



(12)发明专利申请

(10)申请公布号 CN 111194531 A

(43)申请公布日 2020.05.22

(21)申请号 201880066589.1

(22)申请日 2018.09.04

(30)优先权数据

17190779.3 2017.09.13 EP

(85)PCT国际申请进入国家阶段日

2020.04.13

(86)PCT国际申请的申请数据

PCT/EP2018/073650 2018.09.04

(87)PCT国际申请的公布数据

W02019/052844 EN 2019.03.21

(71)申请人 西门子股份公司

地址 德国慕尼黑

(72)发明人 J. 屈纳尔 T. 加西巴

(74)专利代理机构 中国专利代理(香港)有限公司 72001

代理人 李雪娜 陈岚

(51)Int.Cl.

H04L 1/00(2006.01)

H03M 13/37(2006.01)

H04L 29/06(2006.01)

H04L 9/08(2006.01)

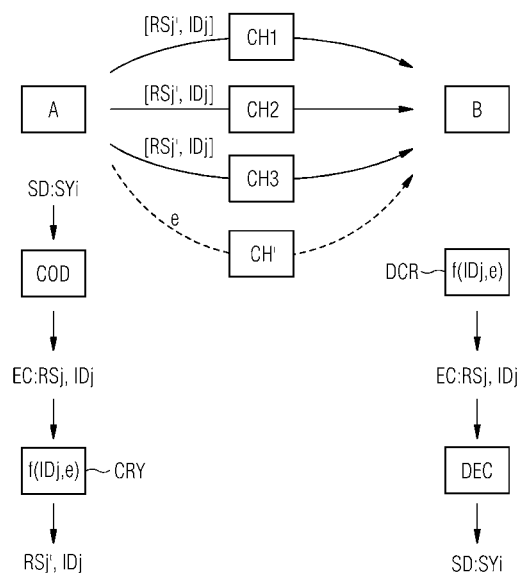
权利要求书2页 说明书6页 附图1页

(54)发明名称

用于在多个信道上发送数字数据的方法

(57)摘要

本发明涉及一种用于在多个信道(CH1, CH2, CH3)上发送数字数据的方法,其中发送器(A)执行以下步骤:-对具有第一数量的源符号(SY_i)的源数据(SD)进行编码(COD),该编码(COD)使得从源数据(SD)生成纠错码(EC),该纠错码(EC)包括比第一数量高的第二数量的修复符号(RS_j)以及标识符(ID_j),其中,每个标识符(ID_j)被分配给对应的修复符号(RS_j),该纠错码(EC)向源数据(SD)添加冗余;-通过基于发送器(A)和接收器(B)之间的共享秘密(e)的加密处理(CRY)来加密每个修复符号(RS_j),其中针对相应修复符号(RS_j)的加密处理(CRY)取决于分配给相应修复符号(RS_j)的标识符(ID_j);-将经加密的修复符号(RS_j')和所分配的标识符(ID_j)的对馈送到连接到接收器(B)的多个信道(CH1, CH2, CH3)。



1. 一种用于在多个信道(CH1,CH2,CH3)上发送数字数据的方法,其中发送器(A)执行以下步骤:

-对具有第一数量的源符号(SY_i)的源数据(SD)进行编码(COD),所述编码(COD)使得从源数据(SD)生成纠错码(EC),所述纠错码(EC)包括比第一数量高的第二数量的修复符号(RS_j)以及标识符(ID_j),其中,每个标识符(ID_j)被分配给对应的修复符号(RS_j),所述纠错码(EC)向源数据(SD)添加冗余;

-通过基于发送器(A)和接收器(B)之间的共享秘密(e)的加密处理(CRY)来加密每个修复符号(RS_j),其中针对相应修复符号(RS_j)的加密处理(CRY)取决于分配给相应修复符号(RS_j)的标识符(ID_j);

