(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112385175 B
(45)授权公告日 2024.04.09

(21)申请号 201980041306.2
(22)申请日 2019.06.17
(65)同一申请的已公布的文献号
申请公布号 CN 112385175 A
(43)申请公布日 2021.02.19
(30)优先权数据
18178252.5 2018.06.18 EP
(85)PCT国际申请进入国家阶段日
2020.12.18
(86)PCT国际申请的申请数据
PCT/EP2019/065791 2019.06.17
(87)PCT国际申请的公布数据
WO2019/243209 EN 2019.12.26
(73)专利权人 皇家飞利浦有限公司
地址 荷兰艾恩德霍芬
(72)发明人 J·A·C·伯恩森
(74)专利代理机构 永新专利商标代理有限公司 72002
专利代理师 孟杰雄
(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/32(2006.01)
H04L 9/12(2006.01)
(56)对比文件
CN 104038828 A,2014.09.10
CN 107667499 A,2018.02.06
CN 1567878 A,2005.01.19
EP 2466508 A1,2012.06.20
US 2011238989 A1,2011.09.29
US 2019132120 A1,2019.05.02
WO 2016027454 A1,2016.02.25
审查员 顾玲玲

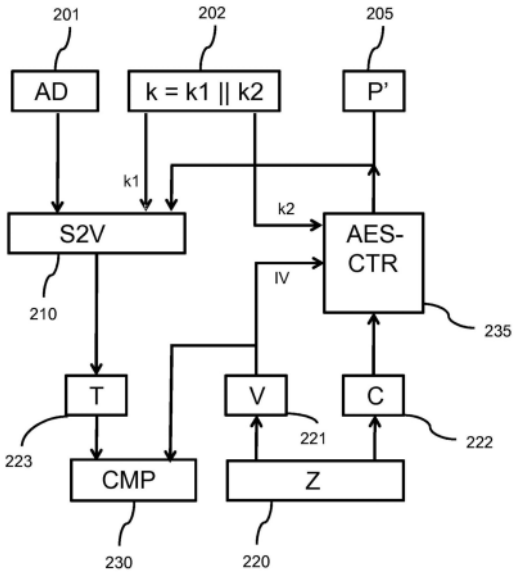
权利要求书3页 说明书20页 附图14页

(54)发明名称

一种用于数据加密和完整性的设备

(57)摘要

一种设备被布置为用于对输入数据进行加密,并且保护输入数据和关联数据的完整性。加密处理器具有被布置为基于所述输入数据来计算完整性值的第一散列单元(311)、被布置为基于所述完整性值和关联数据来计算初始化向量的第二散列单元(310)。散列单元中的至少一个可以是密钥散列单元。加密单元(315)被布置为用于使用所述初始化向量和加密密钥(k2)对所述输入数据进行加密以生成加密数据。实际上,所述初始化向量不同于所述完整性值。由于所述初始化向量取决于所述完整性值和关联数据二者,因此其中的任何更改都将导致解密失败,并且解密数据与原始明文P完全不同。



CN 112385175 B

1.一种用于对输入数据进行加密并且保护所述输入数据和关联数据的完整性的加密方法，

所述方法包括

-使用第一散列函数(311)基于所述输入数据来计算完整性值；

-使用第二散列函数(310)基于所述完整性值和所述关联数据来计算初始化向量，所述初始化向量不同于所述完整性值；

-使用所述初始化向量和加密密钥(k2)对所述输入数据进行加密(315)以生成加密数据；

-基于所述完整性值来生成包括所述加密数据和消息完整性值的输出加密消息。

2.如权利要求1所述的方法，其中，用于计算所述完整性值的所述第一散列函数(311)是使用第一完整性密钥(k3)的第一密钥散列函数。

3.如权利要求1或2所述的方法，其中，用于计算所述初始化向量的所述第二散列函数(310)是使用第二完整性密钥(k1)的第二密钥散列函数。

4.如权利要求1或2所述的方法，其中，生成所述输出加密消息包括通过使用导出密钥(kc)对所述完整性值进行加密(621)来生成所述消息完整性值，所述导出密钥是使用第三散列函数(624)基于所述加密数据而生成的。

5.如权利要求4所述的方法，其中，用于生成所述导出密钥的所述第三散列函数(624)是使用第三完整性密钥(k4)的第三密钥散列函数。

6.如权利要求4所述的方法，其中，所述第一散列函数(311、411)、所述第二散列函数(310、510)和/或所述第三散列函数(624)包括基于签名密钥来计算数字签名。

7.如权利要求1所述的方法，

其中，用于计算所述完整性值的所述第一散列函数(311)是使用第一完整性密钥(k3)的第一密钥散列函数；

其中，用于计算所述初始化向量的所述第二散列函数(310)是使用第二完整性密钥(k1)的第二密钥散列函数；

其中，生成所述输出加密消息包括通过使用导出密钥(kc)对所述完整性值进行加密(621)来生成所述消息完整性值，所述导出密钥是使用第三散列函数(624)基于所述加密数据而生成的，用于生成所述导出密钥的所述第三散列函数(624)是使用第三完整性密钥(k4)的第三密钥散列函数；并且

其中，所述加密密钥(k2)以及所述第一完整性密钥(k3)、第二完整性密钥(k1)和第三完整性密钥(k4)中的至少一个是从秘密主密钥(k)导出的。

8.如权利要求1-2中的任一项所述的方法，其中，所述方法包括确定输入数据的量，以及，一旦确定所述量低于预定阈值，则将填充数据添加到所述输入数据。

9.如权利要求8所述的方法，其中，所述预定阈值是所述加密密钥的长度，并且所述填充数据包括随机数据。

10.如权利要求1-2中的任一项所述的方法，其中，所述输出加密消息不包含所述初始化向量。

11.一种用于对加密数据进行解密并且确定数据和关联数据的完整性的解密方法，所述方法包括

-基于完整性值获得包括所述加密数据和消息完整性值的加密消息,

-使用第二散列函数(310)基于所述完整性值和所述关联数据来计算初始化向量,所述初始化向量不同于所述完整性值;

-使用所述初始化向量和解密密钥(k2)来解密(335)所述加密数据以生成明文;

-使用第一散列函数(311)基于所述明文来计算测试完整性值;

-通过将所述测试完整性值和所述完整性值进行比较来确定所述完整性。

12.如权利要求11所述的方法,其中,用于计算所述测试完整性值的所述第一散列函数(311)是使用第一完整性密钥(k3)的第一密钥散列函数。

13.如权利要求11或12所述的方法,其中,用于计算所述初始化向量的所述第二散列函数(310)是使用第二完整性密钥(k1)的第二密钥散列函数。

14.如权利要求11或12所述的方法,其中,接收所述加密消息包括通过使用导出密钥(kc)解密(625)所述消息完整性值来生成所述完整性值,所述导出密钥是使用第三散列函数(624)基于所述加密数据而生成的。

15.如权利要求14所述的方法,其中,用于生成所述导出密钥的所述第三散列函数(624)是使用第三完整性密钥(k4)的第三密钥散列函数。

16.一种用于对输入数据进行加密并且保护所述输入数据和关联数据的完整性的加密设备,所述设备(110)包括

-输出单元(111),其用于基于完整性值来提供输出加密消息,所述输出加密消息包括加密数据和消息完整性值;以及

加密处理器(112),其具有

-第一散列单元(311),其被布置为基于所述输入数据来计算完整性值,

-第二散列单元(310),其被布置为基于所述完整性值和所述关联数据来计算初始化向量,所述初始化向量不同于所述完整性值,以及

-加密单元(315),其用于使用所述初始化向量和加密密钥(k2)对所述输入数据进行加密以生成加密数据。

17.如权利要求16所述的设备,其中,用于计算所述完整性值的所述第一散列单元(311)是使用第一完整性密钥(k3)的第一密钥散列单元,和/或用于计算所述初始化向量的所述第二散列单元(310)是使用第二完整性密钥(k1)的第二密钥散列单元。

18.一种用于对加密数据进行解密并且确定数据和关联数据的完整性的解密设备,所述设备(120)包括

-输入单元(121),其用于基于完整性值来获得包括所述加密数据和消息完整性值的加密消息;以及

解密处理器(122),其具有

-第二散列单元(310),其被布置为基于所述完整性值和所述关联数据来计算初始化向量,所述初始化向量不同于所述完整性值,

-解密单元(335),其用于使用所述初始化向量和解密密钥(k2)对所述加密数据进行解密以生成明文,

-第一散列单元(311),其被布置为基于所述明文来计算测试完整性值,以及

-比较器(330),其被布置为通过将所述测试完整性值和所述完整性值进行比较来确定

所述完整性。

19.如权利要求18所述的设备,其中,用于计算所述完整性值的所述第一散列单元(311)是使用第一完整性密钥(k3)的第一密钥散列单元,和/或用于计算所述初始化向量的所述第二散列单元(310)是使用第二完整性密钥(k1)的第二密钥散列单元。

20.一种计算机可读介质和/或微处理器可执行介质,其存储有程序代码指令,当在计算机上执行时,所述程序代码指令用于实现如权利要求1至15中的任一项所述的方法。

一种用于数据加密和完整性的设备

技术领域

[0001] 本发明涉及数据的加密和解密,所述数据还具有不被加密的关联数据。

[0002] 本发明涉及数据通信和存储领域,更具体地,提供用于对数据进行加密并且保护数据和关联数据的完整性以及相应地进行解密的设备和方法,以及相应的计算机程序产品。

背景技术

[0003] 当设备需要保护其通信或数据存储的安全时,通常会对其通信进行加密。另外,加密算法很重要,因为它们能够使数据保持私人化。只有当有解密密钥时,才能通过解密获得加密数据的明文。但是,不仅保密或隐私很重要,而且消息的完整性也很重要。攻击者可能会通过更改、删除或添加密文符号来更改已加密的消息。密文的更改在可能会导致解密后的无用数据,但是使用密码知识和某些加密范例的聪明的攻击者可能会成功操纵数据。例如,如果攻击者拥有从一个银行到另一个银行的消息的加密版本,其中包含将一定金额的钱汇入攻击者帐户的指令,并且如果攻击者知道密码文本符号n至m包含他的银行帐户号码,攻击者可以捕获将金额汇入其他人的银行帐户另一条这样的消息,并使用攻击者的银行帐户号码的密文符号更改其密文符号n至m。然后解密可以产生看起来正确的汇款指令。实际上,在不知道解密密钥的情况下更改密文,从而使得在解密之后产生有意义的消息将更加困难,但是这也是可能的。

[0004] 鉴于上述攻击,完整性保护被添加到加密中,例如,通过在加密之前对明文数据计算消息验证码(MAC)并对得到的MAC进行加密,或者通过在加密后对密文计算MAC,并将得到的MAC添加到消息。消息验证代码是一小段信息,其用于对消息进行验证——换言之,以确认消息来自指定的发件人并且未被更改过。MAC算法被设计为使得如果仅任何一比特消息被更改,则MAC的许多比特,优选大约一半比特数的MAC产生变化。需要密钥来创建MAC。如果消息的接收者拥有MAC、MAC密钥和解密密钥,则他能够验证消息未被篡改,消息是由知道MAC密钥的人发送的,并且他能够对其进行解密。众所周知,MAC算法家族是密钥散列消息验证代码(HMAC)算法,例如HMAC-SHA256、HMAC-SHA384和HMAC-SHA512,参见[RFC 6234]。

[0005] 还存在结合加密和完整性保护的密码。AES-SIV(使用高级加密标准(AES)的合成初始化向量(SIV)验证加密,参见[RFC 5297])是这种密码的范例。用于AES-SIV的密钥的一半比特用于加密/解密,而另一半比特用于验证和完整性保护。这意味着,例如当256比特密钥用于AES-SIV时,由AES-SIV完成128比特AES加密。同时,可以检查AES-SIV中关联数据(AD)的真实性和完整性。这意味着,能够在加密之前将两组数据输入至AES-SIV,需要加密的数据和未加密的关联数据,但是对于这两者,其真实性和完整性能够通过AES-SIV解密和完整性检查来证明。支持这种可能性的密码有时称为具有关联数据的验证加密方案(AEAD)。

[0006] 加密数据和关联数据的接收者需要将两者都输入AES-SIV进行解密。AES-SIV对密文进行解密,并将解密后的密文和关联数据输入至完整性检查,以确认完整性和真实性。如

果此检查失败,则必须丢弃已解密的密文。如果已在发送方和接收方之间更改了至少一比特已加密数据或AD,则此检查将失败。

[0007] 例如,改变至少一比特已加密数据将导致失败的真实性/完整性检查。在这种情况下,已解密的密文不同于发送者想要保护的明文。改变至少一比特关联数据将导致失败的真实性/完整性检查。

发明内容

[0008] 在上述AEAD密码中,如果已经更改了某些AD而加密数据保持不变,则解密的密文与发送者想要保护的明文相同。尽管AES-SIV规范要求丢弃解密结果,但由于某些原因,应用程序可能无法这样做,并且无论如何仍使用解密数据,所述解密数据等于原始明文。明文意味着未加密的数据或信息,即,针对加密进入加密算法的输入或来自解密的输出,并且密文意味着加密数据或信息,即来自加密的加密算法中的输出或针对解密的输入。

[0009] 本发明的一个目的是提供用于对输入数据进行加密并且保护输入数据和关联数据的完整性的方法和设备,其避免了当关联数据已经被操纵时使原始明文在解密之后可用。

[0010] 为此目的,提供如所附权利要求中所限定的设备和方法。根据本发明的一个方面,提供一种如权利要求1所述的加密方法。根据本发明的另一方面,提供一种如权利要求11所述的解密方法。根据本发明的另一方面,提供一种如权利要求16所述的加密设备。根据本发明的另一方面,提供如权利要求18所述的解密设备。根据本发明的另一方面,提供一种可从网络下载和/或存储在在计算机可读介质和/或微处理器可执行介质上的计算机程序产品,所述产品包括用于在计算机上执行时实现上述方法的程序代码指令。

