(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 113328859 B
(45)授权公告日 2022.02.22

(21)申请号 202110428242.0
(22)申请日 2021.04.21
(65)同一申请的已公布的文献号
申请公布号 CN 113328859 A
(43)申请公布日 2021.08.31
(73)专利权人 北京连山科技股份有限公司
地址 100000 北京市顺义区赵全营镇东盈路19号3幢二层
(72)发明人 张凯 郑应强 牛德标
(74)专利代理机构 北京冠和权律师事务所 11399
代理人 田春龙
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/00(2022.01)

(56)对比文件
CN 106688204 A,2017.05.17

审查员 李俊洁

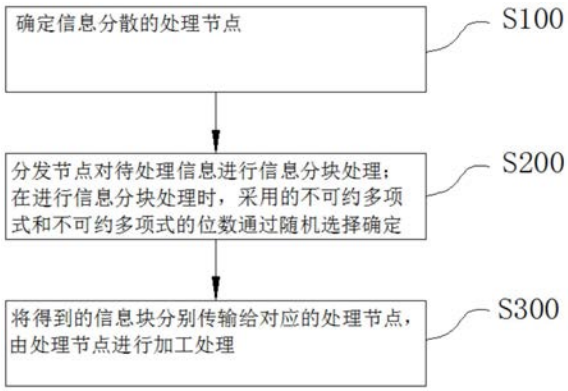
权利要求书3页 说明书8页 附图1页

(54)发明名称

信息分散的处理方法

(57)摘要

本发明提供了一种信息分散的处理方法,包括:确定信息分散的处理节点;分发节点对待处理信息进行信息分块处理;在进行信息分块处理时,采用的不可约多项式和不可约多项式的位数通过随机选择确定;将得到的信息块分别传输给对应的处理节点,由处理节点进行加工处理。本发明的信息分散的处理方法为信息分散的实现提供了更为多变的处理方法,该方案采用随机选择不可约多项式位数和不可约多项式类型对信息进行分散,使得处理过程更为复杂多变,增加攻击者的分析难度,提升信息分散安全性。



CN 113328859 B

1.一种信息分散的处理方法,其特征在于,包括:

确定信息分散的处理节点;

分发节点对待处理信息进行信息分块处理;在进行信息分块处理时,采用的不可约多项式和不可约多项式的项数通过随机选择确定;

将得到的信息块分别传输给对应的处理节点,由处理节点进行加工处理;

所述信息分块处理的过程如下:

所述分发节点在信息分块处理时,提取待处理信息的数据特征,根据数据特征利用预设切分规则,对所述待处理信息进行数据分散处理,得到信息块;

为信息块选取对应的随机数;根据选取的所述随机数,形成填充的预制因子;将所述信息块与所述预制因子进行异或运算,得到数据组合块;

按照所述预设填充规则,为处理节点选取随机因子;以随机因子与预制因子进行匹配运算后,根据运算匹配结果将信息分块处理得到的数据组合块传输至相应随机因子的处理节点;

在信息块传输前进行以下处理:

所述分发节点在线性子空间$GF(p^t)$上随机选取向量$u=(u_1,u_2,\cdots,u_{t-1})$为信息向量,满足$s=ug_0 \bmod p$,分发节点计算加密份额,$S=(s_1,s_2,\cdots,s_n)$,则$s=s_0$,分发节点分别将$s_i$,$i=1,2\cdots,n$作为信息块进行传输;

若处理节点$\{U_1,U_2,\cdots,U_m\}$进行待处理信息恢复,则

当$m=t$时,处理节点各自计算身份向量$(x_1,x_2,\cdots,x_m)$,使得$g_0=(g_1,g_2,\cdots,g_m)(x_1,x_2,\cdots,x_m)^T \bmod p$,处理节点公开组件信息$c_i=s_ix_i \bmod p$,计算得到待处理信息的加密份额:

$$s=\sum_{i=1}^{m} c_i \bmod p$$

其中,t表示通过随机方式确定的不可约多项式的项数;s表示当$m=t$时待处理信息的加密份额;S表示待处理信息;s_0表示初始的加密份额;g_0表示分发节点的线性码;$g_1,g_2,\cdots,g_m$分别表示处理节点的线性码;m表示接收信息块传输的处理节点数量;c_i表示处理节点i公开的组件信息;mod表示取余运算;p表示一大素数;