-将经加密的修复符号(RS_j')和分配的标识符(ID_j)的对馈送到连接到接收器(B)的所述多个信道(CH1、CH2、CH3)。

2. 根据权利要求1所述的方法,其中,所述纠错码(EC)是喷泉码。

3. 根据权利要求1或2所述的方法,其中所述源符号(SY_i)和所述修复符号(RS_j)均是具有相同固定位长度的位序列。

4. 根据前述权利要求中的一项所述的方法,其中,所述加密处理(CRY)使用应用到修复符号(RS_j)的伪随机函数(f(ID_j,e)),所述伪随机函数(f(ID_j,e))取决于共享秘密(e)和被分配要加密的修复符号(RS_j)的标识符(ID_j)。

5. 根据权利要求4所述的方法,其中,所述伪随机函数(f(ID_j,e))生成具有要加密的修复符号(RS_j)的位长度的中间位序列,所述经加密的修复符号(RS_j')是中间位序列与要加密的修复符号(RS_j)的异或组合。

6. 根据前述权利要求中的一项所述的方法,其中,所述多个信道(CH1、CH2、CH3)包括若干独立信道,其中,经加密的修复符号(RS_j') and 所分配的标识符(ID_j)的对被馈送到独立信道(CH1、CH2、CH3),使得每个独立信道(CH1、CH2、CH3)接收至少一对经加密的修复符号(RS_j') and 所分配的标识符(ID_j)。

7. 根据权利要求6所述的方法,其中,所述独立信道(CH1、CH2、CH3)是多路径TCP协议的信道。

8. 根据权利要求6或7所述的方法,其中每个独立信道(CH1、CH2、CH3)中的经加密的修复符号(RS_j') and 所分配的标识符(RS_j)的对的数量小于所述第一数量。

9. 根据权利要求6至8中的一项所述的方法,其中,所述加密处理(COD)还取决于经加密的修复符号(RS_j')被馈送到信道(CH1、CH2、CH3)。

10. 根据前述权利要求中的一项所述的方法,其中,与将经加密的修复符号(RS_j') and 所分配的标识符(ID_j)的对馈送到所述多个信道(CH1、CH2、CH3)并行地,所述共享秘密(e)由发送器(A)馈送到附加信道(CH'),所述附加信道(CH')连接到接收器(B)并且独立于所述多个信道(CH1、CH2、CH3)中的信道。

11. 一种用于处理由根据前述权利要求中的一项所述的方法发送的数字数据的方法,其中,接收器(B)执行以下步骤:

-在多个信道(CH1、CH2、CH3)上接收经加密的修复符号(RS_j') and 所分配的标识符(ID_j)的对;

-通过基于发送器(A)和接收器(B)之间的共享秘密(e)的解密处理(DCR)来解密每个经

加密的修复符号 (RSj'), 从而得到所述纠错码 (EC), 其中针对相应的经加密的修复符号 (RSj') 的解密处理 (CRY) 取决于分配给相应的修复符号 (RSj) 的标识符 (IDj);

- 解码 (DEC) 纠错码 (EC), 使得恢复源数据 (SD)。

12. 一种用于在多个信道 (CH1, CH2, CH3) 上从发送器 (A) 向接收器 (B) 传输数字数据的方法, 其中发送器执行根据权利要求1至10中的一项的方法, 并且接收器 (B) 执行根据权利要求11的方法。

13. 一种用于发送数字数据的发送器, 其中所述发送器 (A) 包括用于执行根据权利要求1至10中的一项所述的方法的装置。

14. 一种用于处理数字数据的接收器, 其中, 所述接收器 (B) 包括用于执行根据权利要求11所述的方法的装置。

15. 一种传输系统, 包括根据权利要求13所述的发送器 (A) 和根据权利要求14所述的接收器 (B)。

用于在多个信道上发送数字数据的方法

技术领域

[0001] 本发明涉及一种用于发送多个信道的数字数据的方法。此外,本发明涉及一种用于处理数字数据的方法,该数字数据由用于发送数字数据的方法来发送。此外,本发明涉及一种用于将数字数据从发送器传输到接收器的方法以及对应的发送器和接收器。此外,本发明涉及包括发送器和接收器的传输系统。

背景技术

[0002] 当从发送器向接收器发送数字数据时,由于传输错误可能发生数据丢失。为了即使在数据丢失的情况下也能重建原始数据,使用所谓的纠错技术,例如前向纠错,其对数字数据进行编码以获得纠错码,其中向数据添加了冗余。