[0011] 用于对输入数据进行加密并且保护输入数据和关联数据的完整性的加密和解密方法和设备的特征具有以下效果。

[0012] 加密过程包括使用第一散列函数基于输入数据来计算完整性值。因此,由于第一散列函数,完整性值被链接到纯输入数据(plain input data),而在操纵明文之后,无法获得相同的完整性值。而且,过程包括使用第二散列函数基于完整性值和关联数据来计算初始化向量。因此,由于第二散列函数,初始化向量被链接到关联数据,而在操纵关联数据或完整性值之后,无法获得相同的向量。实际上,初始化向量将与完整性值不同。而且,加密过程包括使用初始化向量和加密密钥对输入数据进行加密以生成加密数据。而且,加密过程包括基于完整性值生成包括加密数据和消息完整性值的输出加密消息。

[0013] 解密过程包括基于完整性值来获得包括加密数据和消息完整性值的加密消息。而且,解密过程包括使用第二散列函数基于从消息完整性值和关联数据导出的完整性值来计算初始化向量。第二散列函数等于在加密期间使用的第二散列函数,因此初始化向量不同于消息完整性值和完整性值。而且,解密过程包括使用初始化向量和解密密钥对加密数据进行解密,以生成明文,所述解密密钥是秘密的并且等于加密期间使用的加密密钥。备选地,当应用非对称加密时,加密密钥和解密密钥构成协作密钥对,例如,公共密钥和秘密密钥。而且,解密过程包括使用第一散列函数基于明文计算来测试完整性值。第一散列函数等于在加密期间使用的第一散列函数,因此测试完整性值应当等于经由加密消息传输的在加密期间计算的完整性值。而且,解密过程包括通过将测试完整性值和完整性值进行比较来

确定完整性。

[0014] 消息完整性值可以等于完整性值,或者可以例如通过使用秘密密钥加密被进一步保护。有利地,当恶意方操纵关联数据时,对所传输的加密数据进行解密将不会产生原始明文。这是由于初始化向量不同,因为所述向量是在解密侧使用第二散列函数基于接收到的关联数据来计算的。

[0015] 在实施例中,用于计算完整性值的第一散列函数是使用第一完整性密钥的第一密钥散列函数。有利地,由于恶意方将不知道秘密的第一完整性密钥,因此对完整性值的保护增强。而且,优选地,不同的密钥被用于不同的目的,例如,加密目的和完整性保护目的。

[0016] 在实施例中,用于计算初始化向量的第二散列函数是使用第二完整性密钥的第二密钥散列函数。有利地,对初始化向量的保护增强,因为恶意方将不知道秘密的第二完整性密钥。

[0017] 在实施例中,生成输出消息包括通过使用导出密钥对完整性值进行加密来生成消息完整性值,所述导出密钥是使用第三散列函数基于加密数据来生成的。有利地,对完整性值的保护增强,所传输的消息现在包括完整性值的加密版本。此外,由于具有将加密数据作为输入的第三散列函数,恶意方将能够操纵导出密钥。在解密过程中,加密数据中的单个比特数的更改将产生非常不同的导出密钥,因此也产生非常不同的完整性值和初始化向量。因此,解密将完全失败,即,除了失败的完整性测试之外,解密数据将与发送方加密的明文非常不同。可选地,用于生成导出密钥的第三散列函数是使用第三完整性密钥的第三密钥散列函数,这进一步提高了对完整性值的保护。

[0018] 根据本发明的方法可以在计算机上作为计算机实现的方法、或者在专用硬件中、或者在两者的组合中来实现。用于根据本发明的方法的可执行代码可以存储在计算机程序产品上。计算机程序产品的范例包括存储设备(例如记忆棒)、光存储设备(例如光盘)、集成电路、服务器、在线软件等。计算机程序产品可以包括存储在计算机可读介质上的非临时性程序代码装置,当在计算机上执行所述程序产品时,用于执行根据本发明的方法的介质。在实施例中,计算机程序包括计算机程序代码装置,其适于当计算机程序在计算机上运行时执行根据本发明的方法的所有步骤或阶段。优选地,计算机程序体现在计算机可读介质上。提供一种可从网络下载和/或存储在计算机可读介质和/或微处理器可执行介质上的计算机程序产品,所述产品包括用于当在计算机上执行时实现上述方法的程序代码指令。

[0019] 本发明的另一方面提供一种使计算机程序可用于下载的方法。当计算机程序被上载到例如Apple的App商店、Google的Play商店或Microsoft的Windows商店时,以及当可从这样的商店下载计算机程序时,将使用本方面。

[0020] 在所附权利要求中给出了根据本发明的设备和方法的其他优选实施例,其公开内容通过引用并入本文。

附图说明

[0021] 参考在以下说明中以范例方式描述的实施例并参考附图,本发明的这些和其他方面将变得显而易见,在附图中:

[0022] 图1示出了用于对数据进行加密和解密以及保护输入数据和关联数据的完整性的设备,

[0023] 图2示出了根据AES-SIV(现有技术)的加密处理,

[0024] 图3示出了根据AES-SIV(现有技术)的解密处理,

[0025] 图4示出了增强加密的框图,

[0026] 图5示出了增强解密的框图,

[0027] 图6示出了增强加密的第二范例,

[0028] 图7示出了增强解密的第二范例,

[0029] 图8示出了增强加密的第三范例,

[0030] 图9示出了增强解密的第三范例,

[0031] 图10示出了增强加密的第四范例,

[0032] 图11示出了增强解密的第四范例,

[0033] 图12示出了用于对输入数据进行加密并保护输入数据和关联数据的完整性的加密方法,

[0034] 图13示出了用于对加密数据进行解密并确定数据和关联数据的完整性的解密方法,

[0035] 图14a示出了计算机可读介质,以及

[0036] 图14b示出了处理器系统的图示表达。

[0037] 附图仅是示意性的,并未按比例绘制。在附图中,与已经描述的元件相对应的元件可以具有相同的附图标记。

具体实施方式

[0038] 图1示出了用于对数据进行加密和解密并保护数据和关联数据的完整性的设备。用于对数据进行加密和解密并保护输入数据和关联数据的完整性的系统100包括加密设备110和解密设备120。这些设备图示性示出,并且可以构成关于通信的对等体(peer)。然而,类似地,可以在主/从系统、广播系统、存储或数据库系统等中配置设备。消息在设备之间交换以交换加密数据、关联数据和完整性值,如下文所述。而且,设备可以是在物理上分开的或者可以组合在通用设备中,其被配备为执行加密和解密两者。

[0039] 加密设备110具有输出单元111和加密处理器112。同样,解密设备可以具有输入单元121和解密处理器122。下面参考图4、6、8和10进一步阐明加密处理器的功能,并且参考图5、7、9和11进一步阐明解密处理器的功能。

[0040] 所述设备被布置用于经由通信装置输入和输出以通常被称为消息的预定格式的数据,如形状130和连接输入单元111和输出单元121的箭头示意性所示的。所述通信装置可以例如是网络、广播系统或存储设备。所述设备可以被配备用于根据通信协议进行有线或无线通信,或者用于存储和检索所述消息。输入单元111和输出单元121可以被布置为根据通信协议(例如无线协议)连接并进一步进行通信,以发现至少一个其他设备并连接到已发现的设备以交换数据。

[0041] 在图1中,加密设备110可以具有用户接口113,所述用户接口113具有至少一个用户控制元件115。解密设备120可以类似地配备。例如,用户控制元件可以包括触摸屏、各种按钮、鼠标或触摸板等。按钮可以是传统的物理按钮、触摸传感器或虚拟按钮,例如在触摸屏上的或经由鼠标激活的图标上。用户接口也可以是远程用户接口。

[0042] 图2示出了AES-SIV加密(现有技术)的框图。在图中,单元P 203是明文输入,单元AD 201是用于关联数据的输入,例如关联数据的n个向量(AD1…ADn)。单元K 202是用于AES-SIV的密钥。它由K1和K2两个部分组成:K1是用于真实性/完整性检查的密钥,并且K2是用于加密/解密的密钥。单元S2V 210是在基于密码的消息验证代码([CMAC])模式下使用AES的伪随机函数(PRF)。它的输入包括k1、AD和P。S2V的详细说明请参见[RFC 5297]。S2V能够看作是具体的密钥散列函数。单元V 221存储S2V的输出,所述输出用作针对加密单元AES-CTR 215的初始化向量(IV)。V还包括在消息Z 220中,以用作AES-SIV解密期间的验证值。

[0043] 单元AES-CTR是在计数器模式下执行AES的块,请参见[MODES]。K2是密钥,V是AES在计数器模式下使用的初始化向量。在计数器模式下的AES或任何其他密码以如下方式工作。密码用于根据需要生成为伪随机数据的密码块大小(在AES中为128比特)的多个倍数,以便能够使用此伪随机数据作为对要加密或解密的消息进行XOR的密钥流。伪随机密钥流完全由密码、初始化向量V和密钥K确定。初始化向量V或密钥K的1比特变化将产生密钥流的大约50%的比特数变化。在计数器模式下的任何密码的IV可以由随机部分和计数器部分组成,或者可以仅由计数器组成。通过递增IV的计数器部分来生成第一个块之后的密钥流块。密钥流的长度限制为IV的计数器部分的可能性的数量。加密和解密操作是相同的操作,即,在数据流和密钥流之间执行XOR。单元C 222代表加密数据C,其是在计数器模式下由AES加密的明文P。消息Z 220是AES-SIV输出,它由与C结合的完整性值V组成。

[0044] EAS-SIV的以下属性能够通过分析图2中的AES-SIV加密的框图来确定。在表1中能够找到支持这一点的范例。下面讨论的改进的密码也拥有或改进了这些属性。

[0045] 第一属性(P1)如下。由于伪随机函数以及S2V的属性,在明文P中至少一比特的变化将导致在初始化向量V中的许多比特发生变化,因此也将导致加密明文C中的许多比特发生变化,另请参见表1中的实例2。

[0046] 第二属性(P2)如下。在关联数据AD的任何向量中至少一比特的变化将导致初始化向量IV(=完整性值V)中的许多比特发生变化,因此也将导致加密明文C中的许多比特发生变化,另请参见表1中的实例3。

[0047] 第三属性(P3)如下。根据图2,在加密能够开始之前必须对明文P整体进行处理,因为明文的所有比特都用于块CTR的初始化向量的计算,在计数器模式下通过AES进行加密。[RFC 5297]中提到了这种属性。

[0048]

实例	P – 明文输入	AD	V – 完整性值	C – 加密输出
实例 1 [RFC 5297] 的A.1的测试 向量	11223344 55667788 99aabbcc ddee	10111213 14151617 18191a1b 1c1d1e1f 20212223 24252627	85632d07 c6e8f37f 950acd32 0a2ecc93	40c02b96 90c4dc04 daef7f6a fe5c
实例 2 P中的1比特 更改	11223344 5567**7**788 99aabbcc ddee (1个已更改的比特)	10111213 14151617 18191a1b 1c1d1e1f 20212223 2425262	**eeab761c 7dfaee24** **9684596a 871d2d19** (123个已更改的比特)	**916157ca** **11dd8177** **c100cab5 5a89**
实例 3 AD 1中的1 比特更改	11223344 55667788 99aabbcc ddee	10**0**11213 14151617 18191a1b 1c1d1e1f 20212223 24252627 (1个已更改的比特)	**9130e7bb 358730d8** **898b9c36 1592ccb9** (119个已更改的比特)	**9347787e** **890773a1** **b073d851 fde3**
用于加密的密钥来自[RFC 5297]的A.1 (fffefdfc fbfaf9f8 f7f6f5f4 f3f2f1f0 f0f1f2f3 f4f5f6f7 f8f9fafb fcfdfeff)				

[0049] 表1-AES-SIV加密的范例结果

[0050] 图3示出了AES-SIV(现有技术)解密的框图。在图中,单元Z 220是用于AES-SIV解密的输入,它由与加密数据(加密之后的明文P)C相结合的完整性值V组成。单元V 221检索完整性值V,其用作用于单元AES-CTR 235中的AES解密的初始化向量(IV)。完整性值V还用于检查比较器CMP 230中C的有效性(完整性和真实性)。单元C 222检索加密数据C(其是在计数器模式下通过AES加密的明文P)。单元K 202具有用于AES-SIV的密钥,由k1和k2两部分组成。k1是用于真实性/完整性检查的完整性密钥,而k2是用于加密/解密的密钥。

[0051] 单元AES-CTR 235是在计数器模式下执行AES解密的块,参见[MODES],而k2是密钥,并且V是在计数器模式下由AES使用的初始化向量。单元P' 205从块AES-CTR接收解密的明文输出。仅当有效性检查为肯定时,才可以使用明文输出。单元AD具有关联数据,所述关联数据可以与消息Z 220一起传输,或者单独传输。单元S2V 210是在基于密码的消息验证代码([CMAC])模式下使用AES的伪随机函数(PRF),等于图2中的相同单元S2V。测试值T 223是S2V的输出,并且被提供给比较器CMP 230,其中,T与所接收的V进行比较。如果它们相等,

则有效性检查是肯定的,并且解密明文P’与在AES-SIV加密期间使用的明文P相同。如果T和V不相等,则AES-SIV失败,并且必须丢弃解密明文P’。

[0052] 通过分析图3中的AES-SIV解密的框图,能够确定EAS-SIV的以下属性。在表2中能够找到支持这一点的范例。

[0053] 第四属性(P4)如下。使用正确的关联数据AD、不变的初始化向量V和不变的加密数据C作为用于AES-SIV解密的输入,会导致解密明文P’与在AES-SIV加密期间使用的明文P相同。此外,在这种情况下,T等于V,因此AES-SIV在这种情况下不会检测真实性/完整性错误。另请参见表2中的实例4。

[0054] 第五属性(P5)如下。用于对AES-SIV加密明文C进行解密的关联数据AD中任何数量的比特的变化仍导致解密明文P’与在AES-SIV加密期间使用的明文P相同。这是因为关联数据对块CTR的输入(即,在计数器模式下使用AES对C的解密)没有影响。然而,在这种情况下,AES-SIV检测真实性/完整性错误。另请参加2中的实例5。因此,在已知的AES-SIV系统中,所得到的明文P’与P相同,这是需要通过改进密码解决的问题,如下所述。

[0055] 第六属性(P6)如下。用于对AES-SIV加密明文C进行解密的至少一个比特的初始化向量V更改,导致解密明文P’中的许多比特与在AES-SIV解密期间使用的明文P不同。从计数器模式下的AES属性能够很容易地理解这一点。在这种情况下,AES-SIV检测真实性/完整性错误。另请参见表2中的实例6。

