(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 101882995 B
(45)授权公告日 2013.08.07

(21)申请号 200910136410.8
(22)申请日 2009.05.06
(73)专利权人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区科技南路55号
(72)发明人 李杰 邰春玲 王剑
(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 余刚 吴孟秋
(51)Int.Cl.
H04L 9/28(2006.01)
H04L 12/70(2013.01)

(56)对比文件
CN 101179374 A,2008.05.14,
CN 101179374 A,2008.05.14,
CN 1956443 A,2007.05.02,
CN 101258750 A,2008.09.03,
CN 101258750 A,2008.09.03,
CN 1421080 A,2003.05.28,

审查员 范文婧

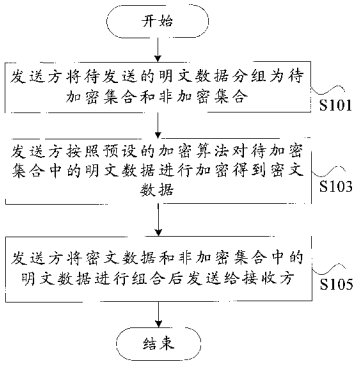
权利要求书6页 说明书13页 附图11页

(54)发明名称

数据发送、接收和传输方法及装置

(57)摘要

本发明公开了一种数据发送、接收和传输方法及装置，在上述方法中，发送方将待发送的明文数据分组为待加密集合和非加密集合，并根据预设的密钥采用预设的加密算法对待加密集合中的明文数据进行加密得到密文数据，再将密文数据和非加密集合中的明文数据进行组合后发送给接收方；接收方将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合，并根据预设的密钥采用预设的解密算法对待解密集合中的密文数据进行解密得到明文数据，再将解密得到的明文数据与非解密集合中的明文数据进行组合。根据本发明提供的技术方案，可以解决相关技术中使用加密和解密算法时需要消耗较多系统计算资源的问题，进而可以节省大量系统计算资源。



CN 101882995 B

1. 一种数据发送方法，其特征在于，包括：

发送方将待发送的明文数据分组为待加密集合和非加密集合；

所述发送方按照预设的加密算法对所述待加密集合中的明文数据进行加密得到密文数据；

所述发送方将所述密文数据和所述非加密集合中的明文数据进行组合后发送给接收方；

其中，所述发送方将待发送的明文数据分组为待加密集合和非加密集合包括：如果所述发送方是第一次向所述接收方发送数据，则所述发送方根据与所述接收方协商的随机数和数据分组算法将所述待发送的明文数据分组为待加密集合和非加密集合；如果所述发送方不是第一次向所述接收方发送数据，则所述发送方根据上一次向所述接收方发送数据时产生的新的随机数，采用所述数据分组算法将待发送的明文数据分组为待加密集合和非加密集合；

所述发送方将所述密文数据和所述非加密集合中的明文数据进行组合包括：如果所述发送方是第一次向所述接收方发送数据，则所述发送方根据与所述接收方协商的随机数和数据组合算法对所述密文数据和所述非加密集合中的明文数据进行组合；如果所述发送方不是第一次向所述接收方发送数据，则所述发送方根据上一次向所述接收方发送数据时产生的新的随机数，采用所述数据组合算法对所述密文数据和所述非加密集合中的明文数据进行组合。

2. 根据权利要求 1 所述的方法，其特征在于，在将待发送的明文数据分组为待加密集合和非加密集合之前，所述方法还包括：

所述发送方与所述接收方进行协商，确定所述预设的加密算法、进行加密时使用的密钥、随机数、随机数序列产生算法、数据分组算法、数据组合算法，其中，所述数据分组算法用于根据所述随机数对所述待发送的明文数据进行分组，所述数据组合算法用于根据所述随机数对所述密文数据和所述非加密集合中的明文数据进行组合。

3. 根据权利要求 2 所述的方法，其特征在于，在所述发送方发送所述密文数据和所述非加密集合中的明文数据之后，还包括：

所述发送方根据所述随机数序列产生算法以及所述随机数产生新的随机数，其中，所述新的随机数用于在下一次发送数据时进行数据分组和数据组合。

4. 一种数据接收方法，其特征在于，包括：

接收方将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合；

按照预设的解密算法对所述待解密集合中的密文数据进行解密得到明文数据；

所述接收方将解密得到的所述明文数据和所述非解密集合中的明文数据进行组合；

其中，所述接收方将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合包括：如果所述接收方是第一次接收所述发送方发送的数据，则所述接收方根据与所述发送方协商的随机数和数据分组算法将所述接收到的数据分组为待解密集合和非解密集合；如果所述接收方不是第一次接收所述发送方发送的数据，则所述接收方根据上一次接收来自所述发送方的数据时产生的新的随机数，采用所述数据分组算法将接收到的数据分组为待解密集合和非解密集合；

所述接收方将解密得到的所述明文数据和所述非解密集合中的明文数据进行组合，包括：如果所述接收方是第一次接收所述发送方发送的数据，则所述接收方根据与所述发送方协商的随机数和数据组合算法对解密得到的所述明文数据与所述非解密集合中的明文数据进行组合；如果所述接收方不是第一次接收所述发送方发送的数据，则所述接收方根据上一次接收所述发送方发送的数据时产生的新的随机数，采用所述数据组合算法对解密得到的所述明文数据与所述非解密集合中的明文数据进行组合。

5. 根据权利要求 4 所述的方法，其特征在于，在所述将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合之前，所述方法还包括：

所述接收方与发送方进行协商，确定所述预设的解密算法、对密文数据进行解密时使用的密钥、随机数、随机数序列产生算法、数据分组算法、数据组合算法，其中，所述数据分组算法用于根据所述随机数对接收到的所述数据进行分组，所述数据组合算法用于根据所述随机数对解密得到的所述明文数据与所述非解密集合中的明文数据进行组合。

6. 根据权利要求 5 所述的方法，其特征在于，所述将解密得到的所述明文数据和所述非解密集合中的明文数据进行组合之后，所述方法还包括：

所述接收方根据所述随机数序列产生算法以及所述随机数产生新的随机数，其中，所述新的随机数用于在下一次接收来自所述发送方的数据时进行数据分组和数据组合。

7. 一种数据发送装置，其特征在于，包括：

分组器，用于将待发送的明文数据分为待加密集合和非加密集合；

加密模块，用于按照预设的加密算法对所述待加密集合中的明文数据进行加密得到密文数据；

组合器，用于将所述加密模块得到的所述密文数据和所述非加密集合中的明文数据进行组合；

发送模块，用于将所述组合器组合后的数据发送给接收方；

第一存储模块，用于保存与所述接收方协商确定的预设的加密算法、对明文数据进行加密时使用的密钥、随机数、随机数序列产生算法、数据分组算法和数据组合算法，其中，所述数据分组算法用于所述分组器根据所述随机数对所述待发送的明文数据进行分组，所述数据组合算法用于所述组合器根据所述随机数对所述密文数据和所述非加密集合中的明文数据进行组合；

其中，所述分组器采用的分组方式为：如果是第一次向所述接收方发送数据，则根据与所述接收方协商的随机数和数据分组算法将所述待发送的明文数据分组为待加密集合和非加密集合；如果不是第一次向所述接收方发送数据，则根据上一次向所述接收方发送数据时产生的新的随机数，采用所述数据分组算法将待发送的明文数据分组为待加密集合和非加密集合；

所述组合器采用的组合方式为：如果是第一次向所述接收方发送数据，则根据与所述接收方协商的随机数和数据组合算法对所述密文数据和所述非加密集合中的明文数据进行组合，如果不是第一次向所述接收方发送数据，则根据上一次向所述接收方发送数据时产生的新的随机数，采用所述数据组合算法对所述密文数据和所述非加密集合中的明文数据进行组合。

8. 根据权利要求 7 所述的装置，其特征在于，所述装置还包括：

随机数产生器，用于根据所述数据分组算法、所述数据组合算法使用的所述随机数，所述随机数序列产生算法产生新的随机数；

第二存储模块，与随机数产生器相连接，用于存储所述随机数产生器产生的所述新的随机数；

所述分组器还用于在下一次向所述接收方发送数据时，根据所述新的随机数使用所述数据分组算法对待发送的明文数据进行数据分组；

所述组合器还用于在下一次向所述接收方发送数据时，根据所述新的随机数使用所述数据组合算法对非加密集合中的明文数据和被所述加密模块加密后的密文数据进行组合。

9. 一种数据接收装置，其特征在于，包括：

接收模块，用于接收来自发送方的数据；

分组器，用于将接收到的所述数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合；

解密模块，用于按照预设的解密算法将所述待解密集合中的密文数据进行解密得到明文数据；

组合器，用于将所述解密模块解密得到的所述明文数据和所述非解密集合中的所述明文数据进行组合；

第一存储模块，用于保存与所述发送方协商确定的预设的解密算法、对所述密文数据进行解密时使用的密钥、随机数、随机数序列产生算法、数据分组算法和数据组合算法，其中，所述数据分组算法用于所述分组器根据所述随机数对所述接收模块接收到的数据进行分组，所述数据组合算法用于所述组合器根据所述随机数对解密得到的明文数据和所述非解密集合中的明文数据进行组合；

所述分组器采用的分组方式为：如果是第一次接收所述发送方发送的数据，则根据与所述发送方协商的随机数和数据分组算法将所述接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合；如果不是第一次接收所述发送方发送的数据，则根据上一次接收所述发送方发送的数据时产生的新的随机数，采用所述数据分组算法将所述接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合；

所述组合器采用的组合方式为：如果是第一次接收所述发送方发送的数据，则根据与所述发送方协商的随机数和数据组合算法对所述解密模块解密得到的所述明文数据和所述非解密集合中的所述明文数据进行组合，如果不是第一次接收所述发送方发送的数据，则根据上一次接收所述发送方发送的数据时产生的新的随机数，采用所述数据组合算法对所述解密模块解密得到的所述明文数据和所述非解密集合中的所述明文数据进行组合。

10. 根据权利要求 9 所述的装置，其特征在于，所述装置还包括：

随机数产生器，用于根据所述数据分组算法、所述数据组合算法使用的所述随机数，所述随机数序列产生算法产生新的随机数；

第二存储模块，与随机数产生器相连接，用于存储所述随机数产生器产生的所述新的随机数；

所述分组器还用于在下一次接收来自所述发送方的数据时，根据所述新的随机数使用所述数据分组算法对接收到的数据进行数据分组；

所述组合器还用于在下一次接收来自所述发送方的数据时，根据所述新的随机数使用

所述数据组合算法对解密得到的明文数据和所述非解密集合中的明文数据进行组合。

11. 一种数据传输方法，其特征在于，包括：

发送方将待发送的明文数据分组为待加密集合和非加密集合，并根据预设的密钥采用预设的加密算法对所述待加密集合中的明文数据进行加密得到密文数据，再将所述密文数据和所述非加密集合中的明文数据进行组合后发送给接收方；

所述接收方将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合，并根据所述预设的密钥采用预设的解密算法对所述待解密集合中的密文数据进行解密得到明文数据，再将解密得到的所述明文数据与所述非解密集合中的明文数据进行组合；

其中，在所述发送方将待发送的明文数据分组为待加密集合和非加密集合之前，所述方法还包括：

所述发送方与所述接收方进行协商，确定所述预设的加密算法和所述预设的解密算法、所述预设的密钥、随机数、随机数序列产生算法、第一数据分组算法、第一数据组合算法、第二数据分组算法和第二数据组合算法，其中，所述第一数据分组算法用于所述发送方根据所述随机数对所述待发送的明文数据进行分组，所述第一数据组合算法用于所述发送方根据所述随机数对所述密文数据和所述非加密集合中的明文数据进行组合，所述第二数据分组算法用于所述接收方根据所述随机数对接收到的所述数据进行分组，所述第二数据组合算法用于所述接收方根据所述随机数对解密得到的所述明文数据与所述非解密集合中的明文数据进行组合，并且，所述第一数据组合算法与所述第二数据分组算法互为可逆，所述第一数据分组算法与所述第二数据组合算法互为可逆；

其中，所述发送方将待发送的明文数据分组为待加密集合和非加密集合包括：如果所述发送方是第一次向所述接收方发送数据，则所述发送方根据与所述接收方协商的随机数和数据分组算法将所述待发送的明文数据分组为待加密集合和非加密集合；如果所述发送方不是第一次向所述接收方发送数据，则所述发送方根据上一次向所述接收方发送数据时产生的新的随机数，采用所述数据分组算法将待发送的明文数据分组为待加密集合和非加密集合；

所述发送方将所述密文数据和所述非加密集合中的明文数据进行组合包括：如果所述发送方是第一次向所述接收方发送数据，则所述发送方根据与所述接收方协商的随机数和数据组合算法对所述密文数据和所述非加密集合中的明文数据进行组合；如果所述发送方不是第一次向所述接收方发送数据，则所述发送方根据上一次向所述接收方发送数据时产生的新的随机数，采用所述数据组合算法对所述密文数据和所述非加密集合中的明文数据进行组合；

