计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2014.20131168
51(12):2593-2603,2014

全同态加密研究动态及其应用概述

刘明洁[1]　　王　安[2]
[1](北京大学北京国际数学研究中心　北京　100871)
[2](清华大学微电子学研究所　北京　100084)
(liumj9705@pku.edu.cn)

Fully Homomorphic Encryption and Its Applications

Liu Mingjie[1] and Wang An[2]
[1](*Beijing International Center for Mathematical Research*, *Peking University*, *Beijing* 100871)
[2](*Institute of Microelectronics*, *Tsinghua University*, *Beijing* 100084)

Abstract　With the development of Internet, especially, the occurrence of the concept of cloud computing, there is an increasing demand for the search and process of encrypted data, which makes the fully homomorphic encryption become more and more important. The concept of fully homomorphic encryption was first introduced by Rivest et al. in 1970s. How to construct such schemes is a hard problem for cryptographers. Until 2009, Gentry presented the first fully homomorphic schemes based on ideal lattice, which is a breakthrough in this field. After that, many cryptographers have done some interesting work which promote the fully homomorphric schemes to be practical in future. Fully homomorphric encryption becomes a very trendy topic in cryptography. This paper discusses the main progress on fully homomorphric schemes including the first homomorphic encryption introduced by Gentry and its optimizations, as well as the fully homorphric schemes based on integer and learning with errors problem (LWE problem). Then, the general application framework of fully homomorphic scheme is provided. Cloud computing, electronic voting and digital watermarking are taken as examples to introduce the significant value of application of fully homomorphric encryption.

Key words　cryptography; public-key cryptography; fully homomorphric encryption; cloud computing; information security

摘　要　随着互联网的发展,尤其是云计算概念的诞生,人们在加密数据搜索与处理等方面的需求日益增加,使得全同态加密变得愈加重要.全同态加密的思想是20世纪70年代Rivest等人首次提出的,如何构造满足全同态性质的体制一直是困扰密码学家的难题,直到2009年Gentry基于理想格提出了第1个全同态加密体制使得该方面的研究取得突破性进展.随后许多密码学家在全同态加密方案的研究上作出了有意义的工作,促进了全同态加密向实用化的发展.对全同态加密的研究动态进行了概要的介绍,包括Gentry提出的第1个全同态加密方案及其优化;基于整数的全同态加密方案;基于LWE问题的全同态加密方案等.随后探讨了全同态加密的一般性应用框架,并以云计算、电子投票、数字水印3个应用为例,介绍了全同态加密的重要应用价值.

收稿日期:2013-08-11;**修回日期**:2014-02-26
基金项目:国家"九七三"重点基础研究发展计划基金项目(2013CB834201);信息保障技术重点实验室开放基金项目(KJ-13-101);中国博士后科学基金面上项目(2013M540786);"十二五"国家密码发展基金密码理论课题(MMJJ201401009);国家自然科学基金项目(61402252)
通信作者:王　安(wanganl@tsinghua.edu.cn)

关键词 密码学;公钥密码学;全同态加密;云计算;信息安全

中图法分类号 TP309.7

1 全同态加密的研究现状

利用同态加密来保护数据的私密性,这个概念最早由 Rivest 等人[1]于 1978 年提出. 该想法的来源是通过加密函数的同态性质,实现对加密后的数据作运算的同时保护数据的私密性. 这个概念被提出之后,密码学家设计出了很多具有同态性质的加密方案,如实现电子投票的体制[2-4]、保密信息检索协议[5-6]等. 近几年,云计算受到广泛关注,而它在实现中遇到的问题之一即是如何保证数据的私密性,全同态加密可以在一定程度上解决这个技术难题.

具体地说同态加密指这样一种加密函数,对明文进行环上的加法和乘法运算再加密,与加密后对密文进行相应的运算,结果是等价的. 由于这个良好的性质,人们可以委托不信任的第三方对数据进行处理,而不泄露信息. 因此,同态加密在云计算、电子政务等方面有重要应用.

具有同态性质的加密函数是指 2 个明文 a,b 满足 $Dec(En(a)\otimes En(b))=a\oplus b$ 的加密函数,其中 En 是加密运算,Dec 是解密运算,$\oplus$,$\otimes$ 分别对应明文和密文域上的运算. 当$\oplus$代表加法时,称该加密为加同态加密. 密码学家设计出很多具有加同态性质的加密体制包括文献[3,7-10]. 当$\otimes$代表乘法时,称该加密为乘同态加密[11]. 2005 年在理论密码学会议(TCC)上,Boneh 等人[12]给出了第 1 个可以同时实现加法和乘法同态的密码体制,该体制可以允许进行任意次的加法运算和一次乘法运算仍然保持同态.

