(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 103988465 B
(45)授权公告日 2017.05.10

(21)申请号 201280061049.7

(22)申请日 2012.12.05

(65)同一申请的已公布的文献号
申请公布号 CN 103988465 A

(43)申请公布日 2014.08.13

(30)优先权数据
13/316,932 2011.12.12 US

(85)PCT国际申请进入国家阶段日
2014.06.11

(86)PCT国际申请的申请数据
PCT/FI2012/051208 2012.12.05

(87)PCT国际申请的公布数据
WO2013/087983 EN 2013.06.20

(73)专利权人 诺基亚技术有限公司
地址 芬兰埃斯波

(72)发明人 J-E·埃克伯格 J-J·H·卡加

(74)专利代理机构 北京市中咨律师事务所 11247
代理人 杨晓光 于静

(51)Int.Cl.
H04L 9/08(2006.01)
H04W 12/04(2006.01)

(56)对比文件
EP 1770900 A1,2007.04.04,
CN 1925681 A,2007.03.07,

审查员 邵娟

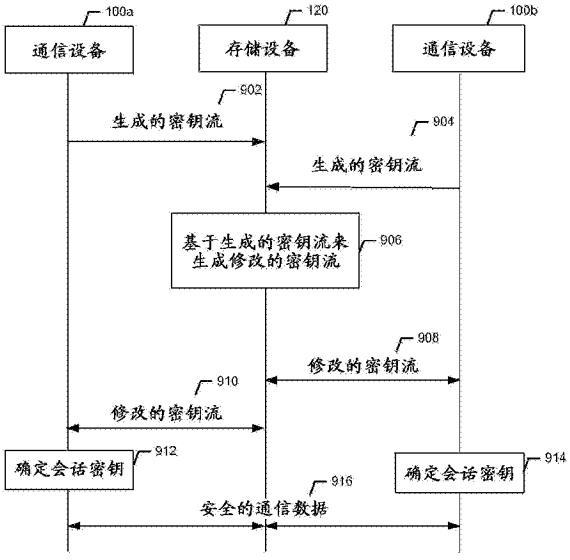
权利要求书9页 说明书13页 附图7页

(54)发明名称

用于实现密钥流层级的方法和装置

(57)摘要

提供了用于在分布式的存储环境中实现密钥流的层级的各种方法。一个示例方法可以包括使得在存储设备上访问生成的密钥流，其中在存储设备在无线电通信范围中的实例中生成密钥流。一个示例方法还可以包括基于生成的密钥流和修改的密钥流来确定会话密钥。在一些示例实施例中，由存储设备基于生成的密钥流和由存储设备从第二设备接收的密钥流来创建修改的密钥流。一个示例方法还可以包括使得通信数据被传送给存储设备或第二设备。在一些示例实施例中，使用会话密钥的至少一部分来保护通信数据，以及通信数据旨在用于第二设备。



CN 103988465 B

1.一种用于实现密钥流层级的方法,包括:

使得在存储设备上访问修改的密钥流,其中由所述存储设备基于生成的密钥流和由所述存储设备从第二设备接收的密钥流来创建所述修改的密钥流;

基于所述生成的密钥流和所述修改的密钥流来确定会话密钥,其中在所述存储设备在无线电通信范围中的实例中,所述生成的密钥流先前被传送给所述存储设备;以及

使得通信数据被传送给所述存储设备或所述第二设备,其中使用所述会话密钥的至少一部分来保护所述通信数据,以及所述通信数据旨在用于所述第二设备。

2.根据权利要求1所述的方法,还包括:

在存储设备在无线电通信范围中的实例中,使得所述生成的密钥流被传送给所述存储设备。

3.根据权利要求1或2中的任何一项所述的方法,其中可在所述存储设备上访问所述会话密钥的至少一部分,其中由所述存储设备上的索引值来确定所述会话密钥的可读的所述部分。

4.根据权利要求1或2中的任何一项所述的方法,还包括:

基于生成的密钥流和修改的密钥流来确定另一个会话密钥;其中由所述存储设备基于所述生成的密钥流和由所述存储设备从第三设备接收的密钥流来创建所述修改的密钥流;以及

使得通信数据被传送给所述存储设备,其中使用所述另一个会话密钥来保护所述通信数据的安全,以及所述通信数据旨在用于所述第三设备。

5.根据权利要求3所述的方法,还包括:

基于生成的密钥流和修改的密钥流来确定另一个会话密钥;其中由所述存储设备基于所述生成的密钥流和由所述存储设备从第三设备接收的密钥流来创建所述修改的密钥流;以及

使得通信数据被传送给所述存储设备,其中使用所述另一个会话密钥来保护所述通信数据的安全,以及所述通信数据旨在用于所述第三设备。

6.根据权利要求1、2或5中的任何一项所述的方法,还包括:

在所述存储设备再次在无线电通信范围中的实例中,使得另一个生成的密钥流被传送给所述存储设备;

基于所述生成的密钥流、所述另一个生成的密钥流和修改的密钥流来确定更新的会话密钥;以及

使得通信数据被传送给所述存储设备或所述第二设备,其中使用所述会话密钥来保护所述通信数据,以及所述通信数据旨在用于所述第二设备。

7.根据权利要求3所述的方法,还包括:

在所述存储设备再次在无线电通信范围中的实例中,使得另一个生成的密钥流被传送给所述存储设备;

基于所述生成的密钥流、所述另一个生成的密钥流和修改的密钥流来确定更新的会话密钥;以及

使得通信数据被传送给所述存储设备或所述第二设备,其中使用所述会话密钥来保护所述通信数据,以及所述通信数据旨在用于所述第二设备。

8.根据权利要求4所述的方法，还包括：

在所述存储设备再次在无线电通信范围中的实例中，使得另一个生成的密钥流被传送给所述存储设备；

基于所述生成的密钥流、所述另一个生成的密钥流和修改的密钥流来确定更新的会话密钥；以及

使得通信数据被传送给所述存储设备或所述第二设备，其中使用所述会话密钥来保护所述通信数据，以及所述通信数据旨在用于所述第二设备。

9.根据权利要求1、2、5、7或8中的任何一项所述的方法，其中基于所述生成的密钥流、所述第二设备的所述密钥流和所述第二设备的标识码的异或来创建所述修改的密钥流。

10.根据权利要求3所述的方法，其中基于所述生成的密钥流、所述第二设备的所述密钥流和所述第二设备的标识码的异或来创建所述修改的密钥流。

11.根据权利要求4所述的方法，其中基于所述生成的密钥流、所述第二设备的所述密钥流和所述第二设备的标识码的异或来创建所述修改的密钥流。

12.根据权利要求6所述的方法，其中基于所述生成的密钥流、所述第二设备的所述密钥流和所述第二设备的标识码的异或来创建所述修改的密钥流。

13.根据权利要求1、2、5、7、8、11或12中的任何一项所述的方法，还包括：

基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥。

14.根据权利要求3所述的方法，还包括：

基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥。

15.根据权利要求4所述的方法，还包括：

基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥。

16.根据权利要求6所述的方法，还包括：

基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥。

17.根据权利要求9所述的方法，还包括：

基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥。

18.根据权利要求1、2、5、7、8、11、12、14-17中的任何一项所述的方法，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

19.根据权利要求3所述的方法，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

20.根据权利要求4所述的方法，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

21.根据权利要求6所述的方法，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

22.根据权利要求9所述的方法，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

23.根据权利要求13所述的方法，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

24.一种用于实现密钥流层级的装置，包括：

至少一个处理器；以及

至少一个存储器，其包含计算机程序代码，所述至少一个存储器和所述计算机程序代码被配置为使用所述至少一个处理器使得所述装置至少：

使得在存储设备上访问修改的密钥流，其中由所述存储设备基于生成的密钥流和由所述存储设备从第二设备接收的密钥流来创建所述修改的密钥流；

基于所述生成的密钥流和所述修改的密钥流来确定会话密钥，其中在所述存储设备在无线电通信范围中的实例中，所述生成的密钥流先前被传送给所述存储设备；以及

使得通信数据被传送给所述存储设备或所述第二设备，其中使用所述会话密钥的至少一部分来保护所述通信数据，以及所述通信数据旨在用于所述第二设备。

25.根据权利要求24所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置以：

在存储设备在无线电通信范围中的实例中，使得所述生成的密钥流被传送给所述存储设备。

26.根据权利要求24或25中的任何一项所述的装置，其中可在所述存储设备上访问所述会话密钥的至少一部分，其中由所述存储设备上的索引值来确定所述会话密钥的可读的所述部分。

27.根据权利要求24或25中的任何一项所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

基于生成的密钥流和修改的密钥流来确定另一个会话密钥；其中由所述存储设备基于所述生成的密钥流和由所述存储设备从第三设备接收的密钥流来创建所述修改的密钥流；以及

使得通信数据被传送给所述存储设备，其中使用所述另一个会话密钥来保护所述通信数据的安全，以及所述通信数据旨在用于所述第三设备。

28.根据权利要求26所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

基于生成的密钥流和修改的密钥流来确定另一个会话密钥；其中由所述存储设备基于所述生成的密钥流和由所述存储设备从第三设备接收的密钥流来创建所述修改的密钥流；以及

使得通信数据被传送给所述存储设备，其中使用所述另一个会话密钥来保护所述通信数据的安全，以及所述通信数据旨在用于所述第三设备。

29.根据权利要求24、25或28中的任何一项所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

在所述存储设备再次在无线电通信范围中的实例中，使得另一个生成的密钥流被传送给所述存储设备；

基于所述生成的密钥流、所述另一个生成的密钥流和修改的密钥流来确定更新的会话密钥；以及

使得通信数据被传送给所述存储设备或所述第二设备，其中使用所述会话密钥来保护所述通信数据，以及所述通信数据旨在用于所述第二设备。

30.根据权利要求26所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

在所述存储设备再次在无线电通信范围中的实例中，使得另一个生成的密钥流被传送给所述存储设备；

基于所述生成的密钥流、所述另一个生成的密钥流和修改的密钥流来确定更新的会话密钥；以及

使得通信数据被传送给所述存储设备或所述第二设备，其中使用所述会话密钥来保护所述通信数据，以及所述通信数据旨在用于所述第二设备。

31.根据权利要求27所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

在所述存储设备再次在无线电通信范围中的实例中，使得另一个生成的密钥流被传送给所述存储设备；

基于所述生成的密钥流、所述另一个生成的密钥流和修改的密钥流来确定更新的会话密钥；以及

使得通信数据被传送给所述存储设备或所述第二设备，其中使用所述会话密钥来保护所述通信数据，以及所述通信数据旨在用于所述第二设备。

32.根据权利要求24、25、28、30或31中的任何一项所述的装置，其中基于所述生成的密钥流、所述第二设备的所述密钥流和所述第二设备的标识码的异或来创建所述修改的密钥流。

33.根据权利要求26所述的装置，其中基于所述生成的密钥流、所述第二设备的所述密钥流和所述第二设备的标识码的异或来创建所述修改的密钥流。

34.根据权利要求27所述的装置，其中基于所述生成的密钥流、所述第二设备的所述密钥流和所述第二设备的标识码的异或来创建所述修改的密钥流。

35.根据权利要求29所述的装置，其中基于所述生成的密钥流、所述第二设备的所述密钥流和所述第二设备的标识码的异或来创建所述修改的密钥流。

36.根据权利要求24、25、28、30、31、33、34或35中的任何一项所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥。

37.根据权利要求26所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥。

38.根据权利要求27所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥。

39.根据权利要求29所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥。

40.根据权利要求32所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥。

41.根据权利要求24、25、28、30、31、33、34、35、38-40中的任何一项所述的装置，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

