DOI:10.13878/j.cnki.jnuist.2017.05.009

张锐[1,2]　谭高升[1,2]　马晖[1,2]　陶杨[1,2]

支持全同态密文计算的访问控制加密方案

摘要

提出支持全同态密文计算的访问控制加密(FH-ACE)方案,并给出基于带错学习(Learning with Error)困难性问题的具体构造.首先,根据全同态加密(Fully Homomorphic Encryption)概念和访问控制加密(Access Control Encryption)概念,给出支持全同态密文计算的访问控制加密方案的定义以及需要满足的安全模型;其次,提出以满足特定条件的全同态加密方案为基本模块的黑盒构造,并分析基于目前的全同态加密方案,具体构造所面临的困难点以及解决方法;最后,基于带错学习困难性问题,给出支持全同态密文计算的访问控制加密方案的具体构造.

关键词

访问控制加密;全同态加密;带错学习;密文计算

中图分类号 TN918.4

文献标志码 A

收稿日期 2017-07-09

资助项目 国家自然科学基金(61632020,61602468);浙江省科技厅重点研发计划(2017C01062)

作者简介

张锐,男,博士,研究员,博士生导师,研究方向为信息安全.r-zhang@iie.ac.cn

1 中国科学院 信息工程研究所 信息安全国家重点实验室,北京,100093

2 中国科学院大学 网络空间安全学院,北京,100093

0 引言

访问控制加密[1]是一种新的密码原语,它不仅实现对发送消息的加密保护,而且控制发送者的消息发送权限.这与传统的基于属性的加密方案[2-4]不同,传统的基于属性的加密方案只对解密者的身份进行控制,而不限制消息发送者的发送权限.另一方面,全同态加密[5-9]是近些年密码学研究的热点,其主要实现数据的密文操作.由于这两种加密具有重要的应用价值,因此,构造同时具有访问控制加密和全同态加密功能的加密方案显得更具意义,我们将其称为支持全同态密文计算的访问控制加密(FH-ACE).FH-ACE 非常适合保护大数据的安全性,其既可以保护数据在传输中的机密性,又可防止因计算机病毒等原因"腐化"的用户向低权限用户泄露信息,同时可以支持云服务器下对大数据的机密处理.

本文首先提出 FH-ACE 方案的定义及安全模型,再以全同态加密方案为基本模块,给出 FH-ACE 方案的抽象构造和证明,最后,基于全同态加密中的 GSW 方案[9],给出 FH-ACE 的具体构造.

FH-ACE 的安全模型与 ACE 的安全模型相似,但增加了全同态密文计算预言机(Oracle)查询.因为全同态算法可以公开计算,所以,全同态算法的存在不会增加攻击者的优势.但是,对于多公钥下的全同态加密方案,因为不同公钥间的用户密文可以相互同态计算,而 FH-ACE 安全模型下,敌手可以查询某些密文的明文信息,所以,无法通过不同用户之间的独立性消除全同态计算算法对安全性的影响,加之多公钥全同态加密研究较少,我们暂且不考虑这种情形下的 FH-ACE.为保证 FH-ACE 的安全性,全同态加密方案需要满足特定的性质,我们将在后文详细介绍.

Damgård 等[1]在 2016 年首次提出 ACE 的概念,并基于加法同态性,给出了基于 DDH 和 Paillier 假设的具体构造,但是他们的方案不支持全同态密文计算;之后,Fuchsbauer 等[10]构造了不同谓词策略下,密文长度是用户数量多项式对数复杂度(Polylog)的 ACE 方案.而我们的工作则将全同态计算功能与访问控制加密功能结合起来,构造支持全同态密文计算的访问控制加密方案.

1 FH-ACE 定义与安全模型

记 FH-ACE=(Setup,Gen,Enc,San,Eval,Dec)为支持全同态密文

计算的访问控制加密方案,由于篇幅限制,我们只给出 Eval 算法的定义,其余算法与文献[1]中 ACE 的定义完全相同.

Eval $(f,c_1^*,c_2^*,\cdots,c_k^*)$:输入接收者的接收密文$(c_1^*,c_2^*,\cdots,c_k^*)$和需要计算的函数$f$;输出同态计算后的密文$c^*$,其中$c_i^* \leftarrow \mathrm{San}(rk,\mathrm{Enc}(ek,m_i))$,$i=1,2,\cdots,k$,注意,$c_i^*$为同一接收者的不同密文.

