(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 108989031 B
(45)授权公告日 2022.07.01

(21)申请号 201810840812.5

(22)申请日 2018.07.27

(65)同一申请的已公布的文献号
申请公布号 CN 108989031 A

(43)申请公布日 2018.12.11

(73)专利权人 上海扈民区块链科技有限公司
地址 202156 上海市崇明区上海市新河镇新中路786号弄5号345室

(72)发明人 赵运磊 程蕾晓 黄兴忠

(74)专利代理机构 上海专利商标事务所有限公司 31100
专利代理师 陈斌

(51)Int.Cl.
H04L 9/08(2006.01)
H04K 1/00(2006.01)

(56)对比文件
CN 107566121 A,2018.01.09
CN 108173643 A,2018.06.15
Andrew Chi-Chih Yao等.《Privacy-Preserving Authenticated Key-Exchange Over Internet》.《IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY》.2014,第9卷(第1期),全文.

审查员 马晨晨

权利要求书2页 说明书5页

(54)发明名称

一种多比特纠错编码解码方法

(57)摘要

一种多比特纠错编码解码方法。运行发明方法的发送方得到$\sigma_1 \in Z_q$和公共参数params,将$\sigma_1 \in Z_q$和params作为输入运行Con(σ_1,params)得到$k_1 \in Z_k$和$v \in Z_t$,其中k和t为整数且其中之一大于2或小于-2,保密存储k_1,并公开传输v给运行发明方法的接收方。接收方得到$\sigma_2 \in Z_q$,$v \in Z_t$和公共参数params,其中σ_2与σ_1满足$|\sigma_2-\sigma_1|_q \leq d$,将$\sigma_2$,v和params作为输入运行Rec($\sigma_2$,v,params),得到$k_2 \in Z_k$。若$\sigma_2$与$\sigma_1$的距离d满足一定的限制条件,则$k_2=k_1$,双方纠错成功。该技术在网络保密通讯领域具有重要应用。

CN 108989031 B

1.一种多比特纠错编码解码方法;其中,{…}表示一个信息或者数值的集合;这里公共参数params＝{q,k,g,aux},其中q,k,g均为整数;aux是可为空的其它辅助公共参数的集合;对于两个整数i,j,其中i≤j,[i,j]表示整数集{i,i+1,…,j};对于任意正整数a,定义Z_a为Z/aZ,Z_a表示为Z_a＝[0,a-1]或者$Z_a=\left[-\lfloor(a-1)/2\rfloor,\lfloor a/2\rfloor\right]$,其中,对于任意实数b,$\lfloor b\rfloor$表示小于或者等于b的最大整数;

发送方运行一个编码算法Con(•),算法输入包含$\sigma_1\in Z_q$和公共参数params,算法对$\sigma_1\in Z_q$基于params进行编码,输出包含(k_1,v),其中$k_1\in Z_k$,$v\in Z_t$,k和t为整数,其中k大于2或小于-2,这意味着,k_1必为多比特;其中,Con(•)算法运行如下:

⑴计算$\sigma_A\in Z_{q'}$,其中q′是一个整数;其中,σ_A的计算方法包括:从集合[0,α-1]或集合$\left[-\lfloor(\alpha-1)/2\rfloor,\lfloor\alpha/2\rfloor\right]$中均匀随机地选取元素e;计算$\sigma_A=\alpha\sigma_1+e\in Z_{q'}$,其中(I)$\sigma_A=\alpha\sigma_1+e \bmod q'$,或(II)$\sigma_A=\alpha\sigma_1+e \bmod^{\pm} q'$,其中,对于任意整数a和正整数b,a $\bmod^{\pm}$b表示在欧几里得除法中a除以b的唯一的落在$\left[-\lfloor(b-1)/2\rfloor,\lfloor b/2\rfloor\right]$中的余数;

⑵计算$k_1\in Z_k$以及$\tilde{v}\in Z_\beta$;其中,$k_1\in Z_k$计算方法包括:$k_1=\lceil\sigma_A/\beta\rfloor \bmod^{\pm} k$,其中,对于任意实数a,⌈a⌋表示与a最接近的整数;或$k_1\in Z_k$＝[0,k-1]的计算方法包括:

(a)若$\sigma_A\in Z_{q'}$＝[0,q′-1],则令$k_1=\lfloor\sigma_A/\beta\rfloor$;

(b)若$\sigma_A\in Z_{q'}$＝[0,q′-1],则当$\sigma_A-\sigma_A \bmod^{\pm}\beta=k\beta$时,令$k_1$＝0;否则,令$k_1=\lceil\sigma_A/\beta\rfloor$;

(c)若$\sigma_A\in Z_{q'}=\left[-\lfloor(q'-1)/2\rfloor,\lfloor q'/2\rfloor\right]$,则当$\sigma_A$＜0时,令$k_1=\lfloor\sigma_A/\beta\rfloor+k$;否则,令$k_1=\lfloor\sigma_A/\beta\rfloor$;

(d)若$\sigma_A\in Z_{q'}=\left[-\lfloor(q'-1)/2\rfloor,\lfloor q'/2\rfloor\right]$,则当$\sigma_A\geq-\beta/2$时,令$k_1=\lceil\sigma_A/\beta\rfloor$;否则,令$k_1=\lceil\sigma_A/\beta\rfloor+k$;

⑶计算$v\in Z_t$,其中v可以公开发送;其中,$\tilde{v}=\sigma_A \bmod^{\pm}\beta$,$v=\lfloor\tilde{v}g/\beta\rfloor$或$v=\lceil\tilde{v}g/\beta\rfloor$;或$\tilde{v}=\sigma_A \bmod\beta$和$v=\lceil\tilde{v}g/\beta\rfloor$;

接收方运行一个解码算法Rec(•),算法输入包含$\sigma_2\in Z_q$,$v\in Z_t$和公共参数params,其中$|\sigma_2-\sigma_1|_q\leq d$,d为一个整数,对于任意整数a,$|a|_q$定义为min{a mod q,q-a mod q},其中,对于任意整数a和正整数b,a mod b表示在欧几里得除法中a除以b的唯一的落在[0,…,b-1]中的余数,min{•}定义为取最小值;算法对$\sigma_2\in Z_q$,$v\in Z_t$基于params进行解码,输出包含k_2,其中$k_2\in Z_k$;若σ_2与σ_1的距离d满足一定的限制条件,则$k_2=k_1$,双方纠错成功;

其中,Rec(σ_2,v,params)的计算方法包括:(1)$k_2=\lceil\alpha\sigma_2/\beta-v/g\rfloor \bmod k$,或(2)$k_2=\lceil\alpha\sigma_2/\beta-(v+1/2)/g\rfloor \bmod k$,或(3)$k_2=\lceil\alpha\sigma_2/\beta-(v+r)/g\rfloor \bmod k$,其中r是一个实数;

其中,d满足的关系式包含:

(1)(2d+2)k＜q(1-1/g),或

(2)(2d+1)k＜q(1-2γ/g),其中γ定义为max{|r|,|1-r|},对于任意实数a,|a|表示取a的绝对值,max{•}定义为取最大值;

(3)(d+1)k＜q(1/2-γ/g)。

2.如权利要求1所述的方法,其中,aux是包含{q′,α,β}的集合的可为空的子集合,其中q'、α、β为整数。

3.如权利要求1或2所述的方法,其中,q,k,g为正整数,和/或,q′＝lcm(q,k)是q和k的

最小公倍数,和/或,α=q′/q,和/或,β=q′/k,和/或,β≥g均为正整数。

4.如权利要求3所述的方法,其中,r为实数,满足0≤r≤1。

5.如权利要求1或2所述的方法,其中,k,g的取值包含:$k=2^{\kappa_1}$,或$g=2^{\kappa_2}$,其中κ_1,κ_2是正整数;q的取值包含:q是素数,或$q=2^{\kappa_3}$,其中κ_3是正整数,或q=kg。

一种多比特纠错编码解码方法

技术领域

[0001] 本发明涉及纠错编码解码技术,在网络保密通讯领域具有重要应用。

背景技术

[0002] 纠错编码解码是技术是用于解决如下问题:两个用户Alice和Bob各自有一个秘密,发送方Alice得到一个秘密数据$\sigma_1\in Z_q$,接受方Bob得到一个秘密数据$\sigma_2\in Z_q$。这些秘密数据在保密通讯中是利用交换格上的带噪音学习问题实例进行相应计算得到的。但是,$\sigma_1\in Z_q$和$\sigma_2\in Z_q$并不相等,因此并不可以作为密钥进行保密通讯。但是它们的距离比较近,发明方法是解决如何从了两个距离比较近的秘密数据中计算出一个相同的密钥,用于保密通讯。