[0056] 第七属性(P7)如下。用于AES-SIV解密的加密输入C的至少一比特更改导致解密明文P’中与AES-SIV加密期间使用的明文P中的相应比特发生变化。从计数器模式下AES的属性能够很容易地理解这一点。在这种情况下,AES-SIV检测真实性/完整性错误。另请参见表2中的实例7。

[0057]

实例	用于解密的 AD 1	用于解密的 V = IV	用于解密的 C 加密输出	P' 加密输出	T=V
实例 4 在 AD、V 和 C 中没有更改	10111213 14151617 18191a1b 1c1d1e1f 20212223 24252627	85632d07 c6e8f37f 950acd32 0a2ecc93	40c02b96 90c4dc04 daef7f6a fe5c	11223344 55667788 99aabbcc ddee (与 P 相同)	是
实例 5 AD 1 中的 1 比特更改	10011213 14151617 18191a1b 1c1d1e1f 20212223 24252627 (1 个已更改的比特)	85632d07 c6e8f37f 950acd32 0a2ecc93	40c02b96 90c4dc04 daef7f6a fe5c	11223344 55667788 99aabbcc ddee (与 P 相同)	否

[0058]

实例	用于解密的 AD 1	用于解密的 V = IV	用于解密的 C 加密输出	P' 加密输出	T=V
实例 6 V 中的 1 比特更改	10111213 14151617 18191a1b 1c1d1e1f 20212223 24252627	85632d07 c6c8f37f 950acd32 0a2ecc93 (1 个已更改的比特)	40c02b96 90c4dc04 daef7f6a fe5c	d88f34a6 5a417f5b aa3ed7c9 ea1a (53 个已更改的比特)	否
实例 7 C 中的 1 比特更改	10111213 14151617 18191a1b 1c1d1e1f 20212223 24252627	85632d07 c6e8f37f 950acd32 0a2ecc93	40c02b96 90c4dc0c daef7f6a fe5c (1 个已更改的比特)	11223344 55667780 99aabbcc ddee (1 个已更改的比特)	否
用于加密和解密的密钥来自[RFC 5297]的 A.1。 在加密期间使用来自[RFC 5297]的 A.1 的明文 P 和 AD 1，以产生（不变的）初始化向量 V 和解密输入 C。					

[0059] 表2-用于AES-SIV解密的范例结果

[0060] 如图4等中所示的增强密码解决上述第五属性(P5)中提到的AES-SIV问题。现在，用于对C进行解密的关联数据AD中任意数量的比特的变化都会导致解密明文P'与加密期间使用的明文P不同。这是因为关联数据对块ENCR的初始化向量IV有直接影响，并且与C的解密类似。而且，在这种情况下，增强密码确实检测完整性错误。因此，在增强系统中，当关联数据被操纵时，所得到的明文P'与P不同。值得注意的是，在下面如此阐明时，保持或增强了如上所述的其他属性。

[0061] 图4示出了增强加密的框图。在图中，单元P 203是明文输入，单元AD 201提供用于关联数据的输入，例如关联数据的n个向量(AD1…AD n)。单元K 202是要使用的密钥，至少包括加密密钥k2。它也可以由k1和k2两个部分组成：k1是可以用于完整性检查的完整性密钥，并且k2是用于加密/解密的密钥。单元HASH 310是散列函数，例如使用基于密码的消息验证代码([CMAC])模式下的AES的伪随机函数，或者在k1的情况下使用的HMAC_SHA256、HMAC_SHA384或HMAC_SHA512[RFC 4868]，或者在不使用K1时的类似SHA256、SHA384或SHA512之类的普通散列函数，参见[RFC 6234]。HASH单元310的输出用作用于加密单元ENCR 315的初始化向量(IV)，其基于加密密钥k2生成加密数据C 322。合适的加密的范例是如上所述的计数器模式下的AES，它是可以在本文中选择的众多密码之一。HASH单元310的输出

是由在计数器模式下的AES使用的初始化向量。使用计数器模式,可以处理任何长度的明文,相反,对于其他模式,例如密码块链接(CBC),仅可以处理密码块长度倍数的明文长度。合适的加密算法的其他范例是电子代码本(ECB)、密码块链接(CBC)、输出反馈(OFB)、密码反馈(CFB)中的AES,或者能够使用具有密文窃取(XTS)的基于XEX的调整后的代码本模式。对于前四个范例模式的说明,请参见[MODES],对于XTS-AES,请参见[XTS-AES]。

[0062] 用于HASH单元310的输入至少包括AD和V、由另一HASH单元HASH 311提供的P的散列。可选地,HASH单元还接收完整性密钥k1作为要被散列的输入的部分。并且,如果选择了密钥散列函数,则密钥HASH单元接收k1作为密钥。

[0063] 单元V 321存储HASH单元311的输出。因此,HASH单元311是执行散列函数的块。这可以是例如来自SHA2家族(SHA-224、SHA-256、SHA-384或SHA-512,请参见[RFC 6234])的散列函数,或使用P作为输入数据的单个分量的来自[RFC 5297]的S2V,或任何其他(优选是用密码写的)散列函数。用于创建以下表3和表4的实施例使用HASH单元311中的SHA-256和HASH单元310中的S2V。HASH单元311也可以是如下面在附图6、7、8和9中所阐明的密钥HASH单元。

[0064] 加密数据C 322和与完整性值V相同的消息完整性值W都包括在消息Z 320中,例如C和V的并置。消息完整性值W也可以是完整性值V的受保护版本,例如,使用其他完整性密钥的加密版本。图10示出了确定W的另一范例。

[0065] 通过分析图4所示的框图,能够确定增强型系统的以下属性。表3中提供了范例支持。

[0066] 第一属性与AES-SIV的属性P1相同。由于散列函数的属性,明文P中的至少一比特的变化将导致用于块ENCR的初始化向量中的许多比特发生变化,因此也将导致加密明文C中的许多比特发生变化,另请参见表3中的实例2。

[0067] 第二属性与AES-SIV的属性P2相同。关联数据AD中的至少一比特的变化将导致用于块ENCR的初始化向量中的许多比特发生变化,因此也将导致加密明文C中的许多比特发生变化,另请参见表3中的实例3。

[0068] 第三属性与AES-SIV的属性P3相同。从图4中还可以明显看出,在能够开始加密之前,必须对明文P进行整体处理,因为明文的所有比特都在块HASH的计算中使用。

[0069]

实例	明文输入 P	AD 1	真实性值 V	加密输出 C
实例 1 使用[RFC 5297]的 A.1 的测试向量	11223344 55667788 99aabbcc ddee	10111213 14151617 18191a1b 1c1d1e1f 20212223 24252627	5a68d9ad f4fd31c0 4a6c8177 4c76e910	265f7491 a2c60ad8 4440e0c1 6cd7
实例 2 P 中的 1 比特更改	11223344 5567**7**788 99aabbcc ddee (1 个已更改的比特)	10111213 14151617 18191a1b 1c1d1e1f 20212223 2425262	**40bcc840** **e023e0be** **0c366b9d** **c58391fc** (126 个已更改的比特)	**a3cc3ae3** **7a2350c5** **58a9db04 8d8a**
实例 3 AD 1 中的 1 比特更改	11223344 55667788 99aabbcc ddee	10**0**11213 14151617 18191a1b 1c1d1e1f 20212223 24252627 (1 个已更改的比特)	5a68d9ad f4fd31c0 4a6c8177 4c76e910 (56 个已更改的比特)	**3f04dd60** **11a2db82** **e64610d8 5b3a**
用于加密的密钥来自[RFC 5297]的 A.1。 (fffefdfc fbfaf9f8 f7f6f5f4 f3f2f1f0 f0f1f2f3 f4f5f6f7 f8f9fafb fcfdfeff)				

[0070] 表3-用于增强加密的范例结果

[0071] 图5示出了增强解密的框图。在该图中,单元Z 320被布置为接收用于解密的输入消息,所述输入消息是通过参考图4所讨论的加密过程生成的。如上所述,消息包括加密数据C和基于完整性值V的消息完整性值W。单元V 321在必要时通过首先解密值W来检索完整性值V。参考图11讨论根据消息确定V的其他范例。单元C 322检索加密数据C,其是根据图4加密的明文P。完整性值V用于检查比较器CMP 330中接收到的数据的有效性(完整性和真实性)。单元K 202具有要使用的秘密密钥(k),其可以分为两部分,k1和k2。k1是可以用于真实性/完整性检查的完整性密钥,而k2是可以用于加密/解密的密钥。单元AD 201具有关联数据,其可以与消息Z 320一起传输,或者单独传输。

[0072] 单元DECR 335是使用与以上在图4中选择的加密兼容的解密执行对来自单元C 322的加密数据进行解密的块,例如在计数器模式下的AES,参见[MODES]。加密密钥k2也是解密密钥,并且初始化向量IV由HASH单元310的输出提供。

[0073] 单元P'205从块DECR接收解密的明文输出。仅当有效性检查为肯定时,才可以使用明文输出。

[0074] HASH单元310是执行与图4所示的加密中的HASH单元310相同的散列函数的块。用于HASH单元310的输入至少包括AD和V(从接收到的消息完整性值W导出)。可选地,散列单元310还接收完整性密钥k1作为要被散列的输入的一部分。并且,如果使用密钥散列函数,则密钥HASH单元接收k1作为密钥。

[0075] HASH单元311是使用P’作为单个分量作为输入来执行与图4所示的加密中的HASH单元311相同的散列函数的块。以下用于创建表3和表4的实施例使用HASH单元311中的SHA-256和HASH单元310中的S2V。

[0076] 测试值T 323是散列单元311的输出,并被提供给比较器CMP 330,在比较器CMP 330中,将T与接收到的V进行比较。如果它们相等,则有效性检查为肯定,并且解密明文P’与加密期间使用的明文P相同。如果T和V不相等,则完整性测试将失败,并且必须丢弃解密明文P’。

[0077] 能够通过分析图5中的解密框图来确定上述增强密码的植入的以下属性,而支持该属性的范例能够在表4中找到。

[0078] 第四属性与AES-SIV的属性P4相同。使用正确的关联数据,不变的完整性值V和不变的加密数据C作为用于解密的输入将导致与加密期间使用的明文P相同的解密明文P’。此外,在这种情况下,T等于V,因此增强密码不检测真实性/完整性错误。另请参见表4中的实例4。

[0079] 第五属性被增强并且不同于AES-SIV的属性P5。用于C的解密的关联数据中的至少一比特的变化将导致解密明文P’中的许多比特不同于加密期间使用的明文P。与AES-SIV一样,在这种情况下,增强密码检测真实性/完整性错误。另请参参见表4中的实例5。然而,与AES-SIV相反,如果附加数据AD已经被操纵,则P’不可用。

[0080] 第六属性与AES-SIV的属性P6相同。用于C的解密的完整性值V的至少一比特的变化导致解密明文P’中的许多比特不同于加密期间使用的明文P。这是因为V也被输入到产生初始化向量的HASH单元310。并且,在这种情况下,检测真实性/完整性错误。另请参见表4中的实例6。

[0081] 第七属性与AES-SIV的属性P7相同。用于解密的加密输入C的至少一个比特的变化导致解密明文P’中相应比特变化。在这种情况下,增强密码检测完整性错误。另请参见表4中的实例7。

[0082]

实例	用于解密的 AD 1	用于解密的真实性值 V	用于解密的加密输入 C	解密输出 P’	T=V
实例 4 在 AD、V 和 C 中无变化	10111213 14151617 18191a1b 1c1d1e1f 20212223 24252627	5a68d9ad f4fd31c0 4a6c8177 4c76e910	265f7491 a2c60ad8 4440e0c1 6cd7	11223344 55667788 99aabbcc ddee (与 P 相同)	是

[0083]

实例	用于解密的 AD 1	用于解密的真实性值 V	用于解密的加密输入 C	解密输出 P'	T=V
实例 5 在 AD 1 中的 1 比特变化	1000 11213 14151617 18191a1b 1c1d1e1f 20212223 24252627 (1 个已更改的比特)	5a68d9ad f4fd31c0 4a6c8177 4c76e910	265f7491 a2c60ad8 4440e0c1 6cd7	**08799ab5 e602a6d2 3bac4bd5 ea03** (56 个已更改的比特)	否
实例 6 在 V 中的 1 比特变化	10111213 14151617 18191a1b 1c1d1e1f 20212223 24252627	5a68d9ad f4dd31c0 4a6c8177 4c76e910 (1 个已更改的比特)	265f7491 a2c60ad8 4440e0c1 6cd7	12d181f7 834ae372 850c6066 263f (62 个已更改的比特)	否
实例 7 在 C 中的 1 比特变化	10111213 14151617 18191a1b 1c1d1e1f 20212223 24252627	5a68d9ad f4fd31c0 4a6c8177 4c76e910	265f7491 a2c60ad0 4440e0c1 6cd7 (1 个已更改的比特)	11223344 55667780 99aabbcc ddee (1 个已更改的比特)	否
用于加密和解密的密钥来自[RFC 5297]的 A.1 。 在加密期间使用来自[RFC 5297]的 A.1 的明文 P and AD 1，以产生（不变的）初始向量 V 和加密输入 C。					

[0084] 表4-用于增强解密的范例结果

[0085] 在上述范例中,计数器模式下的AES用于加密和解密。然而,本发明不限于这种密码或模式。能够使用任何计数器中的密码,例如能够使用计数器模式下的DES或3DES。在[3DES]中对3DES进行了详细说明。DES最初于1977年1月被NIST批准为FIPS46。而且,可以使用任何模式下的任何密码。例如,能够使用电子代码本(ECB)、密码块链接(CBC)、输出反馈(OFB)、密码反馈(CFB)或带密文窃取的基于XEX的调整后的代码本模式(XTS)的AES。对于前四种范例模式的说明,请参见[MODES],对于XTS-AES,请参见[XTS-AES]。模式的选择取决于

应用程序的要求,例如加密或解密是否是可并行的。然而,在[EVAL]中,有人主张,从本文提到的6种模式,“总体而言,[CTR]通常是实现仅隐私加密的最佳和最现代的方式。”图4和5示出了根据本发明的总体上的加密方案。在图4中,块“加密”能够是任何模式下的任何密码,使用密钥k2和块HASH 310的输出作为初始向量对输入P进行加密。HASH 310的函数也可以是S2V,如上文结合图2和3所描述的。同样,图5示出了根据本发明的总体上的解密方案,其中,“解密”能够是任何模式下的任何密码,使用密钥k2和块HASH 310的输出作为初始向量对输入C进行解密。