当$m>t$时,处理节点各自计算身份向量$(x_1',x_2',\cdots,x_m')$,使得$g_0=(g_1,g_2,\cdots,g_t)(x_1',x_2',\cdots,x_m')^T \bmod p$,每个处理节点将身份向量传输给其他处理节点,每个处理节点计算:

$$(x_1,\ x_2,\ \ldots,\ x_m)=\frac{1}{m}\left(\sum_{i=1}^{m}x_1',\ \sum_{i=1}^{m}x_2',\ \ldots,\ \sum_{i=1}^{m}x_m'\right) \bmod p$$

上式中,$x_1,x_2,\cdots,x_m$表示当$m=t$时对应处理节点的身份向量;m表示接收信息块传输的处理节点数量;$x_1',x_2',\cdots,x_m'$表示当$m>t$时对应处理节点的身份向量;

处理节点公开各自的组件信息$c_i=s_ix_i \bmod p$,计算得到待处理信息的加密份额:

$$s'=\sum_{j=1}^{m} c_j \bmod p$$

上式中，s‘表示当m>t时待处理信息的加密份额；m表示接收信息块传输的处理节点数量；c_j表示处理节点j公开的组件信息；mod表示取余运算；p表示一大素数；

所述随机因子引入SHA-256散列函数来获取对应的哈希值；

将获取的所述哈希值作为加密密钥K，并将K分解成子密钥k_i，则有：

K＝k1,k2,k3…k32；

引入二维混沌系统输出随机序列，则有：

$x_i＝\sin(\pi\tau(y_{i-1}+3)x_{i-1}(1-x_{i-1}))$

$y_i＝\sin(\pi\tau(x_i+3)y_{i-1}(1-y_{i-1}))$

其中，x_i和y_i表示第i个处理节点的二维混沌坐标，x_{i-1}和y_{i-1}表示第i-1个处理节点的二维混沌坐标，τ表示系统参数，且0<τ≤1；

利用子密钥k_i来设定三个过渡参数V_1,V_2,V_3，则有：

$$V_1 = \mathrm{mod}\left(\left(k_1 \oplus k_3 \oplus k_5 \ldots \oplus k_{29} \oplus k_{31} + \sum_{i=1}^{32} k_i\right), 2^8\right)/256$$

$$V_2 = \mathrm{mod}\left(\left(k_2 \oplus k_4 \oplus k_6 \ldots \oplus k_{30} \oplus k_{32} + \sum_{i=1}^{32} k_i\right), 2^8\right)/256$$

$$V_3 = \mathrm{mod}\left(\left(k_1 \oplus k_2 \oplus k_3 \ldots \oplus k_{15} \oplus k_{16} + \sum_{i=1}^{32} k_i\right), 2^8\right)/256$$

其中，⊕表示异或运算，mod表示取余运算；

根据计算得到所述过渡参数V_1,V_2,V_3的值，通过预设参数τ,x,y计算初始值τ_0,x_0,y_0，则有：

$\tau_0＝(\tau+V_3)\bmod1$

$x_0＝(x+V_2)\bmod1$

$y_0＝(y+V_1)\bmod1$

根据计算得到的初始值τ_0,x_0,y_0，代入所述二维混沌系统输出的随机序列中，并进行非线性运算，则满足：

$$X_{V_j} = [|x_{V_j}| - x_{V_j} * 10^{14}] \bmod 2^{10}$$

$$Y_{V_j} = [|y_{V_j}| - y_{V_j} * 10^{14}] \bmod 2^{10}$$

其中，X_{V_j}表示加密后的数据组合块，Y_{V_j}表示解密密钥，x_{V_j}表示加密后的信息块，y_{V_j}表示加密后的信息块的解密子密钥，j为加密方法，且j＝1,2,3。

2.根据权利要求1所述的信息分散的处理方法，其特征在于，所述处理节点接收到加密的信息块后，通过检验等式是否成立判断接收到的信息块是否有效，若检验等式不成立，则接收到的信息块无效，重新进行信息块的传输；若检验等式成立，则表明信息块有效，然后利用预设算法计算恢复待处理信息。

3.根据权利要求1所述的信息分散的处理方法，其特征在于，在恢复待处理信息过程中，每个处理节点能够异步公开加密组件信息。

4.根据权利要求1所述的信息分散的处理方法，其特征在于，所述处理节点接收到加密的信息块后，先进行解密还原，再对还原后的信息块进行加工处理，所述加工处理包括存储、转化、传送和发布中的一项或者多项处理内容。

5.根据权利要求1所述的信息分散的处理方法，其特征在于，所述切分规则采用先垂直切分后水平切分的结合方式，在垂直切分后形成多个切分块，依据待处理信息的逻辑关系对各个切分块进行切分调整，调整后的切分块即为信息块。