需要注意,当系统中有多个安全接收等级时,发送者生成的密文会有对应数量的"分块"密文.举例来讲,若系统中有三级安全性的接收用户,分别对应Rec_1,Rec_2,Rec_3,则发送者发送的密文为$c=(c_1,c_2,c_3)$,其中,c_j为发给Rec_j的密文,$j=1,2,3$.如果发送者没有权限向Rec_j发送消息,则c_j为从密文空间C中随机选择的一个密文.

下面,我们给出方案正确性和安全性的定义.

定义 1(正确性) 密文c^*有两种来源,一种是 San 处理后的初始密文,一种是 Eval 同态计算后的密文,我们分别对这两种密文的正确性进行定义.

$$\Pr[\mathrm{Dec}(dk,\mathrm{San}(rk,\mathrm{Enc}(ek,m)))\neq m]\leqslant \mathrm{negl}(\lambda), \tag{1}$$

$$\Pr[\mathrm{Dec}(dk,\mathrm{Eval}(f,c_1^*,c_2^*,\cdots,c_k^*))\neq f(m_1,m_2,\cdots,m_k)]\leqslant \mathrm{negl}(\lambda), \tag{2}$$

其中,$\mathrm{negl}(\lambda)$是关于安全参数的可忽略函数.式(1)、(2)的概率来自各个算法的内部随机投币,且dk,rk,ek都由密钥生成算法合法生成.

定义 2(安全性) 将访问控制加密的安全性分为两部分,一类为关于加密信息的机密性问题,称为不可读规则(No-Read-Rule),一类为关于加密用户发送权限问题,称为不可写规则(No-Write-Rule),分别就这两种安全要求进行定义,与文献[1]中的安全性相比,敌手 只增加关于 Eval 算法的查询能力,由于篇幅限制,我们省略安全游戏的详细说明.

No-Read-Rule:对任意多项式时间敌手 ,要求$|m_0|=|m_1|$,$i_0,i_1\in\{0,1,\cdots,n\}$,且游戏满足如下两个条件:

1)负载机密性(Payload Privacy):在密钥生成 Oracle($O_{\mathrm{Gen}}(\cdot)$)查询中,任意$q=(j,rec)$,必须满足$P(i_0,j)=0=P(i_1,j)$,即查询的解密私钥不能对挑战密文进行解密.

2)发送者匿名性(Sender Anonymity):在密钥生成 Oracle($O_{\mathrm{Gen}}(\cdot)$)查询中,任意$q=(j,rec)$,必须满足$P(i_0,j)=P(i_1,j)$,此处不要求策略等于 0 意味着即使是合法解密者,也无法获得发送者的身份信息,且要求$m_0=m_1$.

在如上任意一个条件下,如有$b'=b$事件发生,称 赢得 No-Read-Rule 游戏.定义 FH-ACE 满足 No-Read-Rule,如果对任意多项式时间敌手 ,有下面不等式成立:

$$\mathrm{Adv}=|\Pr[\text{ 赢得 No-Read-Rule 游戏}]-\frac{1}{2}|\leqslant \mathrm{negl}(\lambda). \tag{3}$$

No-Write-Rule:将对$O_S(\cdot)$的所有查询$q=(j,t)$构成的集合记作Q_S,对$O_S(\cdot)$和$O_R(\cdot)$的所有查询构成的集合记作Q,I_S为由所有Q_S查询中发送者身份$i\in[n]$构成的集合,即$(i,sen)\in Q_S$,J为由所有Q查询中接收者身份$j\in[n]$构成的集合,即$(j,rec)\in Q$.

要求如下条件成立:1)$(n+1,san)\notin Q$;2)$i'\in I_S\cup\{0\}$;3)$\forall i\in I_S,\forall j\in J,P(i,j)=0$.

在满足上面三个条件下,如有$b'=b$事件发生,称敌手 赢得 No-Write-Rule 游戏.定义 FH-ACE 满足 No-Write-Rule,如果对任意多项式时间敌手 ,有下面不等式成立:

$$\mathrm{Adv}=|\Pr[\text{ 赢得 No-Write-Rule 游戏}]-\frac{1}{2}|\leqslant \mathrm{negl}(\lambda). \tag{4}$$

2 基于全同态加密的 FH-ACE 黑盒构造

本章将给出基于全同态加密的 FH-ACE 黑盒构造.全同态加密方案需满足如下两个条件(充分条件):1)全同态加密方案的明文空间是超多项式规模;2)全同态加密方案任意消息的密文分布与密文空间上的均匀分布计算不可区分.

