的第一消息的某个块的哈希值计算，并能够优先处理第二消息的第一个块。因此，更早完成针对第二消息的哈希值计算。

[0447] 本实施例例示了 SHA-1 用作哈希函数。但是，哈希函数可以使用例如 MD5 和 SHA-256 的其它算法。

[0448] 在本实施例中，针对各步骤依次生成扩展消息。但是，也可以在最初同时生成扩展消息。

[0449] 在本实施例的配置中，能够存储针对两个不同消息的哈希中间值。但是，本发明不限于这种特定配置。例如，通过配置三个或更多个哈希中间值存储单元、块计数器和寄存器设置区域等，能够中断和重新开始针对三个或更多个不同的消息的哈希值计算。在本实施例的配置中，配置各自具有能够存储一个哈希中间值的哈希中间值存储区域的多个哈希中间值存储单元。但是本发明不限于这种特定配置。例如，可以配置各自具有能够存储多个哈希中间值的哈希中间值存储区域的一个或多个哈希中间值存储单元。

[0450] 在上述描述中，各个消息的哈希中间值和哈希中间值存储单元之间的对应关系是固定的，如消息 A 和 B 的哈希中间值分别存储在哈希中间值存储单元 A 和 B 中。但是，本发明不限于此。例如，可以配置存储表示哈希中间值存储区域和消息的哈希中间值之间的对应关系的对应关系信息的哈希中间值存储信息存储单元，并可以根据存储在哈希中间值存储信息存储单元中的对应关系信息来决定哈希中间值存储区域。

[0451] 在本实施例中，消息优先级包括两个等级，即高优先级和低优先级。可替换的，消息优先级可以包括三个以上等级，并可以优先执行针对具有较高优先级的消息的哈希值计算。

[0452] 在本实施例中，配置进一步对存储在第一消息存储单元中的消息进行存储的另一个消息存储单元。然而，本发明不限于此。例如，除了第一消息存储单元外，可以根据优先级等级数和哈希中间值存储单元的数量，配置两个或更多个消息存储单元。

[0453] 在本实施例中，CPU 在哈希电路的外部对哈希值计算的填充处理进行处理。但是，也可以在哈希电路内部对填充处理进行处理。

[0454] 在本实施例中，DMAC 用作用于在哈希值计算电路和外部存储器之间交换消息和哈希值的设备。但是，也可以使用其它传输设备。

[0455] 在本实施例中，DMA 输入 / 输出数据的位宽为 64 位。但是，可以使用其它位数。

[0456] 在本实施例中，哈希值计算的各步骤的处理的基本处理时间段 T 等于 DMA 传输处理的基本处理时间段 T。但是，分步处理和 DMA 传输处理的基本处理时间段可以不同。

[0457] 本实施例中，CPU 预先在寄存器的预定区域中设置消息优先级作为处理请求的信息。可替换地，输入数据属性信号可以包括消息优先级。

[0458] 在本实施例中，输入数据属性信号包括消息标识符信息和处理继续信息，并且数

据宽度为 8 位。但是，本发明不限于此。例如，输入数据属性信号还可以包括例如消息优先级信息、块标识符等的其它信息，并可以根据包括的信息来改变信号的数据宽度。

[0459] 在本实施例中，哈希值计算电路通过对各消息的输入块的数量进行计数来识别输入消息的块编号。可替换地，输入数据属性信号还可以包括块编号。

[0460] 在本实施例中，CPU 在哈希值计算电路的寄存器中设置消息的块的数量，哈希值计算电路通过对 DMA 确认信号进行计数来识别具有 CPU 设置的块的数量的消息的供应。但是，可以使用其它方法。例如，CPU 可以通过在寄存器中设置消息传输完成来通知消息传输的完成。

[0461] 在本实施例中，在处理中间根据存储在寄存器的预定区域中的消息优先级的信息，放弃针对具有低优先级的消息的块的哈希值计算。然而，本发明不限于此。例如，属性信号中的消息标识符还可以表示消息优先级，或者可以输入其它处理中断指令信号，从而通过优先执行针对具有高优先级的消息的哈希值计算，来确定放弃针对正在进行计算的消息的哈希值计算。

[0462] 在本实施例的描述中，最初在寄存器中设置关于作为进行哈希值计算的消息的消息 A 和 B 的设置，接着根据输入消息来执行针对消息 A 或 B 的哈希值计算。但是，本发明不限于此。例如，下面分析需要在针对消息 A 或 B 的哈希值计算的中间开始针对消息 C 的哈希值计算的情况。在这种情况下，在处理中间增加针对消息 C 的哈希处理请求的寄存器设置时，能够根据输入消息来执行针对消息 A、B 和 C 的哈希值计算。

[0463] 注意，本发明的实施例不限于上述配置，可以进行各种变型。

[0464] 如上所述，根据第一到第三实施例的配置，能够减少通过针对各个块选择要处理的消息来执行哈希值计算时的开销，并能够保持哈希值计算的安全性。

[0465] << 第四实施例 >>

[0466] 本实施例将说明支持 MD5、SHA1 和 SHA512 作为哈希算法，并且并行处理最多两个消息的哈希值计算装置。以下将并行执行的两个处理称作处理 A 和处理 B。

[0467] 哈希值计算针对包括 16 个字 (word) 的各块，对消息进行处理，并输出 N 个字的哈希值作为其最终结果。该哈希值计算包括如下一系列处理。

[0468] • 将消息分割为各自包括 16 个字的块，并将预定数据添加到消息的最末位置，使得最后的块也包括 16 个字 (以下称作填充处理)。

[0469] • 针对各个包括 16 个字的块执行稍后描述的消息扩展处理、分步处理和加法处理，从而生成哈希中间值。

[0470] 消息扩展处理是使用 16 个字的数据生成 1 个字的扩展消息的运算处理。按原样使用最初输入的消息作为第 1 到第 16 个扩展消息。对于第 17 及随后的扩展消息，使用 16 个字的第 (n-16) 到第 (n-1) 个扩展消息生成 1 个字的第 n 个扩展消息。重复该生成，直到生成第 N 个扩展消息为止。假定 N 为在算法中规定的预定步骤数量。

[0471] 各分步处理是使用包括 W 个字 (W 是由哈希算法规定的整数) 的预定内部状态值和 1 个字的扩展消息来生成下一个内部状态值的运算处理。使用哈希初始值和第一扩展消息来生成第一内部状态值。使用第 (n-1) 个内部状态值和第 n 个扩展消息来生成第 n 个内部状态值。重复该生成，直到生成第 N 个内部状态值为止。

[0472] 加法处理是将从第一个块到紧接的前一个块的哈希中间值和关注的块的第 N 个

内部状态值相加的运算处理。通过将哈希初始值和第一个块的第 N 个内部状态值相加来生成第一个块的哈希中间值。输出针对最后一个块获得哈希中间值，作为针对整个消息的哈希值。

[0473] 针对各个哈希算法，规定了定义 1 个字的位数：针对 MD5 为 32 位，针对 SHA-1 为 32 位，针对 SHA512 为 64 位。

[0474] 针对各个哈希算法，规定了内部状态值和哈希值的字的数量：针对 MD5 为 4 个字 (128 位)，针对 SHA-1 为 5 个字 (160 位)，针对 SHA512 为 8 个字 (256 位)。

[0475] 针对各个哈希算法，规定了预定步骤数量 N：针对 MD5 为 N ＝ 64，针对 SHA-1 为 N ＝ 80，针对 SHA512 为 N ＝ 80。

[0476] (哈希值计算电路)

[0477] 图 25 是示出根据本实施例的哈希值计算电路配置的框图。附图标记 100 表示哈希值计算电路。

[0478] 附图标记 101 表示控制处理 A 和 B 的哈希值计算的哈希值计算控制器，其包括用于控制哈希值计算的寄存器。在哈希值计算电路 100 的外部配置的 CPU 能够经由系统总线 102 访问寄存器。

[0479] 哈希值计算控制器 101 生成以下信号：

[0480] • 指示正在进行处理 A 的信号 A_EXE；

[0481] • 指示处理 A 正在执行的哈希算法的信号 A_ALG；

[0482] • 指示处理 A 正在执行的步骤的数量的信号 A_STP_CNT；

[0483] • 指示处理 A 正在执行的块的数量的信号 A_BLK_CNT；以及

[0484] • 指示在处理 A 中使用的哈希初始值的信号 A_IV。

[0485] 在信号 A_EXE 为“1”时，信号 A_EXE 指示正在进行处理 A，信号 A_ALG 指示 MD5、SHA-1 和 SHA512 的一个。在 A_EXE ＝“1”时，信号 A_STP_CNT 重置为 0，并在响应于输入消息的输入传输请求接收到第一确认时，开始计数。信号 A_STP_CNT 针对各时钟周期从 0 向上计数到 N+1，接着返回到 0。在信号 A_STP_CNT 为 0 到 N-1 时，消息扩展处理执行第 1 到第 N 个处理，并且在信号 A_STP_CNT 为 0 到 N 时，分步处理执行第 1 到第 N 个处理。在信号 A_STP_CNT 为 2 到 N+1 时，加法处理执行第 1 到第 N 个处理。在 A_EXE ＝“1”时，信号 A_BLK_CNT 重置为 0，并在信号 A_STP_CNT 达到 N+1 时向上计数 +1。信号 A_BLK_CNT 向上计数，直到输入消息的块的数量 -1 为止，接着返回到 0。

[0486] 哈希值计算控制器 101 生成信号 A_DMA_REQ 作为到 DMA 控制器 (以下称作 DMAC)A 的数据传输请求，DMAC A 配置在哈希值计算电路 100 的外部，并传输处理 A 使用的输入 / 输出数据。接着，哈希值计算控制器 101 从 DMAC A 接收确认信号 A_DMA_ACK。信号 A_DMA_REQ 和信号 A_DMA_ACK 分别是 2 位的信号。假定信号 A_DMA_REQ[0]/A_DMA_ACK[0] 是用于输入作为要处理的数据的输入消息的输入传输信号，并且信号 A_DMA_REQ[1]/A_DMA_ACK[1] 是用于输出作为哈希值计算结果而获得的哈希值的输出传输信号。

[0487] 此外，哈希值计算控制器 101 生成以下的信号：

[0488] • 指示正在进行处理 B 的信号 B_EXE；

[0489] • 指示处理 B 正在执行的哈希算法的信号 B_ALG；

[0490] • 指示处理 B 正在执行的步骤的数量的信号 B_STP_CNT；

[0491] • 指示处理 B 正在执行的块的数量的信号 B_BLK_CNT ;以及

[0492] • 指示在处理 B 中使用的哈希初始值的信号 B_IV。

[0493] 在信号 B_EXE 为“1”时,信号 B_EXE 指示正在进行处理 B,信号 B_ALG 指示 MD5、SHA-1 和 SHA512 的一个。在 B_EXE =“1”时,信号 B_STP_CNT 重置为 0,并在响应于输入消息的输入传输请求接收到第一确认时,开始计数。信号 B_STP_CNT 针对各时钟周期从 0 向上计数到 N+1,接着返回到 0。在信号 B_STP_CNT 为 0 到 N-1 时,消息扩展处理执行第 1 到第 N 个处理,在信号 B_STP_CNT 为 0 到 N 时,分步处理执行第 1 到第 N 个处理。在信号 B_STP_CNT 为 2 到 N+1 时,加法处理执行第 1 到第 N 个处理。在 B_EXE =“1”时,信号 B_BLK_CNT 重置为 0,并在信号 B_STP_CNT 达到 N+1 时向上计数 +1。信号 B_BLK_CNT 向上计数,直到输入消息的块的数量 -1 为止,接着返回到 0。

[0494] 哈希值计算控制器 101 生成信号 B_DMA_REQ 作为到 DMAC B 的数据传输请求,DMAC B 配置在哈希值计算电路 100 的外部,并传输处理 B 使用的输入 / 输出数据。接着,哈希值计算控制器 101 从 DMAC B 接收确认信号 B_DMA_ACK。信号 B_DMA_REQ 和信号 B_DMA_ACK 分别是 2 位的信号。假定信号 B_DMA_REQ[0]/B_DMA_ACK[0] 是用于输入作为要处理的数据的输入消息的输入传输信号,并且信号 B_DMA_REQ[1]/B_DMA_ACK[1] 是用于输出作为哈希值计算结果而获得的哈希值的输出传输信号。

[0495] 附图标记 103 表示作为与配置在哈希值计算电路 100 的外部的 DMAC 的接口的 DMA IF 单元。附图标记 104 表示与传输处理 A 的输入 / 输出数据的 DMAC A 的接口信号。输入数据总线 A_DMA_IDATA 具有 64 位的宽度,以 64 位为单位来传输作为要处理的数据的输入消息,并且输出 64 位的输入消息 A_MSG。输出数据总线 A_DMA_ODATA 具有 64 位的宽度,并且以 64 位为单位来传输作为哈希值计算结果而获得的哈希值。附图标记 105 表示与传输处理 B 的输入 / 输出数据的 DMAC B 的接口信号。输入数据总线 B_DMA_IDATA 具有 64 位的宽度,以 64 位为单位来传输作为要处理的数据的输入消息,并输出 64 位的输入消息 B_MSG。输出数据总线 B_DMA_ODATA 具有 64 位的宽度,并且以 64 位为单位来传输作为哈希值计算结果而获得的哈希值。

[0496] (接口信号)

[0497] 图 34A 和图 34B 是示出基于接口信号 104 和 105 的操作的示例的时序图。

[0498] T100 到 T105 指示信号 104 的输入传输,T107 到 T110 指示信号 104 的输出传输。在输入传输中,在 T100 中,DMAIF 单元 103 将输入传输请求信号 A_DMA_REQ[0] 断言到 DMAC A。

[0499] 在 T101 中,DMAC A 将第一输入数据 DI0 传输到 DMA IF 单元 103,并断言确认信号 A_DMA_ACK[0]。响应于 T102 中的时钟前沿,同时断言信号 A_DMA_REQ[0] 和信号 A_DMA_ACK[0],以完成数据 DI0 的输入传输,并且 DMAC A 传输第二输入数据 DI1。在输出传输中,在 T107 中,DMA IF 单元 103 将第一输出数据 DO0 输出到 DMAC A,同时断言输出传输请求信号 A_DMA_REQ[1]。在 T108 中,DMAC A 将确认信号 A_DMA_ACK[1] 断言到 DMA IF 单元 103,并接收输出数据。

[0500] 响应于 T109 中的时钟前沿,断言信号 A_DMA_REQ[1] 和信号 A_DMA_ACK[1],以完成数据 DO0 的输出传输,并且 DMA IF 单元 103 传输第二输出数据 DO1。在本实施例中,确定与处理 A 的一个传输请求对应的数据量,并且一旦 DMAC A 断言确认信号,则 DMAC A 连续传输

确定的数据量。假定输入传输针对一个块连续传输 1 个字的数据。在 1 个字少于 64 位的输入数据总线宽度时，通过向低位填充数据来传输该字。假定输出传输与哈希值的字的数量对应地连续传输一个字的数据。在 1 个字少于 64 位的输入数据总线宽度时，通过向低位填充数据来传输该数据。由于 MD5、SHA1 和 SHA512 要求每个时钟 16 个字，因此连续传输 16 次数据。输出传输将哈希值分割为各自具有 64 位的宽度的数据，并连续传输分割的数据。由于 MD5 的哈希值需要 128 位，因此连续传输两次数据。由于 SHA1 的哈希值需要 160 位，因此连续传输 3 次数据。由于 SHA512 的哈希值需要 512 位，因此连续传输 8 次数据。

[0501] T111 到 T116 指示信号 105 的输入传输，T118 到 T122 指示信号 105 的输出传输。在输入传输中，在 T111 中，DMAIF 单元 103 将输入传输请求信号 B_DMA_REQ[0] 断言到 DMAC B。

[0502] 在 T112 中，DMAC B 将第一输入数据 DI0 传输到 DMA IF 单元 103，并断言确认信号 B_DMA_ACK[0]。响应于 T113 中的时钟前沿，同时断言信号 B_DMA_REQ[0] 和信号 B_DMA_ACK[0]，以完成数据 DI0 的输入传输，并且 DMAC B 传输第二输入数据 DI1。在输出传输中，在 T118 中，DMA IF 单元 103 将第一输出数据 DO0 输出到 DMAC B，同时断言输出传输请求信号 B_DMA_REQ[1]。在 T119 中，DMAC B 将确认信号 B_DMA_ACK[1] 断言到 DMAIF 单元 103，并接收输出数据。

[0503] 响应于 T120 中的时钟前沿，断言信号 B_DMA_REQ[1] 和信号 B_DMA_ACK[1]，以完成数据 DO0 的输出传输，并且 DMA IF 单元 103 传输第二输出数据 DO1。在本实施例中，预先确定与处理 B 的一个传输请求对应的数据量，并且一旦 DMAC B 断言确认信号，则 DMAC B 连续传输所确定的数据量。假定输入传输针对一个块连续传输 1 个字的数据。在 1 个字少于 64 位的输入数据总线宽度时，通过向低位填充数据来传输该字。由于 MD5、SHA1 和 SHA512 要求每个时钟 16 个字，因此连续传输 16 次数据。假定输出传输将哈希值分割为各自具有 64 位的宽度的数据，并连续传输分割的数据。由于 MD5 的哈希值需要 128 位，因此连续传输两次数据。由于 SHA1 的哈希值需要 160 位，因此连续传输 3 次数据。由于 SHA512 的哈希值需要 512 位，因此连续传输 8 次数据。

[0504] 附图标记 106 表示扩展消息选择器。扩展消息选择器 106 根据信号 A_EXE、A_ALG、A_STP_CNT、B_EXE、B_ALG 以及 B_STP_CNT，来选择从外部输入的消息 A_MSG 和 B_MSG 以及扩展消息 ExMSG_N。接着，扩展消息选择器 106 输出 32 位的数据 ExMSG_0 和 ExMSG_1。在扩展消息存储单元 107（稍后描述）的区域 0 中存储数据 ExMSG_0，并在扩展消息存储单元 107 的区域 1 中存储数据 ExMSG_1。

[0505] （数据 ExMSG_0 和 ExMSG_1 的选择）

[0506] 图 35 是示出数据 ExMSG_0 和 ExMSG_1 的选择策略的示例的图。附图标记 1001 表示数据 ExMSG_0 的数据选择策略。

[0507] • 附图标记 1001-a 表示正在进行处理 A 的 MD5 哈希值计算，并且要执行第 1 至第 16 个消息扩展处理 (A_EXE = 1、A_ALG = MD5 且 A_STP_CNT = 0 到 15) 的情况。在这种情况下，选择来自 DMAC_A 的传输数据的低 32 位 A_MSG[31 :0]。

[0508] •附图标记 1001-b 表示正在进行处理 A 的 SHA512 哈希值计算，并且要执行第 1 至第 16 个消息扩展处理 (A_EXE = 1、A_ALG = SHA512 且 A_STP_CNT = 0 到 15) 的情况。在这种情况下，选择来自 DMAC A 的传输数据的低 32 位 A_MSG[31 :0]。

[0509] • 附图标记 1001-c 表示正在进行处理 B 的 MD5 哈希值计算，并且要执行第 1 至第 16 个消息扩展处理 (B_EXE = 1、B_ALG = MD5 且 B_STP_CNT = 0 到 15) 的情况。在这种情况下，选择来自 DMAC B 的传输数据的低 32 位 B_MSG[31 :0]。

[0510] •附图标记 1001-d 表示正在进行处理 B 的 SHA512 哈希值计算，并且要执行第 1 至第 16 个消息扩展处理 (B_EXE = 1、B_ALG = SHA512 且 B_STP_CNT = 0 到 15) 的情况。在这种情况下，选择来自 DMAC B 的传输数据的低 32 位 B_MSG[31 :0]。

[0511] • 附图标记 1001-e 表示上述情况以外的情况。在这种情况下，选择稍后描述的扩展消息的低 32 位 ExMSG_N[31 :0]。

[0512] 附图标记 1002 表示数据 ExMSG_1 的数据选择策略。

[0513] • 附图标记 1002-a 表示正在进行处理 A 的 MD5 哈希值计算，并且要执行第 1 至第 16 个消息扩展处理 (A_EXE = 1、A_ALG = MD5 且 A_STP_CNT = 0 到 15) 的情况。在这种情况下，选择来自 DMAC A 的传输数据的低 32 位 A_MSG[31 :0]。

[0514] •附图标记 1002-b 表示正在进行处理 A 的 SHA512 哈希值计算，并且要执行第 1 至第 16 个消息扩展处理 (A_EXE = 1、A_ALG = SHA512 且 A_STP_CNT = 0 到 15) 的情况。在这种情况下，选择来自 DMAC A 的传输数据的高 32 位 A_MSG[63 :32]。

[0515] • 附图标记 1002-c 表示正在进行处理 B 的 MD5 哈希值计算，并且要执行第 1 至第 16 个消息扩展处理 (B_EXE = 1、B_ALG = MD5 且 B_STP_CNT = 0 到 15) 的情况。在这种情况下，选择来自 DMAC B 的传输数据的低 32 位 B_MSG[31 :0]。

[0516] •附图标记 1002-d 表示正在进行处理 B 的 SHA512 哈希值计算，并且要执行第 1 至第 16 个消息扩展处理 (B_EXE = 1、B_ALG = SHA512 且 B_STP_CNT = 0 到 15) 的情况。在这种情况下，选择来自 DMAC B 的传输数据的高 32 位 B_MSG[63 :32]。

[0517] • 附图标记 1002-e 表示上述情况以外的情况。在这种情况下，选择稍后描述的扩展消息的高 32 位 ExMSG_N[63 :32]。

[0518] 根据图 35 所示的选择策略，在正在进行处理 A 或 B 的哈希值计算时，选择在处理中使用的数据；在未正在进行哈希值计算时，输出扩展消息 ExMSG_N，并将其存储在扩展消息存储单元 107 中。

[0519] 附图标记 107 表示存储来自扩展消息选择器 106 的输出数据的扩展消息存储单元 107。扩展消息存储单元 107 包括 1024 位的触发器，其中第 0 到第 511 位形成区域 0，第 512 位到第 1023 位形成区域 1。将来自 1024 位的触发器的输出信号设为 ExMSG[1023 :0]。

[0520] （扩展消息存储单元）

[0521] 图 36 是示出扩展消息存储单元 107 的内部配置的示例的图。附图标记 1101 表示区域 0 的触发器。触发器 1101 针对各时钟将所存储的数据向 LSB 移位 32 位，并在最高的 32 位 ExMSG[511 :480] 中存储 32 位的数据 ExMSG_0。附图标记 1102 表示区域 1 的触发器。触发器 1102 针对各时钟将所存储的数据向 LSB 移位 32 位，并在最高的 32 位 ExMSG[1023 :992] 中存储 32 位的数据 ExMSG_1。

[0522] 附图标记 108-1、108-2 和 108-3 表示执行对应的哈希函数的消息扩展处理的消息扩展处理器。由于消息扩展处理对应于哈希算法而不同，因此配置与各个哈希算法对应的消息扩展处理器。消息扩展处理器 108-1 对应于 MD5。消息扩展处理器 108-2 对应于 SHA1。消息扩展处理器 108-3 对应于 SHA512。预先确定存储消息扩展处理器 108-1、108-2

和 108-3 要处理的数据的扩展消息存储单元 107 的区域。

[0523] MD5 消息扩展处理器 108-1 使用区域 0 作为要处理的数据的存储区域。消息扩展处理器 108-1 输入区域 0 的数据 ExMSG[511 :0]，并输出一个字 (32 位) 的扩展消息 MD5_ExMSG[31 :0]。

[0524] SHA1 消息扩展处理器 108-2 使用区域 1 作为要处理的数据的存储区域。消息扩展处理器 108-2 输入区域 1 的数据 ExMSG[1023 :512]，并输出一个字 (32 位) 的扩展消息 SHA1_ExMSG[31 :0]。

[0525] SHA512 消息扩展处理器 108-3 使用区域 0 和 1 作为要处理的数据的存储区域。将 SHA512 的一个字定义为 64 位，在区域 0 中存储一个字的低 32 位数据，在区域 1 中存储一个字的高 32 位数据。消息扩展处理器 108-3 输入区域 0 和 1 的数据 ExMSG[1023 :0]，并输出一个字 (64 位) 的扩展消息 SHA512_ExMSG[63 :0]。

[0526] 预先确定存储消息扩展处理器 108-1、108-2 和 108-3 要处理的数据的扩展消息存储单元 107 的区域，并连接扩展消息存储单元 107 作为到消息扩展处理器 108-1、108-2 和 108-3 的输入。由于该原因，消息扩展处理器 108-1、108-2 和 108-3 始终以扩展消息存储单元 107 的确定区域中的数据作为输入，来执行消息扩展处理。

[0527] 附图标记 109 表示消息扩展处理结果选择器。消息扩展处理结果选择器 109 根据信号 A_EXE、A_ALG、B_EXE 和 B_ALG 选择 :

[0528] • 来自 MD5 消息扩展处理器 108-1 的输出数据 MD5_ExMSG ;

[0529] • 来自 SHA1 消息扩展处理器 108-2 的输出数据 SHA1_ExMSG ;或

[0530] •来自 SHA512 消息扩展处理器 108-3 的输出数据 SHA512_ExMSG，并输出所选择的数据作为 64 位数据的扩展消息 ExMSG_N。注意，ExMSG_N[31 :0] 是存储在扩展消息存储单元 107 的区域 0 中的扩展消息，ExMSG_N[63 :32] 是存储在扩展消息存储单元 107 的区域 1 中的扩展消息。

[0531] (数据 ExMSG_N[31 :0] 和 ExMSG_N[63 :32] 的选择)

[0532] 图 37 是示出数据 ExMSG_N[31 :0] 和 ExMSG_N[63 :32] 的选择策略的示例的图。附图标记 1201 表示数据 ExMSG_N[31 :0] 的数据选择策略。

[0533] • 附图标记 1201-a 表示正在进行处理 A 的 MD5 哈希值计算 (A_EXE = 1 且 A_ALG = MD5) 的情况。在这种情况下，选择消息扩展处理器 108-1 的输出数据 MD5_ExMSG[31 :0]。

[0534] • 附图标记 1201-b 表示正在进行处理 B 的 MD5 哈希值计算 (B_EXE = 1 且 B_ALG = MD5) 的情况。在这种情况下，选择消息扩展处理器 108-1 的输出数据 MD5_ExMSG[31 :0]。

[0535] •附图标记 1201-c 表示上述情况以外的情况。在这种情况下，选择 SHA512 消息扩展处理器 108-3 的输出数据 SHA512_ExMSG 的低 32 位 SHA512_ExMSG[31 :0]。

[0536] 附图标记 1202 表示数据 ExMSG_N[63 :32] 的数据选择策略。

[0537] •附图标记 1202-a 表示正在进行处理 A 的 SHA1 哈希值计算 (A_EXE = 1 且 A_ALG = SHA1) 的情况。在这种情况下，选择消息扩展处理器 108-2 的输出数据 SHA1_ExMSG[31 :0]。

[0538] •附图标记 1202-b 表示正在进行处理 B 的 SHA1 哈希值计算 (B_EXE = 1 且 B_ALG = SHA1) 的情况。在这种情况下，选择消息扩展处理器 108-2 的输出数据 SHA1_ExMSG[31 :0]。

[0539] •附图标记 1202-c 表示上述情况以外的情况。在这种情况下，选择 SHA512 消息扩展处理器 108-3 的输出数据 SHA512_ExMSG 的高 32 位 SHA512_ExMSG[63 :32]。

[0540] 根据图 37 所示的选择策略，在正在进行处理 A 或 B 的哈希值计算时，选择在处理中使用的来自消息扩展处理器 108-1 或 108-2 的输出 ；在未正在进行哈希值计算时，输出 SHA512 消息扩展处理器 108-3 的输出数据 SHA512_ExMSG，并将其存储在扩展消息存储单元 107 中。

[0541] 附图标记 110 表示内部状态值存储数据选择器。内部状态值存储数据选择器 110 根据信号 A_EXE、A_ALG、A_STP_CNT、A_BLK_CNT、B_EXE、B_ALG、B_STP_CNT 以及 B_BLK_CNT 选择 ：

[0542] • 哈希初始值 A_IV 和 B_IV ；

[0543] • 分步处理结果 TEMP_N ；或

[0544] • 哈希中间值存储数据 IHASH，

[0545] 并输出 256 位的数据 TEMP_0 和 TEMP_1。

[0546] 数据 TEMP_0 存储在内部状态值存储单元 111（稍后描述）的区域 0 中，数据 TEMP_1 存储在内部状态值存储单元 111 的区域 1 中。

[0547] （数据 TEMP_0 和 TEMP_1 的选择）

[0548] 图 38 是示出数据 TEMP_0 和 TEMP_1 的数据选择策略的示例的图。附图标记 1301 表示数据 TEMP_0 的数据选择策略。

[0549] • 附图标记 1301-a 表示正在进行处理 A 的 MD5 哈希值计算、直到第一个块中的第一分步处理 (A_EXE = 1、A_ALG = MD5、A_BLK_CNT = 0 且 A_STP_CNT = 0) 的情况。在这种情况下，选择处理 A 哈希初始值的低 256 位 A_IV[255 :0]。

[0550] •附图标记 1301-b 表示正在进行处理 A 的 SHA512 哈希值计算、直到第一个块中的第一分步处理 (A_EXE = 1、A_ALG = SHA512、A_BLK_CNT = 0 且 A_STP_CNT = 0) 的情况。在这种情况下，选择处理 A 哈希初始值的低 256 位 A_IV[255 :0]。

[0551] • 附图标记 1301-c 表示正在进行处理 A 的 MD5 哈希值计算、直到从第一个块开始的块中的第一分步处理 (A_EXE = 1、A_ALG = MD5、A_BLK_CNT ≠ 0 且 A_STP_CNT = 0) 的情况。在这种情况下，选择通过紧接的前一个块的处理而获得的哈希中间值存储数据的低 256 位 IHASH[255 :0]。

[0552] •附图标记 1301-d 表示正在进行处理 A 的 SHA512 哈希值计算、直到从第一个块开始的块中的第一分步处理 (A_EXE = 1、A_ALG = SHA512、A_BLK_CNT ≠ 0 且 A_STP_CNT = 0) 的情况。在这种情况下，选择通过紧接的前一个块的处理而获得的哈希中间值数据的低 256 位 IHASH[255 :0]。

[0553] • 附图标记 1301-e 表示正在进行处理 B 的 MD5 哈希值计算、直到第一个块中的第一分步处理 (B_EXE = 1、B_ALG = MD5、B_BLK_CNT = 0 且 B_STP_CNT = 0) 的情况。在这种情况下，选择处理 B 哈希初始值的低 256 位 B_IV[255 :0]。

[0554] •附图标记 1301-f 表示正在进行处理 B 的 SHA512 哈希值计算、直到第一个块中的第一分步处理 (B_EXE = 1、B_ALG = SHA512、B_BLK_CNT = 0 且 B_STP_CNT = 0) 的情况。在这种情况下，选择处理 B 哈希初始值的低 256 位 B_IV[255 :0]。

[0555] • 附图标记 1301-g 表示正在进行处理 B 的 MD5 哈希值计算、直到从第一个块开始

的块中的第一分步处理 (B_EXE = 1、B_ALG = MD5、B_BLK_CNT ≠ 0 且 B_STP_CNT = 0) 的情况。在这种情况下,选择通过紧接的前一个块的处理而获得的哈希中间值数据的低 256 位 IHASH[255 :0]。

[0556] •附图标记 1301-h 表示正在进行处理 B 的 SHA512 哈希值计算、直到从第一个块开始的块中的第一分步处理 (B_EXE = 1、B_ALG = SHA512、B_BLK_CNT ≠ 0 且 B_STP_CNT = 0) 的情况。在这种情况下,选择通过紧接的前一个块的处理而获得的哈希中间值数据的低 256 位 IHASH[255 :0]。

[0557] • 附图标记 1301-i 表示上述情况以外的情况。在这种情况下,选择稍后描述的内部状态值数据的低 256 位 TEMP_N[255 :0]。

[0558] 附图标记 1302 表示数据 TEMP_1 的数据选择策略。

[0559] • 附图标记 1302-a 表示正在进行处理 A 的 MD5 哈希值计算、直到第一个块中的第一分步处理 (A_EXE = 1、A_ALG = MD5、A_BLK_CNT = 0 且 A_STP_CNT = 0) 的情况。在这种情况下,选择处理 A 哈希初始值的低 256 位 A_IV[255 :0]。

[0560] •附图标记 1302-b 表示正在进行处理 A 的 SHA512 哈希值计算、直到第一个块中的第一分步处理 (A_EXE = 1、A_ALG = SHA512、A_BLK_CNT = 0 且 A_STP_CNT = 0) 的情况。在这种情况下,选择处理 A 哈希初始值的高 256 位 A_IV[511 :256]。

[0561] • 附图标记 1302-c 表示正在进行处理 A 的 MD5 哈希值计算、直到从第一个块开始的块中的第一分步处理 (A_EXE = 1、A_ALG = MD5、A_BLK_CNT ≠ 0 且 A_STP_CNT = 0) 的情况。在这种情况下,选择通过紧接的前一个块的处理而获得的哈希中间值数据的高 256 位 IHASH[511 :256]。

[0562] •附图标记 1302-d 表示正在进行处理 A 的 SHA512 哈希值计算、直到从第一个块开始的块中的第一分步处理 (A_EXE = 1、A_ALG = SHA512、A_BLK_CNT ≠ 0 且 A_STP_CNT = 0) 的情况。在这种情况下,选择通过紧接的前一个块的处理而获得的哈希中间值数据的高 256 位 IHASH[511 :256]。

[0563] • 附图标记 1302-e 表示正在进行处理 B 的 MD5 哈希值计算、直到第一个块中的第一分步处理 (B_EXE = 1、B_ALG = MD5、B_BLK_CNT = 0 且 B_STP_CNT = 0) 的情况。在这种情况下,选择处理 B 哈希初始值的低 256 位 B_IV[255 :0]。

[0564] •附图标记 1302-f 表示正在进行处理 B 的 SHA512 哈希值计算、直到第一个块中的第一分步处理为止的情况 (B_EXE = 1、B_ALG = SHA512、B_BLK_CNT = 0 且 B_STP_CNT = 0)。在这种情况下,选择处理 B 哈希初始值的高 256 位 B_IV[511 :256]。

[0565] • 附图标记 1302-g 表示正在进行处理 B 的 MD5 哈希值计算、直到从第一个块开始的块中的第一分步处理 (B_EXE = 1、B_ALG = MD5、B_BLK_CNT ≠ 0 且 B_STP_CNT = 0) 的情况。在这种情况下,选择通过紧接的前一个块的处理而获得的哈希中间值数据的高 256 位 IHASH[511 :256]。

[0566] •附图标记 1302-h 表示正在进行处理 B 的 SHA512 哈希值计算、直到从第一个块开始的块中的第一分步处理 (B_EXE = 1、B_ALG = SHA512、B_BLK_CNT ≠ 0 且 B_STP_CNT = 0) 的情况。在这种情况下,选择通过紧接的前一个块的处理而获得的哈希中间值数据的高 256 位 IHASH[511 :256]。

[0567] • 附图标记 1302-i 表示上述情况以外的情况。在这种情况下,选择稍后描述的内

部状态值数据的高 256 位 TEMP_N[511 :256]。

[0568] 根据图 38 所示的选择策略，在正在进行处理 A 或 B 的哈希值计算时，选择在处理中使用的数据；在未正在进行哈希值计算时，输出内部状态值 TEMP_N，并将其存储在内部状态值存储单元 111 中。

[0569] 附图标记 111 表示存储来自内部状态值存储数据选择器 109 的输出数据的内部状态值存储单元。内部状态值存储单元 111 包括 512 位的触发器，第 0 位到第 255 位形成区域 0，第 256 位到第 511 位形成区域 1。将来自 512 位的触发器的输出信号设为 TEMP[511 :0]。区域 0 存储数据 TEMP_0，区域 1 存储数据 TEMP_1。

[0570] 附图标记 112-1、112-2 和 112-3 表示执行分步处理的分步处理器。由于分步处理对应于哈希算法而不同，因此配置与各个哈希算法对应的分步处理器。分步处理器 112-1 对应于 MD5。分步处理器 112-2 对应于 SHA-1。分步处理器 112-3 对应于 SHA512。预先确定存储分步处理器 112-1、112-2 和 112-3 要处理的数据的内部状态值存储单元 111 的区域。

[0571] MD5 分步处理器 112-1 使用区域 0 作为要处理的数据的存储区域。分步处理器 112-1 输入区域 0 的数据 TEMP[127 :0] 和来自扩展消息存储单元 107 的输出数据 ExMSG[511 :480]，并输出 128 位的内部状态值 MD5_TEMP[127 :0]。

[0572] SHA1 分步处理器 112-2 使用区域 1 作为要处理的数据的存储区域。分步处理器 112-2 输入区域 1 的数据 TEMP[255 :128] 和来自扩展消息存储单元 107 的输出数据 ExMSG[1023 :992]，并输出 160 位的内部状态值 SHA1_TEMP[159 :0]。

[0573] SHA512 分步处理器 112-3 使用区域 0 和 1 作为要处理的数据的存储区域。分步处理器 112-3 输入区域 0 和 1 的数据 TEMP[511 :0] 以及来自扩展消息存储单元 107 的输出数据 ExMSG[511 :480] 和 ExMSG[1023 :992]，并输出 512 位的内部状态值 SHA512_TEMP[511 :0]。

[0574] 预先确定分别存储分步处理器 112-1、112-2 和 112-3 要处理的数据的内部状态值存储单元 111 的区域，并连接内部状态值存储单元 111 作为分步处理器的输入。由于该原因，分步处理器 112-1、112-2 和 112-3 始终以内部状态值存储单元 111 的确定区域中的数据作为输入，来执行分步处理。

[0575] 附图标记 113 表示分步处理结果选择器。

[0576] 分步处理结果选择器 113 根据信号 A_EXE、A_ALG、B_EXE 和 B_ALG 选择：

[0577] • 来自 MD5 分步处理器 112-1 的输出数据 MD5_TEMP；

[0578] • 来自 SHA1 分步处理器 112-2 的输出数据 SHA1_TEMP；或

[0579] • 来自 SHA512 分步处理器 112-3 的输出数据 SHA512_TEMP，并输出所选择的数据作为数据 TEMP_N。数据 TEMP_N[255 :0] 是存储在内部状态值存储单元 111 的区域 0 中的内部状态值数据，数据 TEMP_N[511 :256] 是存储在内部状态值存储单元 111 的区域 1 中的内部状态值数据。

[0580] （数据 TEMP_N[255 :0] 和 TEMP_N[511 :256] 的选择）

[0581] 图 39 是示出数据 TEMP_N[255 :0] 和 TEMP_N[511 :256] 的选择策略的示例的图。

[0582] 附图标记 1401 表示数据 TEMP_N[255 :0] 的数据选择策略。

[0583] • 附图标记 1401-a 表示正在进行处理 A 的 MD5 哈希值计算 (A_EXE ＝ 1 且 A_ALG

= MD5) 的情况。在这种情况下，选择 MD5 分步处理器 112-1 的输出数据 MD5_TEMP[127 :0] 作为低 128 位。

[0584] • 附图标记 1401-b 表示正在进行处理 B 的 MD5 哈希值计算 (B_EXE = 1 且 B_ALG = MD5) 的情况。在这种情况下，选择 MD5 分步处理器 112-1 的输出数据 MD5_TEMP[127 :0] 作为低 128 位。

[0585] •附图标记 1401-c 表示上述情况以外的情况。在这种情况下，选择 SHA512 分步处理器 112-3 的输出数据 SHA512_TEMP[127 :0]。始终输出数据 SHA512_TEMP[255 :128]，作为数据 TEMP_N[255 :128]。

[0586] 附图标记 1402 表示数据 TEMP_N[511 :256] 的数据选择策略。

[0587] •附图标记 1402-a 表示正在进行处理 A 的 SHA1 哈希值计算 (A_EXE = 1 且 A_ALG = SHA1) 的情况。在这种情况下，选择 SHA1 分步处理器 112-2 的输出数据 SHA1_TEMP[159 :0] 作为低 160 位。

[0588] •附图标记 1402-b 表示正在进行处理 B 的 SHA1 哈希值计算 (B_EXE = 1 且 B_ALG = SHA1) 的情况。在这种情况下，选择 SHA1 分步处理器 112-2 的输出数据 SHA1_TEMP[159 :0] 作为低 160 位。

[0589] •附图标记 1401-c 表示上述情况以外的情况。在这种情况下，选择 SHA512 分步处理器 112-3 的输出数据 SHA512_TEMP[511 :256]。

[0590] 始终输出数据 SHA512_TEMP[511 :256]，作为数据 TEMP_N[511 :256]。

[0591] 根据图 39 所示的选择策略，在正在进行处理 A 或 B 的哈希值计算时，选择在对应的处理中使用的来自分步处理器的输出 ；在未正在进行哈希值计算时，输出 SHA512 分步处理器 112-3 的输出数据 SHA512_TEMP，并将其存储在内部状态值存储单元 111 中。

[0592] 附图标记 114 表示哈希中间值存储数据选择器。哈希中间值存储数据选择器 114 根据信号 A_EXE、A_ALG、A_BLK_CNT、A_STP_CNT、B_STP_CNT、B_ALG 以及 B_BLK_CNT 选择哈希初始值 A_IV 和 B_IV 以及哈希中间值结果 IHASH_N。接着，哈希中间值存储数据选择器 114 输出 256 位的数据 IHASH_0 和 IHASH_1。

[0593] 数据 IHASH_0 存储在哈希中间值存储单元 115(稍后描述) 的区域 0 中，数据 IHASH_1 存储在哈希中间值存储单元 115 的区域 1 中。

[0594] (数据 IHASH_0 和 IHASH_1 的选择)

[0595] 图 40 是示出数据 IHASH_0 和 IHASH_1 的数据选择策略的示例的图。

[0596] 附图标记 1501 表示数据 IHASH_0 的数据选择策略。

[0597] • 附图标记 1501-a 表示正在进行处理 A 的 MD5 哈希值计算，并且要执行第一个块中的第 N 个加法处理以外的加法处理 (A_EXE = 1、A_ALG = MD5、A_BLK_CNT = 0 且 A_STP_CNT ≠ 65) 的情况。在这种情况下，选择处理 A 哈希初始值的低 256 位 A_IV[255 :0]。

[0598] •附图标记 1501-b 表示正在进行处理 A 的 SHA512 哈希值计算，并且要执行第一个块中的第 N 个加法处理以外的加法处理 (A_EXE = 1、A_ALG = SHA512、A_BLK_CNT = 0 且 A_STP_CNT ≠ 81) 的情况。在这种情况下，选择处理 A 哈希初始值的低 256 位 A_IV[255 :0]。

[0599] • 附图标记 1501-c 表示正在进行处理 B 的 MD5 哈希值计算，并且要执行第一个块中的第 N 个加法处理以外的加法处理 (B_EXE = 1、B_ALG = MD5、B_BLK_CNT = 0 且 B_STP_CNT ≠ 65) 的情况。在这种情况下，选择处理 B 哈希初始值的低 256 位 B_IV[255 :0]。

[0600] •附图标记 1501-d 表示正在进行处理 B 的 SHA512 哈希值计算，并且要执行第一个块中的第 N 个加法处理以外的加法处理 (B_EXE = 1、B_ALG = SHA512、B_BLK_CNT = 0 且 B_STP_CNT ≠ 81) 的情况。在这种情况下，选择处理 B 哈希初始值的低 256 位 B_IV[255 :0]。

[0601] • 附图标记 1501-e 表示上述情况以外的情况。在这种情况下，选择哈希中间值数据（稍后描述）的低 256 位 IHASH_N[255 :0]。

[0602] 附图标记 1502 表示数据 IHASH_1 的数据选择策略。

[0603] • 附图标记 1502-a 表示正在进行处理 A 的 MD5 哈希值计算，并且要执行第一个块中的第 N 个加法处理以外的加法处理 (A_EXE = 1、A_ALG = MD5、A_BLK_CNT = 0 且 A_STP_CNT ≠ 65) 的情况。在这种情况下，选择处理 A 哈希初始值的低 256 位 A_IV[255 :0]。

[0604] •附图标记 1502-b 表示正在进行处理 A 的 SHA512 哈希值计算，并且要执行第一个块中的第 N 个加法处理以外的加法处理 (A_EXE = 1、A_ALG = SHA512、A_BLK_CNT = 0 且 A_STP_CNT ≠ 81) 的情况。在这种情况下，选择处理 A 哈希初始值的高 256 位 A_IV[511 :256]。

[0605] • 附图标记 1502-c 表示正在进行处理 B 的 MD5 哈希值计算，并且要执行第一个块中的第 N 个加法处理以外的加法处理 (B_EXE = 1、B_ALG = MD5、B_BLK_CNT = 0 且 B_STP_CNT ≠ 65) 的情况。在这种情况下，选择处理 B 哈希初始值的低 256 位 B_IV[255 :0]。

[0606] •附图标记 1502-d 表示正在进行处理 B 的 SHA512 哈希值计算，并且要执行第一个块中的第 N 个加法处理以外的加法处理 (B_EXE = 1、B_ALG = SHA512、B_BLK_CNT = 0 且 B_STP_CNT ≠ 81) 的情况。在这种情况下，选择处理 B 哈希初始值的高 256 位 B_IV[511 :256]。

[0607] • 附图标记 1502-e 表示上述情况以外的情况。在这种情况下，选择哈希中间值数据（稍后描述）的高 256 位 IHASH_N[511 :256]。

[0608] 根据图 40 所示的选择策略，在正在进行处理 A 或 B 的哈希值计算时，选择在处理中使用的数据 ；否则，输出哈希中间值 IHASH_N。

[0609] 附图标记 115 表示存储来自哈希中间值存储数据选择器 114 的输出数据的哈希中间值存储单元。哈希中间值存储单元 115 包括 512 位的触发器，第 0 位到第 255 位形成区域 0，第 256 位到第 511 位形成区域 1。将来自 512 位的触发器的输出信号设为 IHASH[511 :0]。区域 0 存储数据 IHASH_0，区域 1 存储数据 IHASH_1。

[0610] 如上所述，加法处理将预定次数的分步处理后的内部状态值相加，以获得作为新的哈希中间值的结果。在本实施例中，针对各周期将值与各第 1 到第 N 个分步处理后的内部状态值相加。但是，哈希中间值存储单元仅存储与第 N 个分步处理后的内部状态值相加的值。

[0611] 数据 IHASH_0 的存储条件为 ：

[0612] •在正在进行处理 A 的 MD5 或 SHA512 哈希值计算并且要执行处理开始时的加法处理或第 N 个加法处理时 ；以及

[0613] •在正在进行处理 B 的 MD5 或 SHA512 哈希值计算并且要执行处理开始时的加法处理或第 N 个加法处理时。

[0614] 数据 IHASH_1 的存储条件为 ：

[0615] • 在正在进行处理 A 的 SHA1 或 SHA512 哈希值计算并且要执行处理开始时的加法

处理或第 N 个加法处理时 ;以及

[0616] • 在正在进行处理 B 的 SHA1 或 SHA512 哈希值计算并且要执行处理开始时的加法处理或第 N 个加法处理时。

[0617] 附图标记 116-1、116-2 和 116-3 表示加法处理器，各加法处理器将分步处理器 112-1、112-2 和 112-3 生成并存储在内部状态值存储单元 111 中的数据，与来自哈希中间值存储单元 115 的输出相加，以生成下一个的哈希中间值。由于加法处理器根据哈希算法而需要不同的位宽，因此配置与各个哈希算法对应的加法处理器。加法处理器 116-1 对应于 MD5。加法处理器 116-2 对应于 SHA1。加法处理器 116-3 对应于 SHA512。预先确定存储加法处理器 116-1、116-2 和 116-3 要处理的数据的哈希中间值存储单元 115 的区域和内部状态值存储单元 111 的区域。

[0618] 假定 MD5 加法处理器 116-1 包括四个 32 位的加法器，并在哈希中间值存储单元 115 的区域 0 中存储要处理的数据。加法处理器 116-1 将哈希中间值存储单元 115 的区域 0 中的数据 IHASH[127 :0] 和内部状态值存储单元 111 的输出数据 TEMP[127 :0] 相加，并输出 128 位的哈希中间值 MD5_IHASH[127 :0]。

[0619] 假定 SHA1 加法处理器 116-2 包括五个 32 位的加法器，并在哈希中间值存储单元 115 的区域 1 中存储要处理的数据。加法处理器 116-2 将哈希中间值存储单元 115 的区域 1 中的数据 IHASH[511 :256] 和内部状态值存储单元 111 的输出数据 TEMP[511 :256] 相加，并输出 160 位的哈希中间值 SHA1_IHASH[159 :0]。

[0620] 假定 SHA512 加法处理器 116-3 包括八个 64 位的加法器，并在哈希中间值存储单元 115 的区域 0 和 1 中存储要处理的数据。加法处理器 116-3 将哈希中间值存储单元 115 的区域 0 和 1 中的数据 IHASH[511 :0] 和内部状态值存储单元 111 的输出数据 TEMP[511 :0] 相加，并输出 512 位的哈希中间值 SHA512_IHASH[255 :0]。

[0621] 加法处理器 116-1、116-2 和 116-3 确定存储它们要处理的数据的内部状态值存储单元 111 的区域，并连接内部状态值存储单元 111 作为它们的输入。由于该原因，加法处理器 116-1、116-2 和 116-3 始终以内部状态值存储单元 111 的确定区域中的数据作为输入，来执行加法处理。

[0622] 附图标记 117 表示哈希中间值结果选择器。哈希中间值结果选择器 117 根据信号 A_EXE、A_ALG、B_EXE 和 B_ALG 选择 :

[0623] • MD5 加法处理器 116-1 的输出数据 MD5_IHASH ;

[0624] • SHA1 加法处理器 116-2 的输出数据 SHA1_IHASH ;或

[0625] • SHA512 加法处理器 116-3 的输出数据 SHA512_IHASH，并输出所选择的数据作为数据 IHASH_N。数据 IHASH_N[255 :0] 是存储在哈希中间值存储单元 115 的区域 0 中的哈希中间值数据，数据 IHASH_N[511 :256] 是存储在哈希中间值存储单元 115 的区域 1 中的哈希中间值数据。

[0626] (数据 IHASH_N[255 :0] 和 IHASH_N[511 :256] 的选择)

[0627] 图 41 是示出数据 IHASH_N[255 :0] 和 IHASH_N[511 :256] 的数据选择策略的示例的图。

[0628] 附图标记 1601 表示数据 IHASH_N[255 :0] 的数据选择策略。

[0629] • 附图标记 1601-a 表示正在进行处理 A 的 MD5 哈希值计算 (A_EXE ＝ 1 且 A_ALG

＝ MD5）的情况。在这种情况下，选择 MD5 加法处理器 116-1 的输出数据 MD5_IHASH[127 ：0] 作为低 128 位。

[0630] • 附图标记 1601-b 表示正在进行处理 B 的 MD5 哈希值计算 (B_EXE ＝ 1 且 B_ALG ＝ MD5）的情况。在这种情况下，选择 MD5 加法处理器 116-1 的输出数据 MD5_IHASH[127 ：0] 作为低 128 位。

[0631] •附图标记 1601-c 表示上述情况以外的情况。在这种情况下，选择 SHA512 加法处理器 116-3 的输出数据 SHA512_IHASH[255 :0]。

[0632] 始终输出数据 SHA512_IHASH[255 :128]，作为数据 IHASH_N[255 :128]。

[0633] 附图标记 1602 表示数据 IHASH_N[511 :256] 的数据选择策略。

[0634] •附图标记 1602-a 表示正在进行处理 A 的 SHA1 哈希值计算 (A_EXE ＝ 1 且 A_ALG ＝ SHA1）的情况。在这种情况下，选择 SHA1 加法处理器 116-2 的输出数据 SHA1_IHASH[159 ：0] 作为低 160 位。

[0635] •附图标记 1602-b 表示正在进行处理 B 的 SHA1 哈希值计算 (B_EXE ＝ 1 且 B_ALG ＝ SHA1）的情况。在这种情况下，选择 SHA1 加法处理器 116-2 的输出数据 SHA1_IHASH[159 ：0] 作为低 160 位。

[0636] •附图标记 1602-c 表示上述情况以外的情况。在这种情况下，选择 SHA512 加法处理器 116-3 的输出数据 SHA512_IHASH[511 :256]。始终输出数据 SHA512_IHASH[511 :416]，作为数据 IHASH_N[511 :416]。

[0637] 根据图 41 的选择策略，在正在进行处理 A 或 B 的哈希值计算时，选择在处理中使用的来自分步处理器的输出。在未正在进行哈希值计算时，输出 SHA512 加法处理器 116-3 的输出数据 SHA512_IHASH，并将其存储在哈希中间值存储单元 115 中。

[0638] （控制器的内部配置）

[0639] 图 26 是示出控制器 101 的内部配置的示例的框图。参照图 26，附图标记 201 表示控制处理 A 的处理 A 控制器。处理 A 控制器 201 包括用于设置哈希值计算所需的参数的处理 A 寄存器组 202、对正在执行的块的数量进行计数的块计数器 A 203 以及对正在执行的步骤的数量进行计数的步骤计数器 A204。

[0640] 图 27 是示出寄存器的规格的图。图 27 中的附图标记 301 到 304 表示包括在处理器 A 寄存器组 202 中的寄存器的规格。

[0641] 附图标记 301 表示用于设置处理 A 的哈希值计算的开始请求的寄存器 A_ENB。当在该寄存器中设置“1”时，寄存器发出开始哈希值计算的指令。在完成哈希值计算时，该寄存器自动清零。附图标记 302 表示用于设置哈希算法的寄存器 A_ALG。在该寄存器中，通过设置“00”来选择 MD5，通过设置“01”来选择 SHA1，并通过设置“10”来选择 SHA512。附图标记 303 表示用于设置进行哈希值计算的消息的块的数量的寄存器 A_BLK。在该寄存器中设置进行哈希值计算的消息的块的数量 -1 的值。附图标记 304 表示用于设置哈希值计算中使用的初始值的寄存器。初始值由各哈希算法规定。

[0642] 当在寄存器 A_ENB 301 中设置“1”以请求开始哈希值计算时，处理 A 控制器 201 向共享资源管理器 209（稍后描述）发出执行在寄存器 A_ALG 中设置的哈希值计算所需的以下内容的使用请求 ：

[0643] • 扩展消息存储单元的区域 ；

[0644] • 内部状态值存储单元的区域；

[0645] • 消息扩展处理器；

[0646] • 分步处理器；以及

[0647] • 加法处理器

[0648] （下文将这些处理器总称为处理引擎）。更具体而言，处理 A 控制器 201 发出扩展消息存储单元的特定区域的使用请求信号 A_ExMSG_REQ，并从共享资源管理器 209 接收使用许可信号 A_ExMSG_ACK。处理 A 控制器 201 发出内部状态值存储单元的特定区域的使用请求信号 A_TEMP_REQ，并从共享资源管理器 209 接收使用许可信号 A_TEMP_ACK。处理 A 控制器 201 发出特定哈希算法的处理引擎的使用请求信号 A_ENG_REQ，并从共享资源管理器 209 接收使用许可信号 A_ENG_ACK。

[0649] 附图标记 205 表示控制处理 B 的处理 B 控制器。与在处理 A 控制器 201 中相同，处理 B 控制器 205 包括处理 B 寄存器组 206、块计数器 B 207 以及步骤计数器 B 208。图 27 中的附图标记 305 到 308 表示包括在处理 B 寄存器组 206 中的寄存器规格。

[0650] 附图标记 305 表示用于设置处理 B 的哈希值计算的开始请求的寄存器。附图标记 306 表示用于设置哈希算法的寄存器。附图标记 307 表示用于设置进行哈希值计算的消息的块的数量的寄存器。该寄存器 307 设置进行哈希值计算的消息的块的数量 -1 的值。附图标记 308 表示用于设置在哈希值计算中使用的初始值的寄存器。寄存器的规格与包括在处理 A 寄存器组 202 中的寄存器 301 到 304 的规格相同。

[0651] 当在寄存器 B_ENB 305 中设置“1”以请求开始哈希值计算时，处理 B 控制器 205 向共享资源管理器 209 发出执行在寄存器 B_ALG 中设置的哈希值计算所需的以下内容的使用请求：

[0652] • 扩展消息存储单元的区域；

[0653] • 内部状态值存储单元的区域；以及

[0654] • 处理引擎。

[0655] 更具体而言，处理 B 控制器 205 发出扩展消息存储单元的特定区域的使用请求信号 B_ExMSG_REQ，并从共享资源管理器 209 接收使用许可信号 B_ExMSG_ACK。处理 B 控制器 205 发出内部状态值存储单元的特定区域的使用请求信号 B_TEMP_REQ，并从共享资源管理器 209 接收使用许可信号 B_TEMP_ACK。处理 B 控制器 205 发出特定哈希算法的处理引擎的使用请求信号 B_ENG_REQ，并从共享资源管理器 209 接收使用许可信号 B_ENG_ACK。

[0656] 附图标记 209 表示管理处理 A 和 B 共享的资源的共享资源管理器。处理 A 和 B 共享的资源包括：

[0657] • 扩展消息存储单元 107；

[0658] • 内部状态值存储单元 111；

[0659] • 哈希中间值存储单元 115；

[0660] • 消息扩展处理器 108-1、108-2 和 108-3；

[0661] • 分步处理器 112-1、112-2 和 112-3；以及

[0662] • 加法处理器 116-1，116-2 和 116-3。

[0663] 附图标记 210 表示管理扩展消息存储单元 107 的使用区域的扩展消息存储区域仲裁器。当处理 A 和 B 发出同一区域的使用请求时，扩展消息存储区域仲裁器 210 对这些请

求进行仲裁，并给予使用许可。

[0664] 附图标记 211 表示内部状态值存储区域仲裁器。当处理 A 和 B 发出同一区域的使用请求时，内部状态值存储区域仲裁器 211 对这些请求进行仲裁，并给予使用许可。将哈希中间值存储单元 115 分割成具有与内部状态值存储单元 111 的区域相同的区域，在给予内部状态值寄存器单元 111 的给定区域的使用许可时，同时给予哈希中间值存储单元 115 的相同区域的使用许可。

[0665] 附图标记 212 表示管理消息扩展处理器 108-1、108-2 和 108-3 的使用的处理引擎仲裁器。当处理 A 和 B 发出同一哈希算法的消息扩展处理器的使用请求时，处理引擎仲裁器 212 对这些请求进行仲裁，并给予使用许可。在给予消息扩展处理器的使用许可时，也给予同一哈希算法的分步处理器和加法处理器的使用许可。

[0666] 附图标记 213 表示指示处理 A 的执行状态的门 A_EXE。在 A_EXE ＝ 1 时，其指示“正在执行”的状态。在给予扩展消息存储单元的使用许可 A_ExMSG_ACK、内部状态值存储区域的使用许可 A_TEMP_ACK 和处理引擎的使用许可 A_ENG_ACK 时，设置 A_EXE ＝ 1（正在执行）。

[0667] 附图标记 214 表示指示处理 B 的执行状态的门 B_EXE。在 B_EXE ＝ 1 时，其指示“正在执行”的状态。在给予扩展消息存储单元的使用许可 B_ExMSG_ACK、内部状态值存储区域的使用许可 B_TEMP_ACK 和处理引擎的使用许可 B_ENG_ACK 时，设置 B_EXE ＝ 1（正在执行）。

[0668] （系统配置示例）

[0669] 图 28 是示出操作哈希值计算电路 100 的系统的配置示例的框图。

[0670] 附图标记 400 表示哈希值计算系统。附图标记 401 表示控制哈希值计算系统 400 的操作的 CPU。附图标记 402 表示存储进行哈希值计算的消息和哈希值等的存储器。附图标记 403 表示将处理 A 的输入消息从存储器 402 传输到哈希值计算电路 100，并将处理 A 的哈希值计算结果从哈希值计算电路 100 传输到存储器 402 的 DMAC A。附图标记 404 表示将处理 B 的输入消息从存储器 402 传输到哈希值计算电路 100，并将处理 B 的哈希值计算结果从哈希值计算电路 100 传输到存储器 402 的 DMAC B。附图标记 405 表示控制哈希值计算系统 400 的中断信号的中断控制器。

[0671] 附图标记 406 表示连接哈希值计算电路 100、CPU 401、存储器 402、DMAC A 403、DMAC B 404 和中断控制器 405 的总线，其包括地址信号、数据信号和控制信号等。附图标记 407 表示从 DMAC A 403 到中断控制器 405 的中断信号。在将处理 A 的哈希值计算结果从哈希值计算电路 100 传输到存储器 402 以后，DMAC A 403 生成中断信号以将传输完成通知给中断控制器 405。附图标记 408 表示从 DMAC B 404 到中断控制器 405 的中断信号。在将处理 B 的哈希值计算结果从哈希值计算电路 100 传输到存储器 402 以后，DMAC B 404 生成中断信号以将传输完成通知给中断控制器 405。中断控制器 405 使用中断信号（未示出）将哈希值计算结果的存储通知给 CPU 401。

[0672] (CPU 的操作)

[0673] 图 29A、图 29B 和图 29C 是示出本实施例的哈希值计算系统中的针对各消息接收的 CPU 的操作序列的流程图。附图标记 501 表示接收消息时的序列。在 CPU 接收消息时，在 ST001 中 CPU 决定处理 A 还是 B 对所接收的消息进行处理。CPU 401 包括指示处理 A 和

B 的处理状态的处理状态表。处理状态表指示“繁忙”或“空闲”。CPU 决定“空闲”的处理 A 或 B 作为用于处理消息的处理。假定在处理 A 和 B 都“空闲”时，处理 A 具有更高优先级。如果处理 A 和 B 都“繁忙”时，CPU 等待，直到它们中的一个变成“空闲”为止。如果 CPU 决定处理 A，则在 ST002 中 CPU 将处理状态表中的处理 A 的状态更新为“繁忙”，并启动处理 A 线程。如果 CPU 决定处理 B，则在 ST003 中 CPU 将处理状态表中的处理 B 的状态更新为“繁忙”，并启动处理 B 线程。

[0674] 附图标记 502 表示在启动线程 A 时执行的序列。在启动处理 A 线程时，在 ST004 中，CPU 在 DMAC A 的寄存器中进行用于将消息从存储器 402 传输到哈希值计算电路 100 的输入传输设置和用于将哈希值从哈希值计算电路 100 传输到存储器 402 的输出传输设置，并启动处理 A 线程。在 ST005 中，CPU 进行用于哈希值计算电路 100 的处理 A 寄存器组中的哈希值计算的设置，并发出处理开始请求。CPU 等待 DMAC A 的数据输出传输的完成 (ST006)，并结束处理 A 线程。

[0675] 附图标记 503 表示在启动线程 B 时执行的序列。在启动处理 B 线程时，在 ST009 中，CPU 在 DMAC B 的寄存器中进行用于将消息从存储器 402 传输到哈希值计算电路 100 的输入传输设置和用于将哈希值从哈希值计算电路 100 传输到存储器 402 的输出传输设置，并启动处理 B 线程。在 ST010 中，CPU 进行用于哈希值计算电路 100 的处理 B 寄存器组中的哈希值计算的设置，并发出处理开始请求。CPU 等待 DMAC B 的数据输出传输的完成 (ST011)，并结束处理 B 线程。

[0676] 附图标记 504 表示在接收处理 A 线程结束通知时的序列。在 ST014 中，CPU 将处理状态表中的处理 A 的状态更新为“空闲”。附图标记 505 表示在接收处理 B 线程结束通知时的序列。在 ST015 中，CPU 将处理状态表中的处理 B 的状态更新为“空闲”。

[0677] （哈希值计算电路的操作）

[0678] 图 30A 和图 30B 是示出本实施例的哈希值计算系统中的哈希值计算电路 100 的操作序列的流程图。

[0679] 附图标记 600 表示接收处理 A 开始请求时的序列。当 CPU 在处理 A 作业开始设置寄存器 301 中设置“1”时，接收处理 A 开始请求。在接收处理 A 开始请求时，处理 A 控制器 201 根据处理 A 哈希算法设置寄存器 302 中的值 A_ALG 发出共享资源使用请求 A_ExMSG_REQ、A_TEMP_REQ 和 A_ENG_REQ(ST101-A)。

[0680] 处理 A 控制器 201 等待共享资源管理器 209 给予许可（确认）A_ExMSG_ACK、A_TEMP_ACK 和 A_ENG_ACK(ST102-A)。在给予许可 A_ExMSG_ACK、A_TEMP_ACK 和 A_ENG_ACK 后，处理 A 控制器 201 向 DMAC A 发出数据输入传输请求 (ST103-A)。在 ST102-A 中接收到确认时，处理 A 控制器 201 开始处理，并更新步骤计数器 A_STP_CNT+1(ST105-A)。在 ST106-A 中，处理 A 控制器 201 确定在哈希算法中规定的针对一个块的数据传输是否完成。如果数据传输尚未完成，则处理返回到 ST103-A 以重新发出数据输入传输请求。如果数据传输完成，则数据输入传输完成，处理进行到 ST107-A。在 ST107-A 中，处理 A 控制器 201 更新步骤计数器 +1。