[0086] HASH单元310和/或HASH单元311还可以体现为如下方式,同时保持不能从输出重构输入的属性。例如,HASH单元可以提供数字签名,例如

[0087] • 密钥散列消息验证代码(HMAC),例如HMAC_SHA1[RFC 2104]或HMAC_SHA256/384/512[RFC 4868],使用(对称)密钥k4,该密钥可以独立于k1和/或k2,可以以某种方式导出或等于k1和/或k2,

[0088] • 使用公共密钥密码术的数字签名,例如数字签名算法(DSA)[FIPS186-4]、基于Rivest-Shamir-Adleman(RSA)的数字签名算法[FIPS 186-4]和椭圆曲线数字签名算法(ECDSA)[FIPS 186-4],使用公共密钥k5和私人密钥k6,其中加密使用私人密钥k6,解密使用公共密钥k5。

[0089] 图6示出了增强加密的第二范例。该框图具有与参考图4描述的上述增强加密类似的元素,但是以下方面是不同的。在图中,单元K 402是要使用的密钥。它由三部分组成:k1,k2和k3;k1是用于完整性检查的完整性密钥,并且k2是用于加密/解密的密钥,而k3是用于密钥HASH单元411中的密钥HASH的另一个完整性密钥。加密单元ENCR 315基于加密密钥k2和来自HASH单元310的初始化向量IV来生成加密数据C 422。

[0090] 用于HASH单元310的输入包括k1、AD和V(由密钥HASH单元411提供的P的散列)。单元V 421存储密钥HASH单元411的输出。加密数据C 422和基于完整性值V 421的消息完整性值W包含在消息Z 420中,例如C和V的并置。可选地,可以对V进行加密以产生消息完整性值W。

[0091] 图7示出了增强解密的第二范例。该框图具有与参考图5所描述的上述增强解密相似的元素,但是以下方面是不同的。在图中,单元Z 420接收通过如参考图6所讨论的加密过程生成的用于解密的输入消息。单元V 421从消息完整性值W检索完整性值V,而单元C 422检索加密数据C,它是根据图6加密的明文P。完整性值V用于检查比较器CMP 330中的接收到的数据的有效性(完整性和真实性)。单元K 402具有要使用的密钥,由k1、k2和k3三个部分组成。k1是用于真实性/完整性检查的完整性密钥,而k2是用于解密的密钥,并且k3是用于HASH单元411中的密钥散列函数的另一个完整性密钥。

[0092] 单元DECR 335是使用如以上在图6中选择的加密兼容的解密来执行对来自单元C 422的加密数据的解密的块。加密密钥k2也是解密密钥,并且初始化向量IV由HASH单元310的输出提供。用于HASH单元310的输入包括k1、AD和V(如从W导出或从W解密的)。单元P’205从块DECR接收解密的明文输出。仅当有效性检查为肯定时,才可以使用明文输出。

[0093] HASH单元411是在使用P’作为输入的同时执行与图6所示的加密中的HASH单元411相同的密钥散列函数的块。测试值T 423是密钥散列单元411的输出,并且被提供给比较器CMP 330,在比较器CMP 330中,将T与接收到的V进行比较。如果它们相等,则有效性检查为

肯定,并且解密明文P'等于加密期间使用的明文P。如果T和V不相等,则完整性测试失败,并且必须丢弃解密明文P'。

[0094] 图8示出了增强加密的第三范例。该框图具有与参考图4和6所述的上述增强加密类似的元素,但在以下方面是不同的。在图中,单元K 502是要使用的密钥。它由k2和k3两部分组成;k2是用于加密/解密的密钥,而k3是用于在P上操作的密钥HASH单元411中的密钥HASH的完整性密钥。加密单元ENCR 315基于加密密钥k2和来自HASH单元510的初始化向量IV来生成加密数据C 522。

[0095] 用于HASH单元510的输入包括AD和V(由密钥HASH单元411提供的P的散列)。单元V 421存储密钥HASH单元411的输出。加密数据C 522和完整性值V 421包括在消息Z 520中。可选地,可以对V进行加密以产生消息完整性值W。

[0096] 图9示出了增强解密的第三范例。该框图具有与参考图5和7所述的上述增强解密相似的元素,但在以下方面是不同的。在图中,单元Z 520接收如参考图8所讨论的由加密处理生成的用于解密的输入消息。单元V 421使用消息完整性值W来检索完整性值V,如上所述,而单元C 522检索加密数据C,它是根据图8加密的明文P。完整性值V用于检查比较器CMP 330中所接收的数据的有效性(完整性和真实性)。单元K 502具有要使用的密钥,由k2和k3两部分组成。k2是用于解密的密钥,并且k3用于密钥HASH单元411中的密钥HASH。

[0097] 单元DECR 335是使用与在图8中所选择的以上加密兼容的解密来执行来自单元C 522的加密数据的解密的块。加密密钥k2也是解密密钥,并且初始化向量IV由HASH单元510的输出提供。用于HASH单元510的输入是AD和V(从W接收的或解密的)。单元P'205从块DECR接收解密的明文输出。仅当有效性检查为肯定时,才可以使用明文输出。

[0098] HASH单元411是使用k3和P'作为输入来执行与图8所示的加密中的密钥HASH单元411相同的密钥散列函数的块。测试值T 423是密钥HASH单元411的输出,并且被提供给比较器CMP 330,在比较器CMP 330中,将T与接收到的V进行比较。如果它们相等,则完整性检查为肯定,并且解密明文P'等于加密期间使用的明文P。如果T和V不相等,则完整性测试失败,并且必须丢弃解密明文P'。

[0099] 看来,增强密码的第三个范例既实用又强大。密钥k仅由两部分组成,而由于单元HASH 411中的密钥散列,很难从完整性值V获得明文P。另一方面,还可能对于两个HASH单元使用两个预定义的散列函数,即没有秘密密钥的散列,仅需要同时用于加密和解密的单个秘密加密密钥k2。

[0100] 图10示出了增强加密的第四范例。该框图具有与参考图4描述的上述增强加密类似的元素,但是在以下方面是不同的。在图中,单元K 602是要使用的密钥,至少包括加密密钥k2。它也可以由k4和k2两部分组成;k4是可以用于另一HASH单元H3 624的完整性密钥,并且k2是将用于加密/解密的密钥。单元HASH 510是散列函数,例如,如参考图8所描述的。HASH单元510的输出被用作用于加密单元ENCR 315的初始化向量(IV),加密单元ENCR 315基于加密密钥k2生成加密数据C 522。上面已经讨论了合适的加密的范例。

[0101] 用于HASH单元510的输入至少是AD和V(由另一HASH单元HASH 311提供的P的散列),如上所述。可选地,类似于参考图4讨论的HASH单元310,HASH单元还接收完整性密钥k1作为要被散列的输入的一部分。并且,如果选择密钥散列函数,则密钥HASH单元接收k1作为密钥。

[0102] 单元HASH 311是散列函数,例如,如参考图4所描述的。可选地,HASH单元还接收完整性密钥k3作为要被散列的输入的一部分,如图6或图8中。此外,如果选择密钥散列函数,则密钥HASH单元接收k3作为钥。单元HASH 311具有P 203作为输入。

[0103] 加密单元E2 621从HASH单元311接收完整性值V,并且从另一HASH单元H3 624接收导出密钥kc。加密单元621对V进行加密以生成消息完整性值W。另一HASH单元624使用加密数据C作为输入。另一HASH单元H3 624可以类似于第一和第二HASH单元,并且可以是密钥HASH单元,其从密钥单元602接收其他的秘密完整性密钥k4。

[0104] 加密数据C 522和基于完整性值V的消息完整性值W包括在消息Z 620中,例如C和W的并置。消息完整性值现在是完整性值V的受保护版本,即,使用导出密钥kc的加密版本。有效地是,保护完整性值免受操纵,同时也不能在不干扰C的解密的情况下操纵加密数据C。因此,C中的单个比特变化将导致解密明文中的许多比特发生变化,如下所阐明的。

[0105] 图11示出了增强解密的第四范例。该框图具有与参考图5所描述的上述增强解密相似的元素,但在以下方面是不同的。在图中,单元Z 620接收如由参考图10所讨论的加密过程生成的用于解密的输入消息。

[0106] 单元D2 625使用来自另一个散列单元H3 624的导出密钥kc通过解密消息完整性值W来导出完整性值V。另一个散列单元H3 624是执行与图10中所示的加密中的另一个散列单元H3 624相同的散列函数的块。另一个HASH单元624的输入是接收到的加密数据C。因此,C中的单个比特变化将导致非常不同的导出密钥kc,并因此导致非常不同的完整性值V和非常不同的初始化向量IV,这因此也将导致非常不同的解密明文P'。另一个HASH单元H3 624可以是密钥HASH单元,其从密钥单元602接收另一个秘密完整性密钥k4。单元C 522检索加密数据C,加密数据C是根据图10加密的明文P。

[0107] 完整性值V用于检查比较器CMP 330中的接收到的数据的有效性(完整性和真实性)。单元K 602具有要使用的秘密密钥(k),它可以由k4和k2两部分组成。密钥k4是可以用于密钥HASH单元624的另一个秘密完整性密钥,而k2是用于加密/解密的密钥。

[0108] HASH单元510至少接收附加数据AD和完整性值V作为输入。可选地,HASH单元510还接收完整性密钥k1作为要被散列的输入的一部分。并且,如果使用密钥散列函数,则密钥HASH单元510接收k1作为密钥。散列单元510是执行与在图10所示的加密中的HASH单元510相同的散列函数的块。

[0109] 测试值T是HASH单元311的输出,并且被提供给比较器CMP 330,在比较器CMP 330中,将T与从消息完整性值W解密的完整性值V进行比较。如果它们相等,则有效性检查为肯定,并且解密明文P'与加密期间使用的明文P相同。如果T和V不相等,则完整性测试失败,并且必须丢弃解密明文P'。

[0110] 看来,增强密码的第四范例既实用又强大。密钥k仅由两部分组成,同时由于单元624中的密钥散列,难以获得明文P和完整性值V。另一方面,也可以使用用于所有HASH单元的三个预定义的散列函数,即,没有秘密密钥的散列,其只需要用于加密和解密的单个秘密加密密钥k2。尽管可以随后由知道加密数据C的任何人检索值V,在最终接收器处不打扰解密和完整性测试的C的操纵仍然是不可能的。

[0111] 图12示出了用于对输入数据进行加密并且保护输入数据和关联数据的完整性的加密方法。在该方法中,加密过程在节点START 701处开始。在第一阶段RCV-DAT 702中,接

收明文P和关联数据AD。接下来,在阶段INTEGR 703中,使用第一散列函数基于明文P计算完整性值V。接下来,在阶段INIT VEC 704中,基于完整性值和关联数据通过使用第二散列函数来计算初始化向量,所述初始化向量与完整性值不同。一个或两个完整性密钥可以用于散列函数,以计算完整性值和/或初始化向量。接下来,在阶段ENCR 705中,使用初始化向量IV和第二加密密钥k2对输入数据P进行加密以生成加密数据C。接下来,在阶段OUT-MSG 706中,生成包括加密数据C和完整性值V的输出加密消息。接下来,除非接收到其他输入数据,否则过程在阶段END 708终止。如果是这样,则该方法在阶段RCV-DAT处继续,如箭头720所示。

[0112] 在实施例中,方法包括在第一阶段RCV-DAT中确定输入数据的量。一旦确定所述量低于预定阈值,将填充数据添加到输入数据,以增加要在一个消息中加密的明文的总量,例如通过在原始明文的开头或结尾处并置填充数据。填充数据可以例如是随机数据或全零数据。例如,如果仅允许密码块长度的倍数的明文长度,则可能需要填充。可选地,预定阈值是加密密钥的长度。填充数据的长度或明文的量可以包括在消息中,例如作为附加数据的一部分。

[0113] 此外,应当注意,加密方法可以包括在阶段OUT-MSG 706中,向消息添加更多数据。然而,输出加密消息将不包含初始化向量,因为这会损害数据保护。例如,在那种情况下,恶意设备可能使用包括在消息中的初始化向量,而不是如现在已经阐明的解密方法中的阶段INIT-VEC 752中所要求的那样经由所述第二散列函数来计算初始化向量。

[0114] 图13示出了用于对加密数据进行解密并且确定数据和关联数据的完整性的解密方法。在该方法中,解密过程在节点START 751处开始。在第一阶段RCV-MSG 752中,接收消息。所获得的加密消息包含都是从消息中检索的加密数据C和完整性值V。而且,与消息一起或单独接收关联数据AD。接下来,在阶段INIT-VEC 753中,基于完整性值和关联数据来计算初始化向量IV,所述初始化向量不同于完整性值。计算涉及散列函数。接下来,在阶段DECRYP 754中,使用初始化向量IV和解密密钥k2对加密数据C进行解密以生成明文P'。接下来,在阶段CALC-T 755中,使用其他散列函数(其等于在加密期间使用的相应散列函数)基于明文P'计算测试值T。一个或两个完整性密钥可以用于散列函数,以计算完整性值和/或初始化向量。接下来,在阶段COMP 756中,比较测试值T和接收到的值V,以通过将测试完整性值和接收到的完整性值进行比较来确定完整性。接下来,一旦在阶段757中确定T等于V,则该过程在阶段END 758处以成功终止。但是,一旦在阶段759中确定T不等于V,则该过程在阶段ABORT 760以失败终止。

[0115] 方法可以例如由固定或移动计算设备中的处理器中的电路和软件执行。上面已经描述了合适的散列函数、加密和解密函数。应当注意,图13示出了用于具有解密作用的设备的方法,所述方法可以与嵌入图12的加密方法的设备协作。

[0116] 如本领域技术人员将显而易见的,实现该方法的许多不同方式是可能的。例如,阶段或步骤的顺序可以改变,或者某些阶段可以并行执行。此外,在步骤之间可以插入其他方法步骤。所插入的步骤可以表示诸如本文所述的方法的改进,或者可以与方法无关。

[0117] 提供可从网络下载和/或存储在计算机可读介质和/或微处理器可执行介质上的计算机程序产品,其包括用于在计算机设备上执行时实现上述方法、连接序列、安全性过程和其他操作的程序代码指令。因此,可以使用软件来执行根据本发明的方法,所述软件包括