发明内容

[0003] 运行发明方法的发送方Alice得到$\sigma_1\in Z_q$和公共参数params,将$\sigma_1\in Z_q$和params作为输入运行Con(σ_1,params)得到$k_1\in Z_k$和$v\in Z_t$,保密存储k_1,并公开传输v给运行发明方法的接收方Bob。Bob得到$\sigma_2\in Z_q$,$v\in Z_t$和公共参数params,其中σ_2与σ_1满足$|\sigma_2-\sigma_1|_q\leq d$,将$\sigma_2$,v和params作为输入运行Rec($\sigma_2$,v,params),得到$k_2\in Z_k$。若$\sigma_2$与$\sigma_1$的距离d满足一定的限制条件,则正确性成立,即$k_2=k_1$,双方纠错成功,生成共同的密钥$k_2=k_1$。该技术在网络保密通讯领域具有重要应用。

[0004] 本发明给出一种高效的多比特纠错编码解码方法;其中,{…}表示一个信息或者数值的集合;这里公共参数params={q,k,g,aux},其中q,k,g均为整数;aux包含运行发明方法的可为空的其它辅助公共参数的集合;对于两个整数i,j,其中$i\leq j$,[i,j]表示整数集{i,i+1,…,j};对于任意正整数a,定义Z_a为Z/aZ,Z_a表示为$Z_a=[0,a-1]$或者$Z_a=\left[-\lfloor (a-1)/2\rfloor,\lfloor a/2\rfloor\right]$,其中,对于任意实数b,$\lfloor b\rfloor$表示小于或者等于b的最大整数;

[0005] 运行发明方法的发送方运行一个编码算法Con(•),算法输入包含$\sigma_1\in Z_q$和公共参数params,算法对$\sigma_1\in Z_q$基于params进行编码操作,输出包含(k_1,v),其中$k_1\in Z_k$,$v\in Z_t$,k和t为整数且其中之一大于2或小于-2;这意味着,k_1和v其中之一必为多比特(即:无法用一个0-1比特来表示)。在实际的实现中,可以对$\sigma_1\in Z_q$做任何可求逆的变换,比如对其平移一定的量(即:加或减去一个数等),此时Rec对$\sigma_2\in Z_q$做相应的逆变换。

[0006] 运行发明方法的发送方运行Con(σ_1,params)得到$k_1\in Z_k$和$v\in Z_t$后,可另外使用一层纠错码加密算法Encode加密f(k_1)得到Encode(f(k_1)),其中,f是关于k_1的函数,然后计算v'=f'(Encode(f(k_1)),k_1),其中,f'是关于f(k_1),k_1的函数,并公开传输v,v'给运行发明方法的接收方Bob。

[0007] 运行发明方法的接受者有一个保密输入$\sigma_2\in Z_q$,收到发送方发送过来的$v\in Z_t$,检查$v\in Z_t$,若$v\in Z_t$则运行一个解码算法,算法输入包含$\sigma_2\in Z_q$,$v\in Z_t$和公共参数params,其中$|\sigma_2-\sigma_1|_q\leq d$,对于任意整数a,$|a|_q$定义为min{a mod q,q-a mod q},其中,对于任意整数a和正整数b,a mod b表示在欧几里得除法中a除以b的唯一的落在[0,…,b-1]中的余数,min

{•}定义为取最小值;$d=f_d(q,k,g)$,f_d是关于q,k,g的函数;算法对$\sigma_2\in Z_q$,$v\in Z_t$基于params进行解码,输出包含k_2,其中$k_2\in Z_k$,满足$k_2=k_1$。

