(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110348229 A
(43)申请公布日 2019.10.18

(21)申请号 201910502704.1

(22)申请日 2019.06.11

(71)申请人 北京思源互联科技有限公司
地址 100102 北京市朝阳区南湖中园316号楼301内18号

(72)发明人 程威

(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 江舟

(51)Int.Cl.
G06F 21/60(2013.01)

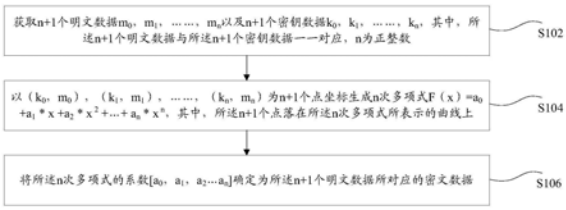
权利要求书3页 说明书14页 附图2页

(54)发明名称

数据的加密方法及装置、数据的解密方法及装置

(57)摘要

本发明公开了一种数据的加密方法及装置、数据的解密方法及装置。其中，该方法包括：获取n+1个明文数据m_0,m_1,……,m_n以及n+1个密钥数据k_0,k_1,……,k_n,其中,所述n+1个明文数据与所述n+1个密钥数据一一对应;以(k_0,m_0),(k_1,m_1),……,(k_n,m_n)为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$,其中,所述n+1个点落在所述n次多项式所表示的曲线上;将所述n次多项式的系数[a_0,a_1,$a_2\cdots a_n$]确定为所述n+1个明文数据所对应的密文数据。本发明解决了多方交互时加密数据传输过程中传输效率较低的技术问题。



CN 110348229 A

1.一种数据的加密方法,其特征在于,包括:

获取n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$以及n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$,其中,所述n+1个明文数据与所述n+1个密钥数据一一对应,n为正整数;

以$(k_0,m_0),(k_1,m_1),\cdots\cdots,(k_n,m_n)$为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$,其中,所述n+1个点落在所述n次多项式所表示的曲线上;

将所述n次多项式的系数$[a_0,a_1,a_2\cdots a_n]$确定为所述n+1个明文数据所对应的密文数据。

2.根据权利要求1所述的方法,其特征在于,获取所述n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$以及所述n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$包括:

获取待传输的n+1个初始数据;

将所述n+1个初始数据中每个初始数据扩展为数据长度为目标长度的所述n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$;

生成与所述n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$一一对应的所述n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$。

3.根据权利要求2所述的方法,其特征在于,将所述n+1个初始数据扩展为数据长度为目标长度的所述n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$包括:

在所述n+1个初始数据中数据长度最长的一个初始数据h_p的数据长度大于或者等于所述目标长度的情况下,在所述n+1个初始数据中除h_p之外的其他n个初始数据$h_0,\cdots\cdots,h_{p-1},h_{p+1}\cdots\cdots,h_n$之后补充第一目标数据,得到所述n个初始数据所对应的n个明文数据$m_0,\cdots\cdots,m_{p-1},m_{p+1}\cdots\cdots,m_n$,其中,所述n个明文数据中每个明文数据的数据长度等于h_p的数据长度,h_p为h_p所对应的明文数据m_p,p为大于等于0且小于等于n的整数;

在所述n+1个初始数据中数据长度最长的一个初始数据h_p的数据长度小于所述目标长度的情况下,在所述n+1个初始数据$h_0,h_1,\cdots\cdots,h_n$之后补充第二目标数据,得到所述n+1个初始数据所对应的n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$,其中,所述n+1个明文数据中每个明文数据的数据长度等于所述目标长度,p为大于等于0且小于等于n的整数。

4.根据权利要求1所述的方法,其特征在于,获取所述n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$以及所述n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$包括:

获取待传输的初始数据g,并生成所述初始数据g所对应的初始密钥k;

将所述初始数据g依据目标长度进行划分,获得所述n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$,其中,在划分得到的第n+1个数据的数据长度小于所述目标长度的情况下,在所述第n+1个数据之后补充第三目标数据,得到数据长度为所述目标长度的所述明文数据m_n;

根据所述初始密钥k通过预设的密钥生成函数生成所述n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$。

5.根据权利要求4所述的方法,其特征在于,根据所述初始密钥k通过预设的密钥生成函数生成所述n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$包括:

通过以下公式得到n+1个长度为length字节的密钥数据$k_0,k_1,\cdots\cdots,k_n$:

$k_0=keccak(seed_0+rand_0,length*(n+1))$,其中,$seed_0=k$,$rand_0$为一随机数random,keccak为单向散列函数;

$k_t=keccak(seed_t+rand_t,length*(n+1))$,其中,$rand_t=rand_0+t$,$seed_t=keccak(k_{t-1}+rand_t,length*(n+1))$,$t=1,2,3,\cdots,n$。

6.根据权利要求1所述的方法,其特征在于,以$(k_0,m_0),(k_1,m_1),\cdots\cdots,(k_n,m_n)$为n+1个

点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$包括：

以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为所述n+1个点坐标采用拉格朗日插值法生成所述n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$。

7.根据权利要求1至6中任一项所述的方法，其特征在于，在将所述n次多项式的系数$[a_0,a_1,a_2\cdots a_n]$确定为所述n+1个明文数据所对应的密文数据之后，所述方法还包括：

在所述接收端为多个接收端的情况下，使用所述n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$分别对应的接收端的公钥分别对所述n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$进行加密，得到n+1个加密密钥$ken_0,ken_1,\cdots\cdots,ken_n$；向所述多个接收端中的每个接收端分别发送所述密文数据和所述n+1个加密密钥中与所述每个接收端对应的加密密钥；

在所述接收端为一个接收端的情况下，使用所述一个接收端的公钥对初始密钥k进行加密，得到加密密钥ken；向所述一个接收端发送所述密文数据和所述加密密钥ken，其中，所述n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$是对所述初始密钥k进行分组得到的。

8.一种数据的解密方法，其特征在于，包括：

获取发送端发送的密文数据$[a_0,a_1,a_2\cdots a_n]$和密钥数据k_i，其中，所述密文数据$[a_0,a_1,a_2\cdots a_n]$为以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为n+1个点坐标生成的n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$的多项式系数，$m_0,m_1,\cdots\cdots,m_n$为n+1个明文数据，$k_0,k_1,\cdots\cdots,k_n$为n+1个密钥数据，所述n+1个明文数据与所述n+1个密钥数据一一对应，所述n+1个点落在所述n次多项式所表示的曲线上，n为正整数；

以密文数据$[a_0,a_1,a_2\cdots a_n]$为多项式的系数生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$；

将所述密钥数据ki作为x值代入所述n次多项式$F(k_i)=a_0+a_1*k_i+a_2*k_i^2+\cdots+a_n*k_i^n$，并将得到的$F(k_i)$确定为所述密钥数据$k_i$所对应的明文数据$m_i$，其中，$0\leq i\leq n$，i为整数。

9.根据权利要求8所述的方法，其特征在于，获取发送端发送的密文数据$[a_0,a_1,a_2\cdots a_n]$和密钥数据k_i包括：

接收所述发送端发送的所述密文数据$[a_0,a_1,a_2\cdots a_n]$和加密密钥ken_i；

使用私钥对所述加密密钥ken_i进行解密，得到所述密钥数据k_i。

10.一种数据的加密装置，其特征在于，包括：

第一获取模块，用于获取n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$以及n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$，其中，所述n+1个明文数据与所述n+1个密钥数据一一对应，n为正整数；