6.根据权利要求2所述的信息分散的处理方法，其特征在于，所述检验等式采用以下等式：

$$w^{s_i} = \prod_{k=0}^{t-1} b_i^{i^k} \bmod q$$

上式中，w^{s_i}表示对第i项信息块的广播消息的承诺，t表示通过随机方式确定的不可约多项式的项数；b_i表示分发节点的第i项信息块的广播消息；mod表示取余运算；q表示一个大素数。

7.根据权利要求1所述的信息分散的处理方法，其特征在于，所述信息块的传输方法如下：

基于所述分发节点的标识信息，获取第一处理节点与所述分发节点之间的连接通道；

获取确定传输的各信息块；

基于需要传输至第一处理节点的信息块的参数确定信息块的文件类信息，确定采用第一传输方式，基于所述第一传输方式以及所述连接通道，将对应信息块传输至所述第一处理节点；

将连接通道以通道镜像方式形成其他各处理节点与所述分发节点连接的镜像通道，确定采用第二传输方式，其中，所述第二传输方式不同于第一传输方式，将其他信息块传输至对应的各处理节点。

信息分散的处理方法

技术领域

[0001] 本发明涉及信息分散处理技术领域，特别涉及一种信息分散的处理方法。

背景技术

[0002] 现有的信息分散处理方法，一般都是采用Shamir加密分享技术，对信息进行分散处理，该方法一般都是通过固定的线性方程组对数据进行变换处理，其中Shamir加密分享具体如下：

[0003] 若对于n个分享节点$\{U_1,U_2,\cdots,U_n\}$，门限值为t，加密为s，p为一大素数，$X_1,X_2,\cdots,X_n$为对应分享节点(处理节点)的身份信息，除了加密s以外，其他参数信息均公开；加密分发时，加密分发节点D在GF(p)上随机选择一个t-1次多项式$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1} \bmod p$，$a_i \in GF(p)$，满足要求$f(0)=a_0=s$，分发节点D计算加密份额$s_i=f(x_i)$，$i=1,2\cdots,n$，并将$s_i$分发给参与节点$U_i$；加密恢复时，假设t个参与节点$\{U_1,U_2,\cdots,U_t\}$试图恢复加密，参与节点分发自己的加密份额并利用拉格朗日插值多项式算法构造：

[0004] $$f(x)=\sum_{i=1}^{t} f(x_i)\prod_{r=1,r\neq i}^{t}\frac{x-x_r}{x_i-x_r} \bmod p$$

[0005] 加密通过计算可得：

[0006] $$s=f(0)=\sum_{i=1}^{t} f(x_i)\prod_{r=1,r\neq i}^{t}\frac{-x_r}{x_i-x_r} \bmod p$$

[0007] Shamir的加密共享方案满足基本的门限需求：

[0008] (1)持有t个或多于t个加密份额的参与节点可以恢复加密；

[0009] (2)少于t个的情况下，加密不能被获得。

[0010] 但是，现用的信息分散采用固定的线性方程组进行运算时，信息处理方法单一，不可约多项式固定，二元域位数固定，导致容易遭受攻击。

发明内容

[0011] 为了解决上述技术问题，本发明提供了一种信息分散的处理方法，包括：

[0012] 确定信息分散的处理节点；

[0013] 分发节点对待处理信息进行信息分块处理；在进行信息分块处理时，采用的不可约多项式和不可约多项式的位数通过随机选择确定；

[0014] 将得到的信息块分别传输给对应的处理节点，由处理节点进行加工处理。

[0015] 可选的，所述信息分块处理的过程如下：

[0016] 所述分发节点在信息分块处理时，提取待处理信息的数据特征，根据数据特征利用预设切分规则，对所述待处理信息进行数据分散处理，得到信息块；

[0017] 为信息块选取对应的随机数；根据选取的所述随机数，形成填充的预制因子；将所

述信息块与所述预制因子进行异或运算，得到数据组合块；

[0018] 按照所述预设填充规则，为处理节点选取随机因子；以随机因子与预制因子进行匹配运算后，根据运算匹配结果将信息分块处理得到的数据组合块传输至相应随机因子的处理节点。

[0019] 可选的，所述处理节点接收到加密的信息块后，通过检验等式是否成立判断接收到的信息块是否有效，若检验等式不成立，则接收到的信息块无效，重新进行信息块的传输；若检验等式成立，则表明信息块有效，然后利用预设算法计算恢复待处理信息。