[0008] 运行发明方法的接收方Bob运行$Rec(\sigma_2,v,params)$,得到$k_2\in Z_k$。若σ_2与σ_1的距离d满足一定的限制条件,则正确性成立,即$k_2=k_1$,双方纠错成功,生成$k_2=k_1$。即便σ_2与σ_1的距离超出d或传输过程引入的噪音缘故,接收方仍可使用纠错码解密算法Decode解密$f''(k_2,v')$得到$Decode(f''(k_2,v'))=f(k_1)$,其中,f″是关于$k_2$,v'的函数,双方纠错成功,生成共同的密钥$f(k_1)$。

具体实施方式

[0009] 本发明给出一种高效的纠错编码解码方法;其中,{…}表示一个信息或者数值的集合;这里公共参数params={q,k,g,aux},其中q,k,g均为整数;辅助参数aux是包含{q′,α,β}的集合的可为空的子集合,其中$q'=f_1(q,k,g)$,$\alpha=f_2(q,k,g)$,$\beta=f_3(q,k,g)$,f_1,f_2,f_3是关于q,k,g的函数;假定公共参数params是固定的并被运行发明方法的用户事先获知;或者,在发明方法运行之前交换和协商这些参数并达成一致。在基于LWE的密钥协商协议当中,这些参数主要是由LWE问题来决定。对于两个整数i,j,其中i≤j,[i,j]表示整数集{i,i+1,…,j};对于任意正整数a,定义Z_a为Z/aZ,在本发明所在的技术领域,Z_a表示为$Z_a=[0,a-1]$或者 $Z_a=\left[-\lfloor (a-1)/2\rfloor,\lfloor a/2\rfloor\right]$,其中,对于任意实数b,$\lfloor b\rfloor$表示小于或者等于b的最大整数,「b」表示与b最接近的整数,且$\lfloor b+1/2\rfloor$=「b」。

[0010] 运行发明方法的发送方运行一个编码算法Con(•),算法输入包含$\sigma_1\in Z_q$和公共参数params,输出包含(k_1,v),其中$k_1\in Z_k$,$v\in Z_t$,$t=f(\beta,g)$,f是关于β,g的函数;算法运行如下:

[0011] ⑴计算$\sigma_A\in Z_{q'}$;

[0012] ⑵计算$k_1\in Z_k$以及$\tilde{v}\in Z_\beta$;

[0013] ⑶计算$v\in Z_t$;

[0014] 运行发明方法的发送方运行$Con(\sigma_1,params)$得到$k_1\in Z_k$和$v\in Z_t$后,可另外使用一层纠错码加密算法Encode加密$f(k_1)$得到$Encode(f(k_1))$,其中,f是关于k_1的函数,然后计算$v'=f'(Encode(f(k_1)),k_1)$,其中,f′是关于$f(k_1)$,$k_1$的函数,并公开传输v,v'给运行发明方法的接收方Bob。

[0015] 运行发明方法的接受者有一个保密输入$\sigma_2\in Z_q$,收到发送方发送过来的$v\in Z_t$,检查$v\in Z_t$,若$v\in Z_t$则运行一个解码算法,算法输入包含$\sigma_2\in Z_q$,$v\in Z_t$和公共参数params,其中$|\sigma_2-\sigma_1|_q\leq d$,对于任意整数a,$|a|_q$定义为min{a mod q,q-a mod q},其中,对于任意整数a和正整数b,a mod b表示在欧几里得除法中a除以b的唯一的落在[0,…,b-1]中的余数,min{•}定义为取最小值;$d=f_d(q,k,g)$,f_d是关于q,k,g的函数;输出包含k_2,其中$k_2\in Z_k$,满足$k_2=k_1$。

[0016] 运行发明方法的接收方Bob运行$Rec(\sigma_2,v,params)$,得到$k_2\in Z_k$。若σ_2与σ_1的距离d满足一定的限制条件,则正确性成立,即$k_2=k_1$,双方纠错成功,生成$k_2=k_1$。即便σ_2与σ_1的距离超出d或传输过程引入的噪音缘故,接收方仍可使用纠错码解密算法Decode解密$f''(k_2,v')$得到$Decode(f''(k_2,v'))=f(k_1)$,其中,f″是关于$k_2$,v'的函数,双方纠错成功,生成共同