所述接收方将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合包括：如果所述接收方是第一次接收所述发送方发送的数据，则所述接收方根据与所述发送方协商的随机数和数据分组算法将所述接收到的数据分组为待解密集合和非解密集合；如果所述接收方不是第一次接收所述发送方发送的数据，则所述接收方根据上一次接收来自所述发送方的数据时产生的新的随机数，采用所述数据分组算法将接收到的数据分组为待解密集合和非解密集合；

所述接收方将解密得到的所述明文数据和所述非解密集合中的明文数据进行组合，包

括：如果所述接收方是第一次接收所述发送方发送的数据，则所述接收方根据与所述发送方协商的随机数和数据组合算法对解密得到的所述明文数据与所述非解密集合中的明文数据进行组合；如果所述接收方不是第一次接收所述发送方发送的数据，则所述接收方根据上一次接收所述发送方发送的数据时产生的新的随机数，采用所述数据组合算法对解密得到的所述明文数据与所述非解密集合中的明文数据进行组合。

12. 一种数据传输系统，其特征在于，包括：

发送装置，包括：

第一分组器，用于将待发送的明文数据分为待加密集合和非加密集合；

加密模块，用于按照预设的加密算法对所述待加密集合中的明文数据进行加密得到密文数据；

第一组合器，用于将所述非加密集合中的明文数据和所述加密模块加密后的所述密文数据进行组合；

发送模块，用于将所述第一组合器组合得到的数据发送给接收装置；

所述接收装置，包括：

接收模块，用于接收来自所述发送装置的数据；

第二分组器，用于将所述接收模块接收到的所述数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合；

解密模块，用于按照预设的解密算法将所述待解密集合中的密文数据进行解密得到明文数据；

第二组合器，用于将所述解密模块解密得到的所述明文数据和所述非解密集合中的明文数据进行组合；

其中，所述发送装置还包括：

第一存储模块，用于保存与所述接收装置协商确定的所述预设的加密算法、对明文数据进行加密时使用的密钥、随机数、随机数序列产生算法、第一数据分组算法和第一数据组合算法，其中，所述第一数据分组算法用于所述第一分组器根据所述随机数对所述待发送的明文数据进行分组，所述第一数据组合算法用于所述第一组合器根据所述随机数对所述密文数据和所述非加密集合中的明文数据进行组合；

所述接收装置还包括：

第二存储模块，用于保存与所述发送装置协商确定的预设解密算法、对所述密文数据进行解密时使用的所述密钥、所述随机数、所述随机数序列产生算法、第二数据分组算法和第二数据组合算法，其中，所述第二数据分组算法用于所述第二分组器根据所述随机数对所述接收模块接收到的数据进行分组，所述第二数据组合算法用于所述第二组合器根据所述随机数对解密得到的明文数据和所述非解密集合中的明文数据进行组合，并且，所述第一数据组合算法与所述第二数据分组算法互为可逆，所述第一数据分组算法与所述第二数据组合算法互为可逆；

其中，

所述第一分组器采用的分组方式为：如果是第一次向所述接收装置发送数据，则根据与所述接收装置协商的随机数和数据分组算法将所述待发送的明文数据分组为待加密集合和非加密集合；如果不是第一次向所述接收装置发送数据，则根据上一次向所述接收装

置发送数据时产生的新的随机数，采用所述数据分组算法将待发送的明文数据分组为待加密集合和非加密集合；

所述第一组合器采用的组合方式为：如果是第一次向所述接收装置发送数据，则根据与所述接收装置协商的随机数和数据组合算法对所述密文数据和所述非加密集合中的明文数据进行组合，如果不是第一次向所述接收装置发送数据，则根据上一次向所述接收装置发送数据时产生的新的随机数，采用所述数据组合算法对所述密文数据和所述非加密集合中的明文数据进行组合；

所述第二分组器采用的分组方式为：如果是第一次接收所述发送装置发送的数据，则根据与所述发送装置协商的随机数和数据分组算法将所述接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合；如果不是第一次接收所述发送装置发送的数据，则根据上一次接收所述发送装置发送的数据时产生的新的随机数，采用所述数据分组算法将所述接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合；

所述第二组合器采用的组合方式为：如果是第一次接收所述发送装置发送的数据，则根据与所述发送装置协商的随机数和数据组合算法对所述解密模块解密得到的所述明文数据和所述非解密集合中的所述明文数据进行组合，如果不是第一次接收所述发送装置发送的数据，则根据上一次接收所述发送装置发送的数据时产生的新的随机数，采用所述数据组合算法对所述解密模块解密得到的所述明文数据和所述非解密集合中的所述明文数据进行组合。

数据发送、接收和传输方法及装置

技术领域

[0001] 本发明涉及通信领域，具体而言，涉及一种数据发送、接收和传输方法及装置。

背景技术

[0002] 通信技术用于为人类交换信息，其在促进科学，技术，文化，教育，生产的发展，提高人类生活的质量方面起到了重大作用。但是，随着通信网络规模的进一步扩大，以及网络通信开放性程度的进一步提高，各通信实体之间信息内容的安全传输受到了极大的威胁。目前，通信网络面临的威胁来自很多方面，并随时间不断变化。

[0003] 当前，通信网络面临的威胁可以宏观地分为自然威胁和人为威胁。其中，自然威胁来自于各种自然灾害、恶劣的空间环境、电磁辐射、电磁干扰以及设备老化等；而人为威胁是指采用人为手段对通信网络进行攻击。这些攻击手段都是通过寻找系统的弱点，以达到破坏、欺骗、窃取数据等目的，从而造成网络用户经济上或者其它方面不可估量的损失。

[0004] 目前，常见的人为网络攻击方法包括以下几种：

[0005] 中断：是对系统的可用性进行攻击，例如，破坏计算机硬件，线路或者文件管理系统。

[0006] 窃听：是对系统保密性进行攻击，例如，搭线窃听，对文件或者程序的非法拷贝等。

[0007] 篡改：是对系统的完整性进行攻击，例如，修改数据文件中的数据，替换某一程序使其执行不同的功能，修改网络中传送的信息内容等。

[0008] 伪造：是对系统的真实性进行攻击，例如，在网络中插入伪造的消息或在文件中插入伪造的记录。

[0009] 网络安全中对于窃听攻击的主要防护手段就是数据加密，通信双方预先协商好通信时使用的密钥和加密方法等，在通信时，发送方使用预定的加密算法和密钥对通信信息进行加密处理，被加密的通信信息称之为密文，然后将上述密文发送给接收方；接收方收到加密的信息后，使用预定的解密算法和密钥对上述密文进行解密，得到加密前的通信信息，即明文。如果密文在发送到接收方的过程中被第三方窃听，但由于第三方难以同时得到解密算法和密钥，因而无法得出明文，从而无法达成窃取通信信息的目的。

[0010] 在实际实施过程中，由于需要有效防止来自攻击者恶意的破解，加密算法一般都设计得比较复杂，因而，在使用加密和解密算法消耗的系统计算资源较多，而且，由于系统业务数量上升，在发送较大明文数据时，需要消耗的计算资源也会相应增多，从而造成对资源的大量耗费，进而使得系统计算资源紧张。

发明内容

[0011] 针对相关技术中使用加密和解密算法时消耗的系统计算资源较多的问题而提出本发明，为此，本发明的主要目的在于提供一种改进的数据发送、接收和传输方案，以解决上述问题。

[0012] 根据本发明的一个方面，提供了一种数据发送方法。

[0013] 根据本发明的数据发送方法包括：发送方将待发送的明文数据分组为待加密集合和非加密集合；发送方按照预设的加密算法对待加密集合中的明文数据进行加密得到密文数据；发送方将密文数据和非加密集合中的明文数据进行组合后发送给接收方。

[0014] 优选地，在将待发送的明文数据分组为待加密集合和非加密集合之前，上述方法还包括：发送方与接收方进行协商，确定预设的加密算法、进行加密时使用的密钥、随机数、随机数序列产生算法、数据分组算法、数据组合算法，其中，数据分组算法用于根据随机数对待发送的明文数据进行分组，数据组合算法用于根据随机数对密文数据和非加密集合中的明文数据进行组合。

[0015] 优选地，上述将待发送的明文数据分组为待加密集合和非加密集合包括：如果发送方是第一次向接收方发送数据，则发送方根据随机数和数据分组算法将待发送的明文数据分组为待加密集合和非加密集合。

[0016] 优选地，上述将密文数据和非加密集合中的明文数据进行组合包括：如果发送方是第一次向接收方发送数据，则发送方根据随机数和数据组合算法对密文数据和非加密集合中的明文数据进行组合。

[0017] 优选地，在发送方发送密文数据和非加密集合中的明文数据之后，上述方法还包括：发送方根据随机数序列产生算法以及随机数产生新的随机数，其中，新的随机数用于在下一次发送数据时进行数据分组和数据组合。

[0018] 根据本发明的另一个方面，提供了一种数据接收方法。

[0019] 根据本发明的数据接收方法包括：接收方将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合；按照预设的解密算法对待解密集合中的密文数据进行解密得到明文数据；接收方将解密得到的明文数据和非解密集合中的明文数据进行组合。

[0020] 优选地，在将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合之前，上述方法还包括：接收方与发送方进行协商，确定预设的解密算法、对密文数据进行解密时使用的密钥、随机数、随机数序列产生算法、数据分组算法、数据组合算法，其中，数据分组算法用于根据随机数对接收到的数据进行分组，数据组合算法用于根据随机数对解密得到的明文数据与非解密集合中的明文数据进行组合。

[0021] 优选地，上述将接收到的密文数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合包括：如果接收方是第一次接收发送方发送的数据，则接收方根据随机数和数据分组算法将接收到的数据分组为待解密集合和非解密集合。

[0022] 优选地，上述将解密得到的明文数据和非解密集合中的明文数据进行组合包括：如果接收方是第一次接收发送方发送的数据，则接收方根据随机数和数据组合算法对解密得到的明文数据与非解密集合中的明文数据进行组合。

[0023] 优选地，将解密得到的明文数据和非解密集合中的明文数据进行组合之后，上述方法还包括：接收方根据随机数序列产生算法以及随机数产生新的随机数，其中，新的随机数用于在下一次接收来自发送方的数据时进行数据分组和数据组合。

[0024] 根据本发明的又一方面，提供了一种数据发送装置。

[0025] 根据本发明的数据发送装置包括：分组器、加密模块、组合器、以及发送模块，其中，分组器，用于将待发送的明文数据分为待加密集合和非加密集合；加密模块，用于按照

预设的加密算法对待加密集合中的明文数据进行加密得到密文数据；组合器，用于将加密模块得到的密文数据和非加密集合中的明文数据进行组合；发送模块，用于将组合器组合后的数据发送给接收方。

[0026] 优选地，上述装置还包括：第一存储模块，用于保存与接收方协商确定的预设的加密算法、对明文数据进行加密时使用的密钥、随机数、随机数序列产生算法、数据分组算法和数据组合算法，其中，上述数据分组算法用于分组器根据随机数对待发送的明文数据进行分组，上述数据组合算法用于组合器对密文数据和非加密集合中的明文数据进行组合。

[0027] 优选地，上述装置还包括：随机数产生器，用于根据数据分组算法、数据组合算法使用的随机数，随机数序列产生算法产生新的随机数；第二存储模块，与随机数产生器相连接，用于存储随机数产生器产生的新的随机数；上述分组器还用于在下一次向接收方发送数据时，根据新的随机数使用数据分组算法对待发送的明文数据进行数据分组；上述组合器还用于在下一次向接收方发送数据时，根据新的随机数使用数据组合算法对非加密集合中的明文数据和被加密模块加密后的密文数据进行组合。

[0028] 根据本发明的再一方面，提供了一种数据接收装置。

[0029] 根据本发明的数据接收装置包括：接收模块、分组器、解密模块和组合器，其中，接收模块，用于接收来自发送方的数据；分组器，用于将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合；解密模块，用于按照预设的解密算法将待解密集合中的密文数据进行解密得到明文数据；组合器，用于将解密模块解密得到的明文数据和非解密集合中的明文数据进行组合。

[0030] 优选地，上述装置还包括：第一存储模块，用于保存与发送方协商确定的预设的解密算法、对密文数据进行解密时使用的密钥、随机数、随机数序列产生算法、数据分组算法和数据组合算法，其中，数据分组算法用于分组器根据随机数对接收模块接收到的数据进行分组，数据组合算法用于组合器根据随机数对解密得到的明文数据和非解密集合中的明文数据进行组合。

[0031] 优选地，上述装置还包括：随机数产生器，用于根据数据分组算法、数据组合算法使用的随机数，随机数序列产生算法产生新的随机数；第二存储模块，与随机数产生器相连接，用于存储随机数产生器产生的新的随机数；分组器还用于在下一次接收来自发送方的数据时，根据新的随机数使用数据分组算法对接收到的数据进行数据分组；组合器还用于在下一次接收来自发送方的数据时，根据新的随机数使用数据组合算法对解密得到的明文数据和非解密集合中的明文数据进行组合。