[0681] 在 ST108-A 中，处理 A 控制器 201 确定 A_STP_CNT 是否超过在哈希算法中规定的值 +1。处理 A 控制器 201 重复 ST107-A，直到超过规定值 +1。如果超过规定值 +1，则处理 A 控制器 201 将步骤计数器清零，并更新块计数器 A_BLK_CNT+1(ST109-A)。在 ST110-A 中，

处理 A 控制器 201 确定 A_BLK_CNT 是否超过在处理 A 块计数设置寄存器 303 中设置的值 A_BLK-1。处理 A 控制器 201 输入数据并执行哈希值计算，直到超过 A_BLK-1。如果 A_BLK_CNT 超过 A_BLK-1，则处理 A 控制器 201 将块计数器清零 (ST111-A)。为了输出哈希值，在 ST112-A 中，处理 A 控制器 201 向 DMAC A 发出数据输出传输请求，并在 ST113-A 中等待确认。处理 A 控制器 201 重复 ST112-A 和 ST113-A，直到针对哈希值的数据传输完成。

[0682] 如果针对哈希值的数据传输完成，则处理 A 控制器 201 将处理 A 作业开始设置寄存器 301 清零 (ST115-A)，并拒绝共享资源使用请求 A_ExMSG_REQ、A_TEMP_REQ 和 A_ENG_REQ(ST116-A)，从而结束该处理。

[0683] 附图标记 601 表示接收处理 B 开始请求时的序列。当 CPU 在处理 B 作业开始设置寄存器 305 中设置“1”时，接收处理 B 开始请求。在接收处理 B 开始请求时，处理 B 控制器 205 根据处理 B 哈希算法设置寄存器 306 中的值 B_ALG，发出共享资源使用请求 B_ExMSG_REQ、B_TEMP_REQ 和 B_ENG_REQ(ST101-B)。处理 B 控制器 205 等待共享资源管理器 209 给予许可（确认）B_ExMSG_ACK、B_TEMP_ACK 和 B_ENG_ACK(ST102-B)。在给予许可 B_ExMSG_ACK、B_TEMP_ACK 和 B_ENG_ACK 后，处理 B 控制器 205 向 DMAC B 发出数据输入传输请求 (ST103-B)。在 ST102-B 中接收到确认时，处理 B 控制器 205 开始处理，并更新步骤计数器 B_STP_CNT+1(ST105-B)。

[0684] 在 ST106-B 中，处理 B 控制器 205 确定在哈希算法中规定的针对一个块的数据传输是否完成。如果数据传输尚未完成，则处理返回到 ST103-B，以重新发出数据输入传输请求。如果数据传输完成，则数据输入传输完成，处理进行到 ST107-B。在 ST107-B 中，处理 B 控制器 205 更新步骤计数器 +1。在 ST108-B 中，处理 B 控制器 205 确定 B_STP_CNT 是否超过在哈希算法中规定的值 +1。处理 B 控制器 205 重复 ST107-B，直到超过规定值 +1。如果超过规定值 +1，则处理 B 控制器 205 将步骤计数器清零，并更新块计数器 B_BLK_CNT+1(ST109-B)。在 ST110-B 中，处理 B 控制器 205 确定 B_BLK_CNT 是否超过在处理 B 块计数设置寄存器 307 中设置的值 B_BLK-1。处理 B 控制器 205 输入数据并执行哈希值计算，直到超过 B_BLK-1。如果 B_BLK_CNT 超过 B_BLK-1，则处理 B 控制器 205 将块计数器清零 (ST111-B)。为了输出哈希值，在 ST112-B 中，处理 B 控制器 205 向 DMAC B 发出数据输出传输请求，并在 ST113-B 中等待确认。处理 B 控制器 205 重复 ST112-B 和 ST113-B，直到针对哈希值的数据传输完成。如果针对哈希值的数据传输完成，则处理 B 控制器 205 将处理 B 作业开始设置寄存器 305 清零 (ST115-B)，并拒绝共享资源使用请求 B_ExMSG_REQ、B_TEMP_REQ 和 B_ENG_REQ(ST116-B)，从而结束该处理。

[0685] （消息示例）

[0686] 图 31 是示出作为在本实施例中进行哈希值计算的三个消息的消息 A、消息 B 和消息 C 的示例的图。假定消息 A 包括使用哈希算法 MD5 执行哈希值计算的请求。消息 A 包括各自包含 16 个字 (512 位）的共计两个块。消息 B 包括使用哈希算法 SHA1 执行哈希值计算的请求。消息 B 包括包含 16 个字 (512 位）的共计一个块。消息 C 包括使用哈希算法 SHA512 执行哈希值计算的请求。消息 C 包括各自包含 16 个字 (1024 位）的共计八个块。

[0687] （处理的详细情况）

[0688] 图 32A 至图 33H 是 CPU 401 以指定的顺序接收消息 A、消息 B 和消息 C 时的时序图。

[0689] 假定在 T00 前接收了消息 A。在接收到消息 A 时，CPU 401 根据图 29A、29B 和 29C 所示的 CPU 操作序列进行操作，在 ST001 中决定要在哈希值计算中使用处理 A。在 ST005 中，CPU 401 设置哈希值计算电路 100 中的处理 A 寄存器组。CPU 401 在寄存器 A_ALG(302) 中设置指示 MD5 的“00”，在寄存器 A_BLK(303) 中设置“1”，在寄存器 A_IV(304) 中设置在 MD5 算法中规定的值，在寄存器 A_ENG(301) 中设置“1”，并发出哈希值计算开始请求。在接收到处理 A 开始请求时，哈希值计算电路 100 根据图 30A 所示的哈希值计算电路的操作序列进行操作，并且在 ST101-A 中，哈希值计算电路 100（或控制器 101）向共享资源管理器 209 发出 MD5 哈希值计算所需的以下使用请求：

[0690] • 扩展消息存储单元 107 的区域 0 的使用请求；

[0691] • 内部状态值存储单元 111 的区域 0 的使用请求；以及

[0692] • MD5 处理引擎的使用请求。

[0693] 由于处理 B 不使用这些资源，因此共享资源管理器 209 给予使用许可 A_ExMSG_ACK、A_TEMP_ACK 和 A_ENG_ACK，从而开始处理。在给予许可 A_ExMSG_ACK、A_TEMP_ACK 和 A_ENG_ACK 时，设置 A_EXE ＝ 1(T00)。

[0694] 在 T00 中，A_EXE ＝“1”，并且 A_ALG ＝ MD5。由于该原因，消息扩展处理结果选择器 109 选择 MD5 消息扩展处理器 108-1 的处理结果 MD5_ExMSG[31 :0] 作为输出 ExMSG_N[31 :0]。接着，分步处理结果选择器 113 选择 MD5 分步处理器 112-1 的处理结果 MD5_TEMP[127 :0] 作为输出 TEMP_N[127 :0]。此外，加法处理结果选择器 117 选择 MD5 加法处理器 116-1 的处理结果 MD5_IHASH[127 :0] 作为输出 IHASH_N[127 :0]。控制器 101 向 DMAC A 发出数据输入传输请求 A_DMA_REQ[0]。

[0695] 在 T01 中，在断言信号 A_DMA_ACK[0] 时，控制器 101 从下一个时钟的前沿开始更新步骤计数器 A_STP_CNT。计数器 A_STP_CNT 针对各时钟周期通过 +1 来进行更新，并在计数器 A_STP_CNT 计数到 65 时，将其清除为零。

[0696] 在区间 T01-T06 中，传输第一个块的输入消息的 16 个字，DMA IF 单元 103 输出数据 A_DMA_IDATA[63 :0] 作为数据 A_MSG[63 :0]。扩展消息存储数据选择器 106 选择输入消息数据 A_MSG[31 :0] 作为输出 ExMSG_0[31 :0]。

[0697] 在区间 T01-T06 中，MD5 消息扩展处理器 108-1 使用扩展消息存储单元 107 的区域 0 作为要处理的数据来执行处理。但是，由于扩展消息存储数据选择器 106 未选择处理结果 ExMSG_N[31 :0]，因此其不在扩展消息存储单元 107 中存储任何数据。在区间 T02-T07 中，扩展消息存储单元 107 存储第 1 到第 16 个扩展消息（输入消息）。

[0698] 在区间 T02-T07 中，MD5 分步处理器 112-1 使用存储在扩展消息存储单元 107 中的第 1 到第 16 个扩展消息作为要处理的数据来执行处理，并生成第 1 到第 16 个内部状态值。在区间 T03-T08 中，将处理结果存储到内部状态值存储单元 111 中。在区间 T0-T1 中，内部状态值存储数据选择器 110 输出哈希初始值 A_IV[255 :0] 作为输出 TEMP_0[255 :0]，并从 T02 开始通过选择 MD5 分步处理结果来输出值 TEMP_N[255 :0]。因此，在 T02 中，MD5 分步处理器 112-1 使用哈希初始值和第一输入消息来生成第一内部状态值。在区间 T03-T08 中，MD5 分步处理器 112-1 使用第 (n-1) 个内部状态值和第 n 个输入消息来生成第 n 个内部状态值 (n ＝ 2 到 16)。

[0699] 在区间 T03-T08 中，MD5 加法处理器 116-1 使用存储在内部状态值存储单元 111

中的第 1 到第 16 个分步处理数据作为要处理的数据，来执行针对第 1 到第 16 个内部状态值的加法处理。但是，由于哈希中间值存储数据选择器 114 未选择处理结果 IHASH_N[255 : 0]，因此其不在哈希中间值存储单元 115 中存储任何数据。

[0700] 在区间 T07-T17 中，扩展消息存储数据选择器 106 选择作为 MD5 消息扩展处理器 108-1 的处理结果的数据 ExMSG[31 :0] 作为输出 ExMSG_0[31 :0]。

[0701] 在区间 T07-T17 中，MD5 消息扩展处理器 108-1 使用存储在扩展消息存储单元 107 的区域 0 中的 16 个字的数据作为要处理的数据，来生成第 17 个到第 64 个扩展消息。在区间 T08-T20 中，将处理结果存储到扩展消息存储单元 107 中。扩展消息存储数据选择器 106 通过选择 MD5 扩展处理结果来输出数据 ExMSG_N[31 :0]。接着，MD5 消息扩展处理器 108-1 使用 16 个字的第 (n-16) 到第 (n-1) 个扩展消息来生成第 n 个扩展消息 (n = 17 到 64)。

[0702] 在区间 T08-T18 中，MD5 分步处理器 112-1 使用存储在扩展消息存储单元 107 中的第 17 到第 64 个扩展消息作为要处理的数据来执行处理，并生成第 17 到第 64 个内部状态值。在区间 T09-T19 中，将处理结果存储到内部状态值存储单元 111 中。内部状态值存储数据选择器 110 通过选择 MD5 分步处理结果来输出值 TEMP_N[255 :0]。因此，在区间 T08-T18 中，MD5 分步处理器 112-1 使用第 (n-1) 个内部状态值和第 n 个输入消息生成第 n 个内部状态值 (n = 17 到 64)。

[0703] 在区间 T09-T19 中，MD5 加法处理器 116-1 使用存储在内部状态值存储单元 111 中的第 17 到第 64 个分步处理数据作为要处理的数据，来执行针对第 17 到第 64 个内部状态值的加法处理。针对在 T19 中生成的第 64 个内部状态值的加法处理结果是第一个块的哈希中间值。在区间 T0-T18 中，哈希中间值存储数据选择器 114 输出哈希初始值 A_IV[255 : 0]，并从 T19 开始输出值 IHASH_N[255 :0]。因此，在 T19 中，MD5 加法处理器 116-1 执行哈希初始值和第 64 个内部状态值的加法处理，并在 T20 中将处理结果存储到哈希中间值存储单元 115 中。

[0704] 在 T20 中，将步骤计数器 A_STP_CNT 清除为零，块计数器 A_BLK_CNT 向上计数到 1。由于 A_BLK_CNT 没有超过 A_BLK 值“1”，因此控制器 101 向 DMAC A 发出下一个块的数据输入传输请求 A_DMA_REQ[0]。

[0705] 在 T21 中断言信号 A_DMA_ACK[0] 时，控制器 101 从下一个时钟的前沿开始更新步骤计数器 A_STP_CNT。计数器 A_STP_CNT 针对各时钟周期通过 +1 来进行更新，并在计数器 A_STP_CNT 计数到 65 时，将其清除为零。

[0706] 在区间 T21-T26 中，传输第二个块的输入消息的 16 个字，DMA IF 单元 103 输出数据 A_DMA_IDATA[63 :0] 作为数据 A_MSG[63 :0]。扩展消息存储数据选择器 106 选择输入消息数据 A_MSG[31 :0] 作为输出 ExMSG_0[31 :0]。

[0707] 在区间 T21-T26 中，MD5 消息扩展处理器 108-1 使用扩展消息存储单元 107 的区域 0 作为要处理的数据来执行处理。但是，由于扩展消息存储数据选择器 106 未选择处理结果 ExMSG_N[31 :0]，因此其不在扩展消息存储单元 107 中存储任何数据。在区间 T22-T27 中，扩展消息存储单元 107 存储第 1 到第 16 个扩展消息（输入消息）。

[0708] 在区间 T22-T27 中，MD5 分步处理器 112-1 使用存储在扩展消息存储单元 107 中的第 1 到第 16 个扩展消息作为要处理的数据来执行处理，并生成第 1 到第 16 个内部状态值。在区间 T23-T28 中，将处理结果存储到内部状态值存储单元 111 中。在区间 T20-T21

中，内部状态值存储数据选择器 110 输出值 IHASH[255 :0] 作为输出 TEMP_0[255 :0]，并从 T22 开始通过选择 MD5 分步处理结果来输出值 TEMP_N[255 :0]。因此，在 T22 中，MD5 分步处理器 112-1 使用前一个块的哈希中间值和第一输入消息来生成第一内部状态值。在区间 T23-T28 中，MD5 分步处理器 112-1 使用第 (n-1) 个内部状态值和第 n 个输入消息生成第 n 个内部状态值 (n ＝ 2 到 16)。

[0709] 在区间 T23-T28 中，MD5 加法处理器 116-1 使用存储在内部状态值存储单元 111 中的第 1 到第 16 个分步处理数据作为要处理的数据，来执行针对第 1 到第 16 个内部状态值的加法处理。但是，由于不满足哈希中间值存储单元 115 的存储条件，因此不存储处理结果。

[0710] 在区间 T27-T42 中，扩展消息存储数据选择器 106 选择作为 MD5 消息扩展处理器 108-1 的处理结果的数据 ExMSG[31 :0] 作为输出 ExMSG_0[31 :0]。

[0711] 在区间 T27-T42 中，MD5 消息扩展处理器 108-1 使用存储在扩展消息存储单元 107 的区域 0 中的 16 个字的数据作为要处理的数据来生成第 17 个到第 64 个扩展消息。在区间 T28-T43 中，将处理结果存储到扩展消息存储单元 107 中。扩展消息存储数据选择器 106 通过选择 MD5 扩展处理结果来输出数据 ExMSG_N[31 :0]。接着，MD5 消息扩展处理器 108-1 使用 16 个字的第 (n-16) 到第 (n-1) 个扩展消息来生成第 n 个扩展消息 (n ＝ 17 到 64)。

[0712] 在区间 T28-T43 中，MD5 分步处理器 112-1 使用存储在扩展消息存储单元 107 中的第 17 到第 64 个扩展消息作为要处理的数据来执行处理，并生成第 17 到第 64 个内部状态值。在区间 T29-T44 中，将处理结果存储到内部状态值存储单元 111 中。内部状态值存储数据选择器 110 通过选择 MD5 分步处理结果来输出值 TEMP_N[255 :0]。因此，在区间 T28-T43 中，MD5 分步处理器 112-1 使用第 (n-1) 个内部状态值和第 n 个输入消息，来生成第 n 个内部状态值 (n ＝ 17 到 64)。

[0713] 在区间 T29-T44 中，MD5 加法处理器 116-1 使用存储在内部状态值存储单元 111 中的第 17 到第 64 个分步处理数据作为要处理的数据，来执行针对第 17 到第 64 个内部状态值的加法处理。针对在 T4 中生成的第 64 个内部状态值的加法处理结果是第二个块的哈希中间值。由于哈希中间值存储单元 115 存储前一个块的哈希中间值，因此执行前一个块的哈希中间值和第 64 个内部状态值的加法处理，并在 T45 中将处理结果存储到哈希中间值存储单元 115 中。

[0714] 在 T45 中，将步骤计数器 A_STP_CNT 清除为零，块计数器 A_BLK_CNT 向上计数到 2。由于 A_BLK_CNT 超过 A_BLK 值“1”，因此控制器 101 将块计数器 A_BLK_CNT 清零并向 DMAC_A 发出哈希值的数据输出传输请求 A_DMA_REQ[1]。

[0715] 在区间 T46-T47 中，断言信号 A_DMA_ACK[1]，并进行 128 位的 MD5 哈希值的输出传输。

[0716] 哈希值计算电路 100 根据图 30A 所示的哈希值计算电路 100 的操作序列进行操作，并在 ST116-A 中拒绝执行 MD5 哈希值计算所需的以下使用请求 :

[0717] • 扩展消息存储单元 107 的区域 0 的使用请求 ;

[0718] • 内部状态值存储单元 111 的区域 0 的使用请求 ;以及

[0719] •MD5 处理引擎 108-1、112-1 和 116-1 的使用请求。接着哈希值计算电路 100 完成消息 A 的哈希值计算。由于拒绝了使用请求，因此也拒绝了使用许可 A_ExMSG_ACK、A_TEMP_

ACK 和 A_ENG_ACK，从而设置 A_EXE ＝ 1(T48)。

[0720] 另一方面，假定在 T05 中接收了消息 B。在接收到消息 B 时，CPU 401 根据图 29A、29B 和 29C 所示的 CPU 操作序列进行操作。在 ST001 中，由于处理 A 正在处理消息，因此 CPU 决定将在哈希值计算中使用处理 B。在 ST011 中，CPU 401 设置哈希值计算电路 100 的处理 B 寄存器组。CPU401 在寄存器 B_ALG(306) 中设置指示 SHA1 的“01”，在寄存器 B_BLK(307) 中设置“0”，在寄存器 B_IV(308) 中设置在 SHA1 算法中规定的值，在寄存器 B_ENB(305) 中设置“1”，并发出哈希值计算开始请求。在接收到处理 B 开始请求时，哈希值计算电路 100 根据图 30B 所示的哈希值计算电路的操作序列进行操作，在 ST101-B 中哈希值计算电路 100（或控制器 101）向共享资源管理器 209 发出 SHA1 哈希值计算所需的以下使用请求：

[0721] • 扩展消息存储单元 107 的区域 1 的使用请求；

[0722] • 内部状态值存储单元 111 的区域 1 的使用请求；以及

[0723] • SHA1 处理引擎的使用请求。

[0724] 由于处理 A 不使用这些资源，因此共享资源管理器 209 给予使用许可 B_ExMSG_ACK、B_TEMP_ACK 和 B_ENG_ACK 从而开始处理。在给予许可 B_ExMSG_ACK、B_TEMP_ACK 和 B_ENG_ACK 时，设置 B_EXE ＝ 1(T06)。

[0725] 在 T06 中，B_EXE ＝“1”并且 B_ALG ＝ SHA1。响应于此，消息扩展处理结果选择器 109 选择 SHA1 消息扩展处理器 108-2 的处理结果 SHA1_ExMSG[31 :0] 作为输出 ExMSG_N[63 :32]。接着，分步处理结果选择器 113 选择 SHA1 分步处理器 112-2 的处理结果 SHA1_TEMP[127 :0] 作为输出 TEMP_N[255 :128]。此外，加法处理结果选择器 117 选择 SHA1 加法处理器 116-2 的处理结果 SHA1_IHASH[159 :0] 作为输出 IHASH_N[511 :256]。控制器 101 向 DMAC B 发出数据输入传输请求 B_DMA_REQ[0]。

[0726] 在 T07 中，在断言信号 B_DMA_ACK[0] 时，控制器 101 从下一个时钟的前沿开始更新步骤计数器 B_STP_CNT。计数器 B_STP_CNT 针对各时钟周期通过 +1 进行更新，并在计数器 B_STP_CNT 计数到 81 时，将其清除为零。

[0727] 在区间 T06-T12 中，传输第一个块的输入消息的 16 个字，并且 DMAIF 单元 103 输出数据 B_DMA_IDATA[63 :0] 作为数据 B_MSG[63 :0]。扩展消息存储数据选择器 106 选择输入消息数据 B_MSG[31 :0] 作为输出 ExMSG_1[31 :0]。

[0728] 在区间 T06-T12 中，SHA1 消息扩展处理器 108-2 使用扩展消息存储单元 107 的区域 1 作为要处理的数据来执行处理。但是，由于扩展消息存储数据选择器 106 未选择处理结果 ExMSG_N[63 :32]，因此其不在扩展消息存储单元 107 中存储任何数据。在区间 T07-T13 中，扩展消息存储单元 107 存储第 1 到第 16 个扩展消息（输入消息）。

[0729] 在区间 T07-T13 中，SHA1 分步处理器 112-2 使用存储在扩展消息存储单元 107 中的第 1 到第 16 个扩展消息作为要处理的数据来执行处理，并生成第 1 到第 16 个内部状态值。在区间 T08-T14 中，将处理结果存储到内部状态值存储单元 111 中。在区间 T06-T07 中，内部状态值存储数据选择器 110 输出哈希初始值 B_IV[255 :0] 作为输出 TEMP_1[255 :0]，并从 T08 开始通过选择 SHA1 分步处理结果来输出值 TEMP_N[511 :256]。因此，在 T08 中，SHA1 分步处理器 112-2 使用哈希初始值和第一输入消息来生成第一内部状态值。在区间 T09-T13 中，SHA1 分步处理器 112-2 使用第 (n-1) 个内部状态值和第 n 个输入消息，来生成第 n 个内部状态值 (n ＝ 2 到 16)。

[0730] 在区间 T08-T14 中，SHA1 加法处理器 116-2 使用存储在内部状态值存储单元 111 中的第 1 到第 16 个分步处理数据作为要处理的数据，来执行针对第 1 到第 16 个内部状态值的加法处理。但是，由于哈希中间值存储数据选择器 114 未选择处理结果 IHASH_N[511 : 256]，因此其不在哈希中间值存储单元 115 中存储任何数据。

[0731] 在区间 T13-T32 中，扩展消息存储数据选择器 106 选择作为 SHA1 消息扩展处理器 108-2 的处理结果的数据 ExMSG[63 :32] 作为输出 ExMSG_1[31 :0]。

[0732] 在区间 T13-T32 中，SHA1 消息扩展处理器 108-2 使用存储在扩展消息存储单元 107 的区域 1 中的 16 个字的数据作为要处理的数据，来生成第 17 个到第 80 个扩展消息。在区间 T14-T33 中将处理结果存储到扩展消息存储单元 107 中。扩展消息存储数据选择器 106 通过选择 SHA1 扩展处理结果来输出数据 ExMSG_N[31 :0]。接着，SHA1 消息扩展处理器 108-2 使用 16 个字的第 (n-16) 到第 (n-1) 个扩展消息，来生成第 n 个扩展消息 (n ＝ 17 到 80)。

[0733] 在区间 T14-T33 中，SHA1 分步处理器 112-2 使用存储在扩展消息存储单元 107 中的第 17 到第 80 个扩展消息作为要处理的数据来执行处理，并生成第 17 到第 80 个内部状态值。在区间 T15-T34 中，将处理结果存储到内部状态值存储单元 111 中。内部状态值存储数据选择器 110 通过选择 SHA1 分步处理结果来输出值 TEMP_N[511 :256]。因此，在区间 T14-T33 中，SHA1 分步处理器 112-2 使用第 (n-1) 个内部状态值和第 n 个输入消息，来生成第 n 个内部状态值 (n ＝ 17 到 80)。

[0734] 在区间 T15-T34 中，SHA1 加法处理器 116-2 使用存储在内部状态值存储单元 111 中的第 17 到第 80 个分步处理数据作为要处理的数据，来执行针对第 17 到第 80 个内部状态值的加法处理。针对在 T34 中生成的第 80 个内部状态值的加法处理结果是第一个块的哈希中间值。在区间 T06-T33 中，哈希中间值存储数据选择器 114 输出哈希初始值 B_IV[255 : 0]，并从 T34 开始输出值 IHASH_N[255 :0]。因此，在 T34 中 SHA1 加法处理器 116-2 执行哈希初始值和第 80 个内部状态值的加法处理，并在 T35 中将处理结果存储到哈希中间值存储单元 115 中。

[0735] 在 T35 中，将步骤计数器 B_STP_CNT 清除为零，块计数器 B_BLK_CNT 向上计数到 1。由于 B_BLK_CNT 超过 B_BLK 值“0”，因此控制器 101 将块计数器 B_BLK_CNT 清零，并向 DMAC B 发出哈希值的数据输出传输请求 B_DMA_REQ[1]。

[0736] 在区间 T36-T38 中，断言信号 B_DMA_ACK[1]，并进行 160 位的 SHA1 哈希值的输出传输。哈希值计算电路 100 根据图 30B 所示的哈希值计算电路 100 的操作序列进行操作，并在 ST116-B 中拒绝执行 SHA1 哈希值计算所需的以下使用请求 :

[0737] • 扩展消息存储单元 107 的区域 1 的使用请求 ;

[0738] • 内部状态值存储单元 111 的区域 1 的使用请求 ;以及

[0739] • SHA1 处理引擎 108-2、112-2 和 116-2 的使用请求。

[0740] 接着哈希值计算电路 100 完成消息 B 的哈希值计算。在拒绝使用许可 B_ExMSG_ACK、B_TEMP_ACK 和 B_ENG_ACK 时，设置 B_EXE ＝ 0(T39)。

[0741] 此外，假定在消息 B 的哈希值计算完成后、在消息 A 的哈希值计算完成前接收了消息 C。在接收到消息 C 时，CPU 401 根据图 29A、29B 和 29C 所示的 CPU 操作序列进行操作。在 ST001 中，由于处理 A 正在处理消息，因此 CPU 决定在哈希值计算中使用处理 B。在 ST011

中，CPU 401 设置哈希值计算电路 100 的处理 B 寄存器组。CPU 401 在寄存器 B_ALG(306) 中设置指示 SHA512 的“10”，在寄存器 B_BLK(307) 中设置“7”，在寄存器 B_IV(308) 中设置在 SHA512 算法中规定的值，在寄存器 B_ENB(305) 中设置“1”，并发出哈希值计算开始请求。

[0742] 在接收到处理 B 开始请求时，哈希值计算电路 100 根据图 30B 所示的哈希值计算电路的操作序列进行操作，并且在 ST101-B 中哈希值计算电路 100（或控制器 101）向共享资源管理器 209 发出 SHA512 哈希值计算所需的以下使用请求：

[0743] • 扩展消息存储单元 107 的区域 0 和区域 1 的使用请求；

[0744] • 内部状态值存储单元 111 的区域 0 和区域 1 的使用请求；以及

[0745] • SHA512 处理引擎的使用请求。

[0746] 由于处理 A 使用扩展消息存储单元 107 的区域 0 和内部状态值存储单元 111 的区域 0，因此共享资源管理器 209 不给予使用许可 B_ExMSG_ACK 和 B_TEMP_ACK。此外，由于处理 A 不使用引擎 108-3、112-3 和 116-3，因此共享资源管理器 209 给予许可 B_ENG_ACK。控制器 101 不开始处理，直到共享资源管理器 209 给予许可 B_ExMSG_ACK 和 B_TEMP_ACK 为止。

[0747] 在 T48 中，在处理 A 完成消息 A 的哈希值计算并拒绝扩展消息存储单元 107 的区域 0 和内部状态值存储单元 111 的区域 0 的使用请求时，给予许可 B_ExMSG_ACK 和 B_TEMP_ACK，并设置 B_EXE ＝ 1。

[0748] 在 T48 中，B_EXE ＝“1”并且 B_ALG ＝ SHA512。因此，消息扩展处理结果选择器 109 选择 SHA512 消息扩展处理器 108-3 的处理结果 SHA512_ExMSG[63 :0] 作为输出 ExMSG_N[63 :0]。接着，分步处理结果选择器 113 选择 SHA512 分步处理器 112-3 的处理结果 SHA512_TEMP[511 :0] 作为输出 TEMP_N[511 :0]。此外，加法处理结果选择器 117 选择 SHA512 加法处理器 116-3 的处理结果 SHA512_IHASH[511 :0] 作为输出 IHASH_N[511 :0]。在 T48 中，控制器 101 向 DMAC B 发出数据输入传输请求 B_DMA_REQ[0]。

[0749] 在 T49 中，在断言信号 B_DMA_ACK[0] 时，控制器 101 从下一个时钟的前沿开始更新步骤计数器 B_STP_CNT。计数器 B_STP_CNT 针对各时钟周期通过 +1 进行更新，并在计数器 B_STP_CNT 计数到 81 时，将其清除为零。

[0750] 在区间 T49-T54 中，传输第一个块的输入消息的 16 个字，并且 DMAIF 单元 103 输出数据 B_DMA_IDATA[63 :0] 作为数据 B_MSG[63 :0]。扩展消息存储数据选择器 106 选择输入消息数据 B_MSG[31 :0] 作为输出 ExMSG_0[31 :0]，并选择输入消息数据 B_MSG[63 :32] 作为输出 ExMSG_1[31 :0]。

[0751] 在区间 T49-T54 中，SHA512 消息扩展处理器 108-3 使用扩展消息存储单元 107 的区域 0 和区域 1 作为要处理的数据来执行处理。但是，由于扩展消息存储数据选择器 106 未选择处理结果 ExMSG_N[63 :0]，因此其不在扩展消息存储单元 107 中存储任何数据。在区间 T50-T55 中，扩展消息存储单元 107 存储第 1 到第 16 个扩展消息（输入消息）。

[0752] 在区间 T50-T55 中，SHA512 分步处理器 112-3 使用存储在扩展消息存储单元 107 中的第 1 到第 16 个扩展消息作为要处理的数据来执行处理，并生成第 1 到第 16 个内部状态值。在区间 T51-T56 中，将处理结果存储到内部状态值存储单元 111 中。在区间 T48-T49 中，内部状态值存储数据选择器 110 输出哈希初始值的低 256 位 B_IV[255 :0] 作为输出 TEMP_0[255 :0]。此外，内部状态值存储数据选择器 110 输出高 256 位 B_IV[511 :256] 作为输出 TEMP_1[255 :0]。从 T50 开始，内部状态值存储数据选择器 110 通过选择 SHA512 分步

处理结果的低 256 位来输出值 TEMP_N[255 :0] 作为输出 TEMP_0[255 :0]。此外，内部状态值存储数据选择器 110 通过选择 SHA512 分步处理结果的高 256 位来输出值 TEMP_N[511 : 256] 作为输出 TEMP_1[255 :0]。因此，在 T50 中，SHA512 分步处理器 112-3 使用哈希初始值和第一输入消息，来生成第一内部状态值。在区间 T51-T55 中，SHA512 分步处理器 112-3 使用第 (n-1) 个内部状态值和第 n 个输入消息来生成第 n 个内部状态值 (n = 2 到 16)。

[0753] 在区间 T51-T56 中，SHA512 加法处理器 116-3 使用存储在内部状态值存储单元 111 中的第 1 到第 16 个分步处理数据作为要处理的数据，来执行针对第 1 到第 16 个内部状态值的加法处理。但是，由于哈希中间值存储数据选择器 114 未选择处理结果 IHASH_ N[511 :0]，因此其不在哈希中间值存储单元 115 中存储任何数据。

[0754] 在区间 T55-T60 中，扩展消息存储数据选择器 106 输出作为 SHA512 消息扩展处理器 108-3 的处理结果的高位的数据 ExMSG_N[31 :0]，来作为输出 ExMSG_0[31 :0]。此外，扩展消息存储数据选择器 106 输出作为 SHA512 消息扩展处理器 108-3 的处理结果的低位的数据 ExMSG_N[63 :32]，作为输出 ExMSG_1[31 :0]。

[0755] 在区间 T55-T60 中，SHA512 消息扩展处理器 108-3 使用存储在扩展消息存储单元 107 的区域 0 和区域 1 中的 16 个字的数据作为要处理的数据，来生成第 17 个到第 80 个扩展消息。在区间 T56-T61 中，将处理结果存储到扩展消息存储单元 107 中。扩展消息存储数据选择器 106 输出作为 SHA512 消息扩展处理器 108-3 的处理结果的高位的数据 ExMSG_N[31 : 0]，来作为输出 ExMSG_0[31 :0]。此外，扩展消息存储数据选择器 106 输出作为 SHA512 消息扩展处理器 108-3 的处理结果的低位的数据 ExMSG_N[63 :32]，来作为输出 ExMSG_1[31 : 0]。接着，SHA512 消息扩展处理器 108-3 使用 16 个字的第 (n-16) 到第 (n-1) 个扩展消息，来生成第 n 个扩展消息 (n = 17 到 80)。

[0756] 在区间 T56-T61 中，SHA512 分步处理器 112-3 使用存储在扩展消息存储单元 107 中的第 17 到第 80 个扩展消息作为要处理的数据来执行处理，并生成第 17 到第 80 个内部状态值。在区间 T57-T62 中，将处理结果存储到内部状态值存储单元 111 中。内部状态值存储数据选择器 110 通过选择 SHA512 分步处理结果来输出值 TEMP_N[511 :0] 的低 256 位 TEMP_N[255 :0]，来作为输出 TEMP_0[255 :0]。此外，内部状态值存储数据选择器 110 输出高 256 位 TEMP_N[511 :256] 来作为输出 TEMP_1[255 :0]。因此，在区间 T56-T61 中，SHA512 分步处理器 112-3 使用第 (n-1) 个内部状态值和第 n 个输入消息，来生成第 n 个内部状态值 (n = 17 到 80)。

[0757] 在区间 T57-T62 中，SHA512 加法处理器 116-3 使用存储在内部状态值存储单元 111 中的第 17 到第 80 个分步处理数据作为要处理的数据，来执行针对第 17 到第 80 个内部状态值的加法处理。针对在 T62 中生成的第 80 个内部状态值的加法处理结果是第一个块的哈希中间值。在区间 T48-T61 中，哈希中间值存储数据选择器 114 输出哈希初始值的低 256 位 B_IV[255 :0] 来作为输出 IHASH_0[255 :0]，并选择高 256 位 B_IV[[511 :256] 来作为输出 IHASH_1[511 :256]。从 T62 开始，哈希中间值存储数据选择器 114 输出值 IHASH_ N[255 :0] 作为输出 IHASH_0[255 :0]，并输出值 IHASH_N[511 :256] 作为输出 IHASH_1[511 : 256]。因此，在 T62 中 SHA512 加法处理器 116-3 执行哈希初始值和第 80 个内部状态值的加法处理，并在 T63 中将处理结果存储到哈希中间值存储单元 115 中。

[0758] 在 T63 中，将步骤计数器 B_STP_CNT 清除为零，块计数器 B_BLK_CNT 向上计数到 1。

由于 B_BLK_CNT 不超过 B_BLK 值“7”，因此控制器 101 向 DMAC B 发出下一个块的数据输入传输请求 B_DMA_REQ[0]。

[0759] 类似地，控制器 101 针对该数量或者更多的块，重复进行处理。

[0760] 在 T66 中，获得针对最后一个块的第 80 个内部状态值的加法处理结果。在 T67 中，将处理结果存储到哈希中间值存储单元 115 中。

[0761] 在 T67 中，将步骤计数器 B_STP_CNT 清除为零，块计数器 B_BLK_CNT 向上计数到 8。由于 B_BLK_CNT 超过 B_BLK 值“7”，因此控制器 101 将块计数器 B_BLK_CNT 清零，并向 DMAC B 发出哈希值的数据输出传输请求 B_DMA_REQ[1]。

[0762] 在区间 T81-T88 中，断言信号 B_DMA_ACK[1]，并进行 512 位的 SHA512 哈希值的输出传输。哈希值计算电路 100 根据图 30B 所示的哈希值计算电路 100 的操作序列进行操作，并在 ST116-B 中拒绝执行 SHA512 哈希值计算所需的以下使用请求：

[0763] • 扩展消息存储单元 107 的区域 0 和区域 1 的使用请求；

[0764] • 内部状态值存储单元 111 的区域 0 和区域 1 的使用请求；以及

[0765] • SHA512 处理引擎 108-3、112-3 和 116-3 的使用请求。

[0766] 接着哈希值计算电路 100 完成消息 C 的哈希值计算。在拒绝使用许可 B_ExMSG_ACK、B_TEMP_ACK 和 B_ENG_ACK 时，设置 B_EXE ＝ 0(T89)。

[0767] 如上所述，上述配置能够处理多个哈希算法、即 MD5、SHA1 和 SHA512 的消息。由于扩展消息存储单元、内部状态值存储单元和哈希中间值存储单元在使用时不会被各个哈希算法占用，因此能够抑制电路规模的增加。

[0768] 此外，能够并行进行消息 A 和消息 B 的处理，能够在消息 C 之前正在进行处理的消息 A 的处理完成时，开始和执行由于其它处理使用共享资源而无法并行处理的消息 C 的哈希值计算。

[0769] 即使在不执行消息处理时，处理引擎也始终针对要处理的数据区域执行处理，并始终更新要处理的数据的区域。由于该原因，当请求并执行特定哈希算法处理时，能够提供能够抑制功耗的变化并能够确保高抗篡改性和高安全性的哈希值计算装置。

[0770] 根据上述配置，能够在抑制电路规模增加的同时执行多个不同的哈希算法的哈希值计算，能够在更少的限制条件下同时执行针对多个消息的哈希值计算。此外，能够提供能够与选择的哈希算法无关地抑制功耗变化并能够确保高抗篡改性和高安全性的哈希值计算装置。

[0771] 中间值存储器单元能够存储来自多个哈希值计算单元中的输出数据中的具有最大位宽的输出数据。也就是说，根据最大位宽来实现上述配置。由于该原因，能够使所处理的哈希算法难以指定。另外，在处理不需要最大位宽的哈希算法时，能够通过使用未使用的位区域来减少哈希值计算的中断和重新开始的时间开销，并通过超前存储处理输入块来加速处理。

[0772] 根据本发明，能够提供能够在处理中间切换针对多个消息的哈希值计算而不降低任何处理性能，并且能够确保高安全性的哈希值计算技术。此外，根据本发明，能够提供能够同时执行多个哈希算法，并能够确保小的电路规模和高安全性的哈希值计算技术。

[0773] 其它实施例

[0774] 本发明的各方面还可以通过读出并执行记录在存储装置上的用于执行上述实施

例的功能的程序的系统或设备的计算机（或诸如CPU或MPU的装置）、以及由系统或设备的计算机例如读出并执行记录在存储装置上的用于执行上述实施例的功能的程序来执行步骤的方法来实现。鉴于此，例如经由网络或者从用作存储装置的各种类型的记录介质（例如计算机可读介质）向计算机提供程序。

[0775] 虽然参照示例性实施例对本发明进行了描述，但是应当理解，本发明不限于所公开的示例性实施例。所附权利要求的范围符合最宽的解释，以覆盖所有变型、等同结构和功能。

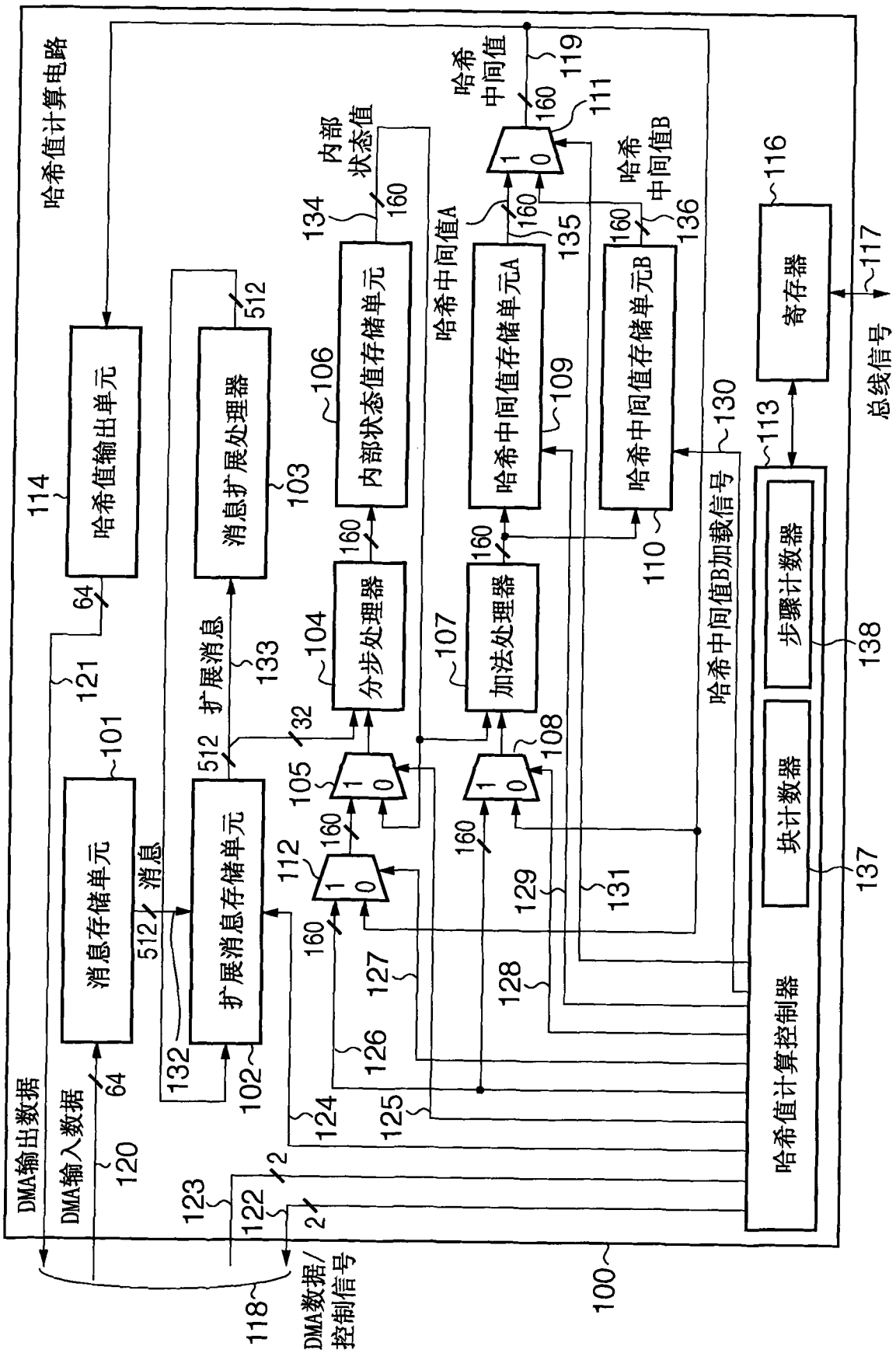

哈希值计算电路
DMA输出数据
DMA输入数据
DMA数据/控制信号
哈希值输出单元
消息存储单元
扩展消息存储单元
消息扩展处理器
分步处理器
加法处理器
内部状态值存储单元
哈希中间值存储单元A
哈希中间值存储单元B
寄存器
块计数器
步骤计数器
哈希值计算控制器
哈希中间值B加载信号
总线信号
消息
扩展消息
内部状态值
哈希中间值
哈希中间值A
哈希中间值B
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138

图 1

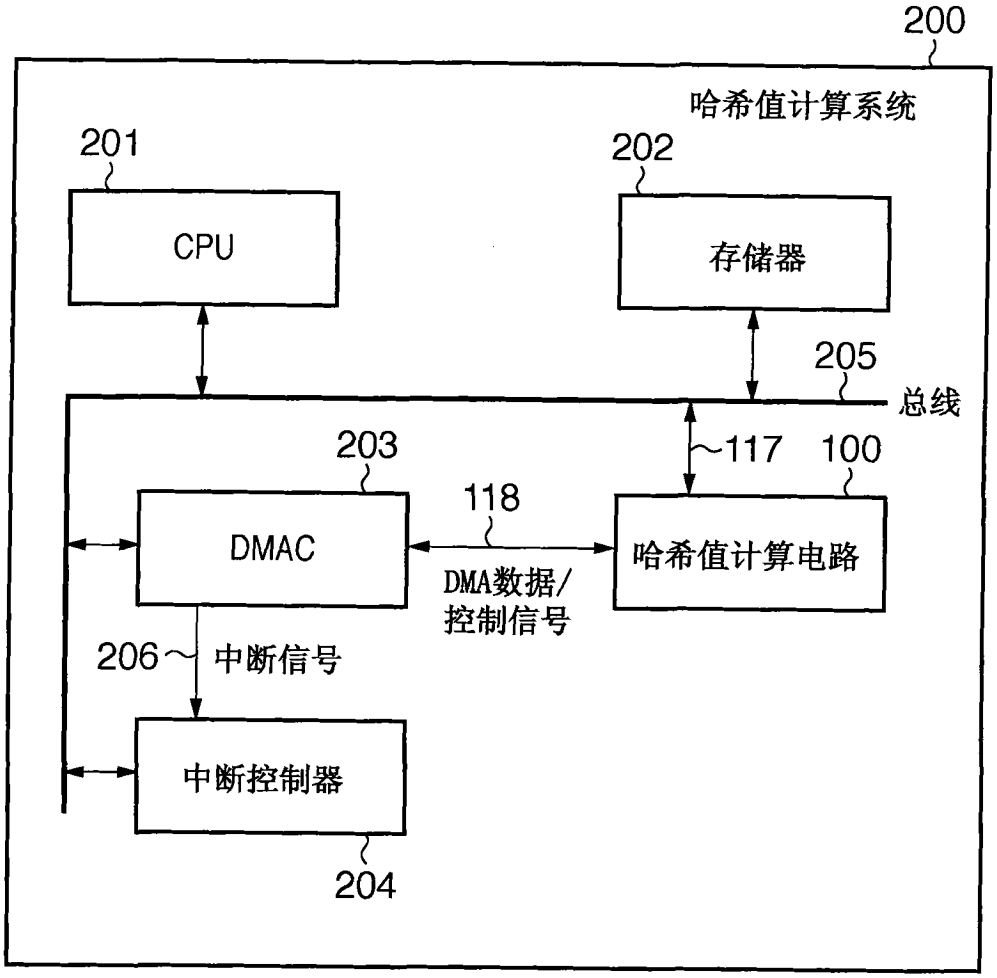

200
哈希值计算系统
201
CPU
202
存储器
205
总线
203
117
100
118
DMAC
哈希值计算电路
DMA数据/
控制信号
206
中断信号
中断控制器
204

图 2

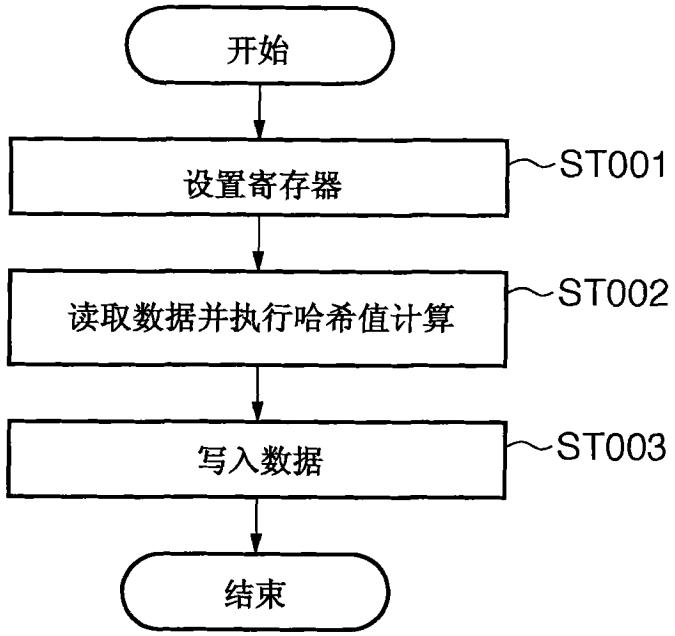

开始
设置寄存器
ST001
读取数据并执行哈希值计算
ST002
写入数据
ST003
结束

图 3

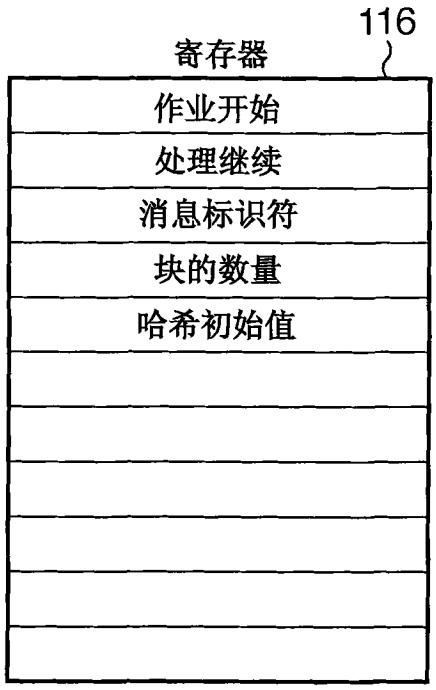

116
寄存器
作业开始
处理继续
消息标识符
块的数量
哈希初始值

图 4

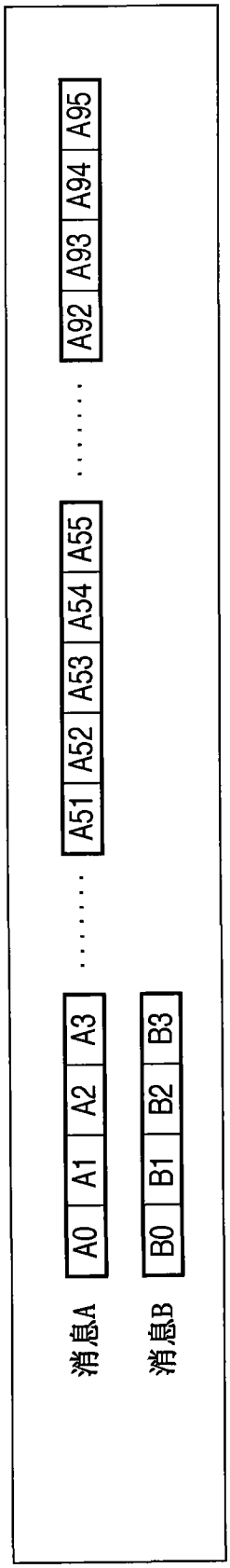

消息A
A0 A1 A2 A3 ..... A51 A52 A53 A54 A55 ..... A92 A93 A94 A95
消息B
B0 B1 B2 B3

图 5

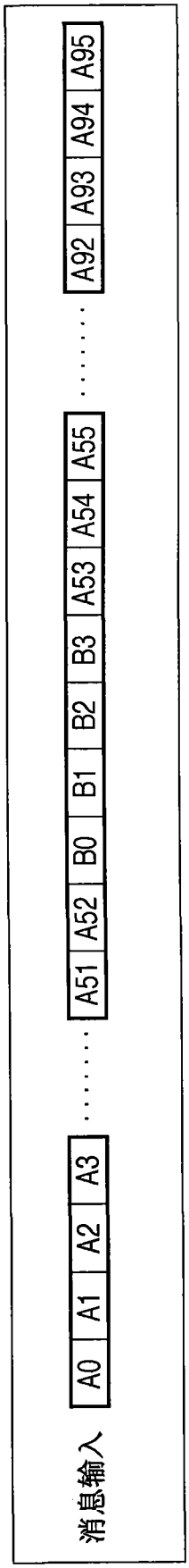

消息输入
A0 A1 A2 A3 ..... A51 A52 B0 B1 B2 B3 A53 A54 A55 ..... A92 A93 A94 A95

图 6

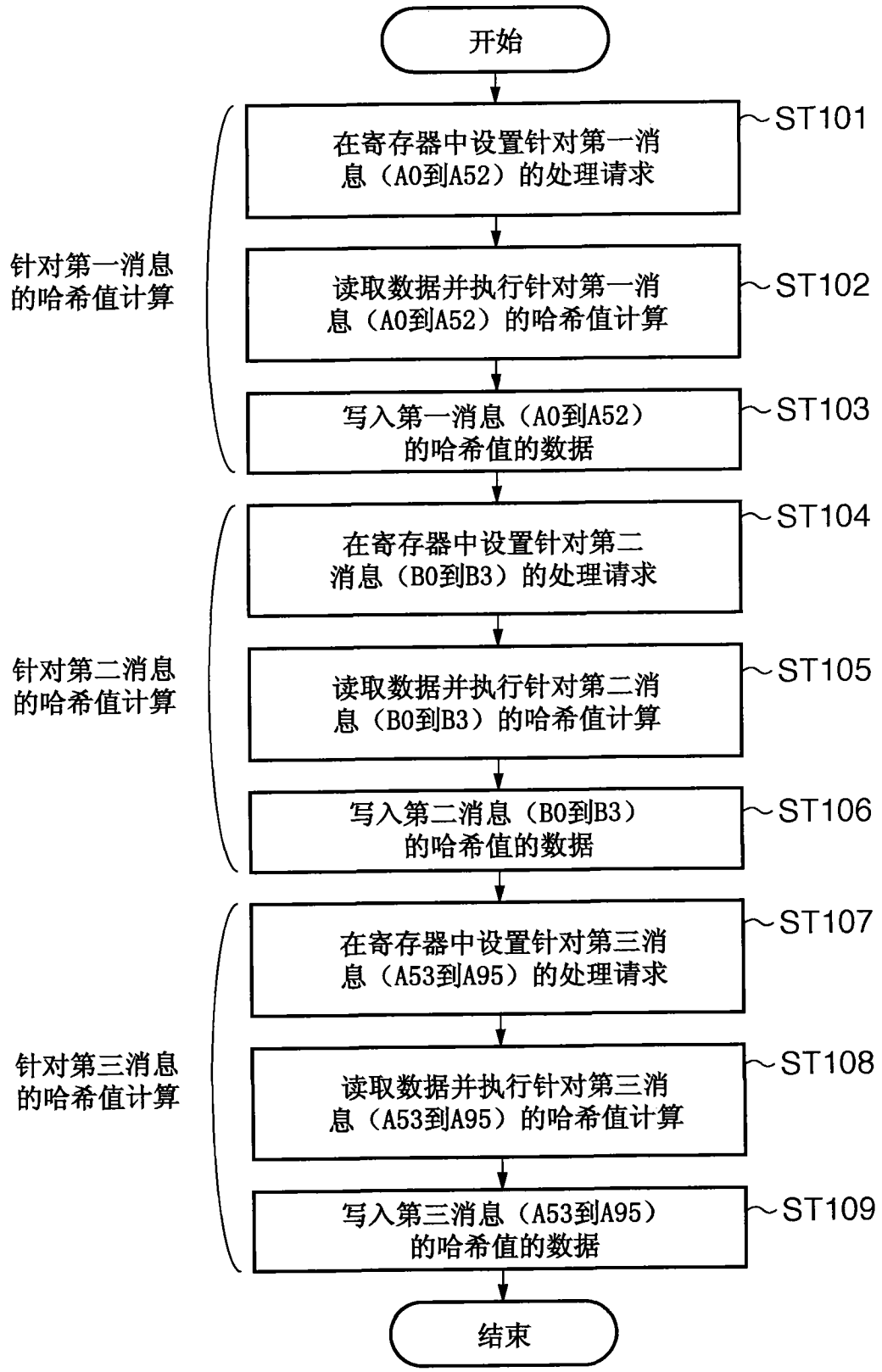

开始
在寄存器中设置针对第一消息（A0到A52）的处理请求
ST101
读取数据并执行针对第一消息（A0到A52）的哈希值计算
ST102
写入第一消息（A0到A52）的哈希值的数据
ST103
针对第一消息的哈希值计算
在寄存器中设置针对第二消息（B0到B3）的处理请求
ST104
读取数据并执行针对第二消息（B0到B3）的哈希值计算
ST105
写入第二消息（B0到B3）的哈希值的数据
ST106
针对第二消息的哈希值计算
在寄存器中设置针对第三消息（A53到A95）的处理请求
ST107
读取数据并执行针对第三消息（A53到A95）的哈希值计算
ST108
写入第三消息（A53到A95）的哈希值的数据
ST109
针对第三消息的哈希值计算
结束

图 7

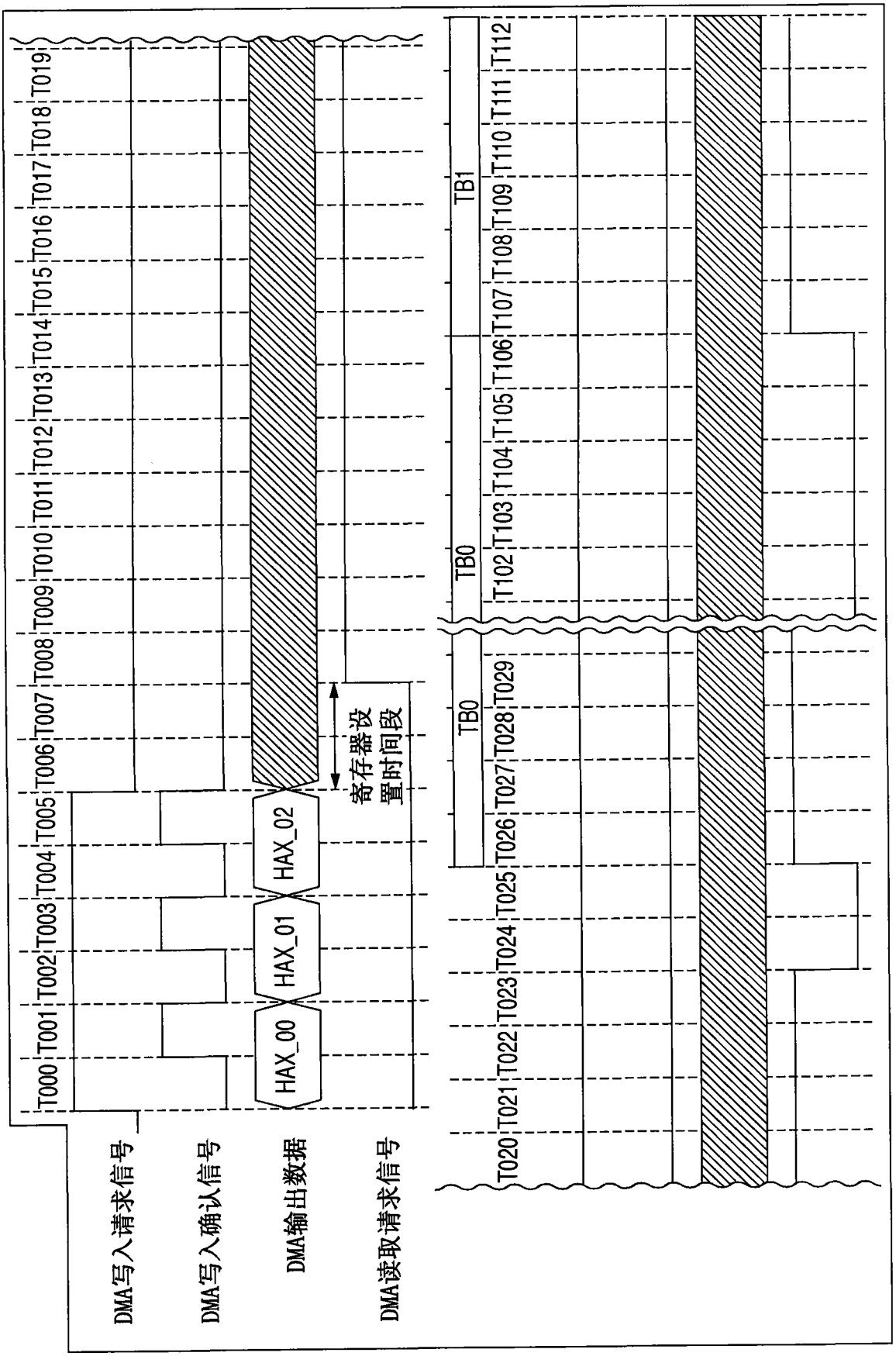

DMA写入请求信号
DMA写入确认信号
DMA输出数据
DMA读取请求信号
HAX_00
HAX_01
HAX_02
寄存器设置时间段
TB0
TB1
T000 T001 T002 T003 T004 T005 T006 T007 T008 T009 T010 T011 T012 T013 T014 T015 T016 T017 T018 T019
T020 T021 T022 T023 T024 T025 T026 T027 T028 T029
T102 T103 T104 T105 T106 T107 T108 T109 T110 T111 T112

图 8A

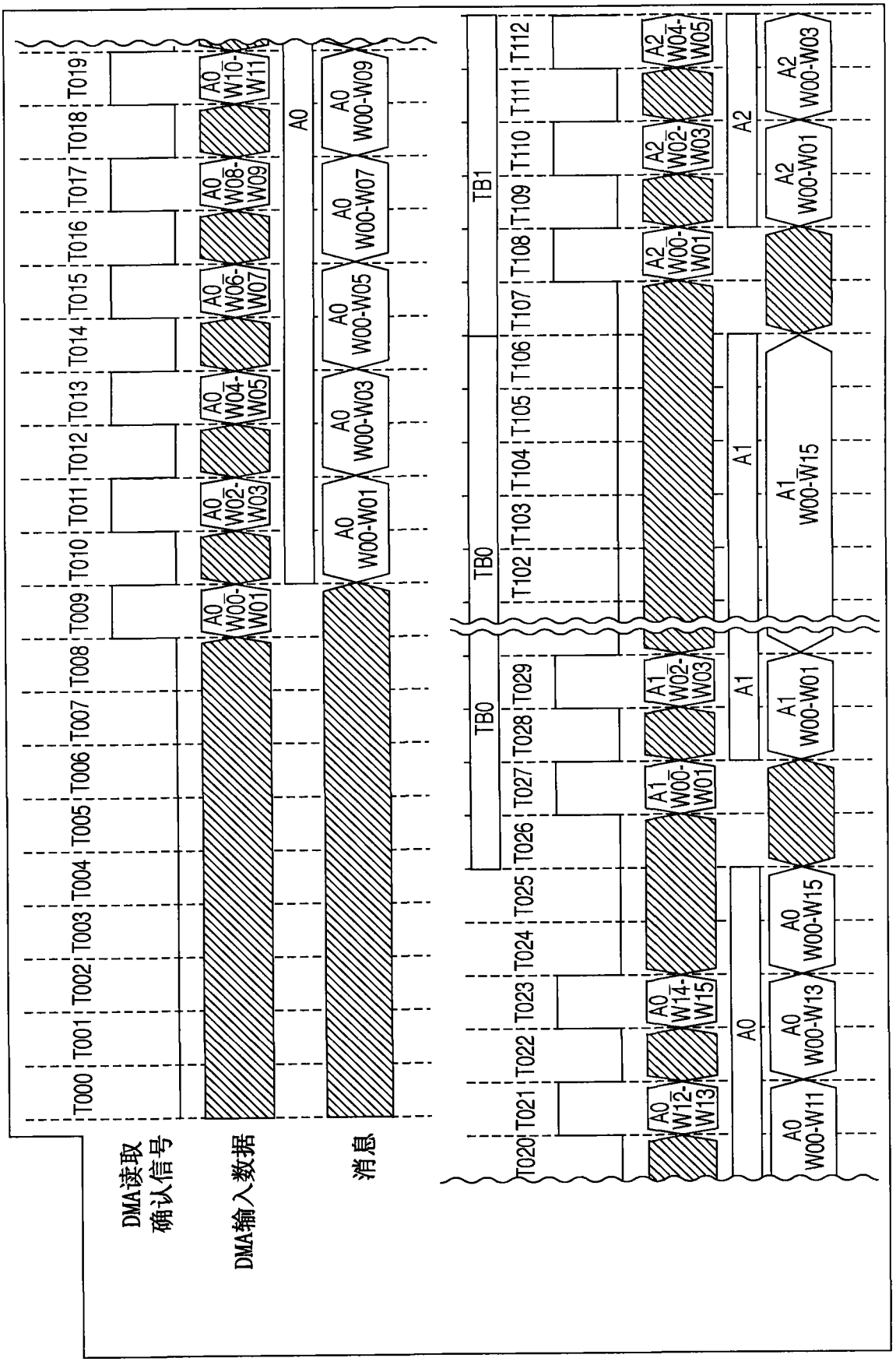

DMA读取确认信号
DMA输入数据
消息
T000 T001 T002 T003 T004 T005 T006 T007 T008 T009 T010 T011 T012 T013 T014 T015 T016 T017 T018 T019 T020 T021 T022 T023 T024 T025 T026 T027 T028 T029 T102 T103 T104 T105 T106 T107 T108 T109 T110 T111 T112
TB0
TB1
A0
A1
A2