第一生成模块，用于以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$，其中，所述n+1个点落在所述n次多项式所表示的曲线上；

第一确定模块，用于将所述n次多项式的系数$[a_0,a_1,a_2\cdots a_n]$确定为所述n+1个明文数据所对应的密文数据。

11.一种数据的解密装置，其特征在于，包括：

第二获取模块，用于获取发送端发送的密文数据$[a_0,a_1,a_2\cdots a_n]$和密钥数据k_i，其中，所述密文数据$[a_0,a_1,a_2\cdots a_n]$为以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为n+1个点坐标生成的n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$的多项式系数，$m_0,m_1,\cdots\cdots,m_n$为n+1个明文数据，$k_0,k_1,\cdots\cdots,k_n$为n+1个密钥数据，所述n+1个明文数据与所述n+1个密钥数据一一对应，所述n+1个点落在所述n次多项式所表示的曲线上，n为正整数；

第二生成模块，用于以密文数据[a_0,a_1,a_2…a_n]为多项式的系数生成n次多项式F(x)＝a_0+a_1*x+a_2*x^2+…+a_n*x^n；

第二确定模块，用于将所述密钥数据k_i作为x值代入所述n次多项式F(k_i)＝a_0+a_1*k_i+a_2*k_i^2+…+a_n*k_i^n，并将得到的F(k_i)确定为所述密钥数据k_i所对应的明文数据m_i，其中，0≤i≤n，i为整数。

12.一种存储介质，其特征在于，所述存储介质中存储有计算机程序，其中，所述计算机程序被设置为运行时执行所述权利要求1至9任一项中所述的方法。

13.一种电子装置，包括存储器和处理器，其特征在于，所述存储器中存储有计算机程序，所述处理器被设置为通过所述计算机程序执行所述权利要求1至9任一项中所述的方法。

数据的加密方法及装置、数据的解密方法及装置

技术领域

[0001] 本发明涉及信息安全领域，具体而言，涉及一种数据的加密方法及装置、数据的解密方法及装置。

背景技术

[0002] 目前的对称加密算法是双方保持一个相同密钥进行同样的加解密算法来传递信息，但是面临对称密钥的管理难题；

[0003] 非对称加密可以帮助对称加密解决密钥管理的问题，但是加密速度和效率仍需提高；

[0004] 在对称加密时，每个消息进行分组或序列加密，密文长度与明文相等，传递消息的效率较低，需要能有算法可以进行快速加密和消息的快速传递。

[0005] 针对上述的问题，目前尚未提出有效的解决方案。

发明内容

[0006] 本发明实施例提供了一种数据的加密方法及装置、数据的解密方法及装置，以至少解决多方交互时加密数据传输过程中传输效率较低的技术问题。

[0007] 根据本发明实施例的一个方面，提供了一种数据的加密方法，包括：

[0008] 获取n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$以及n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$，其中，所述n+1个明文数据与所述n+1个密钥数据一一对应，n为正整数；

[0009] 以$(k_0,m_0),(k_1,m_1),\cdots\cdots,(k_n,m_n)$为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$，其中，所述n+1个点落在所述n次多项式所表示的曲线上；

[0010] 将所述n次多项式的系数$[a_0,a_1,a_2\cdots a_n]$确定为所述n+1个明文数据所对应的密文数据。

[0011] 根据本发明实施例的另一方面，还提供了一种数据的解密方法，包括：

[0012] 获取发送端发送的密文数据$[a_0,a_1,a_2\cdots a_n]$和密钥数据k_i，其中，所述密文数据$[a_0,a_1,a_2\cdots a_n]$为以$(k_0,m_0),(k_1,m_1),\cdots\cdots,(k_n,m_n)$为n+1个点坐标生成的n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$的多项式系数，$m_0,m_1,\cdots\cdots,m_n$为n+1个明文数据，$k_0,k_1,\cdots\cdots,k_n$为n+1个密钥数据，所述n+1个明文数据与所述n+1个密钥数据一一对应，所述n+1个点落在所述n次多项式所表示的曲线上，n为正整数；

[0013] 以密文数据$[a_0,a_1,a_2\cdots a_n]$为多项式的系数生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$；

[0014] 将所述密钥数据k_i作为x值代入所述n次多项式$F(k_i)=a_0+a_1*k_i+a_2*k_i^2+\cdots+a_n*k_i^n$，并将得到的$F(k_i)$确定为所述密钥数据$k_i$所对应的明文数据$m_i$，其中，$0\leqslant i\leqslant n$，i为整数。

[0015] 根据本发明实施例的另一方面，还提供了一种数据的加密装置，包括：

[0016] 第一获取模块，用于获取n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$以及n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$，其中，所述n+1个明文数据与所述n+1个密钥数据一一对应，n为正整数；

[0017] 第一生成模块，用于以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$，其中，所述n+1个点落在所述n次多项式所表示的曲线上；

[0018] 第一确定模块，用于将所述n次多项式的系数$[a_0,a_1,a_2\cdots a_n]$确定为所述n+1个明文数据所对应的密文数据。

[0019] 可选地，第一获取模块包括：

[0020] 第一获取单元，用于获取待传输的n+1个初始数据；

[0021] 扩展单元，用于将所述n+1个初始数据中每个初始数据扩展为数据长度为目标长度的所述n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$；

[0022] 第一生成单元，用于生成与所述n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$一一对应的所述n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$。

[0023] 可选地，扩展单元包括：

[0024] 第一扩展子单元，用于在所述n+1个初始数据中数据长度最长的一个初始数据h_p的数据长度大于或者等于所述目标长度的情况下，在所述n+1个初始数据中除h_p之外的其他n个初始数据$h_0,\cdots\cdots,h_{p-1},h_{p+1}\cdots\cdots,h_n$之后补充第一目标数据，得到所述n个初始数据所对应的n个明文数据$m_0,\cdots\cdots,m_{p-1},m_{p+1}\cdots\cdots,m_n$，其中，所述n个明文数据中每个明文数据的数据长度等于h_p的数据长度，h_p为h_p所对应的明文数据m_p，p为大于等于0且小于等于n的整数；

[0025] 第二扩展子单元，用于在所述n+1个初始数据中数据长度最长的一个初始数据h_p的数据长度小于所述目标长度的情况下，在所述n+1个初始数据$h_0,h_1,\cdots\cdots,h_n$之后补充第二目标数据，得到所述n+1个初始数据所对应的n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$，其中，所述n+1个明文数据中每个明文数据的数据长度等于所述目标长度，p为大于等于0且小于等于n的整数。

[0026] 可选地，第一获取模块包括：

[0027] 第一获取单元，用于获取待传输的初始数据g，并生成所述初始数据g所对应的初始密钥k；

[0028] 划分单元，用于将所述初始数据g依据目标长度进行划分，获得所述n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$，其中，在划分得到的第n+1个数据的数据长度小于所述目标长度的情况下，在所述第n+1个数据之后补充第三目标数据，得到数据长度为所述目标长度的所述明文数据m_n；

[0029] 第二生成单元，用于根据所述初始密钥k通过预设的密钥生成函数生成所述n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$。

[0030] 可选地，第二生成单元用于：

[0031] 通过以下公式得到n+1个长度为length字节的密钥数据$k_0,k_1,\cdots\cdots,k_n$：

[0032] $k_0=keccak(seed_0+rand_0,length*(n+1))$，其中，$seed_0=k$，$rand_0$为一随机数random，keccak为单向散列函数；