[0003] 尽管纠错码使得在数据丢失的情况下能够重构原始源信息,但是这些码不提供对抗侦听数据传输的攻击者的密码保护。为了提供这种密码保护,从现有技术中已知的是,对连同纠错码的对应修复符号一起传输的经编码的符号标识符进行加密。然而,这种加密不是很强。

发明内容

[0004] 本发明的目的是提供一种用于在多个信道上发送数字数据的方法,该方法使得能够对所发送的数字数据进行纠错和强加密。此外,本发明的目的是提供一种从由本发明的方法发送的数字数据中重建源数据的方法。

[0005] 该目的通过独立权利要求来解决。本发明的优选实施例在从属权利要求中描述。

[0006] 本发明的方法提供了一种用于在多个信道上、即在至少一个信道上发送数字数据的机制。术语“信道”应被宽泛地解释,并且可以指从发送器到接收器的任何连续传输路径。即信道也可以具有基于不同传输技术的不同信道部分。在本发明的方法中,发送器执行如下所述的步骤。

[0007] 发送器对具有第一数量的源符号的源数据进行编码,其中编码使得从源数据中生成纠错码,该纠错码包括比第一数量高的第二数量的修复符号以及标识符,其中每个标识符被分配给对应的修复符号。该纠错码向源数据添加冗余。在该步骤中可以使用用于生成这样的纠错码的任何已知技术。特别地,纠错码可以是FEC码(FEC=前向纠错)。在优选实施例中,使用喷泉编码,即纠错码是喷泉码。

[0008] 在已经生成纠错码之后,发送器通过加密处理来加密该码的每个修复符号,该加密处理基于发送器与加密的修复符号将通过其来接收的接收器之间的共享秘密,其中针对相应修复符号的加密处理取决于分配给相应修复符号的标识符。术语“共享秘密”指的是仅应当被发送器和接收器知道的秘密值。

[0009] 在下一步骤中,发送器将经加密的修复符号和分配的标识符的对馈送到多个信道。即,将均包括经加密的修复符号和分配的标识符的对对应馈送到多个信道。

[0010] 本发明的方法具有以下优点:通过不仅基于共享秘密而且依赖于对应的标识符对

修复符号进行加密来提供纠错码的强加密。

[0011] 在本发明的优选实施例中,源符号和修复符号每个都是具有相同固定长度的位序列。

[0012] 在本发明的另一优选变型中,加密处理使用伪随机函数,即伪随机发生器的函数。术语“伪随机函数”以及“伪随机发生器”对于本领域技术人员来说是公知的。将伪随机函数应用于修复符号,其中伪随机函数取决于共享秘密和要加密的修复符号的标识符。该实施例提供了根据共享秘密和修复符号的标识符两者的加密处理的高效实现。

[0013] 在上述变型的优选实现方案中,伪随机函数生成具有要加密的修复符号的位长度的中间位序列,经加密的修复符号是中间位序列与要加密的修复符号的异或(XOR)组合。

[0014] 在另一特别优选的实施例中,多个信道包括若干独立信道,其中,将经加密的修复符号和分配的标识符的对馈送到独立信道,使得每个独立信道都接收至少一对经加密的修复符号和分配的标识符。术语“独立信道”意味着对一个信道的访问不准许对任何其它独立信道的访问。独立信道的使用大大增强了数据传输的安全性,因为需要来自若干信道的信息以便重建整个数据。

[0015] 在上述实施例的优选变型中,独立信道是多径TCP协议的信道。这种协议是从现有技术中已知的。然而,独立信道也可以例如通过不同的传输技术来不同地定义。

[0016] 在特别优选的实施例中,每个独立信道中的经加密的修复符号和分配的标识符的对的数量小于涉及源符号的数量的第一数量。根据该实施例,即使在攻击者成功解密修复符号的情况下,也无法通过单个信道中的修复符号来重构源符号。