[0020] 可选的，在恢复待处理信息过程中，每个处理节点能够异步公开加密组件信息。

[0021] 可选的，在信息块传输前进行以下处理：

[0022] 所述分发节点在线性子空间GF(p^t)上随机选取向量$u=(u_1,u_2,\cdots,u_{t-1})$为信息向量，满足$s=ug_0 \bmod p$，分发节点计算加密份额$S=(s_1,s_2,\cdots,s_n)=uG \bmod p$，则$s=s_0$，分发节点分别将$s_i$，$i=1,2\cdots,n$作为信息块进行传输；

[0023] 若处理节点$\{U_1,U_2,\cdots,U_m\}$进行待处理信息恢复，则

[0024] 当$m=t$时，处理节点各自计算身份向量$(x_1,x_2,\cdots,x_m)$，使得$g_0=(g_1,g_2,\cdots,g_m)(x_1,x_2,\cdots,x_m)^T \bmod p$，处理节点公开组件信息$c_i=s_ix_i \bmod p$，计算得到待处理信息：

[0025] $$s=\sum_{i=1}^{m} c_i \bmod p$$

[0026] 其中，t表示通过随机方式确定的不可约多项式的项数，s表示当$m=t$时待处理信息的加密份额；m表示接收信息块传输的处理节点数量；c_i表示处理节点i公开的组件信息；mod表示取余运算；p表示一大素数；

[0027] 当$m>t$时，处理节点各自计算身份向量$(x_1',x_2',\cdots,x_m')$，使得$g_0=(g_1,g_2,\cdots,g_t)(x_1',x_2',\cdots,x_m')^T \bmod p$，每个处理节点将身份向量传输给其他处理节点，每个处理节点计算：

[0028] $$(x_1,\ x_2,\ \ldots,\ x_m)=\frac{1}{m}\left(\sum_{i=1}^{m}x_1',\ \sum_{i=1}^{m}x_2',\ \ldots,\ \sum_{i=1}^{m}x_m'\right) \bmod p$$

[0029] 上式中，$x_1,x_2,\cdots,x_m$表示当$m=t$时对应处理节点的身份向量；m表示接收信息块传输的处理节点数量；$x_1',x_2',\cdots,x_m'$表示当$m>t$时对应处理节点的身份向量；

[0030] 处理节点公开各自的组件信息$c_i=s_ix_i \bmod p$，计算得到待处理信息的加密份额：

[0031] $$s'=\sum_{j=1}^{m} c_j \bmod p$$

[0032] 上式中，s‘表示当$m>t$时待处理信息的加密份额；m表示接收信息块传输的处理节点数量；c_j表示处理节点j公开的组件信息；mod表示取余运算；p表示一大素数。

[0033] 可选的，所述随机因子引入SHA-256散列函数来获取对应的哈希值；

[0034] 将获取的所述哈希值作为加密密钥K，并将K分解成子密钥k_i，则有：

[0035] K=k1,k2,k3…k32；

[0036] 引入二维混沌系统输出随机序列，则有：

[0037] $x_i = \sin(\pi\tau(y_{i-1}+3)x_{i-1}(1-x_{i-1}))$

[0038] $y_i = \sin(\pi\tau(x_i+3)y_{i-1}(1-y_{i-1}))$

[0039] 其中，x_i和y_i表示第i个处理节点的二维混沌坐标，x_{i-1}和y_{i-1}表示第i-1个处理节点的二维混沌坐标，τ表示系统参数，且0<τ≤1；

[0040] 利用子密钥k_i来设定三个过渡参数V_1，V_2，V_3，则有：

[0041] $$V_1 = \mathrm{mod}\left(\left(k_1 \oplus k_3 \oplus k_5 \ldots \oplus k_{29} \oplus k_{31} + \sum_{i=1}^{32} k_i\right), 2^8\right)/256$$

[0042] $$V_2 = \mathrm{mod}\left(\left(k_2 \oplus k_4 \oplus k_6 \ldots \oplus k_{30} \oplus k_{32} + \sum_{i=1}^{32} k_i\right), 2^8\right)/256$$

[0043] $$V_3 = \mathrm{mod}\left(\left(k_1 \oplus k_2 \oplus k_3 \ldots \oplus k_{15} \oplus k_{16} + \sum_{i=1}^{32} k_i\right), 2^8\right)/256$$