[0032] 根据本发明的再一方面，提供了一种数据传输方法。

[0033] 根据本发明的数据传输方法包括：发送方将待发送的明文数据分组为待加密集合和非加密集合，并根据预设的密钥采用预设的加密算法对待加密集合中的明文数据进行加密得到密文数据，再将密文数据和非加密集合中的明文数据进行组合后发送给接收方；接收方将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合，并根据预设的密钥采用预设的解密算法对待解密集合中的密文数据进行解密得到明文数据，再将解密得到的明文数据与非解密集合中的明文数据进行组合。

[0034] 优选地，在发送将待发送的明文数据分组为待加密集合和非加密集合之前，上述方法还包括：发送方与接收方进行协商，确定预设的加密算法和预设的解密算法、预设的密

钥、随机数、随机数序列产生算法、第一数据分组算法、第一数据组合算法、第二数据分组算法和第二数据组合算法，其中，第一数据分组算法用于发送方根据随机数对待发送的明文数据进行分组，第一数据组合算法用于发送方根据随机数对密文数据和非加密集合中的明文数据进行组合，第二数据分组算法用于接收方根据随机数对接收到的数据进行分组，第二数据组合算法用于接收方根据随机数对解密得到的明文数据与非解密集合中的明文数据进行组合，并且，第一数据组合算法与第二数据分组算法互为可逆，第一数据分组算法与第二数据组合算法互为可逆。

[0035] 根据本发明的再一方面，提供了一种数据传输系统。

[0036] 根据本发明的数据传输系统包括：发送装置和接收装置，其中，发送装置，包括：第一分组器，用于将待发送的明文数据分为待加密集合和非加密集合；加密模块，用于按照预设的加密算法对待加密集合中的明文数据进行加密得到密文数据；第一组合器，用于将非加密集合中的明文数据和加密模块加密后的密文数据进行组合；发送模块，用于将第一组合器组合得到的数据发送给接收装置；其中，接收装置，包括：接收模块，用于接收来自发送装置的数据；第二分组器，用于将接收模块接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合；解密模块，用于按照预设的解密算法将待解密集合中的密文数据进行解密得到明文数据；第二组合器，用于将解密模块解密得到的明文数据和非解密集合中的明文数据进行组合。

[0037] 优选地，上述发送装置还包括：第一存储模块，用于保存与接收装置协商确定的预设的加密算法、对明文数据进行加密时使用的密钥、随机数、随机数序列产生算法、第一数据分组算法和第一数据组合算法，其中，第一数据分组算法用于第一分组器根据随机数对待发送的明文数据进行分组，第一数据组合算法用于第一组合器对密文数据和非加密集合中的明文数据进行组合；上述接收装置还包括：第二存储模块，用于保存与发送装置协商确定的预设解密算法、对密文数据进行解密时使用的密钥、随机数、随机数序列产生算法、第二数据分组算法和第二数据组合算法，其中，第二数据分组算法用于第二分组器根据随机数对接收模块接收到的数据进行分组，第二数据组合算法用于第二组合器根据随机数对解密得到的明文数据和非解密集合中的明文数据进行组合，并且，第一数据组合算法与第二数据分组算法互为可逆，第一数据分组算法与第二数据组合算法互为可逆。

[0038] 通过本发明，发送方在发送通信信息时对随机部分进行加密，接收方在接收通信信息时对上述随机部分进行解密，解决了相关技术中使用加密和解密算法时需要消耗较多系统计算资源的问题，进而节省了大量系统计算资源。

附图说明

[0039] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0040] 图 1 是根据本发明实施例的数据发送方法的流程图；

[0041] 图 2 是根据本发明优选实施例的数据发送方法的详细流程图；

[0042] 图 3 是根据本发明实施例的数据接收方法的流程图；

[0043] 图 4 是根据本发明优选实施例的数据接收方法的详细流程图；

[0044] 图 5 是根据本发明实施例的发送和接收方法相结合过程中数据报文的示意图；

[0045] 图 6 是根据本发明实施例的数据传输方法的流程图；

[0046] 图 7 为根据本发明实施例的数据传输方法的详细流程图；

[0047] 图 8 是根据本发明实施例的数据发送装置示意图；

[0048] 图 9 是根据本发明一种优选实施例的数据发送装置示意图；

[0049] 图 10 是根据本发明另一种优选实施例的数据发送装置示意图；

[0050] 图 11 是根据本发明实施例的数据接收装置示意图；

[0051] 图 12 是根据本发明优选实施例的数据接收装置示意图；

[0052] 图 13 是根据本发明实施例的实例的数据接收装置示意图；

[0053] 图 14 为根据本发明实施例的数据传输装置示意图。

具体实施方式

[0054] 功能概述

[0055] 考虑到相关技术中使用加密和解密算法时需要消耗较多系统计算资源的问题，本发明实施例提供了一种改进的数据发送、接收和传输方案，在发送数据时，发送方将待发送的明文数据分组为待加密集合和非加密集合，并按照预设的加密算法对待加密集合中的明文数据进行加密得到密文数据，然后将加密数据得到的密文数据和非加密集合中的明文数据进行组合后发送给接收方；而在接收方接收数据时，将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合，并按照预设的解密算法将待解密集合中的密文数据进行解密得到明文数据，然后将解密得到的明文数据和非解密集合中的明文数据进行组合获取发送方发送的明文数据。其中，在发送和接收数据时，需要利用随机数完成部分加密和部分解密的功能。

[0056] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本发明。

[0057] 方法实施例

[0058] 根据本发明实施例，首先提供了一种数据发送方法。

[0059] 图 1 是根据本发明实施例的数据发送方法的流程图。如图 1 所示，根据本发明实施例的数据发送方法包括以下步骤（步骤 S101- 步骤 S105）：

[0060] 步骤 S101：发送方将待发送的明文数据分组为待加密集合和非加密集合；

[0061] 在具体实施过程中，在执行步骤 S101 之前，发送方与接收方需要进行协商，以确定预设的加密算法、进行加密时使用的密钥、初始随机数、随机数序列产生算法、数据分组算法、数据组合算法，其中，该数据分组算法用于根据随机数对待发送的明文数据进行分组，该数据组合算法用于根据随机数对非加密集合中的明文数据和对加密得到的密文数据进行组合以供发送方发送。

[0062] 具体地，将待发送的明文数据分组为待加密集合和非加密集合分为以下两种情况：

[0063] (1) 如果发送方是第一次向接收方发送数据，则发送方根据初始随机数，采用上述数据分组算法将待发送的明文数据分组为待加密集合和非加密集合；

[0064] (2) 如果发送方不是第一次向接收方发送数据，则发送方根据上一次向接收方发送数据时产生的新的随机数，采用上述数据分组算法将待发送的明文数据分组为待加密集

合和非加密集合。

[0065] 步骤 S103 :发送方按照预设的加密算法对上述待加密集合中的明文数据进行加密得到密文数据 ;

[0066] 在具体实施过程中,发送方根据与接收方协商的上述密钥,采用上述预设的加密算法,对待加密集合中的明文数据进行加密得到这部分数据的密文数据。

[0067] 步骤 S105 :发送方将上述非加密集合中的明文数据和上述步骤 S103 中得到的密文数据进行组合后发送给接收方。

[0068] 在具体实施过程中,发送方将非加密集合中的明文数据和密文数据进行组合可以分为以下两种情况 :

[0069] (1) 如果发送方是第一次向接收方发送数据,则发送方根据与接收方协商的初始随机数,采用上述数据组合算法对非加密集合中的明文数据和密文数据进行组合 ;

[0070] (2) 如果发送方不是第一次向接收方发送数据,则发送方根据上一次向接收方发送数据时产生的随机数,采用上述数据组合算法对非加密集合中的明文数据和加密后的密文数据进行组合。

[0071] 具体地,在将上述密文数据和非加密集合中的明文数据进行组合并发送之后,发送方需要根据当前使用的随机数,采用上述随机数序列产生算法产生并保存新的随机数,发送方在下一次向接收方发送数据时,可以首先以该新的随机数为参数,使用数据分组算法将待发送的数据分组为非加密集合和待加密集合,在对待加密集合进行加密后,在发送数据之前,发送方以该新的随机数为参数,使用上述数据组合算法,将加密后的密文数据和非加密集合中的明文数据进行组合。

[0072] 图 2 是根据本发明优选实施例的数据发送方法的详细流程图。如图 2 所示,根据本发明优选实施例的数据发送方法包括以下步骤 (步骤 S201- 步骤 S217) :

[0073] 步骤 S201 :发送方与接收方协商加密方法、密钥、初始随机数、随机数序列产生算法以及随机数使用算法,其中,发送方在发送数据时使用的密钥和随机数与接收方在接收数据时使用的密钥和随机数相同,并且,发送方发送数据时采用的随机数序列产生算法和接收方接收数据时采用的随机数序列产生算法相同 ;

[0074] 其中,上述随机数使用算法包括 :发送方发送数据时使用的上述数据分组算法和上述数据组合算法 ;

[0075] 步骤 S203 :发送方获取待发送的数据 ;

[0076] 步骤 S205 :发送方判断是否是第一次向接收方发送数据,如果是,则执行步骤 S207,否则,执行步骤 S209 ;

[0077] 步骤 S207 :在发送方第一次发送数据的情况下,选择上述协商的初始随机数作为当前使用的随机数 ;

[0078] 步骤 S209 :在发送方不是第一次发送数据的情况下,选择上次发送时存储的随机数作为当前使用的随机数 ;

[0079] 步骤 S211 :根据上述选择的随机数,采用上述随机数使用算法 (即上述的数据分组算法) 结合,对发送的明文数据进行分组,分为待加密集合和非加密集合 ;

[0080] 上述步骤 S201- 步骤 S211 相当于图 1 中的步骤 S101。

[0081] 步骤 S213 :发送方使用上述协商的密钥和加密算法,对待加密集合中的数据进行

加密得到密文；

[0082] 该步骤相当于图 1 中的步骤 S103。

[0083] 步骤 S215：根据上述选择的随机数采用随机数使用算法（即上述数据组合算法）对上述加密得到的密文和非加密集合中的明文进行组合，得到一个数据报文并发送；

[0084] 步骤 S217：根据当前使用的随机数采用随机数序列产生算法产生新的随机数，并保存等待下一次发送时使用。

[0085] 步骤 S215 和步骤 S217 相当于图 1 中的步骤 S105。

[0086] 根据本发明实施例提供的上述数据发送方法，可以在发送数据前，对待发送的数据进行部分加密，从而减少了数据加密时消耗的系统资源。

[0087] 根据本发明实施例，还提供了一种数据接收方法。

[0088] 图 3 是根据本发明实施例的数据接收方法的流程图。如图 3 所示，根据本发明实施例的数据接收方法包括主要包括以下步骤（步骤 S301- 步骤 S305）：

[0089] 步骤 S301：接收方将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合；

[0090] 在具体实施过程中，在执行步骤 S301 之前，发送方与接收方需要进行协商，以确定预设的解密算法、对密文数据进行解密时使用的密钥（与上述发送方加密数据时使用的密钥相同）、初始随机数、随机数序列产生算法、数据分组算法、数据组合算法，其中，数据分组算法（与上述发送方发送数据前使用的数据组合算法互为可逆）用于根据随机数对接收到的数据进行分组，数据组合算法（与上述发送方发送数据前使用的数据分组算法互为可逆）用于根据随机数对解密得到的明文数据与非解密集合中的明文数据进行组合。

[0091] 具体地，接收方将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合分为以下两种情况：

[0092] (1) 如果接收方是第一次接收发送方发送的数据，则接收方以上述初始随机数为参数，使用数据分组算法将接收到的数据分组为待解密集合和非解密集合。

[0093] (2) 如果接收方不是第一次接收发送方发送的数据，则接收方以上一次接收来自发送方的数据时产生的新的随机数为参数，采用上述协商的数据分组算法将接收到的数据分组为待解密集合和非解密集合，其中，待解密集合中的数据为密文数据，非解密集合中的数据为明文数据。

[0094] 步骤 S303：按照预设的解密算法对待解密集合中的密文数据进行解密得到明文数据；

[0095] 在具体实施过程中，接收方根据上述协商的密钥采用解密算法，对待解密集合中的密文数据进行解密得到明文数据。

[0096] 步骤 S305：接收方将解密得到的明文数据与非解密集合中的明文数据进行组合。

[0097] 在具体实施过程中，接收方将解密得到的明文数据与非解密集合中的明文数据进行组合可以分为以下两种情况：

[0098] (1) 如果接收方是第一次接收来自发送方的数据，则接收方以上述初始随机数为参数，采用步骤 S301 中协商的数据组合算法将解密得到的明文数据与非解密集合中的明文数据进行组合。

[0099] (2) 如果接收方不是第一次接收来自发送方的数据，则接收方以上一次接收来自

发送方的数据时产生的新的随机数为参数，采用步骤 S301 中协商的数据组合算法将解密得到的明文数据与非解密集合中的明文数据进行组合。

[0100] 在具体实施过程中，将非解密集合中的明文数据和解密得到的明文数据进行组合之后，接收方需要根据当前使用的随机数，采用上述协商的随机数序列产生算法产生并保存新的随机数，其中，该随机数可以在接收方下一次接收来自发送方的数据时，对接收到的数据进行分组，以及对解密后的数据进行组合。