作为构造 FH-ACE 的基本模块,要求全同态加密方案有更强的安全性,即任意消息的密文分布都与密文空间的均匀分布不可区分,称其为"均匀不可区分性".

定义 3(均匀不可区分性) 任取消息$m\in$,记m的密文分布为$\chi_m=\mathrm{Enc}(pk,m)$,概率来自加密算法的随机数,设$X_m$是$\chi_m$上的随机变量,即$X_m\leftarrow\chi_m$,记$U$是方案密文空间$C$上的均匀随机变量,如果$X_m\approx_c U$,即任意消息的密文分布与密文空间上的均匀分布不可区分,则称方案满足均匀不可区分性.

设(FH.SKGen,FH.PKGen,FH.Enc,FH.Eval,FH.Dec)是满足条件 1)、2)(均匀不可区分性)的全同态加密方案,以其作为基本方案,构造 FH-ACE 方案.为了描述简单,首先构造只有单个发送者和单个

接收者的 FH-ACE 方案 1-FH-ACE = (1-Setup, 1-Gen, 1-Enc, 1-Eval, 1-Dec),此时,设发送策略为 $P(1,1)=1$.对于构造多个发送者和多个接收者的 FH-ACE 方案,可以使用文献[1]的思想,重复使用多个 1-FH-ACE 方案,此方法的缺点是密文长度随用户的个数成线性增长.

1-Setup(1^λ, P):输入安全参数和发送策略,调用 $sk \leftarrow$FH.SKGen(1^λ)和(pk,τ)$\leftarrow$FH.PKGen(sk),τ 为全同态计算辅助信息.从全同态加密方案的明文空间随机选取一个值 $\beta \leftarrow$;主私钥 $msk=(\beta,sk)$,系统参数 $pp=(P,pk,\tau)$.此时,发送者的密文空间为两个全同态加密方案的直积 $_{FE}\times$ $_{FE}$,加密权限管理者的密文空间为全同态加密方案的密文空间 $_{FE}$.下面的算法都会包含系统参数 $pp=(P,pk,\tau)$,为了简洁,我们将其省略不写.

1-Gen(msk,i,t):输入系统主私钥 msk,用户身份 $i\in\{1,2\}$,其中 2 特指加密权限管理者的身份,以及用户属性 $t\in\{sen,rec,san\}$,根据输入,分别对应如下输出:

- 1-Gen(msk,1,sen)输出发送者 1 的加密密钥 $ek_1=\beta$.
- 1-Gen(msk,1,rec)输出接收者 1 的解密密钥 $dk_1=sk$.
- 1-Gen(msk,2,san)输出加密权限管理者 San 的权限私钥 $rk=-\beta$.

1-Enc($ek_1=\beta,m$):输入发送者的加密私钥 ek_1,传输消息 $m\in$;输出密文 $c=(c_1,c_2)=$(FH.Enc$_{pk}$(β),FH.Enc$_{pk}$(m))$\in$ $_{FE}\times$ $_{FE}$.其中 FH.Enc$_{pk}$(·)是全同态加密方案的加密算法.

1-San($rk=-\beta,c$):输入加密权限管理者的权限密钥 rk,发送者发送的密文 c;输出处理后的密文 $c^*\in$ $_{FE}$.首先,计算密文 $c_3=$FH.Enc$_{pk}$($-\beta$),其次,从全同态加密方案的明文空间选择任意的随机数 r,计算 $c^*=r\circ(c_1\oplus c_3)\oplus c_2$,其中$\circ$表示密文的数乘运算,$\oplus$表示密文的同态加法运算.

1-Eval($f,c_1^*,c_2^*,\cdots,c_k^*$):输入接收者的接收密文($c_1^*,c_2^*,\cdots,c_k^*$)和希望对密文进行的操作函数 f,调用全同态加密方案的同态计算算法 $c^*\leftarrow$FH.Eval($f,c_1^*,c_2^*,\cdots,c_k^*,\tau$);输出同态计算后的密文 c^*,其中 $c_i^*\leftarrow$San(rk,Enc(ek_1,m_i)),$i=1,2,\cdots,k$.