[0044] 其中，⊕表示异或运算，mod表示取余运算；

[0045] 根据计算得到所述过渡参数V_1，V_2，V_3的值，通过预设参数τ，x，y计算初始值τ_0，x_0，y_0，则有：

[0046] $\tau_0 = (\tau+V_3)\bmod 1$

[0047] $x_0 = (x+V_2)\bmod 1$

[0048] $y_0 = (y+V_1)\bmod 1$

[0049] 根据计算得到的初始值τ_0，x_0，y_0，代入所述二维混沌系统输出的随机序列中，并进行非线性运算，则满足：

[0050] $$X_{V_j} = [|x_{V_j}| - x_{V_j} * 10^{14}] \bmod 2^{10}$$

[0051] $$Y_{V_j} = [|y_{V_j}| - y_{V_j} * 10^{14}] \bmod 2^{10}$$

[0052] 其中，X_{V_j}表示加密后的数据组合块，Y_{V_j}表示解密密钥，j为加密方法，且j=1，2，3。

[0053] 可选的，所述处理节点接收到加密的信息块后，先进行解密还原，再对还原后的信息块进行加工处理，所述加工处理包括存储、转化、传送和发布中的一项或者多项处理内容。

[0054] 可选的，所述切分规则采用先垂直切分后水平切分的结合方式，在垂直切分后形成多个切分块，依据待处理信息的逻辑关系对各个切分块进行切分调整，调整后的切分块即为信息块。

[0055] 可选的，所述检验等式采用以下等式：

[0056] $$w^{s_i} = \prod_{k=0}^{t-1} b_i^{i^k} \bmod q$$

[0057] 上式中，w^{s_i}表示对第i项信息块的广播消息的承诺，t表示通过随机方式确定的不

可约多项式的项数;b_i表示分发节点的第i项信息块的广播消息;mod表示取余运算;q表示一个大素数。

[0058] 可选的,所述信息块的传输方法如下:

[0059] 基于所述分发节点的标识信息,获取第一处理节点与所述分发节点之间的连接通道;

[0060] 获取确定传输的各信息块;

[0061] 基于需要传输至第一处理节点的信息块的参数确定信息块的文件类信息,确定采用第一传输方式,基于所述第一传输方式以及所述连接通道,将对应信息块传输至所述第一处理节点;

[0062] 将连接通道以通道镜像方式形成其他各处理节点与所述分发节点连接的镜像通道,确定采用第二传输方式,其中,所述第二传输方式不同于第一传输方式,将其他信息块传输至对应的各处理节点。

[0063] 本发明的信息分散的处理方法,为信息分散的实现提供了更为多变的处理方法。该方案采用随机选择不可约多项式位数和不可约多项式类型对信息进行分散,使得处理过程更为复杂多变,增加攻击者的分析难度,提升信息分散安全性。

[0064] 本发明的其它特征和优点将在随后的说明书中阐述,并且,部分地从说明书中变得显而易见,或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

[0065] 下面通过附图和实施例,对本发明的技术方案做进一步的详细描述。

附图说明

[0066] 附图用来提供对本发明的进一步理解,并且构成说明书的一部分,与本发明的实施例一起用于解释本发明,并不构成对本发明的限制。在附图中:

[0067] 图1为本发明实施例中一种信息分散的处理方法的流程图。

具体实施方式

[0068] 以下结合附图对本发明的优选实施例进行说明,应当理解,此处所描述的优选实施例仅用于说明和解释本发明,并不用于限定本发明。

[0069] 如图1所示,本发明实施例提供了一种信息分散的处理方法,包括:

[0070] S100确定信息分散的处理节点;

[0071] S200分发节点对待处理信息进行信息分块处理;在进行信息分块处理时,采用的不可约多项式和不可约多项式的位数通过随机选择确定;

[0072] S300将得到的信息块分别传输给对应的处理节点,由处理节点进行加工处理。

[0073] 上述技术方案的工作原理和有益效果为:本方案在进行信息分块处理时,通过随机选择确定采用的不可约多项式和不可约多项式的位数,为信息分散的实现提供了更为多变的处理方法,使得处理过程更为复杂多变,提高了加密被破解的难度,增加攻击者的分析难度,进一步提升了信息分散传输与处理过程中的安全性。

[0074] 在一个实施例中,所述信息分块处理的过程如下:

[0075] 所述分发节点在信息分块处理时,提取待处理信息的数据特征,根据数据特征利

用预设切分规则，对所述待处理信息进行数据分散处理，得到信息块；

[0076] 为信息块选取对应的随机数；根据选取的所述随机数，形成填充的预制因子；将所述信息块与所述预制因子进行异或运算，得到数据组合块；

[0077] 按照所述预设填充规则，为处理节点选取随机因子；以随机因子与预制因子进行匹配运算后，根据运算匹配结果将信息分块处理得到的数据组合块传输至相应随机因子的处理节点。