图 8B

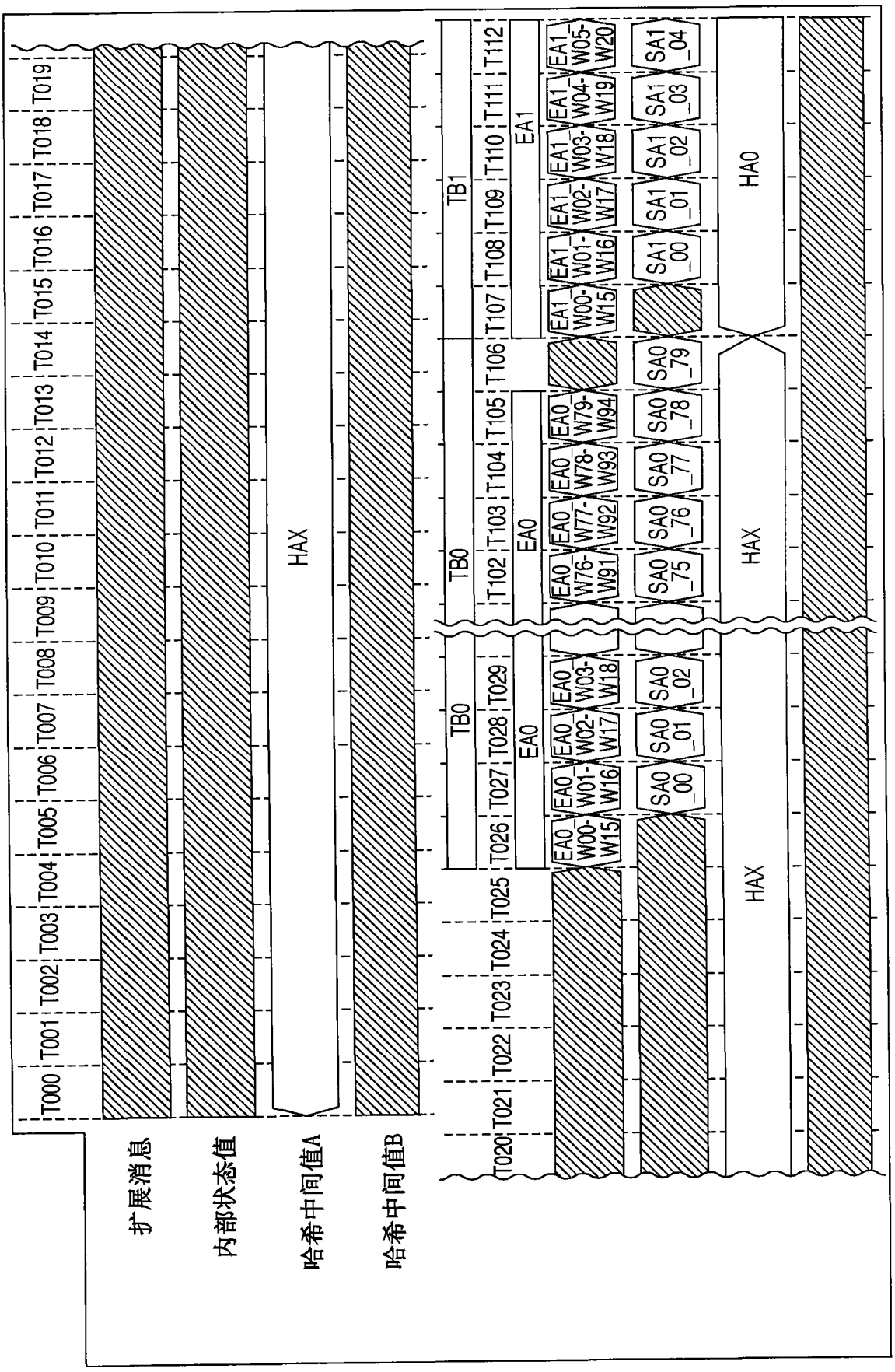

T000
T001
T002
T003
T004
T005
T006
T007
T008
T009
T010
T011
T012
T013
T014
T015
T016
T017
T018
T019
T020
T021
T022
T023
T024
T025
T026
T027
T028
T029
T102
T103
T104
T105
T106
T107
T108
T109
T110
T111
T112
扩展消息
内部状态值
哈希中间值A
哈希中间值B
HAX
TB0
TB1
EA0
EA1
HA0
SA0_00
SA0_01
SA0_02
SA0_75
SA0_76
SA0_77
SA0_78
SA0_79
SA1_00
SA1_01
SA1_02
SA1_03
SA1_04
EA0_W00-W15
EA0_W01-W16
EA0_W02-W17
EA0_W03-W18
EA0_W76-W91
EA0_W77-W92
EA0_W78-W93
EA0_W79-W94
EA1_W00-W15
EA1_W01-W16
EA1_W02-W17
EA1_W03-W18
EA1_W04-W19
EA1_W05-W20

图 8C

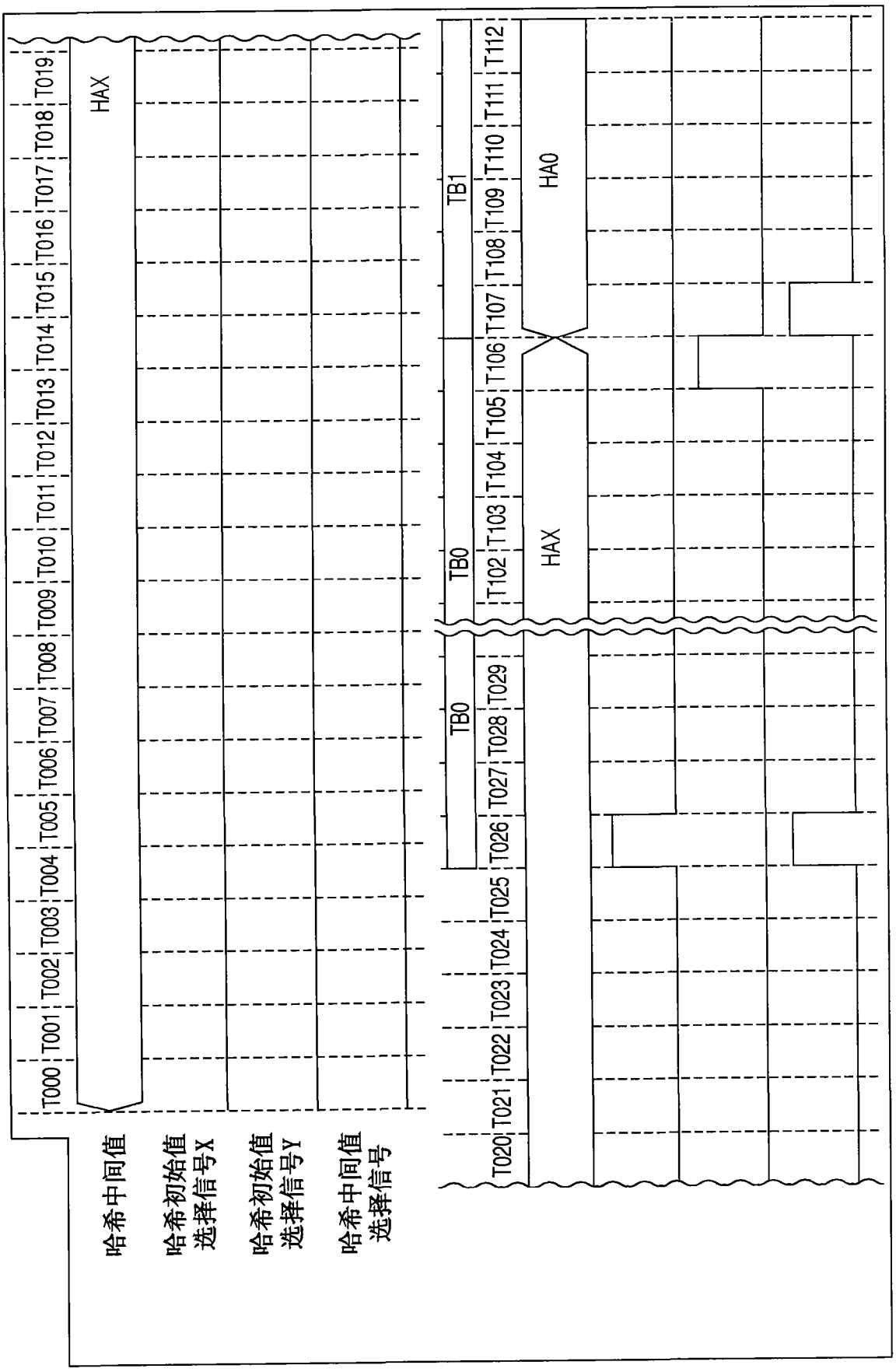

T000
T001
T002
T003
T004
T005
T006
T007
T008
T009
T010
T011
T012
T013
T014
T015
T016
T017
T018
T019
HAX
T020
T021
T022
T023
T024
T025
T026
T027
T028
T029
TB0
T102
T103
T104
T105
T106
T107
T108
T109
T110
T111
T112
TB1
HA0
HAX
哈希中间值
哈希初始值选择信号X
哈希初始值选择信号Y
哈希中间值选择信号

图 8D

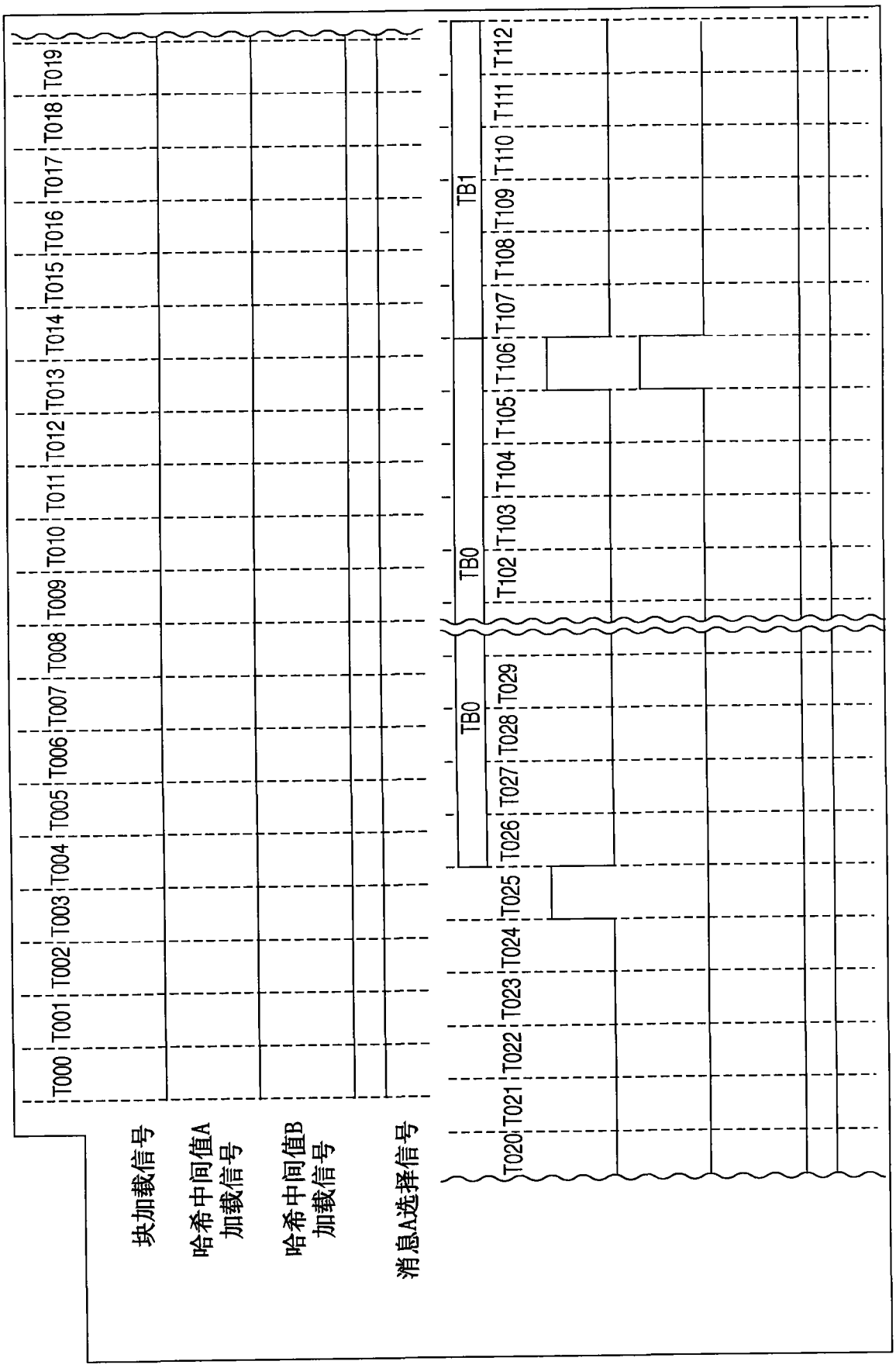

T000
T001
T002
T003
T004
T005
T006
T007
T008
T009
T010
T011
T012
T013
T014
T015
T016
T017
T018
T019
T020
T021
T022
T023
T024
T025
T026
T027
T028
T029
T102
T103
T104
T105
T106
T107
T108
T109
T110
T111
T112
TB0
TB0
TB1
块加载信号
哈希中间值A
加载信号
哈希中间值B
加载信号
消息A选择信号

图 8E

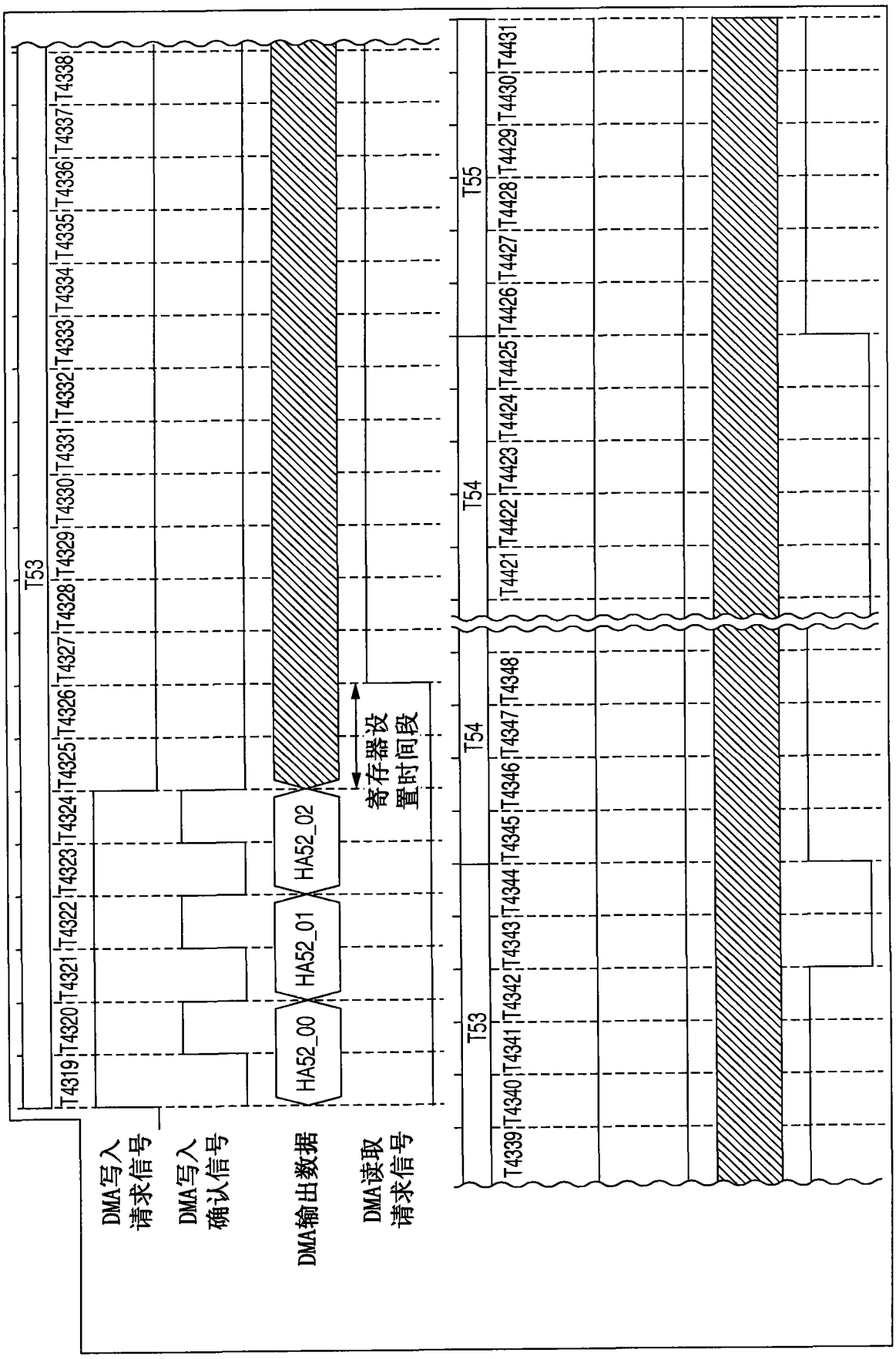

T53
T54
T55
T4319 T4320 T4321 T4322 T4323 T4324 T4325 T4326 T4327 T4328 T4329 T4330 T4331 T4332 T4333 T4334 T4335 T4336 T4337 T4338
T4339 T4340 T4341 T4342 T4343 T4344 T4345 T4346 T4347 T4348
T4421 T4422 T4423 T4424 T4425 T4426 T4427 T4428 T4429 T4430 T4431
HA52_00
HA52_01
HA52_02
寄存器设置时间段
DMA写入请求信号
DMA写入确认信号
DMA输出数据
DMA读取请求信号

图 9A

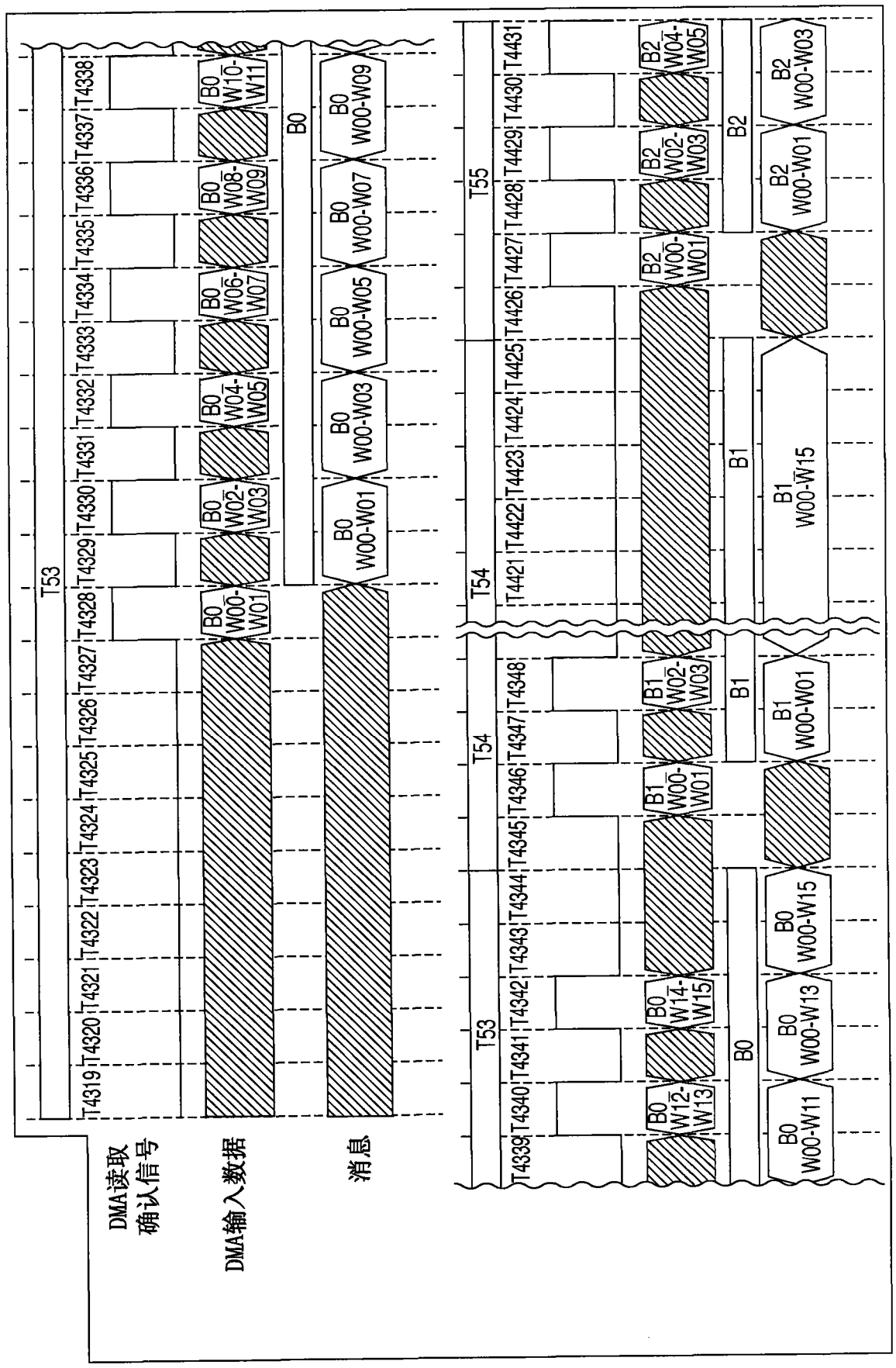

DMA读取确认信号
DMA输入数据
消息
T53
T54
T55
T4319 T4320 T4321 T4322 T4323 T4324 T4325 T4326 T4327 T4328 T4329 T4330 T4331 T4332 T4333 T4334 T4335 T4336 T4337 T4338
T4339 T4340 T4341 T4342 T4343 T4344 T4345 T4346 T4347 T4348
T4421 T4422 T4423 T4424 T4425 T4426 T4427 T4428 T4429 T4430 T4431
B0 W00-W01
B0 W02-W03
B0 W04-W05
B0 W06-W07
B0 W08-W09
B0 W10-W11
B0 W12-W13
B0 W14-W15
B0 W00-W01
B0 W00-W03
B0 W00-W05
B0 W00-W07
B0 W00-W09
B0 W00-W11
B0 W00-W13
B0 W00-W15
B1 W00-W01
B1 W02-W03
B1 W00-W15
B2 W00-W01
B2 W02-W03
B2 W04-W05
B2 W00-W03

图 9B

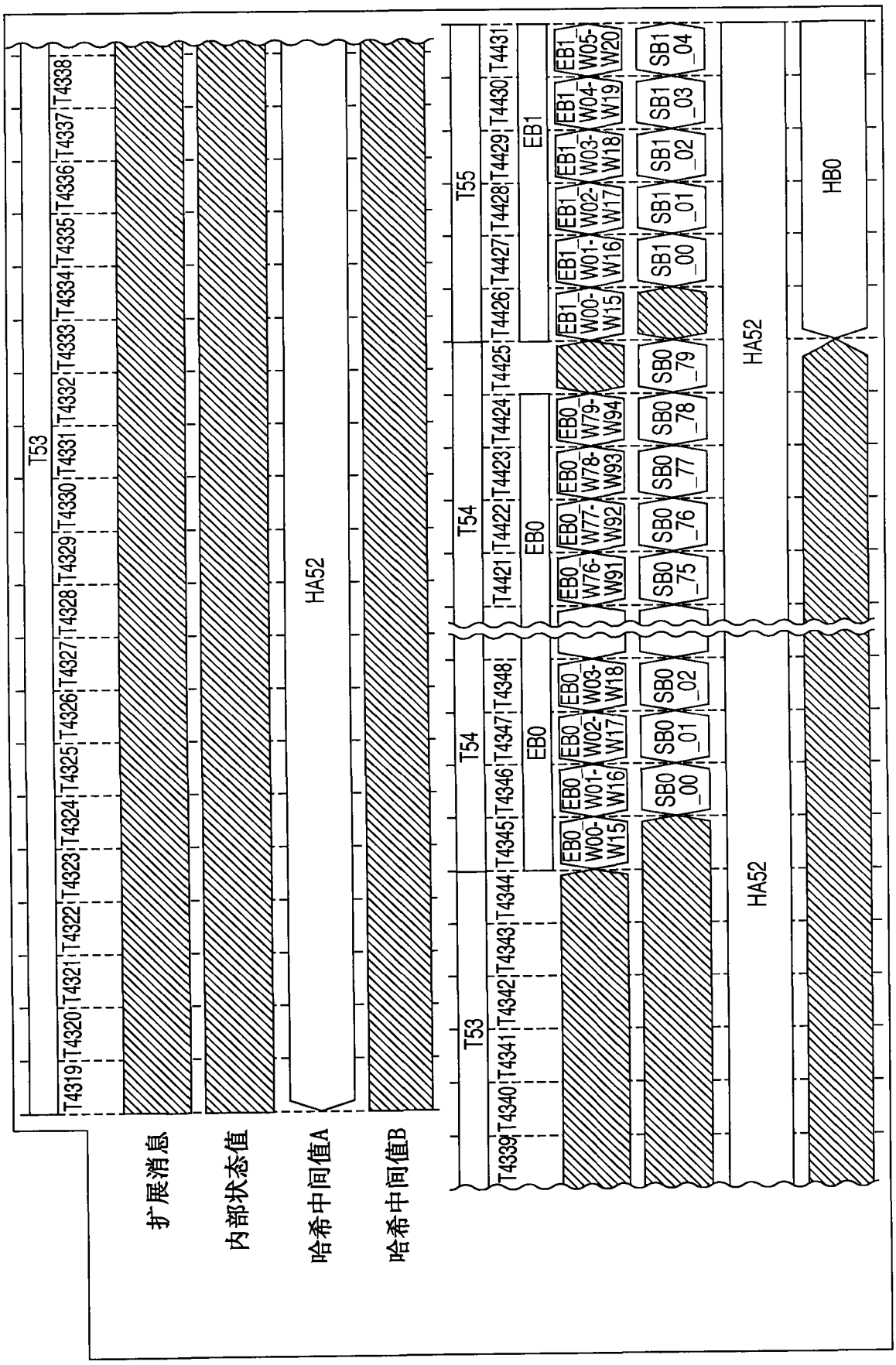

T53
T4319 T4320 T4321 T4322 T4323 T4324 T4325 T4326 T4327 T4328 T4329 T4330 T4331 T4332 T4333 T4334 T4335 T4336 T4337 T4338
扩展消息
内部状态值
HA52
哈希中间值A
哈希中间值B
T53
T4339 T4340 T4341 T4342 T4343 T4344 T4345 T4346 T4347 T4348
T54
T4421 T4422 T4423 T4424 T4425 T4426 T4427 T4428 T4429 T4430 T4431
T55
EB0
EB1
EB0_W00-W15
EB0_W01-W16
EB0_W02-W17
EB0_W03-W18
EB0_W76-W91
EB0_W77-W92
EB0_W78-W93
EB0_W79-W94
EB1_W00-W15
EB1_W01-W16
EB1_W02-W17
EB1_W03-W18
EB1_W04-W19
EB1_W05-W20
SB0_00
SB0_01
SB0_02
SB0_75
SB0_76
SB0_77
SB0_78
SB0_79
SB1_00
SB1_01
SB1_02
SB1_03
SB1_04
HA52
HA52
HB0

图 9C

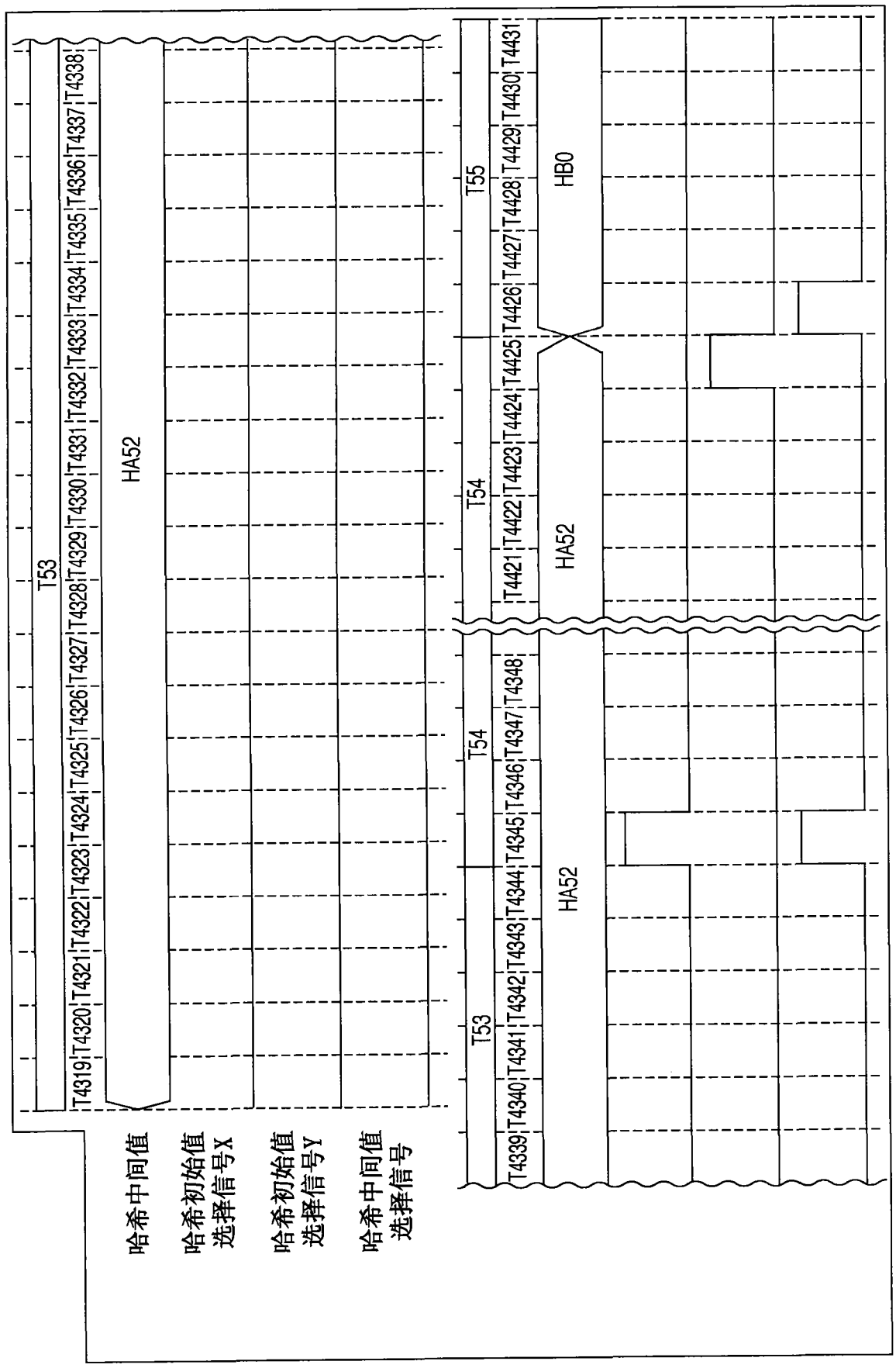

T53
T4319 T4320 T4321 T4322 T4323 T4324 T4325 T4326 T4327 T4328 T4329 T4330 T4331 T4332 T4333 T4334 T4335 T4336 T4337 T4338
HA52
哈希中间值
哈希初始值选择信号X
哈希初始值选择信号Y
哈希中间值选择信号
T53
T4339 T4340 T4341 T4342 T4343 T4344 T4345 T4346 T4347 T4348
T54
HA52
T54
T4421 T4422 T4423 T4424 T4425 T4426 T4427 T4428 T4429 T4430 T4431
HA52
T55
HB0

图 9D

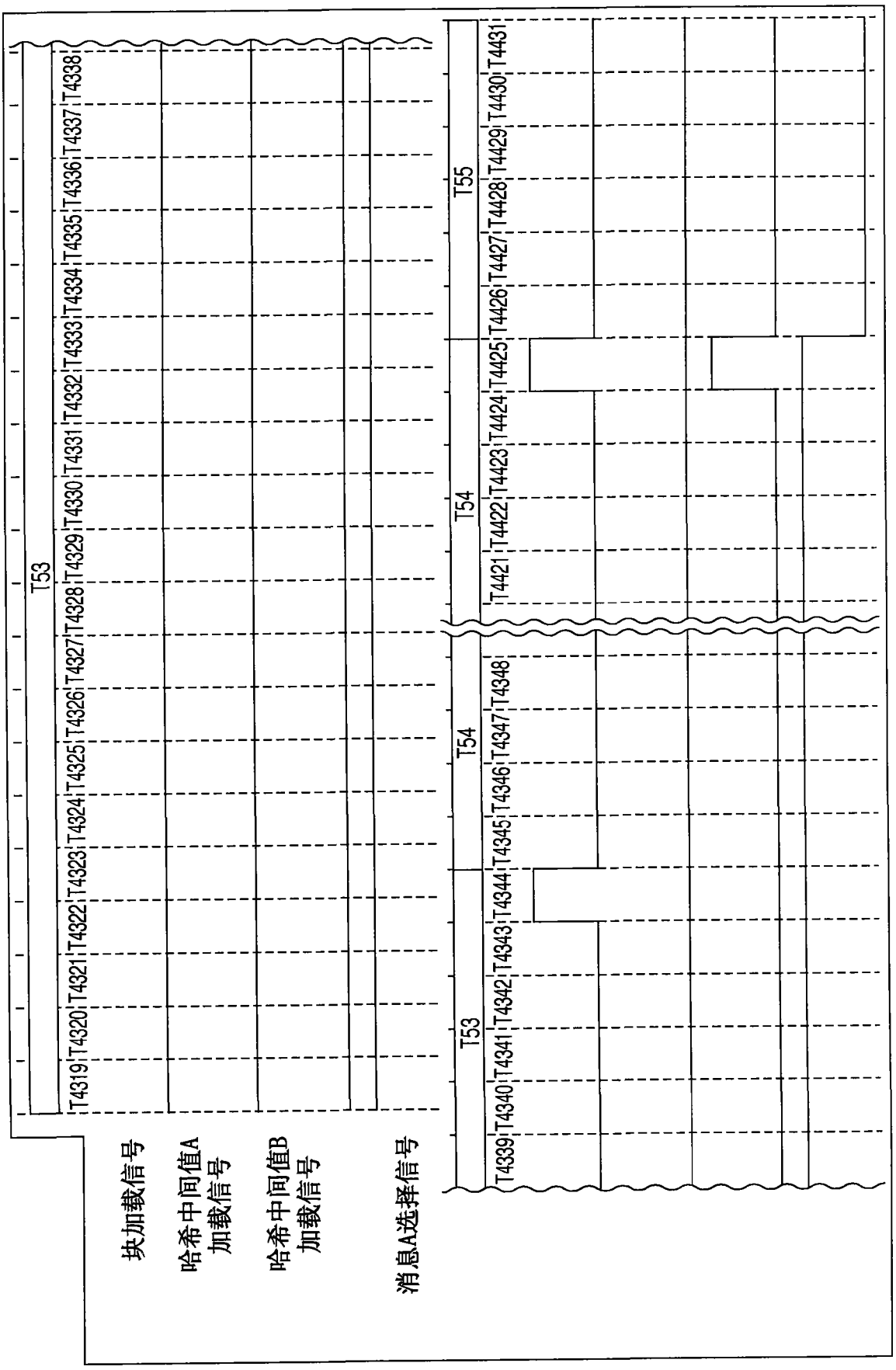

块加载信号
哈希中间值A
加载信号
哈希中间值B
加载信号
消息A选择信号
T53
T54
T55
T4319 T4320 T4321 T4322 T4323 T4324 T4325 T4326 T4327 T4328 T4329 T4330 T4331 T4332 T4333 T4334 T4335 T4336 T4337 T4338
T4339 T4340 T4341 T4342 T4343 T4344 T4345 T4346 T4347 T4348
T4421 T4422 T4423 T4424 T4425 T4426 T4427 T4428 T4429 T4430 T4431

图 9E

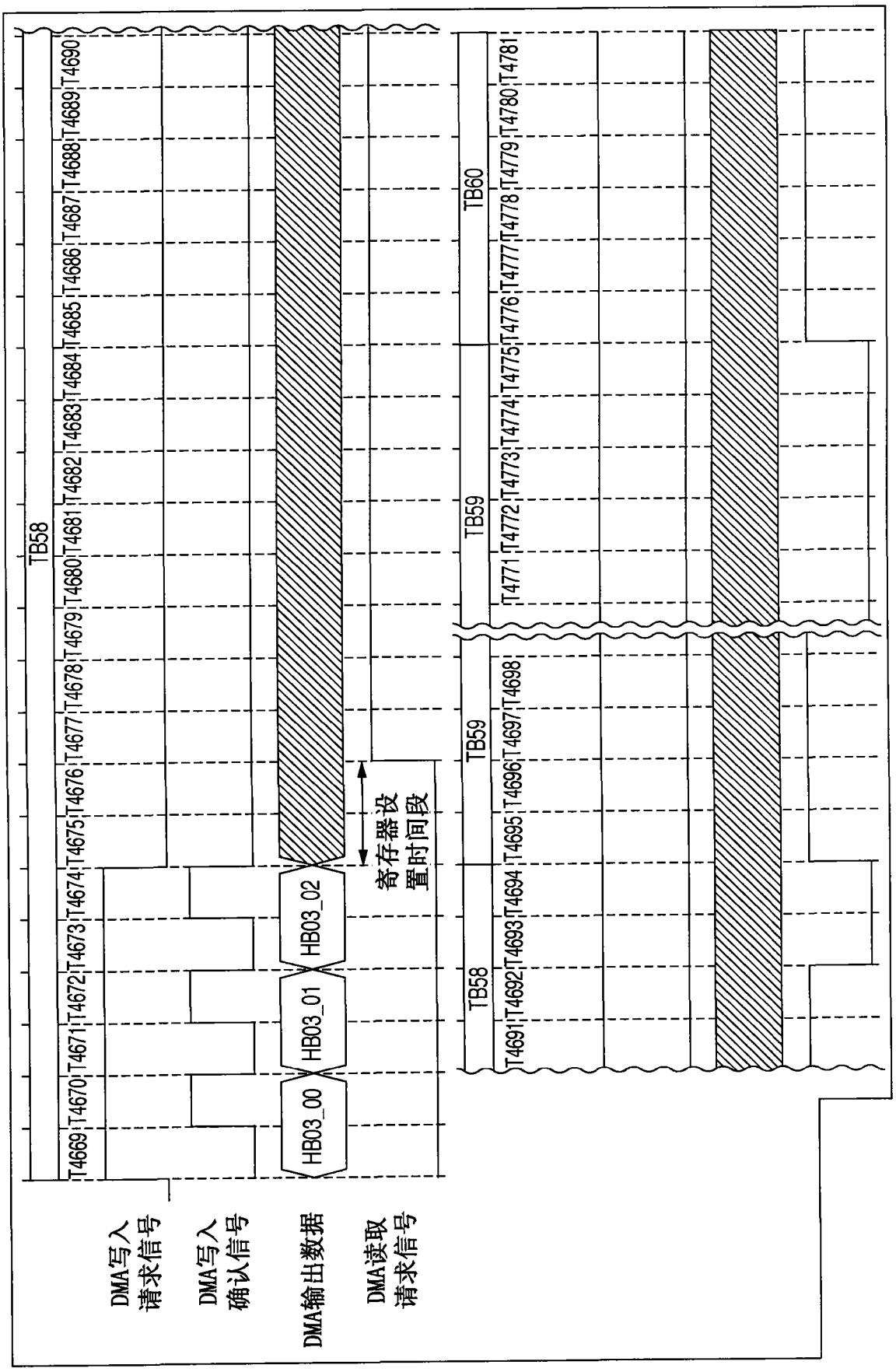

TB58
TB59
TB60
T4669
T4670
T4671
T4672
T4673
T4674
T4675
T4676
T4677
T4678
T4679
T4680
T4681
T4682
T4683
T4684
T4685
T4686
T4687
T4688
T4689
T4690
T4691
T4692
T4693
T4694
T4695
T4696
T4697
T4698
T4771
T4772
T4773
T4774
T4775
T4776
T4777
T4778
T4779
T4780
T4781
HB03_00
HB03_01
HB03_02
寄存器设置时间段
DMA写入请求信号
DMA写入确认信号
DMA输出数据
DMA读取请求信号

图 10A

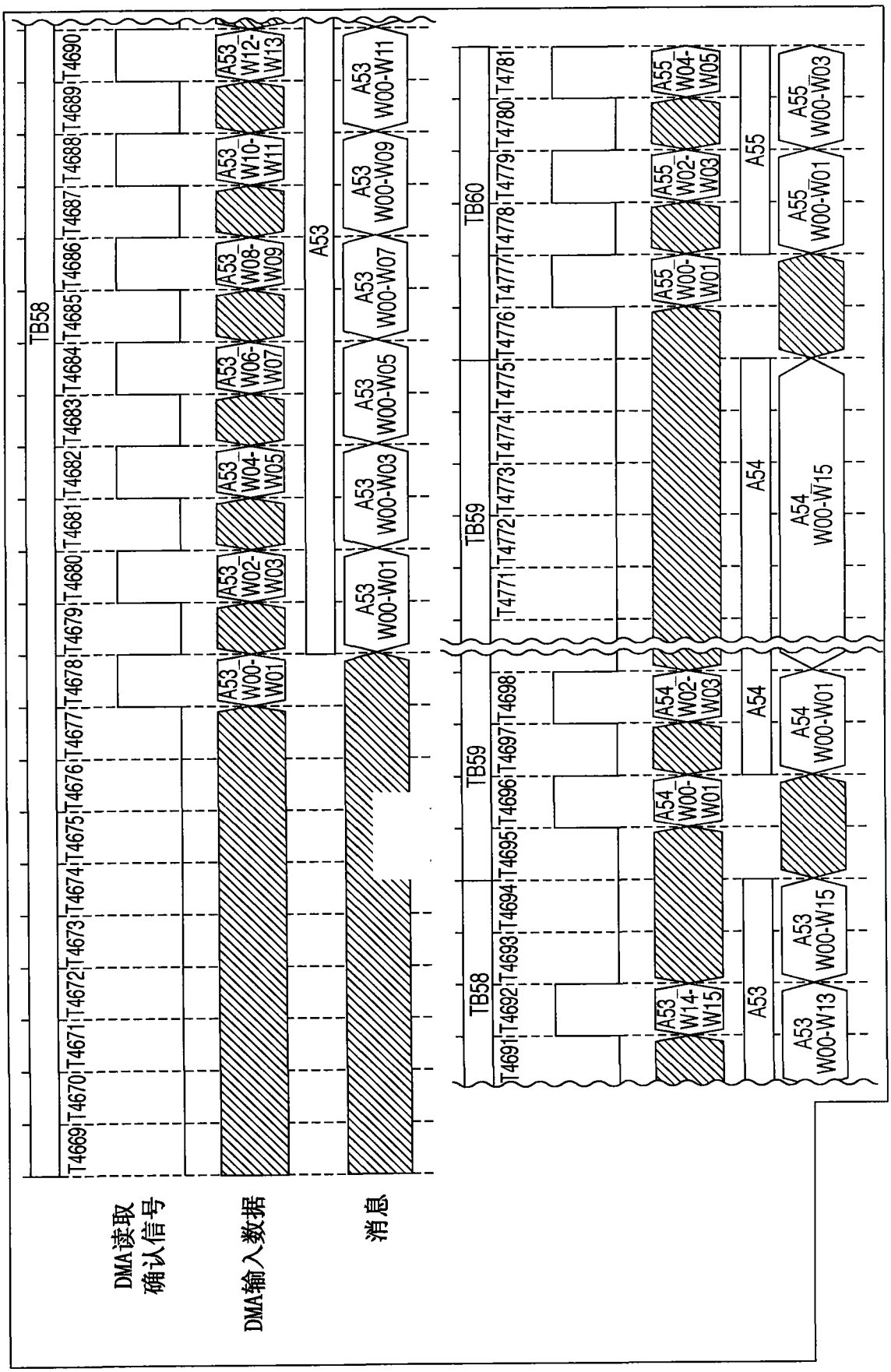

DMA读取确认信号
DMA输入数据
消息
TB58
TB59
TB60
A53
A54
A55
A53_W00-W01
A53_W02-W03
A53_W04-W05
A53_W06-W07
A53_W08-W09
A53_W10-W11
A53_W12-W13
A53_W14-W15
A53_W00-W03
A53_W00-W05
A53_W00-W07
A53_W00-W09
A53_W00-W11
A53_W00-W13
A53_W00-W15
A54_W00-W01
A54_W02-W03
A54_W00-W15
A55_W00-W01
A55_W02-W03
A55_W04-W05
A55_W00-W03
T4669
T4670
T4671
T4672
T4673
T4674
T4675
T4676
T4677
T4678
T4679
T4680
T4681
T4682
T4683
T4684
T4685
T4686
T4687
T4688
T4689
T4690
T4691
T4692
T4693
T4694
T4695
T4696
T4697
T4698
T4771
T4772
T4773
T4774
T4775
T4776
T4777
T4778
T4779
T4780
T4781

图 10B

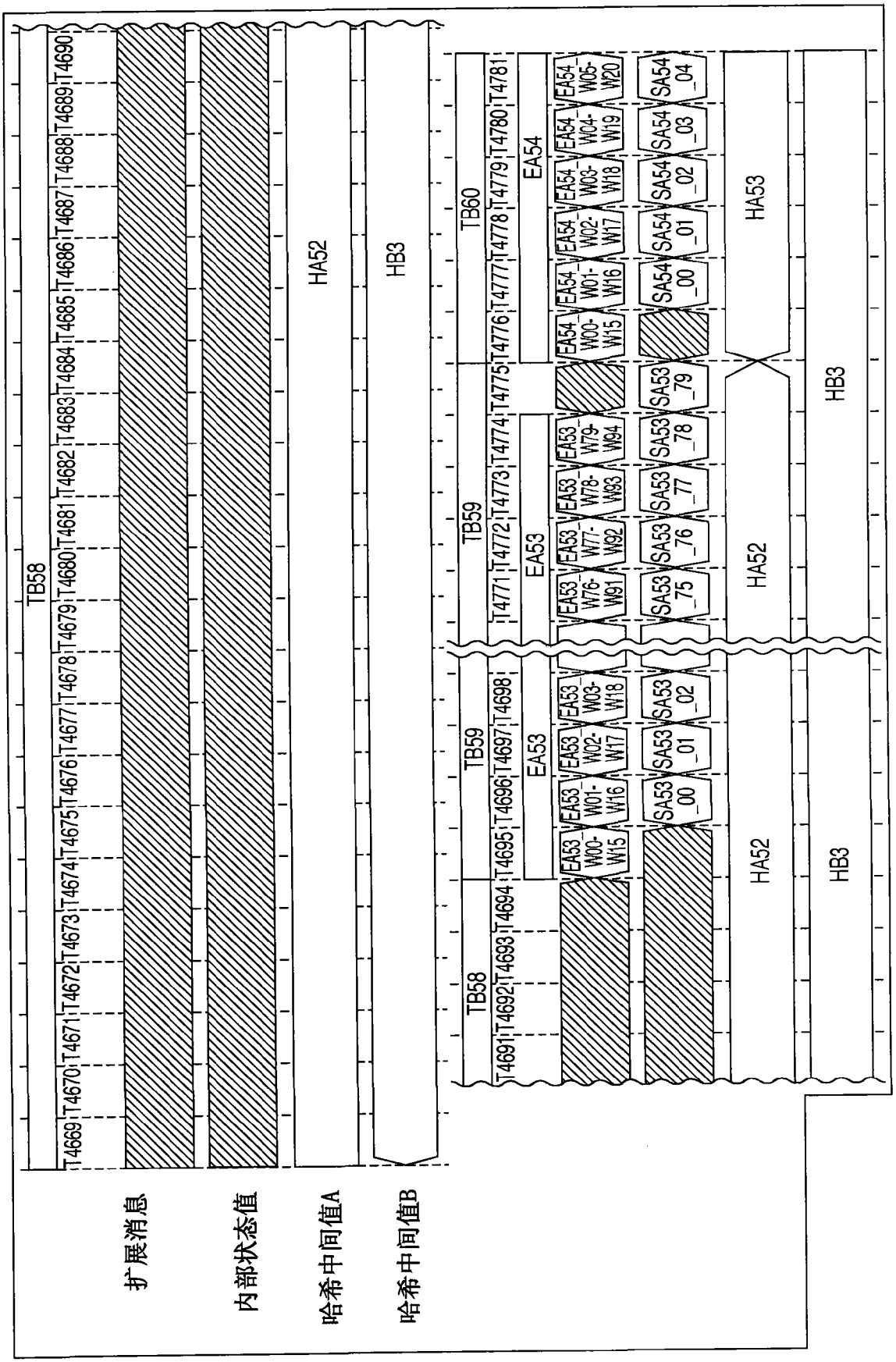

扩展消息
内部状态值
哈希中间值A
哈希中间值B
TB58
TB59
TB60
HA52
HB3
HA53
EA53
EA54
T4669 T4670 T4671 T4672 T4673 T4674 T4675 T4676 T4677 T4678 T4679 T4680 T4681 T4682 T4683 T4684 T4685 T4686 T4687 T4688 T4689 T4690
T4691 T4692 T4693 T4694 T4695 T4696 T4697 T4698 T4771 T4772 T4773 T4774 T4775 T4776 T4777 T4778 T4779 T4780 T4781
EA53_W00-W15
EA53_W01-W16
EA53_W02-W17
EA53_W03-W18
EA53_W76-W91
EA53_W77-W92
EA53_W78-W93
EA53_W79-W94
EA54_W00-W15
EA54_W01-W16
EA54_W02-W17
EA54_W03-W18
EA54_W04-W19
EA54_W05-W20
SA53_00
SA53_01
SA53_02
SA53_75
SA53_76
SA53_77
SA53_78
SA53_79
SA54_00
SA54_01
SA54_02
SA54_03
SA54_04

图 10C

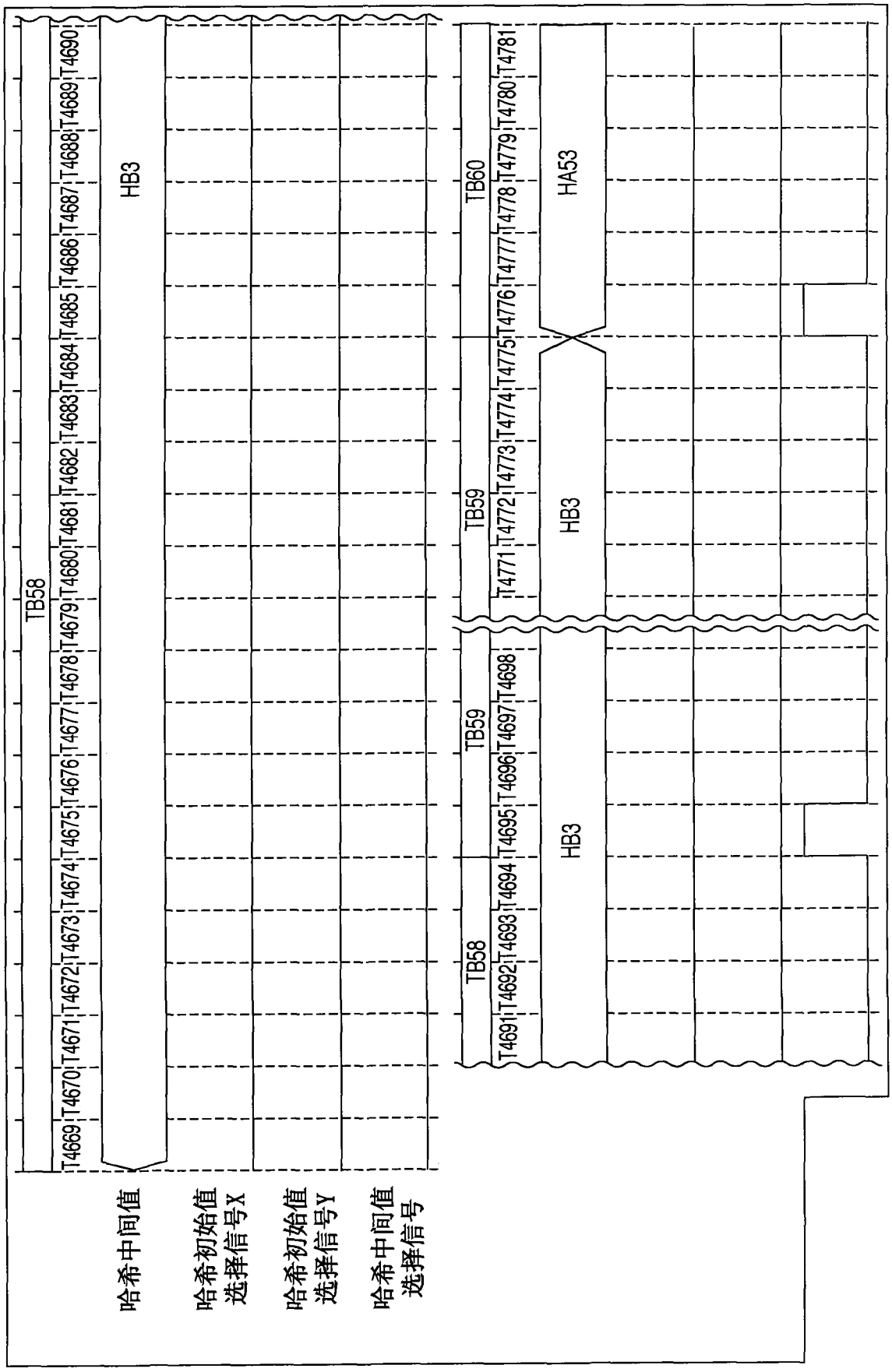

T4669
T4670
T4671
T4672
T4673
T4674
T4675
T4676
T4677
T4678
T4679
T4680
T4681
T4682
T4683
T4684
T4685
T4686
T4687
T4688
T4689
T4690
T4691
T4692
T4693
T4694
T4695
T4696
T4697
T4698
T4771
T4772
T4773
T4774
T4775
T4776
T4777
T4778
T4779
T4780
T4781
TB58
TB59
TB60
HB3
HA53
哈希中间值
哈希初始值选择信号X
哈希初始值选择信号Y
哈希中间值选择信号

图 10D

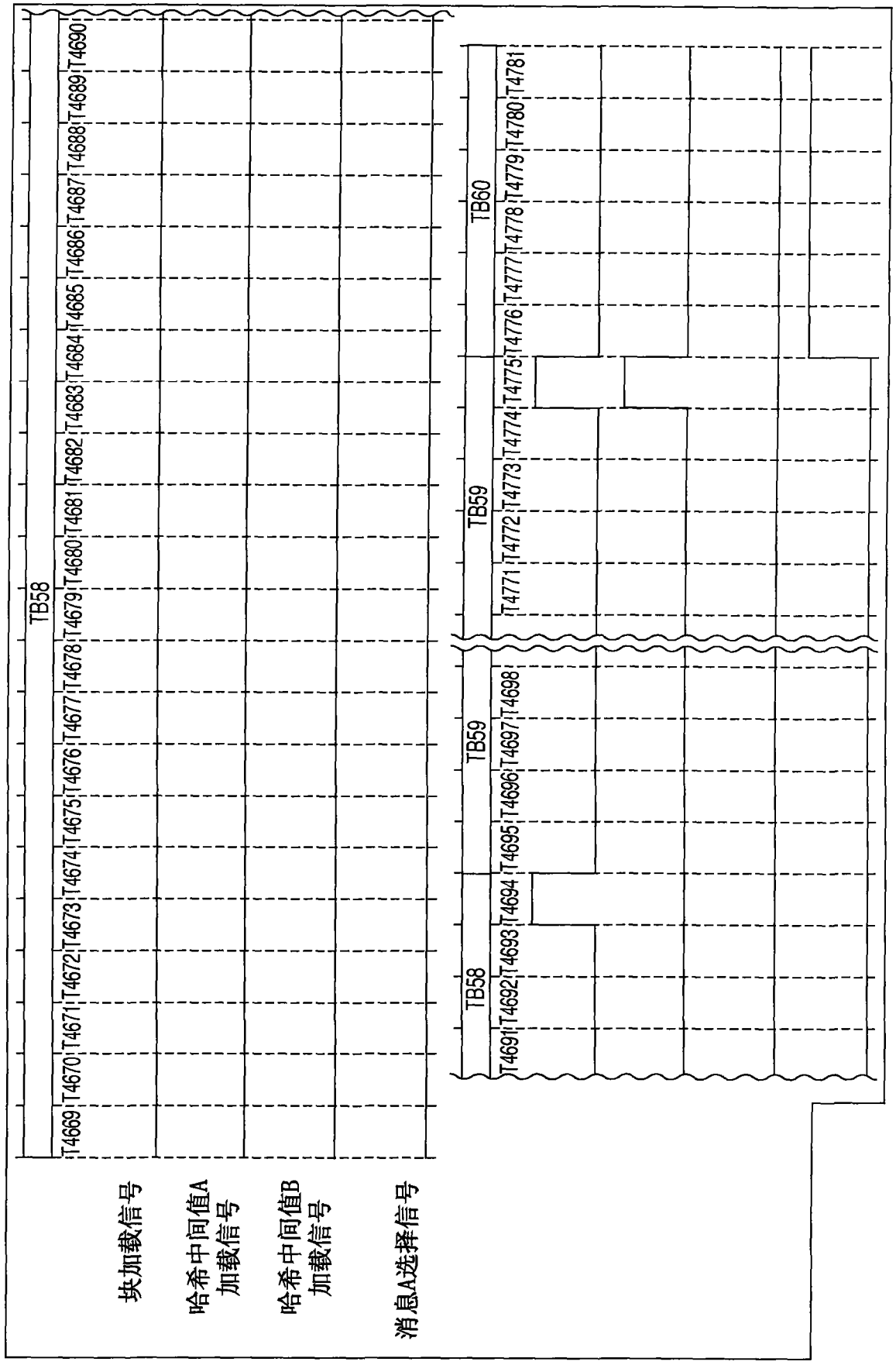

块加载信号
哈希中间值A
加载信号
哈希中间值B
加载信号
消息A选择信号
TB58
TB59
TB59
TB60
T4669 T4670 T4671 T4672 T4673 T4674 T4675 T4676 T4677 T4678 T4679 T4680 T4681 T4682 T4683 T4684 T4685 T4686 T4687 T4688 T4689 T4690
T4691 T4692 T4693 T4694 T4695 T4696 T4697 T4698
T4771 T4772 T4773 T4774 T4775 T4776 T4777 T4778 T4779 T4780 T4781

图 10E

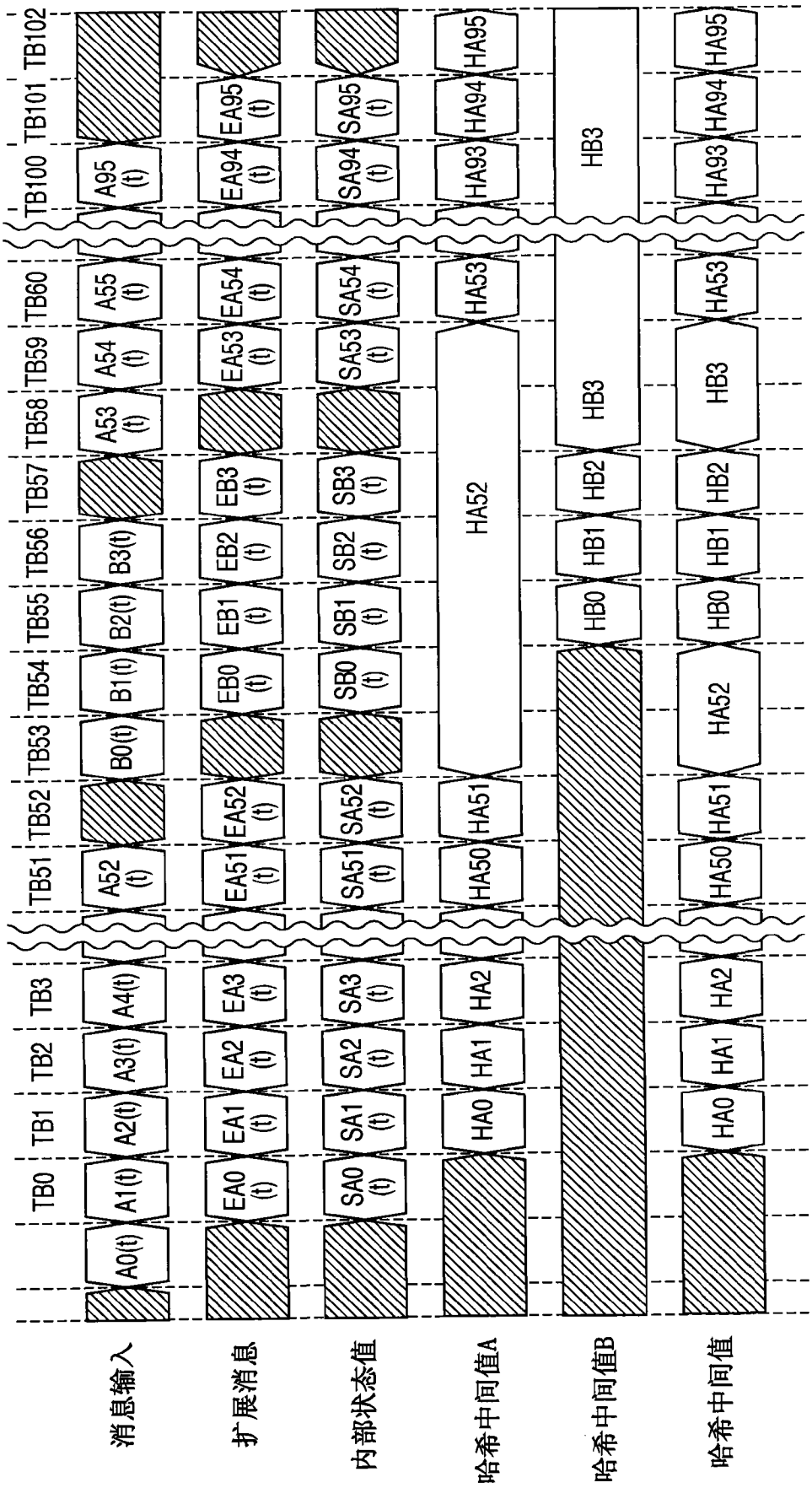

TB0
TB1
TB2
TB3
TB51
TB52
TB53
TB54
TB55
TB56
TB57
TB58
TB59
TB60
TB100
TB101
TB102
消息输入
扩展消息
内部状态值
哈希中间值A
哈希中间值B
哈希中间值
A0(t)
A1(t)
A2(t)
A3(t)
A4(t)
A52 (t)
B0(t)
B1(t)
B2(t)
B3(t)
A53 (t)
A54 (t)
A55 (t)
A95 (t)
EA0 (t)
EA1 (t)
EA2 (t)
EA3 (t)
EA51 (t)
EA52 (t)
EB0 (t)
EB1 (t)
EB2 (t)
EB3 (t)
EA53 (t)
EA54 (t)
EA94 (t)
EA95 (t)
SA0 (t)
SA1 (t)
SA2 (t)
SA3 (t)
SA51 (t)
SA52 (t)
SB0 (t)
SB1 (t)
SB2 (t)
SB3 (t)
SA53 (t)
SA54 (t)
SA94 (t)
SA95 (t)
HA0
HA1
HA2
HA50
HA51
HA52
HA53
HA93
HA94
HA95
HB0
HB1
HB2
HB3

图 11A

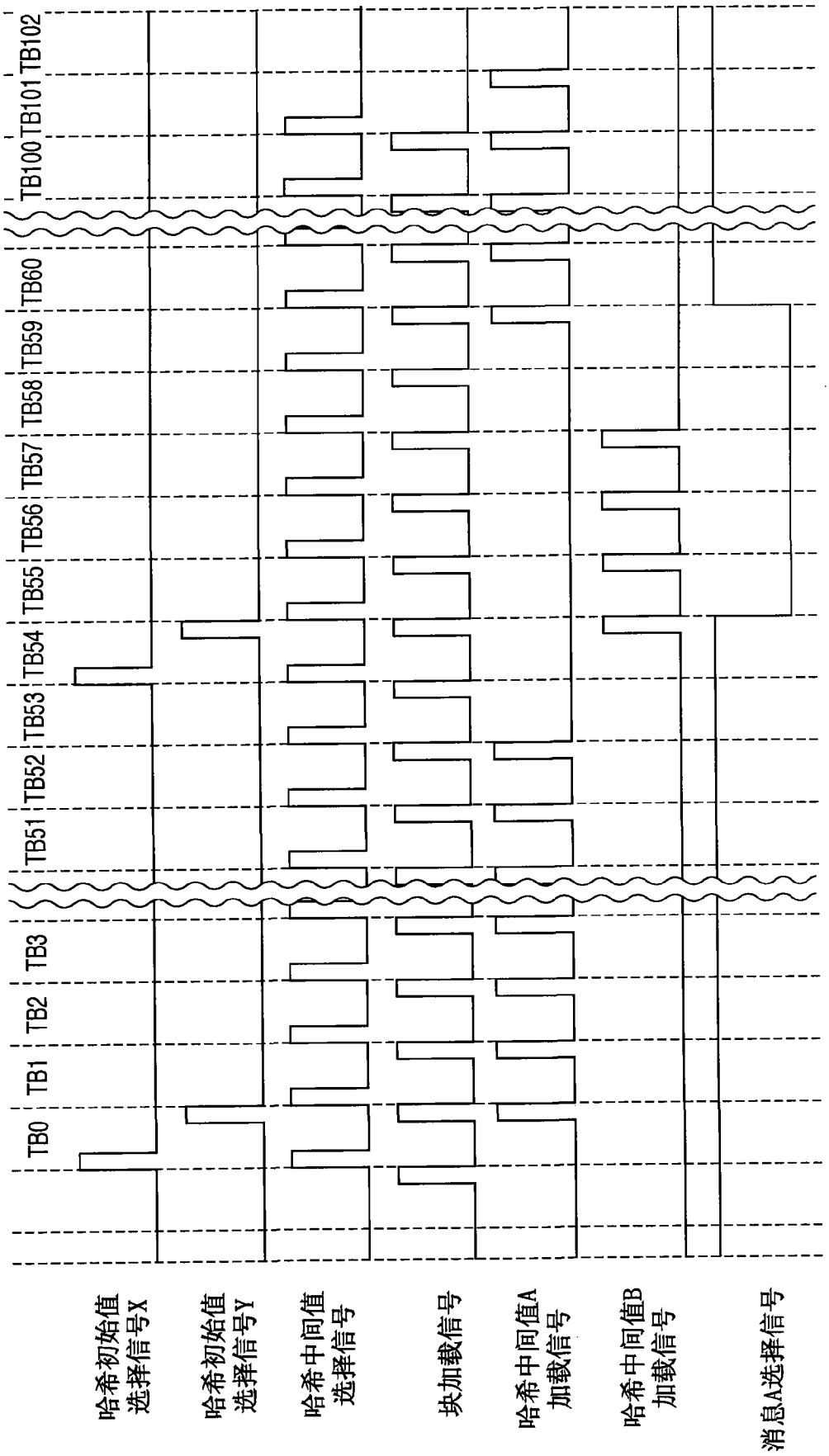

TB0
TB1
TB2
TB3
TB51
TB52
TB53
TB54
TB55
TB56
TB57
TB58
TB59
TB60
TB100
TB101
TB102
哈希初始值选择信号X
哈希初始值选择信号Y
哈希中间值选择信号
块加载信号
哈希中间值A加载信号
哈希中间值B加载信号
消息A选择信号