[0017] 在根据本发明的方法的另一变型中,加密处理还取决于经加密的修复符号被馈送到信道,从而导致对抗攻击的增强的安全性。

[0018] 可以在基于本发明的方法发送数据之前,将上述用于加密的共享秘密通知给接收器。然而,在本发明的优选实施例中,与将经加密的修复符号和分配的标识符的对馈送到多个信道并行地,由发送器将共享秘密馈送到连接到接收器并且独立于多个信道中的信道的附加信道。因此,共享秘密的传输不需要在单独的步骤中执行,而可以是根据本发明的用于发送数据的方法的一部分。

[0019] 除了上述用于发送数字数据的方法之外,本发明还涉及一种用于处理通过本发明的方法或者通过根据本发明的方法的一个或多个优选实施例发送的数字数据的方法。为此,接收器执行以下步骤:

- 在所述多个信道上接收经加密的修复符号和分配的标识符的对;

- 通过基于发送器与接收器之间的共享秘密的解密处理来解密每个经加密的修复符号,从而产生纠错码,其中针对相应的经加密的修复符号的解密处理取决于分配给相应的修复符号的标识符;

- 解码纠错码,使得恢复源数据。

[0020] 在用于发送数字数据的方法使用基于伪随机函数的加密处理的情况下,在以上用于处理数字数据的方法中使用相同的伪随机函数以便对经加密的修复符号进行解密。特别地,在伪随机函数生成中间位序列的情况下,解密将使得对应的经解密的修复符号是中间位序列与经加密的修复符号的XOR组合。

[0021] 本发明还涉及一种用于在多个信道上从发送器向接收器传输数字数据的方法,其

中发送器执行根据本发明或其一个或多个优选实施例的用于发送数字数据的方法,并且其中接收器执行根据本发明或其一个或多个优选实施例的用于处理数字数据的方法。

[0022] 此外,本发明涉及一种用于发送数字数据的发送器,其中该发送器包括用于执行根据本发明或其一个或多个优选实施例的用于发送数字数据的方法的装置。

[0023] 此外,本发明涉及一种用于处理数字数据的接收器,其中该接收器包括用于执行根据本发明或其一个或多个优选实施例的用于处理数字数据的方法的装置。

[0024] 另外,本发明涉及包括上述发送器以及上述接收器的传输系统。

附图说明

[0025] 在下文中将参考附图1详细描述本发明的实施例。该图是图示基于本发明的变型的数字数据的传输的示意图。

具体实施方式

[0026] 图1示出了其中使用三个信道CH1、CH2和CH3在发送器A和接收器B之间传输数字数据的场景。除了这三个信道之外,另外的信道CH'用于传输共享秘密e,如将进一步解释的。

[0027] 如上所述,术语“信道”应被宽泛地解释,并且是指从发送器A到发送器B的连续传输路径,其中该路径可以具有带有不同传输技术的部分。信道CH1、CH2、CH3和CH'彼此独立。即,侦听一个信道的攻击者只接收在该信道中传输的信息,而不接收来自其它信道的信息。

[0028] 在本发明的一个变型中,信道CH1、CH2和CH3可以指不同的UDP因特网流或多径TCP协议的不同信道。与此相对,信道CH'可以指SMS信道。在另一设置中,其中在发送器A和接收器B之间仅使用两个信道,一个信道可以使用中间节点,比如保护来自发送器A或来自接收器B的通信的代理。因此,发送器A可以通过安全信道部分与远程代理通信,所述远程代理继而通过非安全信道部分与接收器B通信。对于另一个信道,情况可以相反。在该信道中,发送器A通过非安全信道部分与接收器B已知的代理进行通信,但是该代理通过安全信道与接收器B通信。如果两个代理不是太靠近,则攻击者几乎不可能控制两个非安全信道。

[0029] 图1所示的实施例导致提供了信道CH1到CH3中的数据的纠错以及高效加密的数据传输。在图1中,将从发送器A传输到发送器B的源数据由附图标记SD表示。这些数据被划分成k个源符号SY_i (i=0,1,...,k-1),其中该划分步骤由发送器A执行。每个源符号SY_i具有固定且相等数量的位b,即b·k对应于源数据SD的源位的总数。