[0101] 图 4 是根据本发明优选实施例的数据接收方法的详细流程图。如图 4 所示，根据本发明优选实施例的数据接收方法包括以下步骤（步骤 S401- 步骤 S417）：

[0102] 步骤 S401：发送方与接收方协商解密方法、密钥、初始随机数、随机数序列产生算法、数据分组算法和数据组合算法；

[0103] 步骤 S403：接收方接收发送方发送的数据报文；

[0104] 步骤 S405：判断是否是第一次解密来自发送方的数据，如果是，则执行步骤 S407，否则，执行步骤 S409；

[0105] 步骤 S407：在接收方第一次解密数据的情况下，选择协商的初始随机数作为当前使用的随机数；

[0106] 步骤 S409：在接收方不是第一次解密数据的情况下，选择上次解密来自发送方的数据时产生的随机数作为当前使用的随机数；

[0107] 步骤 S411：将以上述选择的随机数为参数，采用步骤 S401 中协商的数据分组算法对接收到的数据进行分组，将数据分为待解密集合和非解密集合，其中，待解密集合中包含的数据为密文数据，非解密集合中包含的数据为明文数据，并且，该分组过程与发送方发送数据时的组合过程互为逆过程，即采用步骤 S411 中使用数据分组算法与图 2 中发送数据时的组合过程中采用的数据组合算法相对应；

[0108] 上述步骤 S401- 步骤 S413 相当于图 3 中的步骤 S301。

[0109] 步骤 S413：使用上述协商的密钥，采用上述协商的解密算法对待解密集合进行解密得到明文数据；

[0110] 步骤 S413 相当于图 3 中的步骤 S303。

[0111] 步骤 S415：以上述选择的随机数为参数，采用步骤 S401 中协商的数据组合算法，对上述解密得到的明文数据和非解密集合的密文数据进行组合，得到一个数据报文并提交，其中，此组合过程与发送数据时的分组过程互为逆过程，即步骤 S415 中使用的数据组合算法与图 2 中发送数据的分组过程中采用的数据分组算法相对应；

[0112] 步骤 S417：以当前使用的随机数为参数，使用步骤 S401 中协商的随机数序列产生算法产生新的随机数，并保存等待下一次解密时使用。

[0113] 上述步骤 S415 和步骤 S417 相当于图 3 中的步骤 S305。

[0114] 根据本发明实施例的上述数据接收方法，可以减少数据解密过程中消耗的系统资源。

[0115] 本发明实施例提供的上述数据发送方法和数据接收方法可以结合使用，下面对上述数据发送方法和数据接收方法结合使用进行说明。

[0116] 图 5 是根据本发明实施例的发送和接收方法相结合过程中数据报文的示意图。如图 5 所示，分别示出了第 N 次、第 N+1 次、第 N+2 次（不仅限于此，其他次数发送及接收过

程中的报文形式未示出）发送及接收的数据报文形式，其中，将发送前为加密的数据报文（即，明文数据）分为待加密集合和非加密集合，对待加密集合中的数据报文进行加密（即，图中阴影部分数据报文），并将加密后的数据报文与非加密集合中的数据报文进行组合后发送，接收方接收到上述数据后，对接收到的数据进行分组，将接收到的数据分为待解密集合和非解密集合，其中，待解密集合中的数据为密文数据，非解密集合中的数据为明文数据。然后，接收方将待解密集合中的数据报文进行解密，并将解密后的数据报文与非解密集合中的数据报文进行组合，得到发送方发送的完整的数据报文。

[0117] 根据本发明实施例，还提供了一种数据传输方法。

[0118] 图 6 是根据本发明实施例的数据传输方法的流程图。如图 6 所示，根据本发明实施例的数据传输方法包括以下步骤（步骤 S601- 步骤 603）：

[0119] 步骤 S601：发送方将待发送的明文数据分组为待加密集合和非加密集合，并根据预设的密钥，采用预设的加密算法对待加密集合中的明文数据进行加密得到密文数据，再将该密文数据和非加密集合中的明文数据进行组合后发送给接收方；

[0120] 步骤 S603：接收方将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合，并根据上述密钥，采用预设的解密算法对待解密集合中的密文数据进行解密得到明文数据，再将解密得到的明文数据与非解密集合中的明文数据进行组合。

[0121] 在具体实施过程，发送方向接收方发送数据时，首先与接收方进行协商，具体地，发送方与接收方进行协商确定的参数包括：上述的加密算法和解密算法、预设的密钥（发送方加密时使用的密钥和接收方解密时使用的密钥相同）、随机数（发送方发送数据时使用的随机数与接收方接收数据时使用的随机数相同）、随机数序列产生算法（发送方和接收方采用的随机数序列产生算法相同）、第一数据分组算法（即发送方发送数据时采用的数据分组算法）、第一数据组合算法（即发送方发送数据时采用的数据组合算法）、第二数据分组算法（即接收方接收数据时采用的数据分组算法）和第二数据组合算法（即接收方接收数据时采用的数据组合算法），其中，第一数据分组算法用于发送方根据随机数对待发送的明文数据进行分组，第一数据组合算法用于发送方根据随机数对密文数据和非加密集合中的明文数据进行组合，第二数据分组算法用于接收方根据随机数对接收到的数据进行分组，第二数据组合算法用于接收方根据随机数对解密得到的明文数据与非解密集合中的明文数据进行组合，并且，第一数据组合算法与第二数据分组算法互为可逆，第一数据分组算法与第二数据组合算法互为可逆。

[0122] 图 7 是根据本发明实施例的数据传输方法的详细流程图。如图 7 所示，根据本发明实施例的数据传输方法主要包括以下步骤（步骤 S701- 步骤 S737）：

[0123] 步骤 S701：发送方与接收方协商加 / 解密算法，加 / 解密密钥，初始随机数 R0，确定随机数使用方法 X（包括：上述步骤 S201 中协商的数据分组算法 X1 和数据组合算法 X2，以及上述步骤 S401 中协商的数据组合算法 X3 和数据组合算法 X4）和随机数序列产生算法 Y；

[0124] 步骤 S703：获取待发送数据 (a1，a2，a3，a4，a5，a6，a7，a8，a9，a10)；

[0125] 步骤 S705：选择初始随机数 R0；

[0126] 步骤 S707：以初始随机数 R0 为参数采用随机数使用方法 X（数据分组算法 X1）对待发送数据进行分组，将待发送数据分为待加密集合：(a1，a3，a4，a5，a7，a9，a10)，以及非

加密集合：(a2，a6，a8)；

[0127] 步骤 S709：以协商的密钥的参数，采用协商的加密算法对待加密集合中的数据进行加密，以初始随机数为参数，采用数据组合算法 X2 将加密得到的密文数据与非加密集合的明文数据进行组合得到以下集合：(A1，a2，A3，A4，A5，a6，A7，a8，A9，A10)，并将组合后的集合发送给接收方；

[0128] 步骤 S711：以初始随机数 R0 为参数采用随机数序列产生算法 Y 方法产生随机数 R1，并保存；

[0129] 步骤 S713：接收方接收到来自发送方的数据集合：(A1，a2，A3，A4，A5，a6，A7，a8，A9，A10)，当前为第一次解密来自发送方的数据，因此，选择随机数为 R0；

[0130] 步骤 S715：以初始随机数 R0 为参数，采用数据分组算法 X3 将接收到的数据分组为待解密集合：(A1，A3，A4，A5，A7，A9，A10) 和非解密集合：(a2，a6，a8)；

[0131] 步骤 S717：对待解密集合进行解密，并以初始随机数 R0 为参数，采用数据组合算法 X4 对解密得到的明文数据和非解密集合中的明文数据进行重组，得到明文数据：(a1，a2，a3，a4，a5，a6，a7，a8，a9，a10)；

[0132] 步骤 S719：以初始随机数 R0 为参数，采用随机数序列产生算法 Y 产生新的随机数 R1，并保存；

[0133] 上述步骤 S701 到步骤 S719 为发送方与接收方之间的第一次数据传输，下面为发送方与接收方之间的第二次数据传输过程。

[0134] 步骤 S721：发送方获取待发送数据为以下集合 (b1，b2，b3，b4，b5，b6，b7，b8，b9，b10，b11，b12，b7)；

[0135] 步骤 S723：选择上次保存随机数 R1；

[0136] 步骤 S725：以随机数 R1 为参数，采用数据分组算法 X1 将待发送数据分组为待加密集合：(b2，b3，b4，b6，b7，b10，b11，b12，b7)，以及非加密集合：(b1，b5，b8，b9)；

[0137] 步骤 S727：对待加密集合加密，以随机数 R1 为参数，采用数据组合算法 X2 对加密得到的数据与非加密集合中的数据进行重组得到以下集合：(b1，B2，B3，B4，b5，B6，B7，b8，b9，B10，B11，B12，B13)，并将该集合发送给接收方；

[0138] 步骤 S729：发送方以随机数 R1 为参数，采用随机数序列产生算法 Y 产生得到新的随机数 R2，并保存；

[0139] 步骤 S731：接收方接收来自发送方的数据：(b1，B2，B3，B4，b5，B6，B7，b8，b9，B10，B11，B12，B13)，选择上次保存的随机数 R1；

[0140] 步骤 S733：以随机数 R1 为参数，采用数据分组算法 X3 将接收到的数据分组为待解密集合：(B2，B3，B4，B6，B7，B10，B11，B12，B13)，非解密集合：(b1，b5，b8，b9)；

[0141] 步骤 S735：接收方对待解密集合解密，并以随机数 R1 为参数，采用数据分组算法 X4 对解密后的待解密集合和非解密集合进行组合，得到明文数据：(b1，b2，b3，b4，b5，b6，b7，b8，b9，b10，b11，b12，b13)；

[0142] 步骤 S737：接收方以随机数 R1 为参数，采用随机数序列产生算法 Y 产生得到新的随机数 R2，并保存。

[0143] 对于发送方与接收方后续的数据传输，其过程与上述第二次数据传输过程相似，再此不再赘述。

[0144] 通过上述实施例，发送方在发送通信信息时对待发送的数据进行分组，对待加密部分进行加密，而不是对全部通信信息进行加密；接收方在接收到通信信息后进行分组，对待解密部分进行解密，无需对全部通信信息进行解密，从而节省了大量系统计算资源。

[0145] 装置实施例

[0146] 根据本发明实施例，还提供了一种数据发送装置。

[0147] 图 8 是根据本发明实施例的数据发送装置示意图，图 9 是根据本发明优选实施例的数据发送装置示意图。如图 8 所示，根据本发明实施例的数据发送装置包括：分组器 80、加密模块 84、组合器 82 和发送模块 86。其中，分组器 80，用于将待发送的明文数据分为待加密集合和非加密集合；加密模块 84，与分组器 80 相连接，用于按照预设的加密算法对待加密集合中的明文数据进行加密得到密文数据；组合器 82，与加密模块 84 和分组器 80 相连接，用于将加密模块 84 得到的密文数据和非加密集合中的明文数据进行组合；发送模块 86，与组合器 82 相连接，用于将组合器 82 组合后的数据和发送给接收方。

[0148] 进一步地，如图 9 所示，根据本发明优选实施例的数据发送装置还可以包括：第一存储模块 81，和 / 或，随机数产生器 83 和第二存储模块 85。其中，第一存储模块 81，用于保存与接收方协商确定的预设的加密算法、对明文数据进行加密时使用的密钥、随机数、随机数序列产生算法、数据分组算法和数据组合算法，其中，数据分组算法用于分组器 80 根据随机数对待发送的明文数据进行分组，数据组合算法用于组合器 82 对加密模块 84 加密得到的密文数据和非加密集合中的明文数据进行组合；随机数产生器 83，与第一存储模块 81 和组合器 80 相连接，用于以数据分组算法和数据组合算法当前使用的随机数为参数，根据上述随机数序列产生算法产生新的随机数；第二存储模块 85，与随机数产生器 83 相连接，用于存储随机数产生器 83 产生的新的随机数；则上述分组器 80 还用于在下一次向接收方发送数据时，根据新的随机数使用数据分组算法对待发送的明文数据进行数据分组；上述组合器 82 还用于在下一次向接收方发送数据时，根据新的随机数使用数据组合算法对非加密集合中的明文数据和被加密模块 84 加密后的密文数据进行组合。

[0149] 图 10 是根据本发明另一优选实施例的数据发送装置示意图。如图 10 所示，本实例的数据发送装置的主要包括：随机数产生器 91、分组器 93、组合器 95、加密模块 97、发送模块 99。其中，随机数产生器 91 用于根据初始随机数或者当前分组使用的随机数采用随机数序列产生算法产生一个新的随机数，将该新随机数分别提供给分组器 93 和组合器 95，以及反馈至该随机数产生器 91 以使下一次发送数据时使用，分组器 93 和组合器 95 根据输入的随机数对待处理数据分别进行分组和组合。发送的明文数据经由分组器 93 分组为待加密集合和非加密集合后，待加密集合的数据经过加密模块 97 进行加密得到已加密数据，该已加密数据和非加密集合的数据经过组合器 95 进行组合得到密文数据，该密文数据经过发送模块 99 发送给接收方。