[0033] $k_t=keccak(seed_t+rand_t,length*(n+1))$，其中，$rand_t=rand_0+t$，$seed_t=keccak(k_{t-1}+rand_t,length*(n+1))$，$t=1,2,3,\cdots,n$。

[0034] 可选地，第一生成模块用于：

[0035] 以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为所述n+1个点坐标采用拉格朗日插值法生成所述n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$。

[0036] 可选地，所述装置还包括：

[0037] 第一处理模块，用于在所述接收端为多个接收端的情况下，使用所述n+1个明文数据m_0，m_1，……，m_n分别对应的接收端的公钥分别对所述n+1个密钥数据k_0，k_1，……，k_n进行加密，得到n+1个加密密钥ken_0，ken_1，……，ken_n；向所述多个接收端中的每个接收端分别发送所述密文数据和所述n+1个加密密钥中与所述每个接收端对应的加密密钥；

[0038] 第二处理模块，用于在所述接收端为一个接收端的情况下，使用所述一个接收端的公钥对初始密钥k进行加密，得到加密密钥ken；向所述一个接收端发送所述密文数据和所述加密密钥ken，其中，所述n+1个密钥数据k_0，k_1，……，k_n是对所述初始密钥k进行分组得到的。

[0039] 根据本发明实施例的另一方面，还提供了一种数据的解密装置，包括：

[0040] 第二获取模块，用于获取发送端发送的密文数据$[a_0,a_1,a_2\cdots a_n]$和密钥数据k_i，其中，所述密文数据$[a_0,a_1,a_2\cdots a_n]$为以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为n+1个点坐标生成的n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$的多项式系数，$m_0$，$m_1$，……，$m_n$为n+1个明文数据，$k_0$，$k_1$，……，$k_n$为n+1个密钥数据，所述n+1个明文数据与所述n+1个密钥数据一一对应，所述n+1个点落在所述n次多项式所表示的曲线上，n为正整数；

[0041] 第二生成模块，用于以密文数据$[a_0,a_1,a_2\cdots a_n]$为多项式的系数生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$；

[0042] 第二确定模块，用于将所述密钥数据k_i作为x值代入所述n次多项式$F(k_i)=a_0+a_1*k_i+a_2*k_i^2+\cdots+a_n*k_i^n$，并将得到的$F(k_i)$确定为所述密钥数据$k_i$所对应的明文数据$m_i$，其中，$0\leqslant i\leqslant n$，i为整数。

[0043] 可选地，第二获取模块包括：

[0044] 接收单元，用于接收所述发送端发送的所述密文数据$[a_0,a_1,a_2\cdots a_n]$和加密密钥ken_i；

[0045] 解密单元，用于使用私钥对所述加密密钥ken_i进行解密，得到所述密钥数据k_i。

[0046] 根据本发明实施例的另一方面，还提供了一种存储介质，其特征在于，所述存储介质中存储有计算机程序，其中，所述计算机程序被设置为运行时执行上述任一项中所述的方法。

[0047] 根据本发明实施例的另一方面，还提供了一种电子装置，包括存储器和处理器，其特征在于，所述存储器中存储有计算机程序，所述处理器被设置为通过所述计算机程序执行上述任一项中所述的方法。

[0048] 在本发明实施例中，采用获取n+1个明文数据m_0，m_1，……，m_n以及n+1个密钥数据k_0，k_1，……，k_n，其中，n+1个明文数据与n+1个密钥数据一一对应，n为正整数；以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$，其中，n+1个点落在n次多项式所表示的曲线上；将n次多项式的系数$[a_0,a_1,a_2\cdots a_n]$确定为n+1个明文数据所对应的密文数据的方式，多条不同的明文可以被同时加密成一条密文，增大了对称加密的消息量也提高了信息传输的传输效率，从而实现了提高数据传输过程中的传输效率的技术效果，进而解决了多方交互时加密数据传输过程中传输效率较低的技术问题。

附图说明

[0049] 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：

[0050] 图1是根据本发明实施例的一种可选的数据的加密方法的示意图；

[0051] 图2是根据本发明实施例的一种可选的数据的解密方法的示意图；

[0052] 图3是根据本发明实施例的一种可选的数据的加密装置的示意图；

[0053] 图4是根据本发明实施例的一种可选的数据的解密装置的示意图；

[0054] 图5是根据本发明实施例的一种可选的电子装置的示意图。

具体实施方式

[0055] 为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

[0056] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0057] 根据本发明实施例的一个方面，提供了一种数据的加密方法，如图1所示，该方法包括：

[0058] S102，获取n+1个明文数据m_0，m_1，……，m_n以及n+1个密钥数据k_0，k_1，……，k_n，其中，所述n+1个明文数据与所述n+1个密钥数据一一对应，n为正整数；

[0059] S104，以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$，其中，所述n+1个点落在所述n次多项式所表示的曲线上；

[0060] S106，将所述n次多项式的系数$[a_0,a_1,a_2\cdots a_n]$确定为所述n+1个明文数据所对应的密文数据。

[0061] 可选地，在本实施例中，n+1个明文数据m_0，m_1，……，m_n可以但不限于是传输给一个或者多个接收端的。

[0062] 可选地，在本实施例中，n+1个点坐标(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)可以但不限于是由n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$所表示的曲线上的点。例如：建立一个坐标系，横轴为x，纵轴为y，以k_0，k_1，……，k_n作为x值，m_0，m_1，……，m_n作为y值可以构造n+1个点坐标(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)，通过这n+1个点坐标就可以生成唯一一条曲线，该曲线的次数不大于n次。那么如果希望得到一个明文，只需将该明文对应的密钥代入n次多项式中即可，比如：将k_5代入n次多项式中$F(k_5)=a_0+a_1*k_5+a_2*k_5^2+\cdots+a_n*k_5^n$，得到的$F(k_5)$即为$m_5$。

[0063] 可选地，在本实施例中，得到的n次多项式的系数$[a_0,a_1,a_2\cdots a_n]$即可作为密文数

据进行传输，接收端接收到该密文数据，通过相同的规则构造出以密文数据为系数的多项式，即可使用其掌握到的密钥信息进行解密。

[0064] 可见，通过上述步骤，采用获取n+1个明文数据m_0，m_1，……，m_n以及n+1个密钥数据k_0，k_1，……，k_n，其中，n+1个明文数据与n+1个密钥数据一一对应，n为正整数；以(k_0，m_0)，(k_1，m_1)，……，(k_n，m_n)为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$，其中，n+1个点落在n次多项式所表示的曲线上；将n次多项式的系数[a_0，a_1，$a_2\cdots a_n$]确定为n+1个明文数据所对应的密文数据的方式，多条不同的明文可以被同时加密成一条密文，增大了对称加密的消息量，从而提高了信息加密速率，同时也提高了信息传输的安全性和传输效率，从而实现了提高数据传输过程中的传输效率的技术效果，进而解决了多方交互时加密数据传输过程中传输效率较低的技术问题。

[0065] 作为一种可选的方案，获取所述n+1个明文数据m_0，m_1，……，m_n以及所述n+1个密钥数据k_0，k_1，……，k_n包括：

[0066] S1，获取待传输的n+1个初始数据；

[0067] S2，将所述n+1个初始数据中每个初始数据扩展为数据长度为目标长度的所述n+1个明文数据m_0，m_1，……，m_n；

[0068] S3，生成与所述n+1个明文数据m_0，m_1，……，m_n一一对应的所述n+1个密钥数据k_0，k_1，……，k_n。

[0069] 可选地，在本实施例中，获取到的待传输的初始数据可以但不限于为多个。比如：初始数据可以是2至5个，以保证计算量在一个合理的范围内。

[0070] 可选地，在本实施例中，初始数据可以但不限于是对接收到的原始数据进行转换得到的。初始数据是原始数据转换为计算机可识别数据后的数据，转换方式可以但不限于包括16进制转换或2进制转换。