图 11B

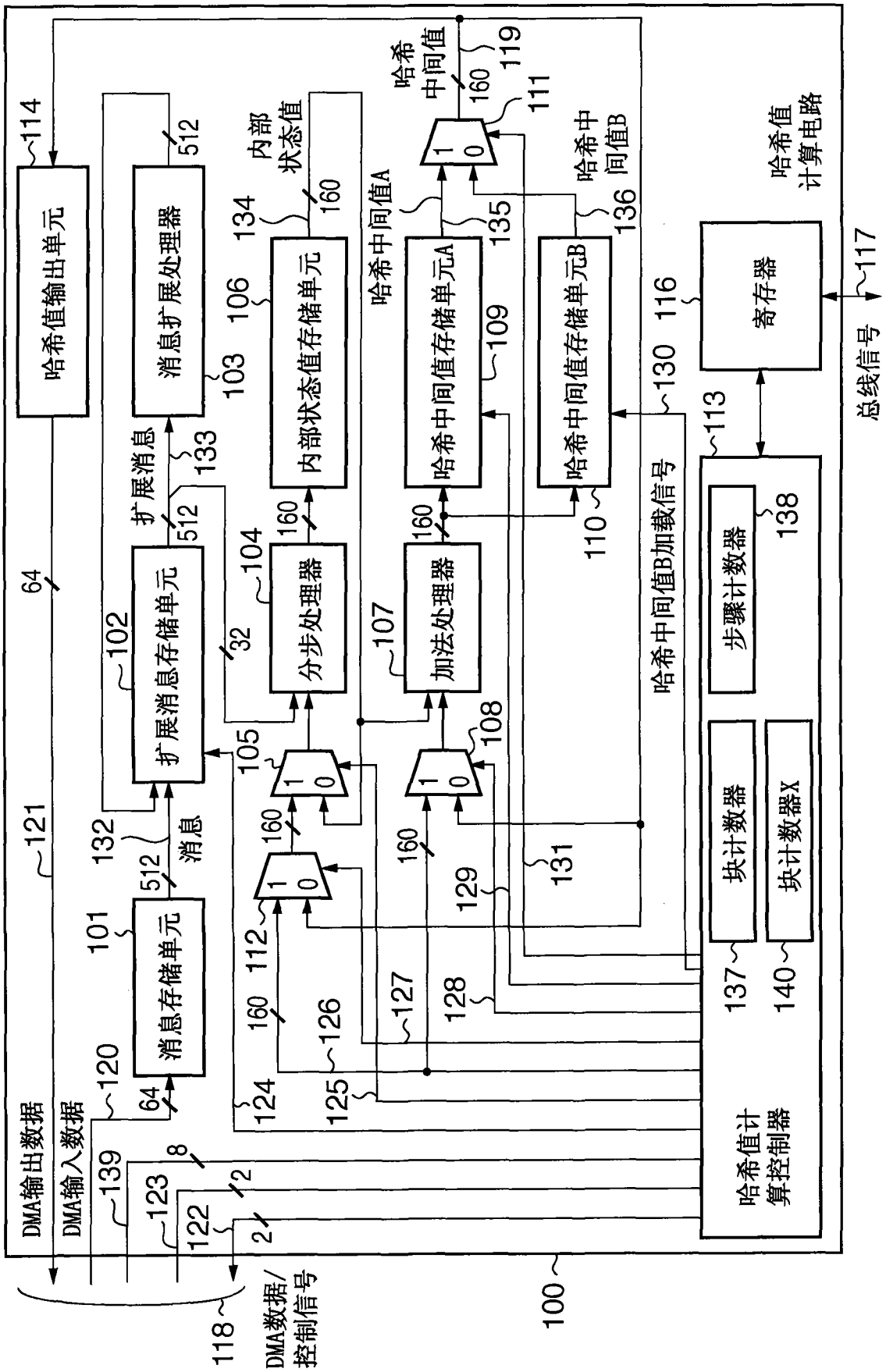

哈希值输出单元
114
消息扩展处理器
512
103
扩展消息
133
内部状态值
160
134
内部状态值存储单元
106
哈希中间值
160
119
111
哈希中间值A
135
哈希中间值存储单元A
109
哈希中间值B
136
哈希中间值存储单元B
110
哈希值计算电路
寄存器
116
117
总线信号
130
哈希中间值B加载信号
113
步骤计数器
138
块计数器
137
块计数器X
140
哈希值计算控制器
100
DMA输出数据
DMA输入数据
64
120
139
123
122
8
2
2
DMA数据/控制信号
118
121
64
扩展消息存储单元
512
101
消息
132
扩展消息存储单元
512
102
32
分步处理器
104
160
内部状态值存储单元
106
加法处理器
160
107
哈希中间值存储单元A
109
1
0
105
108
112
160
160
129
131
124
125
126
127
128
160

图 12

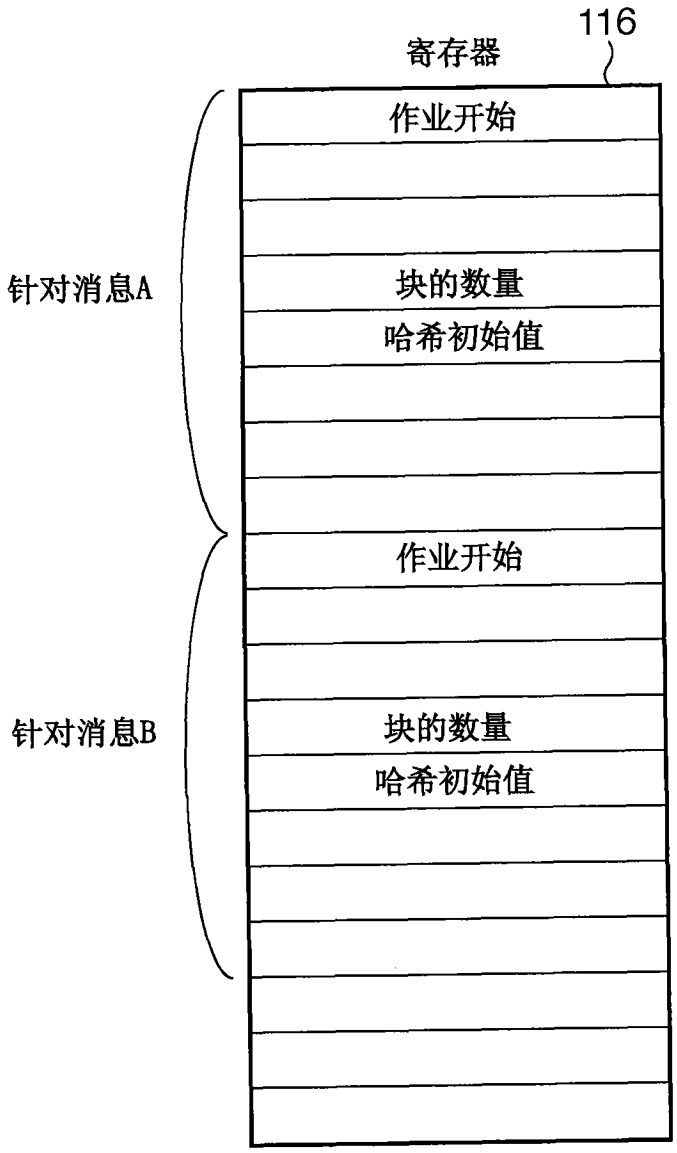


图 13

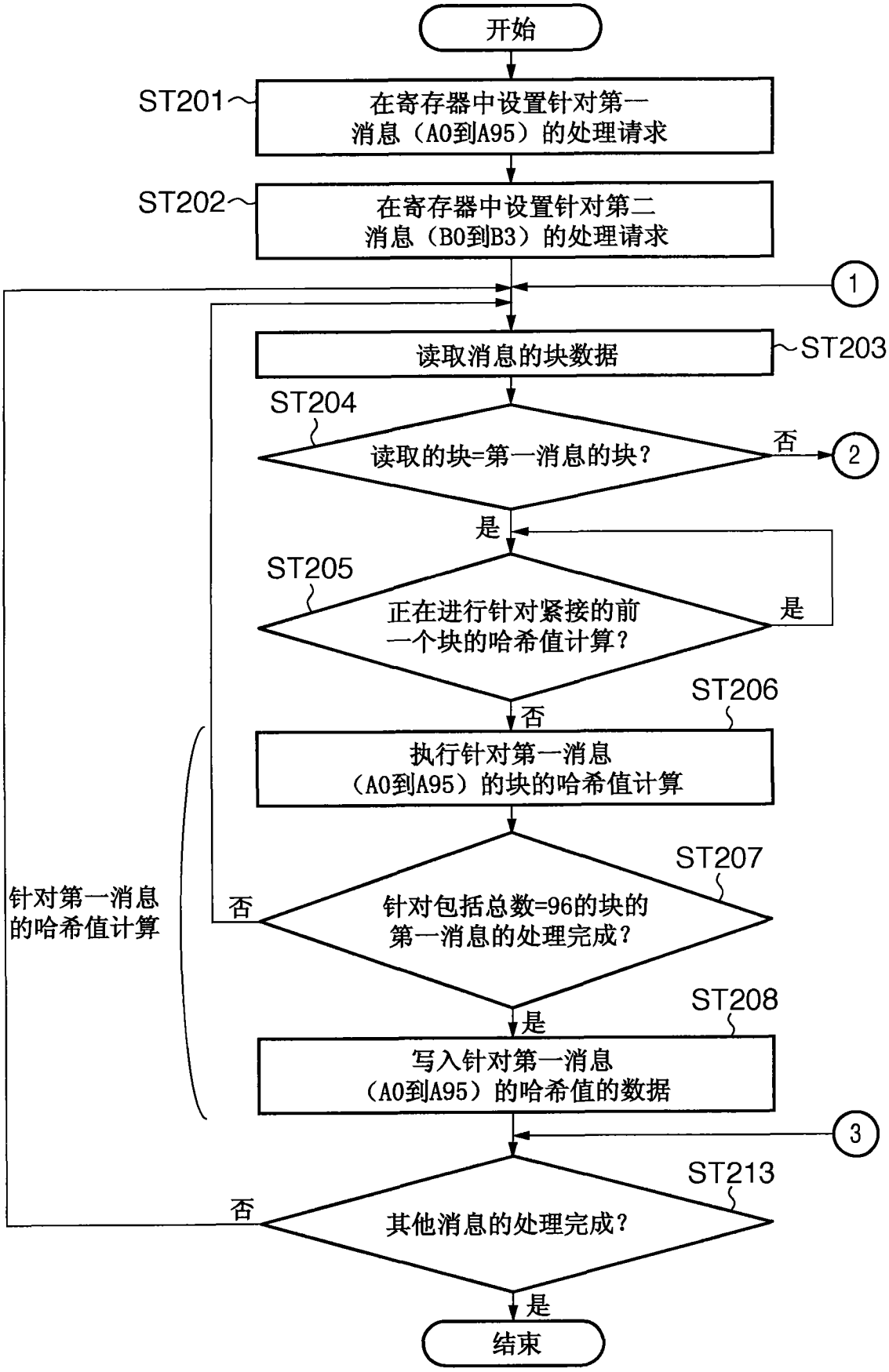

开始
ST201
在寄存器中设置针对第一消息（A0到A95）的处理请求
ST202
在寄存器中设置针对第二消息（B0到B3）的处理请求
1
读取消息的块数据
ST203
ST204
读取的块=第一消息的块？
否
2
是
ST205
正在进行针对紧接的前一个块的哈希值计算？
是
ST206
否
执行针对第一消息（A0到A95）的块的哈希值计算
ST207
针对包括总数=96的块的第一消息的处理完成？
否
针对第一消息的哈希值计算
ST208
是
写入针对第一消息（A0到A95）的哈希值的数据
3
ST213
其他消息的处理完成？
否
是
结束

图 14A

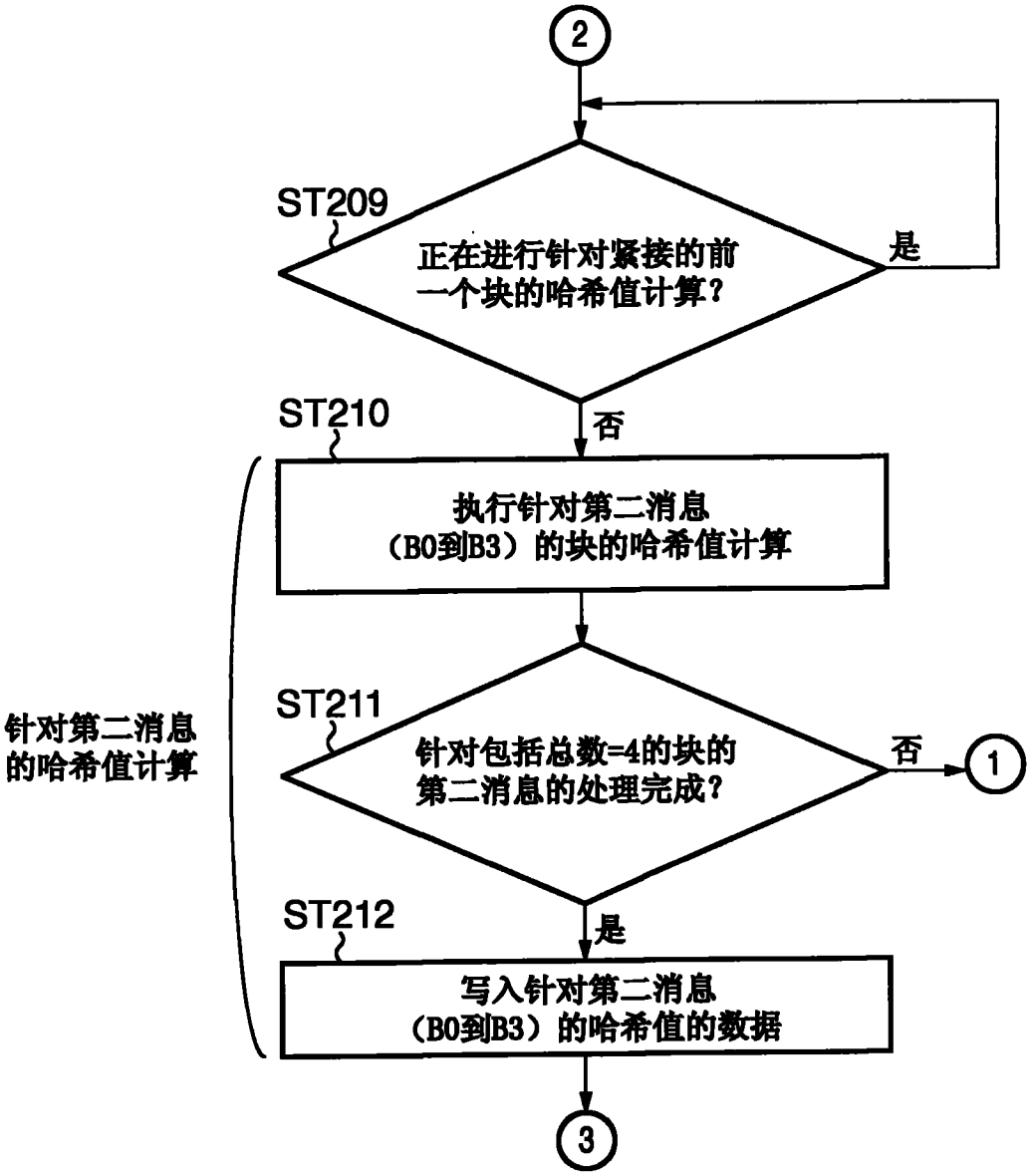

2
ST209
正在进行针对紧接的前一个块的哈希值计算？
是
否
ST210
执行针对第二消息（B0到B3）的块的哈希值计算
针对第二消息的哈希值计算
ST211
针对包括总数=4的块的第二消息的处理完成？
否
1
ST212
是
写入针对第二消息（B0到B3）的哈希值的数据
3

图 14B

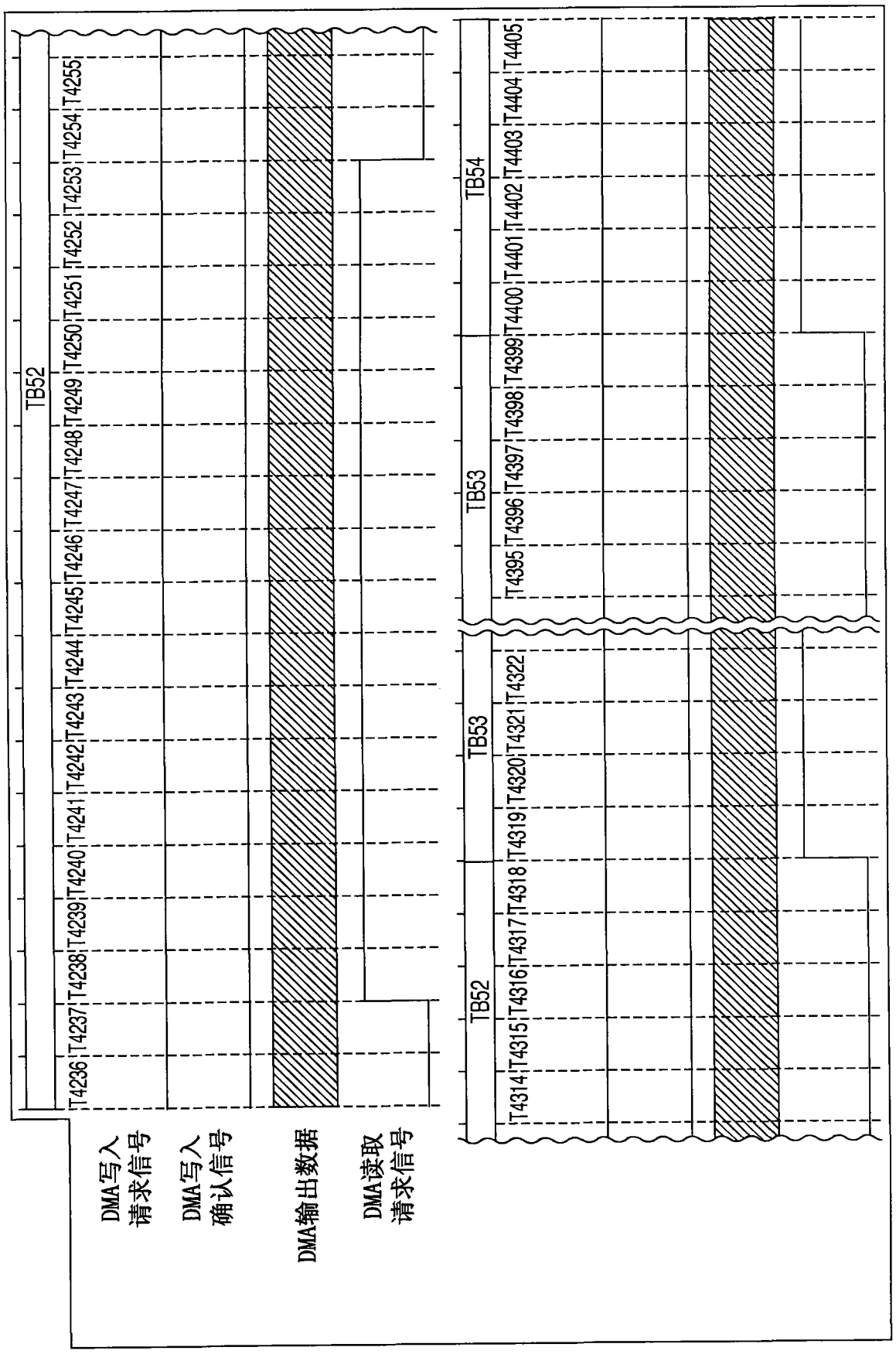

TB52
TB53
TB54
T4236 T4237 T4238 T4239 T4240 T4241 T4242 T4243 T4244 T4245 T4246 T4247 T4248 T4249 T4250 T4251 T4252 T4253 T4254 T4255
T4314 T4315 T4316 T4317 T4318 T4319 T4320 T4321 T4322
T4395 T4396 T4397 T4398 T4399 T4400 T4401 T4402 T4403 T4404 T4405
DMA写入请求信号
DMA写入确认信号
DMA输出数据
DMA读取请求信号

图 15A

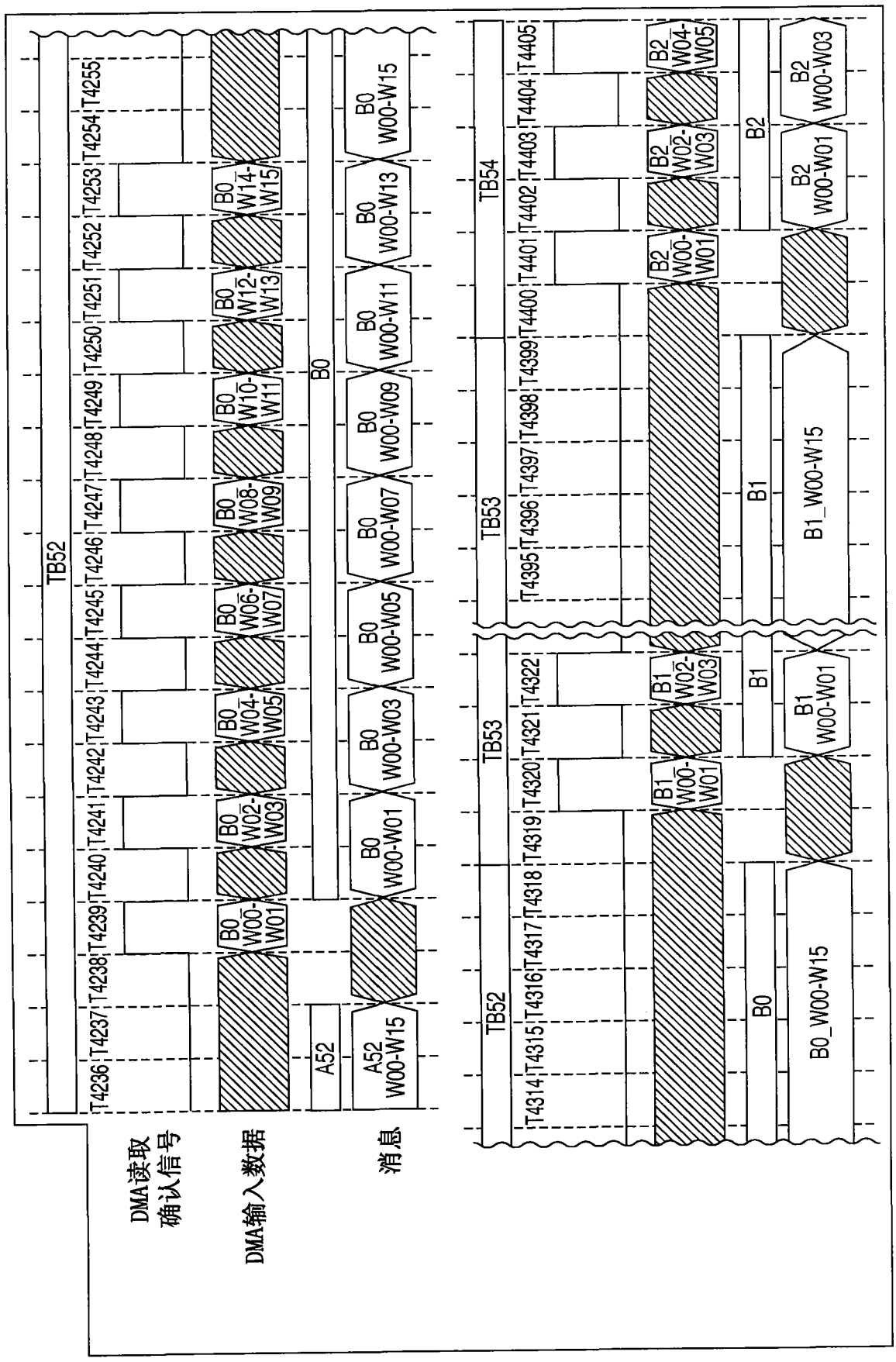

DMA读取确认信号
DMA输入数据
消息
TB52
TB53
TB54
A52
B0
B1
B2
B0_W00-W15
B1_W00-W15

图 15B

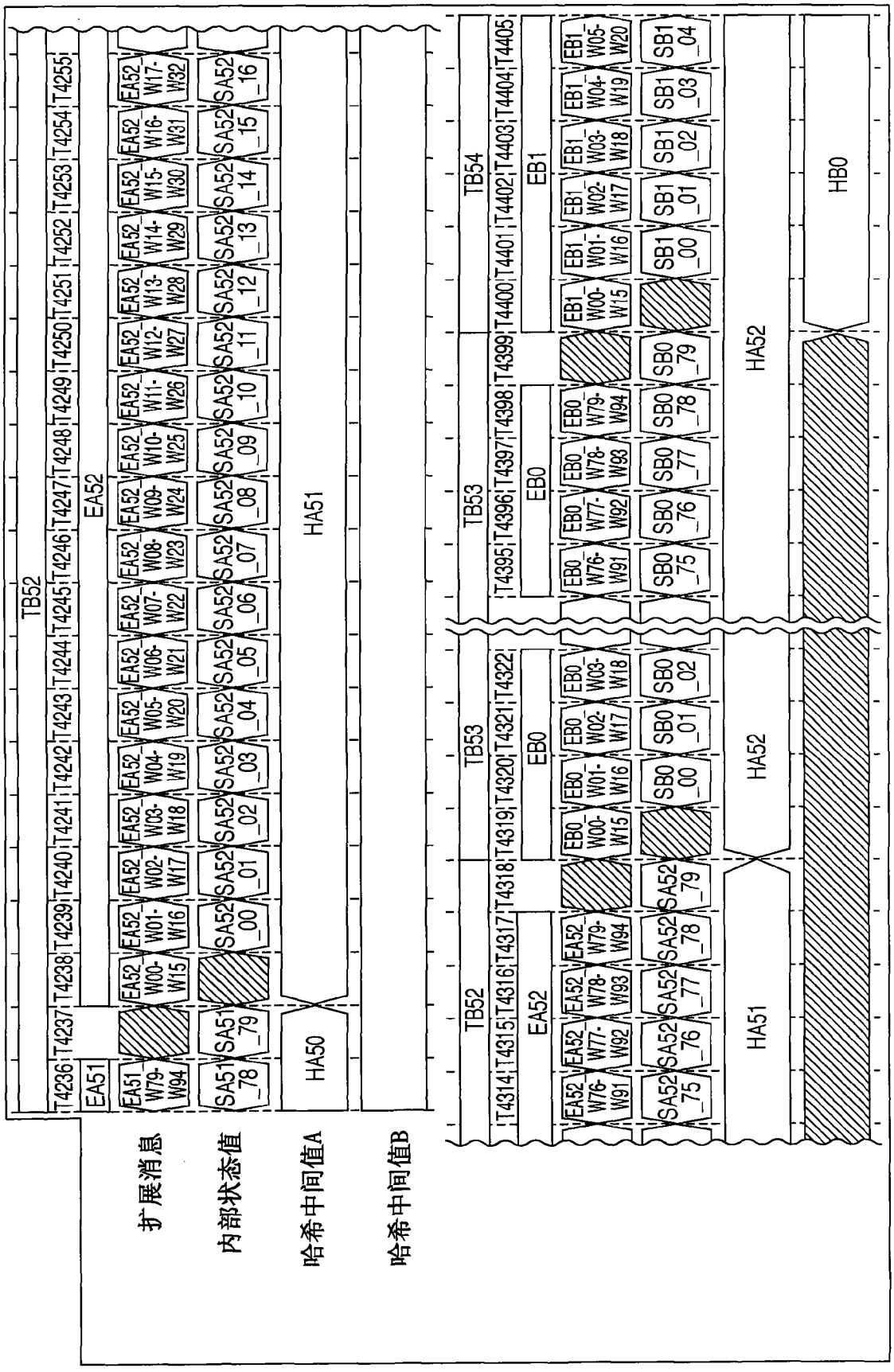

扩展消息
内部状态值
哈希中间值A
哈希中间值B
TB52
TB53
TB54
EA51
EA52
EB0
EB1
HA50
HA51
HA52
HB0
T4236
T4237
T4238
T4239
T4240
T4241
T4242
T4243
T4244
T4245
T4246
T4247
T4248
T4249
T4250
T4251
T4252
T4253
T4254
T4255
T4314
T4315
T4316
T4317
T4318
T4319
T4320
T4321
T4322
T4395
T4396
T4397
T4398
T4399
T4400
T4401
T4402
T4403
T4404
T4405

图 15C

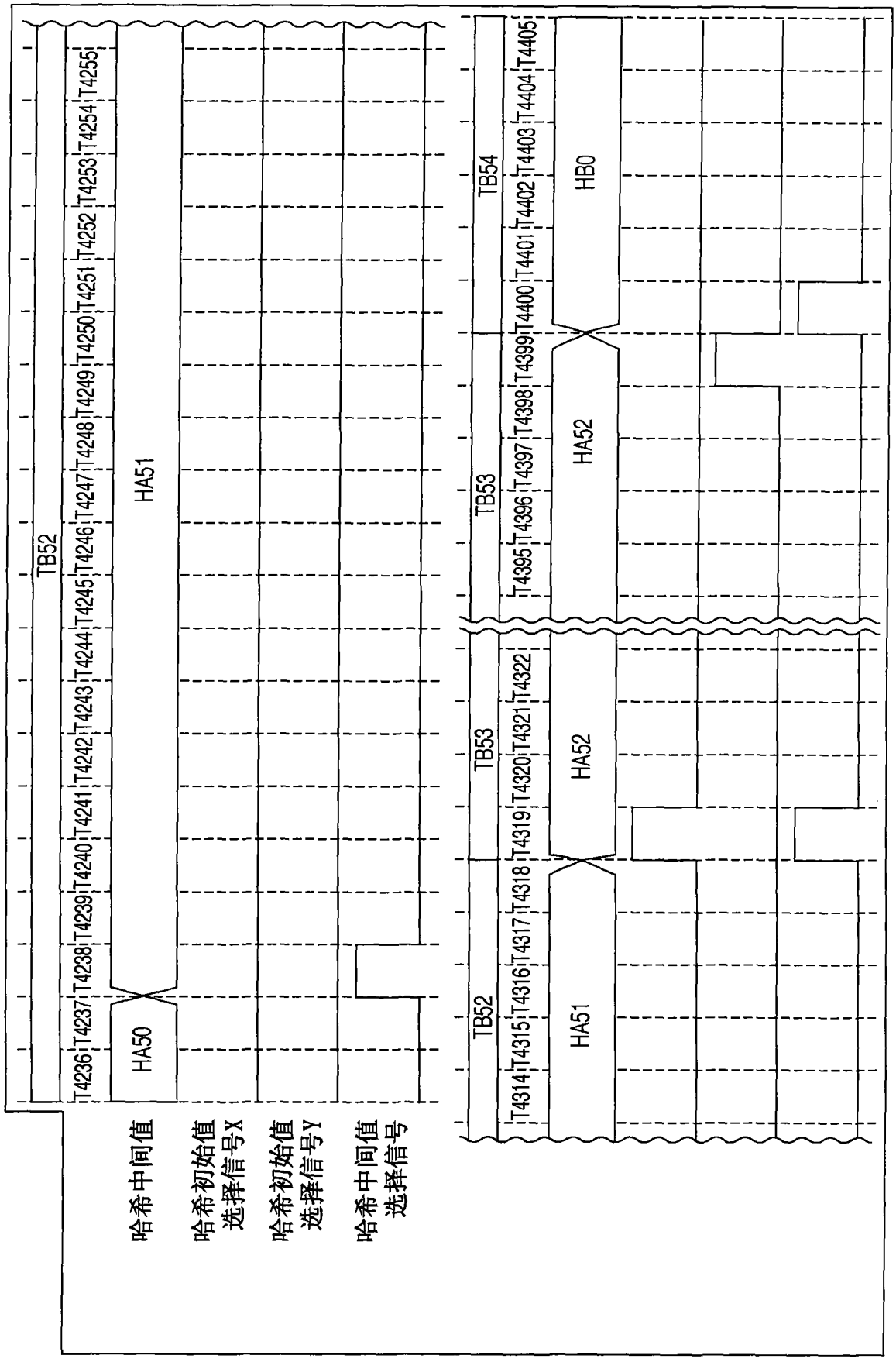

T4236
T4237
T4238
T4239
T4240
T4241
T4242
T4243
T4244
T4245
T4246
T4247
T4248
T4249
T4250
T4251
T4252
T4253
T4254
T4255
T4314
T4315
T4316
T4317
T4318
T4319
T4320
T4321
T4322
T4395
T4396
T4397
T4398
T4399
T4400
T4401
T4402
T4403
T4404
T4405
TB52
TB53
TB54
HA50
HA51
HA52
HB0
哈希中间值
哈希初始值选择信号X
哈希初始值选择信号Y
哈希中间值选择信号

图 15D

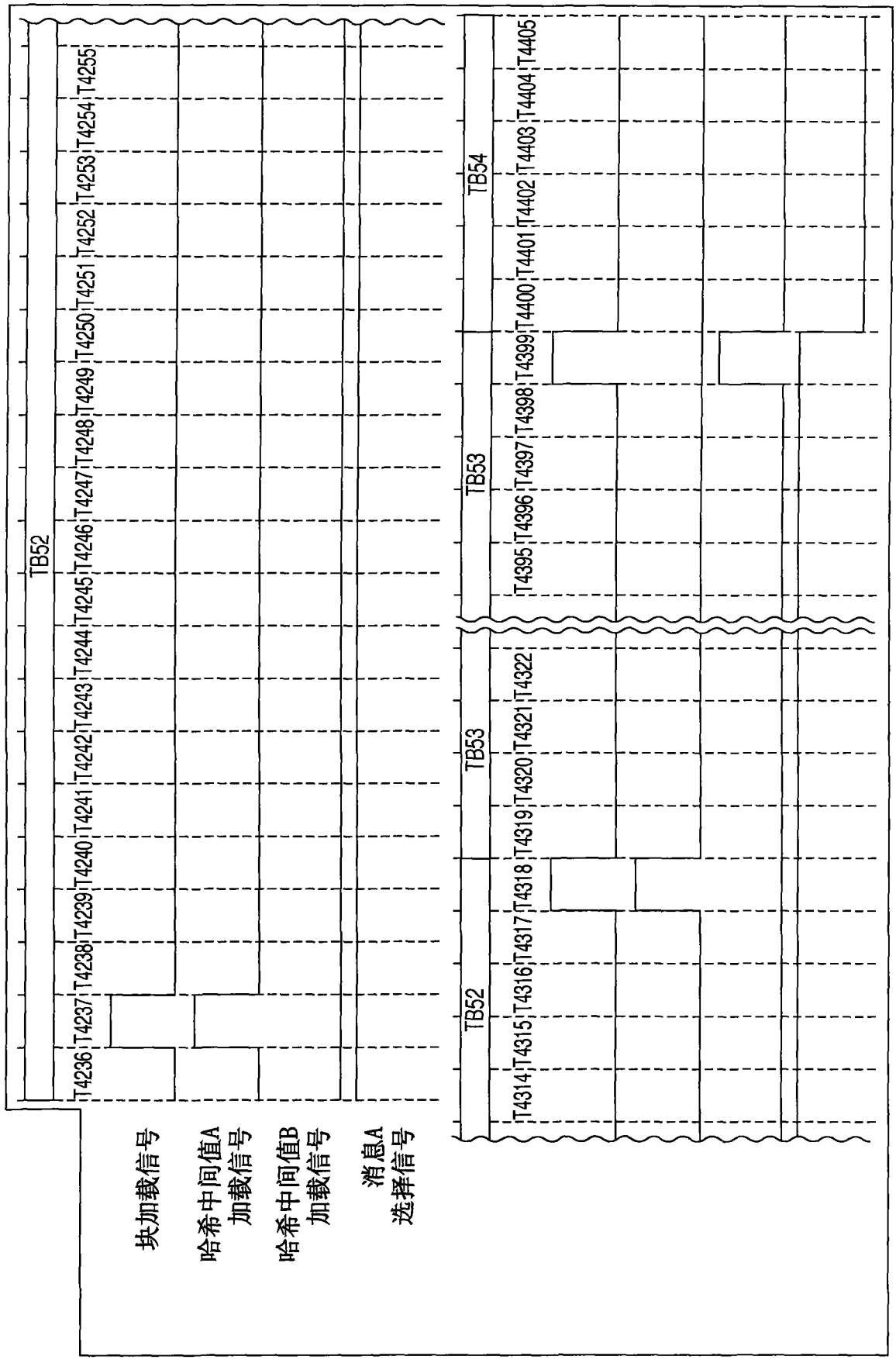

TB52
T4236 T4237 T4238 T4239 T4240 T4241 T4242 T4243 T4244 T4245 T4246 T4247 T4248 T4249 T4250 T4251 T4252 T4253 T4254 T4255
TB52
T4314 T4315 T4316 T4317 T4318 T4319 T4320 T4321 T4322
TB53
T4395 T4396 T4397 T4398 T4399 T4400 T4401 T4402 T4403 T4404 T4405
TB53
TB54
块加载信号
哈希中间值A
加载信号
哈希中间值B
加载信号
消息A
选择信号

图 15E

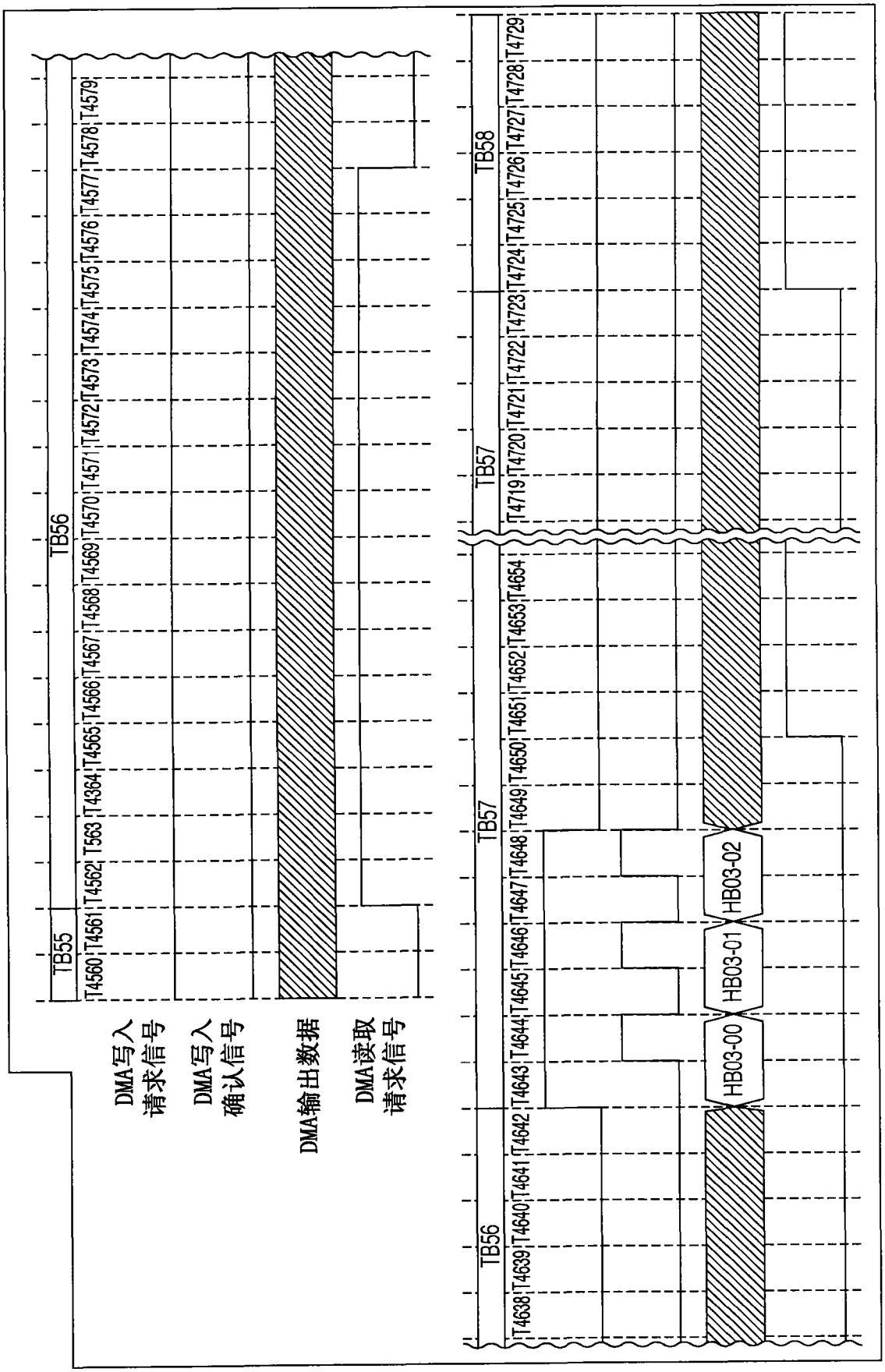

TB55
TB56
TB57
TB58
T4560 T4561 T4562 T563 T4364 T4565 T4566 T4567 T4568 T4569 T4570 T4571 T4572 T4573 T4574 T4575 T4576 T4577 T4578 T4579
T4638 T4639 T4640 T4641 T4642 T4643 T4644 T4645 T4646 T4647 T4648 T4649 T4650 T4651 T4652 T4653 T4654
T4719 T4720 T4721 T4722 T4723 T4724 T4725 T4726 T4727 T4728 T4729
DMA写入请求信号
DMA写入确认信号
DMA输出数据
DMA读取请求信号
HB03-00
HB03-01
HB03-02

图 16A

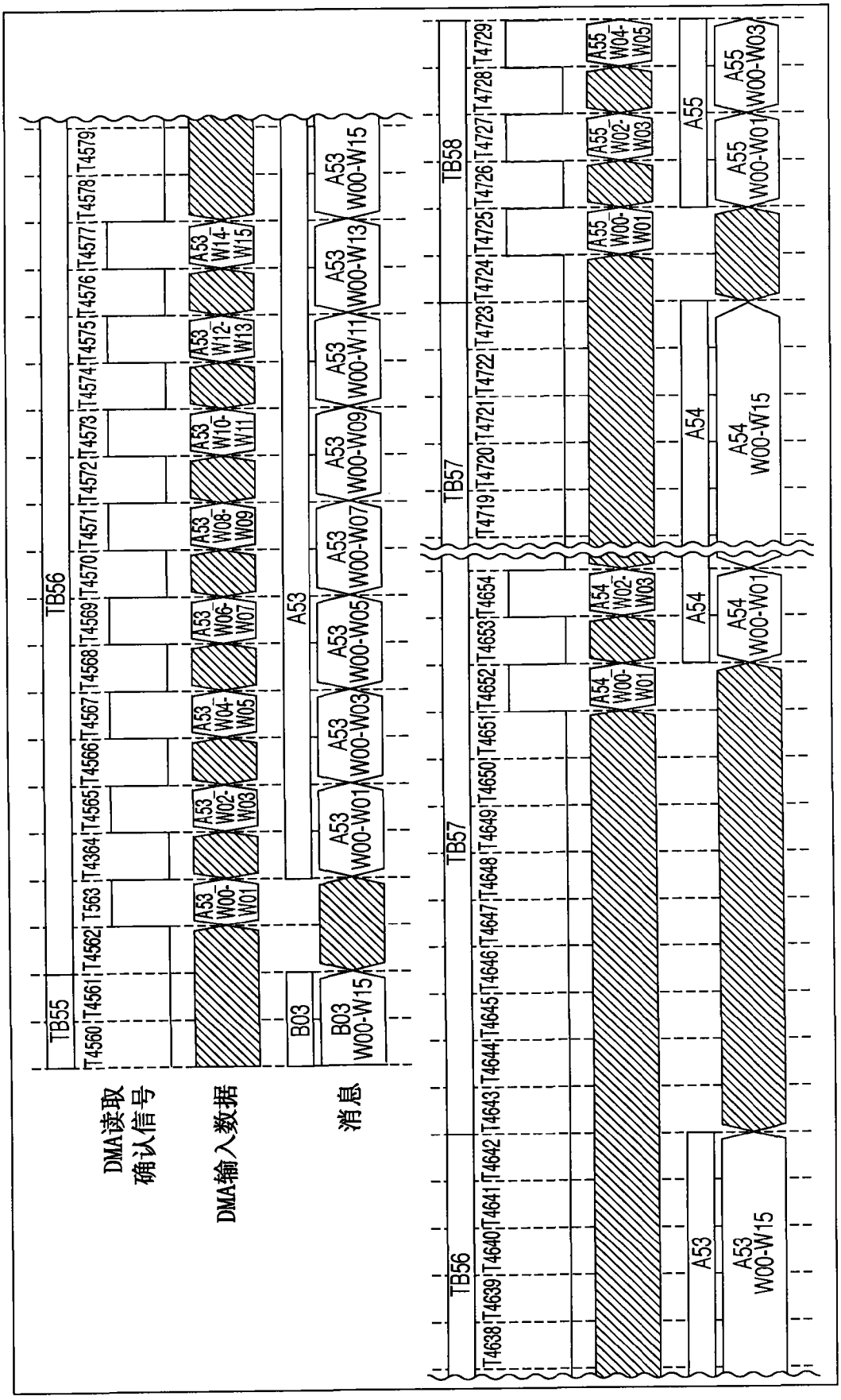


图 16B

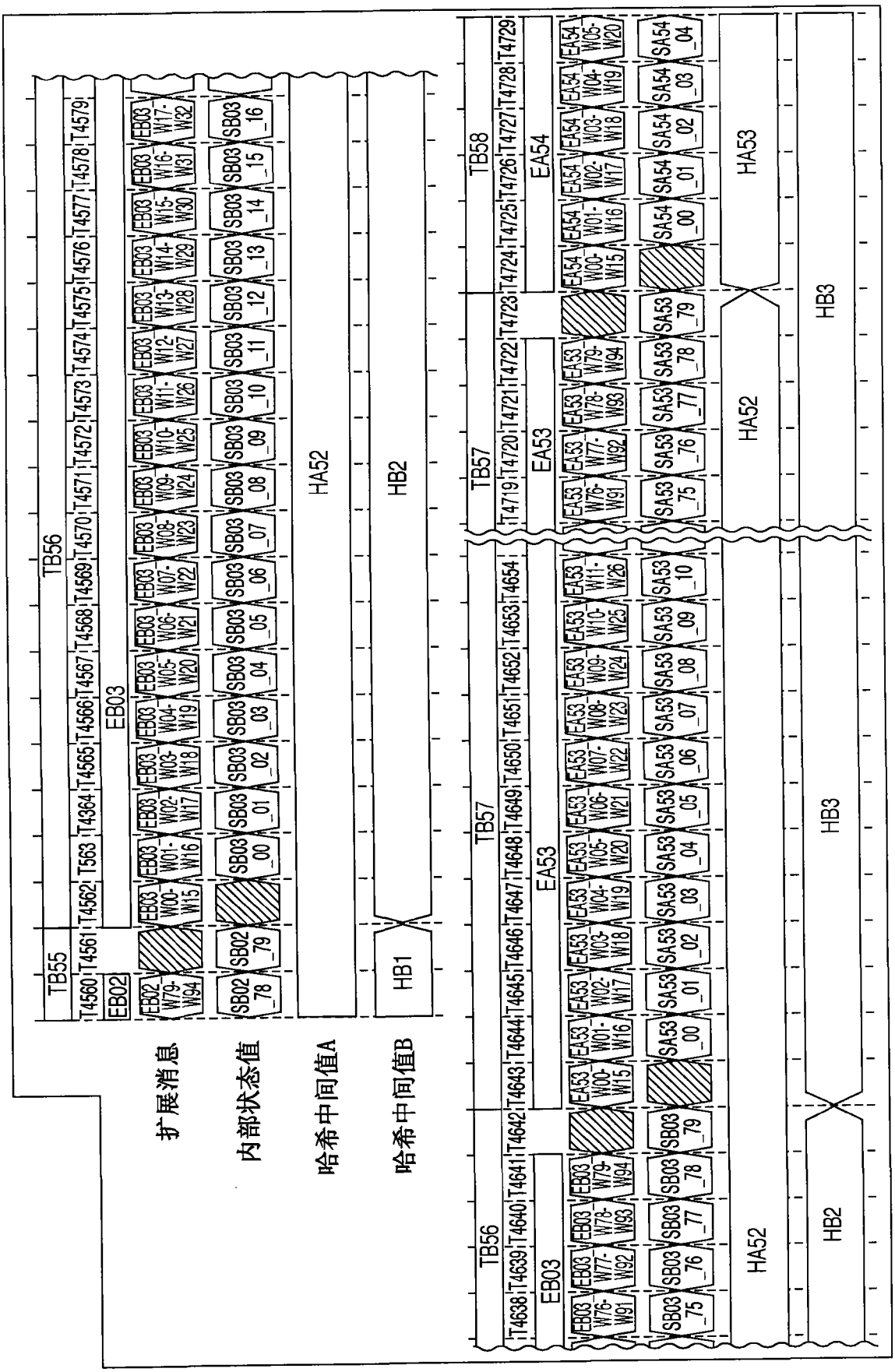

扩展消息
内部状态值
哈希中间值A
哈希中间值B
TB55
TB56
TB57
TB58
EB02
EB03
EA53
EA54
HA52
HA53
HB1
HB2
HB3

图 16C

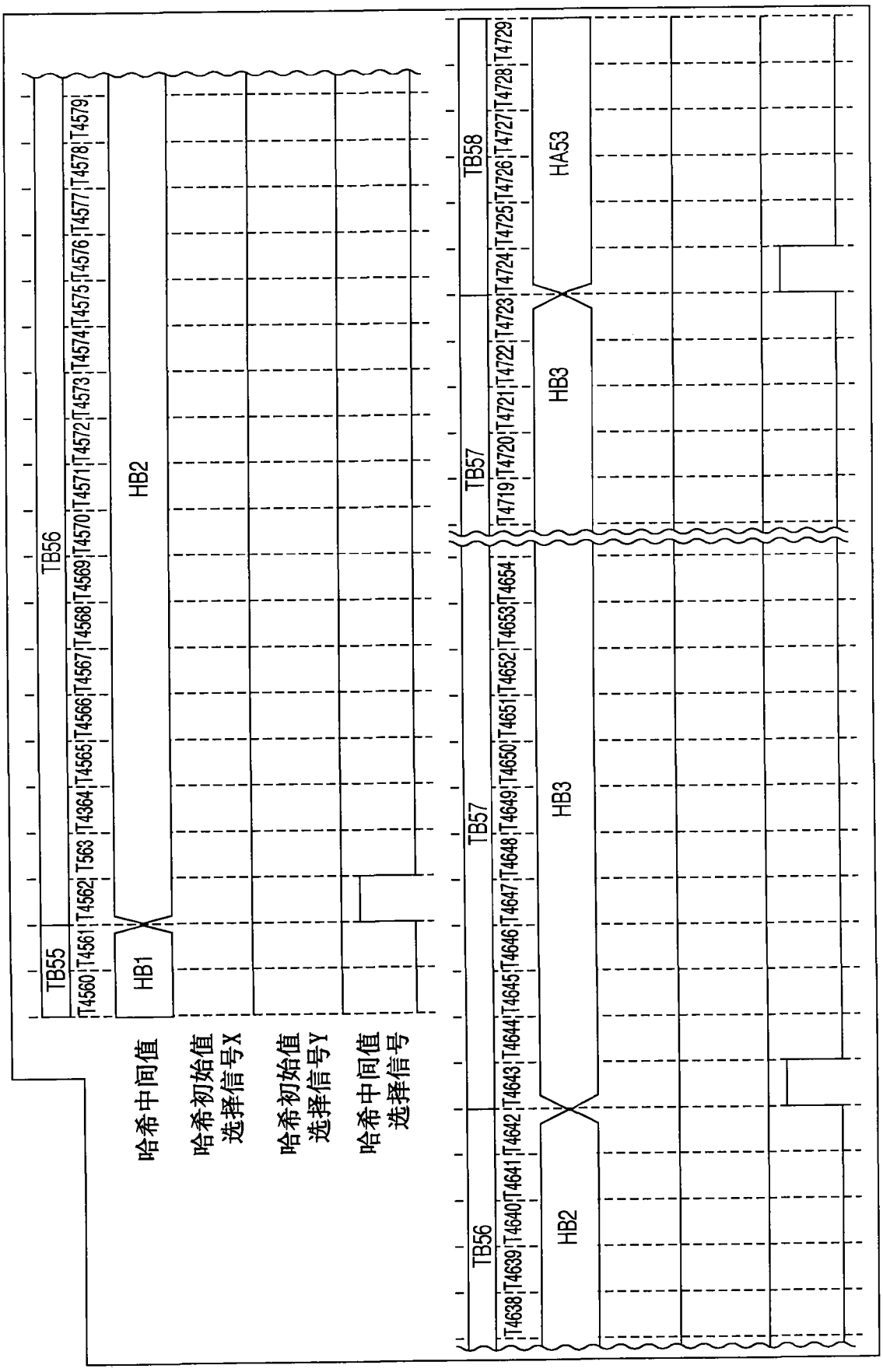

哈希中间值
哈希初始值选择信号X
哈希初始值选择信号Y
哈希中间值选择信号
TB55
TB56
TB57
TB58
HB1
HB2
HB3
HA53
T4560 T4561 T4562 T563 T4364 T4565 T4566 T4567 T4568 T4569 T4570 T4571 T4572 T4573 T4574 T4575 T4576 T4577 T4578 T4579
T4638 T4639 T4640 T4641 T4642 T4643 T4644 T4645 T4646 T4647 T4648 T4649 T4650 T4651 T4652 T4653 T4654
T4719 T4720 T4721 T4722 T4723 T4724 T4725 T4726 T4727 T4728 T4729

图 16D

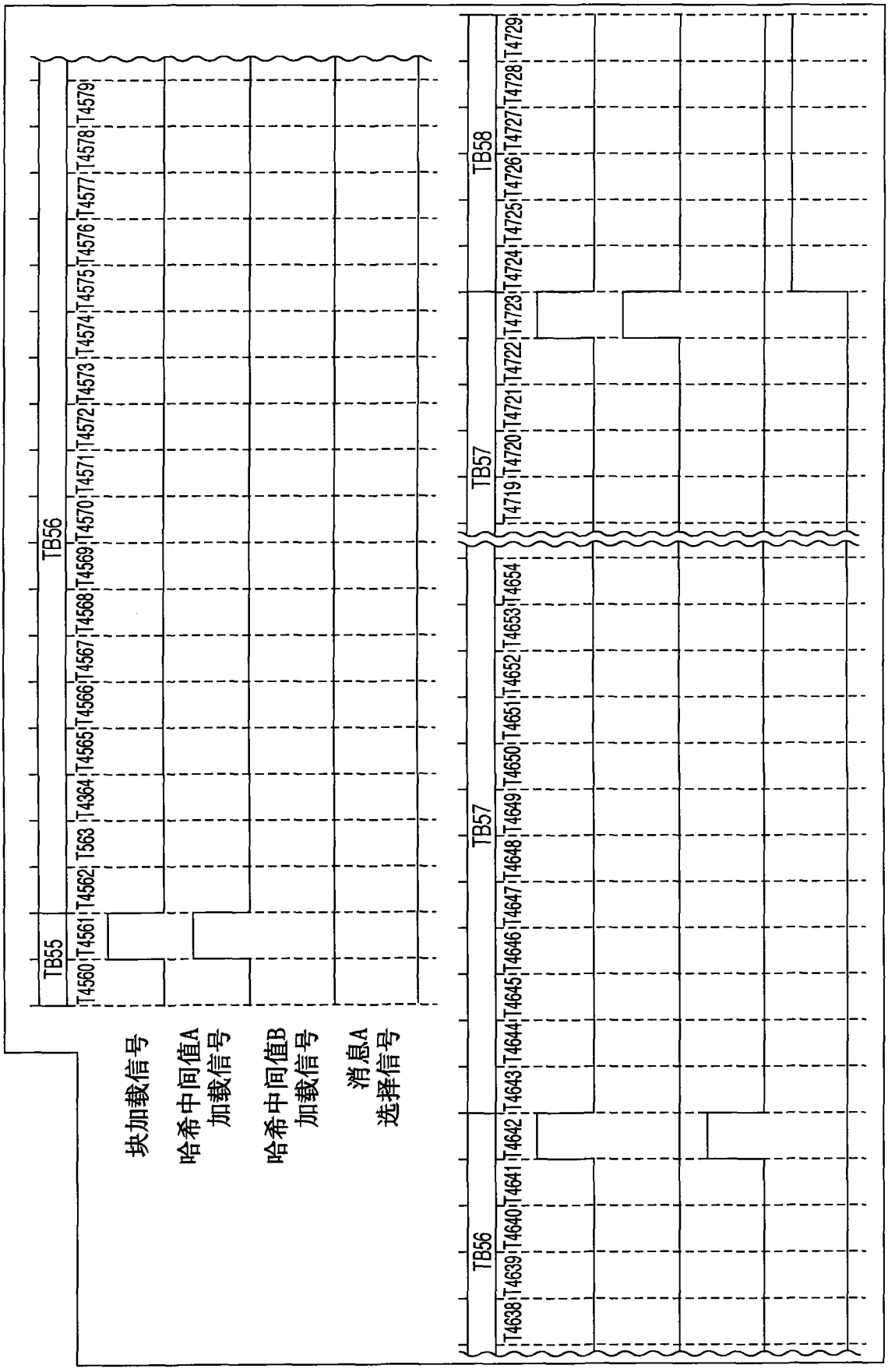

TB55
TB56
TB57
TB58
T4560 T4561 T4562 T563 T4364 T4565 T4566 T4567 T4568 T4569 T4570 T4571 T4572 T4573 T4574 T4575 T4576 T4577 T4578 T4579
T4638 T4639 T4640 T4641 T4642 T4643 T4644 T4645 T4646 T4647 T4648 T4649 T4650 T4651 T4652 T4653 T4654
T4719 T4720 T4721 T4722 T4723 T4724 T4725 T4726 T4727 T4728 T4729
块加载信号
哈希中间值A
加载信号
哈希中间值B
加载信号
消息A
选择信号

图 16E

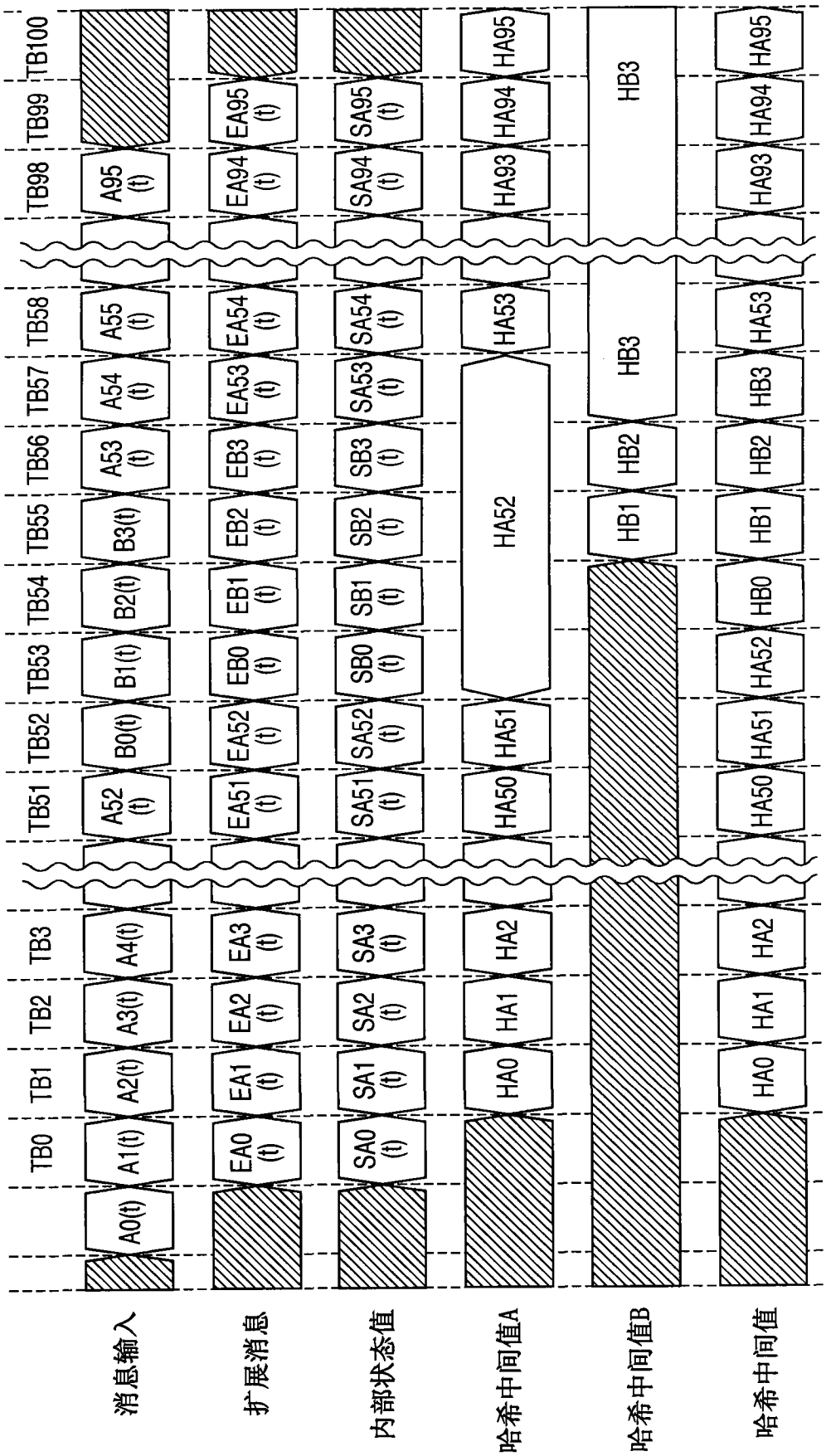

TB0
TB1
TB2
TB3
TB51
TB52
TB53
TB54
TB55
TB56
TB57
TB58
TB98
TB99
TB100
消息输入
扩展消息
内部状态值
哈希中间值A
哈希中间值B
哈希中间值
A0(t)
A1(t)
A2(t)
A3(t)
A4(t)
A52 (t)
B0(t)
B1(t)
B2(t)
B3(t)
A53 (t)
A54 (t)
A55 (t)
A95 (t)
EA0 (t)
EA1 (t)
EA2 (t)
EA3 (t)
EA51 (t)
EA52 (t)
EB0 (t)
EB1 (t)
EB2 (t)
EB3 (t)
EA53 (t)
EA54 (t)
EA94 (t)
EA95 (t)
SA0 (t)
SA1 (t)
SA2 (t)
SA3 (t)
SA51 (t)
SA52 (t)
SB0 (t)
SB1 (t)
SB2 (t)
SB3 (t)
SA53 (t)
SA54 (t)
SA94 (t)
SA95 (t)
HA0
HA1
HA2
HA50
HA51
HA52
HA53
HA93
HA94
HA95
HB0
HB1
HB2
HB3