[0078] 上述技术方案的工作原理和有益效果为：本方案在进行信息分块处理时，通过提取待处理信息的数据特征，结合预设切分规则，将待处理信息分解成若干数量的块，即信息块；再给各信息块逐一选定对应的随机数，形成填充的预制因子，进行异或运算，得到数据组合块；通过为处理节点选取随机因子，以随机因子与预制因子进行匹配运算后，根据运算匹配结果将信息分块处理得到的数据组合块传输至相应随机因子的处理节点；通过随机因子与预制因子的形成的匹配具有的偶发性，提高了破译的难度，进一步增强信息分散处理的安全性和可靠性。

[0079] 在一个实施例中，所述处理节点接收到加密的信息块后，通过检验等式是否成立判断接收到的信息块是否有效，所述检验等式采用以下等式：

[0080] $$w^{s_i} = \prod_{k=0}^{t-1} b_i^{i^k} \bmod q$$

[0081] 上式中，w^{s_i}表示对第i项信息块的广播消息的承诺，t表示通过随机方式确定的不可约多项式的项数；b_i表示分发节点的第i项信息块的广播消息；mod表示取余运算；q表示一个大素数；

[0082] 若检验等式不成立，则接收到的信息块无效，重新进行信息块的传输；若检验等式成立，则表明信息块有效，然后利用预设算法计算恢复待处理信息。

[0083] 上述技术方案的工作原理和有益效果为：本方案处理节点还对接收到的加密的信息块进行检验，通过检验等式是否成立判断接收到的信息块是否有效，若检验等式不成立，则接收到的信息块无效，这时不能进行信息加工处理，需要重新进行信息块的传输；只有在检验等式成立则表明信息块有效，可以进行信息块加工处理，本方案可以防止信息块发生传输或者其他错误造成分散处理错误或者故障，保障信息分散处理的顺利进行。

[0084] 在一个实施例中，在恢复待处理信息过程中，每个处理节点能够异步公开加密组件信息。

[0085] 上述技术方案的工作原理和有益效果为：本方案的每个处理节点彩笔异步公开加密组件信息，实现通讯中由于网络等各种原因，基本不可能多个处理节点实时同步通讯，为了防止选用同步通讯后事实上无法实现所造成的问题，通过选择采用异步公开的方式，能够允许存在不同步通讯的情况，降低处理故障，提高信息处理效率。

[0086] 在一个实施例中，在信息块传输前进行以下处理：

[0087] 所述分发节点在线性子空间$GF(p^t)$上随机选取向量$u=(u_1,u_2,\cdots,u_{t-1})$为信息向量，满足$s=ug_0 \bmod p$，分发节点计算加密份额$S=(s_1,s_2,\cdots,s_n)=uG \bmod p$，则$s=s_0$，分发节点分别将$s_i$，$i=1,2\cdots,n$作为信息块进行传输；

[0088] 若处理节点$\{U_1,U_2,\cdots,U_m\}$进行待处理信息恢复，则

[0089] 当$m=t$时，处理节点各自计算身份向量$(x_1,x_2,\cdots,x_m)$，使得$g_0=(g_1,g_2,\cdots,g_m)(x_1,$

$x_2,\cdots,x_m)^T$ mod p,处理节点公开组件信息$c_i=s_ix_i$ mod p,计算得到待处理信息:

[0090] $$s=\sum_{i=1}^{m}c_i \bmod p$$

[0091] 其中,t表示通过随机方式确定的不可约多项式的项数,s表示当m=t时待处理信息的加密份额;m表示接收信息块传输的处理节点数量;c_i表示处理节点i公开的组件信息;mod表示取余运算;p表示一大素数;

[0092] 当m>t时,处理节点各自计算身份向量$(x_1',x_2',\cdots,x_m')$,使得$g_0=(g_1,g_2,\cdots,g_t)(x_1',x_2',\cdots,x_m')^T$ mod p,每个处理节点将身份向量传输给其他处理节点,每个处理节点计算:

[0093] $$(x_1,\ x_2,\ \ldots,\ x_m)=\frac{1}{m}\left(\sum_{i=1}^{m}x_1',\ \sum_{i=1}^{m}x_2',\ \ldots,\ \sum_{i=1}^{m}x_m'\right) \bmod p$$

[0094] 上式中,$x_1,x_2,\cdots,x_m$表示当m=t时对应处理节点的身份向量;m表示接收信息块传输的处理节点数量;$x_1',x_2',\cdots,x_m'$表示当m>t时对应处理节点的身份向量;

[0095] 处理节点公开各自的组件信息$c_i=s_ix_i$ mod p,计算得到待处理信息的加密份额:

[0096] $$s'=\sum_{j=1}^{m}c_j \bmod p$$

[0097] 上式中,s‘表示当m>t时待处理信息的加密份额;m表示接收信息块传输的处理节点数量;c_j表示处理节点j公开的组件信息;mod表示取余运算;p表示一大素数。