42.根据权利要求26所述的装置，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

43.根据权利要求27所述的装置，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

44.根据权利要求29所述的装置，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

45.根据权利要求32所述的装置，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

46.根据权利要求36所述的装置，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

47.一种用于实现密钥流层级的装置，包括：

用于使得在存储设备上访问修改的密钥流的构件，其中由所述存储设备基于生成的密钥流和由所述存储设备从第二设备接收的密钥流来创建所述修改的密钥流；

用于基于所述生成的密钥流和所述修改的密钥流来确定会话密钥的构件，其中在所述存储设备在无线电通信范围中的实例中，所述生成的密钥流先前被传送给所述存储设备；以及

用于使得通信数据被传送给所述存储设备或所述第二设备的构件，其中使用所述会话密钥的至少一部分来保护所述通信数据，以及所述通信数据旨在用于所述第二设备。

48.根据权利要求47所述的装置，还包括：

用于在存储设备在无线电通信范围中的实例中使得所述生成的密钥流被传送给所述存储设备的构件。

49.根据权利要求47或48中的任何一项所述的装置，其中可在所述存储设备上访问所述会话密钥的至少一部分，其中由所述存储设备上的索引值来确定所述会话密钥的可读的所述部分。

50.根据权利要求47至48中的任何一项所述的装置，还包括：

用于基于生成的密钥流和修改的密钥流来确定另一个会话密钥的构件；其中由所述存储设备基于所述生成的密钥流和由所述存储设备从第三设备接收的密钥流来创建所述修改的密钥流；以及

用于使得通信数据被传送给所述存储设备的构件，其中使用所述另一个会话密钥来保护所述通信数据的安全，以及所述通信数据旨在用于所述第三设备。

51.根据权利要求49所述的装置，还包括：

用于基于生成的密钥流和修改的密钥流来确定另一个会话密钥的构件；其中由所述存储设备基于所述生成的密钥流和由所述存储设备从第三设备接收的密钥流来创建所述修改的密钥流；以及

用于使得通信数据被传送给所述存储设备的构件，其中使用所述另一个会话密钥来保护所述通信数据的安全，以及所述通信数据旨在用于所述第三设备。

52.根据权利要求47、48或51中的任何一项所述的装置，还包括：

用于在所述存储设备再次在无线电通信范围中的实例中使得另一个生成的密钥流被传送给所述存储设备的构件；

用于基于所述生成的密钥流、所述另一个生成的密钥流和修改的密钥流来确定更新的会话密钥的构件；以及

用于使得通信数据被传送给所述存储设备或所述第二设备的构件，其中使用所述会话密钥来保护所述通信数据，以及所述通信数据旨在用于所述第二设备。

53.根据权利要求49所述的装置，还包括：

用于在所述存储设备再次在无线电通信范围中的实例中使得另一个生成的密钥流被传送给所述存储设备的构件；

用于基于所述生成的密钥流、所述另一个生成的密钥流和修改的密钥流来确定更新的会话密钥的构件；以及

用于使得通信数据被传送给所述存储设备或所述第二设备的构件，其中使用所述会话密钥来保护所述通信数据，以及所述通信数据旨在用于所述第二设备。

54.根据权利要求50所述的装置，还包括：

用于在所述存储设备再次在无线电通信范围中的实例中使得另一个生成的密钥流被传送给所述存储设备的构件；

用于基于所述生成的密钥流、所述另一个生成的密钥流和修改的密钥流来确定更新的会话密钥的构件；以及

用于使得通信数据被传送给所述存储设备或所述第二设备的构件，其中使用所述会话密钥来保护所述通信数据，以及所述通信数据旨在用于所述第二设备。

55.根据权利要求47、48、51、53或54中的任何一项所述的装置，其中基于所述生成的密钥流、所述第二设备的所述密钥流和所述第二设备的标识码的异或来创建所述修改的密钥流。

56.根据权利要求49所述的装置，其中基于所述生成的密钥流、所述第二设备的所述密钥流和所述第二设备的标识码的异或来创建所述修改的密钥流。

57.根据权利要求50所述的装置，其中基于所述生成的密钥流、所述第二设备的所述密钥流和所述第二设备的标识码的异或来创建所述修改的密钥流。

58.根据权利要求52所述的装置，其中基于所述生成的密钥流、所述第二设备的所述密钥流和所述第二设备的标识码的异或来创建所述修改的密钥流。

59.根据权利要求47、48、51、53、54、56-58中的任何一项所述的装置，还包括：

用于基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥的构件。

60.根据权利要求49所述的装置，还包括：

用于基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥的构件。

61.根据权利要求50所述的装置，还包括：

用于基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥的构件。

62.根据权利要求52所述的装置，还包括：

用于基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥的构件。

63.根据权利要求55所述的装置，还包括：

用于基于所述生成的密钥流和所述修改的密钥流的异或来确定会话密钥的构件。

64.根据权利要求47、48、51、53、54、56-58、60-63中的任何一项所述的装置，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

65.根据权利要求49所述的装置，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

66.根据权利要求50所述的装置，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

67.根据权利要求52所述的装置，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

68.根据权利要求55所述的装置，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

69.根据权利要求59所述的装置，其中所述第二设备包括被嵌入在通信设备中的射频存储器卡。

70.一种用于实现密钥流层级的方法，包括：

在第一设备在无线电通信范围中的实例中，接收第一生成的密钥流；

在第二设备在无线电通信范围中的实例中，接收第二生成的密钥流；

基于所述第二设备的标识指示符和所述第一生成的密钥流来生成第一修改的密钥流；以及

基于所述第一设备的标识指示符和所述第二生成的密钥流来生成第二修改的密钥流。

71.根据权利要求70所述的方法，还包括：

在生成所述第一修改的密钥流或所述第二修改的密钥流中的至少一个修改的密钥流的实例中，修改索引值，其中所述索引值指示可以由至少一个设备访问的所述第一生成的密钥流或所述第二生成的密钥流中的至少一个生成的密钥流的一部分。

72.根据权利要求70或71中的任何一项所述的方法，还包括：

接收来自所述第一设备的加密的数据，其中所述加密的数据是使用由所述第一设备基于所述第一生成的密钥流和所述第一修改的密钥流生成的会话密钥来进行加密的。

73.根据权利要求70或71中的任何一项所述的方法，还包括：

在第三设备在无线电通信范围中的实例中，接收第三生成的密钥流；

基于所述第二设备的标识指示符和所述第二生成的密钥流来生成第三修改的密钥流；以及

基于所述第一设备的标识指示符和所述第一生成的密钥流来生成第四修改的密钥流。

74.根据权利要求72所述的方法，还包括：

在第三设备在无线电通信范围中的实例中，接收第三生成的密钥流；

基于所述第二设备的标识指示符和所述第二生成的密钥流来生成第三修改的密钥流；以及

基于所述第一设备的标识指示符和所述第一生成的密钥流来生成第四修改的密钥流。

75.一种用于实现密钥流层级的装置，包括：

至少一个处理器；以及

至少一个存储器，其包含计算机程序代码，所述至少一个存储器和所述计算机程序代码被配置为使用所述至少一个处理器使得所述装置至少：

在第一设备在无线电通信范围中的实例中，接收第一生成的密钥流；

在第二设备在无线电通信范围中的实例中，接收第二生成的密钥流；

基于所述第二设备的标识指示符和所述第一生成的密钥流来生成第一修改的密钥流；以及

基于所述第一设备的标识指示符和所述第二生成的密钥流来生成第二修改的密钥流。

76.根据权利要求75所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

在生成所述第一修改的密钥流或所述第二修改的密钥流中的至少一个修改的密钥流的实例中，修改索引值，其中所述索引值指示可以由至少一个设备访问的所述第一生成的密钥流或所述第二生成的密钥流中的至少一个生成的密钥流的一部分。

77.根据权利要求75或76中的任何一项所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

接收来自所述第一设备的加密的数据，其中所述加密的数据是使用由所述第一设备基于所述第一生成的密钥流和所述第一修改的密钥流生成的会话密钥来进行加密的。

78.根据权利要求75或76中的任何一项所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

在第三设备在无线电通信范围中的实例中，接收第三生成的密钥流；

基于所述第二设备的标识指示符和所述第二生成的密钥流来生成第三修改的密钥流；以及

基于所述第一设备的标识指示符和所述第一生成的密钥流来生成第四修改的密钥流。

79.根据权利要求77所述的装置，其中包含所述计算机程序代码的所述至少一个存储器还被配置为使用所述至少一个处理器使得所述装置：

在第三设备在无线电通信范围中的实例中，接收第三生成的密钥流；

基于所述第二设备的标识指示符和所述第二生成的密钥流来生成第三修改的密钥流；以及

基于所述第一设备的标识指示符和所述第一生成的密钥流来生成第四修改的密钥流。

80.一种用于实现密钥流层级的装置，包括：

用于在第一设备在无线电通信范围中的实例中接收第一生成的密钥流的构件；

用于在第二设备在无线电通信范围中的实例中接收第二生成的密钥流的构件；

用于基于所述第二设备的标识指示符和所述第一生成的密钥流来生成第一修改的密钥流的构件；以及

用于基于所述第一设备的标识指示符和所述第二生成的密钥流来生成第二修改的密钥流的构件。

81.根据权利要求80所述的装置，还包括：

用于在生成所述第一修改的密钥流或所述第二修改的密钥流中的至少一个修改的密钥流的实例中修改索引值的构件，其中所述索引值指示可以由至少一个设备访问的所述第一生成的密钥流或所述第二生成的密钥流中的至少一个生成的密钥流的一部分。

82.根据权利要求80或81中的任何一项所述的装置，还包括：

用于接收来自所述第一设备的加密的数据的构件，其中所述加密的数据是使用由所述

第一设备基于所述第一生成的密钥流和所述第一修改的密钥流生成的会话密钥来进行加密的。

83.根据权利要求80或81中的任何一项所述的装置，还包括：

用于在第三设备在无线电通信范围中的实例中接收第三生成的密钥流的构件；

用于基于所述第二设备的标识指示符和所述第二生成的密钥流来生成第三修改的密钥流的构件；以及

用于基于所述第一设备的标识指示符和所述第一生成的密钥流来生成第四修改的密钥流的构件。

84.根据权利要求82所述的装置，还包括：

用于在第三设备在无线电通信范围中的实例中接收第三生成的密钥流的构件；

用于基于所述第二设备的标识指示符和所述第二生成的密钥流来生成第三修改的密钥流的构件；以及

用于基于所述第一设备的标识指示符和所述第一生成的密钥流来生成第四修改的密钥流的构件。

用于实现密钥流层级的方法和装置

技术领域

[0001] 各种实施例一般涉及密钥协商和安全性，并且更具体地，涉及用于实现密钥流层级(hierarchy)的方法和装置。

背景技术

[0002] 相对于高速通信技术和强大但紧凑的处理能力，移动计算设备不断地变得更强大和动态。由于对能够执行复杂的计算机化任务的紧凑的手持型设备以及提升通信速度的需求，计算技术的演进正朝着利用以分布式数据存储和计算能力的形式的分布式资源，以及能够有效地利用本地的分布式内容和连通性。由于对这些分布式资源的访问常常与其它设备(例如，在本地域中)共享，因此关注的是由这些资源和各种用户设备处理的数据的可靠性和安全性。

发明内容

[0003] 此处描述了使得能够例如在分布式的存储环境中的密钥流层级的示例方法、示例装置和示例计算机程序产品。一些示例实施例可以被配置为使得能够分发用于一对一的通信和/或组通信的生成的密钥流。所述生成的密钥流可以被创建和/或存储在存储设备上(例如，射频(RF)存储器标签、通用串行总线(USB)存储器、有源或无源的嵌入式RF存储器标签和/或独立的RF存储器标签)。例如，在通信设备已经与存储设备接触的实例中，所述示例方法、示例装置和示例计算机程序产品被配置为生成用于所述通讯设备的密钥流。由所述通讯设备创建的示例密钥流连同用于其它通信设备的其它密钥流可以被存储在所述存储设备上。在一些示例实施例中，然后，可以基于存储在所述存储设备上的两个或更多的密钥流来创建会话密钥。示例会话密钥可以用于对通信进行加密和/或使得通信能够被存储在通信设备之间的存储设备上。