图 17A

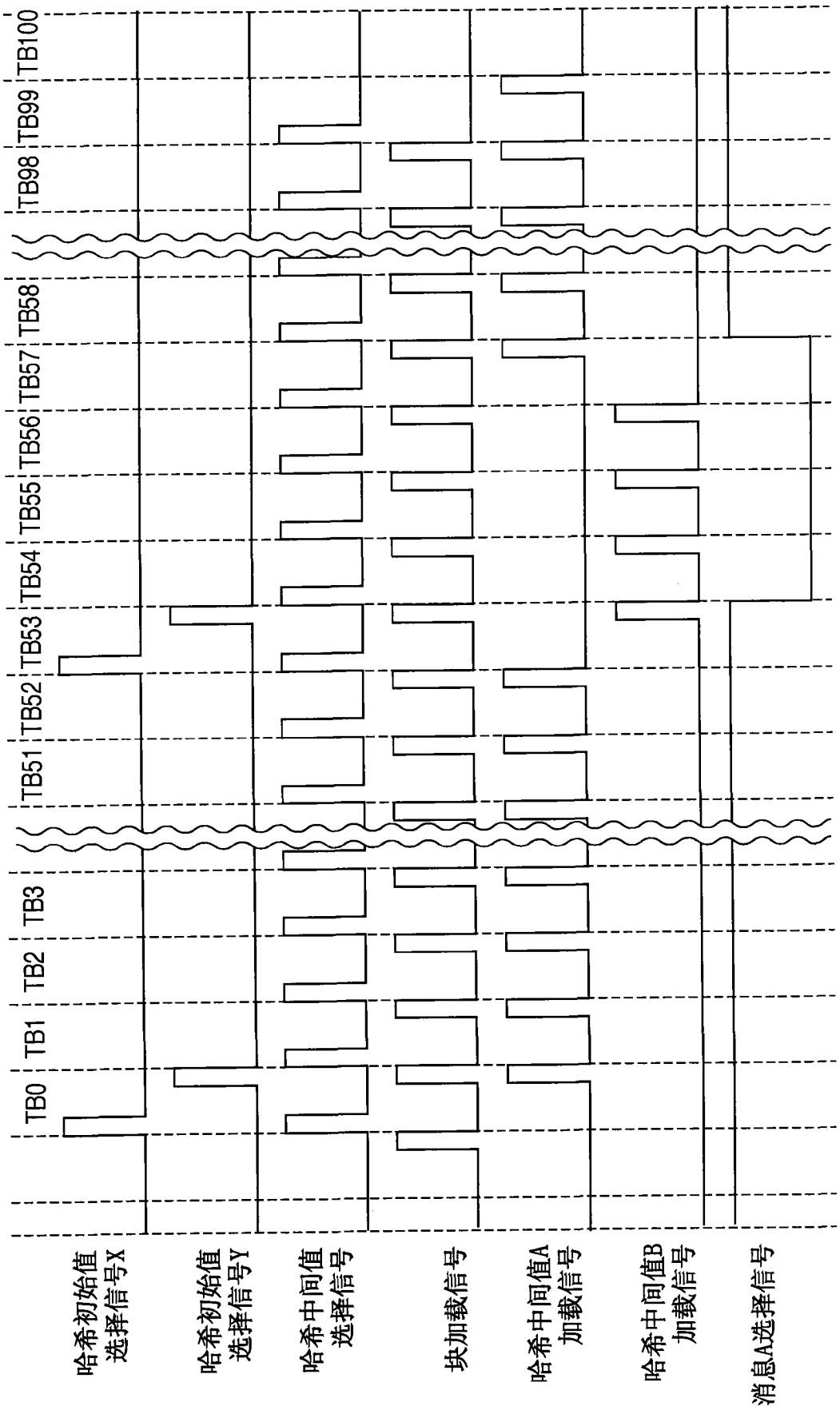

TB0
TB1
TB2
TB3
TB51
TB52
TB53
TB54
TB55
TB56
TB57
TB58
TB98
TB99
TB100
哈希初始值选择信号X
哈希初始值选择信号Y
哈希中间值选择信号
块加载信号
哈希中间值A加载信号
哈希中间值B加载信号
消息A选择信号

图 17B

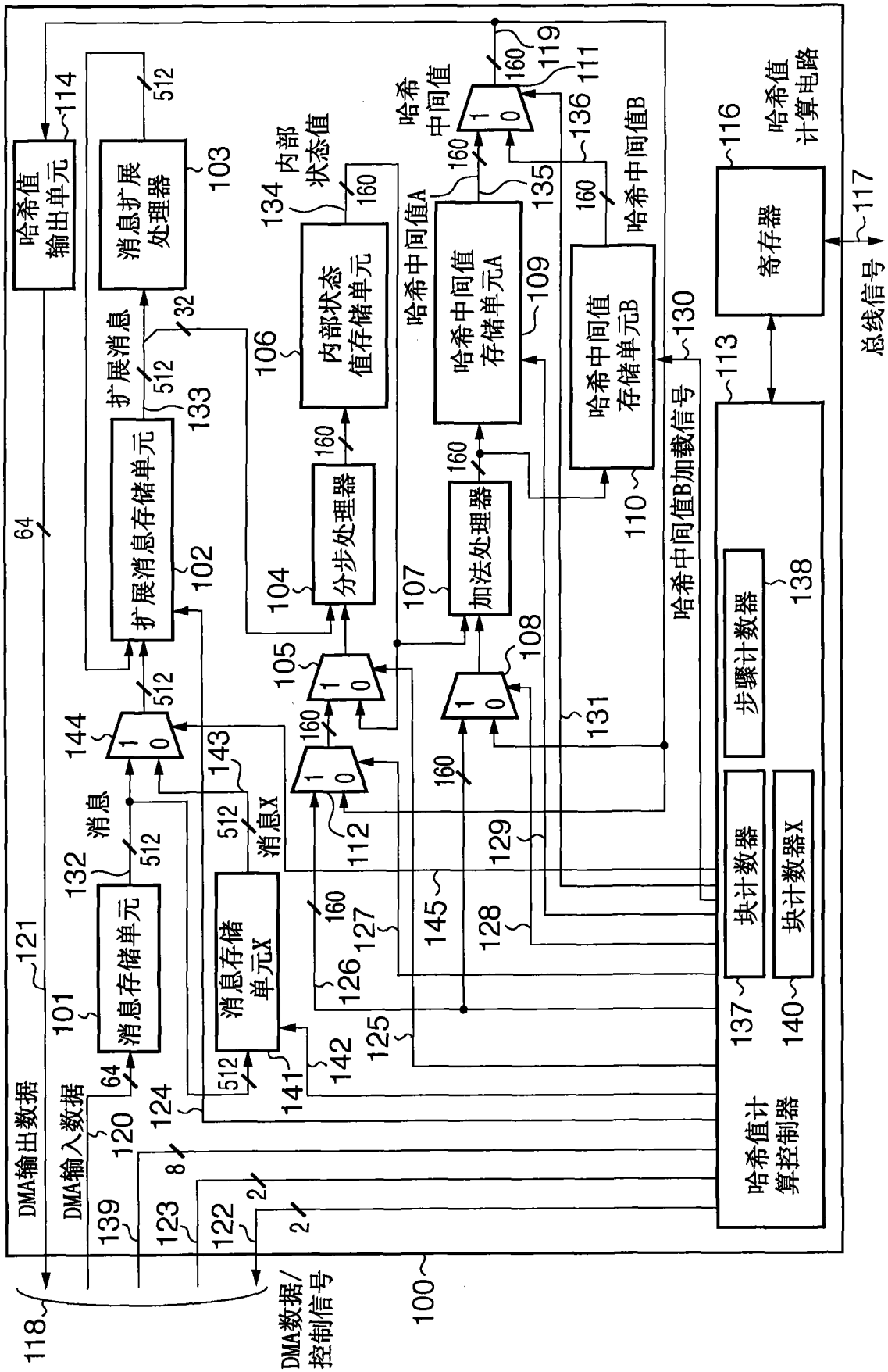

哈希值输出单元
消息扩展处理器
扩展消息存储单元
内部状态值存储单元
分步处理器
加法处理器
哈希中间值存储单元A
哈希中间值存储单元B
寄存器
哈希值计算电路
消息存储单元
消息存储单元X
步骤计数器
块计数器
块计数器X
哈希值计算控制器
DMA输出数据
DMA输入数据
DMA数据/控制信号
总线信号
哈希中间值A
哈希中间值B
哈希中间值B加载信号
内部状态值
消息
消息X
扩展消息

图 18

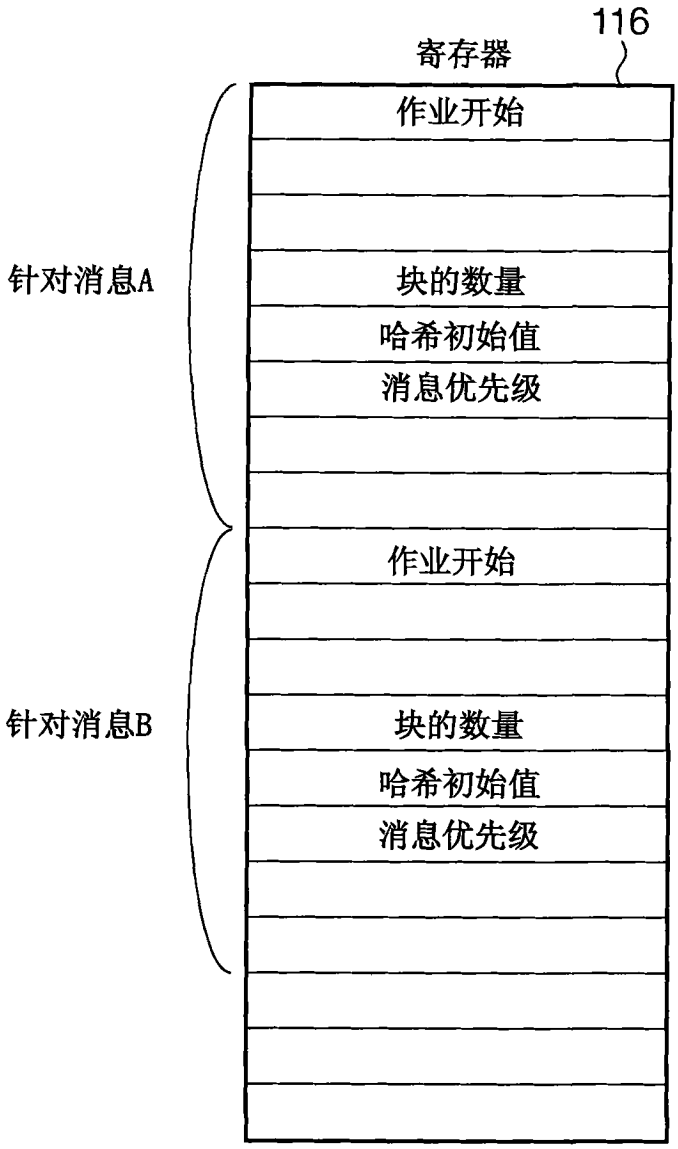

116
寄存器
作业开始
针对消息A
块的数量
哈希初始值
消息优先级
作业开始
针对消息B
块的数量
哈希初始值
消息优先级

图 19

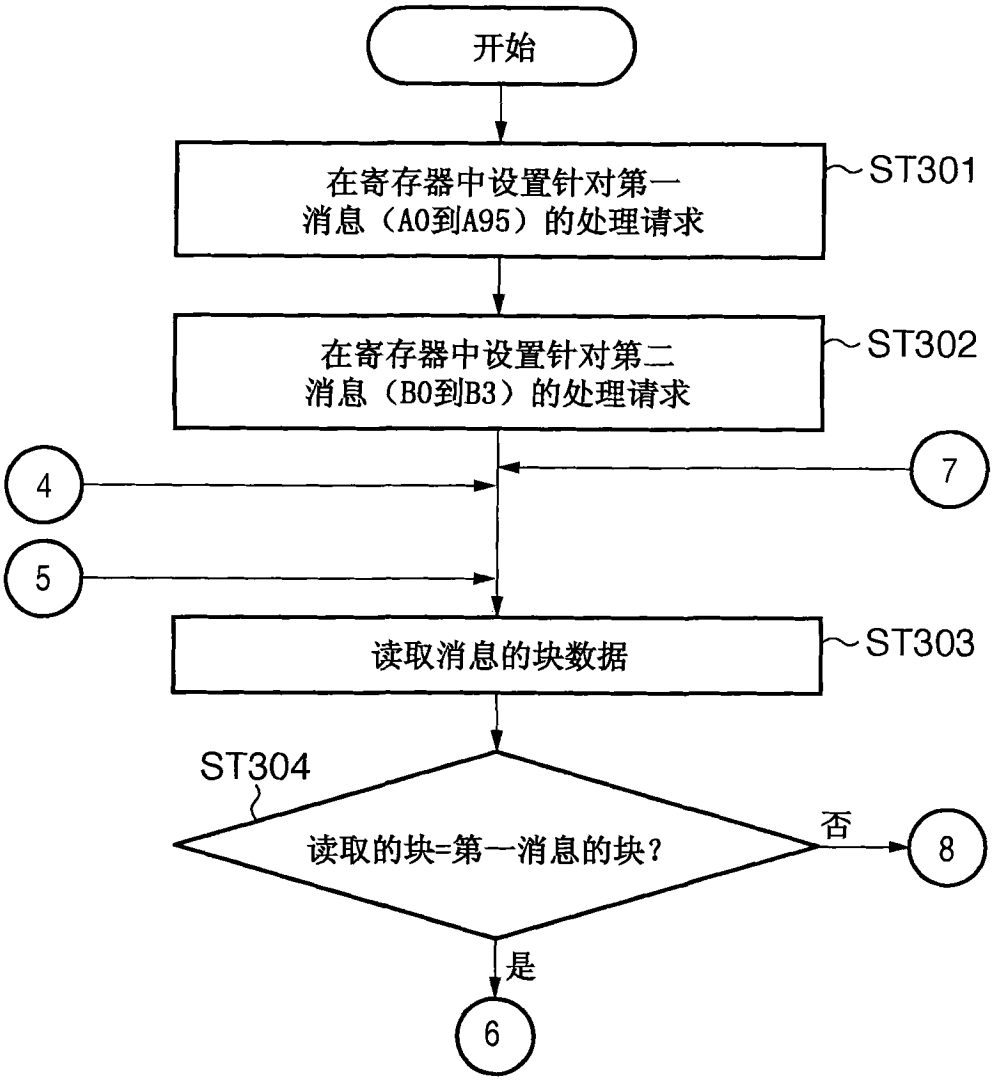

开始
在寄存器中设置针对第一消息（A0到A95）的处理请求
ST301
在寄存器中设置针对第二消息（B0到B3）的处理请求
ST302
4
5
7
读取消息的块数据
ST303
ST304
读取的块=第一消息的块？
否
8
是
6

图 20A

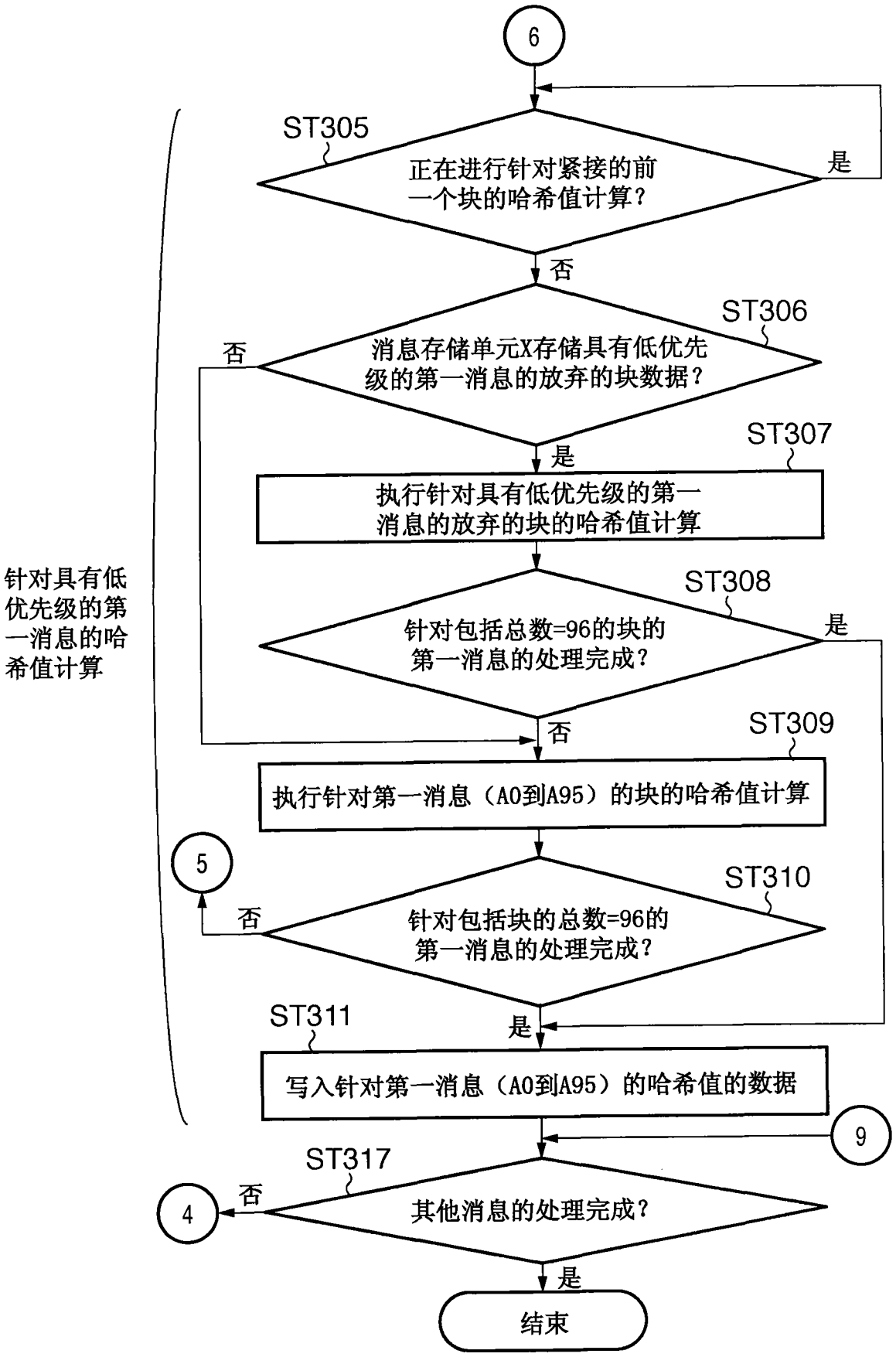

6
ST305
正在进行针对紧接的前一个块的哈希值计算？
是
否
ST306
消息存储单元X存储具有低优先级的第一消息的放弃的块数据？
否
是
ST307
执行针对具有低优先级的第一消息的放弃的块的哈希值计算
ST308
针对包括总数=96的块的第一消息的处理完成？
是
否
ST309
执行针对第一消息（A0到A95）的块的哈希值计算
5
ST310
针对包括块的总数=96的第一消息的处理完成？
否
ST311
是
写入针对第一消息（A0到A95）的哈希值的数据
9
ST317
其他消息的处理完成？
否
4
是
结束
针对具有低优先级的第一消息的哈希值计算

图 20B

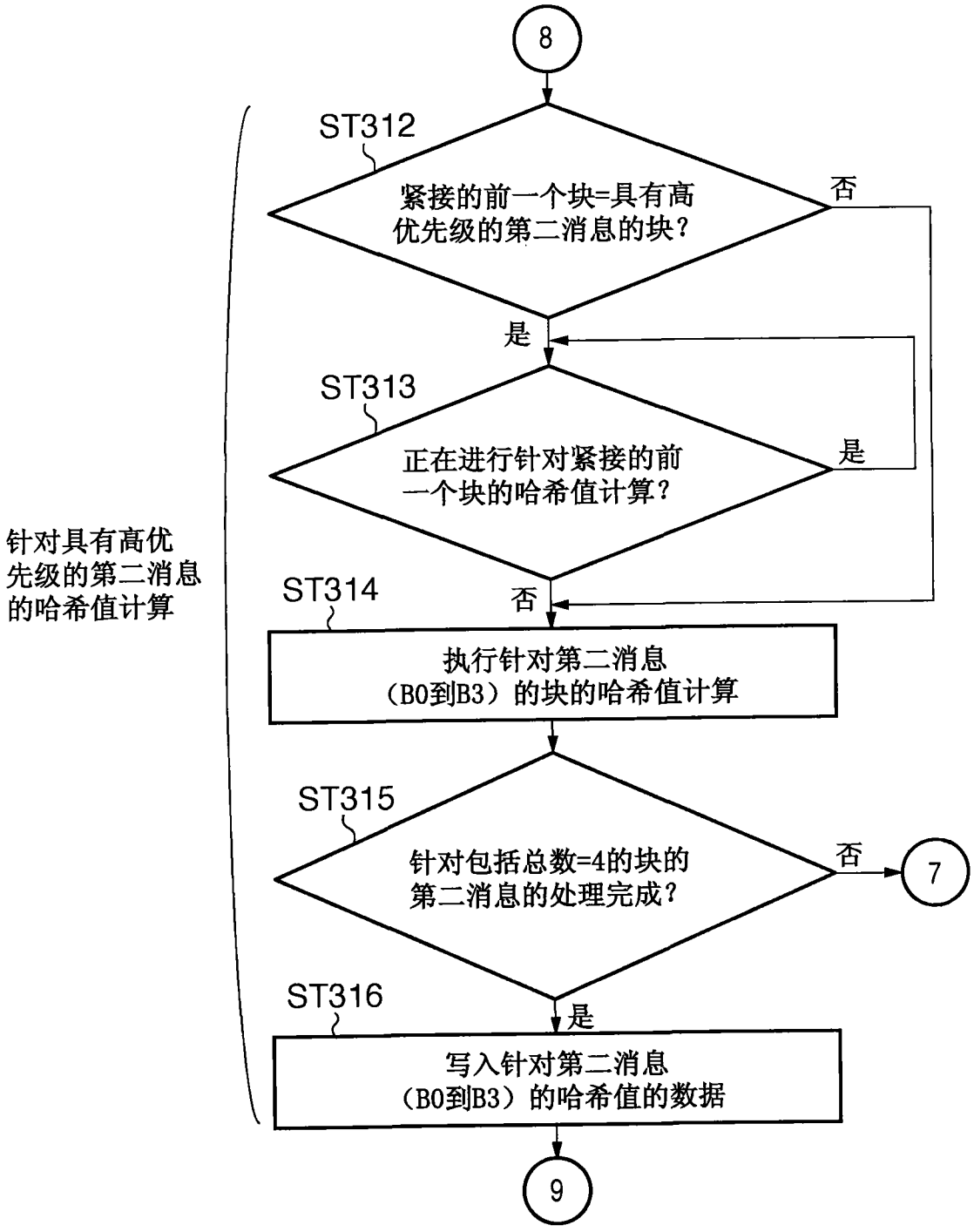

8
ST312
紧接的前一个块=具有高优先级的第二消息的块？
否
是
ST313
正在进行针对紧接的前一个块的哈希值计算？
是
针对具有高优先级的第二消息的哈希值计算
ST314
否
执行针对第二消息（B0到B3）的块的哈希值计算
ST315
针对包括总数=4的块的第二消息的处理完成？
否
7
ST316
是
写入针对第二消息（B0到B3）的哈希值的数据
9

图 20C

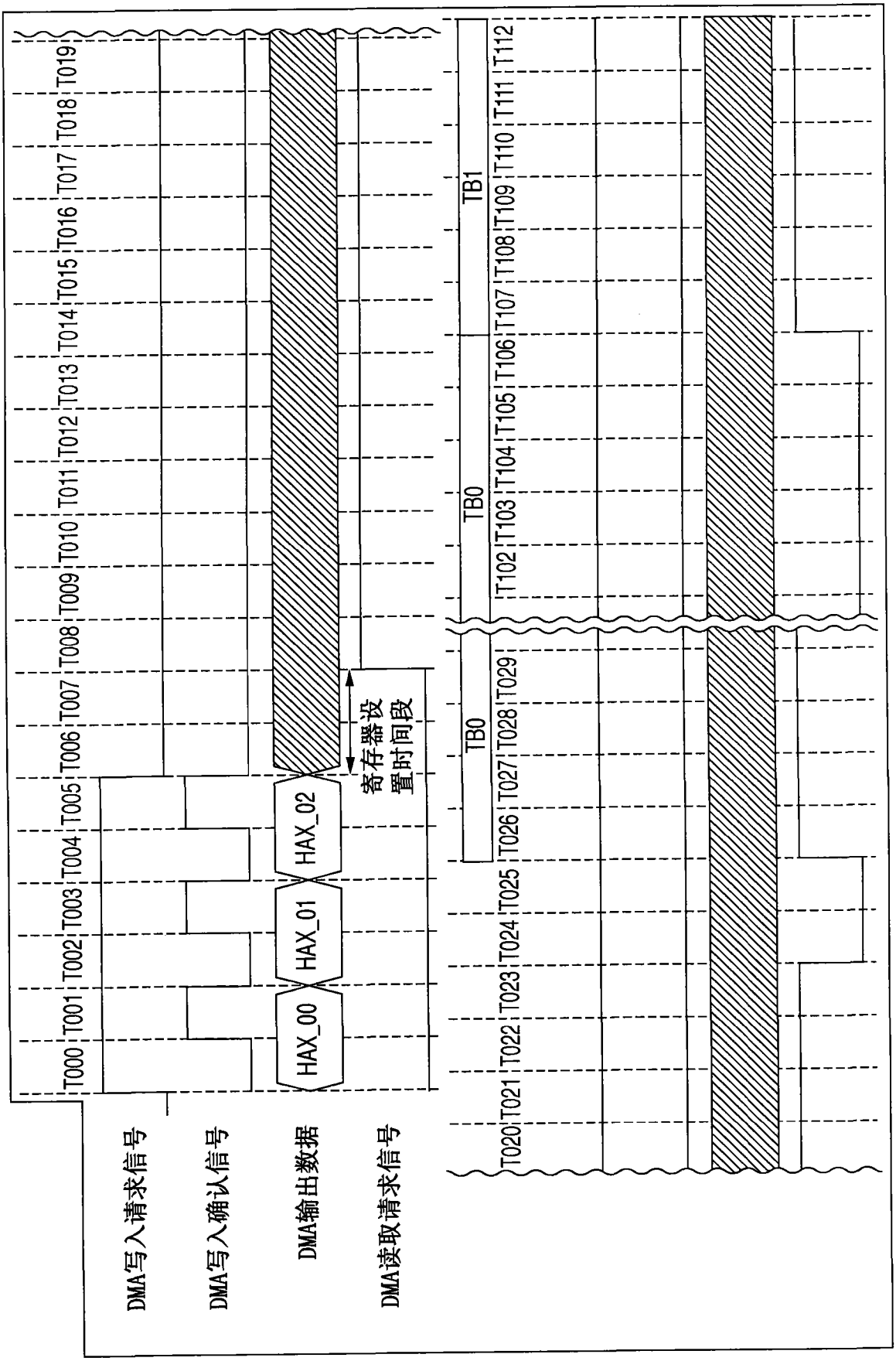

DMA写入请求信号
DMA写入确认信号
DMA输出数据
DMA读取请求信号
T000 T001 T002 T003 T004 T005 T006 T007 T008 T009 T010 T011 T012 T013 T014 T015 T016 T017 T018 T019
T020 T021 T022 T023 T024 T025 T026 T027 T028 T029
T102 T103 T104 T105 T106 T107 T108 T109 T110 T111 T112
HAX_00
HAX_01
HAX_02
寄存器设置时间段
TB0
TB0
TB0
TB1

图 21A

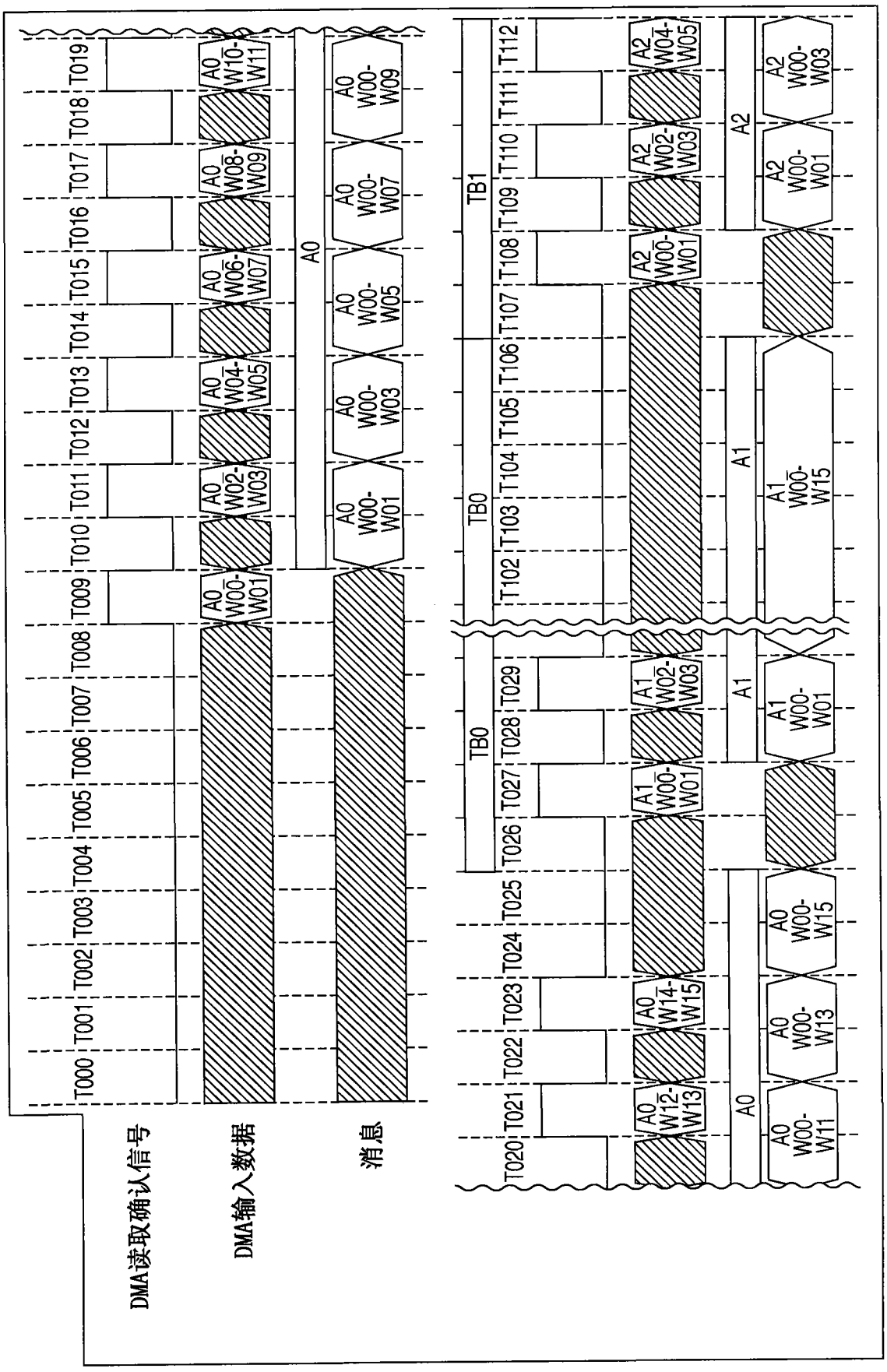

DMA读取确认信号
DMA输入数据
消息
T000 T001 T002 T003 T004 T005 T006 T007 T008 T009 T010 T011 T012 T013 T014 T015 T016 T017 T018 T019
T020 T021 T022 T023 T024 T025 T026 T027 T028 T029 T102 T103 T104 T105 T106 T107 T108 T109 T110 T111 T112
TB0
TB1
A0
A1
A2

图 21B

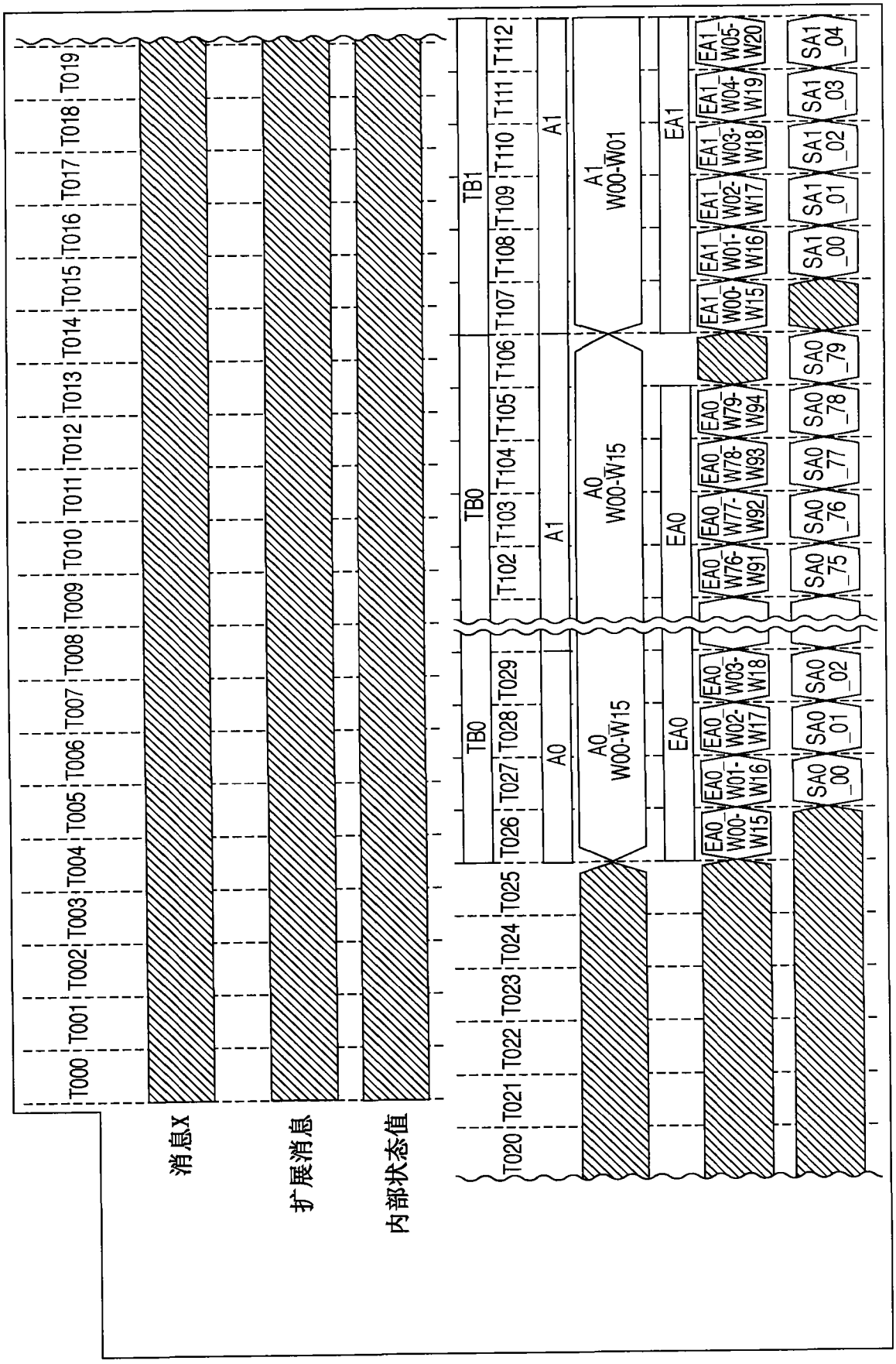

T000
T001
T002
T003
T004
T005
T006
T007
T008
T009
T010
T011
T012
T013
T014
T015
T016
T017
T018
T019
T020
T021
T022
T023
T024
T025
T026
T027
T028
T029
T102
T103
T104
T105
T106
T107
T108
T109
T110
T111
T112
消息X
扩展消息
内部状态值
TB0
TB1
A0
A1
EA0
EA1
SA0_00
SA0_01
SA0_02
SA0_75
SA0_76
SA0_77
SA0_78
SA0_79
SA1_00
SA1_01
SA1_02
SA1_03
SA1_04
A0 W00-W15
A1 W00-W01
EA0_W00-W15
EA0_W01-W16
EA0_W02-W17
EA0_W03-W18
EA0_W76-W91
EA0_W77-W92
EA0_W78-W93
EA0_W79-W94
EA1_W00-W15
EA1_W01-W16
EA1_W02-W17
EA1_W03-W18
EA1_W04-W19
EA1_W05-W20

图 21C

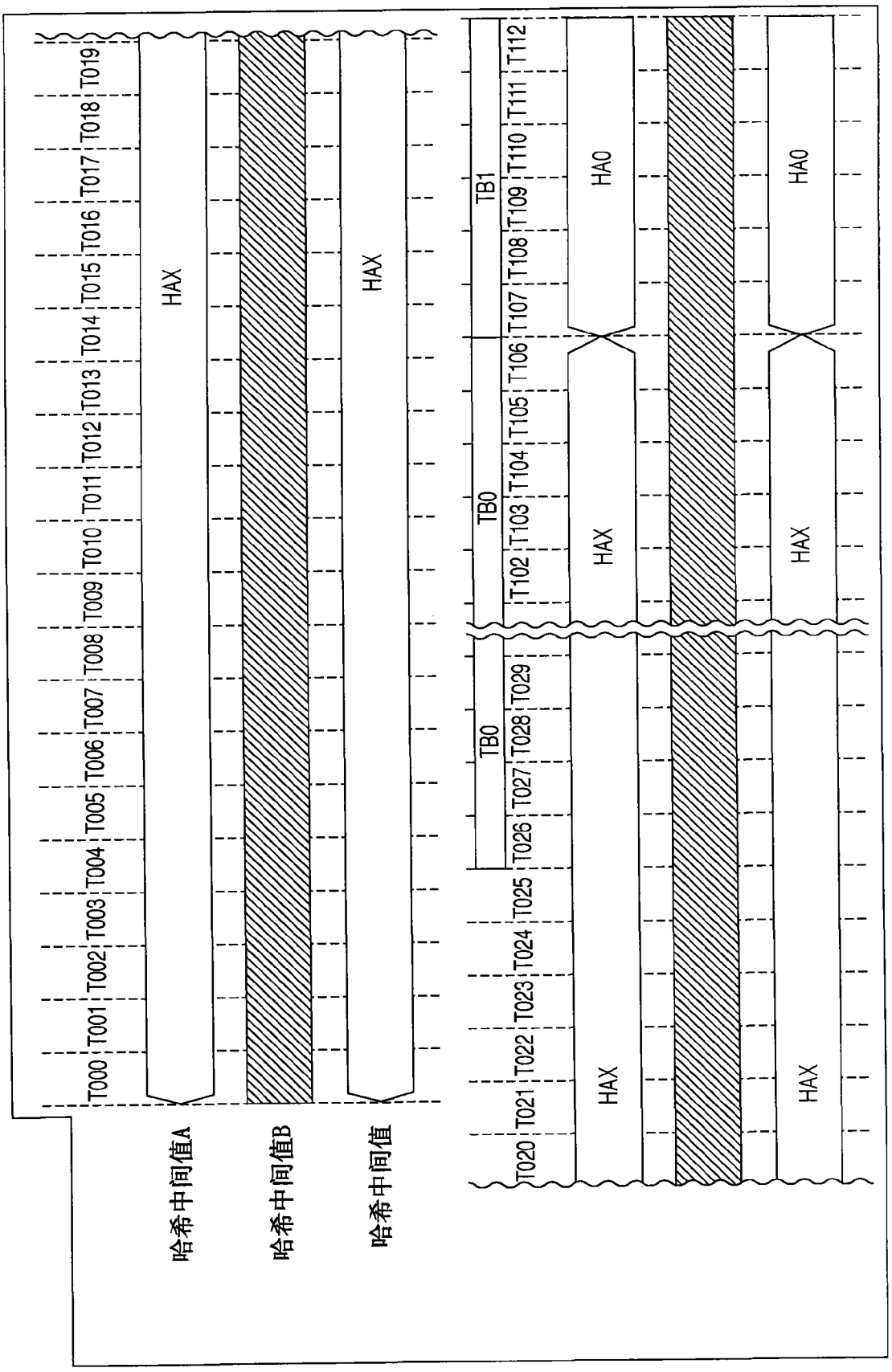

T000
T001
T002
T003
T004
T005
T006
T007
T008
T009
T010
T011
T012
T013
T014
T015
T016
T017
T018
T019
T020
T021
T022
T023
T024
T025
T026
T027
T028
T029
T102
T103
T104
T105
T106
T107
T108
T109
T110
T111
T112
TB0
TB0
TB1
HAX
HAX
HAX
HAX
HAX
HA0
HA0
哈希中间值A
哈希中间值B
哈希中间值

图 21D

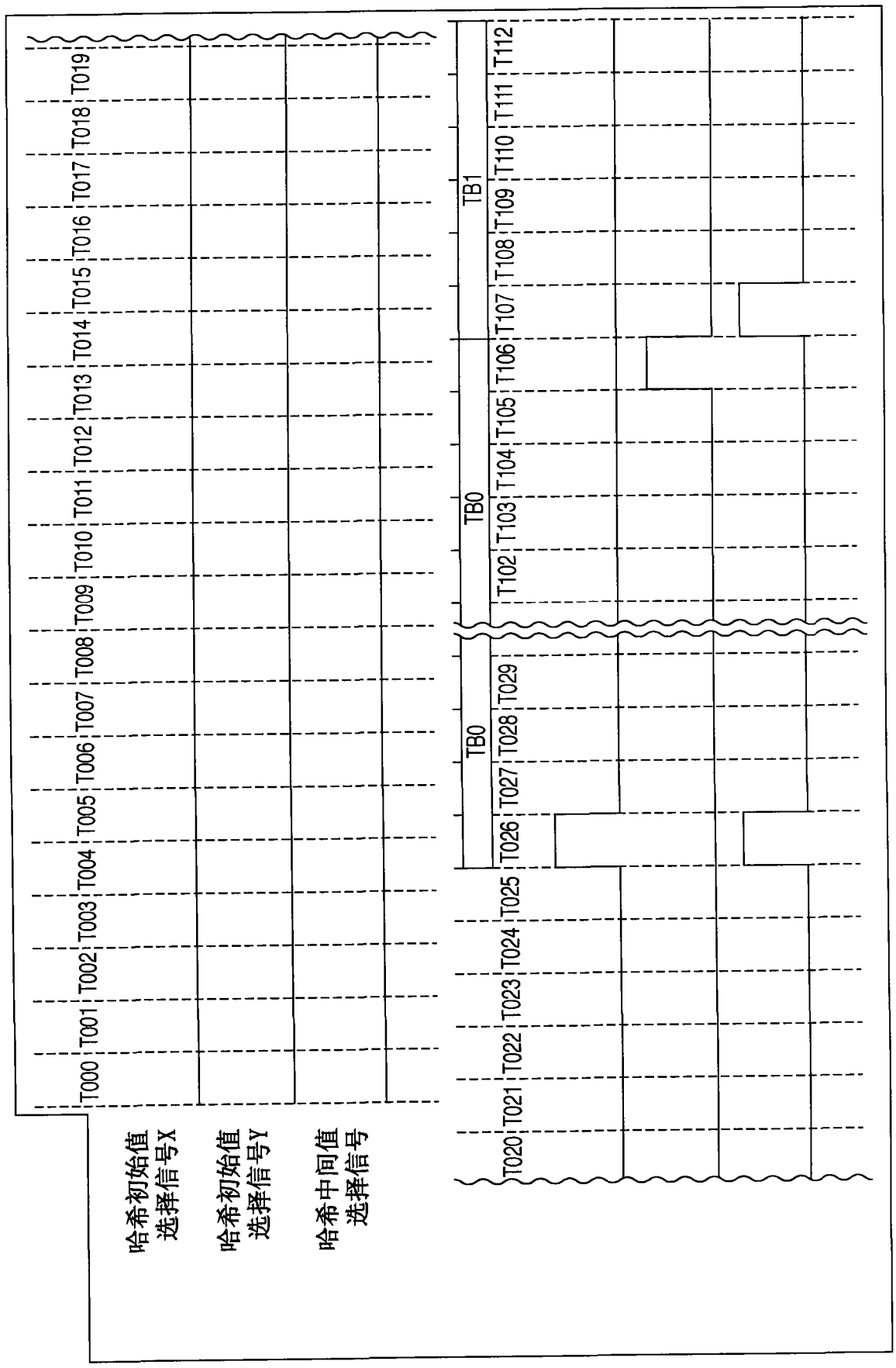

T000
T001
T002
T003
T004
T005
T006
T007
T008
T009
T010
T011
T012
T013
T014
T015
T016
T017
T018
T019
T020
T021
T022
T023
T024
T025
T026
T027
T028
T029
T102
T103
T104
T105
T106
T107
T108
T109
T110
T111
T112
TB0
TB0
TB1
哈希初始值选择信号X
哈希初始值选择信号Y
哈希中间值选择信号

图 21E

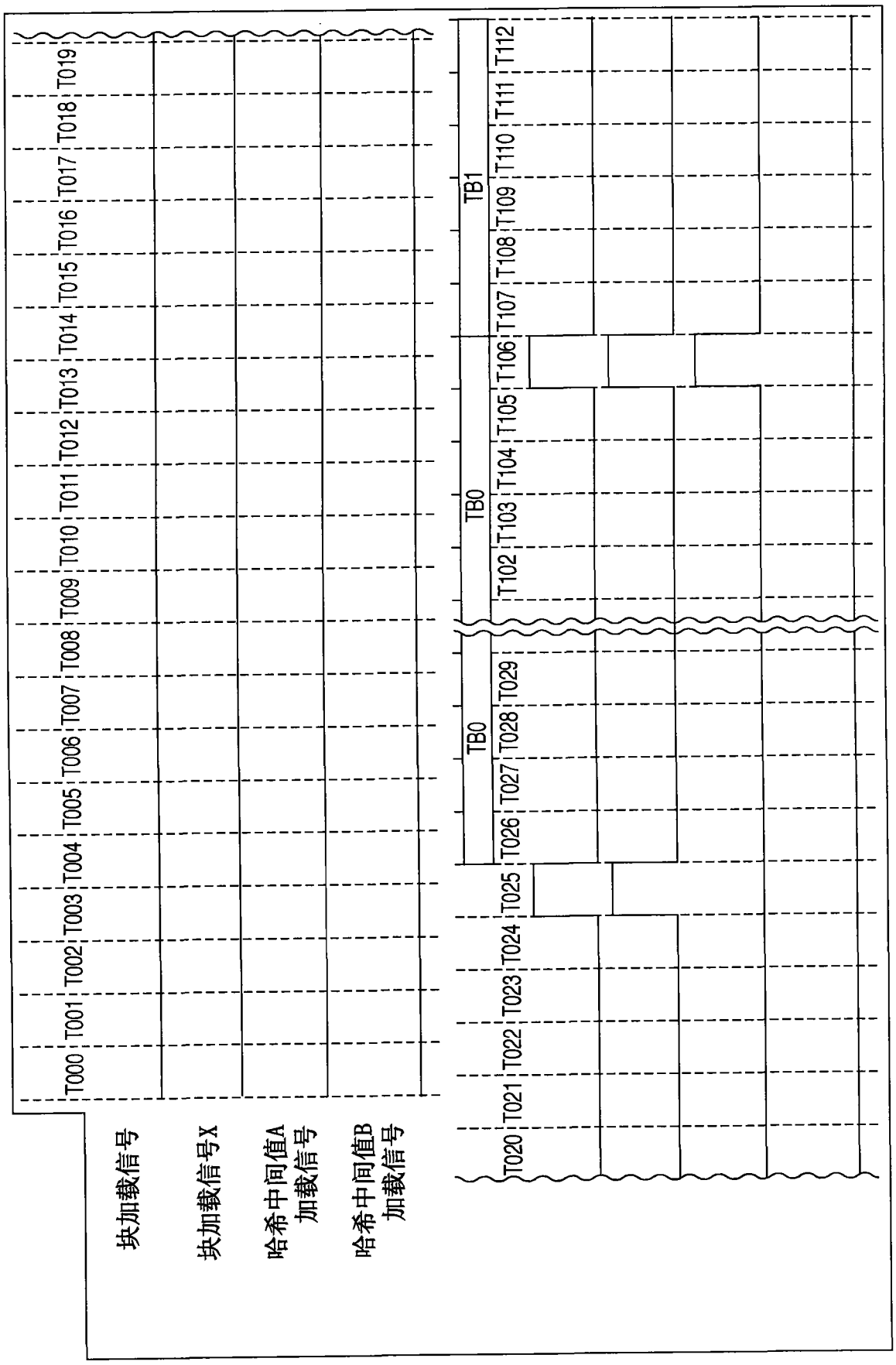

块加载信号
块加载信号X
哈希中间值A加载信号
哈希中间值B加载信号
T000 T001 T002 T003 T004 T005 T006 T007 T008 T009 T010 T011 T012 T013 T014 T015 T016 T017 T018 T019
T020 T021 T022 T023 T024 T025 T026 T027 T028 T029
T102 T103 T104 T105 T106 T107 T108 T109 T110 T111 T112
TB0
TB0
TB1

图 21F

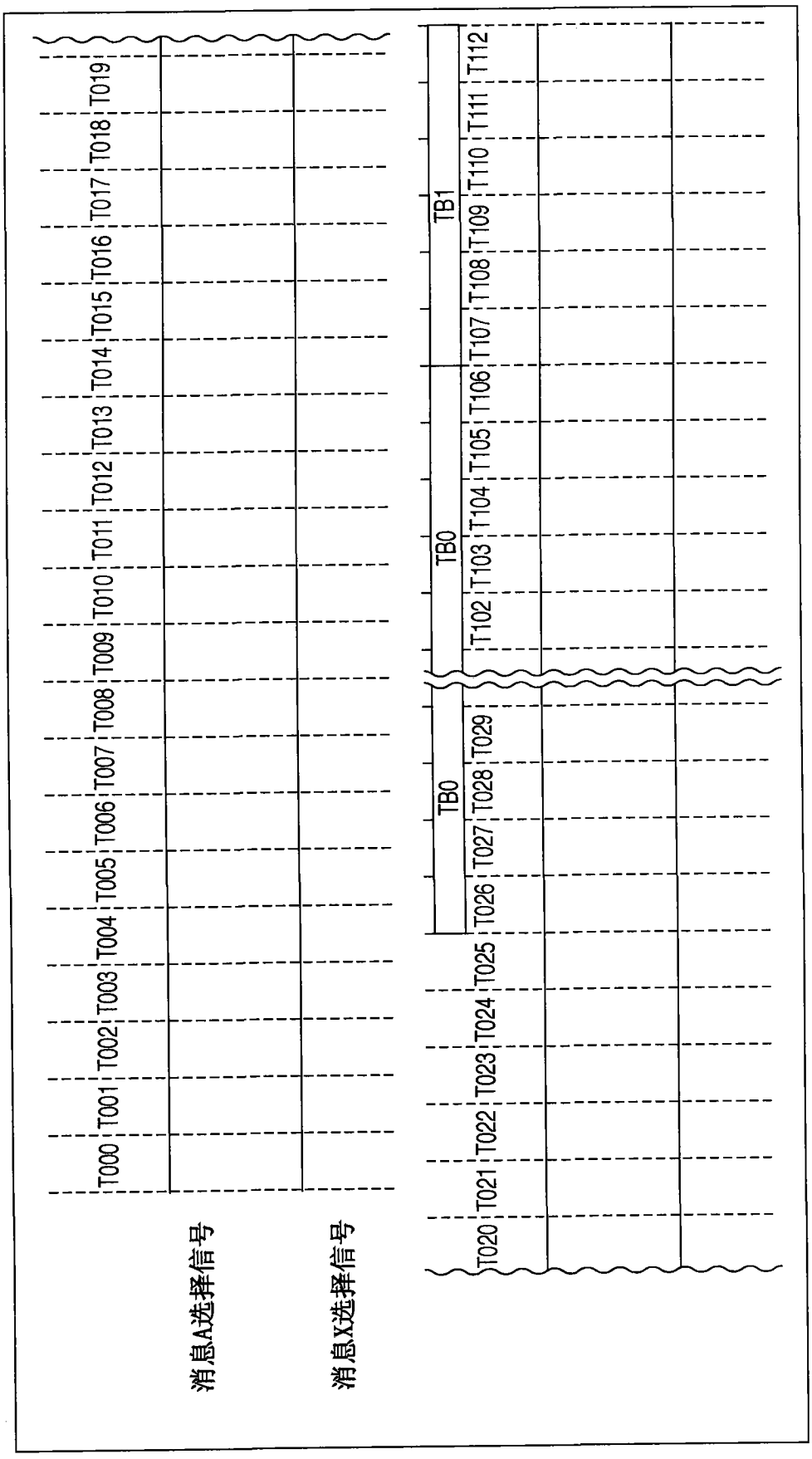

T000
T001
T002
T003
T004
T005
T006
T007
T008
T009
T010
T011
T012
T013
T014
T015
T016
T017
T018
T019
T020
T021
T022
T023
T024
T025
T026
T027
T028
T029
T102
T103
T104
T105
T106
T107
T108
T109
T110
T111
T112
TB0
TB0
TB1
消息A选择信号
消息X选择信号

图 21G

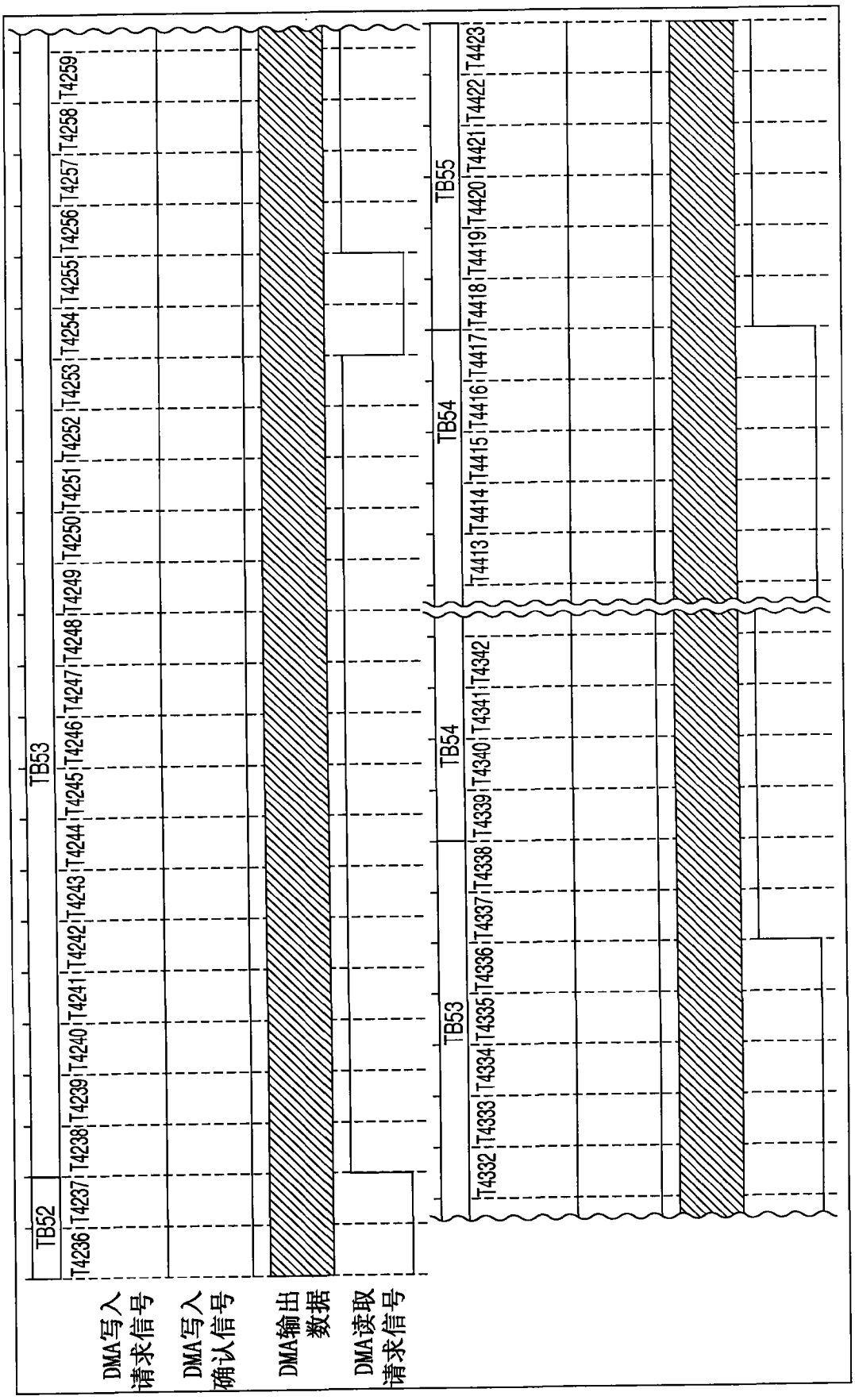

DMA写入请求信号
DMA写入确认信号
DMA输出数据
DMA读取请求信号
TB52
TB53
TB54
TB55
T4236 T4237 T4238 T4239 T4240 T4241 T4242 T4243 T4244 T4245 T4246 T4247 T4248 T4249 T4250 T4251 T4252 T4253 T4254 T4255 T4256 T4257 T4258 T4259
T4332 T4333 T4334 T4335 T4336 T4337 T4338 T4339 T4340 T4341 T4342
T4413 T4414 T4415 T4416 T4417 T4418 T4419 T4420 T4421 T4422 T4423

图 22A

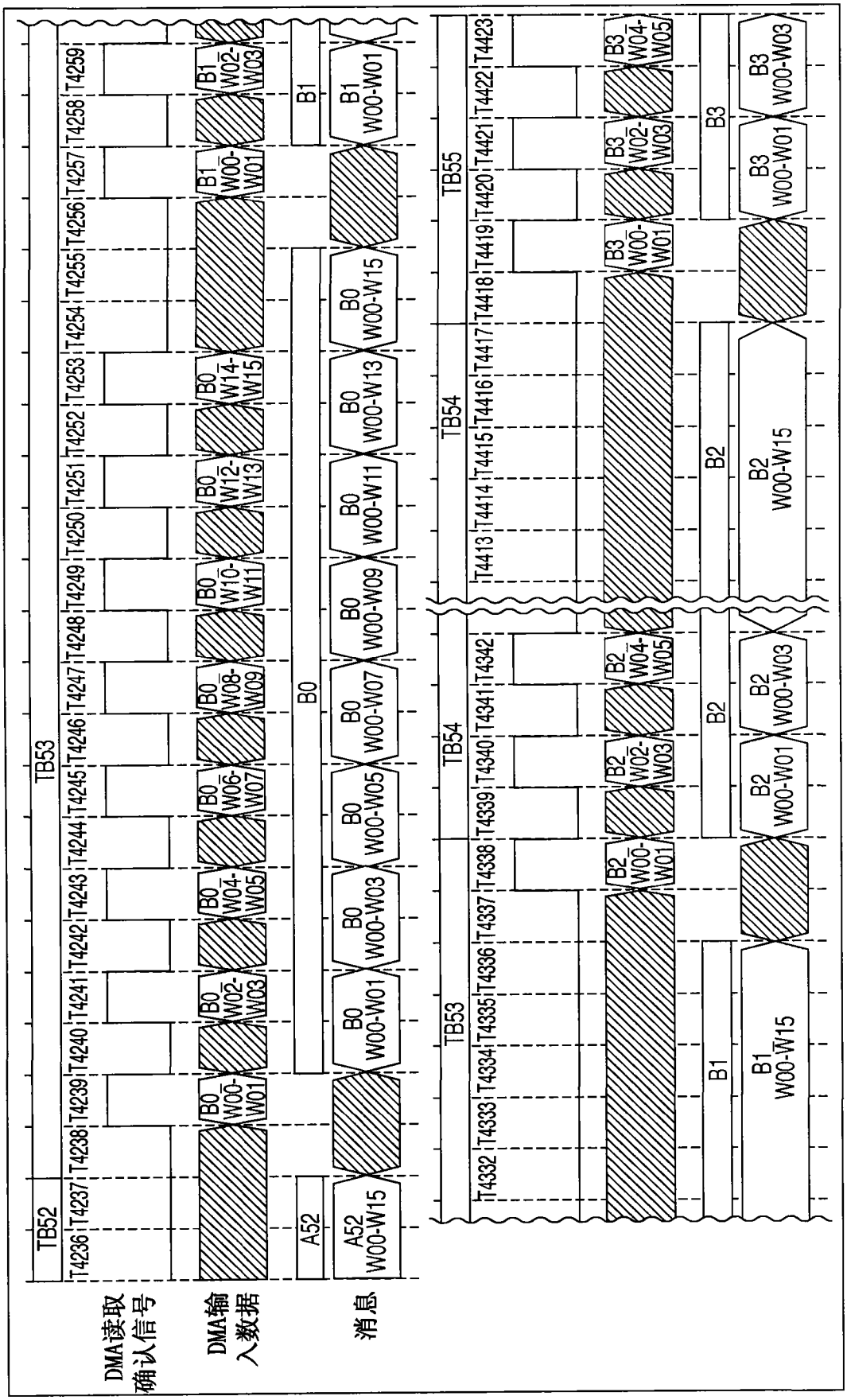

DMA读取确认信号
DMA输入数据
消息
TB52
TB53
TB54
TB55
A52
B0
B1
B2
B3
T4236 T4237 T4238 T4239 T4240 T4241 T4242 T4243 T4244 T4245 T4246 T4247 T4248 T4249 T4250 T4251 T4252 T4253 T4254 T4255 T4256 T4257 T4258 T4259
T4332 T4333 T4334 T4335 T4336 T4337 T4338 T4339 T4340 T4341 T4342
T4413 T4414 T4415 T4416 T4417 T4418 T4419 T4420 T4421 T4422 T4423
A52 W00-W15
B0 W00-W01
B0 W02-W03
B0 W04-W05
B0 W06-W07
B0 W08-W09
B0 W10-W11
B0 W12-W13
B0 W14-W15
B0 W00-W03
B0 W00-W05
B0 W00-W07
B0 W00-W09
B0 W00-W11
B0 W00-W13
B0 W00-W15
B1 W00-W01
B1 W02-W03
B1 W00-W03
B1 W00-W15
B2 W00-W01
B2 W02-W03
B2 W04-W05
B2 W00-W03
B2 W00-W15
B3 W00-W01
B3 W02-W03
B3 W04-W05
B3 W00-W03

图 22B

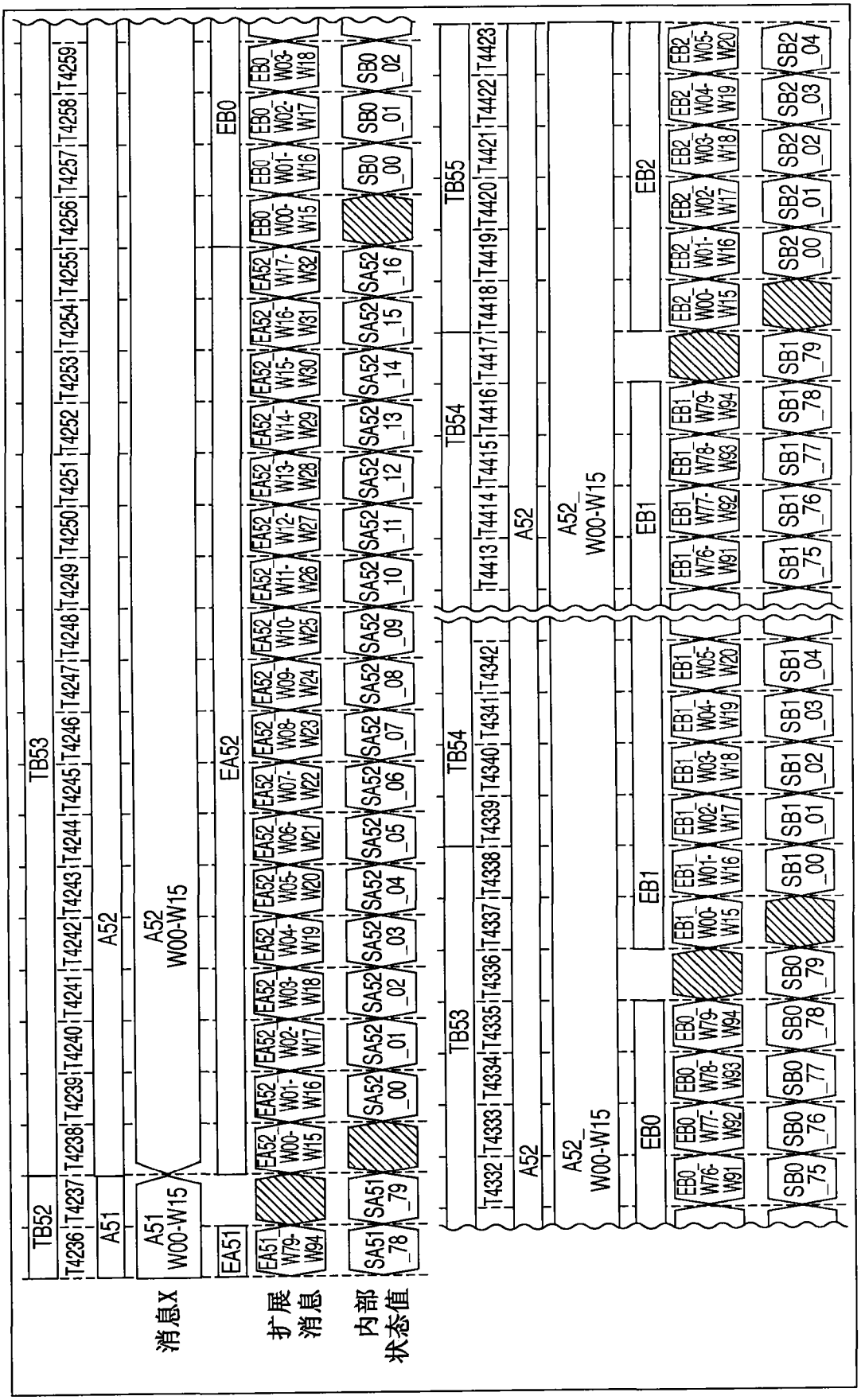

消息X
扩展消息
内部状态值
TB52
TB53
TB54
TB55
A51
A52
EA51
EA52
EB0
EB1
EB2
SA51_78
SA52_00
SA52_01
SA52_02
SA52_03
SA52_04
SA52_05
SA52_06
SA52_07
SA52_08
SA52_09
SA52_10
SA52_11
SA52_12
SA52_13
SA52_14
SA52_15
SA52_16
SB0_75
SB0_76
SB0_77
SB0_78
SB0_79
SB0_00
SB0_01
SB0_02
SB1_75
SB1_76
SB1_77
SB1_78
SB1_79
SB1_00
SB1_01
SB1_02
SB1_03
SB1_04
SB2_00
SB2_01
SB2_02
SB2_03
SB2_04