全同态加密指同时满足加同态和乘同态性质,可以进行任意多次加和乘运算的加密函数. 用数学公式来表达,即

$$Dec(f(En(m_1),En(m_2),\cdots,En(m_k)))=f(m_1,m_2,\cdots,m_k), \tag{1}$$

或者写成:

$$f(En(m_1),En(m_2),\cdots,En(m_k))=En(f(m_1,m_2,\cdots,m_k)). \tag{2}$$

如果 f 是任意函数,称为全同态加密. 直到 2009 年,IBM 的研究人员 Gentry[13]第 1 次设计出一个真正的全同态加密体制,即可以在不解密的条件下对加密数据进行任何可以在明文上进行的运算. 使得对加密信息仍能进行深入和无限的分析,而不会影响其保密性. 经过这一突破,存储他人机密电子数据的电脑销售商就能受用户委托来充分分析数据,不用频繁与用户交互,也不必看到任何隐私数据. 同态加密技术将允许公司将敏感的信息储存在远程服务器里,既避免从当地的主机端发生泄密,又依然保证了信息的使用和搜索. 用户也得以使用搜索引擎进行查询并获取结果,而不用担心搜索引擎会留下自己的查询记录.

Gentry[13]的同态加密体制是基于理想格设计的,我们将在下面的章节中对该体制作详细的介绍. 其主要思想是先构造了一个部分同态加密的体制,该体制仅能保证对明文进行较低次数的多项式运算时的同态性,然后利用 Squash 技术降低解密函数的多项式次数,实现 Bootstrapping,通过在不知道密钥的情况下更新密文,从而减少扰动,实现全同态加密. 但该体制在期望的安全强度上远达不到实用的程度.

随后很多密码学家在全同态加密体制的研究方面取得进展. 2010 年 Dijk 等人[14]利用 Gentry 的技术提出了基于整数的全同态加密体制. 该体制比 Gentry 的体制更简洁,但仍不实用. 2010 年 Smart 等人[15]在 PKC 上简化了 Gentry09 体制的实现,但仍然无法实现 Bootstrapping 的步骤. 2011 年 Gentry 等人[16]利用一些技术对 Gentry09 体制的实现作进一步的简化,包括提出了部分同态加密方案的新的密钥生成算法,不需要对整个多项式求逆的优化实现方法、时间空间部分平衡等,减少密钥和密文长度,使得部分参数的实现成为可能.

为了提高全同态加密的效率,2011 年之后密码学家又先后提出了不用 Squash 和 Bootstrapping 的体制[17-18],使得全同态加密继续向实用化靠近.

2 Gentry 基于理想格的全同态加密体制

2.1 Gentry 全同态加密的基本思想

2009 年 Gentry[13]给出了第 1 个全同态加密体制,该体制的构造分为如下 3 步:1)构造一个部分同态加密体制,对加密数据进行次数比较低的多项式的运算时可以保持同态性,即式(2)成立;2)降低解密多项式的次数;3)利用 Bootstrapping 实现全同态

加密.该构造过程的核心是找到一个体制,使得式(2)成立的函数 f 的次数尽量高,而其加密函数的次数尽量低,一旦式(2)中的 f 对解密函数成立,该体制即被称为 Bootstrapping 的,即可以转化成一个全同态加密体制.

Gentry 构造的部分同态加密体制是一个类 GGH[19] 的基于理想格的体制,并且证明了在密钥生成算法恰当的情况下,这个体制的安全性可以归约到理想格上最坏情况的某些困难问题.但这个部分同态加密体制不是 Bootstrapping 的,Gentry 经过在公钥中加一部分秘密密钥的暗示信息,降低解密函数的次数.在稀疏背包问题困难的假设下,这些信息不会影响体制的安全性.

2.2 理想格基础

n 维格是 $\mathbb{R}^n$ 中的离散子集,具体地说是 n 个线性无关向量的整系数线性组合,这 n 个向量称为格的一组基.一个格有很多不同的格基,格基的性质对求解格中困难问题的难度有很大的影响.格的行列式定义为格基 $\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n\}$ 组成的基本体 $P(\boldsymbol{B})=\left\{\sum_{i=1}^{n}x_i\boldsymbol{b}_i:x_i\in[-1/2,1/2)\right\}$ 的体积,记 $\det(L)=vol(P(\boldsymbol{B}))$,行列式是对格基的不变量.