[0150] 通过本发明实施例提供的上述数据发送装置，可以在发送通信信息时对待发送信息的部分进行加密，无需对全部通信信息进行加密，节省了大量系统计算资源。

[0151] 根据本发明实施例，还提供了一种数据接收装置，该数据接收装置可以与图 8、9 和 10 中的数据发送装置结合使用。

[0152] 图 11 是根据本发明实施例的数据接收装置示意图。如图 11 所示，根据本发明实施例的数据接收装置包括：分组器 110、组合器 112、解密模块 114 以及接收模块 116，其中，接

收模块 116，用于接收来自发送方的数据；分组器 110，与接收模块 116 相连接，用于将接收到的数据分组为待解密集合和非解密集合，其中，待解密集合中的数据为密文数据，非解密集合中的数据为明文数据；解密模块 114，与分组器 110 相连接，用于按照预设的解密算法将待解密集合中的密文数据进行解密得到明文数据；组合器 112，与解密模块 114 相连接，用于将非解密集合中的明文数据和解密后得到的明文数据进行组合。

[0153] 图 12 是根据本发明优选实施例的数据接收装置示意图。如图 12 所示，根据本发明优选实施例的数据接收装置还可以包括：第一存储模块 111、随机数产生器 113、第二存储模块 115。其中，第一存储模块 111，用于保存与发送方协商确定的预设解密算法、对密文数据进行解密时使用的密钥、随机数、随机数序列产生算法、数据分组算法和数据组合算法；分组器 110 可以根据该数据分组算法和随机数对接收模块 116 接收到的数据进行分组，并且，组合器 110 还可以根据该数据组合算法和随机数对解密得到的明文数据和非解密集合中的明文数据进行组合；随机数产生器 113，与分组器 110 和组合器 112 相连接，用于根据当前分组接收到的密文数据时使用的随机数和随机数序列产生算法产生新的随机数。第二存储模块 115，与随机数产生器 113 相连接，用于存储随机数产生器 113 产生的新的随机数。

[0154] 进一步地，上述分组器 110 还用于在下一次接收发送方发送的数据时，根据上述新的随机数采用上述数据分组算法对接收到的数据进行数据分组；上述组合器 112 还用于在下一次接收发送方发送的数据时，根据上述新的随机数采用上述数据组合算法对解密得到的明文数据和非解密集合中的明文数据进行组合。

[0155] 图 13 是根据本发明另一优选实施例的数据接收装置示意图。如图 13 所示，本实例的数据接收装置的主要包括：随机数产生器 131、分组器 133、组合器 135、解密模块 136、接收模块 139。其中，随机数产生器 131 用于根据初始随机数或者当前分组使用的随机数结合随机数序列产生算法产生一个新的随机数，将该新随机数分别提供给分组器 133 和组合器 135，并反馈至该随机数产生器 131。分组器 133 和组合器 135 分别以输入的随机数为参数，使用数据分组算法和数据组合算法对待处理数据进行分组和组合，接收的密文数据经由分组器 133 分组为待解密集合和非解密集合，其中，待加密集合的数据经过解密模块 136 进行解密得到已解密数据，该已解密数据和非解密集合的数据经过组合器 135 进行组合得到明文数据。

[0156] 通过上述实施例提供的上述接收装置，可以对接收到的数据的部分进行解密，无需对全部通信信息进行解密，节省了大量系统计算资源。

[0157] 根据本发明实施例，还提供了一种数据传输系统。

[0158] 图 14 为根据本发明实施例的数据传输系统示意图。如图 14 所示，根据本发明实施例的数据传输装置包括：发送装置 1 和接收装置 3。其中，发送装置 1 可以为上述图 8 中的数据发送装置，接收装置 3 可以为上述图 11 中的数据接收装置。

[0159] 其中，发送装置 1 可以包括：第一分组器 11，用于将待发送的明文数据分为待加密集合和非加密集合；加密模块 13，与第一分组器 11 相连接，用于按照预设的加密算法对待加密集合中的明文数据进行加密得到密文数据；第一组合器 17，与加密模块 13 连接，用于将非加密集合中的明文数据和加密模块 13 加密后的密文数据进行组合；发送模块 15，与第一组合器 17 连接，用于将第一组合器 17 组合得到的数据发送给接收装置 3；

[0160] 进一步地，发送装置 1 还可以包括 ：第一存储模块 19，用于保存与接收装置 3 协商确定的预设的加密算法、对明文数据进行加密时使用的密钥、随机数、随机数序列产生算法、第一数据分组算法和第一数据组合算法，其中，第一数据分组算法用于第一分组器 11 根据随机数对待发送的明文数据进行分组，第一数据组合算法用于第一组合器 17 对密文数据和非加密集合中的明文数据进行组合 ；

[0161] 接收装置 3 包括 ：接收模块 31，用于接收来自发送装置 1 的数据 ；第二分组器 33，用于将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合 ；解密模块 35，与第二分组器 33 相连接，用于按照预设的解密算法将待解密集合中的密文数据进行解密得到明文数据 ；第二组合器 37，与解密模块 35 相连接，用于将解密模块 35 解密得到的明文数据和非解密集合中的明文数据进行组合。

[0162] 进一步地，上述接收装置还包括 ：第二存储模块 37，用于保存与发送装置 1 协商确定的预设解密算法、对密文数据进行解密时使用的密钥、随机数、随机数序列产生算法、第二数据分组算法和第二数据组合算法，其中，第二数据分组算法用于第二分组器 33 根据随机数对接收模块接收到的数据进行分组，第二数据组合算法用于第二组合器 37 根据随机数对解密得到的明文数据和非解密集合中的明文数据进行组合，并且，第一数据组合算法与第二数据分组算法互为可逆，第一数据分组算法与第二数据组合算法互为可逆。

[0163] 综上所述，通过本发明的上述实施例，发送方在发送通信信息时，对信息进行随机分组，再利用密钥和加密算法对分组后的随机部分进行加密，之后将上述加密的随机部分与非加密部分组合后进行发送 ；接收方在接收到通信信息时，对信息进行随机分组，再利用密钥和解密算法对分组后的随机部分进行解密，之后将上述解密的随机部分与非解密部分组合后进行提交，解决了相关技术中使用加密和解密算法时需要消耗较多系统计算资源的问题，节省了大量系统计算资源，便于大量通信数据在网络中的安全传输，进而降低了传输数据开销。

[0164] 显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0165] 以上仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

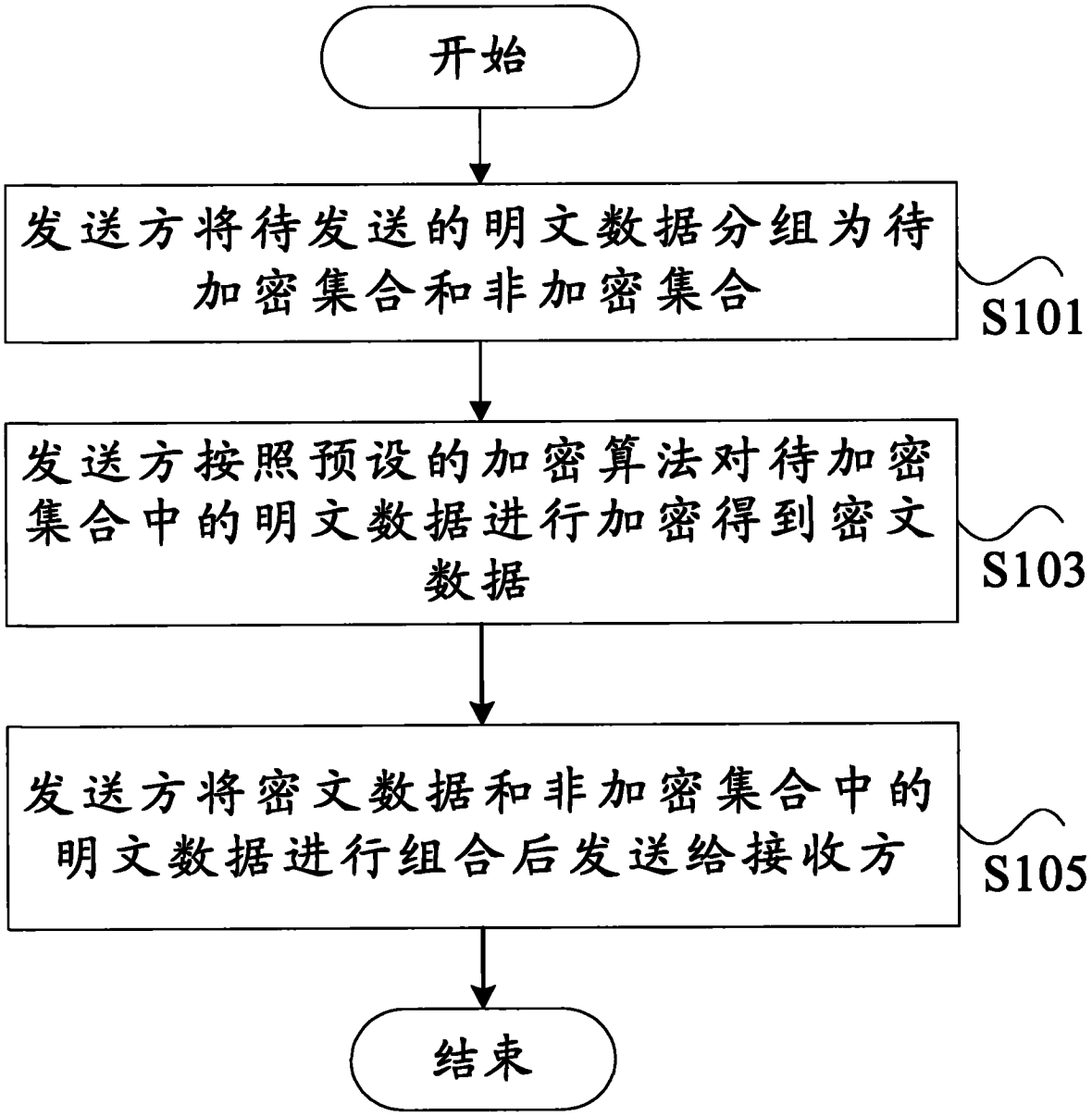

开始
发送方将待发送的明文数据分组为待加密集合和非加密集合
S101
发送方按照预设的加密算法对待加密集合中的明文数据进行加密得到密文数据
S103
发送方将密文数据和非加密集合中的明文数据进行组合后发送给接收方
S105
结束

图 1

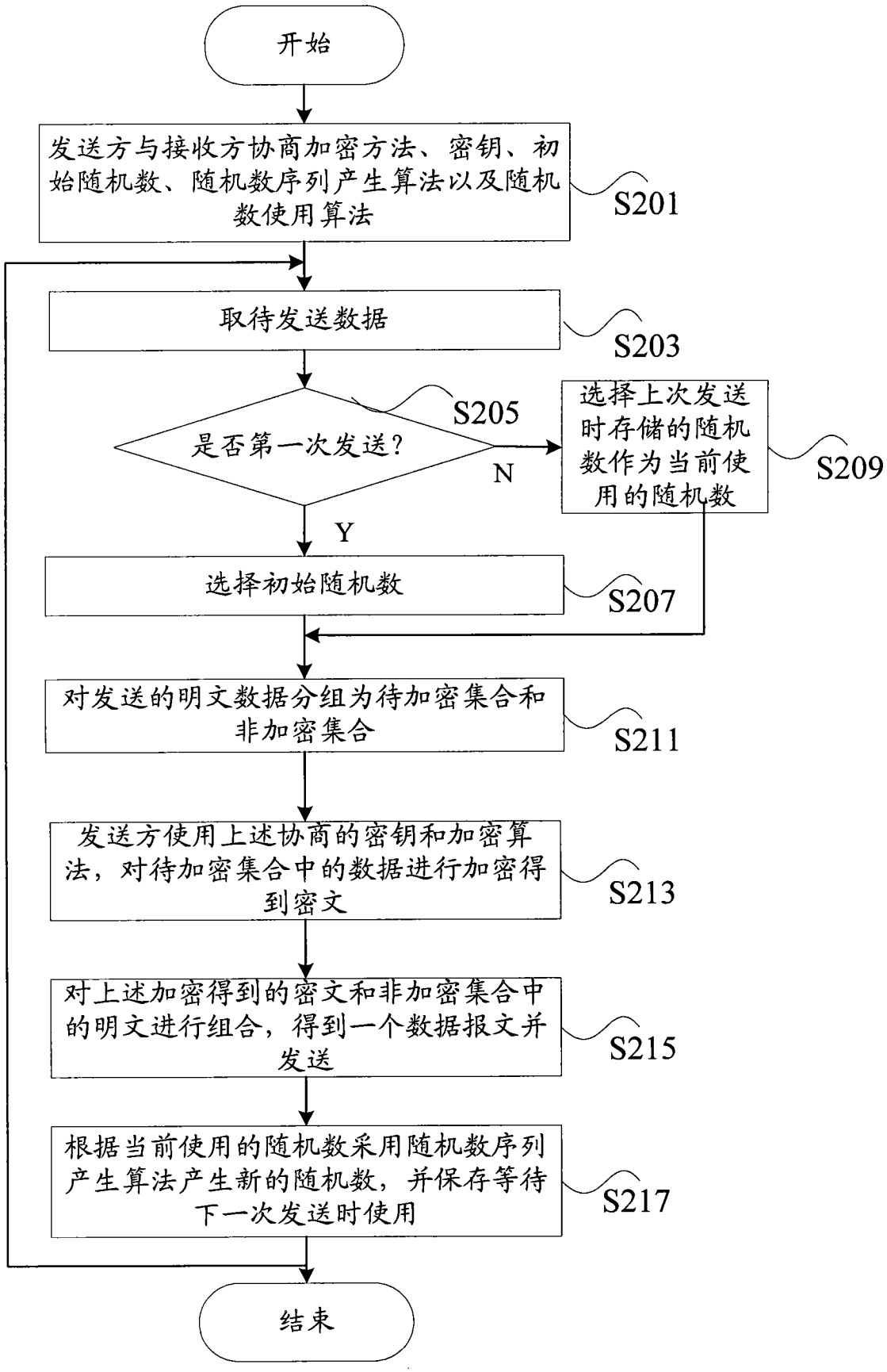

开始
发送方与接收方协商加密方法、密钥、初始随机数、随机数序列产生算法以及随机数使用算法
S201
取待发送数据
S203
是否第一次发送?
S205
N
选择上次发送时存储的随机数作为当前使用的随机数
S209
Y
选择初始随机数
S207
对发送的明文数据分组为待加密集合和非加密集合
S211
发送方使用上述协商的密钥和加密算法，对待加密集合中的数据进行加密得到密文
S213
对上述加密得到的密文和非加密集合中的明文进行组合，得到一个数据报文并发送
S215
根据当前使用的随机数采用随机数序列产生算法产生新的随机数，并保存等待下一次发送时使用
S217
结束