图 22C

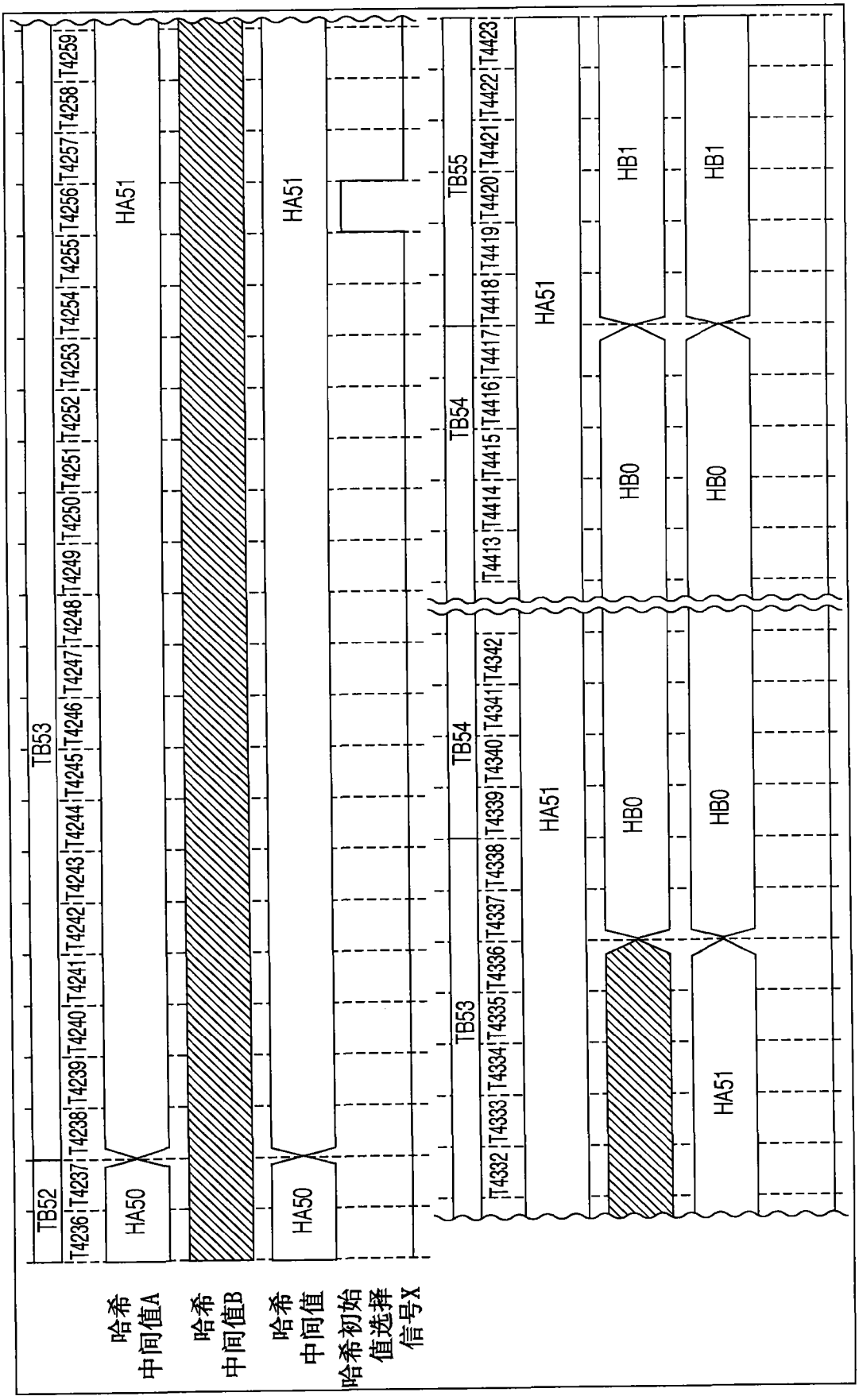

哈希中间值A
哈希中间值B
哈希中间值
哈希初始值选择信号X
TB52
TB53
TB54
TB55
T4236 T4237 T4238 T4239 T4240 T4241 T4242 T4243 T4244 T4245 T4246 T4247 T4248 T4249 T4250 T4251 T4252 T4253 T4254 T4255 T4256 T4257 T4258 T4259
T4332 T4333 T4334 T4335 T4336 T4337 T4338 T4339 T4340 T4341 T4342
T4413 T4414 T4415 T4416 T4417 T4418 T4419 T4420 T4421 T4422 T4423
HA50
HA51
HB0
HB1

图 22D

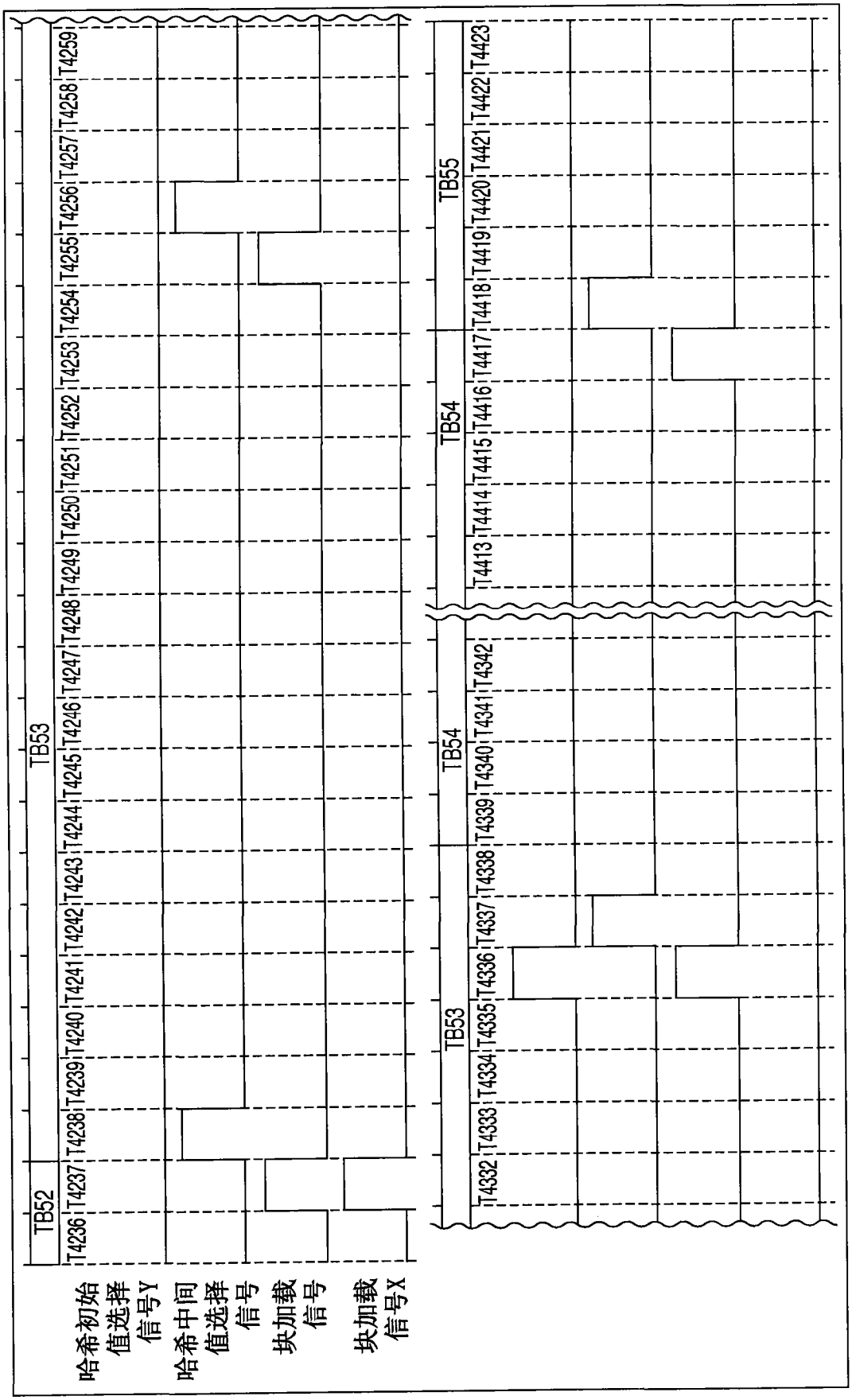

哈希初始值选择信号Y
哈希中间值选择信号
块加载信号
块加载信号X
TB52
TB53
TB54
TB55
T4236 T4237 T4238 T4239 T4240 T4241 T4242 T4243 T4244 T4245 T4246 T4247 T4248 T4249 T4250 T4251 T4252 T4253 T4254 T4255 T4256 T4257 T4258 T4259
T4332 T4333 T4334 T4335 T4336 T4337 T4338 T4339 T4340 T4341 T4342
T4413 T4414 T4415 T4416 T4417 T4418 T4419 T4420 T4421 T4422 T4423

图 22E

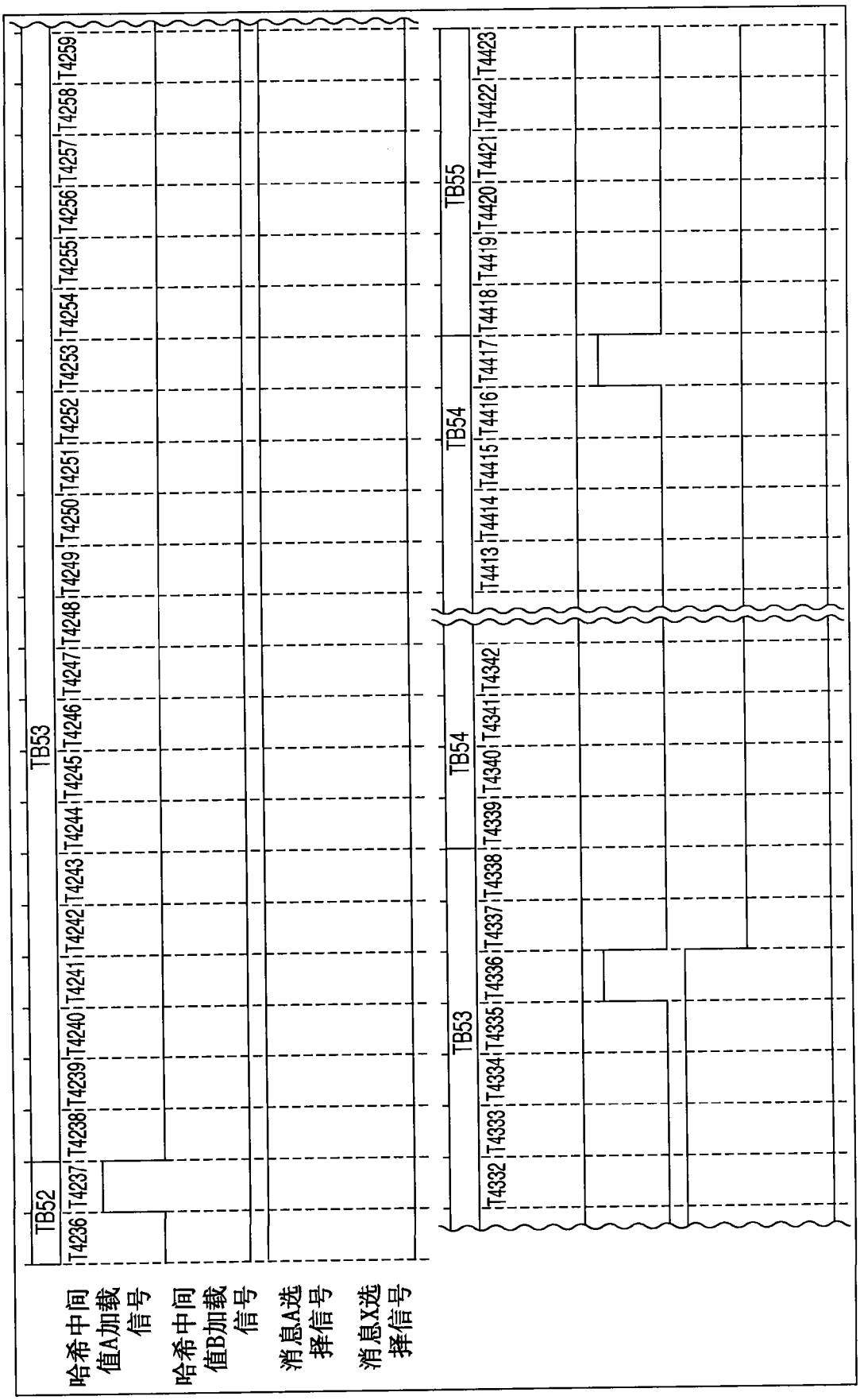

哈希中间值A加载信号
哈希中间值B加载信号
消息A选择信号
消息X选择信号
TB52
TB53
TB54
TB55
T4236 T4237 T4238 T4239 T4240 T4241 T4242 T4243 T4244 T4245 T4246 T4247 T4248 T4249 T4250 T4251 T4252 T4253 T4254 T4255 T4256 T4257 T4258 T4259
T4332 T4333 T4334 T4335 T4336 T4337 T4338 T4339 T4340 T4341 T4342
T4413 T4414 T4415 T4416 T4417 T4418 T4419 T4420 T4421 T4422 T4423

图 22F

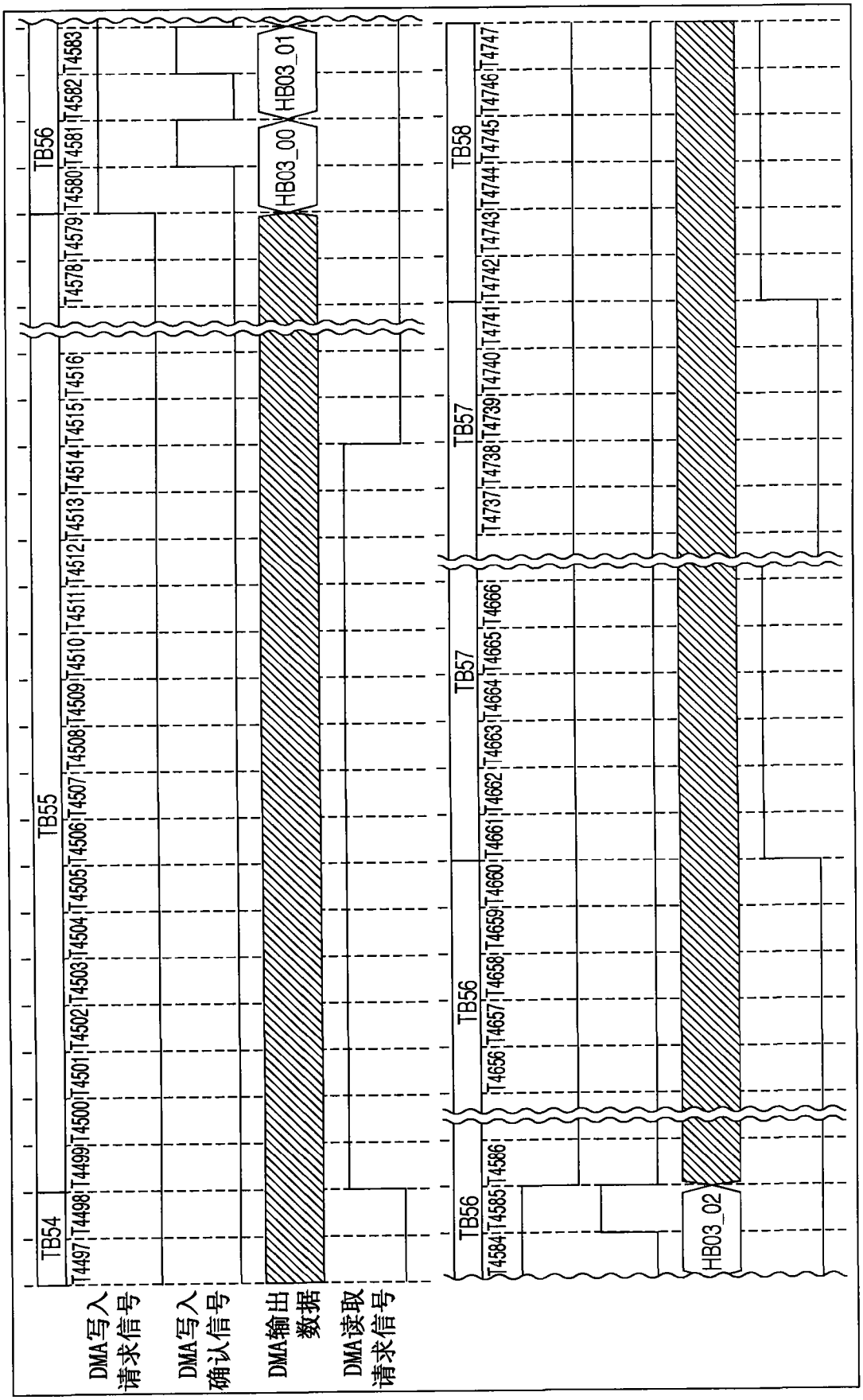

DMA写入请求信号
DMA写入确认信号
DMA输出数据
DMA读取请求信号
TB54
TB55
TB56
TB57
TB58
HB03_00
HB03_01
HB03_02
T4497 T4498 T4499 T4500 T4501 T4502 T4503 T4504 T4505 T4506 T4507 T4508 T4509 T4510 T4511 T4512 T4513 T4514 T4515 T4516
T4578 T4579 T4580 T4581 T4582 T4583
T4584 T4585 T4586
T4656 T4657 T4658 T4659 T4660 T4661 T4662 T4663 T4664 T4665 T4666
T4737 T4738 T4739 T4740 T4741 T4742 T4743 T4744 T4745 T4746 T4747

图 23A

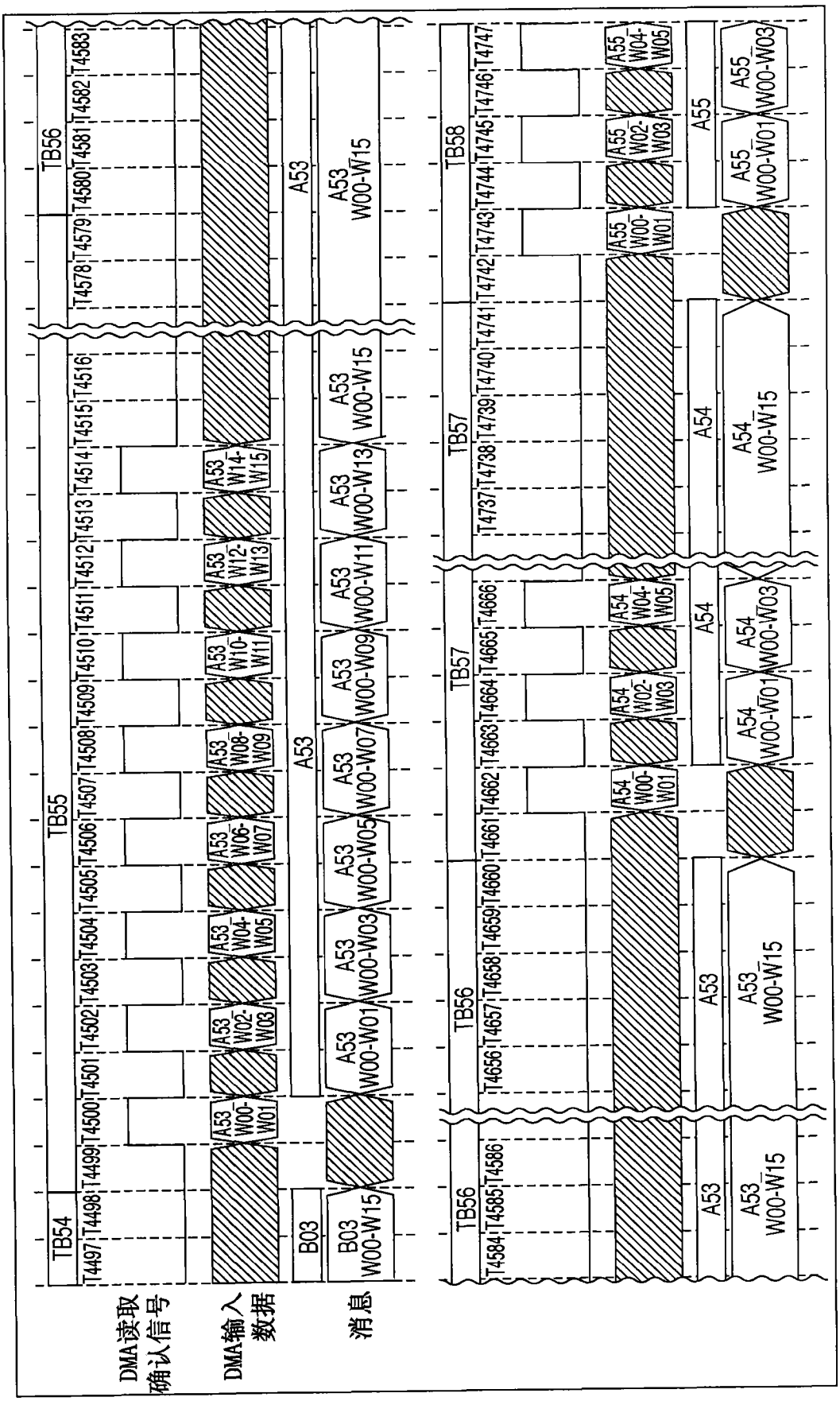

DMA读取确认信号
DMA输入数据
消息
TB54
TB55
TB56
TB57
TB58
A53
A54
A55
B03
T4497
T4498
T4499
T4500
T4501
T4502
T4503
T4504
T4505
T4506
T4507
T4508
T4509
T4510
T4511
T4512
T4513
T4514
T4515
T4516
T4578
T4579
T4580
T4581
T4582
T4583
T4584
T4585
T4586
T4656
T4657
T4658
T4659
T4660
T4661
T4662
T4663
T4664
T4665
T4666
T4737
T4738
T4739
T4740
T4741
T4742
T4743
T4744
T4745
T4746
T4747

图 23B

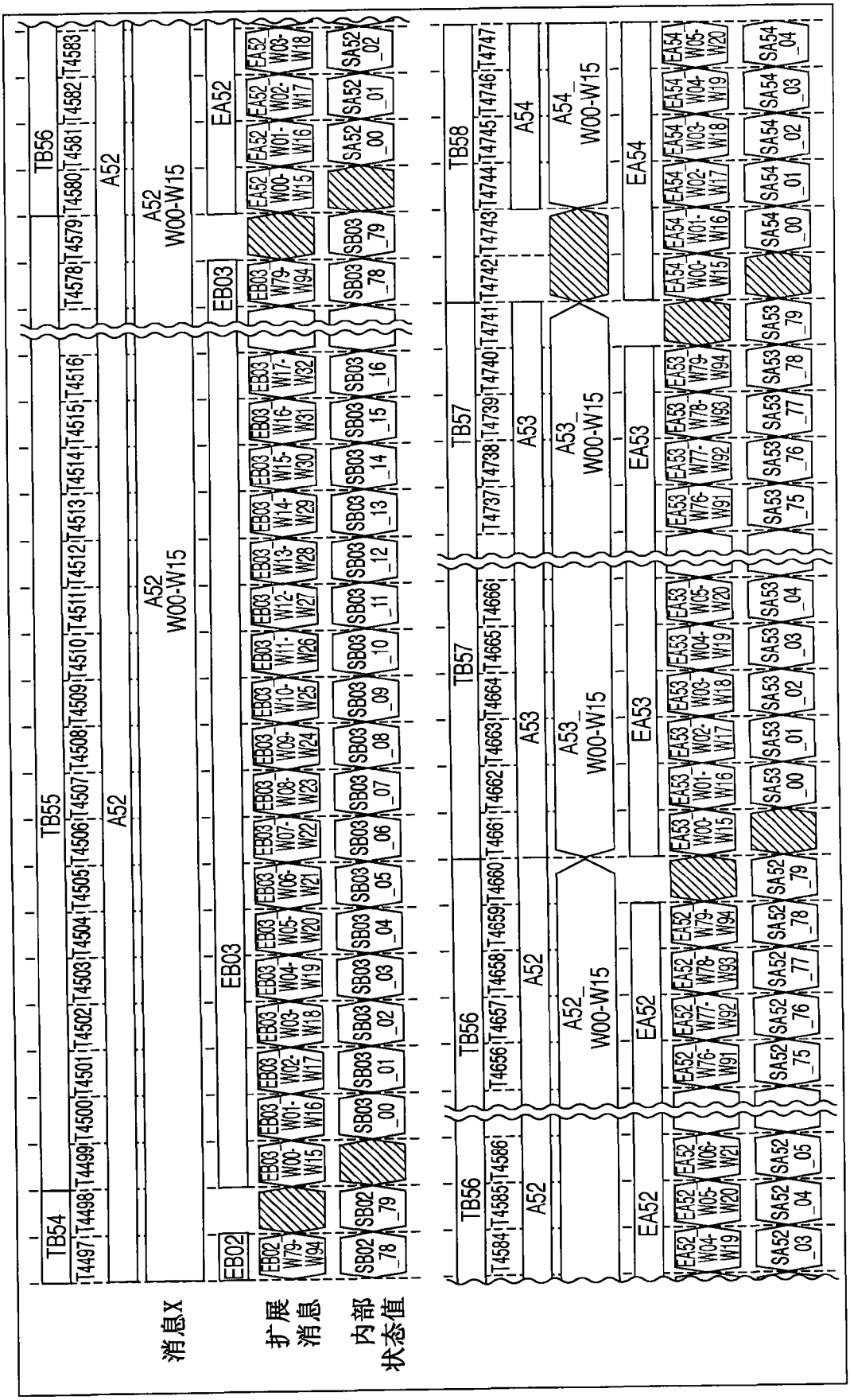

消息X
扩展消息
内部状态值
TB54
TB55
TB56
TB57
TB58
A52
A52 W00-W15
EB03
EB02
EA52
SB03
SB02
SA52
A53
A53_ W00-W15
EA53
SA53
A54
A54_ W00-W15
EA54
SA54

图 23C

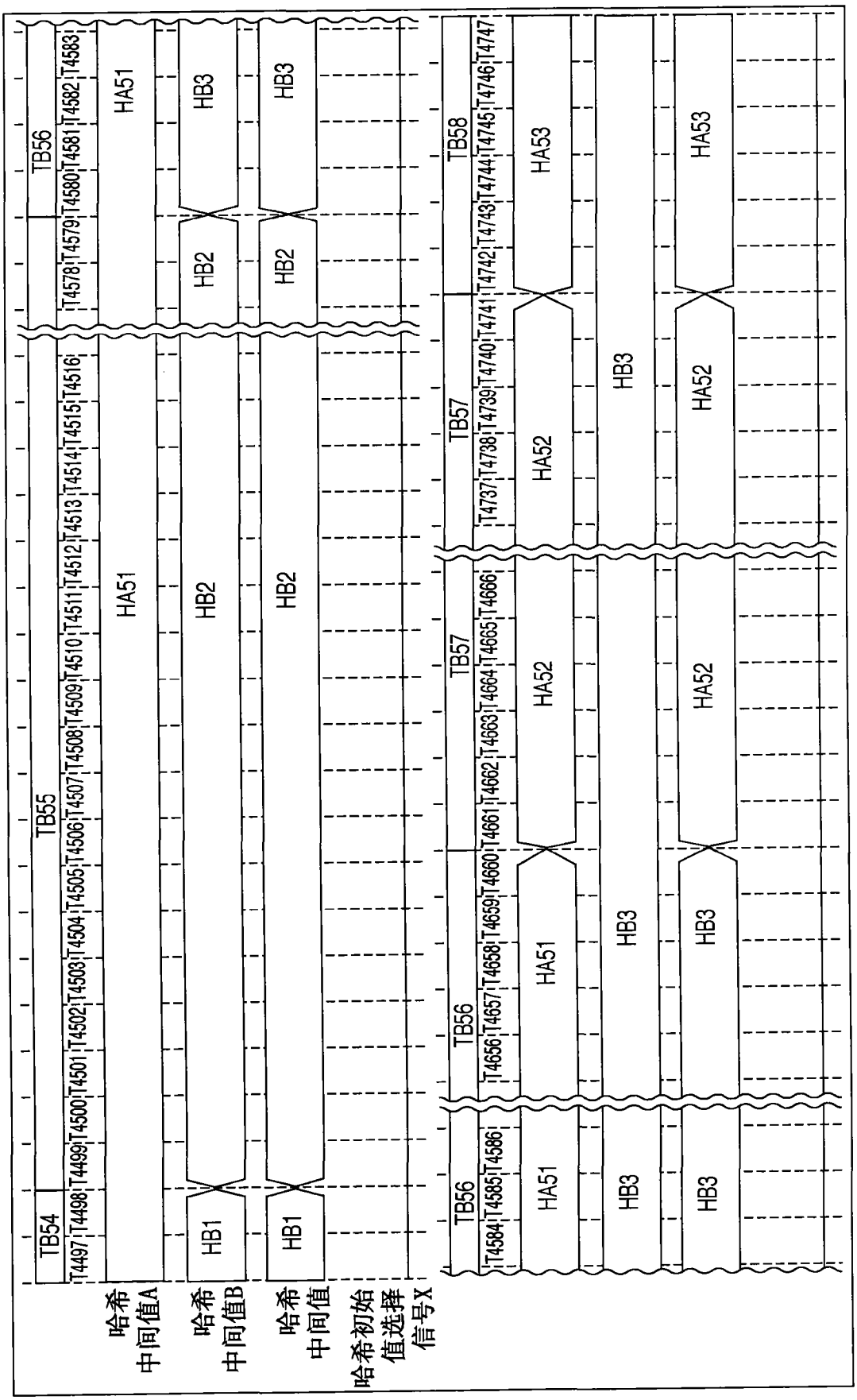

哈希中间值A
哈希中间值B
哈希中间值
哈希初始值选择信号X
TB54
TB55
TB56
TB57
TB58
HA51
HA52
HA53
HB1
HB2
HB3

图 23D

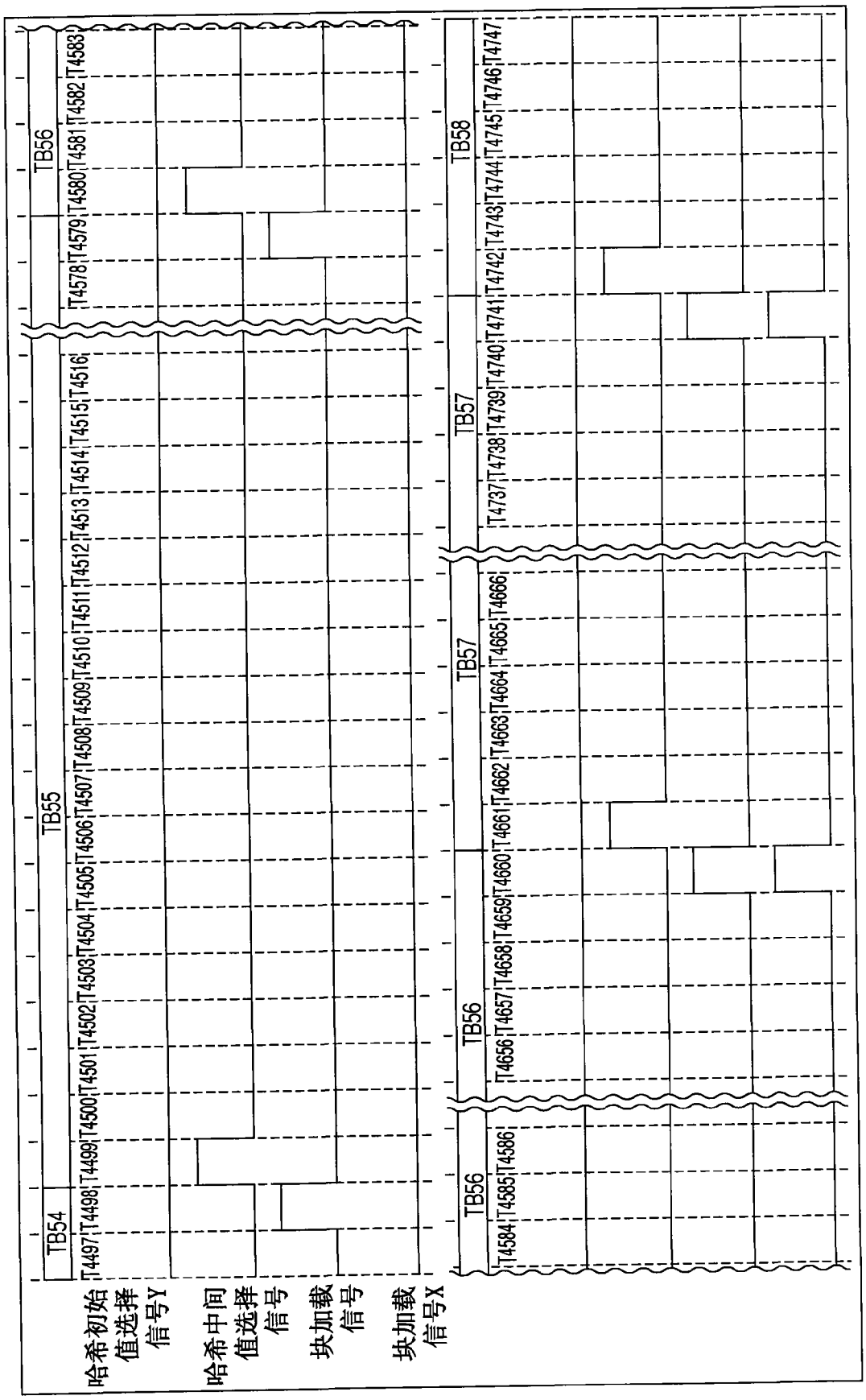

哈希初始值选择信号Y
哈希中间值选择信号
块加载信号
块加载信号X
TB54
TB55
TB56
TB57
TB58
T4497 T4498 T4499 T4500 T4501 T4502 T4503 T4504 T4505 T4506 T4507 T4508 T4509 T4510 T4511 T4512 T4513 T4514 T4515 T4516
T4578 T4579 T4580 T4581 T4582 T4583
T4584 T4585 T4586
T4656 T4657 T4658 T4659 T4660 T4661 T4662 T4663 T4664 T4665 T4666
T4737 T4738 T4739 T4740 T4741 T4742 T4743 T4744 T4745 T4746 T4747

图 23E

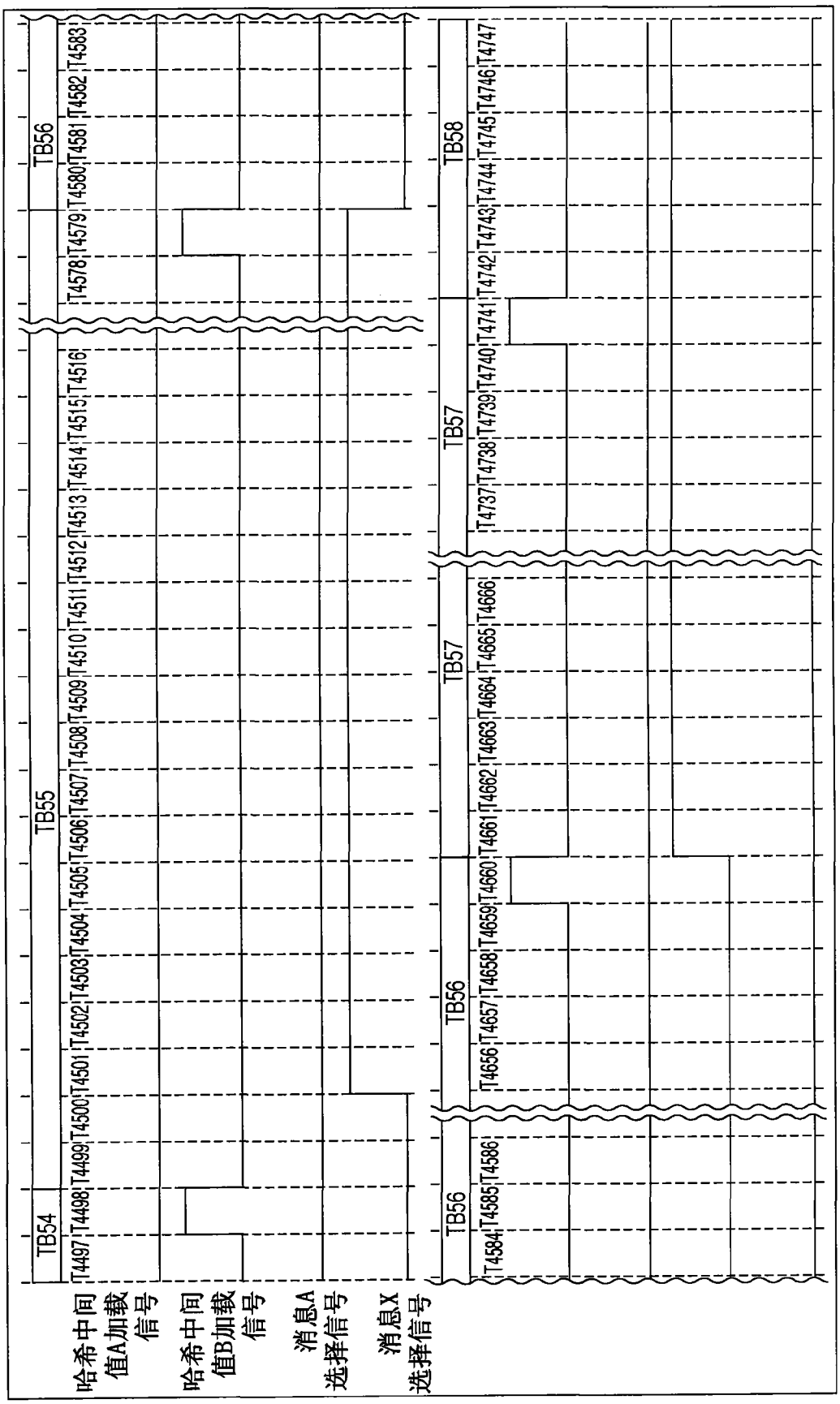

TB54
TB55
TB56
TB56
TB57
TB57
TB58
T4497 T4498 T4499 T4500 T4501 T4502 T4503 T4504 T4505 T4506 T4507 T4508 T4509 T4510 T4511 T4512 T4513 T4514 T4515 T4516
T4578 T4579 T4580 T4581 T4582 T4583
T4584 T4585 T4586
T4656 T4657 T4658 T4659 T4660 T4661 T4662 T4663 T4664 T4665 T4666
T4737 T4738 T4739 T4740 T4741 T4742 T4743 T4744 T4745 T4746 T4747
哈希中间值A加载信号
哈希中间值B加载信号
消息A选择信号
消息X选择信号

图 23F

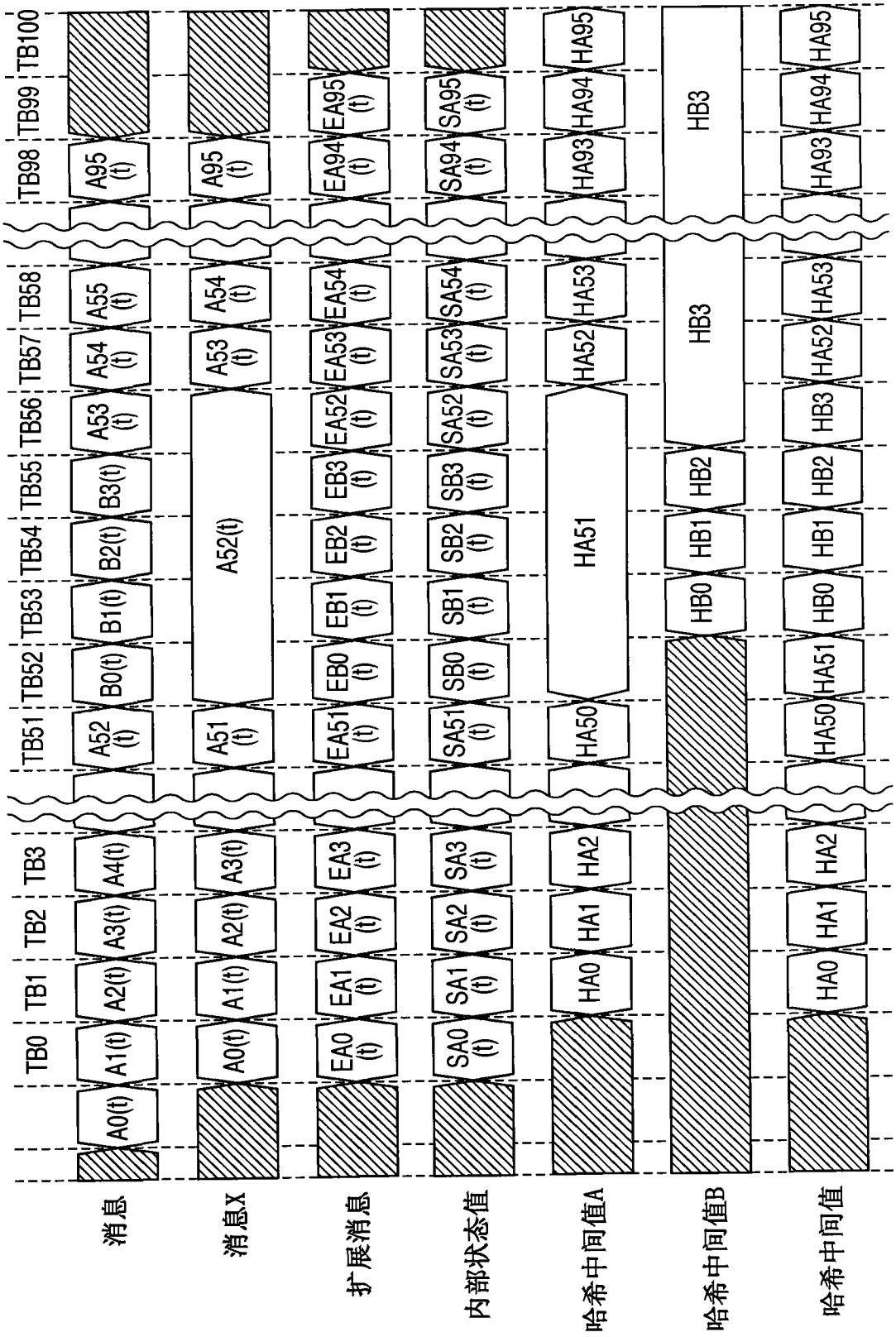

TB0
TB1
TB2
TB3
TB51
TB52
TB53
TB54
TB55
TB56
TB57
TB58
TB98
TB99
TB100
消息
消息X
扩展消息
内部状态值
哈希中间值A
哈希中间值B
哈希中间值

图 24A

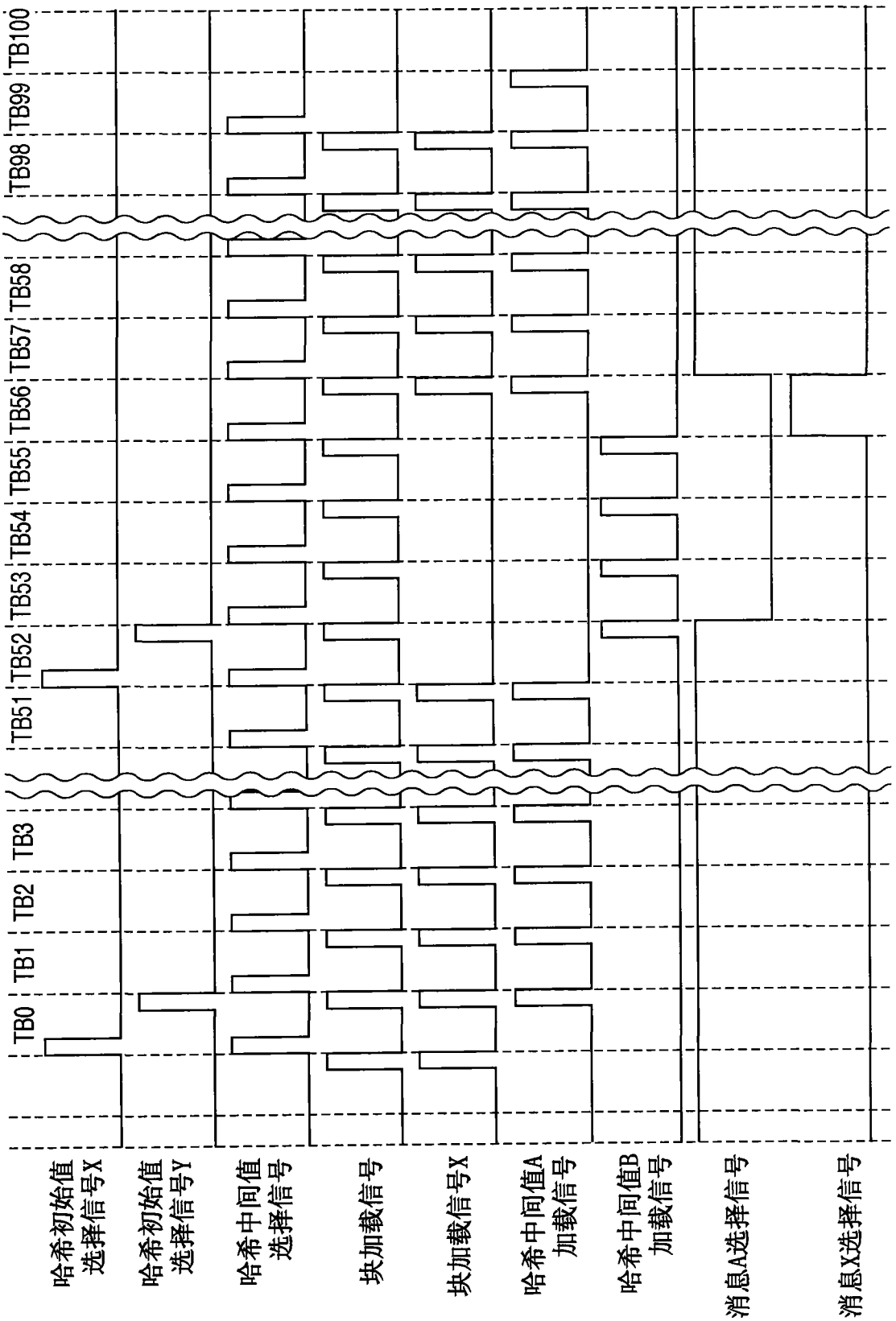

TB0
TB1
TB2
TB3
TB51
TB52
TB53
TB54
TB55
TB56
TB57
TB58
TB98
TB99
TB100
哈希初始值选择信号X
哈希初始值选择信号Y
哈希中间值选择信号
块加载信号
块加载信号X
哈希中间值A加载信号
哈希中间值B加载信号
消息A选择信号
消息X选择信号

图 24B

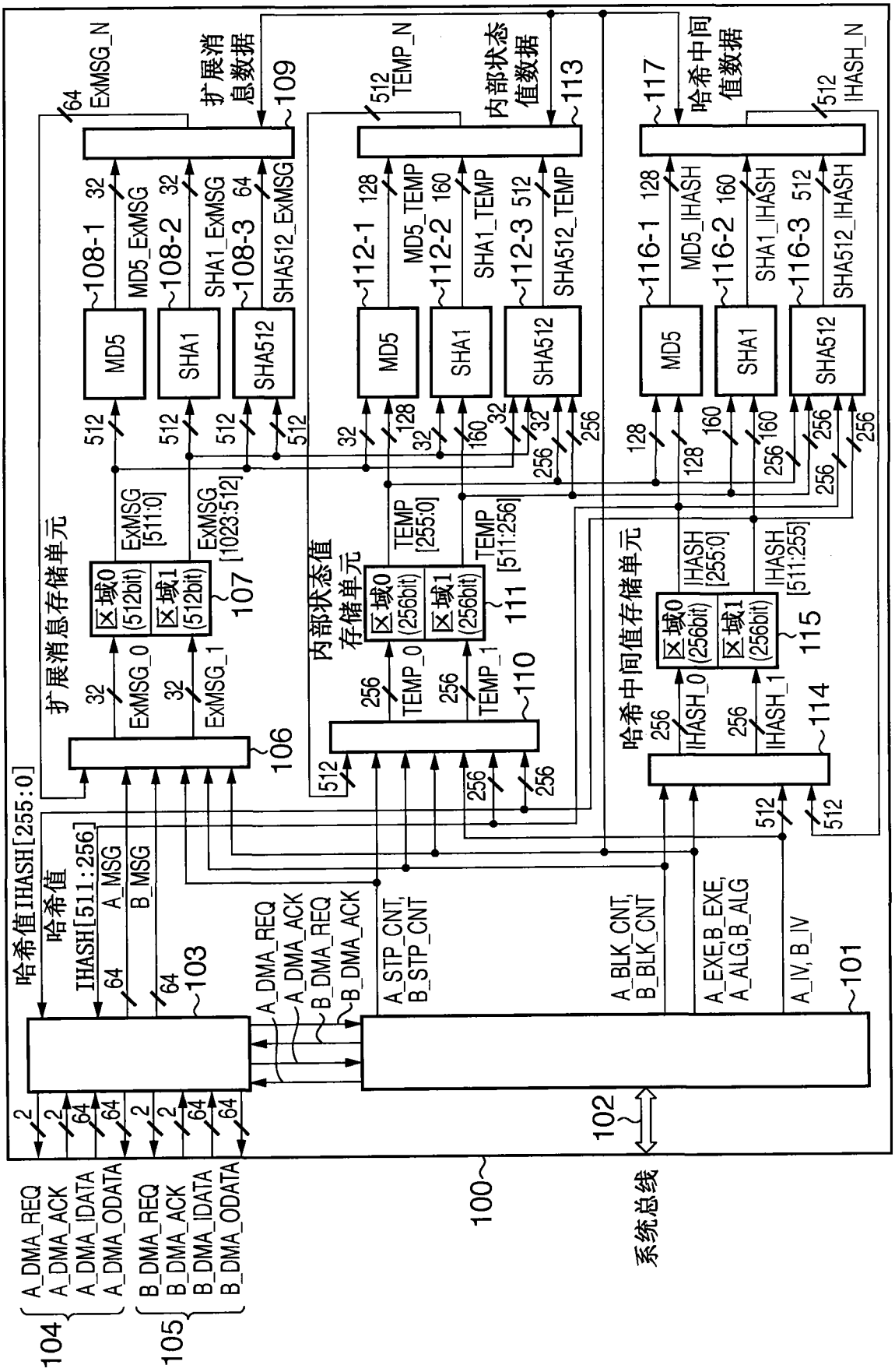

哈希值IHASH[255:0]
哈希值
IHASH[511:256]
A_MSG
B_MSG
103
扩展消息存储单元
106
ExMSG_0
ExMSG_1
区域0 (512bit)
区域1 (512bit)
107
ExMSG [511:0]
ExMSG [1023:512]
ExMSG_N
扩展消息数据
109
MD5
SHA1
SHA512
108-1
108-2
108-3
MD5_ExMSG
SHA1_ExMSG
SHA512_ExMSG
内部状态值存储单元
TEMP_0
TEMP_1
区域0 (256bit)
区域1 (256bit)
110
111
TEMP [255:0]
TEMP [511:256]
TEMP_N
内部状态值数据
113
112-1
112-2
112-3
MD5_TEMP
SHA1_TEMP
SHA512_TEMP
哈希中间值存储单元
IHASH_0
IHASH_1
区域0 (256bit)
区域1 (256bit)
114
115
IHASH [255:0]
IHASH [511:255]
哈希中间值数据
117
116-1
116-2
116-3
MD5_IHASH
SHA1_IHASH
SHA512_IHASH
IHASH_N
A_DMA_REQ
A_DMA_ACK
B_DMA_REQ
B_DMA_ACK
A_STP_CNT, B_STP_CNT
A_BLK_CNT, B_BLK_CNT
A_EXE,B_EXE, A_ALG,B_ALG
A_IV, B_IV
101
102
100
系统总线
104
105
A_DMA_REQ
A_DMA_ACK
A_DMA_IDATA
A_DMA_ODATA
B_DMA_REQ
B_DMA_ACK
B_DMA_IDATA
B_DMA_ODATA

图 25

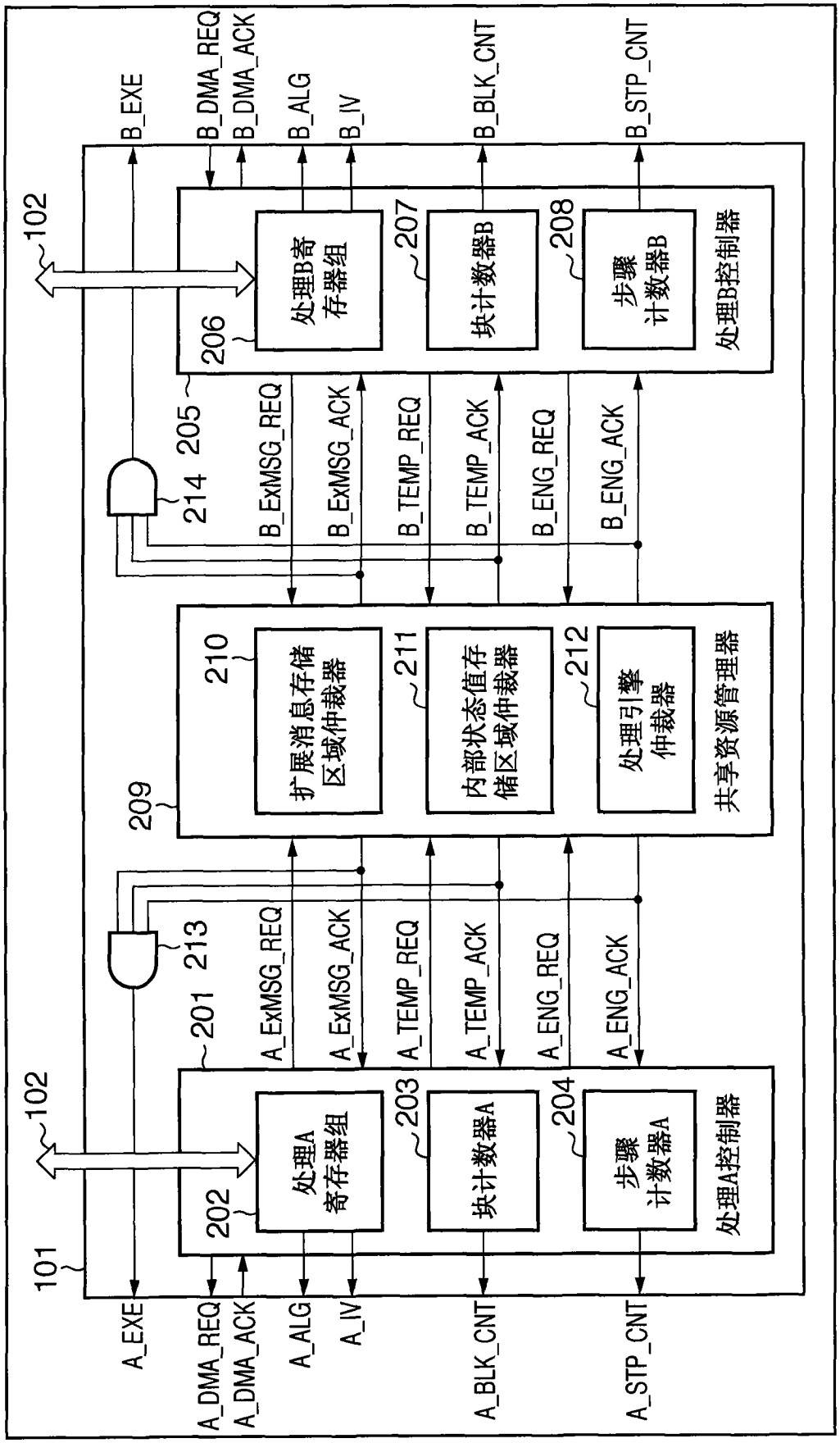

101
102
102
201
202
203
204
205
206
207
208
209
210
211
212
213
214
A_EXE
A_DMA_REQ
A_DMA_ACK
A_ALG
A_IV
A_BLK_CNT
A_STP_CNT
A_ExMSG_REQ
A_ExMSG_ACK
A_TEMP_REQ
A_TEMP_ACK
A_ENG_REQ
A_ENG_ACK
B_EXE
B_DMA_REQ
B_DMA_ACK
B_ALG
B_IV
B_BLK_CNT
B_STP_CNT
B_ExMSG_REQ
B_ExMSG_ACK
B_TEMP_REQ
B_TEMP_ACK
B_ENG_REQ
B_ENG_ACK
处理A寄存器组
块计数器A
步骤计数器A
处理A控制器
处理B寄存器组
块计数器B
步骤计数器B
处理B控制器
扩展消息存储区域仲裁器
内部状态值存储区域仲裁器
处理引擎仲裁器
共享资源管理器

图 26

处理A作业开始设置寄存器

301

Bits	Name	Access	Function
0	A_ENB	R/W	作业开始 在作业结束时自动清零 1:start

处理A哈希算法设置寄存器

302

Bits	Name	Access	Function
1:0	A_ALG	R/W	选择哈希算法 "00" : MD5 "01" : SHA1 "10" : SHA512

处理A块设置寄存器

303

Bits	Name	Access	Function
15:0	A_BLK	R/W	消息数据的块的数量

处理A初始值设置寄存器

304

Bits	Name	Access	Function
511:0	A_IV	R/W	初始值

处理B作业开始设置寄存器

305

Bits	Name	Access	Function
0	B_ENB	R/W	开始作业；在作业结束时自动清零 1:start

处理B哈希算法设置寄存器

306

Bits	Name	Access	Function
1:0	B_ALG	R/W	选择哈希算法 "00" : MD5 "01" : SHA1 "10" : SHA512

处理B块设置寄存器

307

Bits	Name	Access	Function
15:0	B_BLK	R/W	消息数据的块的数量

处理B初始值设置寄存器

308

Bits	Name	Access	Function
511:0	B_IV	R/W	初始值

图 27

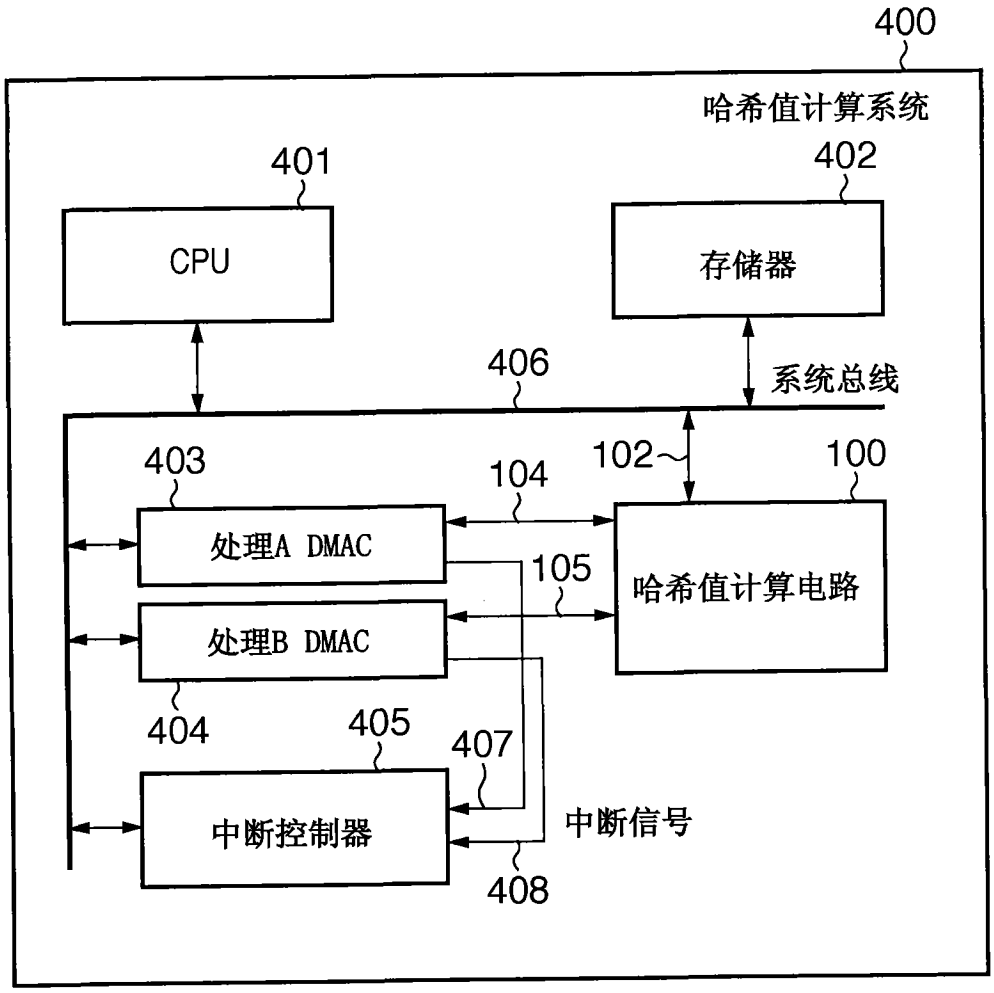

400
哈希值计算系统
401
CPU
402
存储器
406
系统总线
403
102
100
104
处理A DMAC
105
哈希值计算电路
处理B DMAC
404
405
407
中断控制器
中断信号
408

图 28

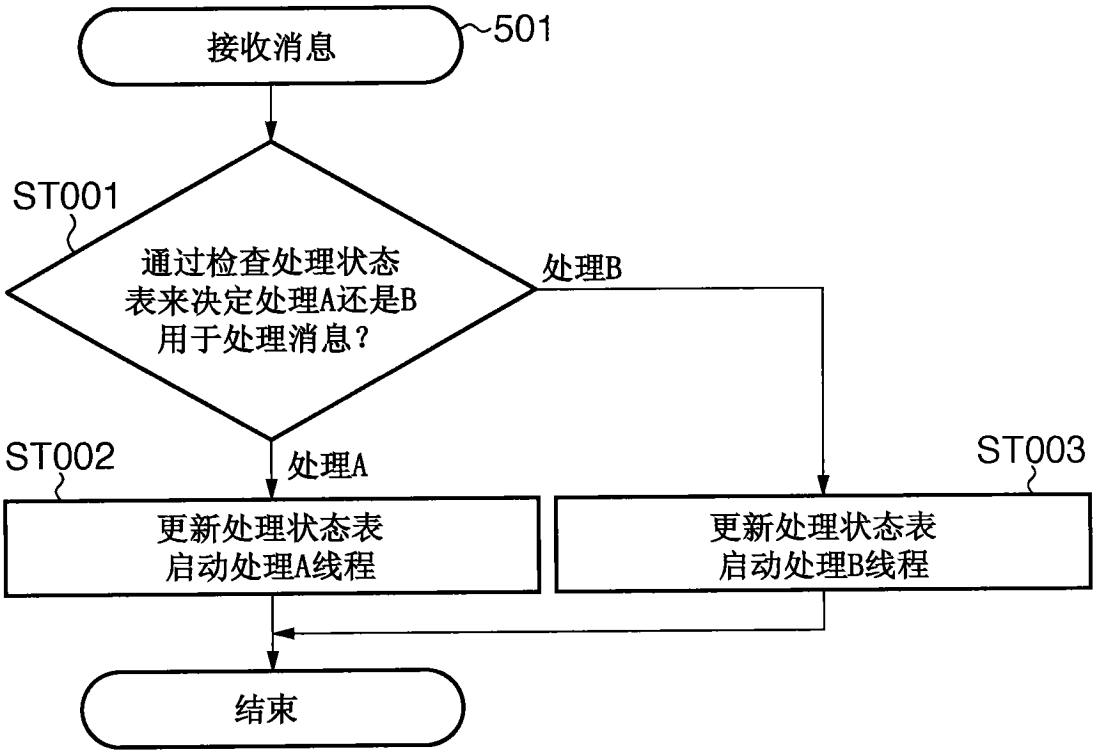

接收消息
501
ST001
通过检查处理状态
表来决定处理A还是B
用于处理消息？
处理B
处理A
ST002
更新处理状态表
启动处理A线程
ST003
更新处理状态表
启动处理B线程
结束