[0004] 在一个实施例中，提供了一种方法，所述方法包括使得在存储设备上访问生成的密钥流。在一些示例实施例中，在所述存储设备在无线电通信范围中的实例中，生成所述密钥流。这个实施例的方法还可以包含基于生成的密钥流和修改的密钥流来确定会话密钥。在一些示例实施例中，由所述存储设备基于所述生成的密钥流和由所述存储设备从第二设备接收的密钥流来创建所述修改的密钥流。这个实施例的方法还可以包含使得通信数据被传送给所述存储设备或所述第二设备。在一些示例实施例中，使用所述会话密钥的至少一部分来保护所述通信数据，并且所述通信数据旨在用于所述第二设备。

[0005] 在另一个实施例中，提供了一种装置，所述装置包含至少一个处理器和包含计算机程序代码的至少一个存储器，所述至少一个存储器和所述计算机程序代码被配置为使用所述至少一个处理器使得所述装置以至少使得在存储设备上访问生成的密钥流。在一些示例实施例中，在所述存储设备在无线电通信范围中的实例中，生成所述密钥流。所述至少一个存储器和计算机程序代码还可以被配置为使用所述至少一个处理器使得所述装置基于生成的密钥流和修改的密钥流来确定会话密钥。在一些示例实施例中，由所述存储设备基

于所述生成的密钥流和由所述存储设备从第二设备接收的密钥流来创建所述修改的密钥流。所述至少一个存储器和计算机程序代码还可以被配置为使用所述至少一个处理器使得所述装置使得通信数据被传送给所述存储设备或所述第二设备。在一些示例实施例中，使用所述会话密钥的至少一部分来保护所述通信数据，并且所述通信数据旨在用于所述第二设备。

[0006] 在又一个实施例中，可以提供计算机程序产品，所述计算机程序产品包含：至少一个非短暂性的计算机可读存储介质，其具有存储在其中的计算机可读程序指令，所述计算机可读程序指令包含被配置为使得在存储设备上访问生成的密钥流的程序指令。在一些示例实施例中，在所述存储设备在无线电通信范围中的实例中，生成所述密钥流。所述计算机可读程序指令还可以包含被配置为基于生成的密钥流和修改的密钥流来确定会话密钥的程序指令。在一些示例实施例中，由所述存储设备基于所述生成的密钥流和由所述存储设备从第二设备接收的密钥流来创建所述修改的密钥流。所述计算机可读程序指令还可以包含被配置为使得通信数据被传送给所述存储设备或所述第二设备的程序指令。在一些示例实施例中，使用所述会话密钥的至少一部分来保护所述通信数据，所述通信数据旨在用于所述第二设备。

[0007] 在又一个实施例中，提供了一种装置，所述装置包含用于使得在存储设备上访问生成的密钥流的构件。在一些示例实施例中，在所述存储设备在无线电通信范围中的实例中，生成所述密钥流。这个实施例的所述装置还可以包含：用于基于生成的密钥流和修改的密钥流来确定会话密钥的构件。在一些示例实施例中，由所述存储设备基于所述生成的密钥流和由所述存储设备从第二设备接收的密钥流来创建所述修改的密钥流。这个实施例的所述装置还可以包含用于使得通信数据被传送给所述存储设备或所述第二设备的构件。在一些示例实施例中，使用所述会话密钥的至少一部分来保护所述通信数据，所述通信数据旨在用于所述第二设备。

[0008] 在一个实施例中，提供了一种方法，所述方法包括：在第一设备在无线电通信范围中的实例中，接收第一生成的密钥流。这个实施例的所述方法还可以包含在第二设备在无线电通信范围中的实例中，接收第二生成的密钥流。这个实施例的所述方法还可以包含基于所述第二设备的标识指示符和所述第二生成的密钥流来生成第一修改的密钥流。这个实施例的所述方法还可以包含基于所述第一设备的标识指示符和所述第一生成的密钥流来生成第二修改的密钥流。

[0009] 在另一个实施例中，提供了一种装置，所述装置包含至少一个处理器和包含计算机程序代码的至少一个存储器，所述至少一个存储器和所述计算机程序代码被配置为使用所述至少一个处理器使得所述装置在第一设备在无线电通信范围中的实例中，至少接收第一生成的密钥流。所述至少一个存储器和所述计算机程序代码还被配置为使用所述至少一个处理器使得所述装置在第二设备在无线电通信范围中的实例中，接收第二生成的密钥流。所述至少一个存储器和所述计算机程序代码还被配置为使用所述至少一个处理器使得所述装置基于所述第二设备的标识指示符和所述第二生成的密钥流来生成第一修改的密钥流。所述至少一个存储器和所述计算机程序代码还被配置为使用所述至少一个处理器使得所述装置基于所述第一设备的标识指示符和所述第一生成的密钥流来生成第二修改的密钥流。

[0010] 在又一个实施例中，可以提供计算机程序产品，所述计算机程序产品包含：至少一个非短暂性的计算机可读存储介质，其具有存储在其中的计算机可读程序指令，所述计算机可读程序指令包含被配置为在第一设备在无线电通信范围中的实例中接收第一生成的密钥流的程序指令。所述计算机可读程序指令还可以包含被配置为在第二设备在无线电通信范围中的实例中接收第二生成的密钥流的程序指令。所述计算机可读程序指令还可以包含被配置为基于所述第二设备的标识指示符和所述第二生成的密钥流来生成第一修改的密钥流的程序指令。所述计算机可读程序指令还可以包含被配置为基于所述第一设备的标识指示符和所述第一生成的密钥流来生成第二修改的密钥流的程序指令。

[0011] 在又一个实施例中，提供了一种装置，所述装置包含用于在第一设备在无线电通信范围中的实例中接收第一生成的密钥流的构件。这个实施例的所述装置还可以包含用于在第二设备在无线电通信范围中的实例中接收第二生成的密钥流的构件。这个实施例的所述装置还可以包含用于基于所述第二设备的标识指示符和所述第二生成的密钥流来生成第一修改的密钥流的构件。这个实施例的所述装置还可以包含用于基于所述第一设备的标识指示符和所述第一生成的密钥流来生成第二修改的密钥流的构件。

附图说明

[0012] 已经如此总体地描述了一些示例实施例，现在将参照附图，附图未必按等比例绘制，以及其中：

[0013] 图1说明了根据一些示例实施例的示例的分布式存储环境；

[0014] 图2说明了依照一些示例实施例的存储在存储设备上的示例密钥流；

[0015] 图3说明了依照一些示例实施例的存储在存储设备上的示例修改的密钥流；

[0016] 图4说明了根据示例实施例的示例会话密钥生成方法；

[0017] 图5说明了根据示例实施例的被配置为在分布式存储环境中实现密钥流层级的装置的框图；

[0018] 图6说明了根据示例实施例的被配置为在分布式存储环境中实现密钥流层级的移动设备的框图；

[0019] 图7说明了根据一些示例实施例的用于在通信设备中实现密钥流层级的示例方法的流程图；

[0020] 图8说明了根据一些示例实施例的用于在存储设备中实现密钥流层级的示例方法的流程图；以及

[0021] 图9说明了根据一些示例实施例的信令流程图。

具体实施方式

[0022] 现在在下文中将参照附图来更全面地描述示例实施例，其中示出了一些实施例而不是全部的实施例。实际上，实施例可以采取许多不同的形式，以及不应当被认为是限制于本文所阐述的实施例；相反，提供了这些实施例以便本公开将符合可适用的法律要求。全文中，类似的标记指类似的元素。根据一些示例实施例，术语“数据”、“内容”、“信息”和类似的术语可以交替地使用以指能够被传送、接收、在其上进行操作和/或存储的数据。此外，如本文所使用的术语“或”不是用于排他的方式(即，作为异-或)，而是被定义为包括集合中的至

少一个选项以及可能地集合内的一个或多个其它选项的运算符。

[0023] 如本文说使用的，术语“电路”指以下中的所有：(a)仅硬件的电路实现方式(诸如仅模拟和/或数字电路中的实现方式)；(b)针对电路和软件(和/或固件)的组合，诸如(如果适用)：(i)针对处理器(多个)的组合或(ii)针对处理器(多个)/软件(包含数字信号处理器(多个)、软件和存储器(多个)，其一起工作以使得装置(诸如移动电话或服务器)执行各种功能)的部分；和(c)针对电路，诸如微处理器(多个)或微处理器(多个)的一部分，其需要软件或固件以用于操作，即使软件或固件不是物理呈现的。

[0024] “电路”的这种定义应用于本申请中(包含在任何权利要求中)的这个术语的所有使用。作为又一个示例，如在本申请中使用的，术语“电路”还将覆盖仅处理器(或多个处理器)或处理器的一部分以及其(或它们的)附带的软件和/或固件的实现方式。术语“电路”还将覆盖(例如如果可以适用于特定要求保护的元素)用于移动电话的基带集成电路或专用集成电路或服务器、蜂窝网络设备或其它网络设备中的类似的集成电路。

[0025] 图1说明了示例分布式存储环境105，其包括通信设备100a、100b和100n以及至少一个存储设备120。通信设备100a-n可以被具体化为任何类型的用户设备(UE)(例如，蜂窝电话、移动终端、智能电话、阅读器、写字板或平板设备、计算机或诸如此类)，或UE的组件，其被配置为包括计算和通信(例如，近距离无线，包含近场通信(NFC)和任何其它未来的高速近距离连接)能力。可替代地或另外地，在一些实施例中，无线供电(例如，如NFC，UHF)和无线通信(例如，脉冲UWB)可以共存。

[0026] 环境105可以包括一个或多个独立的存储设备，其被嵌入在通信设备100a-n以及没有被嵌入或集成在通信设备中的存储设备中，诸如RF存储器标签。在存储设备是独立设备的实例中，示例存储设备120可以包括集成电路(IC)和存储器。存储器可以被配置为操作在有源或无源模式中。每个存储设备120还可以实现机载或远程引擎，其管理和实现存储资源可能要求的功能，包含例如逻辑更新、存储器配置、数据记录管理和/或诸如此类。该引擎可以被实现成硬件和/或硬件和软件的组合。在一些示例实施例中，该引擎可以分别由IC来实现，并且可配置和维护存储器的配置，可以被远程地实现，以及可以被配置为在各种时间与存储设备120进行接口以执行逻辑更新、标签和存储器配置、数据记录管理，以及诸如此类。存储设备120可以被具体化成包括用于执行功能的内部电源的有源存储器标签，或依赖于接收的功率信号以向标签供电并执行功能的无源存储器标签。根据各种示例实施例，存储设备120可以支持无线通信，包含NFC，这里例如有一个无线电频率用于无线功率传送(例如，在NFC、超高频(UHF)或诸如此类)以及其它频率用于无线数据传送(例如，脉冲超宽带(UWB))。

[0027] 如上所述，存储设备120和利用存储设备120的系统可以支持示例智能空间和/或类似的环境。这些环境可以提供设备(例如，阅读器/写入器设备和诸如RF存储器标签的存储设备)之间的10-100 Mbit/s的高数据速率通信。标签的存储器可以包括在非常高数据速率的通信信道(例如，在7.9GHz的脉冲无线电超宽带(UWB))上进行操作的大能力(例如，一或更多千兆比特)。系统或环境可以基于NFC和/或UHF，以及系统或环境可以使得能够智能空间，这里许多设备可以使用共享视图的资源和服务。智能空间可以例如通过允许用户向网络灵活地引入新的设备以及从任何设备来访问多个设备系统中的一些或所有信息来提供更好的用户体验。照此，这些技术可以将高无线接入速度结合到具有高存储密度的存储

器组件，例如可以是嵌入式或独立的RF存储器标签。这些设备能够通过两个设备“接触”或位于彼此近距离中以用于高带宽通信来几乎同时地接收或发送大量的数据。

[0028] 通过嵌入式和独立的存储设备120的操作，环境105可以允许共享的存储资源的实现方式。在这点上，例如，通信设备100a-n可以在存储设备120上存储数据(例如，文件、媒体对象、图像、通信、数据产品和/或诸如此类)。为了实现这种类型的资源共享，可以实现密钥流的层级、密钥生成和密钥分发。