[0030] 根据图1,发送器首先执行基于已知纠错技术的编码步骤COD,以便从源数据SD生成纠错码EC。该纠错码包括n个修复符号RS_j (j=0,1,...,n-1)以及针对每个修复符号的所谓的经编码的符号标识符ID_j。修复符号具有与源符号相同的位数b。然而,修复符号的数量可以大于源符号的数量,即,n是大于k的数目。

[0031] 在优选实施例中,编码步骤COD生成公知的喷泉码。然而,也可以生成其它类型的纠错码,只要编码技术COD导致将冗余添加到原始源数据SD的码,使得即使在传输期间丢失一些信息,也可以在传输之后恢复源数据。

[0032] 当生成喷泉码作为纠错码EC时,通常通过首先根据经编码的符号标识符ID_j计算度d来确定相应修复符号RS_j,度d是1和k之间的范围中的整数。其次,给定计算的度,从源数据中选择d个源符号。然后对这些所选择的源符号进行异或,以便产生修复符号RS_j。理想的

喷泉码可以从任何k个不同的修复符号中恢复源信息。

[0033] 在已经计算纠错码EC之后,发送器A在相应修复符号RS_j上应用加密方法CRY。该加密使用伪随机函数f(ID_j,e),其根据相应的经编码的符号标识符ID_j并且根据发送器A和接收器B之间的共享秘密e生成b个随机位。这些随机位与对应的修复符号RS_j进行异或,以便获得经加密的修复符号RS_j'。

[0034] 发送器A和发送器B可能在源数据SD的传输之前就已经接收到共享秘密e。然而,如图1的实施例所示,在信道CH1到CH3上的数据传输的同时,在信道CH'上在发送器A和发送器B之间传输共享秘密e。

[0035] 本发明的基本特征在于以下事实:加密CRY不仅基于共享秘密e,而且还取决于经编码的符号标识符ID_j。这提高了数据传输的安全性,因为对于不同的修复符号RS_j加密处理是不同的。

[0036] 图1的加密CRY导致经加密的修复符号RS_j',其中非加密的修复符号RS_j的相应标识符ID_j被分配给相应经加密的修复符号RS_j'。在下一步骤中,由发送器A在信道CH1至CH3上发送经加密的修复符号和经编码的符号标识符的相应对[RS_j',ID_j],其中每个信道传送那些对的子集。在不是所有修复符号被接收器B接收到的情况下,需要将经编码的符号标识符ID_j连同经加密的修复符号RS_j'一起发送,以便确定已经丢失了哪些修复符号。需要该信息以便在数据丢失的情况下重建源符号。

[0037] 在本文描述的实施例中,在信道CH1至CH3中的每一个上传输的加密的经修复符号和经编码的符号标识符的对的数量总是小于源符号的原始数量k。这确保了侦听一个信道的攻击者即使在他成功解密了经加密的修复符号RS_j'的情况下也不能重建来自该信道的任何源符号。

[0038] 在已经通过信道CH1至CH3接收到对[RS_j',ID_j]以及通过信道CH'接收到共享秘密e之后,接收器B执行解密方法DCR,以便对经加密的修复符号RS_j'进行解密。该解密使用与加密方法相同的函数f(ID_j,e)。为了获得经解密的修复符号RS_j,作为函数f(ID_j,e)的值的随机位序列与相应的经加密的修复符号RS_j'进行异或,即 $RS_j = RS_j' \text{ XOR } f(ID_j, e)$ 。

[0039] 作为解密步骤DCR的结果,获得了包括非加密的修复符号RS_j和对应的经编码的符号标识符ID_j的原始纠错码EC。此后,接收器执行与编码COD相反的解码DEC,以使用源符号SY_i重建原始源数据SD。即使在丢失了一些修复符号的情况下,该解码也能够恢复源数据。

[0040] 在图1的实施例的一种修改中,修复符号的加密附加地取决于在其上发送相应修复符号的信道。这可以通过伪随机函数f来实现,该伪随机函数f附加地取决于对应的信道CH_x(x=1,2,3)。即,使用伪随机函数f(ID_j,e,CH_x)。对于接收器B来说,有正确识别信道的若干选择。例如,信道可以向接收器B标识它们自己(例如,通过静态分配、广播信息、对等数据交换、散列等)。替代地,接收器B能够识别信道。例如,接收器可以知道第一信道使用UDP,而第二信道使用邮件信道等等,或者发送器可能已经发送了关于数据的一些标签以识别信道。