图 2

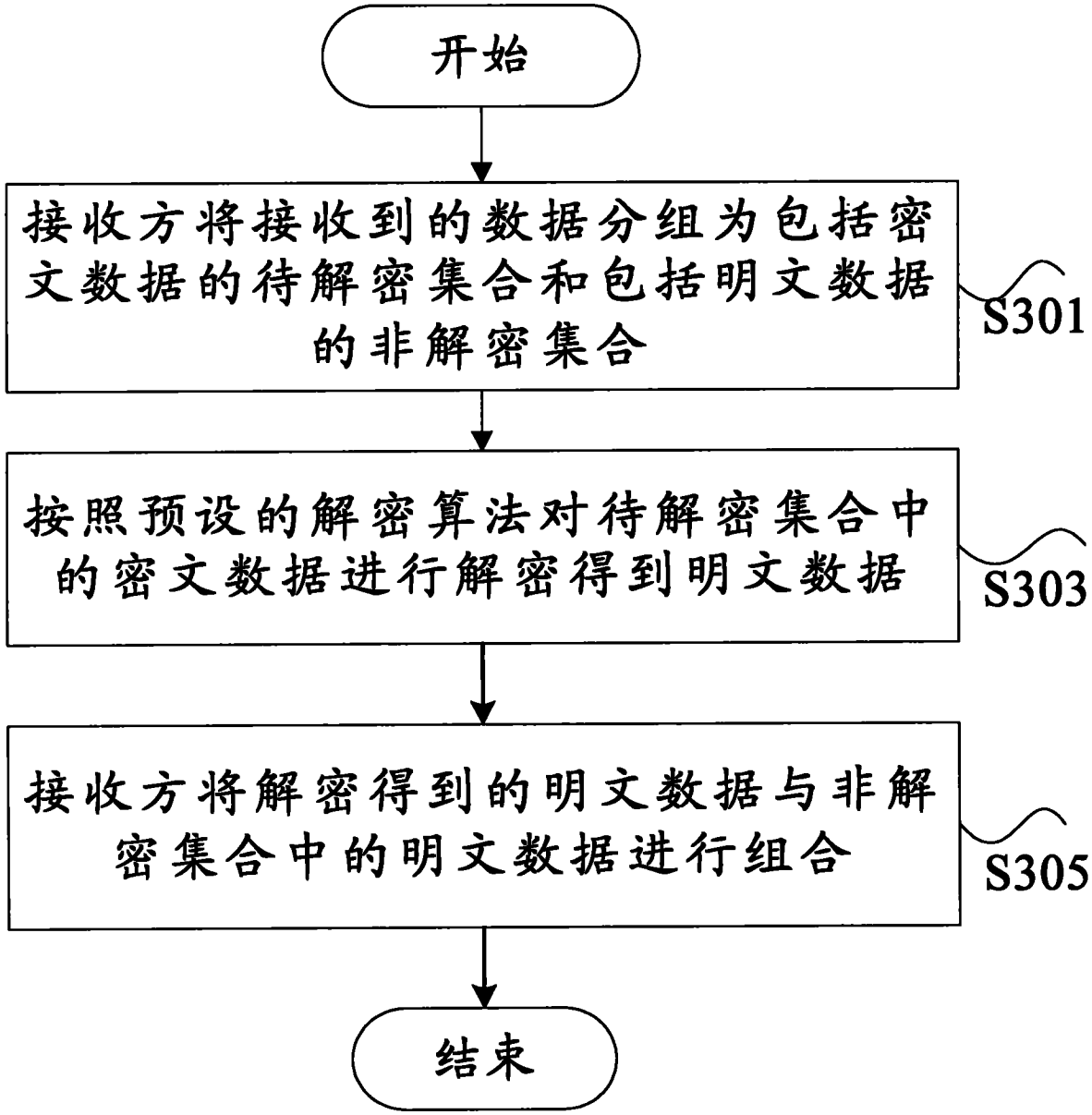

开始
接收方将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合
S301
按照预设的解密算法对待解密集合中的密文数据进行解密得到明文数据
S303
接收方将解密得到的明文数据与非解密集合中的明文数据进行组合
S305
结束

图 3

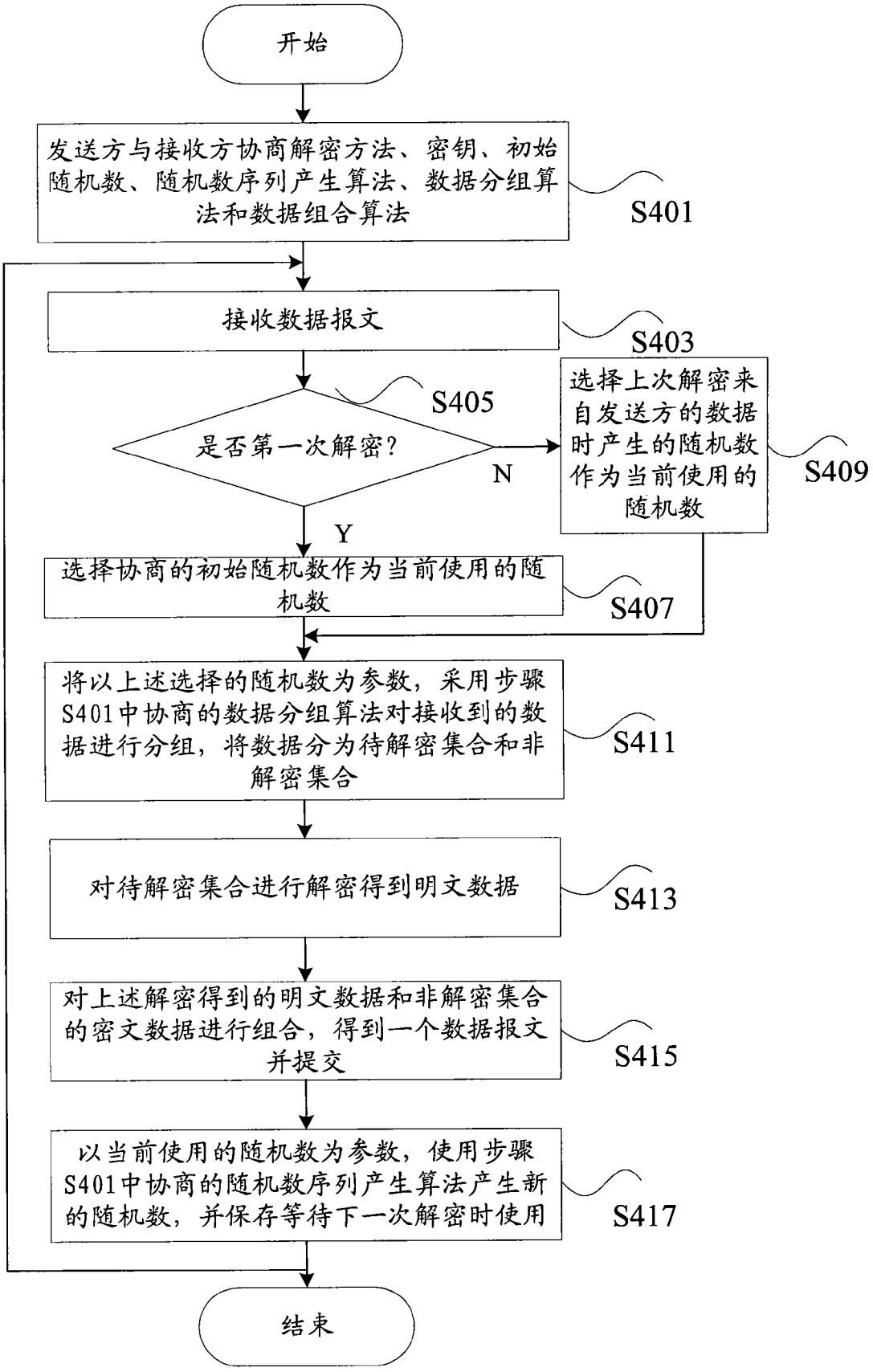

开始
发送方与接收方协商解密方法、密钥、初始随机数、随机数序列产生算法、数据分组算法和数据组合算法
S401
接收数据报文
S403
S405
是否第一次解密?
N
Y
选择上次解密来自发送方的数据时产生的随机数作为当前使用的随机数
S409
选择协商的初始随机数作为当前使用的随机数
S407
将以上述选择的随机数为参数，采用步骤S401中协商的数据分组算法对接收到的数据进行分组，将数据分为待解密集合和非解密集合
S411
对待解密集合进行解密得到明文数据
S413
对上述解密得到的明文数据和非解密集合的密文数据进行组合，得到一个数据报文并提交
S415
以当前使用的随机数为参数，使用步骤S401中协商的随机数序列产生算法产生新的随机数，并保存等待下一次解密时使用
S417
结束

图 4

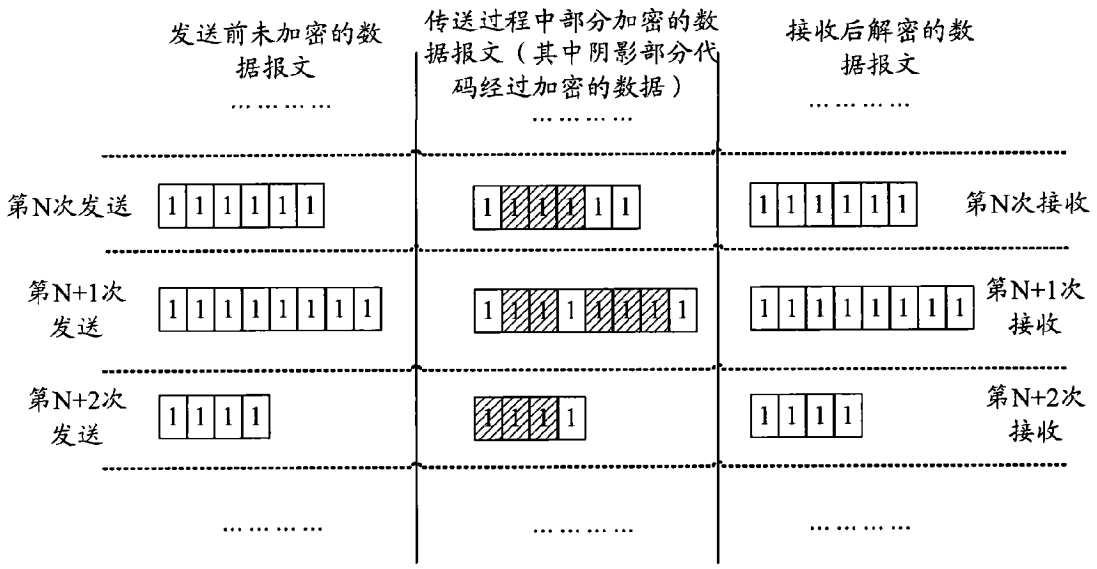

发送前未加密的数据报文
……
传送过程中部分加密的数据报文（其中阴影部分代码经过加密的数据）
……
接收后解密的数据报文
……
第N次发送
第N次接收
第N+1次发送
第N+1次接收
第N+2次发送
第N+2次接收