图 29A

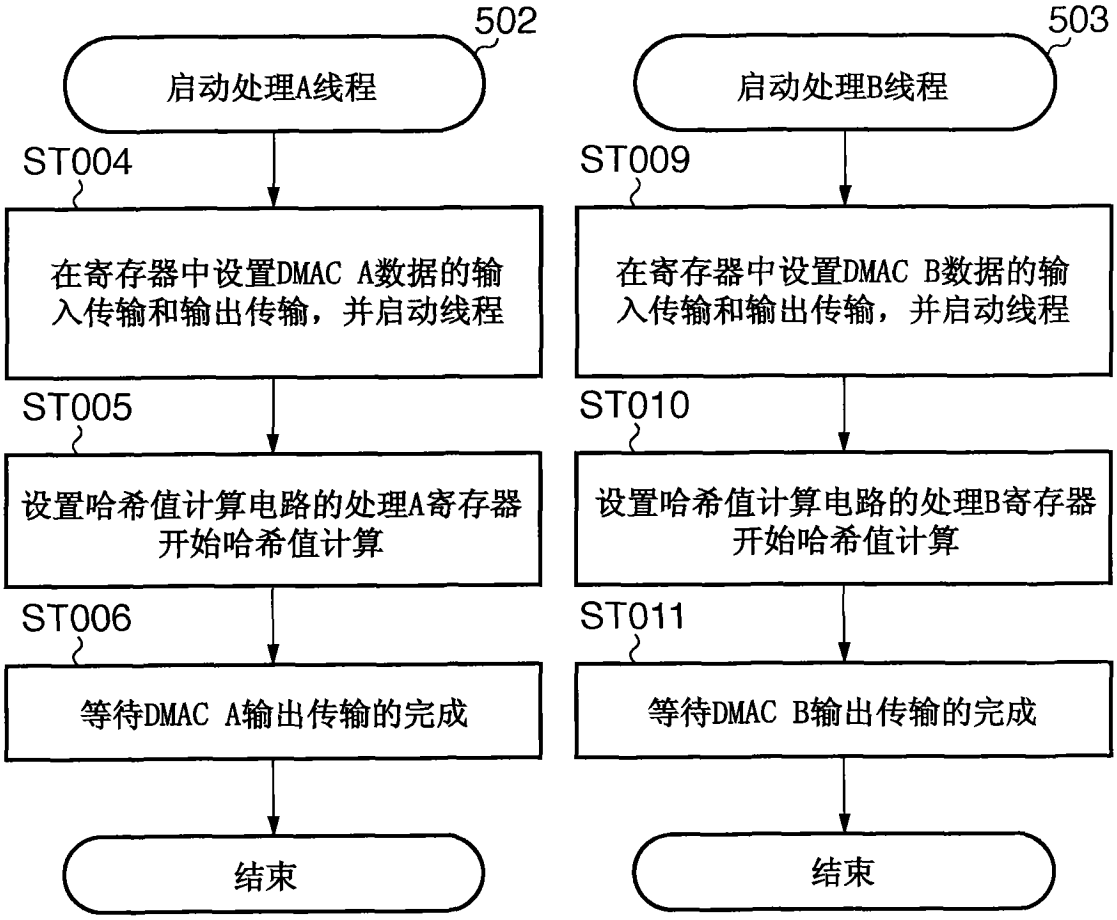

502
启动处理A线程
ST004
在寄存器中设置DMAC A数据的输入传输和输出传输，并启动线程
ST005
设置哈希值计算电路的处理A寄存器开始哈希值计算
ST006
等待DMAC A输出传输的完成
结束
503
启动处理B线程
ST009
在寄存器中设置DMAC B数据的输入传输和输出传输，并启动线程
ST010
设置哈希值计算电路的处理B寄存器开始哈希值计算
ST011
等待DMAC B输出传输的完成
结束

图 29B

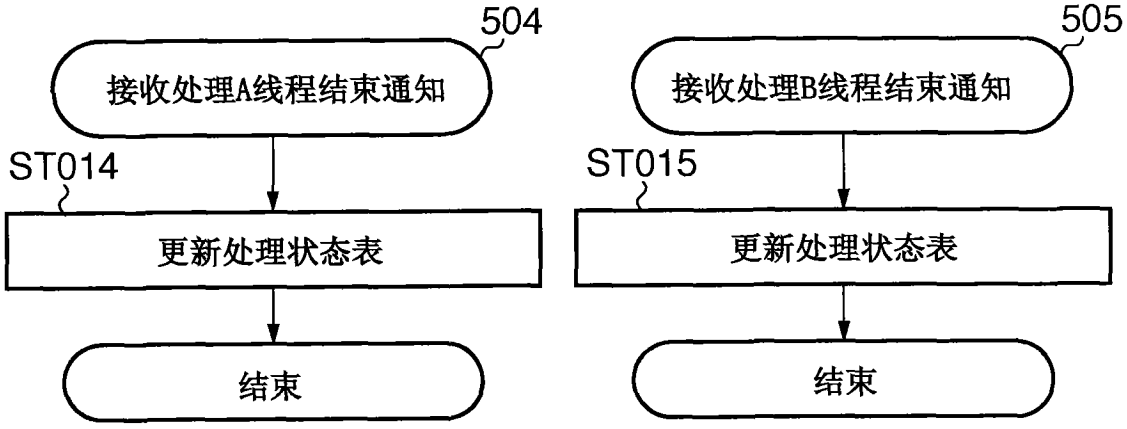

504
接收处理A线程结束通知
ST014
更新处理状态表
结束
505
接收处理B线程结束通知
ST015
更新处理状态表
结束

图 29C

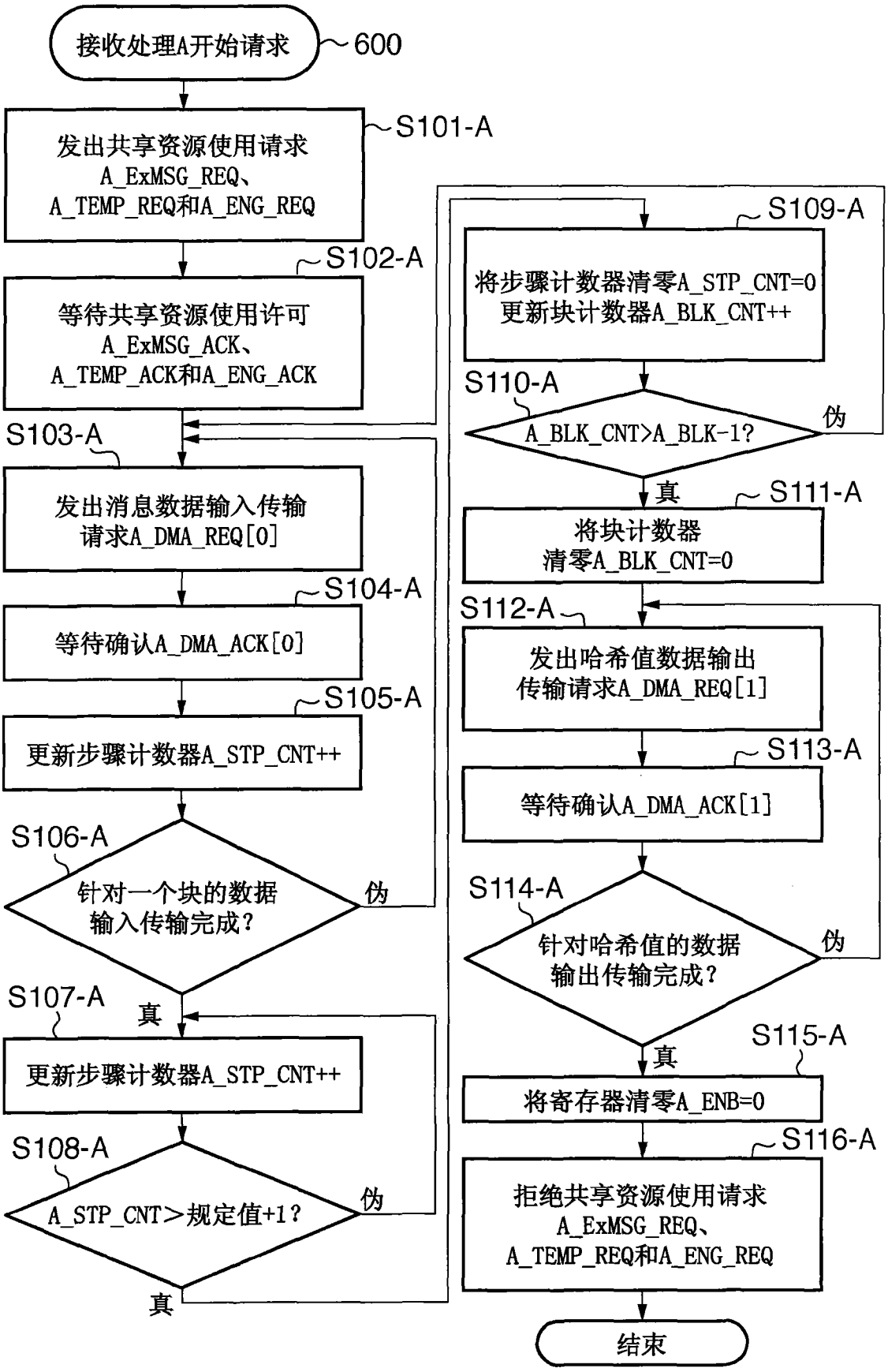

接收处理A开始请求
600
发出共享资源使用请求
A_ExMSG_REQ、
A_TEMP_REQ和A_ENG_REQ
S101-A
等待共享资源使用许可
A_ExMSG_ACK、
A_TEMP_ACK和A_ENG_ACK
S102-A
S103-A
发出消息数据输入传输
请求A_DMA_REQ[0]
S104-A
等待确认A_DMA_ACK[0]
S105-A
更新步骤计数器A_STP_CNT++
S106-A
针对一个块的数据
输入传输完成?
伪
真
S107-A
更新步骤计数器A_STP_CNT++
S108-A
A_STP_CNT>规定值+1?
伪
真
S109-A
将步骤计数器清零A_STP_CNT=0
更新块计数器A_BLK_CNT++
S110-A
A_BLK_CNT>A_BLK-1?
伪
真
S111-A
将块计数器
清零A_BLK_CNT=0
S112-A
发出哈希值数据输出
传输请求A_DMA_REQ[1]
S113-A
等待确认A_DMA_ACK[1]
S114-A
针对哈希值的数据
输出传输完成?
伪
真
S115-A
将寄存器清零A_ENB=0
S116-A
拒绝共享资源使用请求
A_ExMSG_REQ、
A_TEMP_REQ和A_ENG_REQ
结束

图 30A

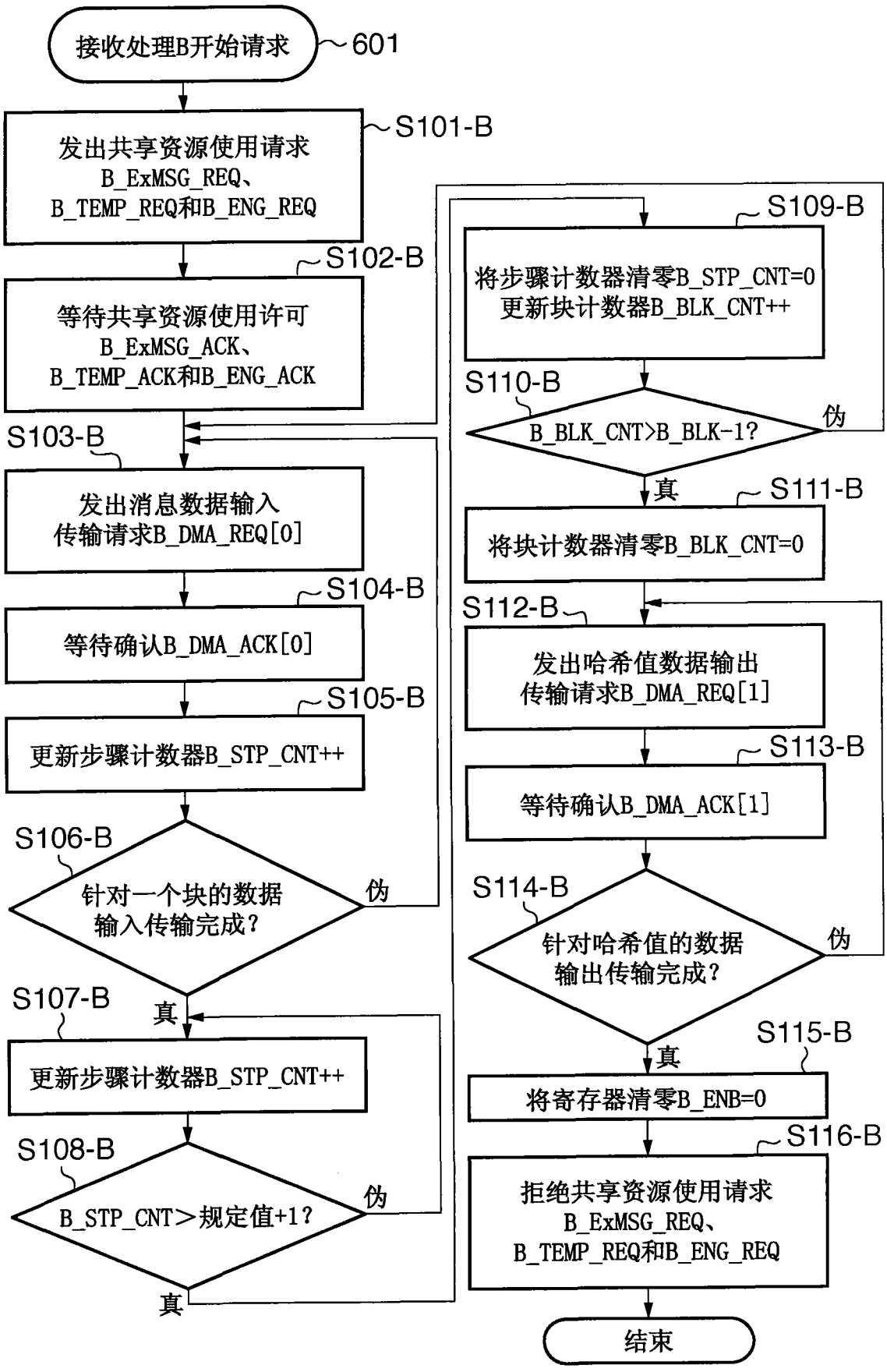

接收处理B开始请求
601
发出共享资源使用请求
B_ExMSG_REQ、
B_TEMP_REQ和B_ENG_REQ
S101-B
等待共享资源使用许可
B_ExMSG_ACK、
B_TEMP_ACK和B_ENG_ACK
S102-B
S103-B
发出消息数据输入
传输请求B_DMA_REQ[0]
S104-B
等待确认B_DMA_ACK[0]
S105-B
更新步骤计数器B_STP_CNT++
S106-B
针对一个块的数据
输入传输完成？
伪
真
S107-B
更新步骤计数器B_STP_CNT++
S108-B
B_STP_CNT＞规定值+1？
伪
真
S109-B
将步骤计数器清零B_STP_CNT=0
更新块计数器B_BLK_CNT++
S110-B
B_BLK_CNT>B_BLK-1?
伪
真
S111-B
将块计数器清零B_BLK_CNT=0
S112-B
发出哈希值数据输出
传输请求B_DMA_REQ[1]
S113-B
等待确认B_DMA_ACK[1]
S114-B
针对哈希值的数据
输出传输完成？
伪
真
S115-B
将寄存器清零B_ENB=0
S116-B
拒绝共享资源使用请求
B_ExMSG_REQ、
B_TEMP_REQ和B_ENG_REQ
结束

图 30B

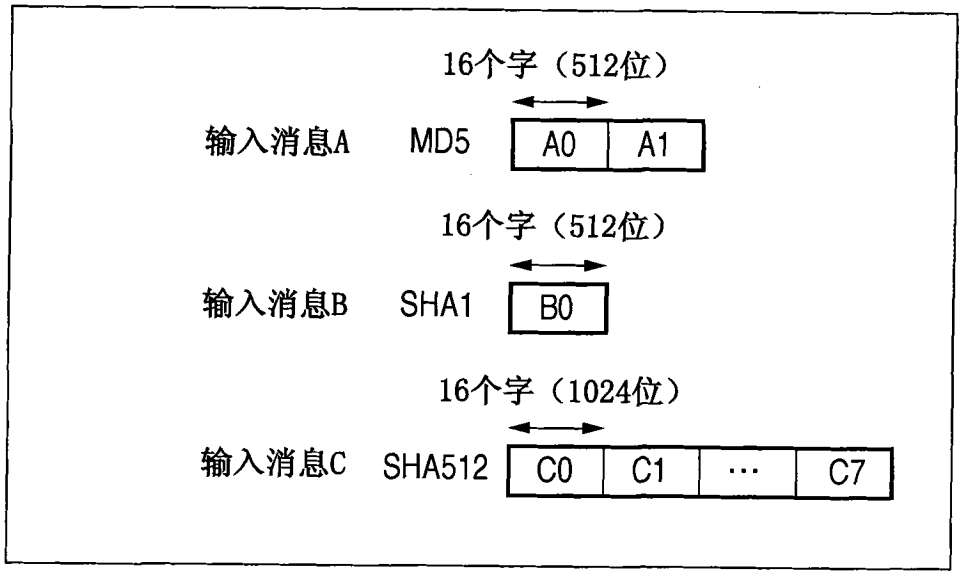

16个字（512位）
输入消息A
MD5
A0
A1
16个字（512位）
输入消息B
SHA1
B0
16个字（1024位）
输入消息C
SHA512
C0
C1
…
C7

图 31

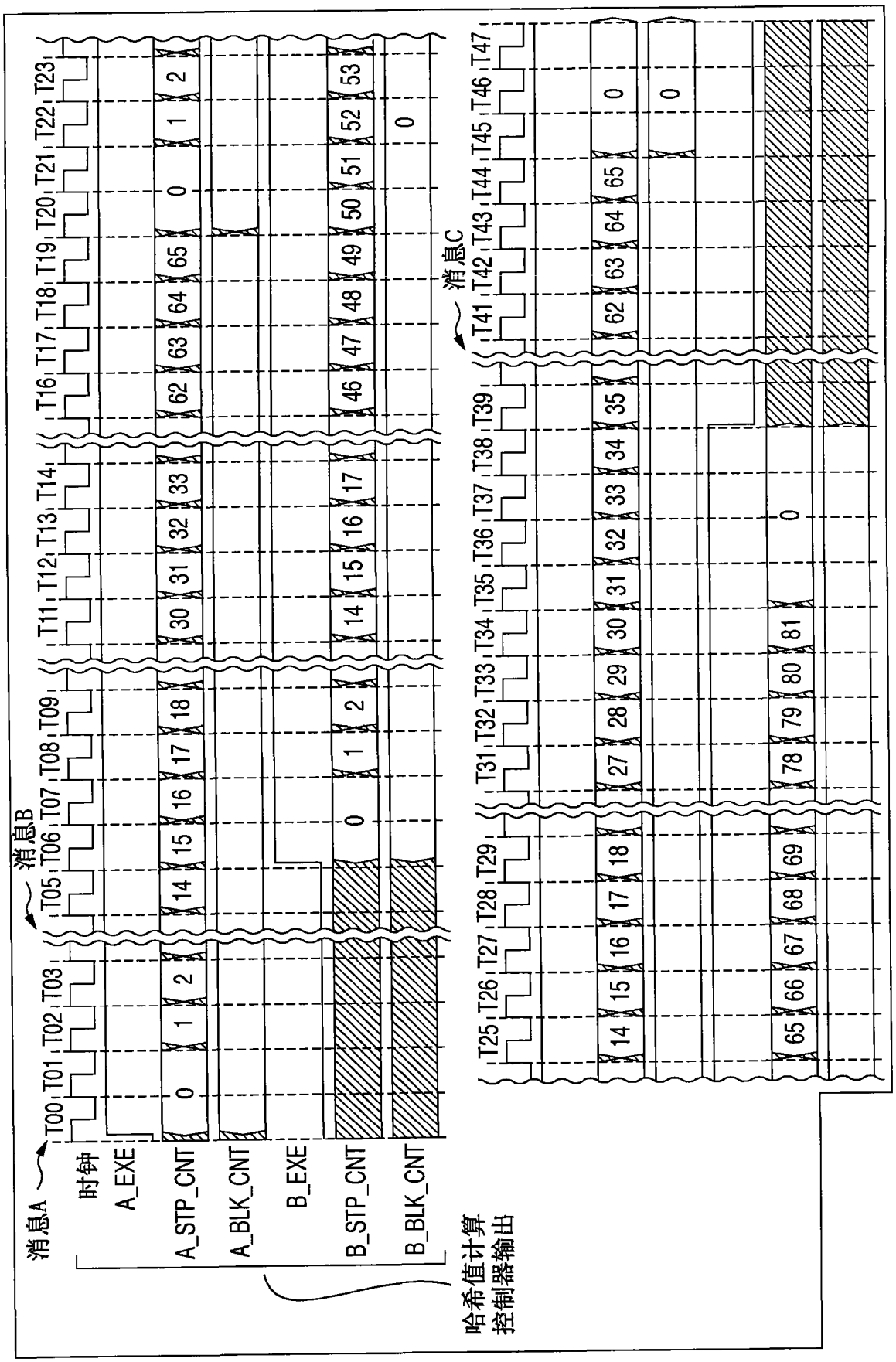

消息A
消息B
消息C
时钟
A_EXE
A_STP_CNT
A_BLK_CNT
B_EXE
B_STP_CNT
B_BLK_CNT
哈希值计算控制器输出
T00 T01 T02 T03 T05 T06 T07 T08 T09 T11 T12 T13 T14 T16 T17 T18 T19 T20 T21 T22 T23
T25 T26 T27 T28 T29 T31 T32 T33 T34 T35 T36 T37 T38 T39 T41 T42 T43 T44 T45 T46 T47

图 32A

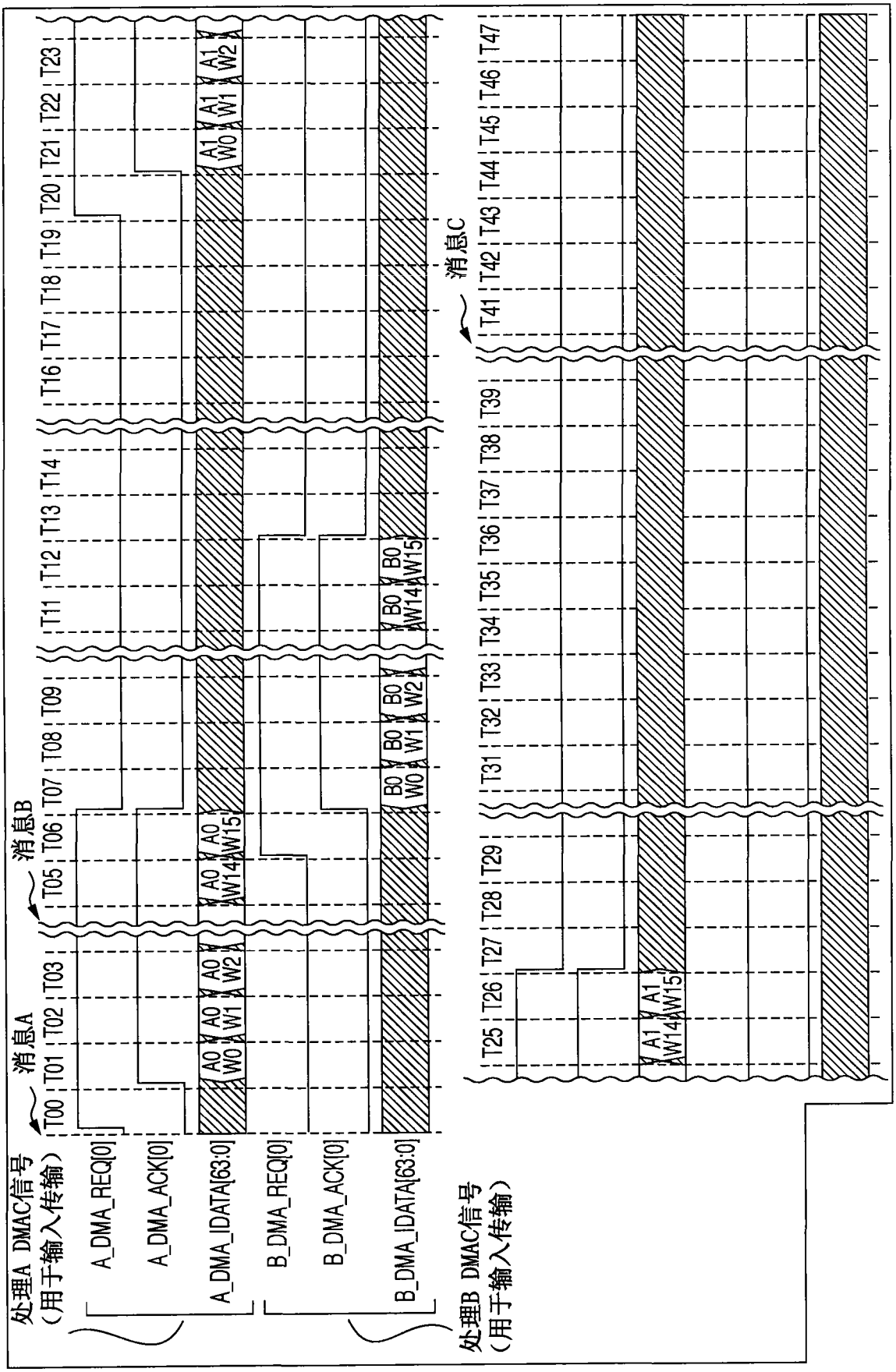

处理A DMAC信号
（用于输入传输）
A_DMA_REQ[0]
A_DMA_ACK[0]
A_DMA_IDATA[63:0]
B_DMA_REQ[0]
B_DMA_ACK[0]
B_DMA_IDATA[63:0]
处理B DMAC信号
（用于输入传输）
消息A
消息B
消息C
T00 T01 T02 T03 T05 T06 T07 T08 T09 T11 T12 T13 T14 T16 T17 T18 T19 T20 T21 T22 T23 T25 T26 T27 T28 T29 T31 T32 T33 T34 T35 T36 T37 T38 T39 T41 T42 T43 T44 T45 T46 T47
A0 W0
A0 W1
A0 W2
A0 W14
A0 W15
A1 W0
A1 W1
A1 W2
A1 W14
A1 W15
B0 W0
B0 W1
B0 W2
B0 W14
B0 W15

图 32B

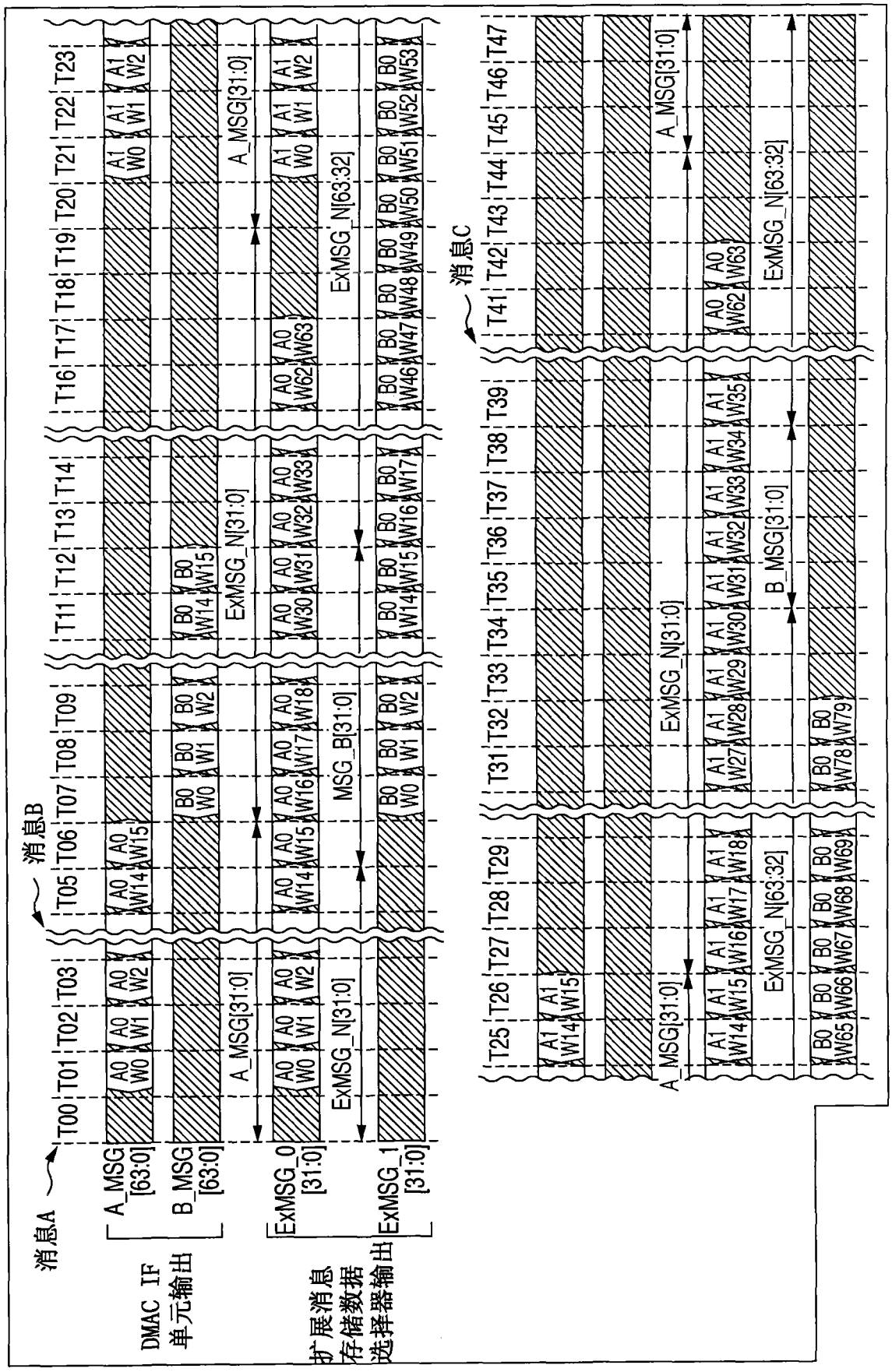

消息A
消息B
消息C
DMAC IF
单元输出
扩展消息
存储数据
选择器输出
A_MSG
[63:0]
B_MSG
[63:0]
ExMSG_0
[31:0]
ExMSG_1
[31:0]
A_MSG[31:0]
B_MSG[31:0]
ExMSG_N[31:0]
ExMSG_N[63:32]

图 32C

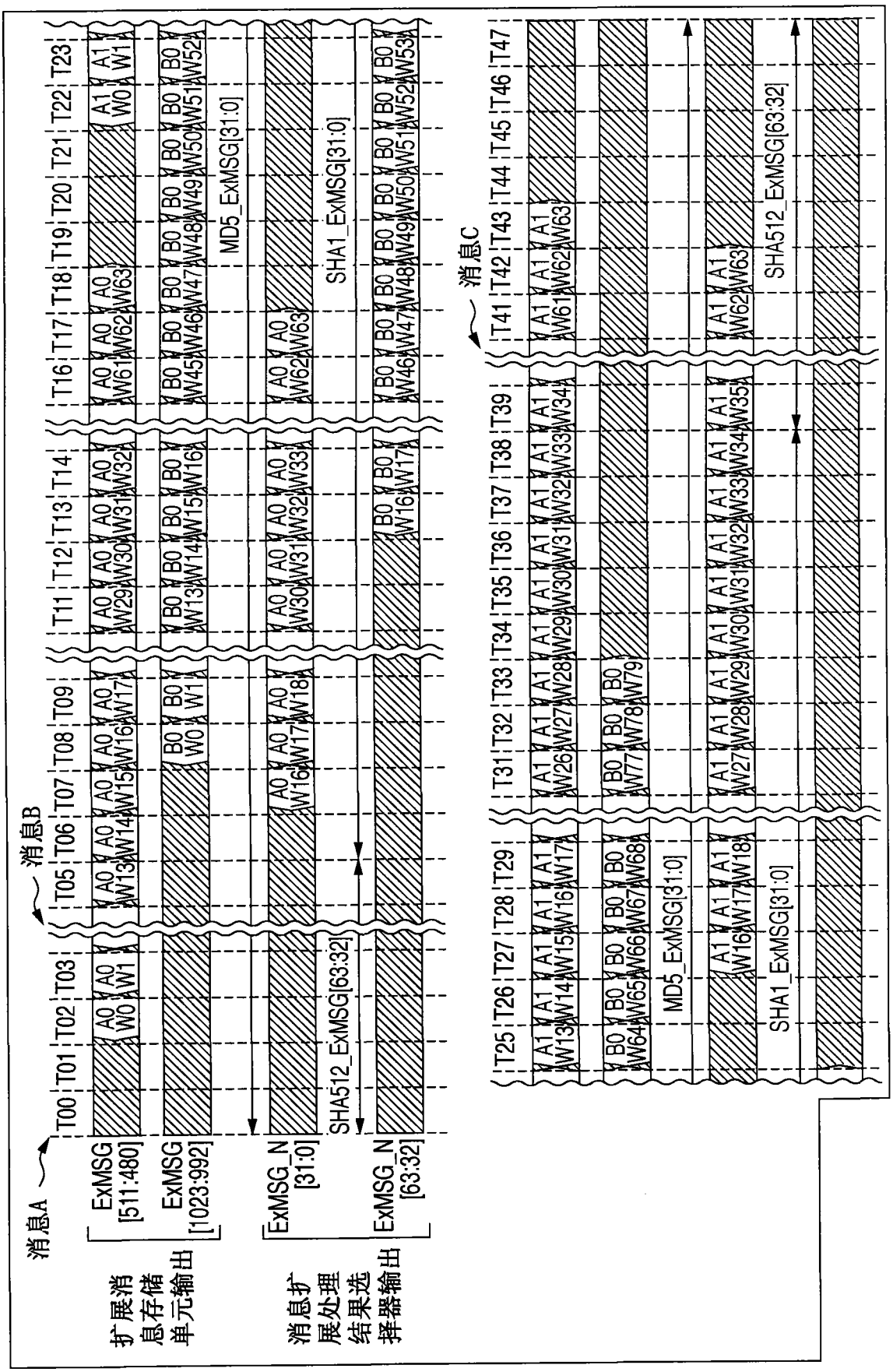

消息A
消息B
消息C
扩展消息存储单元输出
消息扩展处理结果选择器输出
ExMSG [511:480]
ExMSG [1023:992]
ExMSG_N [31:0]
ExMSG_N [63:32]
SHA512_ExMSG[63:32]
MD5_ExMSG[31:0]
SHA1_ExMSG[31:0]
SHA512_ExMSG[63:32]

图 32D

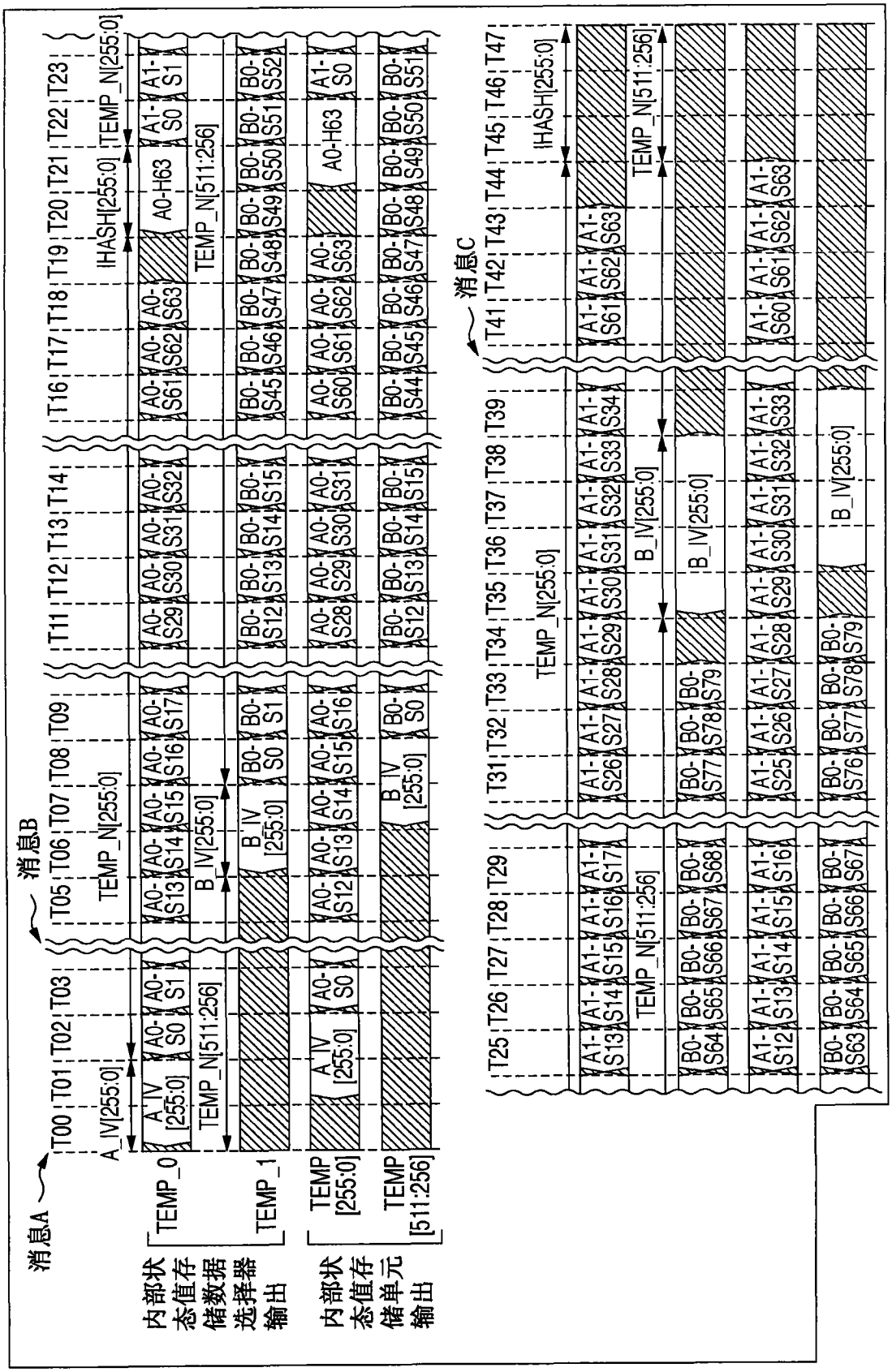

消息A
消息B
消息C
T00 T01 T02 T03 T05 T06 T07 T08 T09 T11 T12 T13 T14 T16 T17 T18 T19 T20 T21 T22 T23
T25 T26 T27 T28 T29 T31 T32 T33 T34 T35 T36 T37 T38 T39 T41 T42 T43 T44 T45 T46 T47
A_IV[255:0]
TEMP_N[255:0]
IHASH[255:0]
TEMP_N[511:256]
B_IV[255:0]
TEMP_0
TEMP_1
TEMP [255:0]
TEMP [511:256]
内部状态值存储数据选择器输出
内部状态值单元输出

图 32E

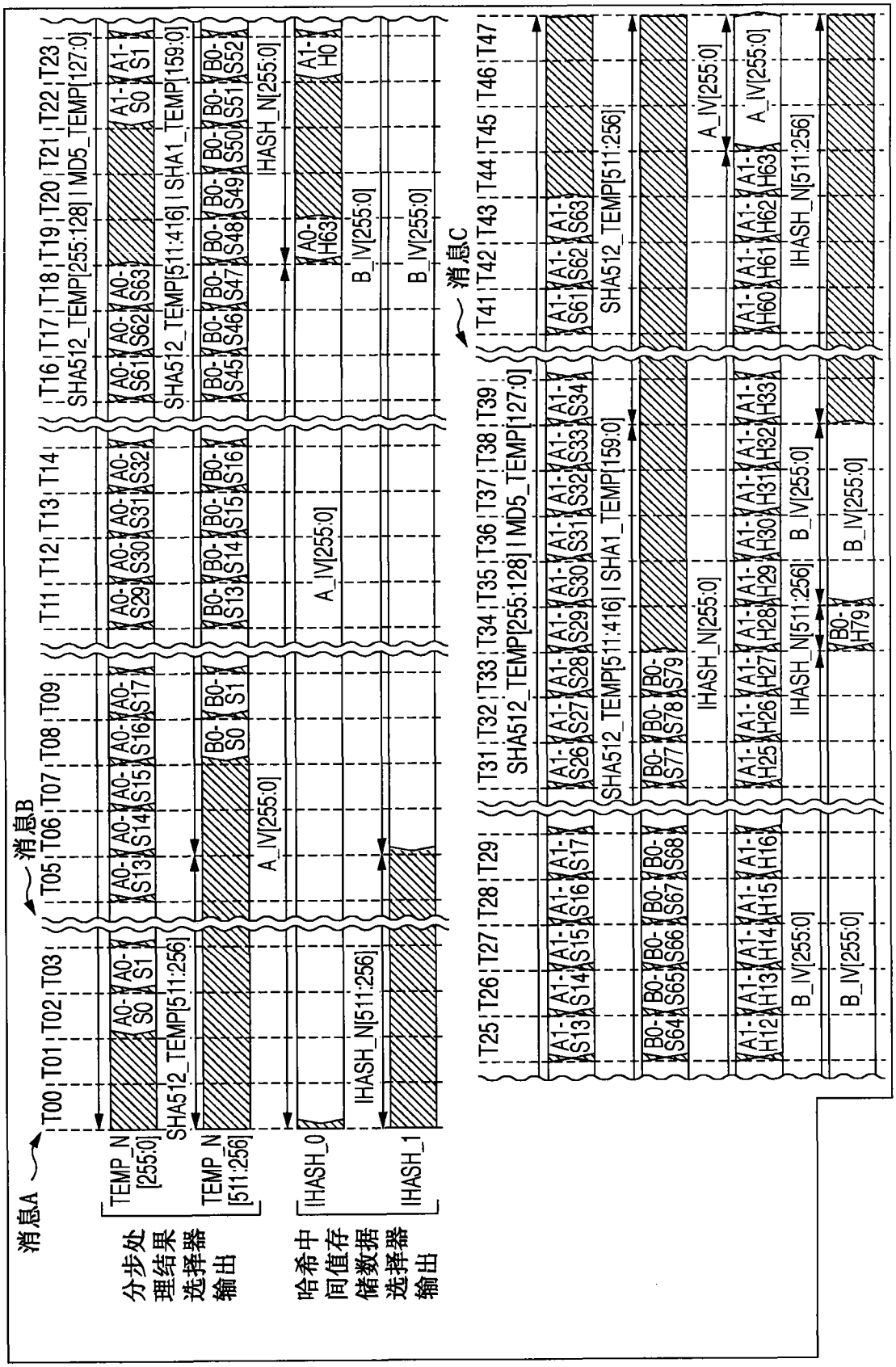

消息A
消息B
消息C
T00 T01 T02 T03 T05 T06 T07 T08 T09 T11 T12 T13 T14 T16 T17 T18 T19 T20 T21 T22 T23
T25 T26 T27 T28 T29 T31 T32 T33 T34 T35 T36 T37 T38 T39 T41 T42 T43 T44 T45 T46 T47
TEMP_N [255:0]
TEMP_N [511:256]
IHASH_0
IHASH_1
SHA512_TEMP[511:256]
SHA512_TEMP[255:128]
MD5_TEMP[127:0]
SHA512_TEMP[511:416]
SHA1_TEMP[159:0]
IHASH_N[255:0]
IHASH_N[511:256]
A_IV[255:0]
B_IV[255:0]
分步处理结果选择器输出
哈希中间值存储数据选择器输出

图 32F

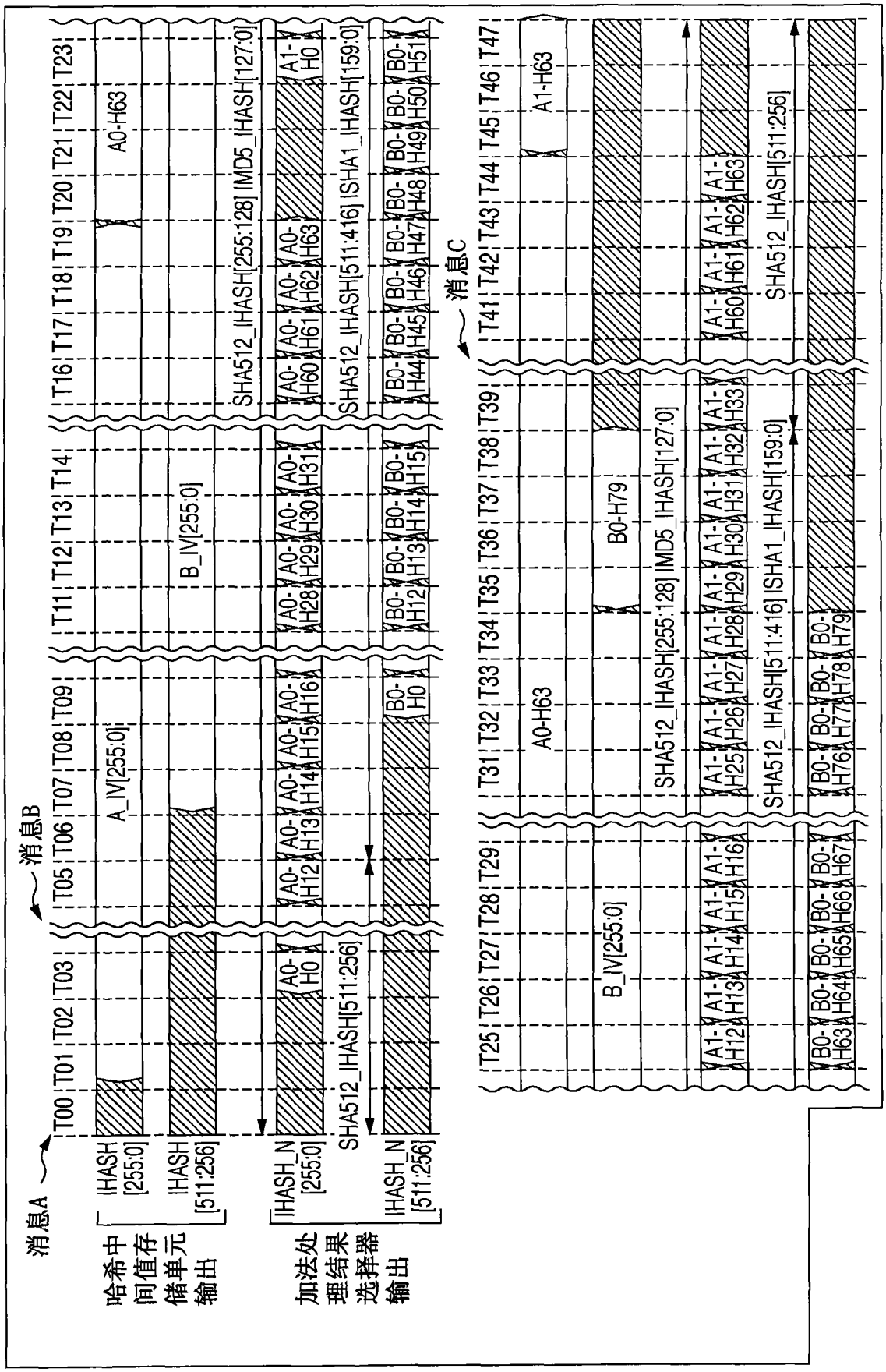

消息A
消息B
消息C
哈希中间值存储单元输出
加法处理结果选择器输出
IHASH[255:0]
IHASH[511:256]
IHASH_N[255:0]
IHASH_N[511:256]
T00 T01 T02 T03 T05 T06 T07 T08 T09 T11 T12 T13 T14 T16 T17 T18 T19 T20 T21 T22 T23
T25 T26 T27 T28 T29 T31 T32 T33 T34 T35 T36 T37 T38 T39 T41 T42 T43 T44 T45 T46 T47
A_IV[255:0]
B_IV[255:0]
A0-H63
A1-H63
B0-H79
SHA512_IHASH[255:128] IMD5_IHASH[127:0]
SHA512_IHASH[511:416] ISHA1_IHASH[159:0]
SHA512_IHASH[511:256]
SHA512_IHASH[159:0] ISHA1_IHASH[511:416]

图 32G

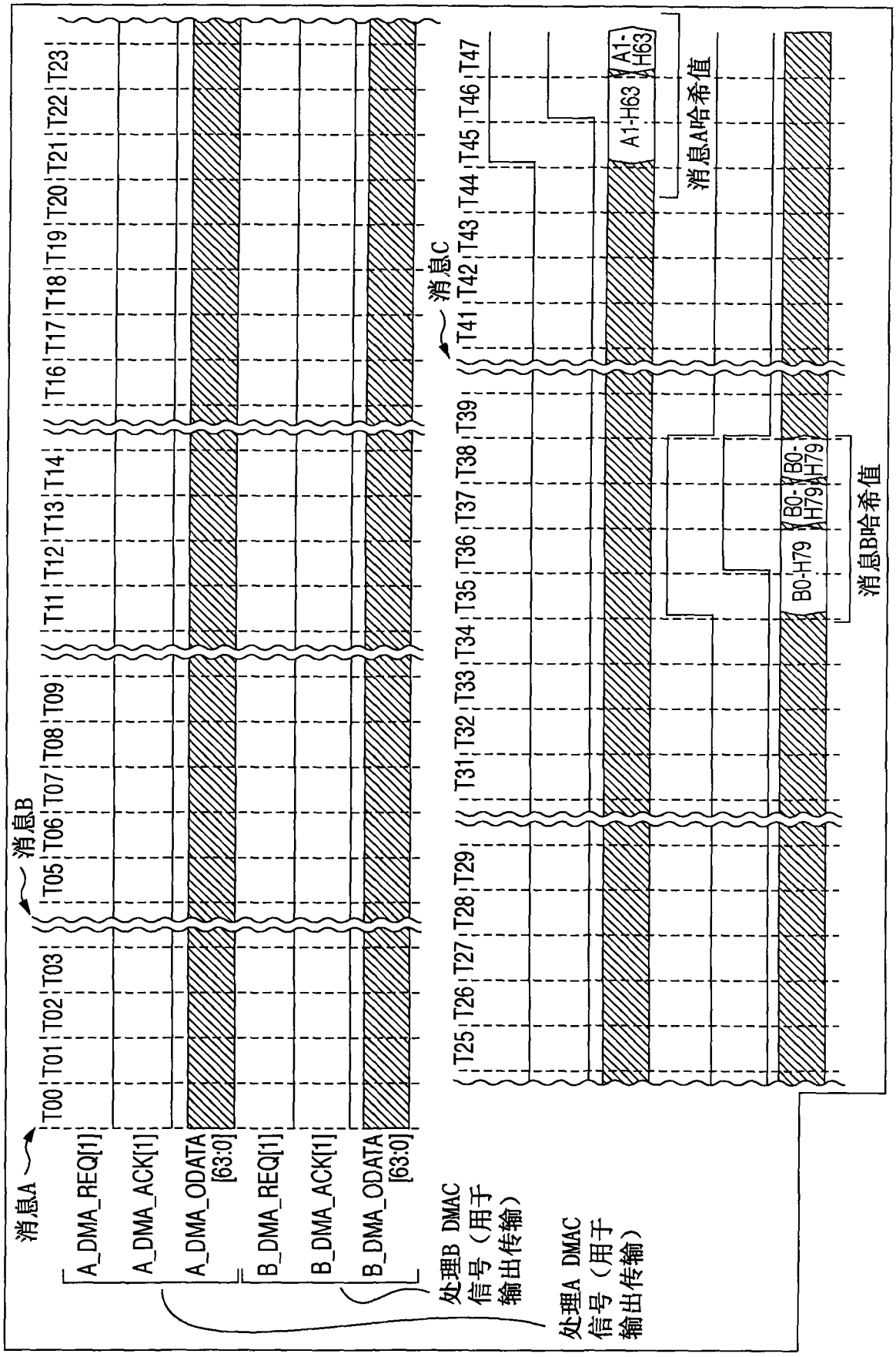

消息A
消息B
消息C
T00 T01 T02 T03 T05 T06 T07 T08 T09 T11 T12 T13 T14 T16 T17 T18 T19 T20 T21 T22 T23
T25 T26 T27 T28 T29 T31 T32 T33 T34 T35 T36 T37 T38 T39 T41 T42 T43 T44 T45 T46 T47
A_DMA_REQ[1]
A_DMA_ACK[1]
A_DMA_ODATA [63:0]
B_DMA_REQ[1]
B_DMA_ACK[1]
B_DMA_ODATA [63:0]
处理B DMAC 信号（用于输出传输）
处理A DMAC 信号（用于输出传输）
A1-H63
B0-H79
消息A哈希值
消息B哈希值

图 32H

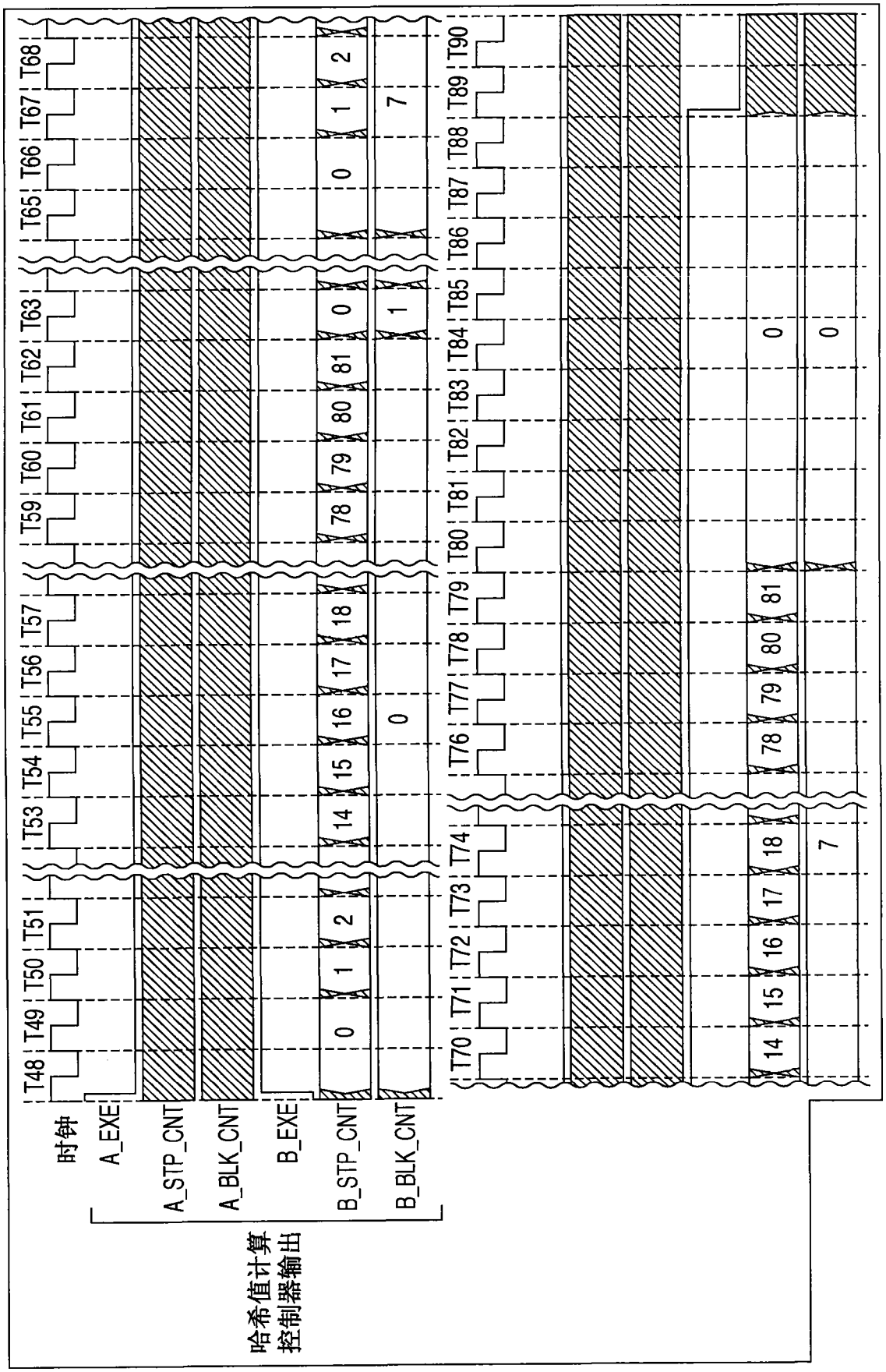

T48 T49 T50 T51 T53 T54 T55 T56 T57 T59 T60 T61 T62 T63 T65 T66 T67 T68 T70 T71 T72 T73 T74 T76 T77 T78 T79 T80 T81 T82 T83 T84 T85 T86 T87 T88 T89 T90
时钟
A_EXE
A_STP_CNT
A_BLK_CNT
B_EXE
B_STP_CNT
B_BLK_CNT
哈希值计算控制器输出
0 1 2 14 15 16 17 18 78 79 80 81 0 1 7 0 14 15 16 17 18 7 78 79 80 81 0 0

图 33A

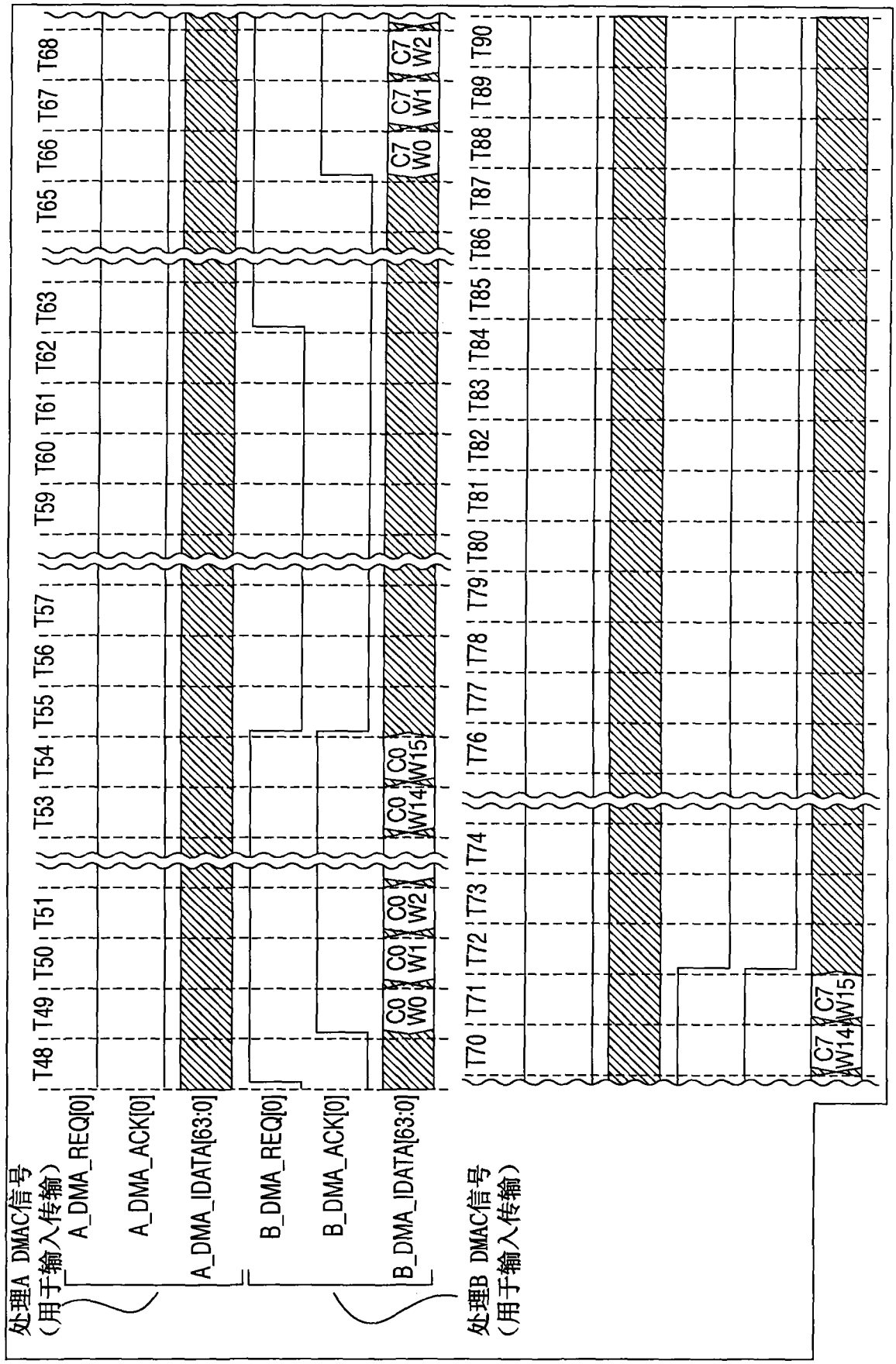

处理A DMAC信号
（用于输入传输）
A_DMA_REQ[0]
A_DMA_ACK[0]
A_DMA_IDATA[63:0]
B_DMA_REQ[0]
B_DMA_ACK[0]
B_DMA_IDATA[63:0]
处理B DMAC信号
（用于输入传输）
T48 T49 T50 T51 T53 T54 T55 T56 T57 T59 T60 T61 T62 T63 T65 T66 T67 T68
T70 T71 T72 T73 T74 T76 T77 T78 T79 T80 T81 T82 T83 T84 T85 T86 T87 T88 T89 T90
C0 W0
C0 W1
C0 W2
C0 W14
C0 W15
C7 W0
C7 W1
C7 W2
C7 W14
C7 W15

图 33B

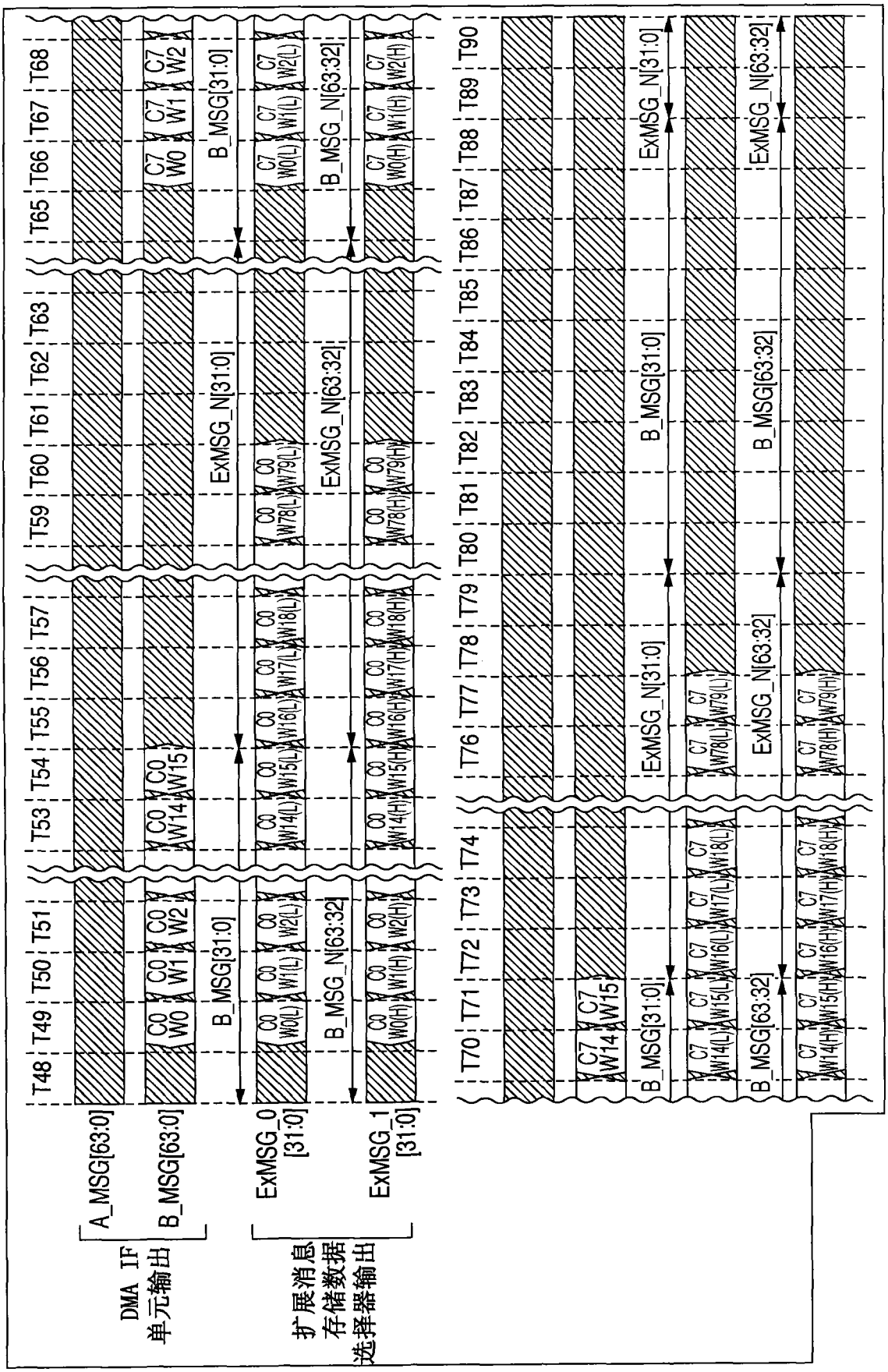

T48 T49 T50 T51 T53 T54 T55 T56 T57 T59 T60 T61 T62 T63 T65 T66 T67 T68
T70 T71 T72 T73 T74 T76 T77 T78 T79 T80 T81 T82 T83 T84 T85 T86 T87 T88 T89 T90
A_MSG[63:0]
B_MSG[63:0]
ExMSG_0 [31:0]
ExMSG_1 [31:0]
DMA IF 单元输出
扩展消息存储数据选择器输出
B_MSG[31:0]
B_MSG_N[63:32]
ExMSG_N[31:0]
ExMSG_N[63:32]