[0098] 上述技术方案的工作原理和有益效果为:本方案限定在信息块传输前通过分发节点在线性子空间$GF(p^t)$上随机选取向量,计算加密份额后进行信息块传输;在处理节点$\{U_1,U_2,\cdots,U_m\}$进行待处理信息恢复,根据收信息块传输的处理节点数量与不可约多项式的项数对比,处理节点计算出的待处理信息的加密份额存在差异,因而在进行待处理信息恢复时,需要采用不同的算法进行处理;本方案避免了由于不可约多项式的项数选择的随机性可能导致的待处理信息恢复问题,保障了信息分散处理的顺利进行。

[0099] 在一个实施例中,所述随机因子引入SHA-256散列函数来获取对应的哈希值;

[0100] 将获取的所述哈希值作为加密密钥K,并将K分解成子密钥k_i,则有:

[0101] K=k1,k2,k3…k32;

[0102] 引入二维混沌系统输出随机序列,则有:

[0103] $x_i=\sin(\pi\tau(y_{i-1}+3)x_{i-1}(1-x_{i-1}))$

[0104] $y_i=\sin(\pi\tau(x_i+3)y_{i-1}(1-y_{i-1}))$

[0105] 其中,x_i和y_i表示第i个处理节点的二维混沌坐标,x_{i-1}和y_{i-1}表示第i-1个处理节点的二维混沌坐标,τ表示系统参数,且$0<\tau\leqslant 1$;

[0106] 利用子密钥k_i来设定三个过渡参数V_1,V_2,V_3,则有:

[0107] $$V_1=\bmod\left(\left(k_1\oplus k_3\oplus k_5\ldots\oplus k_{29}\oplus k_{31}+\sum_{i=1}^{32}k_i\right),\ 2^8\right)/256$$

[0108] $$V_2 = \mathrm{mod}\left(\left(k_2 \oplus k_4 \oplus k_6 \ldots \oplus k_{30} \oplus k_{32} + \sum_{i=1}^{32} k_i\right),\ 2^8\right)/256$$

[0109] $$V_3 = \mathrm{mod}\left(\left(k_1 \oplus k_2 \oplus k_3 \ldots \oplus k_{15} \oplus k_{16} + \sum_{i=1}^{32} k_i\right),\ 2^8\right)/256$$

[0110] 其中，⊕表示异或运算，mod表示取余运算；

[0111] 根据计算得到所述过渡参数V_1，V_2，V_3的值，通过预设参数τ，x，y计算初始值τ_0，x_0，y_0，则有：

[0112] $\tau_0 = (\tau + V_3) \bmod 1$

[0113] $x_0 = (x + V_2) \bmod 1$

[0114] $y_0 = (y + V_1) \bmod 1$

[0115] 根据计算得到的初始值τ_0，x_0，y_0，代入所述二维混沌系统输出的随机序列中，并进行非线性运算，则满足：

[0116] $$X_{V_j} = [|x_{V_j}| - x_{V_j} * 10^{14}] \bmod 2^{10}$$

[0117] $$Y_{V_j} = [|y_{V_j}| - y_{V_j} * 10^{14}] \bmod 2^{10}$$

[0118] 其中，X_{V_j}表示加密后的数据组合块，Y_{V_j}表示解密密钥，j为加密方法，且j＝1，2，3。

[0119] 上述技术方案的工作原理和有益效果为：本方案对处理节点选取的随机因子，引入SHA-256散列函数来获取对应的哈希值，以该哈希值作为加密密钥；引入二维混沌系统输出随机序列，利用子加密密钥设定三个过渡参数，计算得到系统参数和二维混沌坐标初始值，代入所述二维混沌系统输出的随机序列中进行非线性运算，得到数据组合块和解密密钥；本方案可以为处理节点解密恢复待处理信息提供基础，消除信息分散后的处理障碍，提高信息分散处理效率。

[0120] 在一个实施例中，所述处理节点接收到加密的信息块后，先进行解密还原，再对还原后的信息块进行加工处理，所述加工处理包括存储、转化、传送和发布中的一项或者多项处理内容；所述切分规则采用先垂直切分后水平切分的结合方式，在垂直切分后形成多个切分块，依据待处理信息的逻辑关系对各个切分块进行切分调整，调整后的切分块即为信息块。