[0029] 因此，提供了一些示例实施例、方法和装置以用于实现包含存储设备120的密钥流层级(例如在分布式存储环境中)。这样做，在通信设备100a-n接触存储设备120或在存储设备120的近距离中的实例中，各种示例实施例使得生成的密钥流(诸如密钥流140a、140b和140n)能够被存储在存储设备120上。如本文所描述的，存储设备120可以是任何类型的存储设备，但是存储被实现成非易失性存储器，以及可以被配置为操作在有源或无源模式中。存储设备还可以采取被嵌入在移动通信设备中的RF存储器标签的形式(还被称为电子标签)或采取单独的RF存储器标签的形式。

[0030] 在一些示例实施例中，可以针对进入到存储设备120的通信范围中的每个通信设备100a-n生成密钥流140a-n。密钥流140a-n可以包含随机或伪随机的字符流。从而导致存储设备120具有用于已经在存储设备120的通信范围中或与其接触的每个通信设备100a-n的至少一个密钥流，但是在一些示例实施例中超过一个密钥流140a-n。如本文中所描述的，环境105可以包含在多个位置中的多个存储设备120。

[0031] 在各种示例实施例中，存储设备120还可以被配置为通过整合()从一个或多个通信设备100a-n接收的两个或更多的生成的密钥流来修改生成的密钥流。例如，可以通过整合(例如，异或(XOR))用于第一通信设备100a的至少一个会话密钥、第二通信设备100b的标识码和用于第二通信设备100b的至少一个会话密钥来创建修改的密钥流。

[0032] 在一些示例实施例中，还可以使用由第一通信设备100a和/或第二通信设备100b生成的密钥流的一部分来对修改的密钥流进行加密。可以通过当前被存储在存储设备120上的多达索引i的密钥流中的每个密钥流来对修改的密钥流进行修改，这里i是当前存储在存储设备120上的密钥流的数量。所生成的修改的密钥流可以包含第一通信设备100a和第二通信设备100b之间的共享的秘密(例如，密钥)。存储设备120可以包含i^2个密钥，这里单个密钥出现两次(例如，在用于一对通信设备的每个密钥流中出现一次)。然后，在通信设备100a-n接触(例如，在通信范围中)存储设备120的实例中，可以使得通信设备100a-n中的任何通信设备可以获得修改的密钥流。在一些示例实施例中，其它通信设备可以获得修改的密钥流。在攻击者也具有原始的生成的密钥流的实例中，对于攻击者而言修改的密钥流是有用的。

[0033] 使用修改的密钥流，通信设备100a-n还被配置为使用生成的密钥流和修改的密钥流的异或来生成会话密钥。在一些示例实施例中，例如，通信设备100a-n可以访问存储设备120，以及还可以使得使用会话密钥或使用会话密钥的一部分对通信(例如，消息、文件和/或诸如此类)进行加密或完整性保护，以及被存储在用于另一个通信设备100a-n的存储设备120上。

[0034] 可替代地或另外地，存储设备120还被附着和/或嵌入在通信设备中，诸如通信设备100a-n。在这种情况下，存储设备120可以由通信设备来操作，以及可以用于设备至设备

的通信。在这种情况下，嵌入的存储器标签可以由通信设备进行供电或可以自己进行供电。

[0035] 图2和图3说明了在一个或多个通信设备(诸如参照图1示出的通信设备100a-n)接触存储设备120的实例中存储设备120的示例初始化和设置。在一些示例实施例中以及参照图2，可以针对进入存储设备120的通信范围中的每个通信设备100a-n生成密钥流。诸如密钥流140a的密钥流可以在通信设备100a和存储设备120首次接触时由通信设备生成，并且可以包含存储在存储设备120上的伪随机字符串。在一些示例实施例中，每当通信设备接触存储设备时，可以创建用于该通信设备的密钥流。例如，接触的通信设备可以使得密钥流(密钥流1，具有创建的密钥标识(keyID))被创建，以及可以在首次接触时(在t＝0)将它传递给接收的目标设备。

[0036] 在各种示例实施例中，密钥流可以由标识码160(例如媒体访问控制(MAC)地址、标识码和/或其它识别因素)和随机字符串(例如，随机序列)组成。通信设备100a和通信设备100b两者都可以使得具有如由标识框160示出的对应标识的密钥流被存储在存储设备120上。作为示例，通信设备100a可以具有76的标识码，以及通信设备100b可以具有31的标识码。

[0037] 在通信设备100a在随后的时间接触存储设备120的实例中，可以更新先前存储的密钥流，和/或可以添加新的密钥流。例如，在通信设备100a的第二次接触(在t＝T)的实例中，可以创建第二密钥流(具有不同的密钥标识的密钥流2)，其提供不同于在第一次接触中所创建的密钥流的密钥流。例如，在通信设备100a在接触数据流的中间被中断(例如，电话呼叫)的实例中，可以更新密钥流。在用于密钥流的定时器已经期满的实例中，还可以更新密钥流。定时器可以用于限制密钥流可以使用的持续时间。例如，在预定的时间后，先前生成的密钥流可以被删除和/或标记为不可用，以及可能需要生成新的密钥流。

[0038] 在一些示例实施例中，通信设备(诸如通信设备100a)可以被配置为自动地使得生成的密钥流被存储在任何存储设备120上。也就是说，在没有用户的交互的情况下，通信设备可以使得密钥流被生成并传递给存储设备120。可替代地或另外地，在一些示例实施例中，用户可以诸如通过与通信设备100a和/或存储设备120进行交互使得生成密钥流。密钥流的生成通常发生在通信设备上，尽管在一些示例实施例中密钥流的生成可以发生在存储设备上。

[0039] 在通信设备100b接触存储设备120的实例中，可以使得密钥流140b被传递给存储设备120。一旦存储设备120在存储设备中具有至少两个密钥流，则使用示例IC，存储设备120可以通过执行更新使两个或更多的密钥流被整合。在添加新的密钥流(例如，有源存储设备)时或当存储设备下一次被激活时(例如，无源存储设备)时可以发生更新。

[0040] 现在参照图3，在一些示例实施例中，可以在属于两个或多个通信设备的两个密钥流、多个密钥流之间和/或在存储在存储设备120中的所有密钥流之间执行更新。更新可以修改密钥流的隙(slot)，诸如在密钥流150a上的第一标识隙180a，或者在可替代的示例实施例中，它可以更新随后未使用的标识隙。例如，为了识别生成的密钥流为连接到另一个通信设备，诸如通信设备100b，可以使用异或将第一标识隙180a和密钥流150b的设备标识码170b进行整合。例如，1A->1A异或31->2B。此外，还可以更新密钥流150b的标识隙190b(例如82->82异或76->F4)。生成的修改的密钥流包括包含通信设备对的身份的新的值。

[0041] 在一些示例实施例中，还更新密钥部位(诸如例如密钥部位200a和200b)或会话密

钥的位置。还可以通过执行密钥部位200a和密钥部位200b，成对的密钥流的材料块(material block)220a和材料块220b的异或，来更新用于密钥流150a的密钥部位200a和用于密钥流150b的密钥部位200b。例如，可以通过14->14异或A5异或20->91来更新密钥流150a的密钥部位200a，以及可以通过FF->FF异或A5异或20->7A来更新密钥流150b的密钥部位200b。因为使用密钥材料块220a和材料块220块，所以密钥材料块220可以被置零，以便例如隐藏密钥材料块，使得攻击者不能反向工程原始的密钥流140a和140b。

[0042] 在一个示例实施例中，密钥流的更新可以包含但不限制于以下实现方式：

[0043] 当插入新的Id{x+1}和密钥流KS{x+1}时：

[0044] for i＝1至x

[0045] KTS{i}[x+1][id]＝KTS{i}[x+1][id]异或Id{x+1}

[0046] KTS{x+1}[i][id]＝KTS{x+1}[i][id]异或Id{i}

[0047] KTS{i}[x+1][密钥]＝KTS{i}[x+1][密钥]异或KTS{i}[x+1][km]异或KTS{x+1}[i][km]

[0048] KTS{x+1}[i][密钥]＝KTS{x+1}[i][密钥]异或KTS{i}[x+1][km]异或KTS{x+1}[i][km]

[0049] KTS{i}[x+1][km]＝0

[0050] KTS{x+1}[i][km]＝0

[0051] 下一个i

[0052] 这里一个密钥流隙(KTS)的大小是len(Id)+2*len(密钥)

[0053] 在一些示例实施例中，可选地，现在可以由通信设备100a使用修改的密钥流150a和修改的密钥流150b来对用于通信设备100b的通信进行加密/解密，并且反之亦然。在一些实施例中，在通信设备100a和/或通信设备100b接触存储设备120的实例中，可以更新修改的密钥流150a。可替代地或另外地，修改的密钥流150a和修改的密钥流150b还可以用于其它的安全功能，例如完整性保护，或这两者。例如，修改的密钥流的第一部分可以用于加密/解密，以及修改的密钥流的第二部分可以用于完整性保护。

[0054] 在执行更新后，存储设备120可以被配置为使得修改的密钥流的一部分可以使用，诸如例如在密钥流140a和密钥流140b已经被组合成如图3中示出的后，存储设备120可以被配置为基于索引值来显示修改的密钥流150a和修改的密钥流150b。索引值对存储卡设备是共同的，并且定义密钥流的可读部分和不可读部分之间的边界。由于在缺省实施例中定义的成对的密钥生成算法的方式，因此索引可以对所有的密钥流是共同的，但是对于使用一些其它组合算法的特定密钥流来说还可以是个体的，诸如索引值240a和240b。

[0055] 在一些示例实施例中，可以使得密钥流的修改部分可以获得，因为在没有原始生成的密钥流的情况下，修改的密钥流可能是无意义的。在一些示例实施例中，在已经修改了特定密钥流的实例中，可以由存储设备120来调节索引值。

[0056] 可替代地或另外地，在一些示例实施例中，通信设备100a和通信设备100b可以被配置为直接进行通信。例如，在一些实施例中，基于生成会话密钥，可以在不使用存储设备的情况下将数据加密并直接传送给另一个通信设备。可替代地或另外地，在通信设备100a和通信设备100b之间没有在存储设备上成对的实例中，则可以基于由通信设备100a和通信设备100b两者与另一个存储设备的历史接触来创建成对。可以基于第一通信设备100a和第

二通信设备100b之间的相似性来创建紧急对。可替代地或另外地，可以创建用于一个或多个未接触的设备的会话密钥，该会话密钥可以在此类设备接触存储设备的实例中被传递。

[0057] 可替代地或另外地，在第一通信设备100a试图向第二通信设备100b传递数据的实例中，通信设备100a和通信设备100b可以试图确定它们是否共享共同的密钥流，诸如存储设备120上的修改的密钥流。在它们确实共享密钥流的实例中，则该密钥流可以用作用于安全功能(例如数据的加密)的会话密钥，以及即使在没有存储设备120的情况下可以使用该密钥流。然而，在通信设备100a和通信设备100b之间没有共同的密钥流的实例中，则通信设备100a可以试图确定在这两个通信设备之间有多少个(如果有)用于其它通信设备的共同的密钥流标识是共同的。在通信设备100a和通信设备100b之间的共同密钥流的数量超过预定阈值的实例中，则通信设备100a可以认为通信设备100b是可以信任的，从而使得能够创建通信设备100a和通信设备100b两者都可以理解的修改的密钥流。

[0058] 可替代地或另外地，存储设备120可以与服务器或其它远程设备通信。在这些示例实施例中的存储设备可以被配置为与服务器直接通信，或可以使用中间的设备(诸如通信设备100a-n)以与服务器通信。在存储设备与服务器通信的实施例中，存储设备120可以下载用于特定通信设备的密钥流，它可以验证通信设备和/或诸如此类的身份。在一些示例实施例中，存储设备可以诸如从社交网站来获得用于通信设备的用户的标识信息。