图 33C

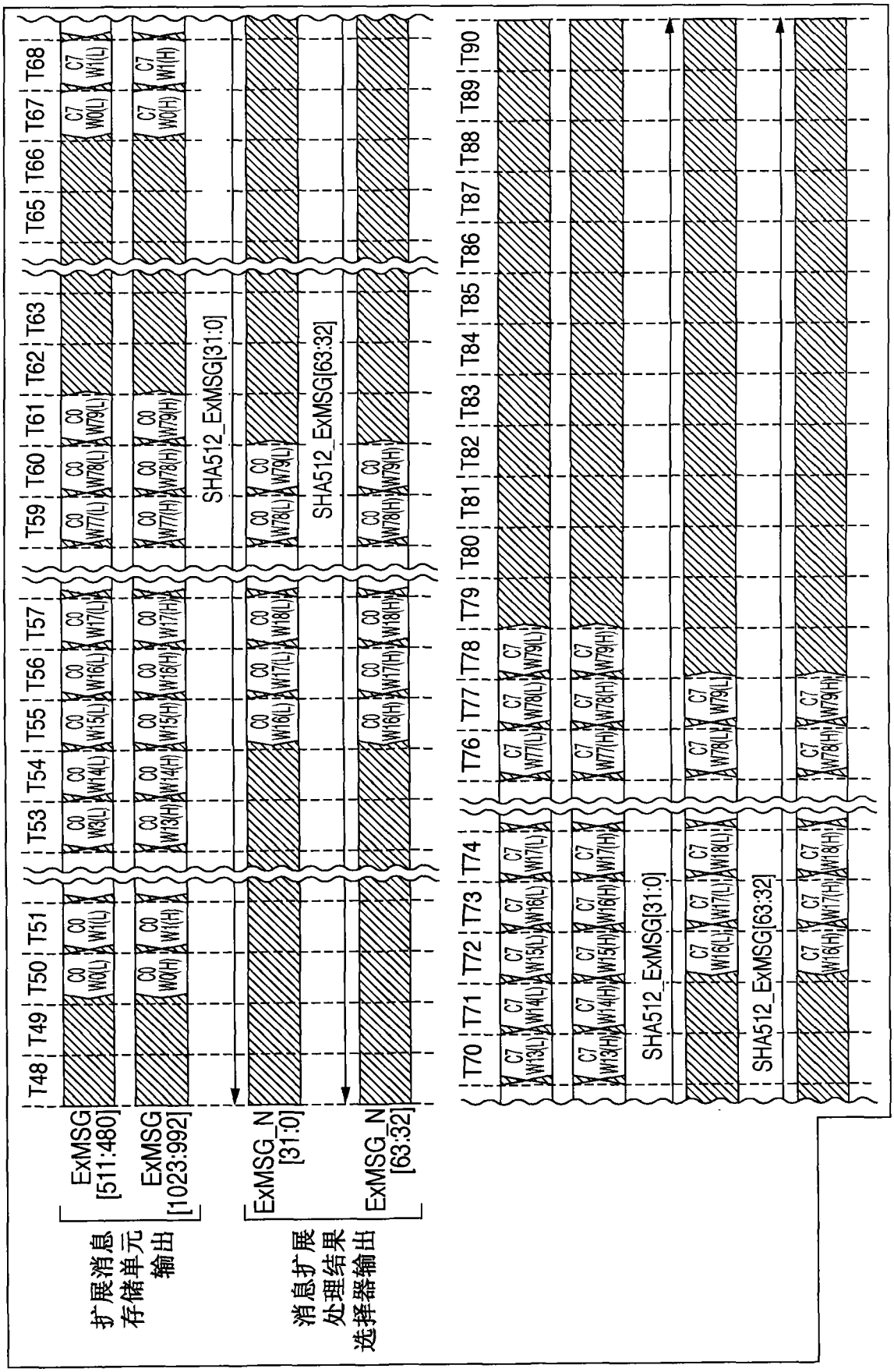

T48 T49 T50 T51 T53 T54 T55 T56 T57 T59 T60 T61 T62 T63 T65 T66 T67 T68
T70 T71 T72 T73 T74 T76 T77 T78 T79 T80 T81 T82 T83 T84 T85 T86 T87 T88 T89 T90
ExMSG [511:480]
ExMSG [1023:992]
ExMSG_N [31:0]
ExMSG_N [63:32]
扩展消息存储单元输出
消息扩展处理结果选择器输出
SHA512_ExMSG[31:0]
SHA512_ExMSG[63:32]
SHA512_ExMSG[31:0]
SHA512_ExMSG[63:32]

图 33D

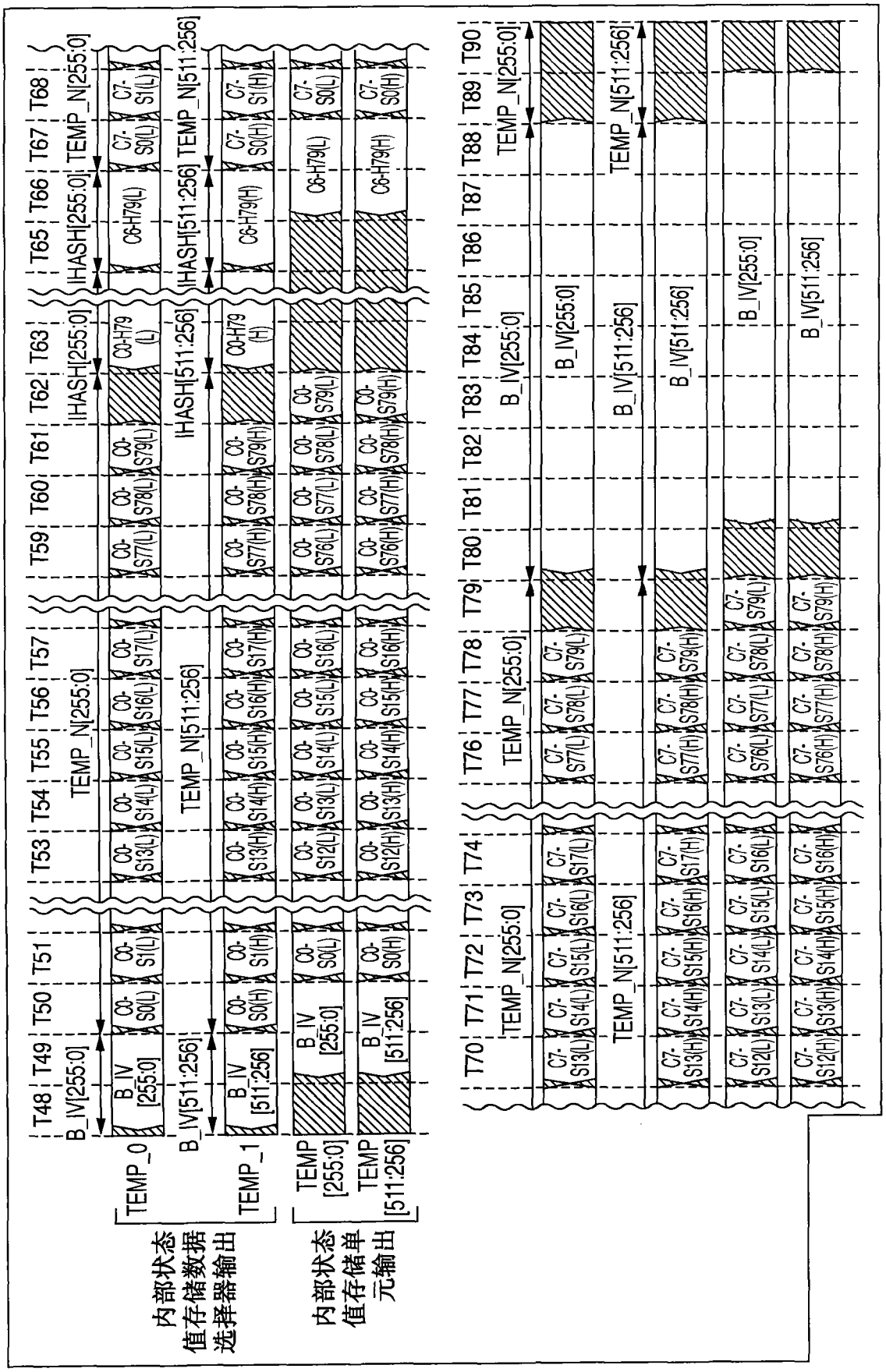

T48 T49 T50 T51 T53 T54 T55 T56 T57 T59 T60 T61 T62 T63 T65 T66 T67 T68
B_IV[255:0]
TEMP_N[255:0]
IHASH[255:0]
TEMP_N[255:0]
B_IV [255:0]
C0-S0(L)
C0-S1(L)
C0-S13(L)
C0-S14(L)
C0-S15(L)
C0-S16(L)
C0-S17(L)
C0-S77(L)
C0-S78(L)
C0-S79(L)
C0-H79 (L)
C6-H79(L)
C7-S0(L)
C7-S1(L)
TEMP_0
B_IV[511:256]
TEMP_N[511:256]
IHASH[511:256]
TEMP_N[511:256]
B_IV [511:256]
C0-S0(H)
C0-S1(H)
C0-S13(H)
C0-S14(H)
C0-S15(H)
C0-S16(H)
C0-S17(H)
C0-S77(H)
C0-S78(H)
C0-S79(H)
C0-H79 (H)
C6-H79(H)
C7-S0(H)
C7-S1(H)
TEMP_1
B_IV [255:0]
C0-S12(L)
C0-S13(L)
C0-S14(L)
C0-S15(L)
C0-S16(L)
C0-S76(L)
C0-S77(L)
C0-S78(L)
C0-S79(L)
C6-H79(L)
C7-S0(L)
TEMP [255:0]
B_IV [511:256]
C0-S12(H)
C0-S13(H)
C0-S14(H)
C0-S15(H)
C0-S16(H)
C0-S76(H)
C0-S77(H)
C0-S78(H)
C0-S79(H)
C6-H79(H)
C7-S0(H)
TEMP [511:256]
内部状态值存储数据选择器输出
内部状态值存储单元输出
T70 T71 T72 T73 T74 T76 T77 T78 T79 T80 T81 T82 T83 T84 T85 T86 T87 T88 T89 T90
TEMP_N[255:0]
B_IV[255:0]
TEMP_N[255:0]
C7-S12(L)
C7-S13(L)
C7-S14(L)
C7-S15(L)
C7-S16(L)
C7-S76(L)
C7-S77(L)
C7-S78(L)
C7-S79(L)
TEMP_N[511:256]
B_IV[511:256]
TEMP_N[511:256]
C7-S12(H)
C7-S13(H)
C7-S14(H)
C7-S15(H)
C7-S16(H)
C7-S76(H)
C7-S77(H)
C7-S78(H)
C7-S79(H)
B_IV[255:0]
B_IV[511:256]

图 33E

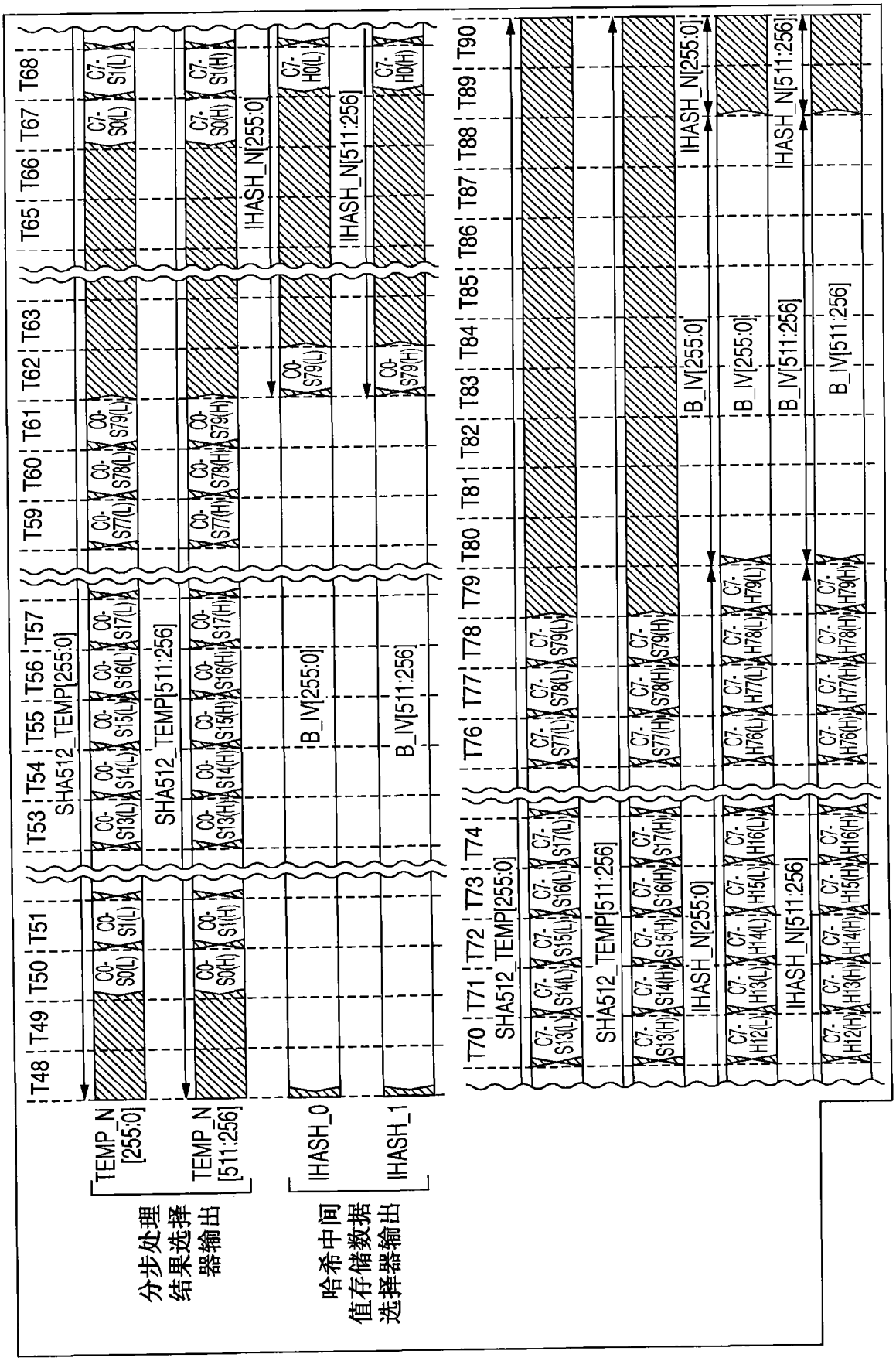

T48 T49 T50 T51 T53 T54 T55 T56 T57 T59 T60 T61 T62 T63 T65 T66 T67 T68
SHA512_TEMP[255:0]
SHA512_TEMP[511:256]
TEMP_N [255:0]
TEMP_N [511:256]
IHASH_0
IHASH_1
IHASH_N[255:0]
IHASH_N[511:256]
B_IV[255:0]
B_IV[511:256]
分步处理结果选择器输出
哈希中间值存储数据选择器输出
T70 T71 T72 T73 T74 T76 T77 T78 T79 T80 T81 T82 T83 T84 T85 T86 T87 T88 T89 T90
SHA512_TEMP[255:0]
SHA512_TEMP[511:256]
IHASH_N[255:0]
IHASH_N[511:256]
B_IV[255:0]
B_IV[511:256]

图 33F

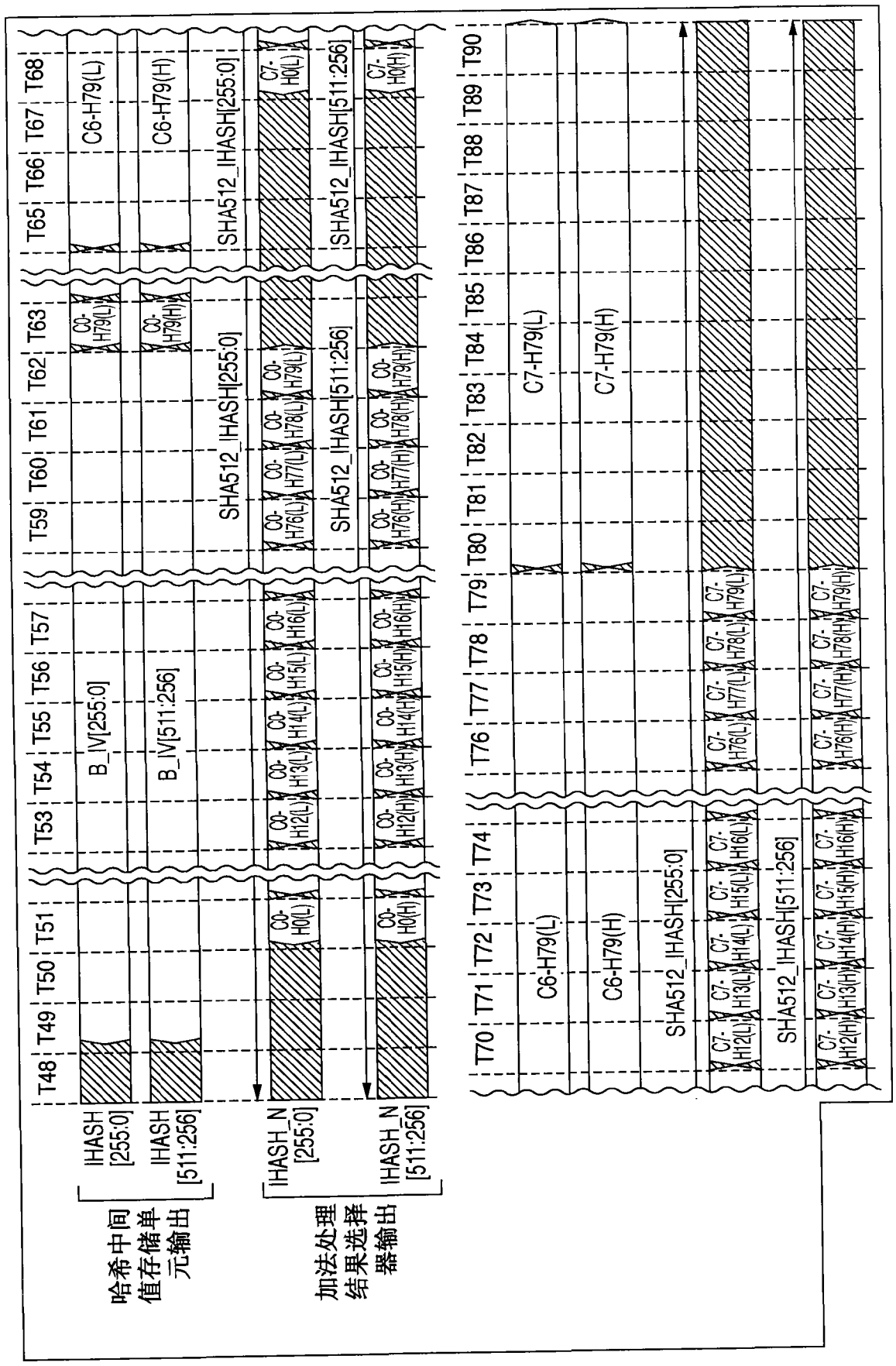

T48 T49 T50 T51 T53 T54 T55 T56 T57 T59 T60 T61 T62 T63 T65 T66 T67 T68
T70 T71 T72 T73 T74 T76 T77 T78 T79 T80 T81 T82 T83 T84 T85 T86 T87 T88 T89 T90
IHASH [255:0]
IHASH [511:256]
IHASH_N [255:0]
IHASH_N [511:256]
哈希中间值存储单元输出
加法处理结果选择器输出
B_IV[255:0]
B_IV[511:256]
C6-H79(L)
C6-H79(H)
SHA512_IHASH[255:0]
SHA512_IHASH[511:256]
C7-H79(L)
C7-H79(H)

图 33G

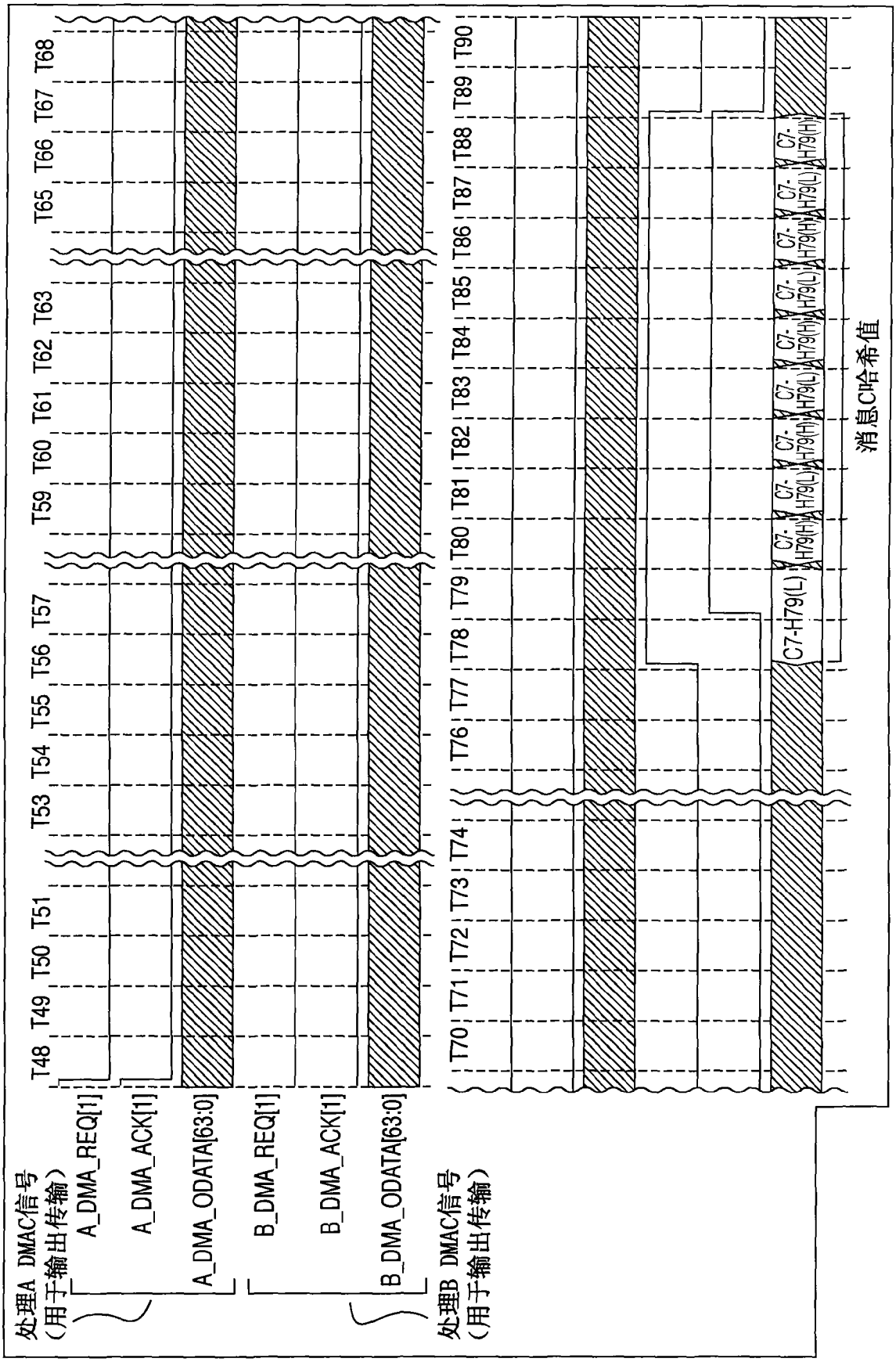

处理A DMAC信号（用于输出传输）
A_DMA_REQ[1]
A_DMA_ACK[1]
A_DMA_ODATA[63:0]
B_DMA_REQ[1]
B_DMA_ACK[1]
B_DMA_ODATA[63:0]
处理B DMAC信号（用于输出传输）
T48 T49 T50 T51 T53 T54 T55 T56 T57 T59 T60 T61 T62 T63 T65 T66 T67 T68
T70 T71 T72 T73 T74 T76 T77 T78 T79 T80 T81 T82 T83 T84 T85 T86 T87 T88 T89 T90
C7-H79(L)
消息C哈希值

图 33H

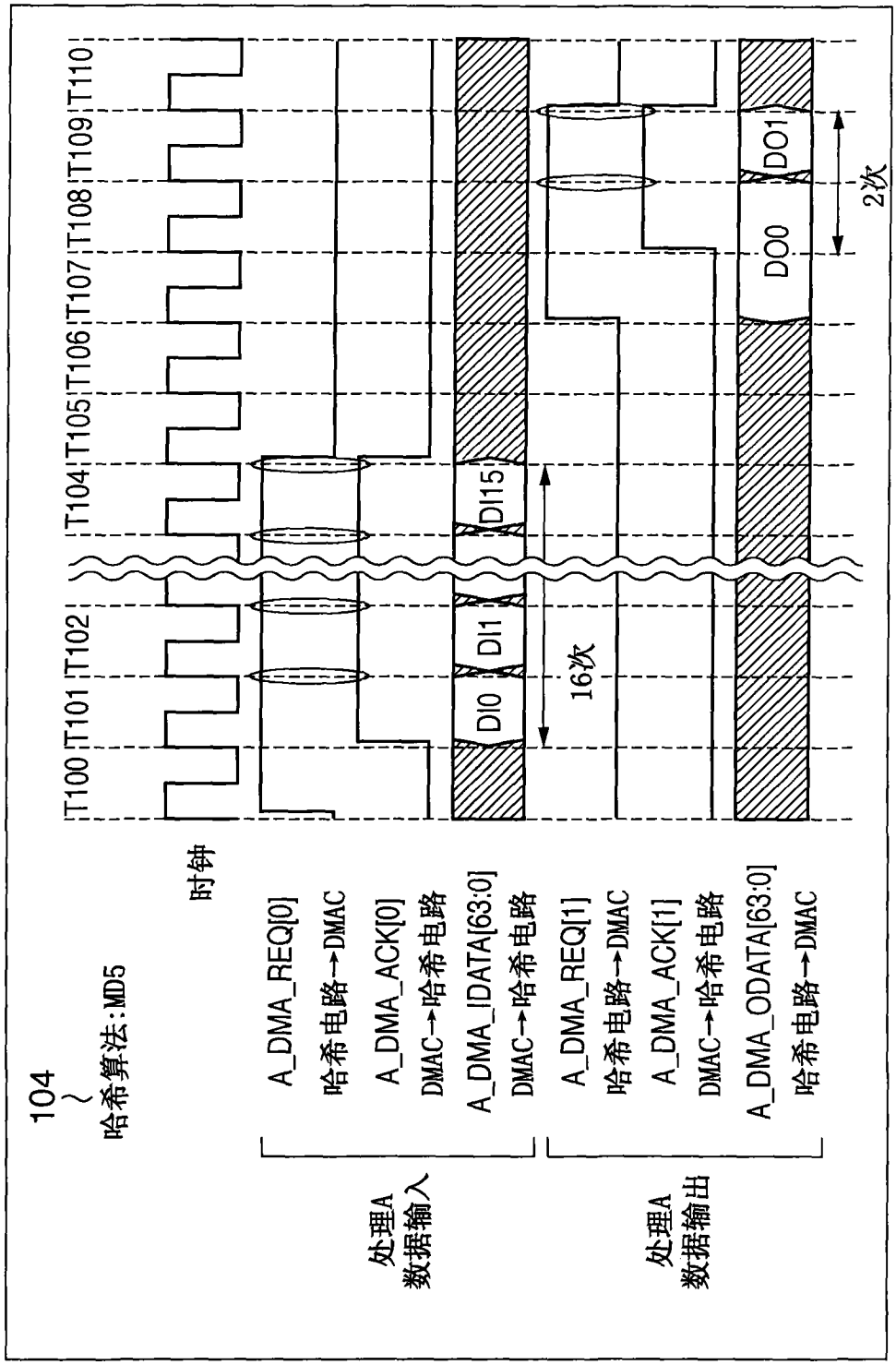

104
哈希算法:MD5
时钟
T100
T101
T102
T104
T105
T106
T107
T108
T109
T110
A_DMA_REQ[0]
哈希电路→DMAC
A_DMA_ACK[0]
DMAC→哈希电路
A_DMA_IDATA[63:0]
DMAC→哈希电路
DI0
DI1
DI15
16次
处理A
数据输入
A_DMA_REQ[1]
哈希电路→DMAC
A_DMA_ACK[1]
DMAC→哈希电路
A_DMA_ODATA[63:0]
哈希电路→DMAC
DO0
DO1
2次
处理A
数据输出

图 34A

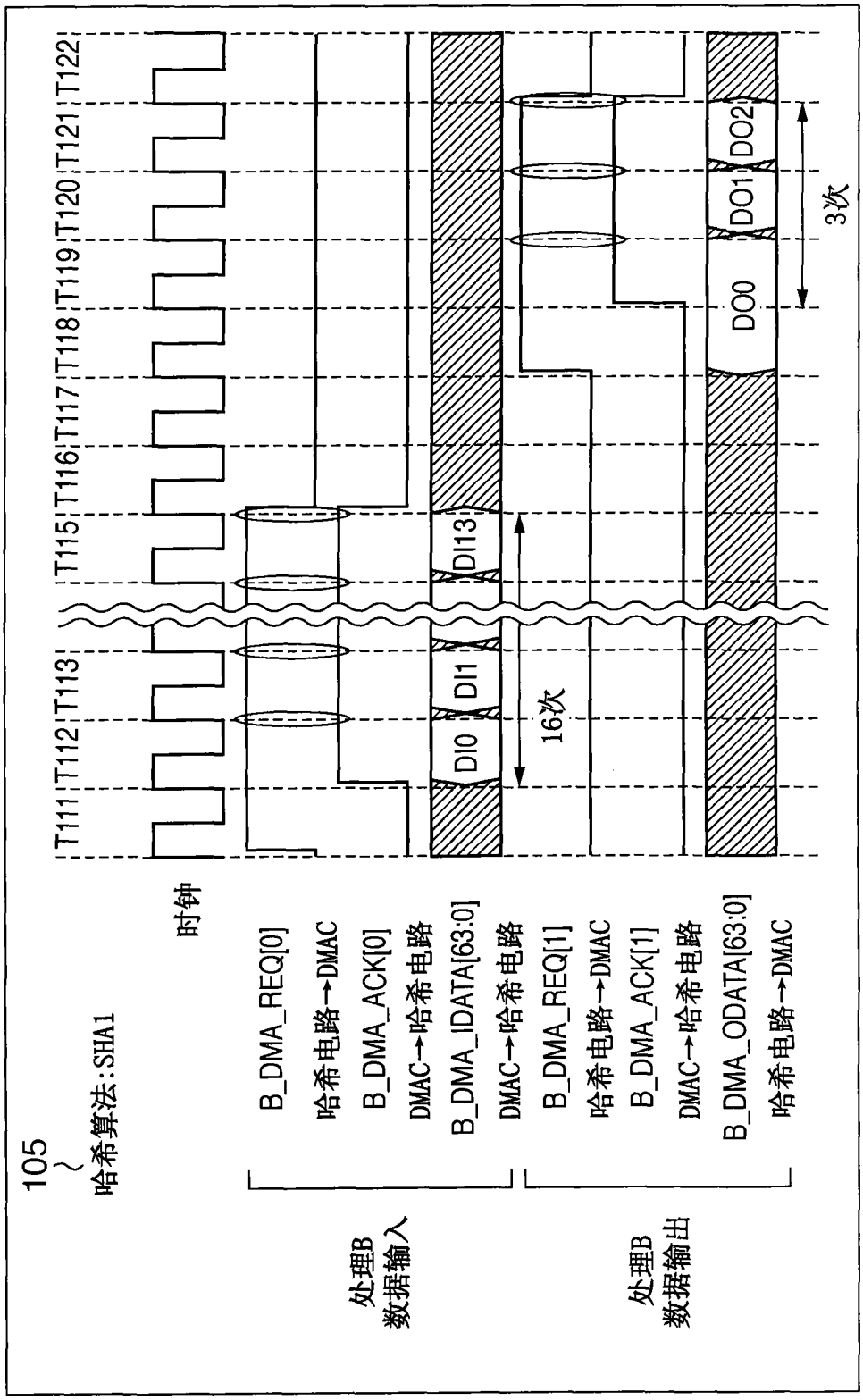

105
哈希算法:SHA1
时钟
T111
T112
T113
T115
T116
T117
T118
T119
T120
T121
T122
B_DMA_REQ[0]
哈希电路→DMAC
B_DMA_ACK[0]
DMAC→哈希电路
B_DMA_IDATA[63:0]
DMAC→哈希电路
DI0
DI1
DI13
16次
处理B
数据输入
B_DMA_REQ[1]
哈希电路→DMAC
B_DMA_ACK[1]
DMAC→哈希电路
B_DMA_ODATA[63:0]
哈希电路→DMAC
DO0
DO1
DO2
3次
处理B
数据输出

图 34B

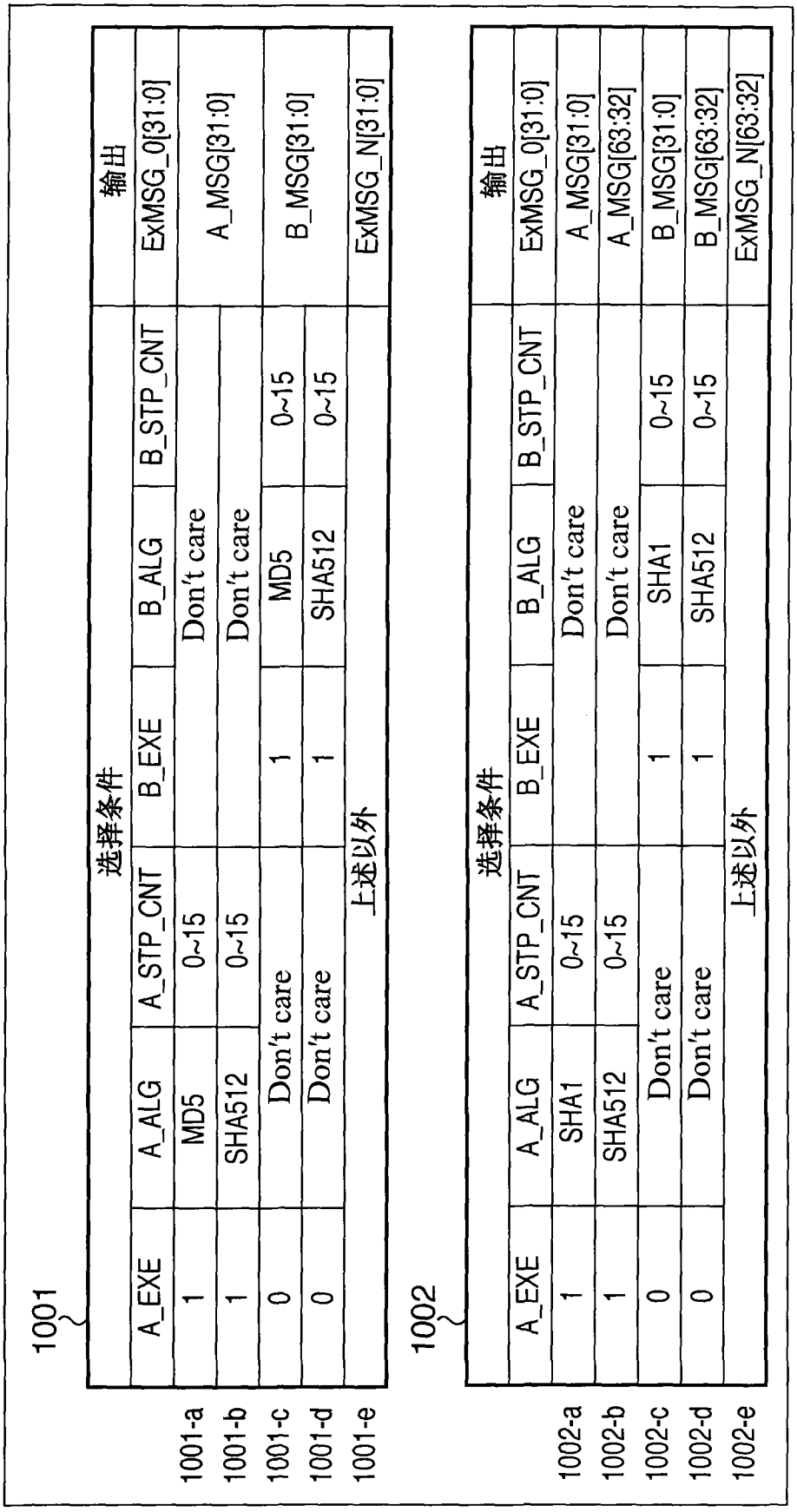

1001
选择条件
输出
A_EXE
A_ALG
A_STP_CNT
B_EXE
B_ALG
B_STP_CNT
ExMSG_O[31:0]
1001-a
1
MD5
0~15
Don't care
A_MSG[31:0]
1001-b
1
SHA512
0~15
Don't care
1001-c
0
Don't care
1
MD5
0~15
B_MSG[31:0]
1001-d
0
Don't care
1
SHA512
0~15
1001-e
上述以外
ExMSG_N[31:0]
1002
选择条件
输出
A_EXE
A_ALG
A_STP_CNT
B_EXE
B_ALG
B_STP_CNT
ExMSG_O[31:0]
1002-a
1
SHA1
0~15
Don't care
A_MSG[31:0]
1002-b
1
SHA512
0~15
Don't care
A_MSG[63:32]
1002-c
0
Don't care
1
SHA1
0~15
B_MSG[31:0]
1002-d
0
Don't care
1
SHA512
0~15
B_MSG[63:32]
1002-e
上述以外
ExMSG_N[63:32]

图 35

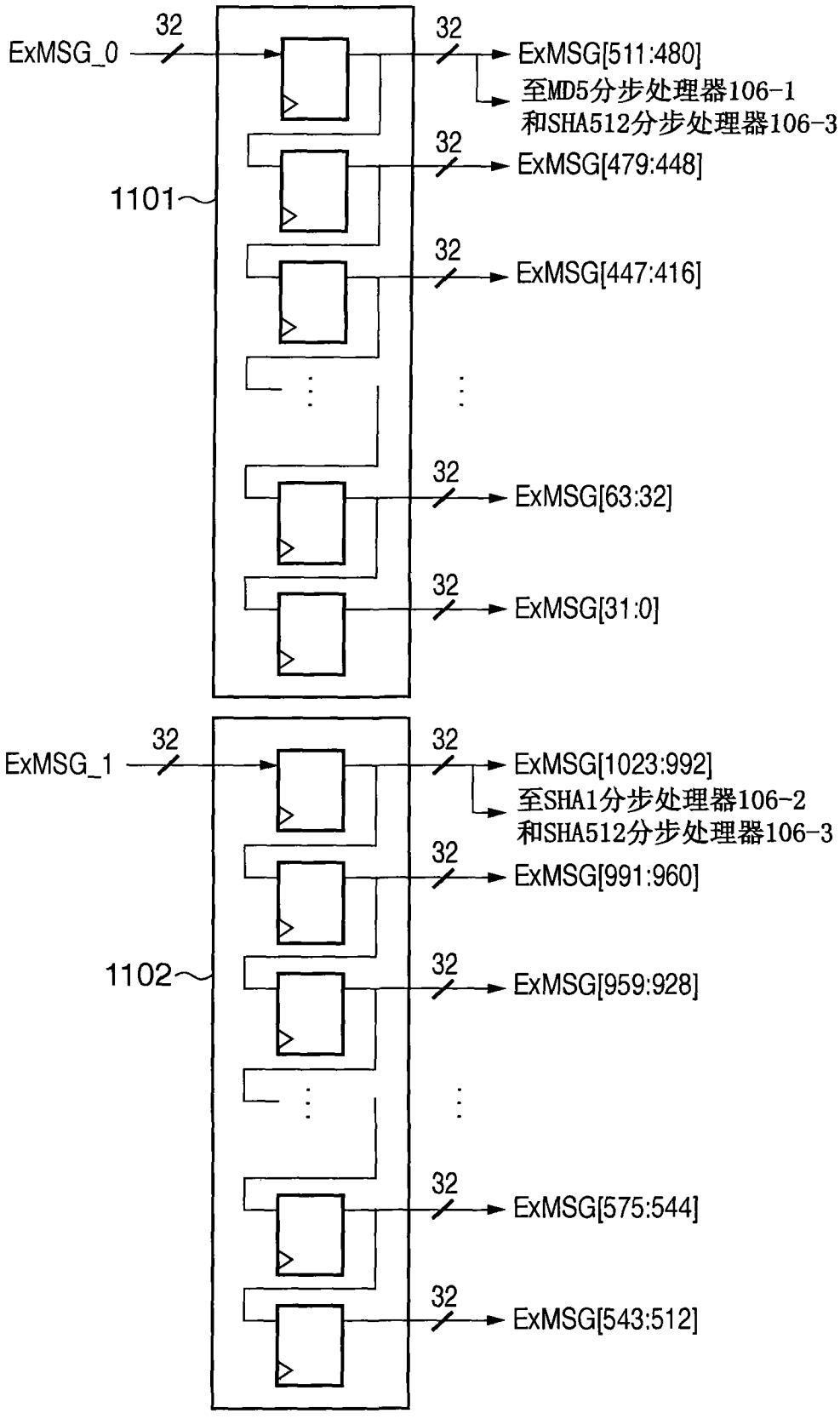

ExMSG_0
32
32
ExMSG[511:480]
至MD5分步处理器106-1
和SHA512分步处理器106-3
32
ExMSG[479:448]
1101
32
ExMSG[447:416]
32
ExMSG[63:32]
32
ExMSG[31:0]
ExMSG_1
32
32
ExMSG[1023:992]
至SHA1分步处理器106-2
和SHA512分步处理器106-3
32
ExMSG[991:960]
1102
32
ExMSG[959:928]
32
ExMSG[575:544]
32
ExMSG[543:512]

图 36

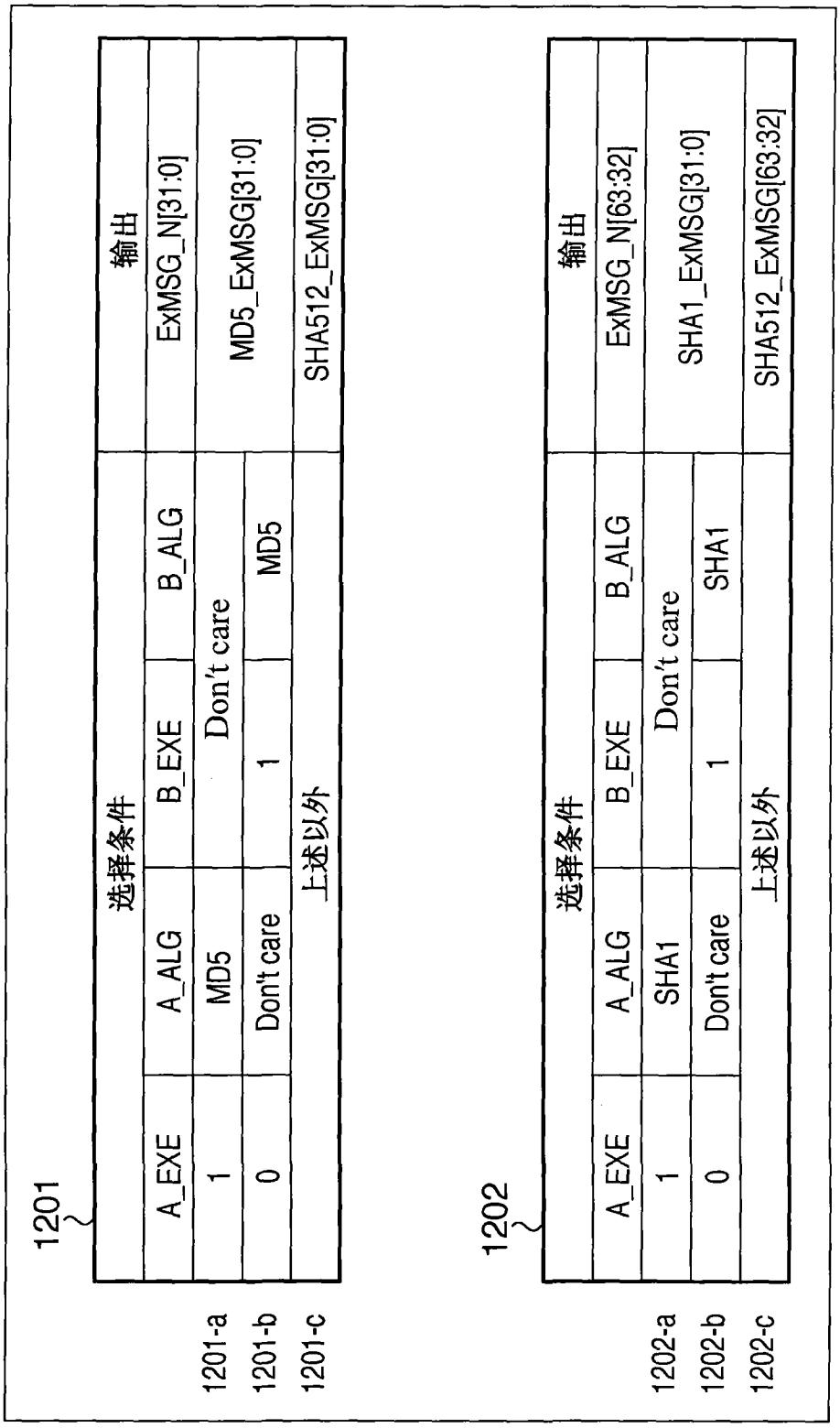

1201
选择条件
输出
A_EXE
A_ALG
B_EXE
B_ALG
ExMSG_N[31:0]
1
MD5
Don't care
MD5_ExMSG[31:0]
0
Don't care
1
MD5
上述以外
SHA512_ExMSG[31:0]
1201-a
1201-b
1201-c
1202
选择条件
输出
A_EXE
A_ALG
B_EXE
B_ALG
ExMSG_N[63:32]
1
SHA1
Don't care
SHA1_ExMSG[31:0]
0
Don't care
1
SHA1
上述以外
SHA512_ExMSG[63:32]
1202-a
1202-b
1202-c

图 37

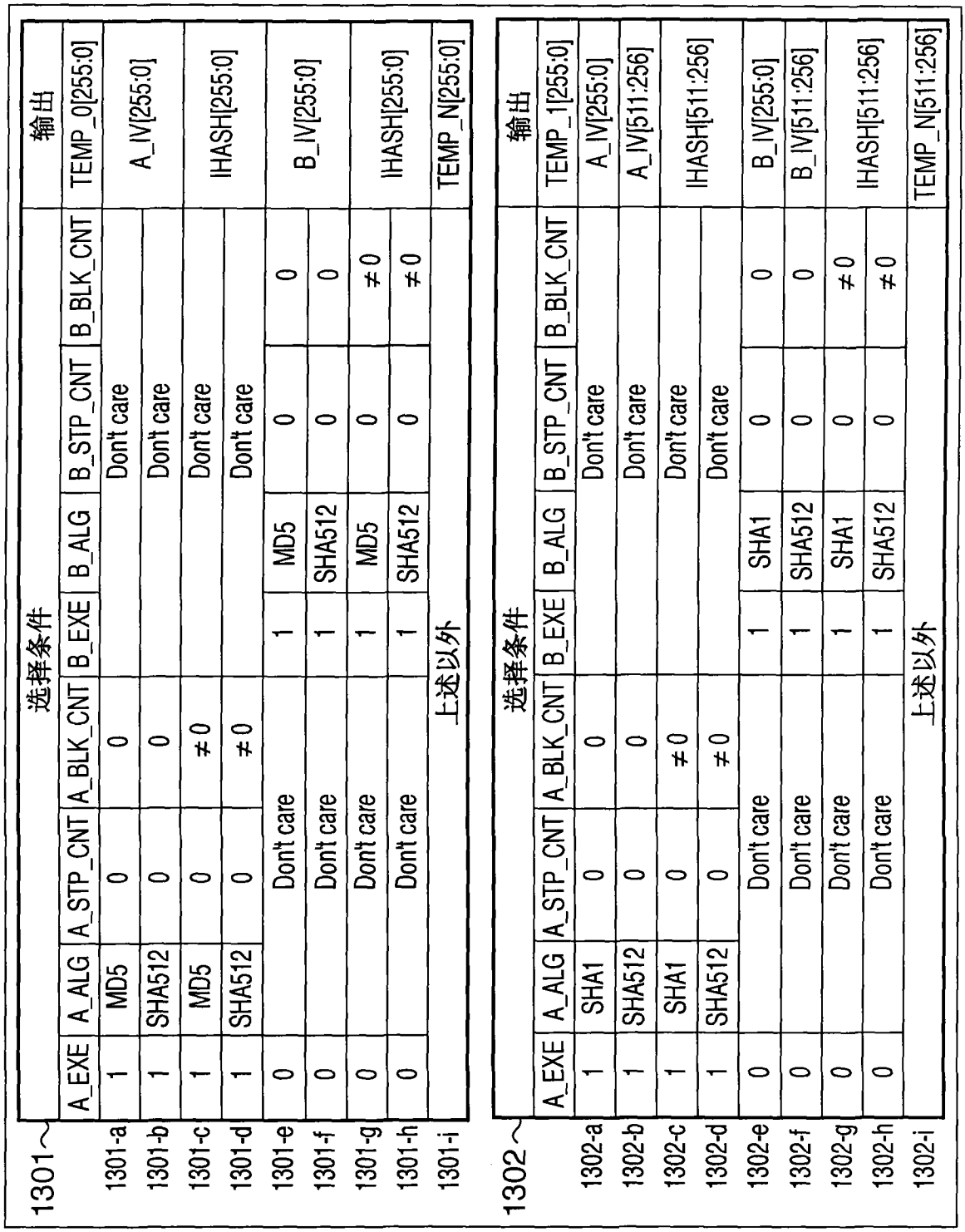

1301
选择条件
输出
A_EXE
A_ALG
A_STP_CNT
A_BLK_CNT
B_EXE
B_ALG
B_STP_CNT
B_BLK_CNT
TEMP_0[255:0]
1301-a
1
MD5
0
0
Don't care
A_IV[255:0]
1301-b
1
SHA512
0
0
Don't care
1301-c
1
MD5
0
≠0
Don't care
IHASH[255:0]
1301-d
1
SHA512
0
≠0
Don't care
1301-e
0
Don't care
1
MD5
0
0
B_IV[255:0]
1301-f
0
Don't care
1
SHA512
0
0
1301-g
0
Don't care
1
MD5
0
≠0
IHASH[255:0]
1301-h
0
Don't care
1
SHA512
0
≠0
1301-i
上述以外
TEMP_N[255:0]
1302
选择条件
输出
A_EXE
A_ALG
A_STP_CNT
A_BLK_CNT
B_EXE
B_ALG
B_STP_CNT
B_BLK_CNT
TEMP_1[255:0]
1302-a
1
SHA1
0
0
Don't care
A_IV[255:0]
1302-b
1
SHA512
0
0
Don't care
A_IV[511:256]
1302-c
1
SHA1
0
≠0
Don't care
IHASH[511:256]
1302-d
1
SHA512
0
≠0
Don't care
1302-e
0
Don't care
1
SHA1
0
0
B_IV[255:0]
1302-f
0
Don't care
1
SHA512
0
0
B_IV[511:256]
1302-g
0
Don't care
1
SHA1
0
≠0
IHASH[511:256]
1302-h
0
Don't care
1
SHA512
0
≠0
1302-i
上述以外
TEMP_N[511:256]

图 38

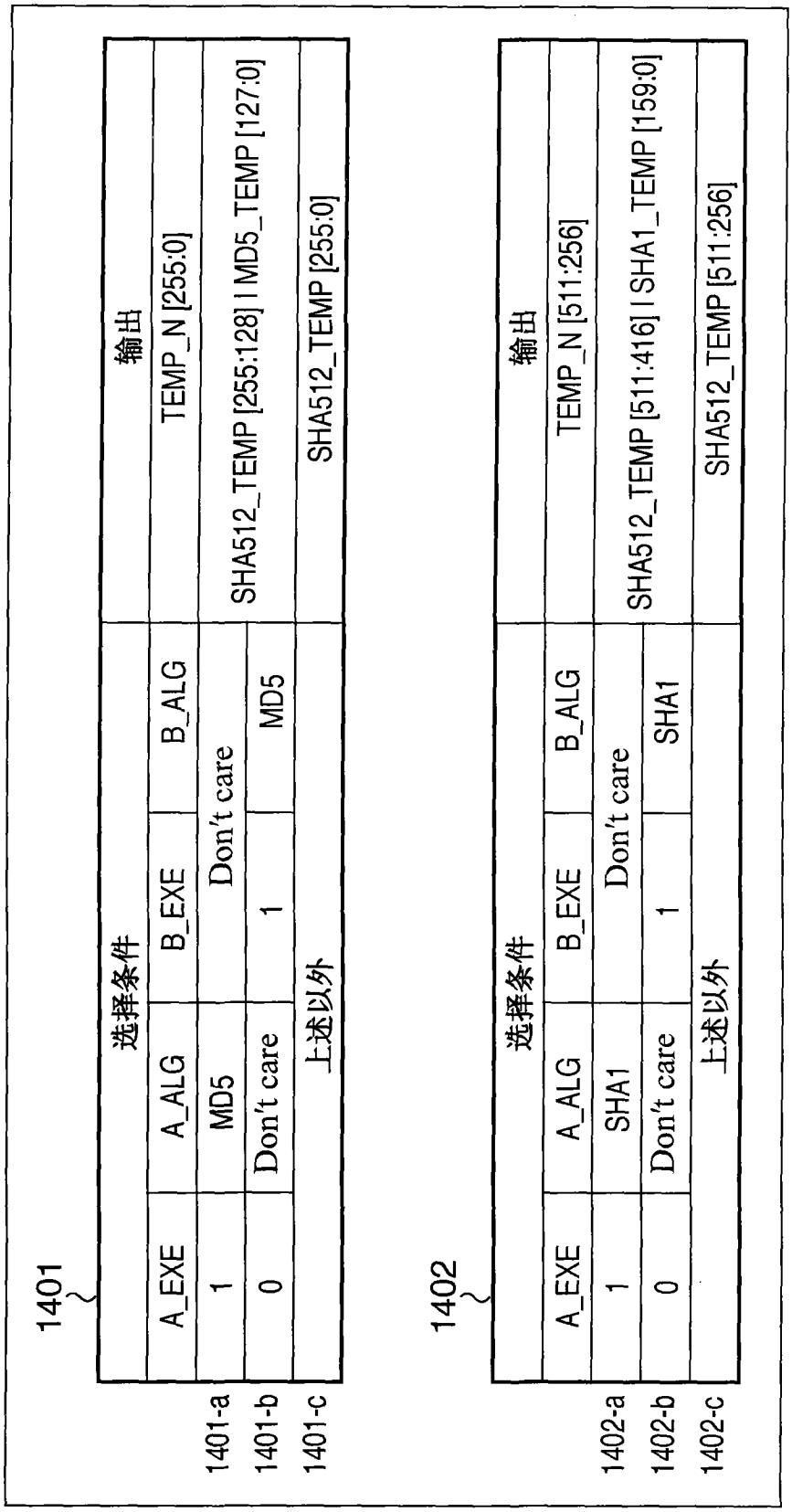

1401
选择条件
输出
A_EXE
A_ALG
B_EXE
B_ALG
TEMP_N [255:0]
1401-a
1
MD5
Don't care
SHA512_TEMP [255:128] | MD5_TEMP [127:0]
1401-b
0
Don't care
1
MD5
1401-c
上述以外
SHA512_TEMP [255:0]
1402
选择条件
输出
A_EXE
A_ALG
B_EXE
B_ALG
TEMP_N [511:256]
1402-a
1
SHA1
Don't care
SHA512_TEMP [511:416] | SHA1_TEMP [159:0]
1402-b
0
Don't care
1
SHA1
1402-c
上述以外
SHA512_TEMP [511:256]

图 39

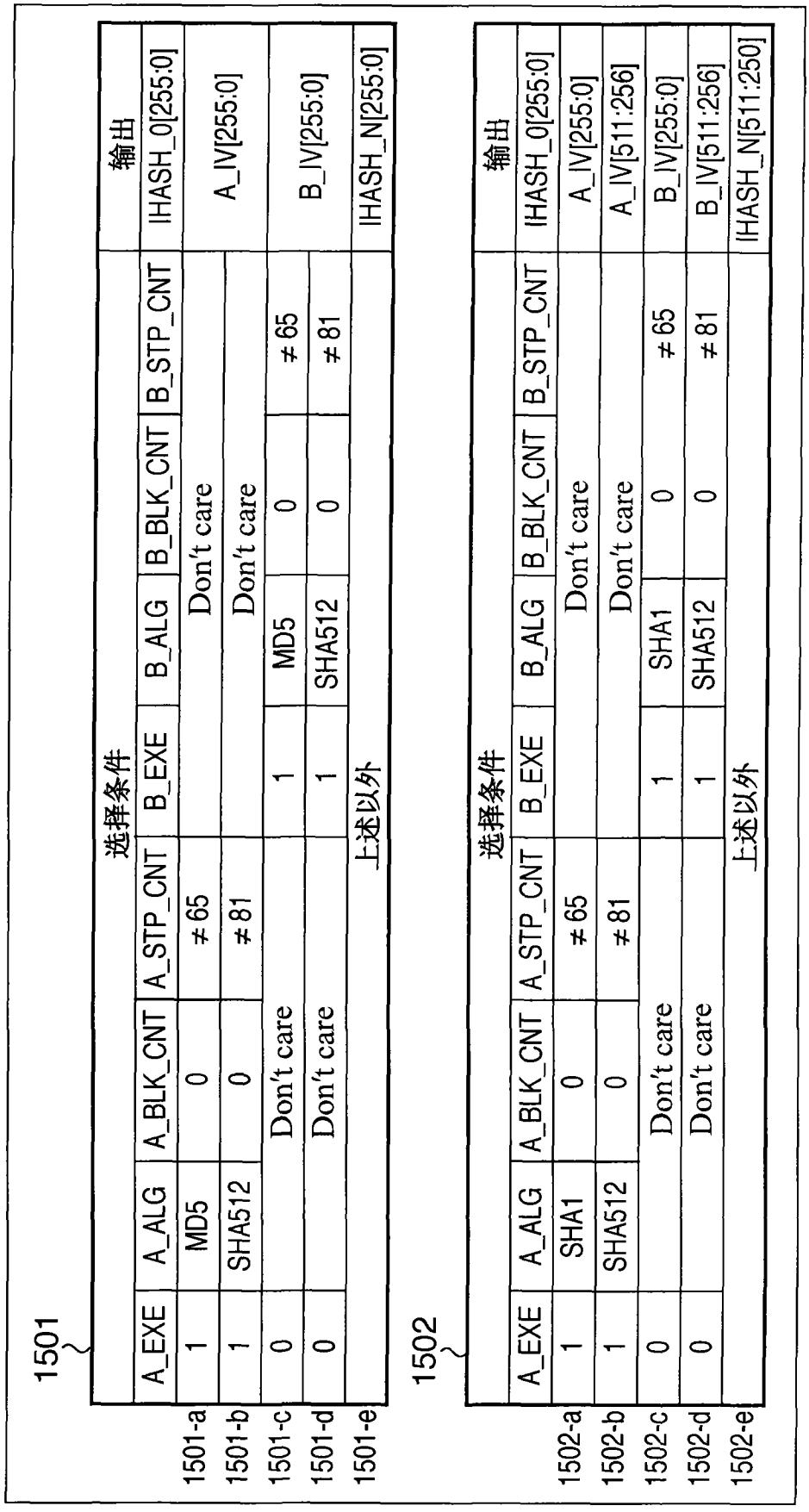

1501
选择条件
输出
A_EXE
A_ALG
A_BLK_CNT
A_STP_CNT
B_EXE
B_ALG
B_BLK_CNT
B_STP_CNT
IHASH_0[255:0]
1501-a
1
MD5
0
≠65
Don't care
A_IV[255:0]
1501-b
1
SHA512
0
≠81
Don't care
1501-c
0
Don't care
1
MD5
0
≠65
B_IV[255:0]
1501-d
0
Don't care
1
SHA512
0
≠81
1501-e
上述以外
IHASH_N[255:0]
1502
选择条件
输出
A_EXE
A_ALG
A_BLK_CNT
A_STP_CNT
B_EXE
B_ALG
B_BLK_CNT
B_STP_CNT
IHASH_0[255:0]
1502-a
1
SHA1
0
≠65
Don't care
A_IV[255:0]
1502-b
1
SHA512
0
≠81
Don't care
A_IV[511:256]
1502-c
0
Don't care
1
SHA1
0
≠65
B_IV[255:0]
1502-d
0
Don't care
1
SHA512
0
≠81
B_IV[511:256]
1502-e
上述以外
IHASH_N[511:250]

图 40

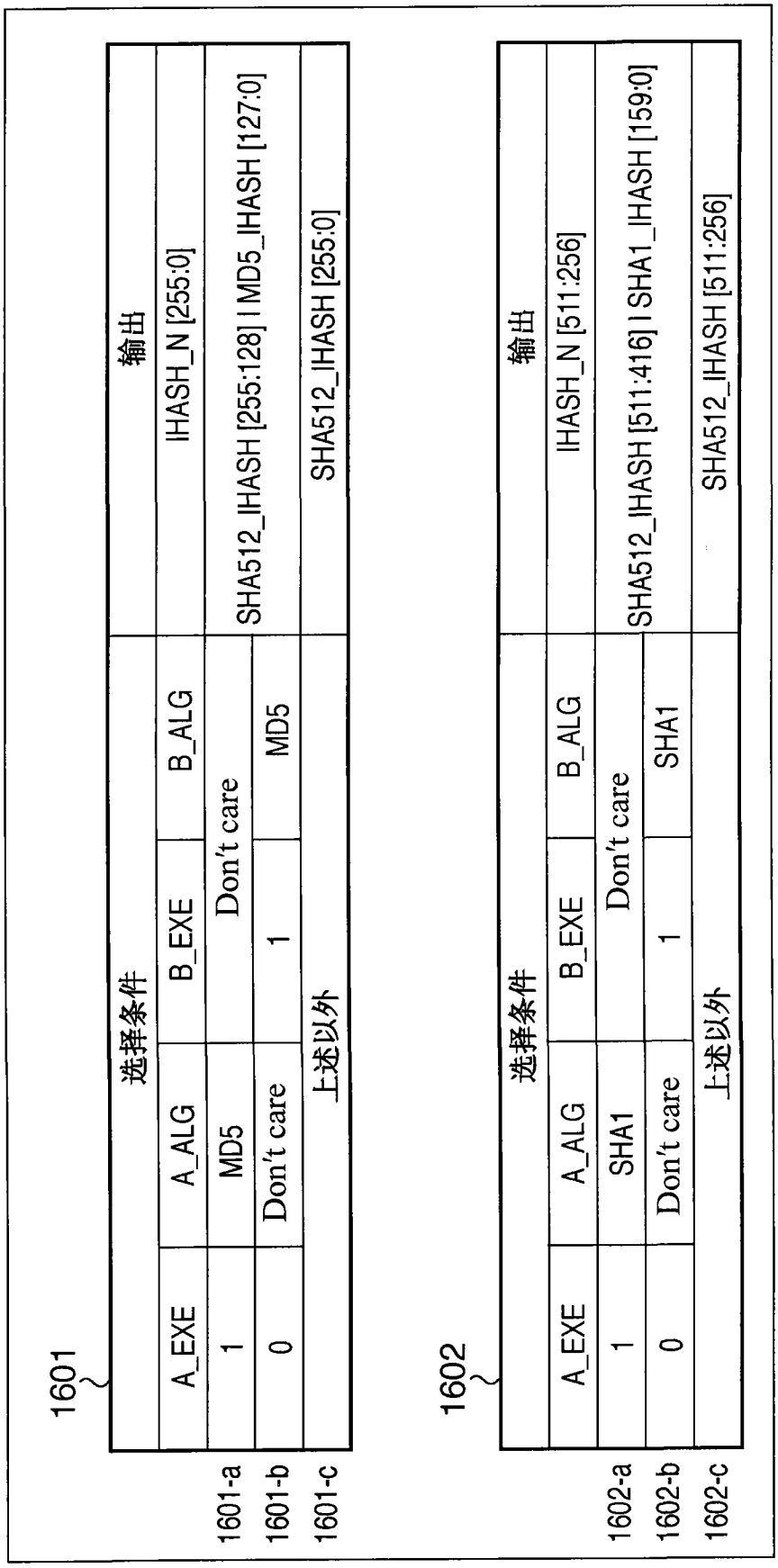

1601
选择条件
输出
A_EXE
A_ALG
B_EXE
B_ALG
IHASH_N [255:0]
1601-a
1
MD5
Don't care
SHA512_IHASH [255:128] | MD5_IHASH [127:0]
1601-b
0
Don't care
1
MD5
1601-c
上述以外
SHA512_IHASH [255:0]
1602
选择条件
输出
A_EXE
A_ALG
B_EXE
B_ALG
IHASH_N [511:256]
1602-a
1
SHA1
Don't care
SHA512_IHASH [511:416] | SHA1_IHASH [159:0]
1602-b
0
Don't care
1
SHA1
1602-c
上述以外
SHA512_IHASH [511:256]

图 41