1-Dec($dk_1=sk,c^*$):输入接收的密文 c^* 和解密密钥 $dk=sk$,调用全同态加密方案的解密算法 $m'\leftarrow$FH.Dec(sk,c^*);输出解密消息 $m'\in M\cup\{\perp\}$.其中$\{\perp\}$表示对于一些非法密文,解密可以失败.

下面对方案的正确性和安全性进行分析.

定理 1(1-FH-ACE 正确性) 如果全同态加密方案满足正确性要求,则 1-FH-ACE 方案也满足定义 1 的正确性要求.

证明 显然.

定理 2(1-FH-ACE 安全性) 如果构造 1-FH-ACE 方案的全同态加密方案满足条件:1)全同态加密方案的明文空间是超多项式规模;2)全同态加密方案满足均匀不可区分性安全定义.则 1-FH-ACE 是安全的,即满足 No-Read-Rule 和 No-Write-Rule 的安全要求.

证明 首先证明方案满足 No-Read-Rule 的安全性要求,即方案满足 Payload Privacy 和 Sender Anonymity.

Payload Privacy:因为方案中只有一个发送者和一个接收者,所以$(i_0,i_1)\in\{0,1\}\times\{0,1\}$,我们分两种情况证明.

1) $(i_0,i_1)=(0,0)$,显然,此时对 m_0,m_1 的挑战密文均是从密文空间中均匀随机选取,与 m_0,m_1 独立,所以,即使敌手 询问解密密钥 dk_1,也无法获得 m_0,m_1 的信息,所以,此时敌手的优势为 0,即 Adv =0.

2) $(i_0,i_1)\neq(0,0)$,根据条件要求,询问解密私钥的身份 j 与挑战身份 i_0,i_1 的关系为 $P(i_0,j)=0=P(i_1,j)$,所以,敌手 此种情况无法查询解密密钥 Oracle.此时由 m_0 或者 m_1 产生的挑战密文或者是正常生成的全同态加密密文,或者从全同态加密方案的密文空间中均匀随机选取,由全同态加密方案满足均匀随机性的安全定义,此时 m_0 和 m_1 对应的挑战密文是不可区分的,即 Adv $\leqslant$negl(λ).

Sender Anonymity:同样$(i_0,i_1)\in\{0,1\}\times\{0,1\}$,且 $m_0=m_1$,对解密私钥 Oracle 查询的身份要求为 $P(i_0,j)=P(i_1,j)$,所以分三种情况进行讨论.

1) $(i_0,i_1)=(0,0)$,这种情况与 Payload Privacy 的情形相同,ek_1 的密文从全同态加密方案的密文空间均匀随机选取,与挑战身份无关,而消息的密文部分则完全相同,所以,敌手的优势为 0,即 Adv =0.

2) $(i_0,i_1)=(1,1)$,此时,挑战密文是合法生成的密文,且敌手可以询问解密密钥 dk_1,但是,此时加密密钥 ek_1 和加密消息 m 在两个挑战密文中是完全相同的,所以,敌手的优势同样为 0,即 Adv =0.

3) $i_0\neq i_1$,不妨设 $i_0=0,i_1=1$,由限制条件 $P(i_0,$

$j)=P(i_1,j)$,此时敌手不能询问解密私钥 dk_1,所以对 $b=0$ 时的挑战密文、加密私钥的密文从全同态加密方案的密文空间均匀随机选取,消息的密文正常生成;$b=1$ 时的挑战密文中,加密私钥的密文为 ek_1,消息的密文正常生成.根据全同态加密方案的均匀不可区分性,敌手的优势是可以忽略的,即 Adv $\leqslant$ negl(λ).

通过以上证明,可以得到构造的 1-FH-ACE 方案满足 No-Read-Rule 安全.下面,再证明方案是 No-Write-Rule 安全的.

根据 No-Write-Rule 中集合 I_S 的取值分情况讨论.因为 I_S 是由密钥生成 Oracle O_S 查询中发送者身份构成的集合,且方案只有一个发送者,所以 I_S 的取值只有两种情况,$I_S=\{1\}$ 或 $I_S=\varnothing$,即要么在 O_S 查询中询问发送者的私钥 ek_1,要么不询问发送者的发送私钥.对于 O_R 中是否询问 ek_1 对攻击目标没有影响,所以不做限制.