[0059] 图4说明了由本发明的一些示例实施例的示例通信设备和存储设备执行的操作。当在操作中时，如参照图2和图3描述的，可以创建密钥流并将其传送以存储在由通信设备接触的多个存储设备上。在密钥流302中示出了被创建的用于通信设备100a的示例密钥流的一部分，以及示例密钥流308中示出了被创建的用于通信设备100b的示例密钥流的一部分。如参照图2和图3描述的，然后，可以基于密钥流302、通信设备100b的标识码(例如31)和密钥流308的异或来创建修改的密钥流304。类似地，可以基于密钥流308、通信设备100a的标识码(例如76)和密钥流302的异或来创建密钥流310。密钥流304和密钥流310类似于相对于图3生成和示出的密钥流。

[0060] 在一些示例实施例中以及在通信设备100a试图使得加密的通信被存储在用于通信设备100b的存储设备120上的实例中，通信设备100a可以将密钥流302与修改的密钥流304进行异或以发现用于如由标识码(例如标识码76)标识的通信设备100b的会话密钥314(在密钥流306中示出)。可以使用会话密钥(例如会话密钥85)对指向通信设备100b的通信进行加密。如图3中示出的，通信设备100b可以通过计算密钥流308和密钥流310的异或来获得同一会话密钥316(在密钥流312中示出)以对通信进行解密。

[0061] 以上已经描述了一些示例实施例，图5和图6描绘了示装置，该装置可以被配置为执行如本文所述的各种功能，包含相对于图1至图4以及相关联的文本所描述的那些功能。另外，图7和图8说明了可以由并入本文所述的各种特征和功能的图5和图6的装置来执行的示例方法或算法。

[0062] 现在参照图5，示例实施例被描绘为装置500，其可以被具体化为电子设备，诸如独立的或嵌入式的RF存储器标签。在一些示例实施例中，装置500可以是移动电子设备(诸如通信设备100a-n或存储设备120)的一部分。如移动设备，装置500可以是移动和/或无线通信节点(诸如例如移动和/或无线服务器、计算机、接入点、手持型无线设备(例如电话、手写板/平板设备、便携式数字助理(PDA)、移动电视机、游戏设备、相机、视频记录器、音频/视频

播放器、无线电、数字图书阅读器、和/或全球定位系统(GPS)设备)、无线存储器标签、上述的任何组合,或诸如此类)的一部分。不管电子设备的类型,装置500还可以包括计算能力。

[0063] 图5说明了示例装置500的框图,其可以包括各种组件或以其它方式与各种组件通信,各种组件包含但不限于:处理器505、存储设备510、输入/输出(I/O)接口506、通信接口515和密钥流管理器540。根据一些实施例,处理器505(其可以被嵌入作为IC)可以被具体化成用于实现示例实施例的各种功能的各种构件,包含例如微处理器,协处理器,控制器,特定用途集成电路,诸如例如ASIC(专用集成电路),FPGA(现场可编程门阵列),或硬件加速器,处理电路或诸如此类。根据一个示例实施例,处理器505可以表示协同操作的多个处理器或一个或多个多核心处理器。此外,处理器505可以由多个晶体管、逻辑门、时钟(例如振荡器)、其它电路和诸如此类组成以促进执行本文所述的功能。处理器505可以但不是必须包括一个或多个附属的数字信号处理器。在一些示例实施例中,处理器505可以被配置为执行存储在存储设备510中的指令或以其它方式处理器505而言可以访问的指令。处理器505可以被配置为进行操作使得处理器使得或引导装置500执行本文所述的各种功能。

[0064] 无论被配置成硬件或经由存储在计算机可读存储介质上的指令,还是由其组合,当相应地配置时,处理器505可以是能够根据示例实施例的执行操作的实体和构件。因此,在处理器505被具体化成ASIC、FPGA或诸如此类,或其一部分的示例实施例中,处理器505可以是被特定配置的硬件以用于执行本文所述的操作和本文所述的算法。可替代地,在处理器505被具体化成存储在计算机可读存储介质上的指令的执行器的示例实施例中,该指令可以特定地配置处理器505以执行本文所述的算法和操作。在一些示例实施例中,处理器505可以是特定设备(例如,移动通信设备)的处理器,其被配置为用于通过经由用于执行本文所述的算法、方法和操作的执行指令来进一步配置处理器505来使用示例实施例。

[0065] 存储设备510可以是一个或多个有形的和/或非短暂性的计算机可读存储介质,其可以包括易失性和/或非易失性的存储器。在一些示例实施例中,存储设备510包括随机存取存储器(RAM)(包含动态和/或静态RAM)、片上或片外缓存存储器和/或诸如此类。此外,存储设备510可以包括非易失性存储器,其可以嵌入式的和/或可移动的,以及可以包括例如只读存储器、闪速存储器、磁存储设备(例如,硬盘、软盘驱动器、磁带等)、光盘驱动器和/或介质、非易失性的随机存取存储器(NVRAM)、各种类型的固态存储设备(例如,闪速存储器),和/或诸如此类。存储设备510可以包括用于数据的临时存储的缓存区域。在这点上,存储设备510中的一些或全部存储设备可以被包括在处理器505内。在一些示例实施例中,存储设备510可以经由共享总线与处理器505和/或其它组件进行通信。在一些示例实施例中,存储设备510可以被配置为提供将数据(诸如例如参考标记的特点)安全存储在存储设备510的可信任的模块中。

[0066] 此外,存储设备510可以被配置为存储指令、数据、应用、计算机可读程序代码指令和算法,和/或诸如此类,以用于使得处理器505和示例装置500能够依照本文所述的示例实施例来执行各种功能。例如,存储设备510可以被配置为对由处理器505处理的输入数据进行缓冲。另外地或可替代地,存储设备510可以被配置为存储用于由处理器505执行的指令。

[0067] I/O接口506可以是具体化成硬件或软件和硬件的组合的任何设备、电路或构件,其被配置为使处理器505与其它电路或设备(诸如用户接口525)进行接口。在一些示例实施例中,I/O接口可以具体化成总线或与总线进行通信,该总线由多个组件共享。在一些示例

实施例中，处理器505可以经由I/O接口506与存储器510进行接口。I/O接口506可以被配置为将信号或数据转换成可以由处理器505解释的形式。I/O接口506还可以执行输入和输出的缓冲以支持处理器505的操作。根据一些示例实施例，处理器505和I/O接口506可以被组合在被配置为执行或使得装置500执行各种功能的单个芯片或集成电路上。

[0068] 在一些实施例中，装置500或装置500的组件中的一些组件(例如，处理器505和存储设备510)可以被具体化成芯片或芯片组。也就是说，装置500可以包括：一个或多个物理封装(例如芯片)，其包含在结构装配件(例如基板)上的材料、组件和/或线。结构装配件可以提供物理强度，尺寸节省和/或用于包括在其上的组件电路的电气交互的限制。因此在一些情况下，装置500可以被配置为在单个芯片或单个“片上系统”上实现实施例。照此，在一些情况下，芯片或芯片组可以构成用于执行本文所述的功能以及相对于处理器505的构件。

[0069] 通信接口515可以是具体化成硬件、计算机程序产品或硬件和计算机程序产品的组合的任何设备或构件(例如电路)，其被配置为接收和/或传送来自/去往网络(包含但不限于智能空间或类似的RF存储器标签环境和/或与示例装置500通信的任何其它设备或模块)的数据。通信接口515可以被配置为经由有线或无线连接以及经由任何类型的通信协议(诸如支持蜂窝通信或进场通信的通信协议)来传递信息。根据各种示例实施例，通信接口515可以被配置为支持在各种网络(包含但不限于：基于互联网协议的网络(例如互联网)、蜂窝网络，或诸如此类)中的通信的传输和接收。此外，通信接口515可以被配置为支持设备至设备的通信，诸如在移动自组织网络(MANET)中。处理器505还可以被配置为通过例如控制被包括在通信接口515内的硬件来促进经由该通信接口515的通信。在这点上，通信接口515可以包括：例如通信驱动器电路(例如支持经由例如光纤连接的有线通信的电路)、一个或多个天线、传送器、接收器、收发器和/或支持硬件，包含例如用于使得能够通信的处理器。经由通信接口515，示例装置500可以以设备至设备的方式和/或经由经由基站、节点B、增强的节点B、接入点、服务器、网关、路由器或诸如此类的间接通信与各种其它网络实体进行通信。

[0070] 示例装置500的密钥流管理器540可以是部分地或全部地具体化成硬件、计算机程序产品或硬件和计算机程序产品的组合的任何构件或设备，诸如实现存储的指令以配置示例装置500的处理器505，存储被配置为执行本文所述的功能的可执行的程序代码指令的存储设备510，或被配置为执行如本文所述的密钥流管理器540的功能的硬件配置的处理器505。在一些示例实施例中，密钥流管理器540可以被配置为实现相对于图1的存储设备120的引擎和IC所描述的功能。在示例实施例中，处理器505包括或控制密钥流管理器540。密钥流管理器540可以被部分地或全部地具体化成类似于处理器505但是与处理器505分开的处理器。在这点上，密钥流管理器540可以与处理器505通信。在各种示例实施例中，密钥流管理器540可以部分地或全部地驻留在不同的装置上，使得可以由第一装置来执行密钥流管理器540的功能中的一些或全部功能，以及可以由一个或多个其它装置来执行密钥流管理器540的功能中的剩余功能。例如，通信设备的密钥流装置可以使得创建和/或操作密钥流，而存储设备120的密钥流管理器540可以被配置为执行各种密钥流的整合。

[0071] 此外，装置500和处理器505可以被配置为经由密钥流管理器540来执行各种功能。在这点上，密钥流管理器540可以被配置为实现本文所述的操作和功能中的一些或全部操作和功能。例如，密钥流管理器540可以被配置为实现以上相对于图1至图4所述的功能以及

以其它方式所述的功能。此外，根据一些示例实施例，密钥流管理器540可以被配置为执行图7和图8所述的操作以及描述的其变型。

[0072] 在这点上，参照图7，在700，在第一设备在存储设备的无线电通信范围中的实例中，密钥流管理器540(当由示例通信设备来具体化时)可以被配置为使得生成的密钥流被传送给存储设备。在710，在存储设备在无线电通信范围中的实例中，密钥流管理器540可以被配置为使得在存储设备上访问生成的修过的密钥流或从存储设备来接收生成的修改的密钥流，以及在720，密钥流管理器540可以被配置为基于生成的密钥流和修改的密钥流来确定会话密钥。在一些示例实施例中，由存储设备基于生成的密钥流和由存储设备从第二设备接收的密钥流来创建修改的密钥流。此外，在730，密钥流管理器540可以被配置为使得通信数据(例如，完整性保护数据和/或解密的数据)被传送给存储设备或第二设备。在各种示例实施例中，使用会话密钥的至少一部分来保护通信数据，以及该通信数据旨在用于第二设备。可替代地或另外地，在一些示例实施例中，密钥流管理器540可以被配置为使得安全的通信数据被直接传送给第二设备。

[0073] 在740，密钥流管理器540还可以被配置为基于由第一设备和第三设备与存储设备的先前连接来确定用于第一设备和第三设备的另一会话密钥。最后，在750，在第一设备和第三设备在无线电通信范围中的实例中，密钥流管理器540可以被配置为使得基于另一个会话密钥第一设备能够与第三设备进行通信。

[0074] 参照图8，在800，在第一设备在无线电通信范围中的实例中，密钥流管理器540(当由示例存储设备来具体化时)可以被配置为接收第一生成的密钥流，以及在810，在第二设备在无线电通信范围中的实例中，密钥流管理器540可以被配置为接收第二生成的密钥流。此外，在820，密钥流管理器540可以被配置为基于第二设备的标识指示符和第一生成的密钥流来生成第一修改的密钥流，以及在830基于第一设备的标识指示符和第二生成的密钥流来生成第二修改的密钥流。