图 5

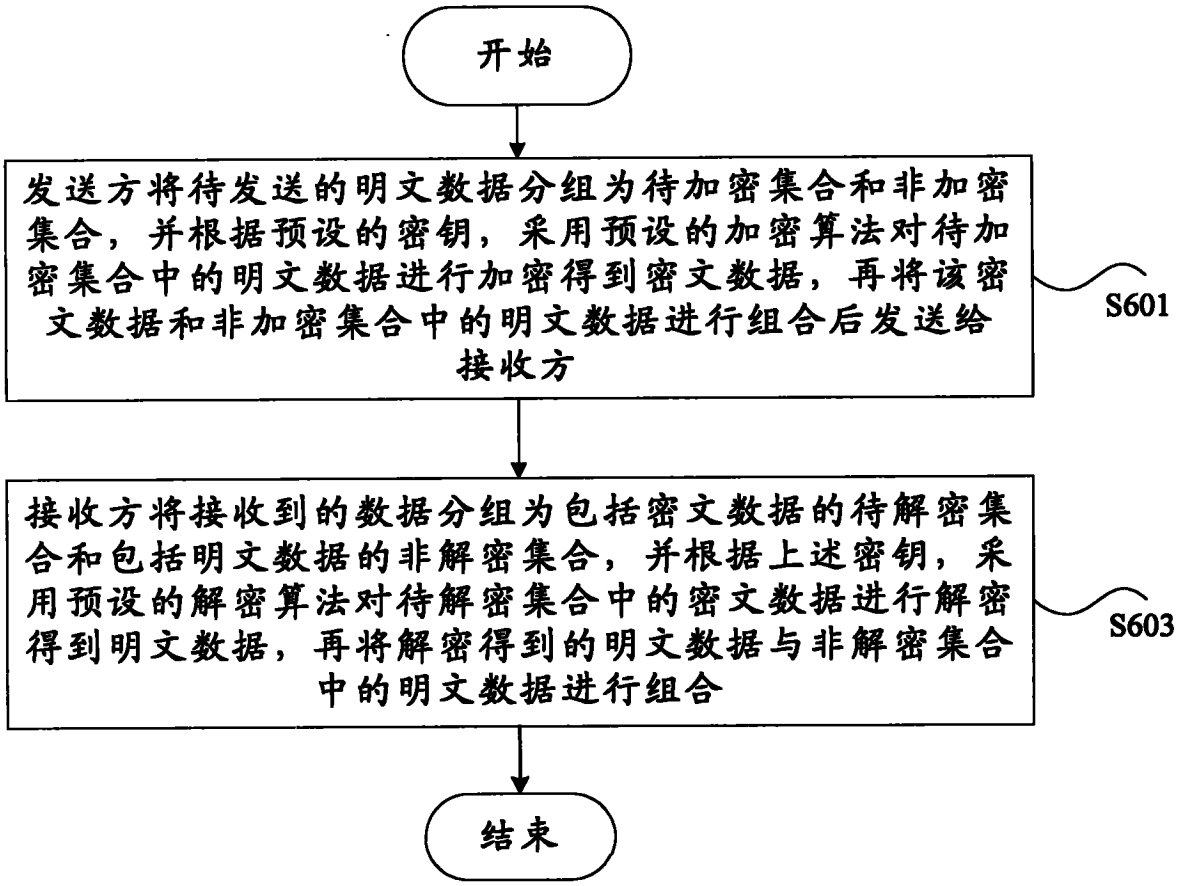

开始
发送方将待发送的明文数据分组为待加密集合和非加密集合，并根据预设的密钥，采用预设的加密算法对待加密集合中的明文数据进行加密得到密文数据，再将该密文数据和非加密集合中的明文数据进行组合后发送给接收方
S601
接收方将接收到的数据分组为包括密文数据的待解密集合和包括明文数据的非解密集合，并根据上述密钥，采用预设的解密算法对待解密集合中的密文数据进行解密得到明文数据，再将解密得到的明文数据与非解密集合中的明文数据进行组合
S603
结束

图 6

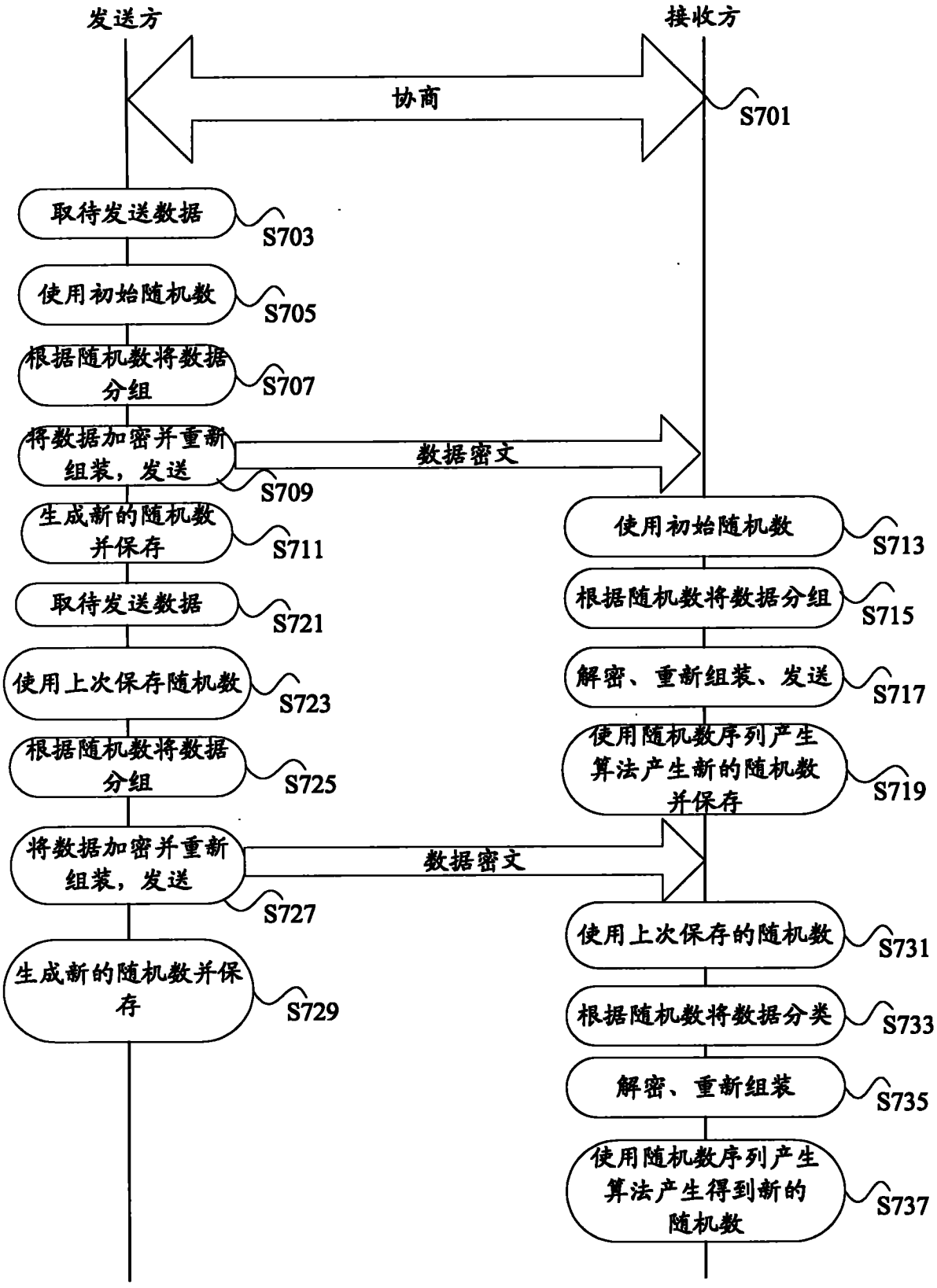

发送方
接收方
协商
S701
取待发送数据
S703
使用初始随机数
S705
根据随机数将数据分组
S707
将数据加密并重新组装，发送
数据密文
S709
生成新的随机数并保存
S711
使用初始随机数
S713
取待发送数据
S721
根据随机数将数据分组
S715
使用上次保存随机数
S723
解密、重新组装、发送
S717
根据随机数将数据分组
S725
使用随机数序列产生算法产生新的随机数并保存
S719
将数据加密并重新组装，发送
数据密文
S727
使用上次保存的随机数
S731
生成新的随机数并保存
S729
根据随机数将数据分类
S733
解密、重新组装
S735
使用随机数序列产生算法产生得到新的随机数
S737