[0071] 可选地，在本实施例中，获取到的待传输的n+1个初始数据的长度可能各不相同，可以将其扩展为长度相同的n+1个明文数据m_0，m_1，……，m_n。

[0072] 可选地，在本实施例中，目标长度可以但不限于是初始数据中长度最长的数据的长度，或者也可以是预设的长度，比如384bit，768bit等等。

[0073] 可选地，在本实施例中，密钥长度可以表示算法的强度，n+1个密钥数据k_0，k_1，……，k_n的密钥长度相同，每个密钥数据的密钥长度leng可以但不限于至少为128bit。

[0074] 作为一种可选的方案，将所述n+1个初始数据扩展为数据长度为目标长度的所述n+1个明文数据m_0，m_1，……，m_n包括：

[0075] S1，在所述n+1个初始数据中数据长度最长的一个初始数据h_p的数据长度大于或者等于所述目标长度的情况下，在所述n+1个初始数据中除h_p之外的其他n个初始数据h_0，……，h_{p-1}，h_{p+1}……，h_n之后补充第一目标数据，得到所述n个初始数据所对应的n个明文数据m_0，……，m_{p-1}，m_{p+1}……，m_n，其中，所述n个明文数据中每个明文数据的数据长度等于h_p的数据长度，h_p为h_p所对应的明文数据m_p，p为大于等于0且小于等于n的整数；

[0076] S2，在所述n+1个初始数据中数据长度最长的一个初始数据h_p的数据长度小于所述目标长度的情况下，在所述n+1个初始数据h_0，h_1，……，h_n之后补充第二目标数据，得到所述n+1个初始数据所对应的n+1个明文数据m_0，m_1，……，m_n，其中，所述n+1个明文数据中每个明文数据的数据长度等于所述目标长度，p为大于等于0且小于等于n的整数。

[0077] 可选地，在本实施例中，可以但不限于根据初始数据中数据长度最长的一个初始数据h_p的数据长度与目标长度之间的关系对初始数据进行扩展，比如：如果初始数据h_p的数据长度超过了目标长度，则以初始数据h_p的数据长度为明文数据的长度对初始数据进行扩展，如果初始数据h_p的数据长度没有超过目标长度，则以目标长度为明文数据的长度对初始数据进行扩展。

[0078] 可选地，在本实施例中，数据扩展的方式可以但不限于是在长度不足的初始数据之后补充预先规定的数据。

[0079] 可选地，在本实施例中，第一目标数据和第二目标数据可以相同，也可以不同。比如：第一目标数据为0、第二目标数据为1，或者，第一目标数据为1、第二目标数据为0，或者，第一目标数据和第二目标数据均为0，或者，第一目标数据和第二目标数据均为1等等。

[0080] 作为一种可选的方案，获取所述n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$以及所述n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$包括：

[0081] S1，获取待传输的初始数据g，并生成所述初始数据g所对应的初始密钥k；

[0082] S2，将所述初始数据g依据目标长度进行划分，获得所述n+1个明文数据m_0，$m_1,\cdots\cdots,m_n$，其中，在划分得到的第n+1个数据的数据长度小于所述目标长度的情况下，在所述第n+1个数据之后补充第三目标数据，得到数据长度为所述目标长度的所述明文数据m_n；

[0083] S3，根据所述初始密钥k通过预设的密钥生成函数生成所述n+1个密钥数据k_0，$k_1,\cdots\cdots,k_n$。

[0084] 可选地，在本实施例中，可以但不限于对获取到的待传输的一个初始数据采用数据分组的方式进行加密。

[0085] 可选地，在本实施例中，可以但不限于根据初始密钥的长度对待传输的初始数据g进行分组。比如：按照初始密钥k的密钥长度的目标倍数进行分组。

[0086] 可选地，在本实施例中，初始密钥k的密钥长度为leng，可以但不限于按3*leng的长度大小对初始数据进行分组。

[0087] 可选地，在本实施例中，采用以下方式之一生成n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$：

[0088] 方式一，采用SM2中密钥生成函数kdf(k,klen)，其中，klen＝length*(n+1)；length为密钥数据的长度，可自由设定，如128bit；将密钥函数的返回值按照length长度依次划分为n+1个值，作为密钥数据$k_0,k_1,\cdots\cdots,k_n$。

[0089] 方式二，采用自定义密钥生成函数keccakrand：

[0090] k_0＝keccak($seed_0$+$rand_0$,length*(n+1))，其中$seed_0$＝k，$rand_0$为一随机数random；

[0091] k_t＝keccak($seed_t$+$rand_t$,length*(n+1))，其中$rand_t$＝$rand_0$+t，$seed_t$＝keccak(k_{t-1}+$rand_t$,length*(n+1))，t＝1,2,3,…,n；

[0092] keccak为单向散列函数；

[0093] 由此获取n+1个长度为length字节的密钥数据$k_0,k_1,\cdots\cdots,k_n$。密钥数据的长度length优选与初始密钥k的密钥长度leng相同，例如均为128bit。

[0094] 作为一种可选的方案，以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$包括：

[0095] 以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为所述n+1个点坐标采用拉格朗日插值法生成所

述n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$。

[0096] 可选地，在本实施例中，n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$可以但不限于为拉格朗日多项式，优选拉格朗日多项式。

[0097] 作为一种可选的方案，在将所述n次多项式的系数$[a_0,a_1,a_2\cdots a_n]$确定为所述n+1个明文数据所对应的密文数据之后，所述方法还包括：

[0098] S1，在所述接收端为多个接收端的情况下，使用所述n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$分别对应的接收端的公钥分别对所述n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$进行加密，得到n+1个加密密钥$ken_0,ken_1,\cdots\cdots,ken_n$；向所述多个接收端中的每个接收端分别发送所述密文数据和所述n+1个加密密钥中与所述每个接收端对应的加密密钥；

[0099] S2，在所述接收端为一个接收端的情况下，使用所述一个接收端的公钥对初始密钥k进行加密，得到加密密钥ken；向所述一个接收端发送所述密文数据和所述加密密钥ken，其中，所述n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$是对所述初始密钥k进行分组得到的。

[0100] 可选地，在本实施例中，使用接收端的公钥对其对应的密钥数据进行加密，得到加密密钥，将密文数据和加密密钥一起发送至对应的接收端，从而使得接收端能够使用加密密钥来获取密文数据对应的明文数据。

[0101] 可选地，在本实施例中，还可以但不限于以如下方式之一发送密钥：采用密钥协商算法，如DHE或ECDHE，协商获得密钥，以协商密钥加密发送；线下提前共享密钥等等。

[0102] 可选地，在本实施例中，在接收端为一个接收端的情况下，发送端与接收端以预设密钥生成函数对所述初始密钥k进行分组，其中，预设密钥生成函数包括但不限于SM2中密钥生成函数kdf(k,klen)或自定义密钥生成函数keccakrand，在此不再赘述。