1) $I_S=\{1\}$:根据 No-Write-Rule 定义中的相关描述,攻击目标(c,i')中的 $i'\in I_S\cup\{0\}$ 所以 $i'\in\{1,0\}$;根据条件 3)的限制,对 $\forall i\in I_S$, $\forall j\in J$,都有 $P(i,j)=0$,所以敌手　不能查询解密私钥 dk_1.此时,无论 $b=0$ 还是 $b=1$,算法 San 的输入密文或者从全同态加密方案两个密文空间的直积 $C_{FE}\times C_{FE}$ 中均匀随机选择,或者通过 ek_1 合法生成密文.又挑战密文为$c'=r\circ(c_1\oplus c_3)\oplus c_2$,其中 $c_3=$FH.Enc$(-\beta)$,由于敌手不具有解密私钥 dk_1,根据 c_3 与密文空间上的均匀分布不可区分性,显然,无论 $b=0$ 还是 $b=1$,c'与全同态加密方案密文空间上的均匀分布不可区分,所以,敌手区分的优势是可忽略的,即 Adv $\leqslant$negl(λ).

2) $I_S=\varnothing$:利用如上的分析方式,得到 $i'\in\{0\}$,敌手在生成攻击目标时,可以查询解密私钥 dk_1,在后期 O_R 查询中,可以获得加密私钥 ek_1,但是,ek_1 同样不会对攻击目标带来影响,所以,ek_1 不会增加敌手攻击的优势.下面证明,即使敌手拥有 dk_1,其仍然无法对挑战密文 c'进行区分.此时,我们不能简单判定敌手的攻击密文仍是从全同态密文空间均匀随机选择的两个密文,而且,敌手完全可以对挑战密文 c'进行解密.为了证明此时 San 在 $b=0$ 和 $b=1$ 下生成的挑战密文对于敌手仍是不可区分的,只需要证明此种情形下,除可忽略的概率之外,San 的输出与输入是独立的,即 San 可以把输入的密文转化成任意消息的任意密文.设 San 输入密文中,加密私钥为 β'',加密的消息为 m''(无论来自敌手还是来自挑战者生成的密文),则 San 输出的密文和密文对应的消息分别为 $c'=r\circ(c_1\oplus c_3)\oplus c_2$, $m'=r(\beta''-\beta)+m''$.

因为全同态加密方案的密文空间是超多项式的,所以,$\beta''=\beta$ 概率是可忽略的,再由 r 的任意性可知,m'可以是任意消息.其次,根据全同态加密方案的均匀不可区分性,c_3 在全同态密文空间中与均匀分布不可区分,所以 c'在全同态加密方案的密文空间中与其上的均匀分布不可区分,即与(c_1,c_2)无关.所以,除了可忽略的概率之外,San 的输出与输入是独立的.至此,我们证明了以上方案满足 No-Write-Rule 安全性.

以上证明构造的方案满足 No-Read-Rule 和 No-Write-Rule 安全性要求,定理 2 证毕.

3　基于 LWE 的 FH-ACE 的具体构造

设(GSW.SKGen, GSW.PKGen, GSW.Enc, GSW.Eval, GSW.Dec)为 GSW 方案[9]的相应算法,以此算法为基本模块,可以实例化构造 FH-ACE.首先给出 GSW 方案性质描述:

引理 1(正确性)　设密文 $\boldsymbol{C}=$ Flatten$(\mu\boldsymbol{I}_N+$ BitDecomp$(\boldsymbol{RA}))$ 由方案中的算法合法生成,$\boldsymbol{e}\leftarrow\chi^m$, $\boldsymbol{v}=$Powerof2 $(\boldsymbol{s})$,如果 $\|\boldsymbol{e}\|_1\leqslant\frac{q}{8}$,则方案可以正确解密.

证明　对消息 $\mu\in\{0,1\}$ 的情形进行分析,其他情形可以参考[9].解密算法计算 $\boldsymbol{Cv}=\mu\boldsymbol{v}+\boldsymbol{R}\cdot\boldsymbol{e}$,设 $v_i\in\left(\frac{q}{4},\frac{q}{2}\right]$,取 $\boldsymbol{C}$ 的第 i 行 $\boldsymbol{C}_i$,得 $x_i=\langle\boldsymbol{C}_i,\boldsymbol{v}\rangle=\mu v_i+\langle\boldsymbol{R}_i,\boldsymbol{e}\rangle$,误差项 $|\langle\boldsymbol{R}_i,\boldsymbol{e}\rangle|\leqslant\|\boldsymbol{e}\|_1\leqslant\frac{q}{8}$,所以 $\left[\frac{x_i}{v_i}\right]=\left[\frac{\mu v_i+\langle\boldsymbol{R}_i,\boldsymbol{e}\rangle}{v_i}\right]=\left[\mu+\frac{\langle\boldsymbol{R}_i,\boldsymbol{e}\rangle}{v_i}\right]$,　又 $\left|\frac{\langle\boldsymbol{R}_i,\boldsymbol{e}\rangle}{v_i}\right|<\frac{1}{2},\mu\in\{0,1\}$,所以 $\left[\frac{x_i}{v_i}\right]=\mu$, $\left[\frac{x_i}{v_i}\right]$ 表示对内部实数近似取整.