[0041] 当使用取决于信道的函数时,发送器A计算信道CH_x的 $RS_j' = RS_j \text{ XOR } f(ID_j, e, CH_x)$,并且通过信道CH_x发送对[RS_j',ID_j]。在接收器侧,通过计算 $RS_j = RS_j' \text{ XOR } f(ID_j, e, CH_x)$ 来还原通过信道CH_x接收的修复符号。在已经基于函数f(ID_j,e,CH_x)还原修复符号之后,可以使用参考图1描述的标准纠错解码DEC以便恢复源数据SD。

[0042] 在下文中,描述了源符号的编码和加密以及对应的解码和解密的示例。在该示例中,发送器希望向接收器发送以下三个源符号:

```
SY0 = 00001010
SY1 = 10100000
SY2 = 10101010
```

发送器首先生成七个修复符号RS1至RS6形式的喷泉码,如下:

```
RS0 = SY0           = 00001010
RS1 = SY1           = 10100000
RS2 = SY2           = 10101010

RS3 = SY0 XOR SY1   = 10101010
RS4 = SY0 XOR SY2   = 10100000
RS5 = SY1 XOR SY2   = 00001010
RS6 = SY0 XOR SY1 XOR SY2 = 00000000
```

经编码的符号标识符ID_j与每个修复符号RS_j(j=0,1,⋯,6)相关联。例如,标识符可以被选择为ID₀=0、ID₁=1、ID₂=2、ID₃=3、ID₄=4、ID₅=5、ID₆=6。发送器还例如通过由伪随机生成器计算随机数e=33来生成共享秘密e。基于共享秘密e和经编码的符号标识符ID_j,函数f(ID_j,e)针对相应的七个修复符号RS₀至RS₆生成以下中间位序列:

```
f(ID0,e) = 00010101
f(ID1,e) = 10111101
f(ID2,e) = 11011100
f(ID3,e) = 01000010
f(ID4,e) = 01010001
f(ID5,e) = 01001011
f(ID6,e) = 11010001
```

基于那些中间位序列,发送器计算经加密的修复符号RS_j如下:

```
RS0' = RS0 XOR f(ID0,e) = 00001010 XOR 00010101 = 00011111
RS1' = RS1 XOR f(ID1,e) = 10100000 XOR 10111101 = 00011101
RS2' = RS2 XOR f(ID2,e) = 10101010 XOR 11011100 = 01110110
RS3' = RS3 XOR f(ID3,e) = 10101010 XOR 01000010 = 11101001
RS4' = RS4 XOR f(ID4,e) = 10100000 XOR 01010001 = 11110001
RS5' = RS5 XOR f(ID5,e) = 00001010 XOR 01001011 = 01000001
RS6' = RS6 XOR f(ID6,e) = 00000000 XOR 11010001 = 11010001
```

在下一步骤中,通过至少一个信道,例如因特网,发送经编码的修复符号RS_j和分配的标识符ID_j的对。即,通过至少一个信道发送对[RS₀',ID₀]、[RS₁',ID₁]、[RS₂',ID₂]、[RS₃',ID₃]、[RS₄',ID₄]、[RS₅',ID₅]和[RS₆',ID₆]。与此相对,共享秘密e=33通过另一不同信道发送,例如通过SMS来发送。在接收到e和对[RS_j',ID_j] (其中一些对可能由于信道错误而被丢弃)时,接收器可以通过使用f(ID_j,e),即通过确定RS_j=RS_j' XOR f(ID_j,e),从

RSj'重新计算RSj。然后,对正确接收的修复符号执行标准纠错解码,以便恢复包括源符号SY0、SY1和SY2的原始源信息。

[0043] 在前述内容中,在用于加密和解密纠错码的处理中使用伪随机函数f。然而,也可以可能使用正常函数来代替伪随机函数。然而,在函数f的输出长度比共享秘密e的长度长的情况下,优选地使用伪随机函数而不是正常函数。