[0103] 根据本发明实施例的一个方面，提供了一种数据的解密方法，如图2所示，该方法包括：

[0104] S202，获取发送端发送的密文数据$[a_0,a_1,a_2\cdots a_n]$和密钥数据k_i，其中，所述密文数据$[a_0,a_1,a_2\cdots a_n]$为以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为n+1个点坐标生成的n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$的多项式系数，$m_0,m_1,\cdots\cdots,m_n$为n+1个明文数据，$k_0,k_1,\cdots\cdots,k_n$为n+1个密钥数据，所述n+1个明文数据与所述n+1个密钥数据一一对应，所述n+1个点落在所述n次多项式所表示的曲线上，n为正整数；

[0105] S204，以密文数据$[a_0,a_1,a_2\cdots a_n]$为多项式的系数生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$；

[0106] S206，将所述密钥数据k_i作为x值代入所述n次多项式$F(k_i)=a_0+a_1*k_i+a_2*k_i^2+\cdots+a_n*k_i^n$，并将得到的$F(k_i)$确定为所述密钥数据$k_i$所对应的明文数据$m_i$，其中，$0\leqslant i\leqslant n$，i为整数。

[0107] 可选地，在本实施例中，接收端接收到密文数据，即n次多项式的系数，采用加密方相同的方式将其转换成n次多项式，并利用其掌握的密钥数据对n次多项式进行解密，得到明文数据。接收端只需将密钥数据代入n次多项式，得到的结果即为明文数据，解密速度快，效率高。

[0108] 作为一种可选的方案，获取发送端发送的密文数据$[a_0,a_1,a_2\cdots a_n]$和密钥数据k_i包括：

[0109] S1，接收所述发送端发送的所述密文数据$[a_0,a_1,a_2\cdots a_n]$和加密密钥ken_i；

[0110] S2，使用私钥对所述加密密钥ken_i进行解密，得到所述密钥数据k_i。

[0111] 可选地，在本实施例中，将密钥信息随密文数据一起发送给接收端，该密钥信息是使用接收端的公钥加密过的加密密钥，接收端使用其私钥对加密密钥进行解密，得到其对应的密钥数据，再使用密钥数据对密文数据进行解密。

[0112] 可选地，在本实施例中，还可以但不限于以如下方式之一解密获取密钥数据：采用预设协商密钥或其他共享密钥对接收到的加密密钥进行解密，得到其对应的密钥数据。

[0113] 可选地，在接收端为一个接收端的情况下，本发明实施例的数据的解密方法包括：

[0114] S202，获取发送端发送的密文数据$[a_0,a_1,a_2\cdots a_n]$和初始密钥k，其中，所述密文数据$[a_0,a_1,a_2\cdots a_n]$为以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为n+1个点坐标生成的n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$的多项式系数，$m_0,m_1,\cdots\cdots,m_n$为初始数据g进行分组得到的n+1个明文数据，$k_0,k_1,\cdots\cdots,k_n$为初始密钥k进行分组得到的n+1个密钥数据，所述n+1个明文数据与所述n+1个密钥数据一一对应，所述n+1个点落在所述n次多项式所表示的曲线上，n为正整数；其中，初始数据g及初始密钥k的分组方式如前所述，在此不再赘述；

[0115] S204，以密文数据$[a_0,a_1,a_2\cdots a_n]$为多项式的系数生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$；

[0116] S206，将所述密钥数据k_i作为x值代入所述n次多项式$F(k_i)=a_0+a_1*k_i+a_2*k_i^2+\cdots+a_n*k_i^n$，并将得到的$F(k_i)$确定为所述密钥数据$k_i$所对应的明文数据$m_i$，其中，$0\leqslant i\leqslant n$，i为整数；

[0117] S208，将步骤S206获得的n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$组合生成初始数据g。

[0118] 需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

[0119] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，或者网络设备等)执行本发明各个实施例所述的方法。

[0120] 根据本发明实施例的另一个方面，还提供了一种用于实施上述数据的加密方法的数据的加密装置，如图3所示，该装置包括：

[0121] 第一获取模块32，用于获取n+1个明文数据$m_0,m_1,\cdots\cdots,m_n$以及n+1个密钥数据$k_0,k_1,\cdots\cdots,k_n$，其中，所述n+1个明文数据与所述n+1个密钥数据一一对应，n为正整数；

[0122] 第一生成模块34，用于以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$，其中，所述n+1个点落在所述n次多项式所表示的曲线上；

[0123] 第一确定模块36，用于将所述n次多项式的系数$[a_0,a_1,a_2\cdots a_n]$确定为所述n+1个明文数据所对应的密文数据。

[0124] 作为一种可选的方案，第一获取模块包括：

[0125] 第一获取单元，用于获取待传输的n+1个初始数据；

[0126] 扩展单元，用于将所述n+1个初始数据中每个初始数据扩展为数据长度为目标长度的所述n+1个明文数据m_0，m_1，……，m_n；

[0127] 第一生成单元，用于生成与所述n+1个明文数据m_0，m_1，……，m_n一一对应的所述n+1个密钥数据k_0，k_1，……，k_n。

[0128] 作为一种可选的方案，扩展单元包括：

[0129] 第一扩展子单元，用于在所述n+1个初始数据中数据长度最长的一个初始数据h_p的数据长度大于或者等于所述目标长度的情况下，在所述n+1个初始数据中除h_p之外的其他n个初始数据h_0，……，h_{p-1}，h_{p+1}……，h_n之后补充第一目标数据，得到所述n个初始数据所对应的n个明文数据m_0，……，m_{p-1}，m_{p+1}……，m_n，其中，所述n个明文数据中每个明文数据的数据长度等于h_p的数据长度，h_p为h_p所对应的明文数据m_p，p为大于等于0且小于等于n的整数；

[0130] 第二扩展子单元，用于在所述n+1个初始数据中数据长度最长的一个初始数据h_p的数据长度小于所述目标长度的情况下，在所述n+1个初始数据h_0，h_1，……，h_n之后补充第二目标数据，得到所述n+1个初始数据所对应的n+1个明文数据m_0，m_1，……，m_n，其中，所述n+1个明文数据中每个明文数据的数据长度等于所述目标长度，p为大于等于0且小于等于n的整数。

[0131] 作为一种可选的方案，第一获取模块包括：

[0132] 第一获取单元，用于获取待传输的初始数据g，并生成初始数据g所对应的初始密钥k；

[0133] 划分单元，用于将所述初始数据g依据目标长度进行划分，获得所述n+1个明文数据m_0，m_1，……，m_n，其中，在划分得到的第n+1个数据的数据长度小于所述目标长度的情况下，在所述第n+1个数据之后补充第三目标数据，得到数据长度为所述目标长度的所述明文数据m_n；

[0134] 第二生成单元，用于根据初始密钥k通过预设的密钥生成函数生成n+1个密钥数据k_0，k_1，……，k_n。

[0135] 可选地，第二生成单元用于：

[0136] 通过以下公式得到n+1个长度为length字节的密钥数据k_0，k_1，……，k_n：

[0137] k_0＝keccak(seed$_0$+rand$_0$,length*(n+1))，其中，seed$_0$＝k，rand$_0$为一随机数random，keccak为单向散列函数；

[0138] k_t＝keccak(seed$_t$+rand$_t$,length*(n+1))，其中，rand$_t$＝rand$_0$+t，seed$_t$＝keccak(k_{t-1}+rand$_t$,length*(n+1))，t＝1,2,3,…,n。