的密钥$f(k_1)$。

[0017] 如上所述的方法，其中，q,k,g为正整数，和/或，$q'=\mathrm{lcm}(q,k)$是q和k的最小公倍数，和/或，$\alpha=q'/q$，和/或，$\beta=q'/k$，和/或，$\beta\geq g$均为正整数。当然，在发明方法的实际应用中，q'、α、β、t还可以是q、k、g的其它函数和变换，比如：q'是lcm(q,k)的一个函数或变换，α是q'/q的一个函数或变换，β是q'/k的一个函数或变换。

[0018] 如上所述的方法，其中，σ_A是$Z_{q'}$上的随机分布或均匀分布，或者σ_A可以有效地转换为$Z_{q'}$上的均匀分布。

[0019] 如上所述的方法，其中，σ_A的计算方法包括：从集合[0,α-1]或集合$[-\lfloor(\alpha-1)/2\rfloor,\lfloor\alpha/2\rfloor]$中均匀随机地选取元素e；计算$\sigma_A=\alpha\sigma_1+e\in Z_{q'}$。

[0020] 如上所述的方法，其中，$\sigma_A=\alpha\sigma_1+e\in Z_{q'}$的计算方法包括：

[0021] (1)$\sigma_A=\alpha\sigma_1+e \bmod q'$，或

[0022] (2)$\sigma_A=\alpha\sigma_1+e \bmod^{\pm} q'$，其中，对于任意整数a和正整数b，$a \bmod^{\pm} b$表示在欧几里得除法中a除以b的唯一的落在$\left[-\lfloor(b-1)/2\rfloor,\lfloor b/2\rfloor\right]$中的余数。

[0023] 如上所述的方法，其中，$k_1=h_1(\sigma_A,\alpha,\beta,k)$，$\tilde{v}=h_2(\sigma_A,\alpha,\beta,k)$，$h_1,h_2$是关于$\sigma_A,\alpha,\beta,k$的函数。一般而言，$h_1$输出的是$\sigma_A$关于公共参数的高位信息，而$h_2$输出的是$\sigma_A$关于公共参数的低位信息，或者二者的输出相反。

[0024] 如上所述的方法，其中，$k_1\in Z_k$计算方法包括：$k_1=\lfloor\sigma_A/\beta\rfloor \bmod k$或者$k_1=\lceil\sigma_A/\beta\rceil \bmod^{\pm} k$；和/或，$\tilde{v}\in Z_\beta$的计算方法包括：$\tilde{v}=\sigma_A \bmod \beta$或者$\tilde{v}=\sigma_A \bmod^{\pm} \beta$。

[0025] 如上所述的方法，其中，$k_1\in Z_k=[0,k-1]$的计算方法包括：

[0026] (1)若$\sigma_A\in Z_{q'}=[0,q'-1]$，则令$k_1=\lfloor\sigma_A/\beta\rfloor$；

[0027] (2)若$\sigma_A\in Z_{q'}=[0,q'-1]$，则当$\sigma_A-\sigma_A \bmod^{\pm}\beta=k\beta$时，令$k_1=0$；否则，令$k_1=\lceil\sigma_A/\beta\rceil$；

[0028] (3)若$\sigma_A\in Z_{q'}=\left[-\lfloor(q'-1)/2\rfloor,\lfloor q'/2\rfloor\right]$，则当$\sigma_A<0$时，令$k_1=\lfloor\sigma_A/\beta\rfloor+k$；否则，令$k_1=\lfloor\sigma_A/\beta\rfloor$；

[0029] (4)若$\sigma_A\in Z_{q'}=\left[-\lfloor(q'-1)/2\rfloor,\lfloor q'/2\rfloor\right]$，则当$\sigma_A\geq -\beta/2$时，令$k_1=\lceil\sigma_A/\beta\rceil$；否则，令$k_1=\lceil\sigma_A/\beta\rceil+k$。

[0030] 如上所述的方法，其中，$v=h(\tilde{v},g,\beta)$，h是关于$\tilde{v}$,g,β的函数。一般而言，v是σ_A关于公共参数的低位信息。

[0031] 如上所述的方法，其中，$v\in Z_t$的计算方法包括：

[0032] (1)$v=\lfloor\tilde{v}g/\beta\rfloor$，或

[0033] (2)$v=\lceil\tilde{v}g/\beta\rceil$。

[0034] 如上所述的方法，其中，$v\in Z_t$中t的取值包含：t=g或t=g+1。一般而言，t是g的一个函数(比如，对g做平移操作)。

[0035] 如上所述的方法，其中，解码算法$\mathrm{Rec}(\sigma_2,v,\mathrm{params})=h_R(\sigma_2,v,q,k,g)$，$h_R$是关于$\sigma_2,v,q,k,g$的可有效计算的函数。