[0075] 现在参照图6，提供了依照本发明的各种实施例的更具体的示例装置。图6的示例装置是移动终端10，该移动终端10被配置为在诸如蜂窝通信网络的无线网络内进行通信，该移动终端10可以包含诸如电子标签32的存储设备。移动终端10可以被配置为经由电子标签32来执行如本文所述的通信设备100a-n、存储设备120和/或装置500的功能。电子标签32可以经由内部的有线通信信道或经由具有天线12的RF通信与处理器20进行通信。更具体地，可以使得移动终端10经由处理器20来执行相对于图1-4和/或图7-9所述的功能。在这点上，根据一些示例实施例，处理器20可以被配置为执行相对于密钥流管理器540所描述的功能。处理器20可以是被配置为类似于连同例如I/O接口506的处理器505的集成电路或芯片。此外，易失性存储器40和非易失性存储器42可以被配置为作为计算机可读存储介质来支持处理器20的操作。在一些示例实施例中，电子标签32可以含有天线部分和存储器部分，在此类示例实施例中，电子标签32可以被配置为独立于移动终端10进行通信。可替代地或另外地，移动终端10可以承担电子标签的功能。

[0076] 移动终端10还可以包括：天线12、传送器14和接收器16，其可以被包括作为移动终端10的通信接口的一部分。可替代地或另外地，在一些实施例中，移动终端10可以包括另外的天线和/或无线无线电设备，以便使得能够无线供电和将数据传递给远程存储器标签，诸如有源存储器标签或无源无电池的存储器标签。还可以包括扬声器24、麦克风26、显示器28

(其可以是触摸屏显示器)以及小键盘作为用户接口的一部分。

[0077] 作为示例以及参照图9的信令流程图,两个或更多的通信设备(诸如通信设备100a和通信设备100b)可以被配置为使用存储设备120以安全的方式进行通信。依照本发明的一些示例实施例以及在通信设备100a接触存储设备120或在存储设备120的通信范围中的实例中,通信设备100a可以生成密钥流以及使得所生成的密钥流被传送给存储设备120。见信号902。类似地,在通信设备100b在存储设备120的通信范围中的实例中,通信设备100b可以生成密钥流以及使得所生成的密钥流被传送给存储设备120。见信号904。

[0078] 在一些示例实施例中以及在接收到两个或更多的生成的密钥流的实例中,在操作906,存储设备120可以被配置为对所接收的生成的密钥流进行修改。参照图2-4、7和图8示出并描述的修改密钥流的一些示例方法。在通信设备(诸如通信设备100a和/或通信设备100b)在存储设备120的通信范围中的实例中,通信设备100a和/或通信设备100b可以访问和/或接收修改的密钥流。见信号908和信号910。

[0079] 在一些示例实施例中,通信设备100a和/或通信设备100b可以基于在操作912和/或操作914处生成的密钥流和修改的密钥流来确定会话密钥。会话密钥可以被配置为保护通信设备100a和通信设备100b之间的通信的安全。在通信设备100a和/或通信设备100b可以试图传递通信数据的实例中,则确定的会话密钥的至少一部分可以用于保护通信数据的安全。由会话密钥的至少一部分保护安全的通信数据然后可以被传送给存储设备120和/或在通信设备100a和通信设备100b之间直接传递。

[0080] 图2-4和图7-9说明了根据示例实施例的示例系统、方法和/或计算机程序产品的流程图或过程。应当理解的是,流程图中的每个操作和/或流程图中的操作的组合可以由各种构件来实现。用于执行流程图的操作、流程图中的操作的组合,或本文所述的示例实施例的其它功能的构件可以包括:硬件,和/或包含计算机可读存储介质(与描述传播信号的计算机可读传输介质相对照)的计算机程序产品,计算机可读存储介质具有存储在其中的一个或多个计算机代码指令、程序指令或可执行的计算机程序代码指令。在这点上,用于执行图2-4和图7-9以及本文中以其它方式描述的操作和功能的程序代码指令可以被存储在示例装置(诸如示例装置500或通信设备100a-n)的存储设备上,诸如存储设备510、易失性存储器40或非易失性存储器42,并且由处理器(诸如存储器505或处理器20)来执行。如将了解的是,可以从计算机可读存储介质将任何此类程序代码指令加载到计算机或其它可编程装置(例如,处理器505、存储设备510或诸如此类)上以产生特定的机器,使得特定的机器成为用于实现流程图的操作中指定的功能。还可以将这些程序代码指令存储在能够引导计算机、处理器或其它可编程构件以特定方式执行功能从而生成特定机器或特定的制造品的计算机可读存储介质中。存储在计算机可读存储介质中的指令可以产生制造品,这里制造品成为用于实现流程图的操作中所指定的功能的构件。程序代码指令可以从计算机可读存储介质来取回并且被加载到计算机、处理器或其它可编程装置中以配置计算机、处理器或其它可编程装置以执行将在计算机、处理器或其它可编程装置上执行的或由其执行的操作。可以顺序地执行程度代码指令的取回、加载和执行,使得每次取回、加载和执行一个指令。在一些示例实施例中,可以并行地取回、加载和/或执行,使得一起取回、加载和/或执行多个指令。程序代码指令的执行可以产生计算机实现的过程,使得由计算机、处理器或其它可编程装置执行的指令提供用于实现流程图的操作中指定的功能的操作。

[0081] 因此，由处理器执行的与流程图的操作相关联的指令，或在计算机可读存储介质中存储与流程图的框或操作相关联的指令，支持用于执行指定功能的操作的组合。还应当理解的是，流程图的一个或多个操作，以及流程图中的框或操作的组合可以由执行指定功能的专用的基于硬件的计算机系统和/或处理器，或专用硬件和程序代码指令的组合来实现。

[0082] 有利地，以及依照本发明的一些示例实施例，团队中的两个或更多的成员能够使用不安全的存储器标签来交换安全的数据。例如，团队成员可以工作在包括用于临时存储和取回的存储器标签的一个或多个房间中。依照本文所述的一些示例实施例的描述，团队的这些成员可以具有团队成员之间的确定的一个或多个会话密钥。因此，在团队的成员在不安全的位置的实例中，团队成员可以使用先前部署的会话密钥经由不安全的RF存储器标签或其它存储器设备来传递数据而没有例如攻击者访问该数据的危险。

[0083] 有利地，以及依照本发明的一些示例实施例，通信设备可以被配置为将使用确定的会话密钥的至少一部分来安全保护的数据传递给与票务系统(例如，公共交通)、金融系统(例如，自动柜员机、用户之间的金融交易)、支付系统、销售系统的点和/或诸如此类集成的RF存储器标签。此类用户可以例如有利地允许通信设备和另外的通信设备或RF存储器标签之间的私有的、金融或其它安全数据的交换。

[0084] 本文中阐述的许多修改和其它实施例将进入已经受益于在上述描述和相关联的附图中呈现的教示的与这些实施例相关的领域的技术人员的脑海中。因此，应当理解的是，实施例不限制于所公开的特定实施例，以及修改和其它实施例旨在被包括在所附权利要求书的范围内。此外，虽然上述描述和相关联的附图在元素和/或功能的某些示例组合的上下文中描述了示例实施例，但是应当了解的是，可以由不背离所附权利要求书的范围的备选实施例来提供元素和/或功能的不同组合。在这点上，例如除了那些以上明确公开以外，元素和/或功能的不同组合也可以被设想为在所附权利要求中的一些权利要求中进行阐述。虽然本文使用了特定的术语，但是它们仅用于一般和描述性的含义而不是用于限制的目的。

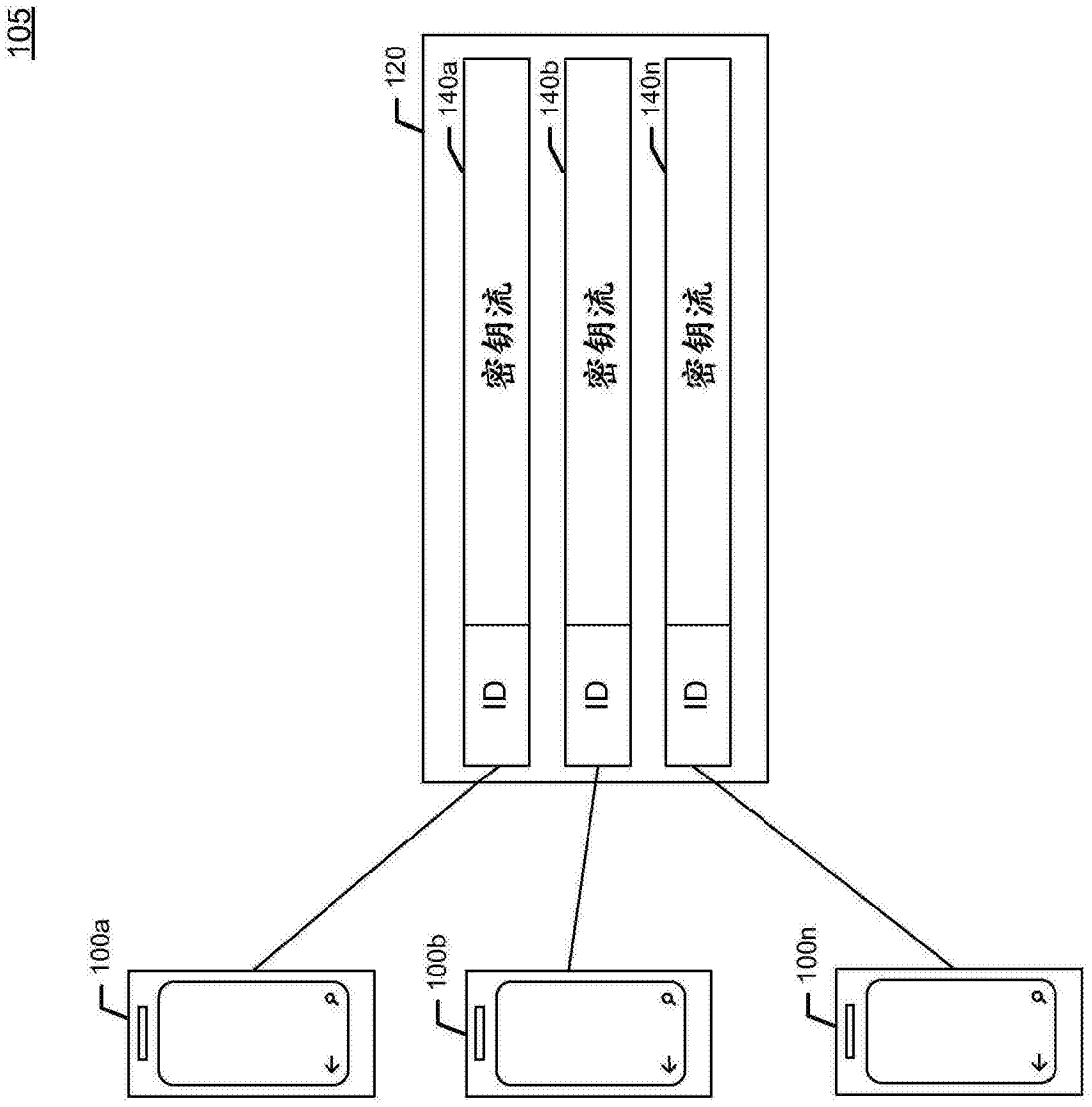


图1

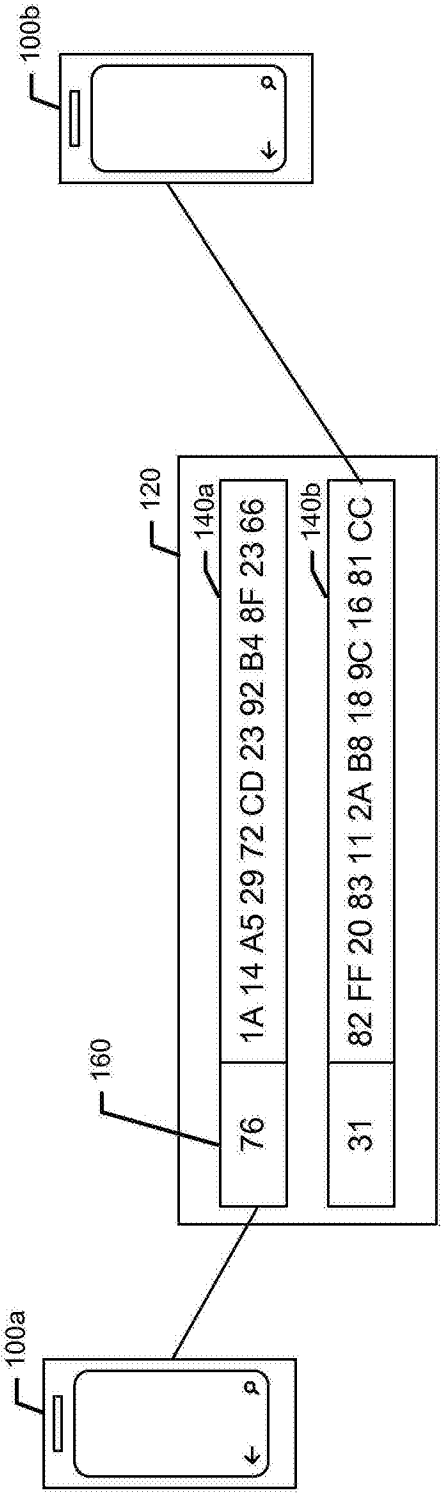

100b
120
140a
140b
1A 14 A5 29 72 CD 23 92 B4 8F 23 66
82 FF 20 83 11 2A B8 18 9C 16 81 CC
160
76
31
100a