用于使处理器系统执行相应方法的指令。

[0118] 通常,执行上述加密过程的设备中的每一个都包括耦接到存储器的处理器,所述存储器包含存储在设备处的适当的软件代码;例如,该软件可以是已经下载的和/或存储在相应存储器中的,例如,诸如RAM之类的易失性存储器或诸如闪存之类的非易失性存储器(未示出)。设备可以例如配备有微处理器和存储器(未示出)。可选择地,可以全部或部分地以可编程逻辑,例如作为现场可编程门阵列(FPGA))来实现设备。设备和服务器可以全部或部分地实现为所谓的专用集成电路(ASIC),即针对其具体用途定制的集成电路(IC)。例如,可以例如使用诸如Verilog、VHDL等的硬件描述语言在CMOS中实现电路。

[0119] 软件可以仅包括由系统的具体子实体采取的那些步骤。软件可以存储在诸如硬盘、软盘、存储器等的合适的存储介质中。软件可以作为信号沿着有线、无线或使用诸如因特网的数据网络发送。可以使软件可用于服务器上的下载和/或远程使用。可以使用布置为配置可编程逻辑(例如,现场可编程门阵列(FPGA))以执行方法的比特流来执行根据本发明的方法。应当理解,软件可以是源代码、目标代码、源代码和目标代码中间的代码(例如部分编译形式的)的形式,或者是适合用于实现根据本发明的方法的任何其他形式。涉及计算机程序产品的实施例包括与所阐述的至少一种方法中的每个处理步骤相对应的计算机可执行指令。这些指令可以细分为子例程和/或存储在一个或多个可以静态或动态链接的文件中。涉及计算机程序产品的另一实施例包括与所阐述的至少一个系统和/或产品的每个装置相对应的计算机可执行指令。

[0120] 图14a示出了具有包括计算机程序1020的可写部分1010的计算机可读介质1000,计算机程序1020包括用于使处理器系统执行参考图1、图4至图11所述的一种或多种上述方法和过程的指令。计算机程序1020可以作为物理标记或借助于对计算机可读介质1000的磁化而体现在计算机可读介质1000上。但是,也可以想象任何其他合适的实施例。此外,应当理解,尽管计算机可读介质1000在本文中被示为光盘,但是计算机可读介质1000可以是诸如硬盘、固态存储器、闪存等的任何合适的计算机可读介质,并且可以是不可记录的或可记录的。计算机程序1020包括用于使处理器系统执行所述方法的指令。

[0121] 图14b以示意性表示示出了根据参考图1、图4至图11所描述的设备或方法的实施例的处理器系统1100。处理器系统可以包括电路1110,例如一个或多个集成电路。在图中示意性示出了电路1110的架构。电路1110包括处理单元1120,例如CPU,用于运行计算机程序组件以执行根据实施例的方法和/或实现其模块或单元。电路1110包括用于存储编程代码、数据等的存储器1122。存储器1122的一部分可以是只读的。电路1110可以包括通信元件1126,例如天线、收发器、连接器或两者、等等。电路1110可以包括专用集成电路1124,用于执行方法中所定义的部分或全部处理。处理器1120、存储器1122、专用IC 1124和通信元件1126可以经由互连1130(例如,总线)彼此连接。处理器系统1110可以被布置为分别使用连接器和/或天线进行有线和/或无线通信。

[0122] 应当理解,为清楚起见,以上详细说明参考不同的功能单元和处理器描述了本发明的实施例。但是,显而易见的是,可以在不背离本发明的情况下使用在不同功能单元或处理器之间的任何适当的功能的分布。例如,被图示为由分开的单元、处理器或控制器执行的功能可以由相同的处理器或控制器执行。因此,对特定功能单元的参照仅应被视为对用于提供所描述的功能的适当装置的参照,而不是指示严格的逻辑或物理结构或组织。能够以

任何适当的形式来实现本发明,包括硬件、软件、固件或它们的任何组合。

[0123] 应当注意,在本文件中,单词“包括”不排除存在所列元件或步骤之外的元件或步骤,并且元件之前的单词“一”或“一个”不排除存在多个这样的元件,任何附图标记不限制权利要求的范围,可以通过硬件和软件儿者来实现本发明,并且可以由相同的硬件或软件项来表示几个“装置”或“单元”,以及处理器以与硬件元件协作来实现一个或多个单元的功能。此外,本发明不限于实施例,并且本发明在于以上描述的或在互不相同的从属权利要求中叙述的每个新颖的特征或特征的组合。

[0124] 总而言之,设备被布置为用于对输入数据进行加密并且保护输入数据和关联数据的完整性。加密处理器具有被布置为基于输入数据来计算完整性值的第一HASH单元、被布置为基于完整性值和关联数据来计算初始化向量的第二HASH单元。HASH单元中的至少一个可以是密钥HASH单元。加密单元被布置为使用初始化向量和加密密钥对输入数据进行加密以生成加密数据。有效地是,初始化向量与完整性值是不同的。由于初始化向量取决于完整性值和关联数据,因此其中的任何变化都将导致解密失败,解密数据与原始明文P完全不同。

[0125] 参考文献:

[0126] [3DES]SP 800-67Rev.2,Recommendation for the Triple Data Encryption Algorithm(TDEA)Block Cipher

[0127] [CMAC]Dworkin,M.,"Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication",NIST Special Publication800-38B,May 2005.

[0128] [DH]Diffie,W.;Hellman,M.(1976),"New directions in cryptography",IEEE Transactions on Information Theory,22(6):644-654

[0129] [DSS]"Digital Signature Standard(DSS)",USA,National Institute of Standards and Technology,Federal Information Processing Standard(FIPS)186-4.

[0130] [EVAL]Phillip Rogaway,"Evaluation of Some Blockcipher Modes of Operation",University of California,Davis,February 10,2011.

[0131] [MODES]Dworkin,M.,"Recommendation for Block Cipher Modes of Operation:Methods and Techniques",NIST Special Publication 800-38A, 2001edition.

[0132] [RFC2104]"HMAC:Keyed-Hashing for Message Authentication",February 1997.

[0133] [RFC4868]"Using HMAC-SHA-256,HMAC-SHA-384,and HMAC-SHA-512 with IPsec",May 2007

[0134] [RFC5297]Synthetic Initialization Vector(SIV)Authenticated Encryption Using the Advanced Encryption Standard(AES),October 2008,(https://datatracker.ietf.org/doc/rfc5297/)

[0135] [RFC6234]US Secure Hash Algorithms(SHA and SHA-based HMAC and HKD,May 2011,(https://datatracker.ietf.org/doc/rfc6234/)

[0136] [XTS-AES]Dworkin,M.,"Recommendation for block cipher modes of operation:The XTS-AES mode of confidentiality on storage devices",NIST

Special Publication 800-38E,Jan.2010.