[0139] 作为一种可选的方案，第一生成模块用于：

[0140] 以(k_0,m_0)，(k_1,m_1)，……，(k_n,m_n)为所述n+1个点坐标采用拉格朗日插值法生成所述n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$。

[0141] 作为一种可选的方案，上述装置还包括：

[0142] 第一处理模块，用于在接收端为多个接收端的情况下，使用n+1个明文数据m_0，m_1，……，m_n在多个接收端中分别对应的接收端的公钥分别对n+1个密钥数据k_0，k_1，……，k_n进行加密，得到n+1个加密密钥ken_0，ken_1，……，ken_n；向多个接收端中的每个接收端分别发

送密文数据和n+1个加密密钥中与每个接收端对应的加密密钥；

[0143] 第二处理模块，用于在所述接收端为一个接收端的情况下，使用所述一个接收端的公钥对初始密钥k进行加密，得到加密密钥ken；向所述一个接收端发送所述密文数据和所述加密密钥ken，其中，所述n+1个密钥数据k_0，k_1，……，k_n是对所述初始密钥k进行分组得到的。

[0144] 根据本发明实施例的另一个方面，还提供了一种用于实施上述数据的解密方法的数据的解密装置，如图4所示，该装置包括：

[0145] 第二获取模块42，用于获取发送端发送的密文数据[a_0，a_1，a_2…a_n]和密钥数据k_i，其中，所述密文数据[a_0，a_1，a_2…a_n]为以(k_0，m_0)，(k_1，m_1)，……，(k_n，m_n)为n+1个点坐标生成的n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$的多项式系数，$m_0$，$m_1$，……，$m_n$为n+1个明文数据，$k_0$，$k_1$，……，$k_n$为n+1个密钥数据，所述n+1个明文数据与所述n+1个密钥数据一一对应，所述n+1个点落在所述n次多项式所表示的曲线上，n为正整数；

[0146] 第二生成模块44，用于以密文数据[a_0，a_1，a_2…a_n]为多项式的系数生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$；

[0147] 第二确定模块46，用于将所述密钥数据k_i作为x值代入所述n次多项式$F(k_i)=a_0+a_1*k_i+a_2*k_i^2+\cdots+a_n*k_i^n$，并将得到的$F(k_i)$确定为所述密钥数据$k_i$所对应的明文数据$m_i$，其中，$0\leqslant i\leqslant n$，i为整数。

[0148] 作为一种可选的方案，第二获取模块包括：

[0149] 接收单元，用于接收发送端发送的密文数据[a_0，a_1，a_2…a_n]和加密密钥ken_i；

[0150] 解密单元，用于使用私钥对加密密钥ken_i进行解密，得到密钥数据k_i。

[0151] 本发明实施例的应用环境可以但不限于参照上述实施例中的应用环境，本实施例中对此不再赘述。本发明实施例提供了用于实施上述实时通信的连接方法的一种可选的具体应用示例。

[0152] 作为一种可选的实施例，上述数据的加解密方法可以但不限于应用于数据传输过程中对数据进行加解密处理的场景中。在本场景中，提出了一种多明文对称加解密的方法，该方法基于拉格朗日多项式的原理，构造n+1个点，可以得到幂不超过n的唯一一个拉格朗日多项式。

[0153] 场景一，将一个明文m发送给一个接收端，初始密钥为k。

[0154] 将接收到的原始明文转为16进制后得到初始数据g，按3*leng(这里是优选方式，至少384bit可以达到安全要求)的长度大小进行分组，对于分组得到的最后一个明文数据的大小不够时，用0进行补位。假设分组后获得n+1组明文数据m_0，m_1，……，m_n，则将初始密钥k通过预设函数进行分组得到n+1组密钥数据k_0，k_1，……，k_n。

[0155] 密钥的分组方式可以但不限于包括如下之一：

[0156] 方式一，采用SM2中密钥生成函数kdf(k，klen)，其中，klen＝length*(n+1)；length为密钥数据的长度，可自由设定，如128bit；将密钥函数的返回值按照length长度依次划分为n+1个值，作为密钥数据k_0，k_1，……，k_n。

[0157] 方式二，采用自定义密钥生成函数keccakrand：

[0158] k_0＝keccak($seed_0$+$rand_0$，length*(n+1))，其中$seed_0$＝k，$rand_0$为一随机数random；

[0159] k_t=keccak($seed_t$+$rand_t$,length*(n+1))，其中$rand_t$=$rand_0$+t，$seed_t$=keccak(k_{t-1}+$rand_t$,length*(n+1))，t=1,2,3,…,n；

[0160] keccak为单向散列函数；

[0161] 由此获取n+1个长度为length字节的密钥数据k_0,k_1,……,k_n。密钥数据的长度length优选与初始密钥k的密钥长度leng相同，例如均为128bit。

[0162] 通过上述方式将明文分组后的每一组明文与密钥组合构造点坐标，构造的点坐标为(k_i,m_i)(0≤i≤n,i为整数)，即以密钥为x-横坐标，明文为y-纵坐标。代入所有的点根据拉格朗日插值法进行计算，得到如下唯一的多项式：

[0163] $F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$；

[0164] 将得到的每一个明文分组的最终系数数组[a_0,a_1,…,a_n]作为密文数据发送。

[0165] 接收端解密时，根据系数数组构造形成多项式，根据初始密钥k及预设密钥生成函数获取密钥数据k_1,k_2,……,k_n，分别将密钥数据代入多项式可得到所有分组的明文数据m_0,m_1,……,m_n，组合后得到最终的初始数据g，即$f(k_0)||f(k_1)||\cdots||f(k_n)$。

[0166] 可选地，在本实施例中，分组的数量可以但不限于不超过5。

[0167] 可选地，在本实施例中，还提供了一个在聊天场景中加解密的方式，将上述对称加密方式应用在一个聊天加密场景中，构造一个单窗口的多明文加密系统如下：

[0168] 在同一个聊天界面中，用户A给用户B发送加密聊天消息。用户A随机生成初始密钥k，将要发送的消息转换成16进制后(即初始数据g)按照上述方法分组为5个明文消息，对应地将初始密钥k分组为5把密钥，根据上述多明文对称加密方式，生成最终的密文msgenc。

[0169] 用户A使用用户B的公钥加密k得到ken。消息中转服务器收到发送的密文后，将密文msgenc和ken发送给用户B。

[0170] 用户B收到密文后，使用自身的私钥解密ken得到k，以相同方法对k进行分组得到5把密钥，分别代入5把密钥和msgenc根据上述多明文对称加密算法解密得到最终的5个明文消息，将5个明文消息进行组合得到初始数据g。

[0171] 场景二，将n+1个明文m_0,m_1,……,m_n发送给多个接收端。

[0172] 令n为不小于1的正整数，随机生成n+1个长度均为leng的对称密钥(k_0,…,k_n)，密钥长度即算法的强度，密钥长度leng可以但不限于至少为128bit。

[0173] 将接收到的n+1个原始数据转16进制后得到n+1个明文(m_0,…,m_n)，其中，以最长的明文为准，将其他n个明文的长度按0补位，使n+1个明文的长度相同。其中，若最长明文不足384bit，则将n+1个明文按0补位，均补齐384bit。

[0174] 将明文与密钥组合构造点坐标，点构造坐标为(k_i,m_i)，即以密钥为x-横坐标，明文为y-纵坐标。代入所有的点根据拉格朗日插值法进行计算，得到如下唯一的多项式：