图2

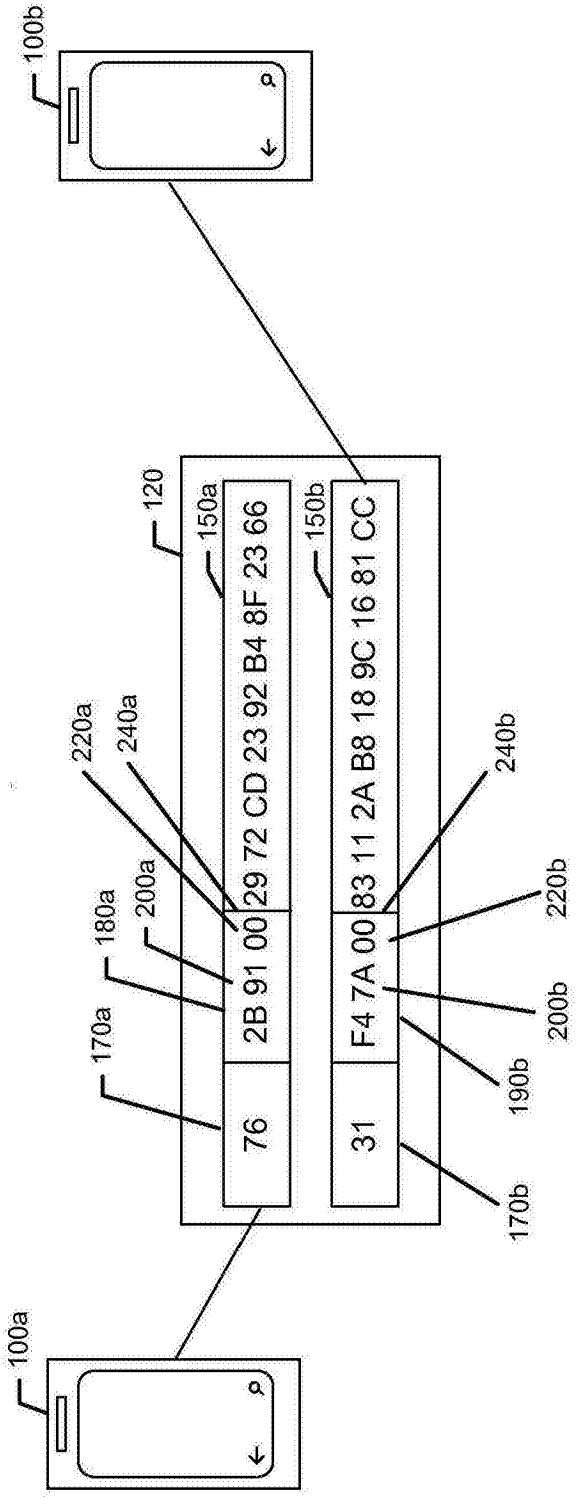

100b
120
150a
150b
220a
240a
240b
180a
200a
220b
2B 91 00 29 72 CD 23 92 B4 8F 23 66
F4 7A 00 83 11 2A B8 18 9C 16 81 CC
170a
200b
190b
76
31
170b
100a

图3

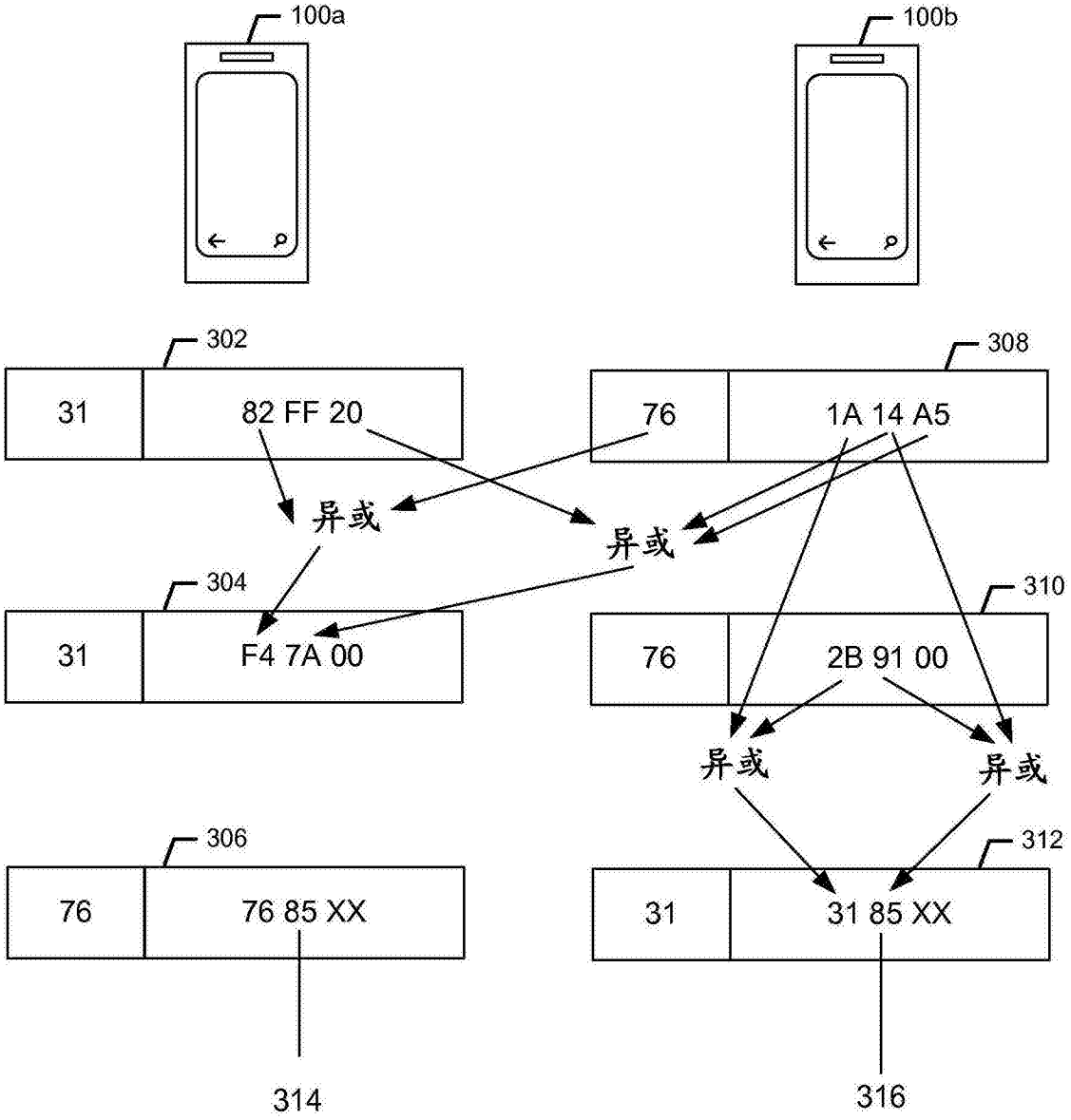

100a
100b
302
31
82 FF 20
308
76
1A 14 A5
异或
异或
304
31
F4 7A 00
310
76
2B 91 00
异或
异或
306
76
76 85 XX
312
31
31 85 XX
314
316