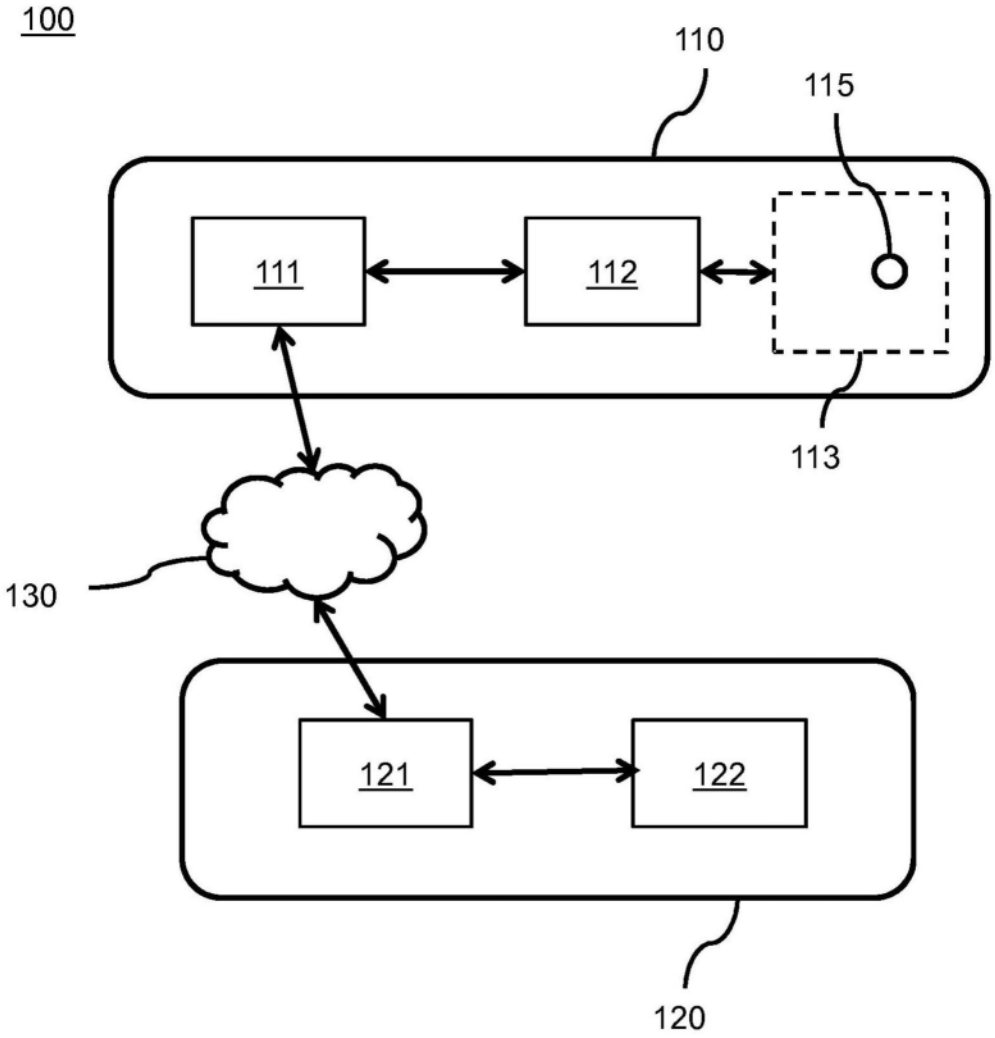


图1

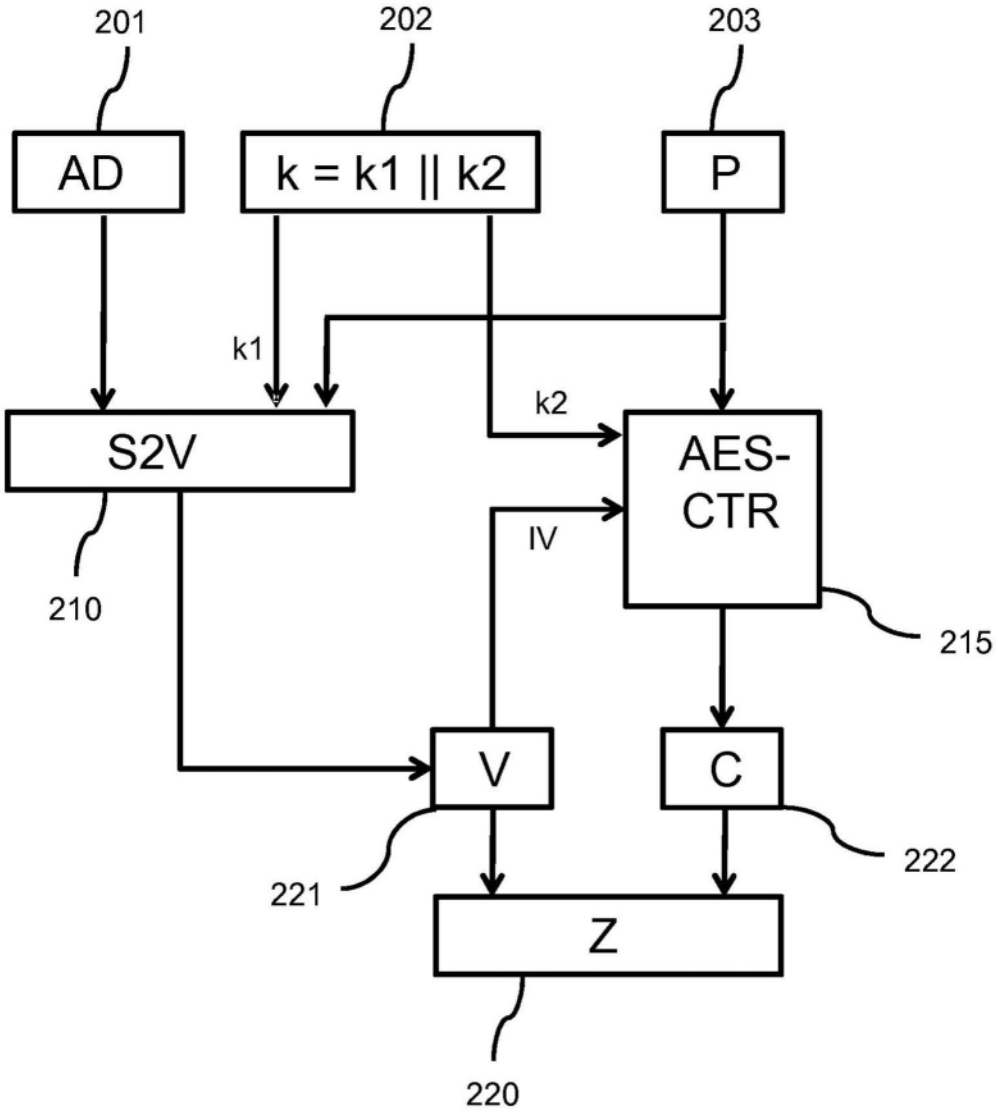

201
202
203
AD
k = k1 || k2
P
k1
k2
S2V
AES-
CTR
IV
210
215
V
C
221
222
Z
220

图2

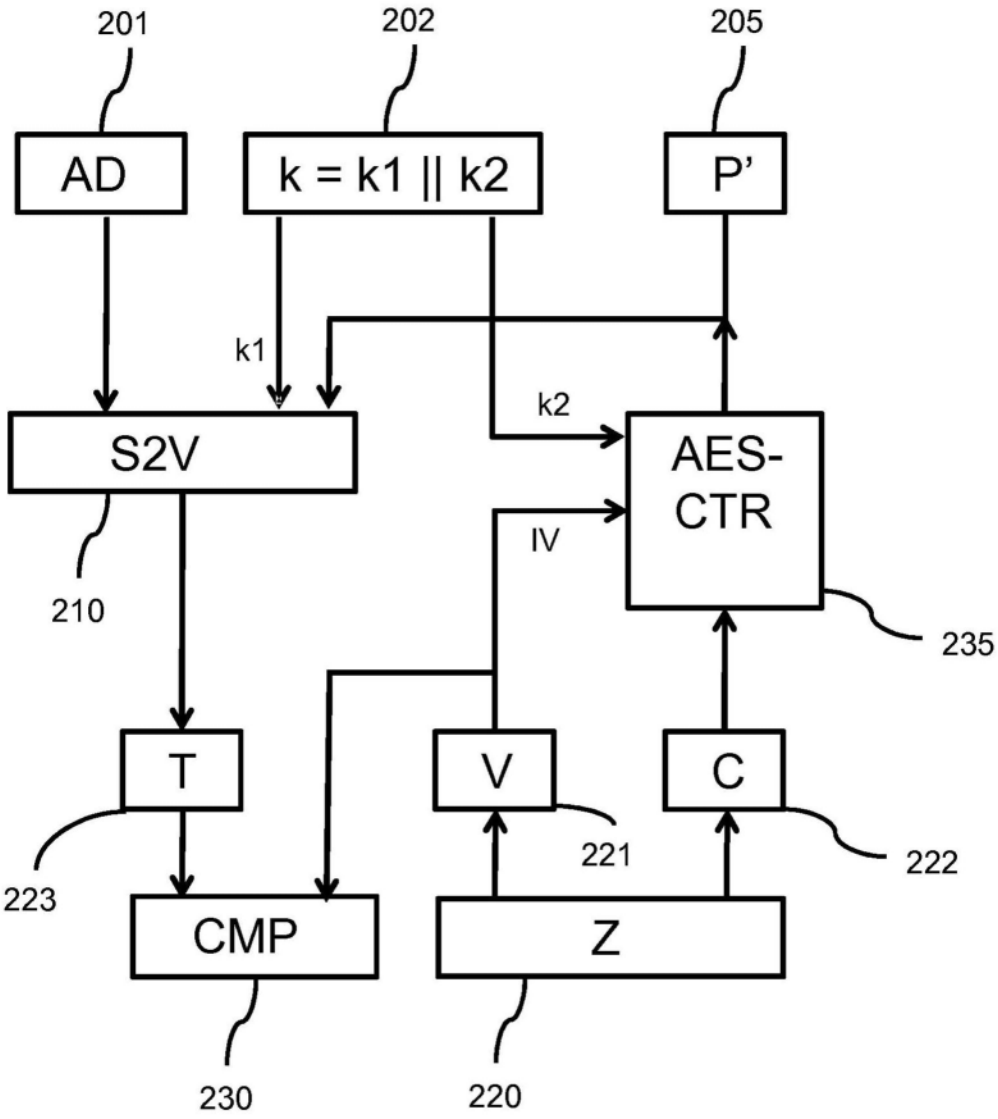

201
202
205
AD
k = k1 || k2
P'
k1
k2
S2V
AES-
CTR
IV
210
235
T
V
C
223
221
222
CMP
Z
230
220

图3

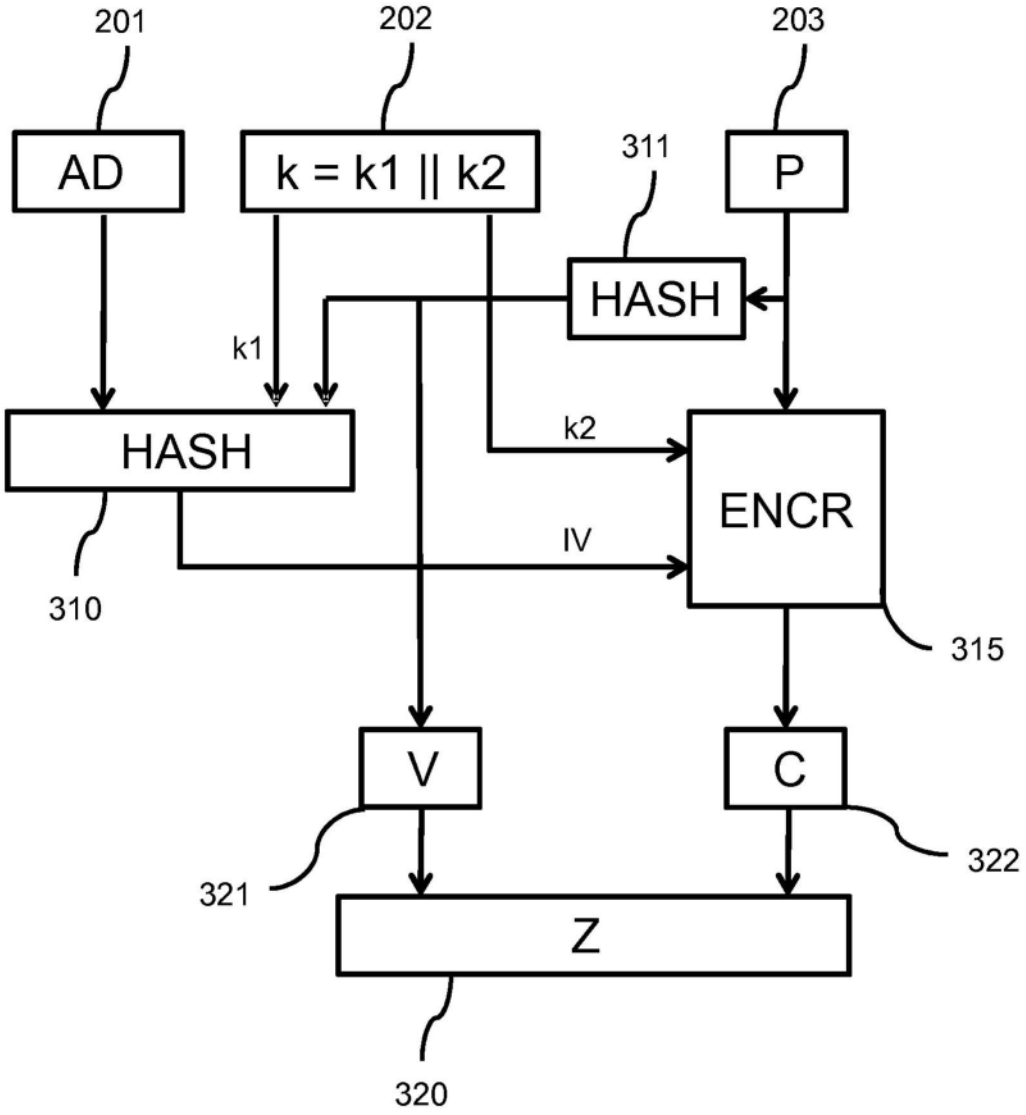

201
202
203
AD
k = k1 || k2
311
P
HASH
k1
HASH
k2
ENCR
IV
310
315
V
C
321
322
Z
320

图4

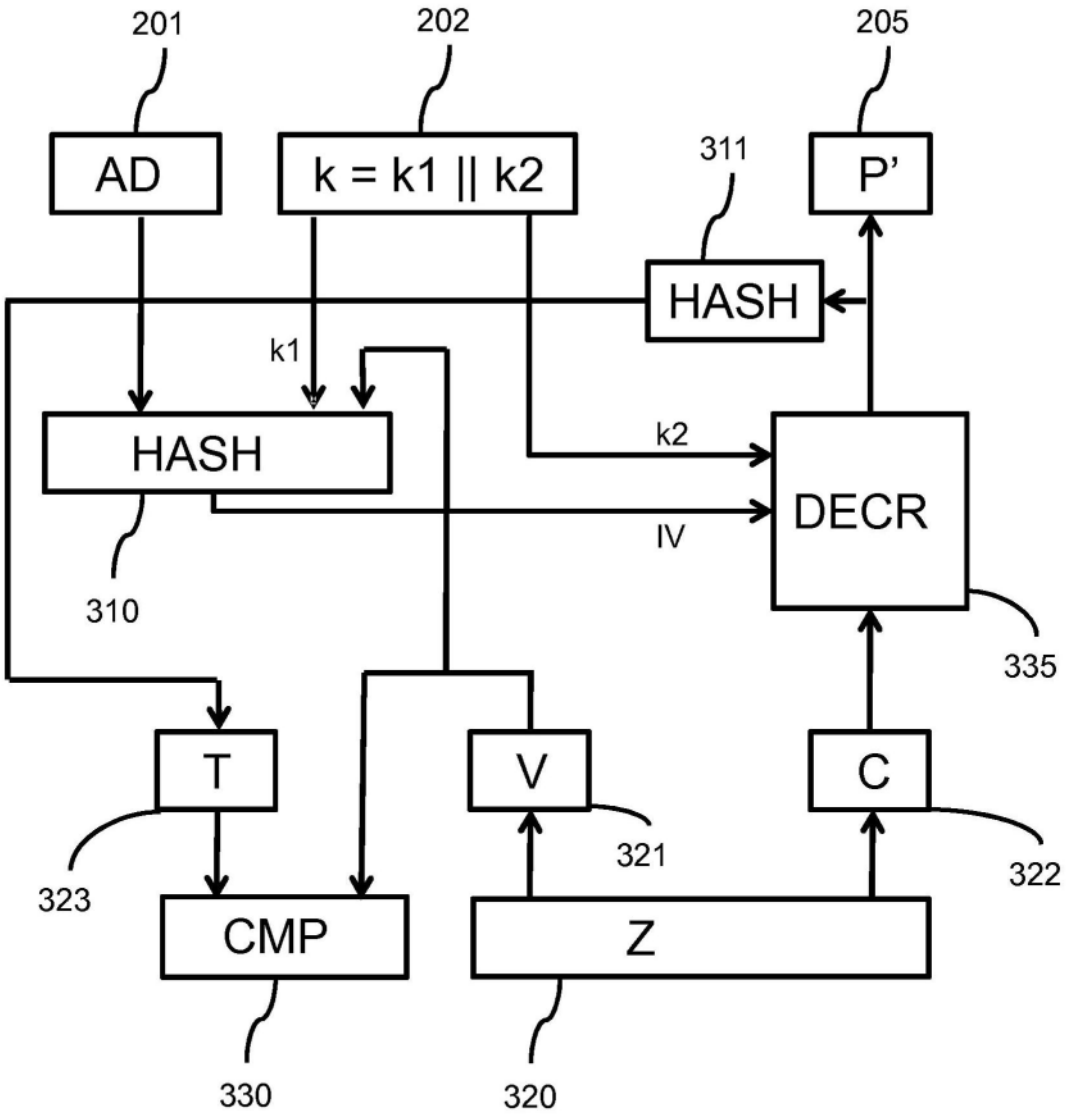

201
202
205
AD
k = k1 || k2
311
P'
HASH
k1
HASH
k2
DECR
IV
310
335
T
V
C
323
321
322
CMP
Z
330
320

图5

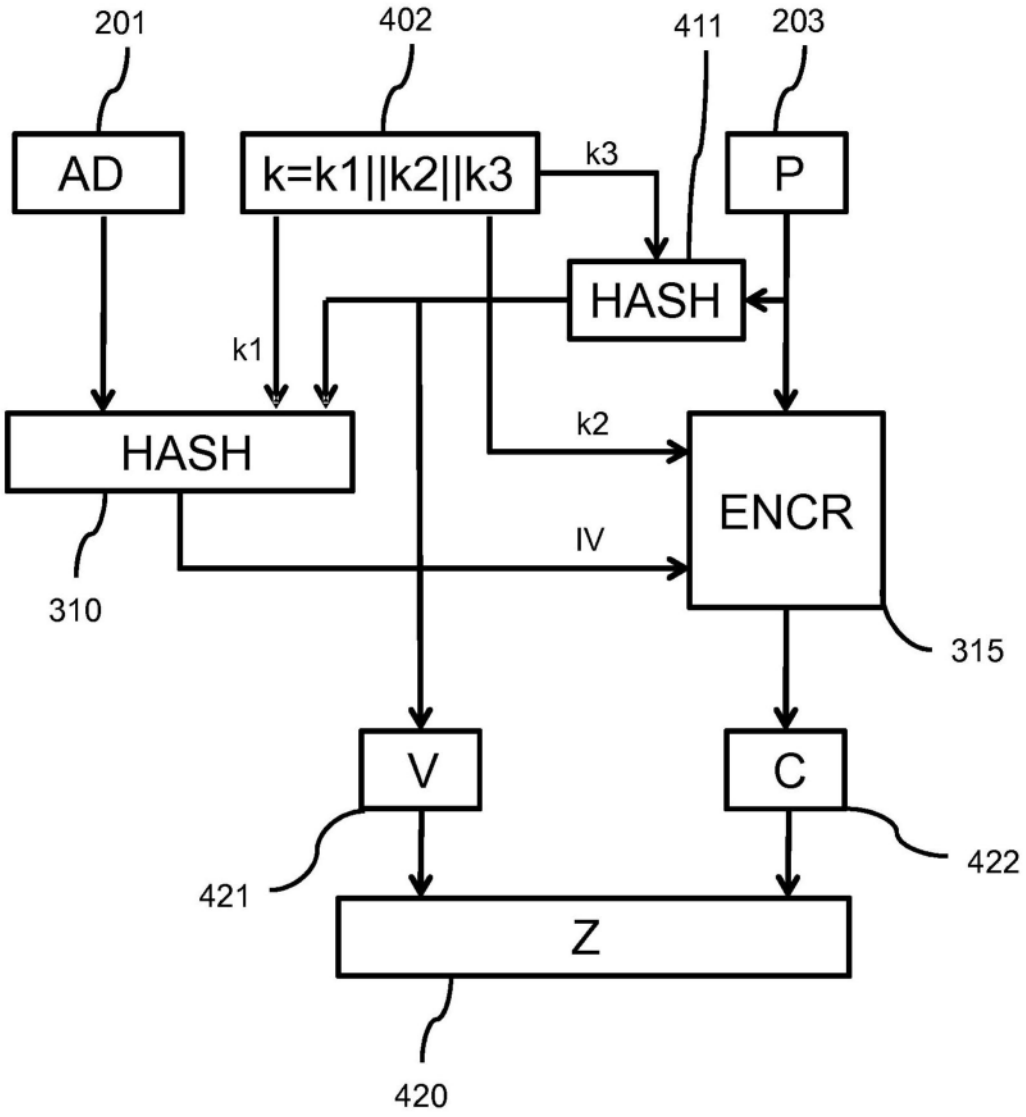

201
402
411
203
AD
k=k1||k2||k3
k3
P
HASH
k1
HASH
k2
ENCR
IV
310
315
V
C
421
422
Z
420