[0044] 如上所述的本发明具有若干优点。特别地,提供了一种用于数据传输的方法,该方法实现通过添加冗余的纠错以及通过根据纠错码中的相应修复符号的经编码的符号标识符对纠错码进行加密的高安全性二者。

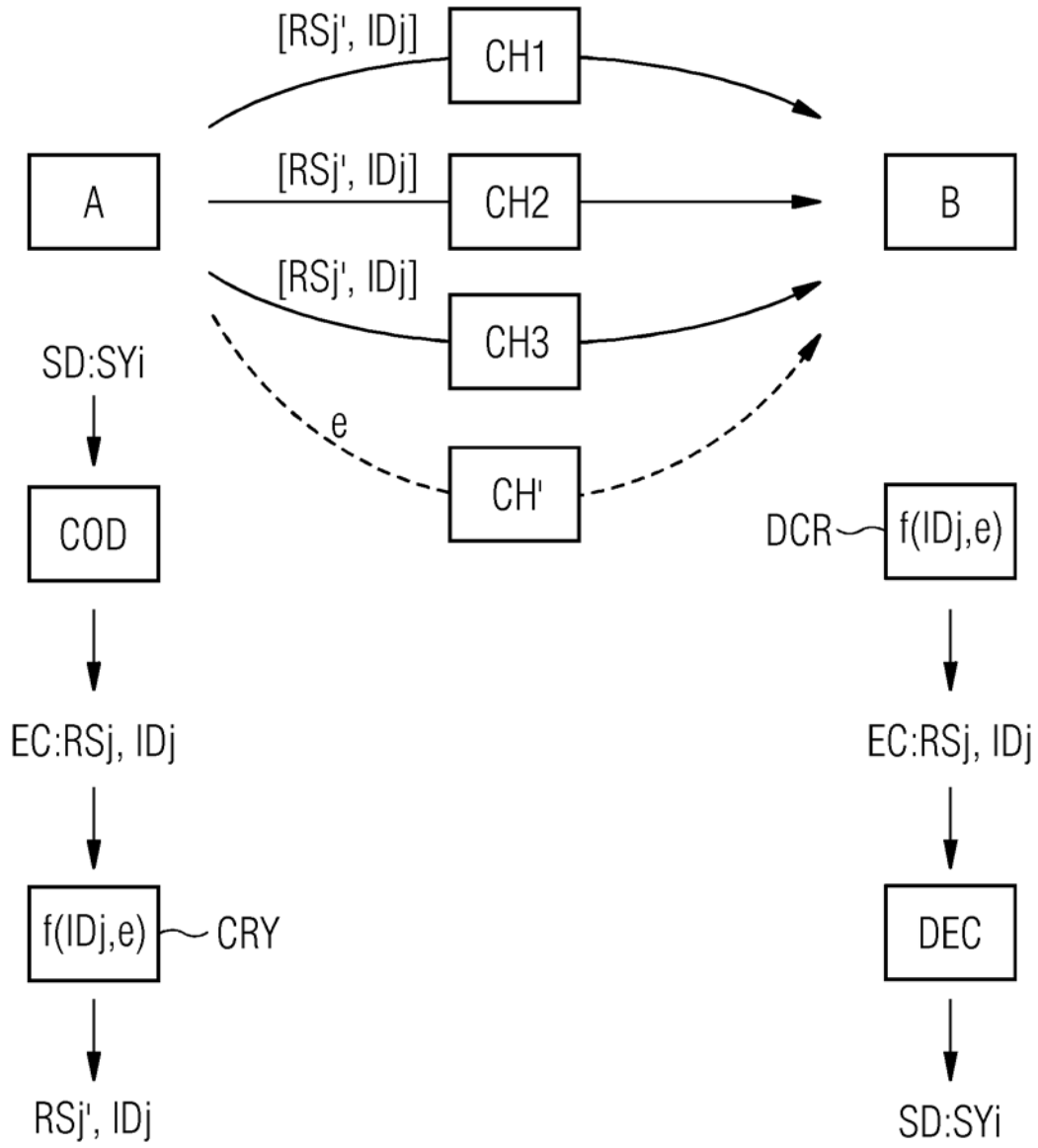


图 1