引理 2(安全性 Lemma 1[9])　设参数 $params=(n,q,\chi,m)$ 的设置满足 LWE 困难性问题假设,且矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{R}$ 按照方案中的方式生成,则联合分布$(\boldsymbol{A},\boldsymbol{RA})$ 与密文空间 $Z_q^{m\times(n+1)}\times Z_q^{N\times(n+1)}$ 上的均匀分布计算不可区分.

引理的证明非常简单,这里不再赘述.通过论述可知,GSW 方案显然满足定理 1 与定理 2 的要求,所以有如下推论:

推论 1　GSW 方案可以作为构造支持全同态密

文计算的访问控制加密方案的基本方案:

通过观察分析,GSW 类方案(目前存在许多关于 GSW 方案的变形)可能是构造 FH-ACE 方案的最佳选择,其他方案主要受限于支持的明文空间不是超多项式规模,无法保证方案加密密钥的安全性.对于定理 2 所要求的均匀不可区分性,只是构造方案的充分条件之一,而寻找构造 FH-ACE 的全同态方案所满足的充要条件,则需要进一步研究.

4 结束语

本文构造了一种新的密码学原语,支持全同态密文操作的访问控制加密(FH-ACE),此处的访问控制加密与已有的基于属性的加密不同,其既可以保护传输消息的机密性,又可以控制消息发送者的发送权限,而后者是基于属性的加密方案所不具备的.本文首先提出了支持全同态密文操作的访问控制加密方案的定义与安全模型,然后给出作为基本模块的全同态加密方案需要满足的性质,并给出 FH-ACE 的抽象构造和证明,最后基于 GSW 方案,给出方案的具体构造和分析.

参考文献

References

[1] Damgård I, Haagh H, Orlandi C. Access control encryption: Enforcing information flow with cryptography [C] // Theory of Cryptography Conference, 2016: 547-576

[2] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C] // ACM conference on Computer and Communications Security, 2006: 89-98

[3] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization [C] // International Conference on Practice and Theory in Public Key Cryptography, 2011: 53-70

[4] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C] // IEEE Symposium on Security and Privacy, 2007: 321-334

[5] Gentry C. Fully homomorphic encryption using ideal lattices [J]. ACM Symposium on Theory of Computing, 2009, 9(4): 169-178

[6] Dijk M V, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers [C] // International Conference on Theory and Applications of Cryptographic Techniques, 2010: 24-43

[7] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE [J]. SIAM Journal on Computing, 2014, 43(2): 831-871

[8] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping [J]. ACM Transactions on Computation Theory, 2014, 6(3): 1-13

[9] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based [C] // Advances in Cryptology-CRYPTO, 2013: 75-92

[10] Fuchsbauer G, Gay R, Kowalczyk L, et al. Access control encryption for equality, comparison, and more [C] // IACR International Workshop on Public Key Cryptography, 2017: 88-118

Access control encryption with fully homomorphic operations on the ciphertext

ZHANG Rui[1,2] TAN Gaosheng[1,2] MA Hui[1,2] TAO Yang[1,2]

1 State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing 100093

2 School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100093

Abstract We propose an access control encryption (ACE) scheme which supports the fully homomorphic operations on the ciphertext, and give a concrete construction from Learning with Error (LWE). Firstly, we show the definition and security model of ACE supporting the fully homomorphic operations under the ciphertext according to the concept of the fully homomorphic encryption (FHE) and ACE. Secondly, we make a black-box construction based on the fully homomorphic encryption which satisfies the certain conditions. Finally, we show a concrete construction based on LWE.

Key words access control encryption; fully homomorphic encryption; learning with error; ciphertext computation