[0121] 上述技术方案的工作原理和有益效果为：本方案对切分规则进行了限定，采用先垂直切分后水平切分的两者结合方式，待处理信息经垂直切分后形成多个切分块，然后依据待处理信息的逻辑关系，对各个切分块进行切分调整，以调整后的切分块作为信息块，采用本方案，既可以保证切分的效率，又能够让各信息块保留一定的横向联系信息，有利于处理节点进行解密恢复。

[0122] 在一个实施例中，所述信息块的传输方法如下：

[0123] 基于所述分发节点的标识信息，获取第一处理节点与所述分发节点之间的连接通

道；

[0124] 获取确定传输的各信息块；

[0125] 基于需要传输至第一处理节点的信息块的参数确定信息块的文件类信息，确定采用第一传输方式，基于所述第一传输方式以及所述连接通道，将对应信息块传输至所述第一处理节点；

[0126] 将连接通道以通道镜像方式形成其他各处理节点与所述分发节点连接的镜像通道，确定采用第二传输方式，其中，所述第二传输方式不同于第一传输方式，将其他信息块传输至对应的各处理节点。

[0127] 上述技术方案的工作原理和有益效果为：本方案通过获取第一处理节点与所述分发节点之间的连接通道，根据需要传输至第一处理节点的信息块的参数确定信息块的文件类信息，选择采用第一传输方式进行第一处理节点的信息块传输；然后采用通道镜像方式形成其他各处理节点与所述分发节点连接的镜像通道，采用第二传输方式通过镜像通道实现其他处理节点对应的信息块传输；通过镜像可以快速实现传输连接，提高传输效率。

[0128] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

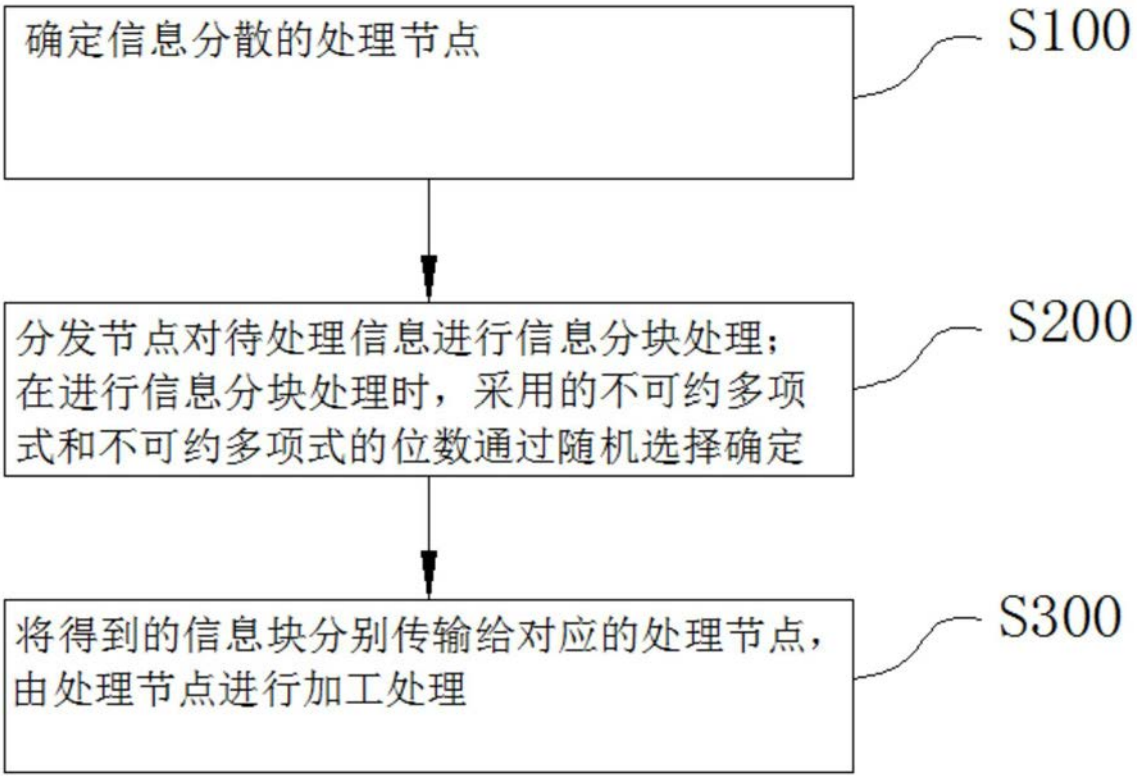

确定信息分散的处理节点
S100
分发节点对待处理信息进行信息分块处理；
在进行信息分块处理时，采用的不可约多项
式和不可约多项式的位数通过随机选择确定
S200
将得到的信息块分别传输给对应的处理节点，
由处理节点进行加工处理
S300

图1