[0175] $F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$

[0176] 将得到的n+1个明文的最终系数数组[a_0,a_1,…,a_n]作为密文进行传输给对应的接收端。

[0177] 接收端解密时，每一个解密方根据系数数组构造形成每个明文的多项式，代入其掌握的对称密钥k_i可解密得到其对应的明文m_i，即n+1个解密方分别解密获得$f(k_0)$、$f(k_1)$、…、$f(k_n)$；0≤i≤n,i为整数。

[0178] 上述加解密方式理论上支持n+1方同时参与进行多明文对称加密运算，可选地，可

以在多方参与运算时，对接收密文方进行分组，每组参与方可以不超过5。接收方分组后，通过层层传递，每次传递使用上述的多明文对称加密方式，可以最终快速实现多明文的加密传递，且计算幂不超过5。

[0179] 可选地，在本实施例中，还提供了另一个在群聊场景中加解密的方式，将上述对称加密方式应用在一个群聊加密场景中，构造一个单窗口的多明文加密系统如下：

[0180] 在同一个聊天界面中，用户user给用户u1、用户u2、用户u3、用户u4和用户u5同时发送加密聊天消息。用户user随机生成5把密钥k_1到k_5，分别把要发送的5条不同消息与此5把密钥，按照上述方法将5条不同消息转16进制后，补齐为相同长度，根据上述多明文对称加密方法，生成最终的密文msgenc。

[0181] 用户user分别使用5个用户的公钥分别加密k_1，k_2，k_3，k_4，k_5得到ken_1，ken_2，ken_3，ken_4，ken_5。消息中转服务器收到发送的密文后，按对应接收方组合密文，分别发送给对应的用户，即给用户u1转发msgenc||ken_1，给用户u2转发msgenc||ken_2，依次类推。

[0182] 接收方的用户收到密文后，以用户u1举例，其使用自身的私钥解密ken_1得到k_1，代入k_1和msgenc根据多明文对称加密算法解密得到最终的明文m_1，其它用户类推可分别得到自己对应的明文消息。

[0183] 可选地，在本实施例中，每次加密都随机产生新的对称密钥。

[0184] 通过上述加解密方式，多条不同接收方的明文可以被同时加密成一条密文，增大了对称加密的消息量。多条消息加密成一条密文，与传统对称加密算法相比，即保障了分组快速加密，同时将明文映射成系数时大大缩减了信息大小。加密的计算过程非常简单，降低了数据传输的复杂度，且每次对称密钥都随机产生，达到一次一密的效果。

[0185] 根据本发明实施例的又一个方面，还提供了一种用于实施上述数据的加密的电子装置，如图5所示，该电子装置包括：一个或多个(图中仅示出一个)处理器502、存储器504、传感器506、编码器508以及传输装置510，该存储器中存储有计算机程序，该处理器被设置为通过计算机程序执行上述任一项方法实施例中的步骤。

[0186] 可选地，在本实施例中，上述电子装置可以位于计算机网络的多个网络设备中的至少一个网络设备。

[0187] 可选地，在本实施例中，上述处理器可以被设置为通过计算机程序执行以下步骤：

[0188] S1，获取n+1个明文数据m_0，m_1，……，m_n以及n+1个密钥数据k_0，k_1，……，k_n，其中，所述n+1个明文数据与所述n+1个密钥数据一一对应，n为正整数；

[0189] S2，以(k_0，m_0)，(k_1，m_1)，……，(k_n，m_n)为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$，其中，所述n+1个点落在所述n次多项式所表示的曲线上；

[0190] S3，将所述n次多项式的系数[a_0，a_1，$a_2\cdots a_n$]确定为所述n+1个明文数据所对应的密文数据。

[0191] 可选地，本领域普通技术人员可以理解，图5所示的结构仅为示意，电子装置也可以是智能手机(如Android手机、iOS手机等)、平板电脑、掌上电脑以及移动互联网设备(Mobile Internet Devices，MID)、PAD等终端设备。图5其并不对上述电子装置的结构造成限定。例如，电子装置还可包括比图5中所示更多或者更少的组件(如网络接口、显示装置等)，或者具有与图5所示不同的配置。

[0192] 其中，存储器504可用于存储软件程序以及模块，如本发明实施例中的数据的加密

方法和装置对应的程序指令/模块，处理器502通过运行存储在存储器504内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的目标组件的控制方法。存储器504可包括高速随机存储器，还可以包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器504可进一步包括相对于处理器502远程设置的存储器，这些远程存储器可以通过网络连接至终端。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0193] 上述的传输装置510用于经由一个网络接收或者发送数据。上述的网络具体实例可包括有线网络及无线网络。在一个实例中，传输装置510包括一个网络适配器(Network Interface Controller,NIC)，其可通过网线与其他网络设备与路由器相连从而可与互联网或局域网进行通讯。在一个实例中，传输装置510为射频(Radio Frequency,RF)模块，其用于通过无线方式与互联网进行通讯。

[0194] 其中，具体地，存储器504用于存储应用程序。

[0195] 本发明的实施例还提供了一种存储介质，该存储介质中存储有计算机程序，其中，该计算机程序被设置为运行时执行上述任一项方法实施例中的步骤。

[0196] 可选地，在本实施例中，上述存储介质可以被设置为存储用于执行以下步骤的计算机程序：

[0197] S1，获取n+1个明文数据m_0，m_1，……，m_n以及n+1个密钥数据k_0，k_1，……，k_n，其中，所述n+1个明文数据与所述n+1个密钥数据一一对应，n为正整数；

[0198] S2，以(k_0，m_0)，(k_1，m_1)，……，(k_n，m_n)为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\cdots+a_n*x^n$，其中，所述n+1个点落在所述n次多项式所表示的曲线上；

[0199] S3，将所述n次多项式的系数[a_0，a_1，$a_2\cdots a_n$]确定为所述n+1个明文数据所对应的密文数据。

[0200] 可选地，存储介质还被设置为存储用于执行上述实施例中的方法中所包括的步骤的计算机程序，本实施例中对此不再赘述。

[0201] 可选地，在本实施例中，本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令终端设备相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：闪存盘、只读存储器(Read-Only Memory，ROM)、随机存取器(Random Access Memory,RAM)、磁盘或光盘等。

[0202] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0203] 上述实施例中的集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在上述计算机可读取的存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在存储介质中，包括若干指令用以使得一台或多台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。

[0204] 在本发明的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0205] 在本申请所提供的几个实施例中，应该理解到，所揭露的客户端，可通过其它的方式实现。其中，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，仅仅为一

种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

[0206] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0207] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0208] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