[0036] 如上所述的方法，其中，Rec(σ_2,v,params)的计算方法包括：

[0037] (1)$k_2=\lceil \alpha\sigma_2/\beta-v/g \rfloor \bmod k$，或

[0038] (2)$k_2=\lceil \alpha\sigma_2/\beta-(v+1/2)/g \rfloor \bmod k$，或

[0039] (3)$k_2=\lceil \alpha\sigma_2/\beta-(v+r)/g \rfloor \bmod k$，其中r是一个实数。

[0040] 如上所述的方法，其中，d满足的关系式包含：

[0041] (1)$(2d+1)k<q(1-1/g)$，或

[0042] (2)$(2d+2)k<q(1-1/g)$，或

[0043] (3)$(2d+1)k<q(1-2\gamma/g)$，其中γ定义为$\max\{|r|,|1-r|\}$，对于任意实数a，|a|表示取a的绝对值，max{•}定义为取最大值。

[0044] (4)$(d+1)k<q(1/2-\gamma/g)$。

[0045] 如上所述的方法，其中，实数$r\in[0,1]$。

[0046] 如上所述的方法，其中，k,g的取值包含：$k=2^{\kappa_1}$，或$g=2^{\kappa_2}$，其中κ_1,κ_2是正整数；q的取值包含：q是素数，或$q=2^{\kappa_3}$，其中κ_3是正整数，或$q=kg$。

[0047] 在发明方法的实际应用中，示例的Con和Rec具体实施方式如下：示例实施方式一：

[0048] Con(σ_1,params)：

[0049] 1.从集合$\left[-\lfloor(\alpha-1)/2\rfloor,\lfloor\alpha/2\rfloor\right]$中均匀随机地选取元素e；

[0050] 2.计算$\sigma_A=\alpha\sigma_1+e \bmod q'$；

[0051] 3.当$\sigma_A-\sigma_A \bmod^{\pm}\beta=k\beta$时，令$k_1=0$；否则，令$k_1=\lceil\sigma_A/\beta\rfloor$；

[0052] 4.计算$\tilde{v}=\sigma_A \bmod^{\pm}\beta$；

[0053] 5.计算$v=\lceil\tilde{v}g/\beta\rfloor$；

[0054] 6.保密存储k_1，公开传输v；

[0055] Rec(σ_1,v,params)：

[0056] 1.$k_2=\lceil\alpha\sigma_2/\beta-v/g\rfloor \bmod k$；

[0057] 2.保密存储k_2。

[0058] 其中，示例的参数取值包括：

[0059] (1)β,g取偶数且$g\leq\beta\leq 2g$。

[0060] (2)β,g取奇数。

[0061] 示例实施方式二：

[0062] Con(σ_1,params)：

[0063] 1.从集合$\left[-\lfloor(\alpha-1)/2\rfloor,\lfloor\alpha/2\rfloor\right]$中均匀随机地选取元素e；

[0064] 2.计算$\sigma_A=\alpha\sigma_1+e \bmod q'$；

[0065] 3.当$\sigma_A-\sigma_A \bmod^{\pm}\beta=k\beta$时，令$k_1=0$；否则，令$k_1=\lceil\sigma_A/\beta\rfloor$；

[0066] 4.计算$\tilde{v}=\sigma_A \bmod^{\pm}\beta$；

[0067] 5.计算$v=\lfloor\tilde{v}g/\beta\rfloor$；

[0068] 6.保密存储k_1，公开传输v；

[0069] Rec(σ_1,v,params)：

[0070] 1.$k_2=\lceil\alpha\sigma_2/\beta-(v+1/2)/g\rfloor \bmod k$；

[0071] 2.保密存储k_2。

[0072] 其中,示例的参数取值包括:

[0073] ⑴β取偶数,g取奇数,且g≤β≤2g。

[0074] ⑵β取奇数,g取偶数。当β是素数时,这是较佳的实施方式。