图4

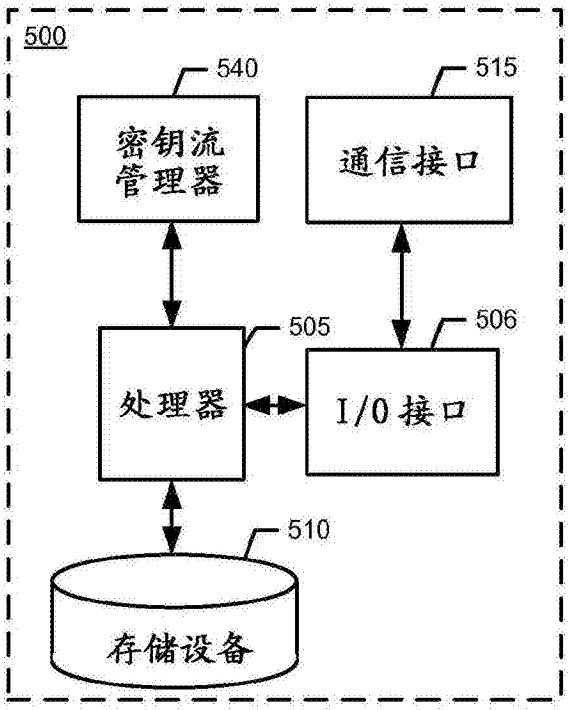

500
540
密钥流管理器
515
通信接口
505
处理器
506
I/O 接口
510
存储设备

图5

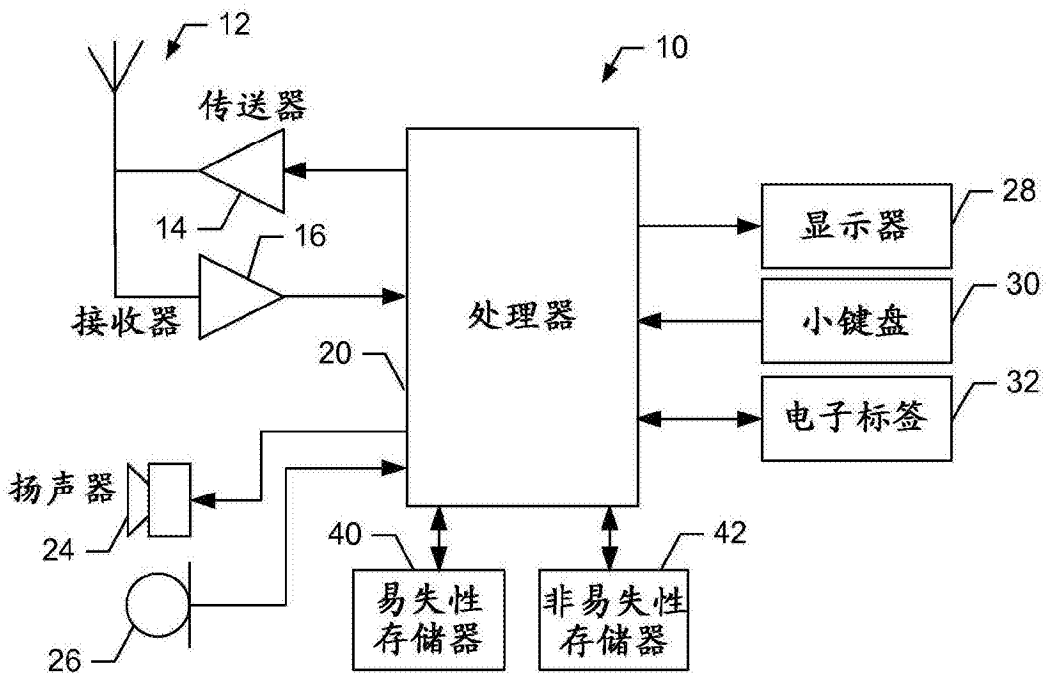

12
传送器
10
14
16
接收器
处理器
20
显示器
28
小键盘
30
电子标签
32
扬声器
24
26
40
易失性存储器
42
非易失性存储器

图6

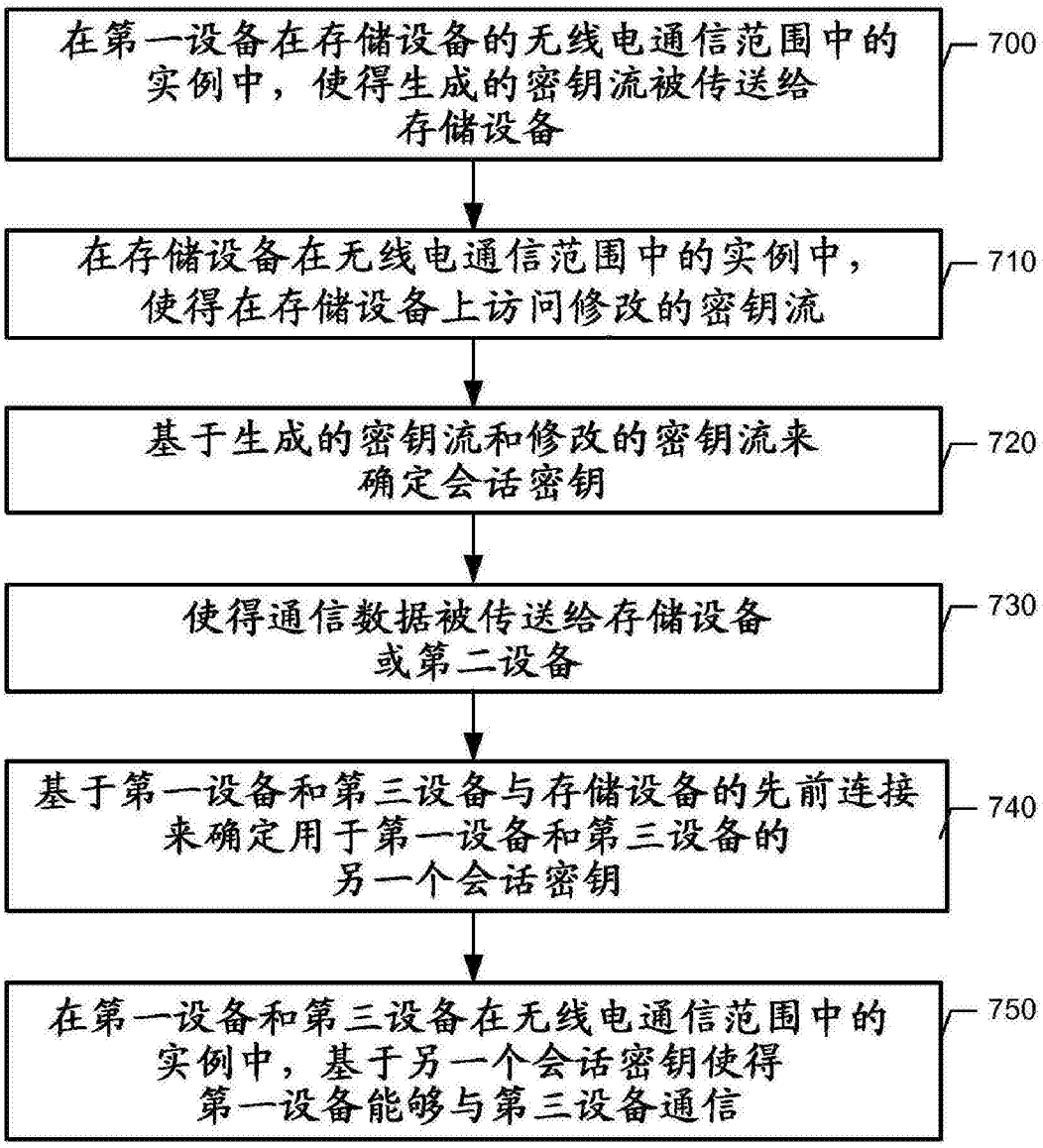

在第一设备在存储设备的无线电通信范围中的实例中，使得生成的密钥流被传送给存储设备
700
在存储设备在无线电通信范围中的实例中，使得在存储设备上访问修改的密钥流
710
基于生成的密钥流和修改的密钥流来确定会话密钥
720
使得通信数据被传送给存储设备或第二设备
730
基于第一设备和第三设备与存储设备的先前连接来确定用于第一设备和第三设备的另一个会话密钥
740
在第一设备和第三设备在无线电通信范围中的实例中，基于另一个会话密钥使得第一设备能够与第三设备通信
750

图7

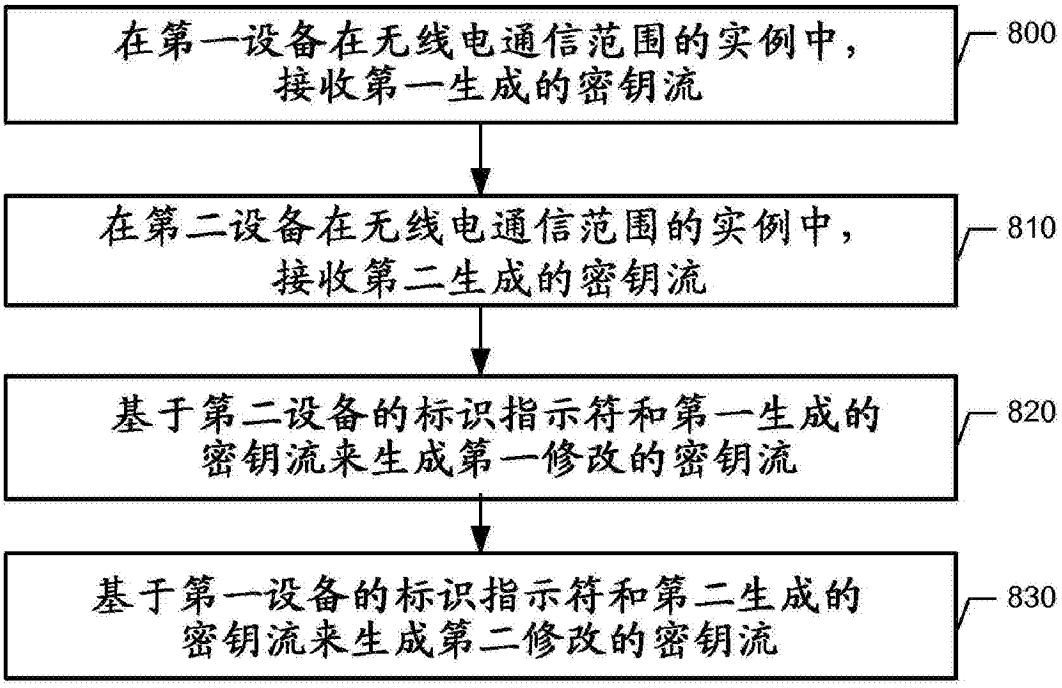

在第一设备在无线电通信范围的实例中，接收第一生成的密钥流
800
在第二设备在无线电通信范围的实例中，接收第二生成的密钥流
810
基于第二设备的标识指示符和第一生成的密钥流来生成第一修改的密钥流
820
基于第一设备的标识指示符和第二生成的密钥流来生成第二修改的密钥流
830

图8

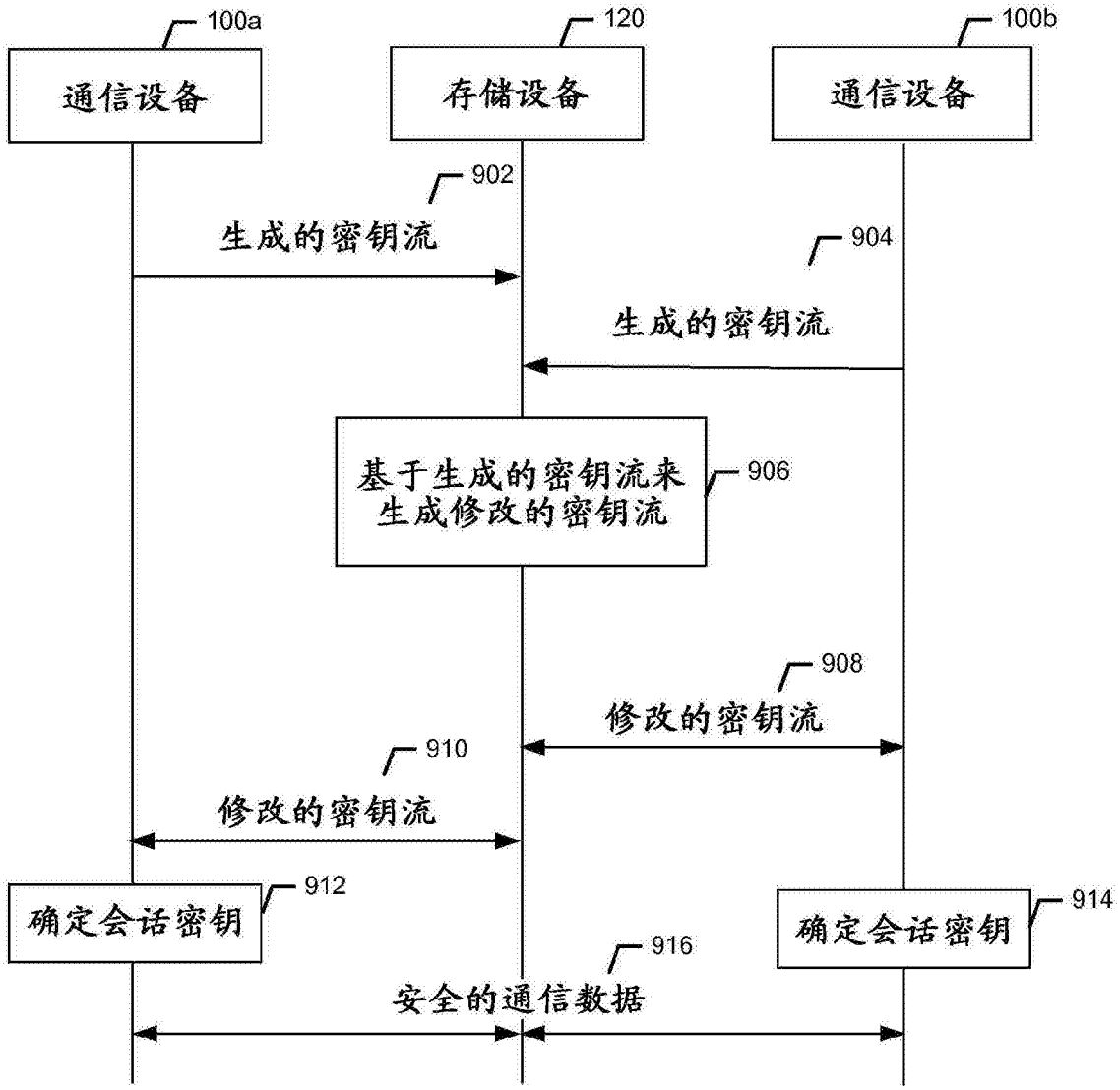

100a
通信设备
120
存储设备
100b
通信设备
902
生成的密钥流
904
生成的密钥流
基于生成的密钥流来
生成修改的密钥流
906
908
修改的密钥流
910
修改的密钥流
确定会话密钥
912
确定会话密钥
914
916
安全的通信数据

图9