图 7

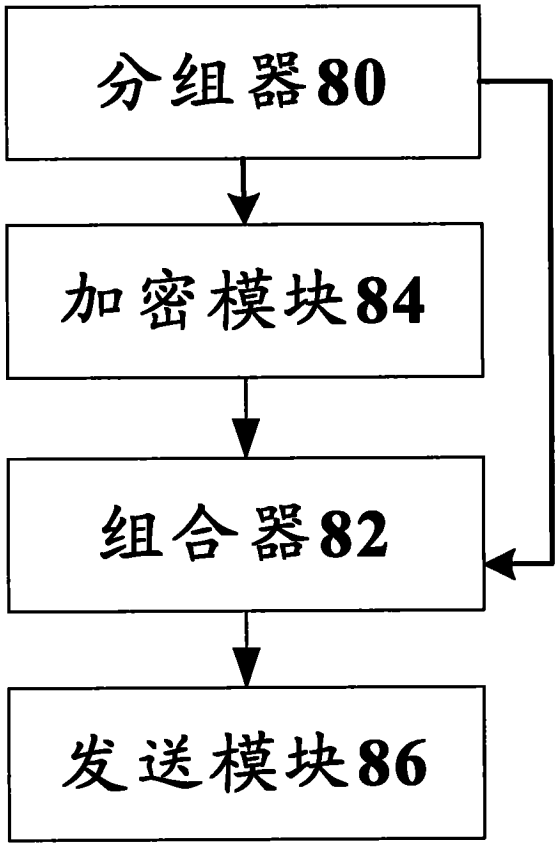


图 8

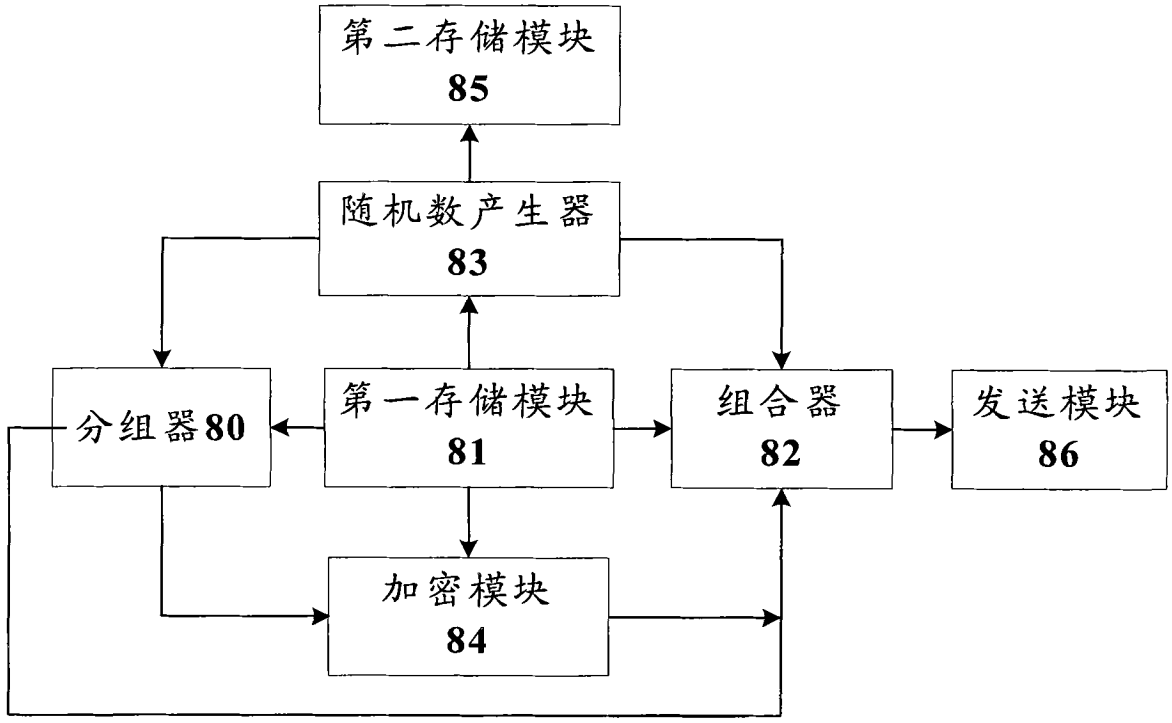

第二存储模块
85
随机数产生器
83
分组器80
第一存储模块
81
组合器
82
发送模块
86
加密模块
84

图 9

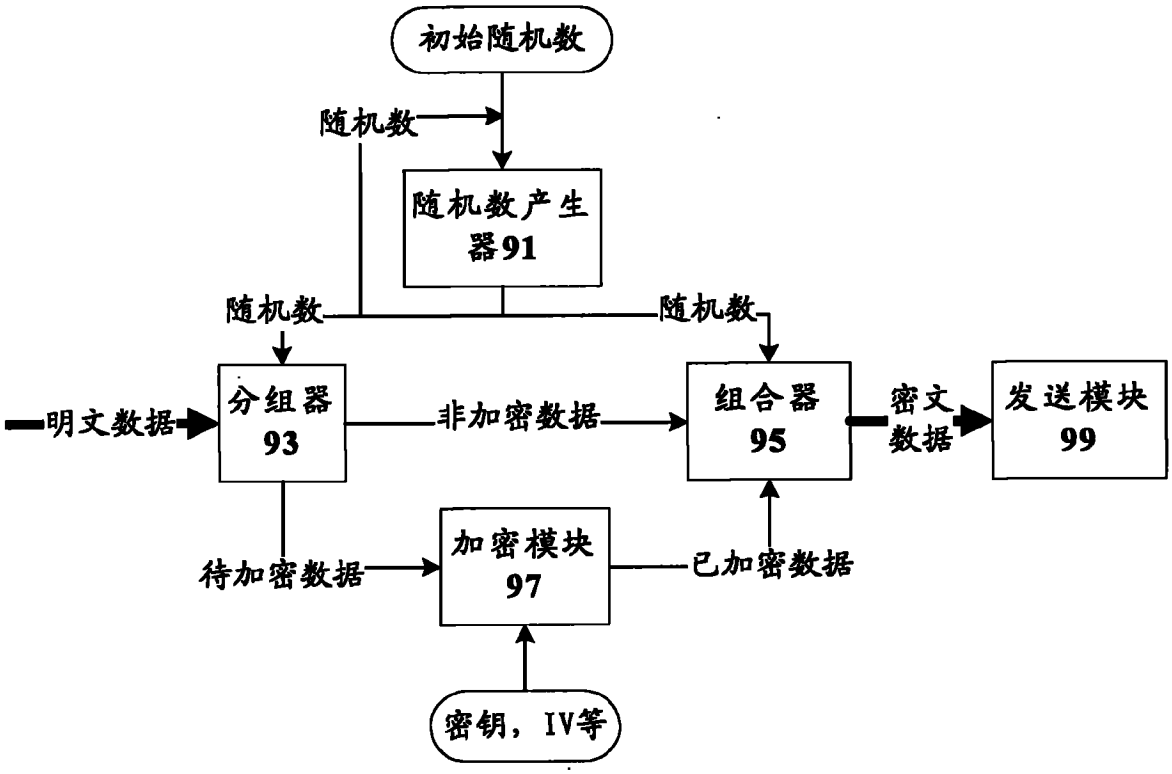

初始随机数
随机数
随机数产生
器91
随机数
随机数
明文数据
分组器
93
非加密数据
组合器
95
密文
数据
发送模块
99
待加密数据
加密模块
97
已加密数据
密钥，IV等

图 10

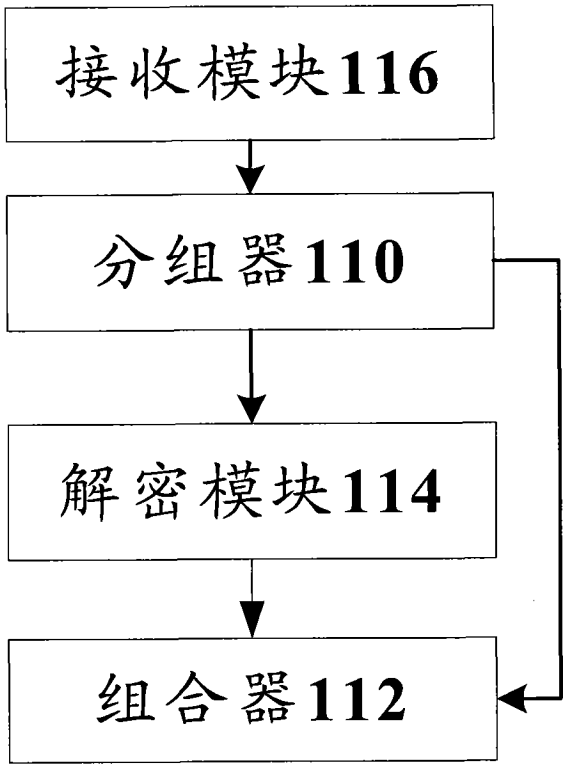

接收模块116
分组器110
解密模块114
组合器112

图 11

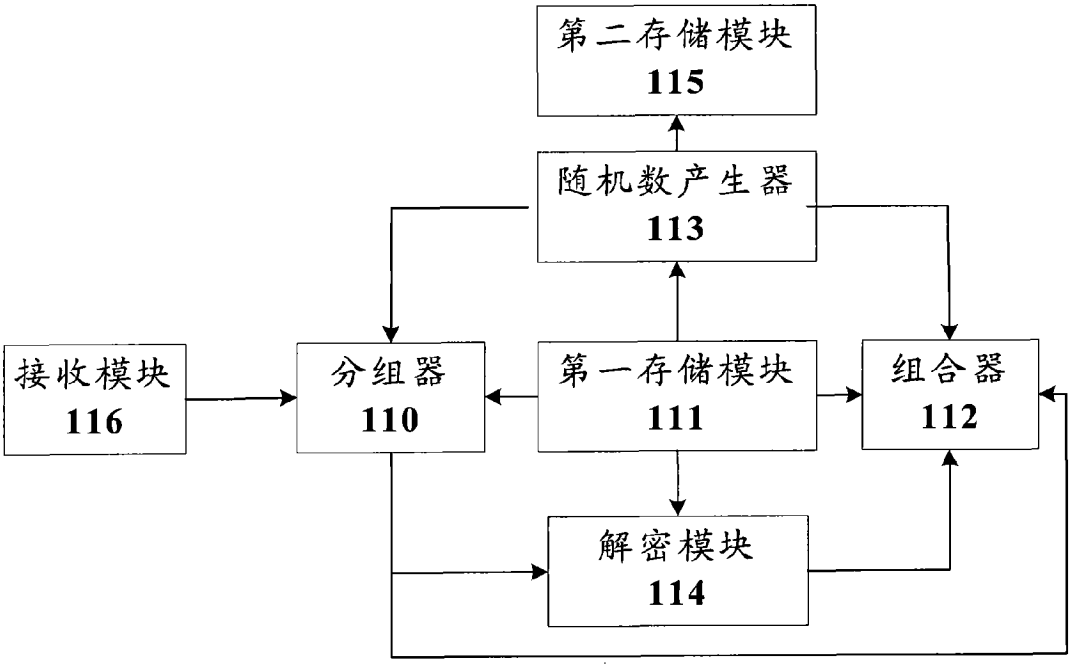

第二存储模块
115
随机数产生器
113
接收模块
116
分组器
110
第一存储模块
111
组合器
112
解密模块
114

图 12

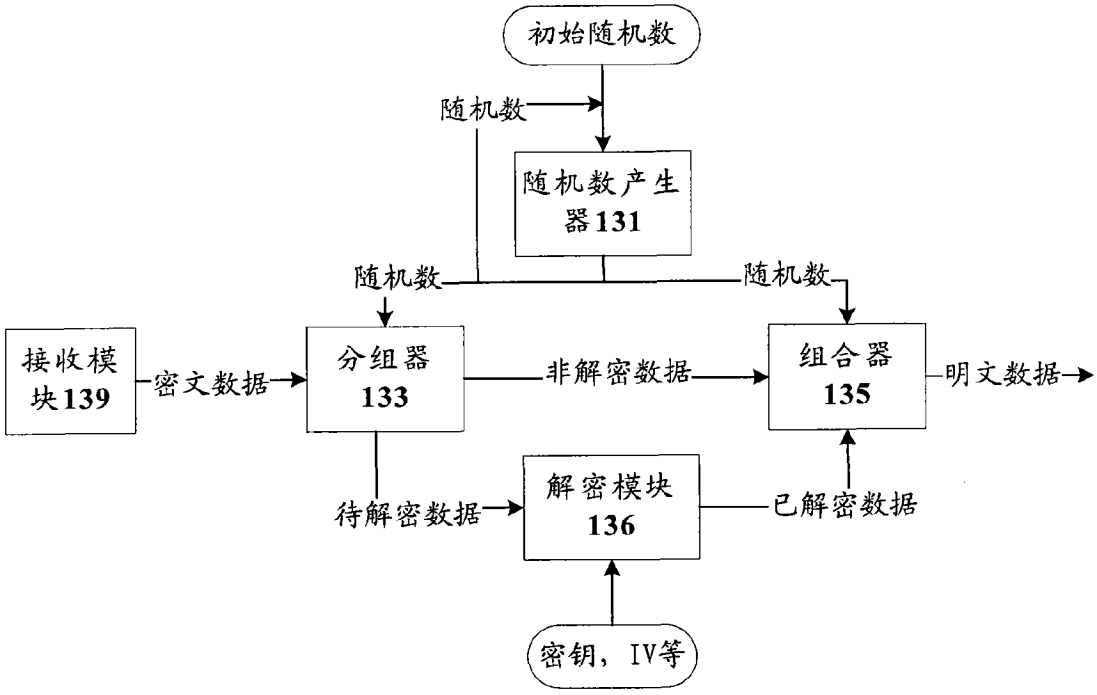

初始随机数
随机数
随机数产生器131
随机数
随机数
接收模块139
密文数据
分组器133
非解密数据
组合器135
明文数据
待解密数据
解密模块136
已解密数据
密钥，IV等

图 13

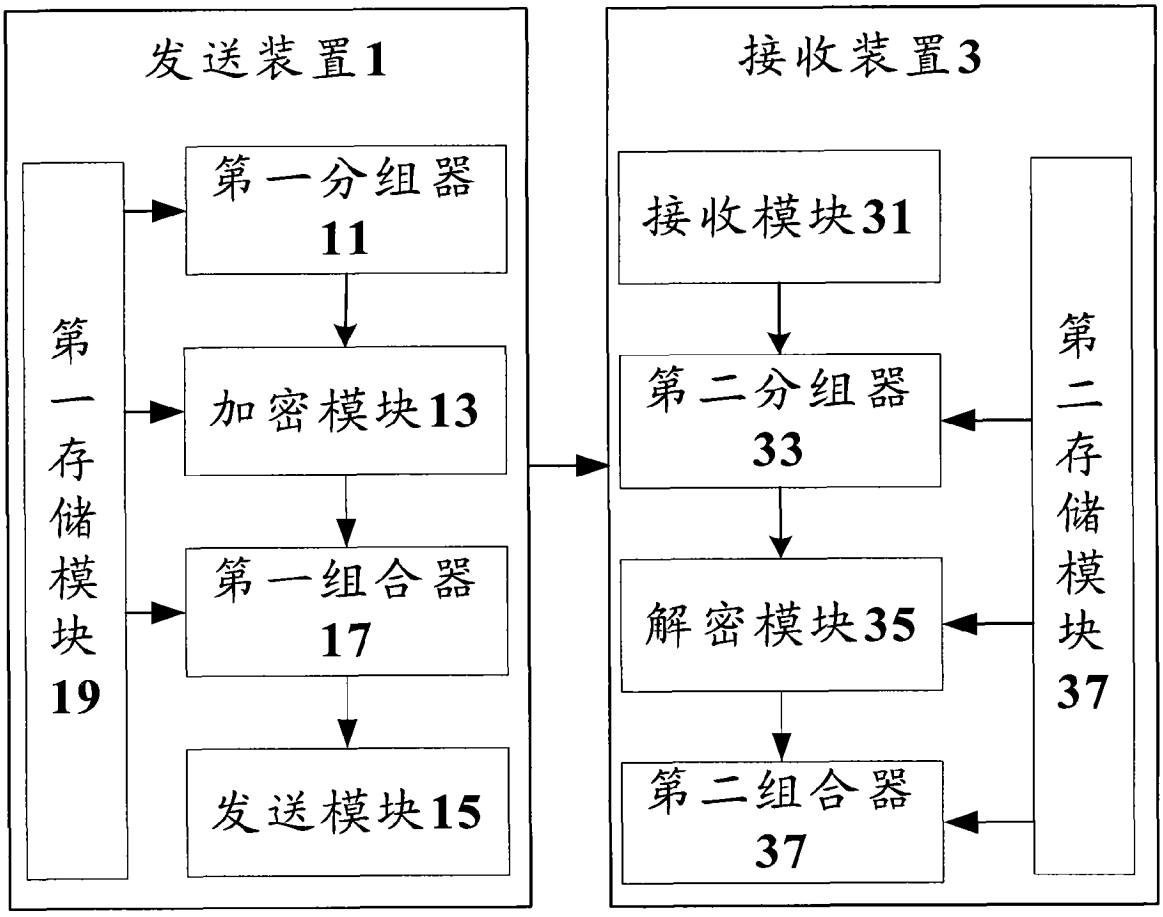

发送装置1
第一分组器
11
加密模块13
第一组合器
17
发送模块15
第一存储模块
19
接收装置3
接收模块31
第二分组器
33
解密模块35
第二组合器
37
第二存储模块
37

图 14