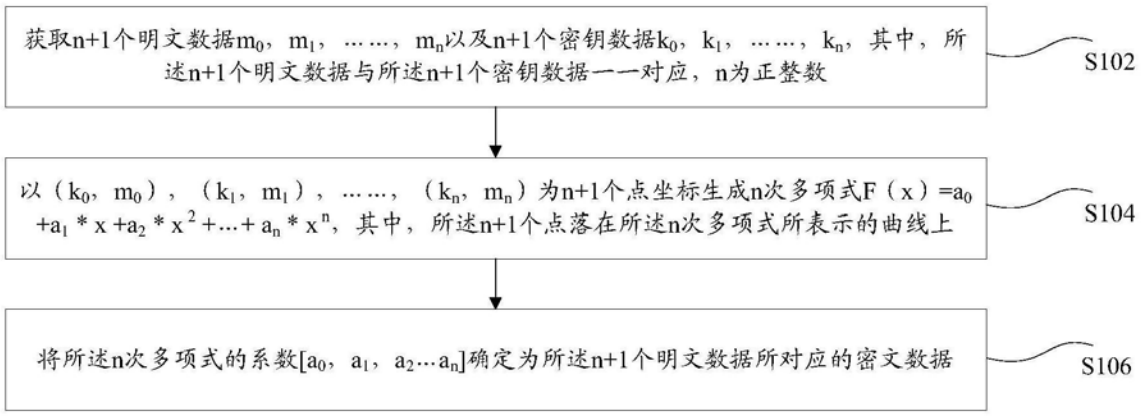

获取n+1个明文数据m_0，m_1，……，m_n以及n+1个密钥数据k_0，k_1，……，k_n，其中，所述n+1个明文数据与所述n+1个密钥数据一一对应，n为正整数
S102
以（k_0，m_0），（k_1，m_1），……，（k_n，m_n）为n+1个点坐标生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\ldots+a_n*x^n$，其中，所述n+1个点落在所述n次多项式所表示的曲线上
S104
将所述n次多项式的系数[a_0，a_1，$a_2\cdots a_n$]确定为所述n+1个明文数据所对应的密文数据
S106

图1

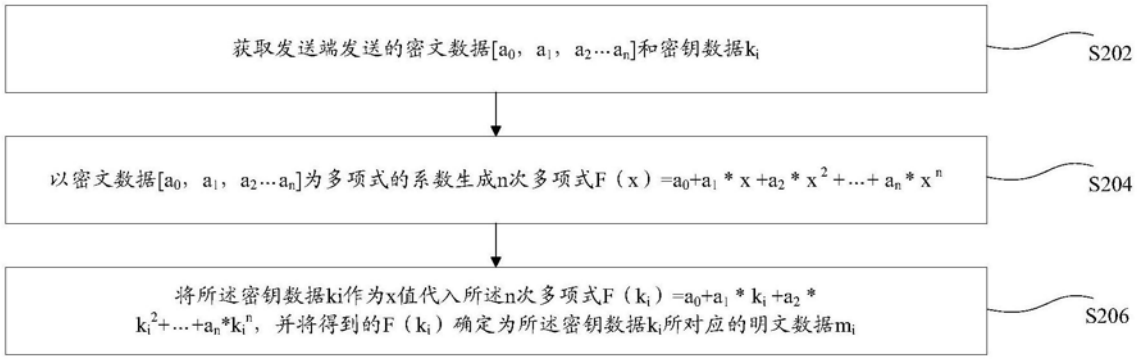

获取发送端发送的密文数据[a_0，a_1，$a_2\cdots a_n$]和密钥数据k_i
S202
以密文数据[a_0，a_1，$a_2\cdots a_n$]为多项式的系数生成n次多项式$F(x)=a_0+a_1*x+a_2*x^2+\ldots+a_n*x^n$
S204
将所述密钥数据ki作为x值代入所述n次多项式$F(k_i)=a_0+a_1*k_i+a_2*k_i^2+\ldots+a_n*k_i^n$，并将得到的$F(k_i)$确定为所述密钥数据$k_i$所对应的明文数据$m_i$
S206

图2

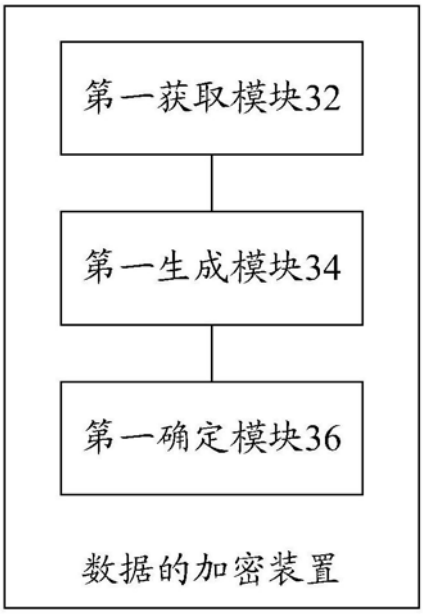

第一获取模块32
第一生成模块34
第一确定模块36
数据的加密装置

图3

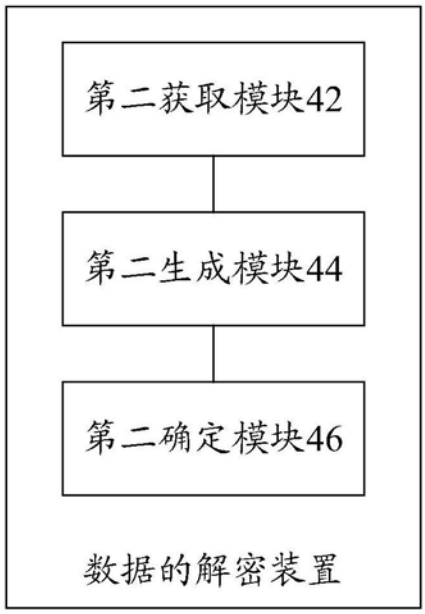

第二获取模块42
第二生成模块44
第二确定模块46
数据的解密装置

图4

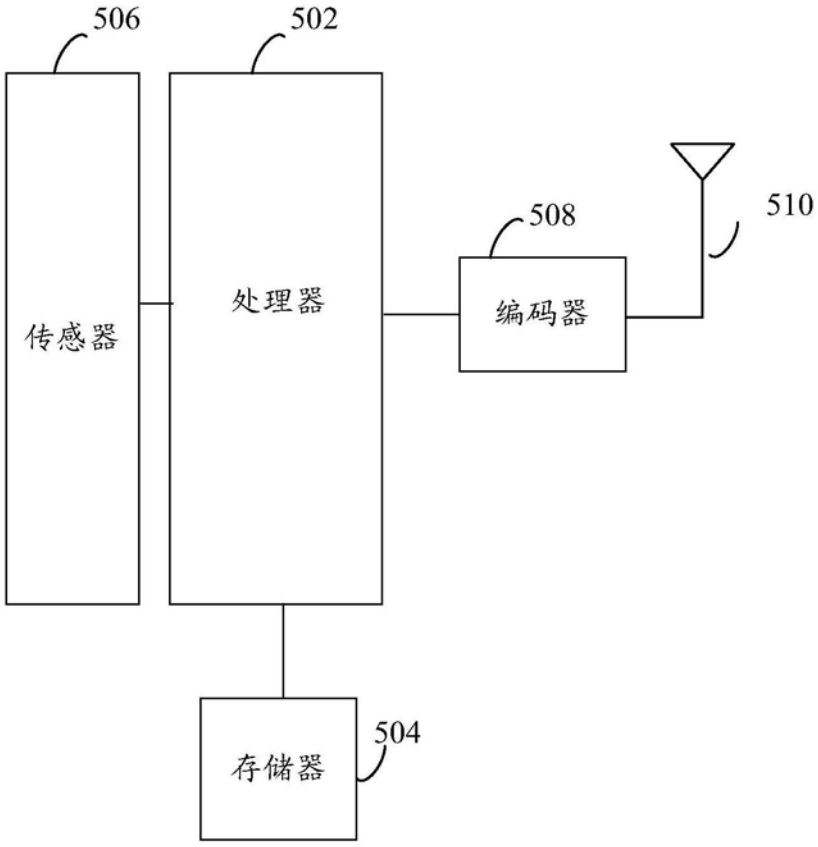

506
502
508
510
传感器
处理器
编码器
存储器
504

图5