图6

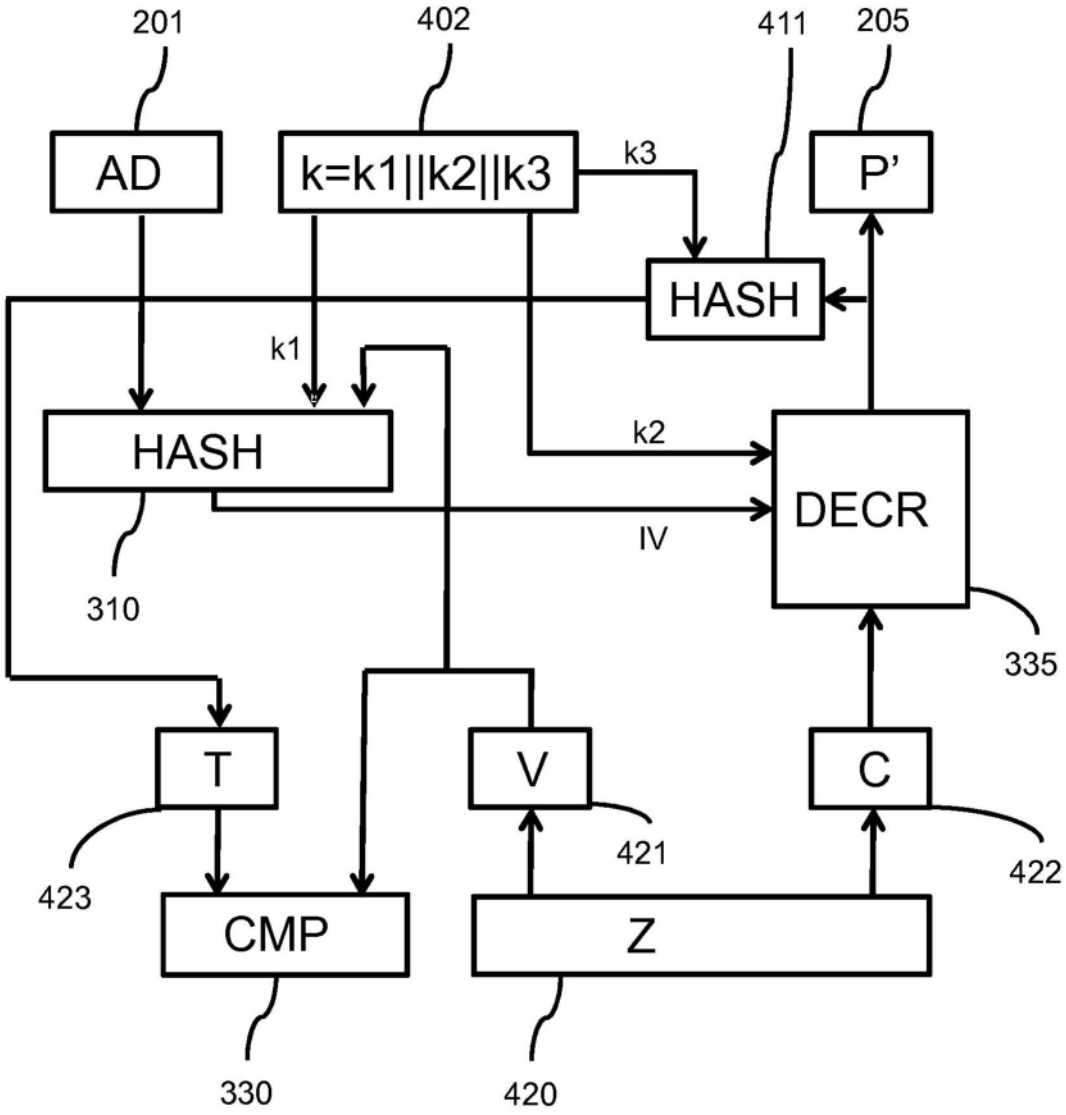

201
402
411
205
AD
k=k1||k2||k3
k3
P'
HASH
k1
HASH
k2
DECR
IV
310
335
T
V
C
423
421
422
CMP
Z
330
420

图7

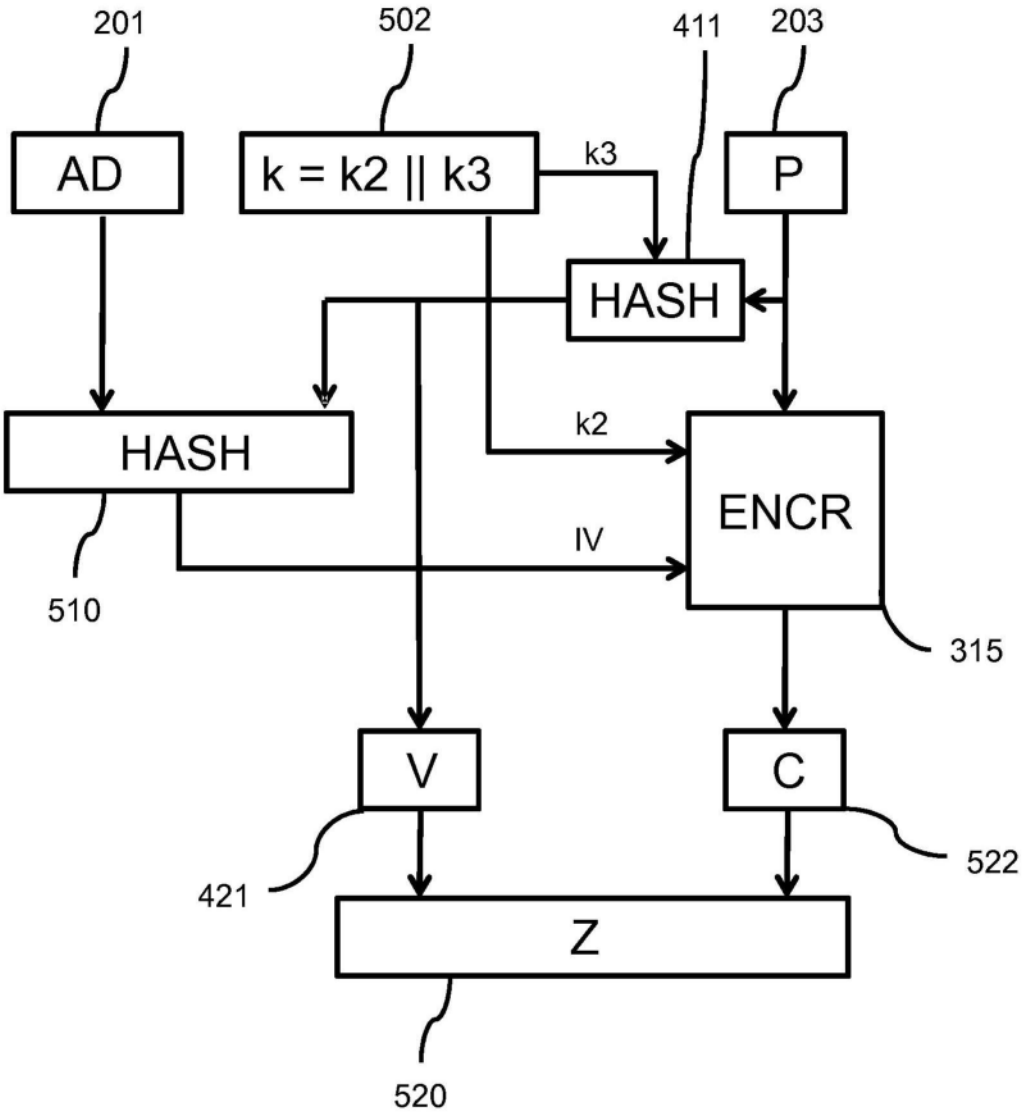

201
502
411
203
AD
k = k2 || k3
k3
P
HASH
HASH
k2
ENCR
IV
510
315
V
C
421
522
Z
520

图8

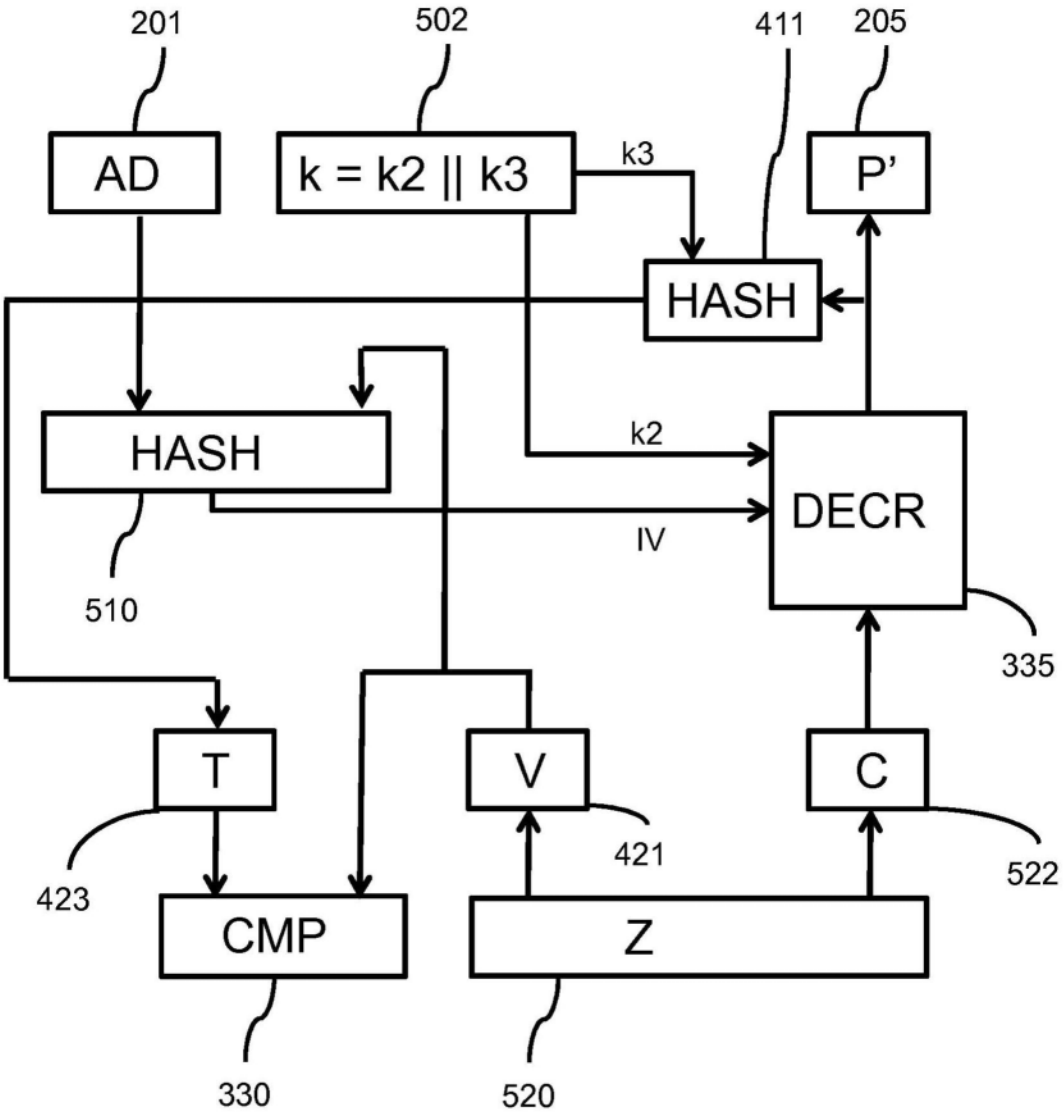

201
502
411
205
AD
k = k2 || k3
k3
P'
HASH
HASH
k2
DECR
IV
510
335
T
V
C
423
421
522
CMP
Z
330
520

图9

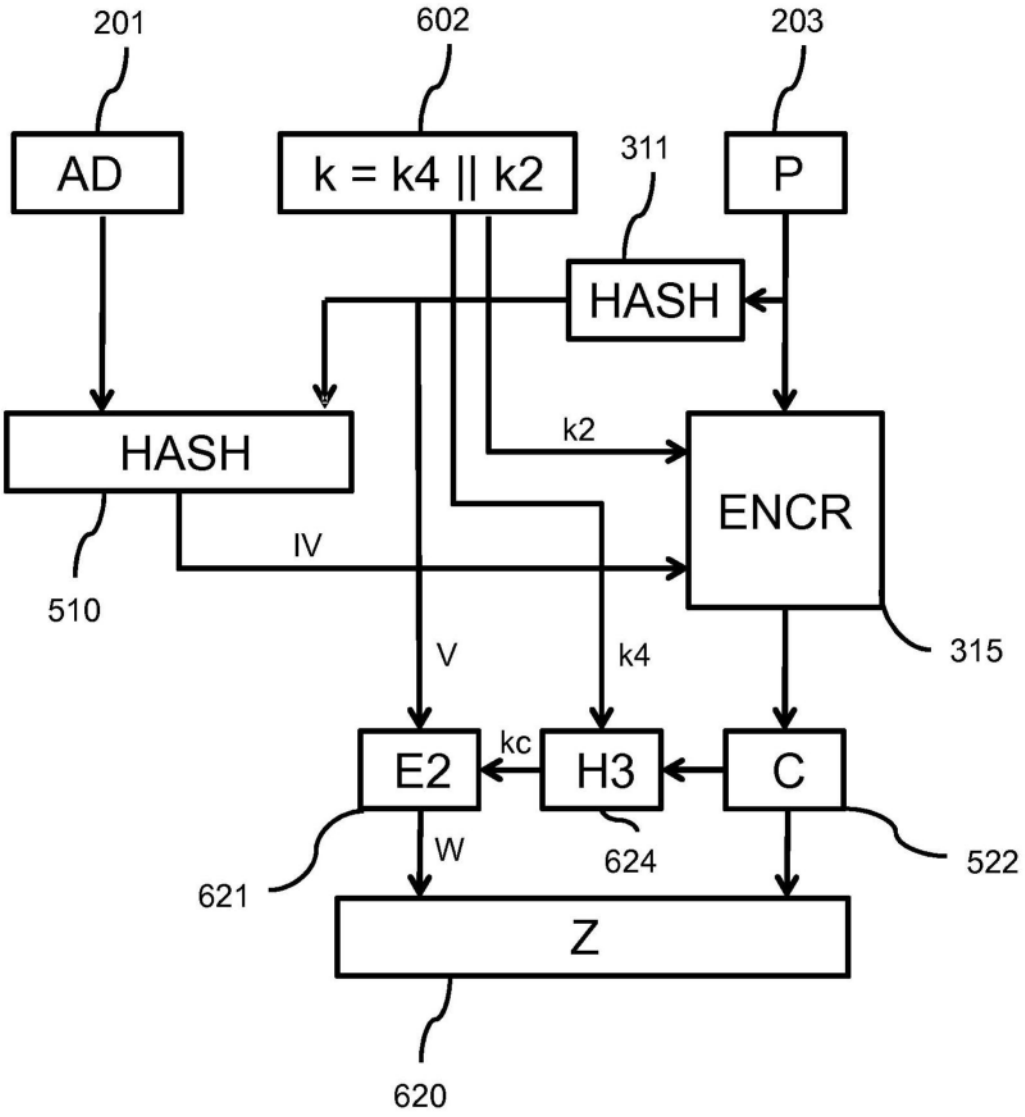

201
602
203
AD
k = k4 || k2
311
P
HASH
HASH
k2
ENCR
510
IV
315
V
k4
E2
kc
H3
C
W
624
621
522
Z
620

图10

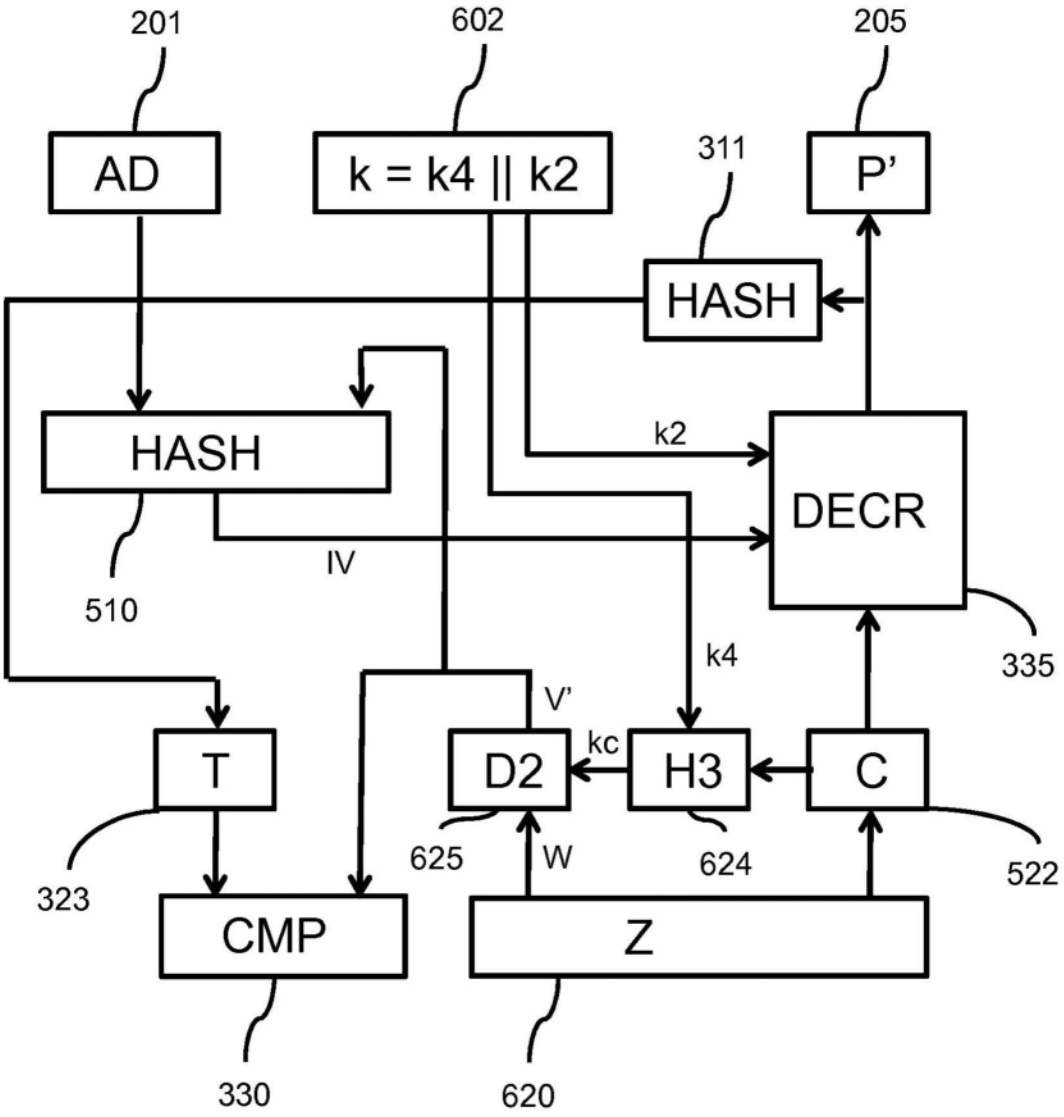

201
602
205
AD
k = k4 || k2
311
P'
HASH
HASH
k2
DECR
510
IV
335
k4
V'
T
D2
kc
H3
C
323
625
W
624
522
CMP
Z
330
620

图11

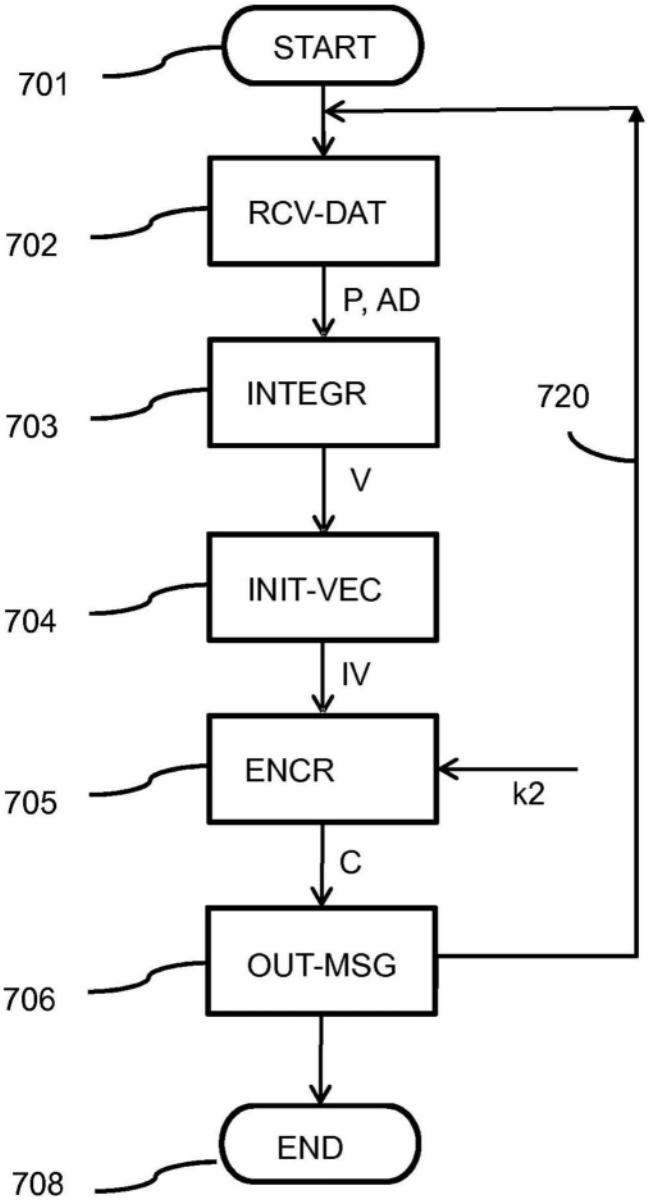

START
701
RCV-DAT
702
P, AD
INTEGR
703
720
V
INIT-VEC
704
IV
ENCR
705
k2
C
OUT-MSG
706
END
708

图12

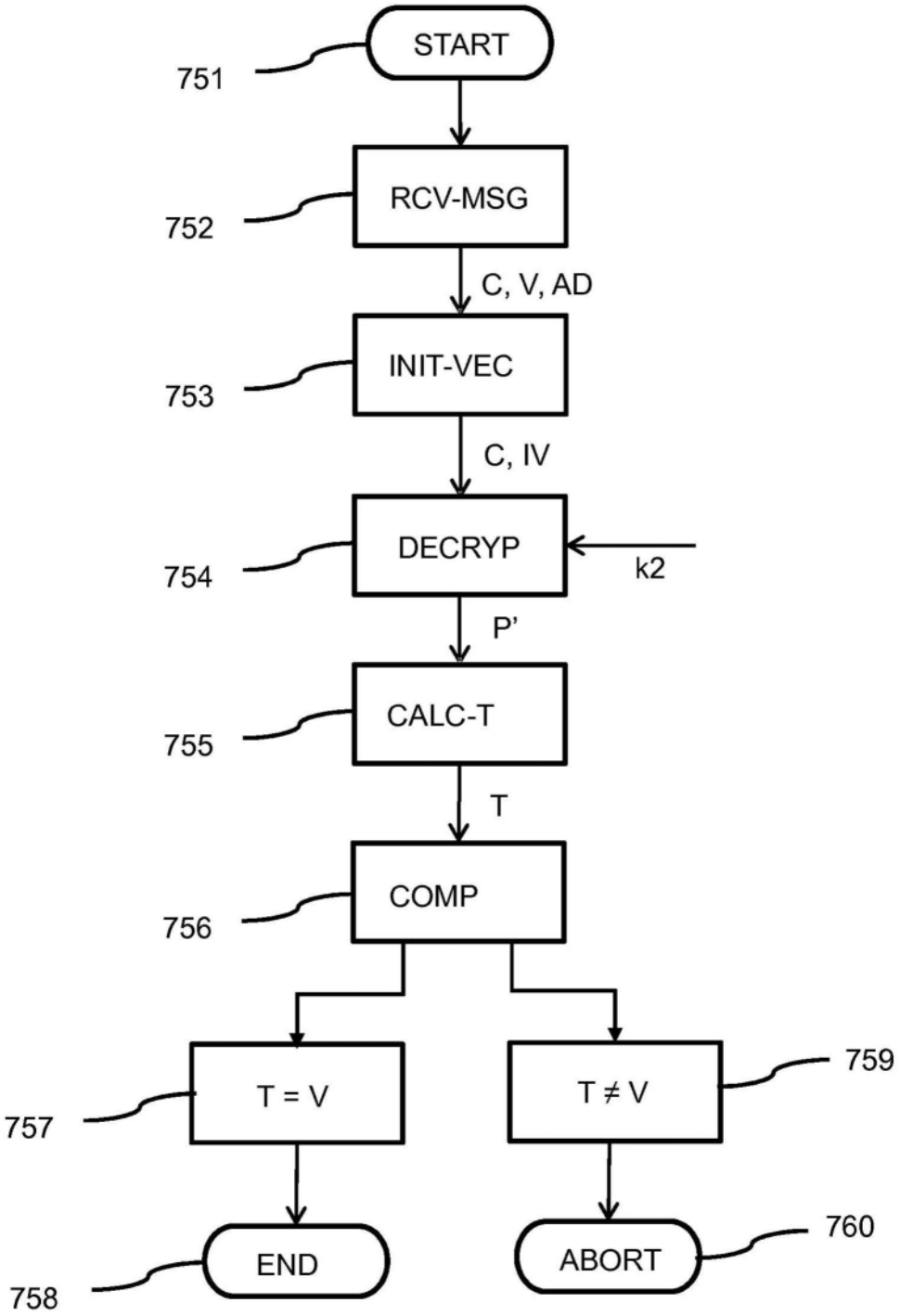

START
751
RCV-MSG
752
C, V, AD
INIT-VEC
753
C, IV
DECRYP
754
k2
P'
CALC-T
755
T
COMP
756
T = V
757
T ≠ V
759
END
758
ABORT
760

图13

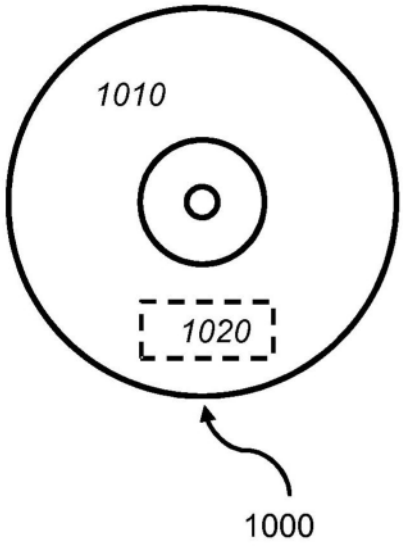


图14a

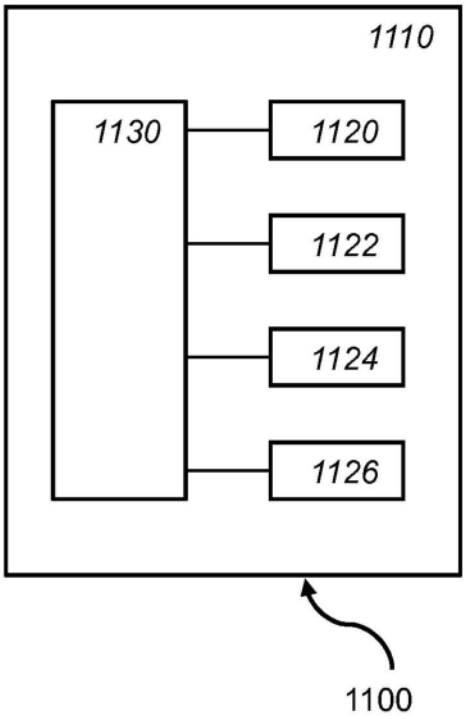


图14b