$f(x)$ 是一个 n 次整系数不可约多项式,通常取 $f(x)=x^n+1$,n 是 2 的方幂.R 是整系数多项式模多项式 $f(x)$ 得到的环,$R=\mathbb{Z}[x]/(f(x))$.每个环里的元素是次数不超过 $n-1$ 的多项式,因此可以表示成 $\mathbb{Z}^n$ 中的一个向量.I 是 R 中的一个理想即对 R 中元素加法和乘法有封闭性.因此 I 中的元素构成一个格,称为理想格.R 中的一个元素 $\boldsymbol{v}$ 生成的理想对应的格可以由这样一组向量生成:

$$\boldsymbol{v}_i=\boldsymbol{v}\times x^i \bmod f(x):i\in[0,n-1].$$

2.3 Gentry 的部分同态加密体制

Gentry 的部分同态加密体制是一种 GGH 类基于理想格的体制.公钥是一个理想格 J 的随机的"坏"格基 $\boldsymbol{B}_{pk}$ 和一个小的理想 I 的格基 $\boldsymbol{B}_I$(用来将明文转换成扰动变量).比如 $I=(2)$,即所有系数为偶数的向量集合.

通过将明文处理成扰动变量,密文是一个距离理想格 J 很近的向量.具体地说,明文空间是 $\{0,1\}$,将 0 编码成 0^n,1 编码成 0^n1,即将明文嵌入到 $R/I=\{0,1\}^n$ 中.对编码后的明文 $\boldsymbol{m}\in\{0,1\}^n$,我们选择一个随机的短向量 $\boldsymbol{r}$,计算 $\boldsymbol{e}=2\boldsymbol{r}+\boldsymbol{m}$,输出密文 $\boldsymbol{c}\leftarrow\boldsymbol{e} \bmod \boldsymbol{B}_{pk}$.

体制中的私钥(J 的好的格基)是一个短向量 $\boldsymbol{w}\in J^{-1}$,解密过程就是计算 $\boldsymbol{w}\times\boldsymbol{c}$ 的分数部分.由于 $\boldsymbol{c}=\boldsymbol{j}+\boldsymbol{e}$,其中 $\boldsymbol{j}\in J$,所以有 $\boldsymbol{w}\times\boldsymbol{c}=\boldsymbol{w}\times\boldsymbol{j}+\boldsymbol{w}\times\boldsymbol{e}$.而 $\boldsymbol{w}\times\boldsymbol{j}$ 在环 R 中,即是一个整向量,因此 $\boldsymbol{w}\times\boldsymbol{c}$ 与 $\boldsymbol{w}\times\boldsymbol{e}$ 有相同的分数部分.如果 $\boldsymbol{w}$ 和 $\boldsymbol{e}$ 足够小,特别是如果能保证 $\boldsymbol{w}\times\boldsymbol{e}$ 的所有系数都小于 1/2,$\boldsymbol{w}\times\boldsymbol{e}$ 与 $\boldsymbol{w}\times\boldsymbol{e}$ 的分数部分$[\boldsymbol{w}\times\boldsymbol{e}]$相同.解密者只需对密文 $\boldsymbol{c}$ 乘上 $\boldsymbol{w}^{-1}$,即可得到 $\boldsymbol{e}$,计算 $\boldsymbol{m}\leftarrow\boldsymbol{e} \bmod 2$ 恢复 $\boldsymbol{m}$.在 Gentry 的原文中实际解密过程稍有不同.通过计算 $\boldsymbol{m}\leftarrow\boldsymbol{c}-[\boldsymbol{w}\times\boldsymbol{c}] \bmod 2$ 解密.

这个体制是部分同态的,2 个密文 $\boldsymbol{c}_1=\boldsymbol{j}_1+\boldsymbol{e}_1$,$\boldsymbol{c}_2=\boldsymbol{j}_2+\boldsymbol{e}_2$,它们的和可以表示成 $\boldsymbol{j}_3+\boldsymbol{e}_3$,其中,$\boldsymbol{j}_3=\boldsymbol{j}_1+\boldsymbol{j}_2\in J$,$\boldsymbol{e}_3=\boldsymbol{e}_1+\boldsymbol{e}_2$ 是小的扰动向量.2 个密文的乘积可以写成:$\boldsymbol{j}_4+\boldsymbol{e}_4$,其中 $\boldsymbol{j}_4=\boldsymbol{j}_1\times(\boldsymbol{j}_2+\boldsymbol{e}_2)+\boldsymbol{e}_1\times\boldsymbol{j}_2\in J$,$\boldsymbol{e}_4=\boldsymbol{e}_1\times\boldsymbol{e}_2$,仍然较小.经过若干次乘法和加法在扰动大小还没有超过解密半径之前,该算法是同态的,即这是一个部分同态算法,具体可以进行的运算次数与具体参数选择有关.

2.4 Gentry 的全同态加密体制

Gentry 的部分同态加密体制对式(2)只能对低次数的函数 f 成立,当 f 的次数过大时,扰动变量超过秘密密钥的解密范围,同态性质就无法保持.为了实现全同态加密 Gentry 引入了 Bootstrapping 的思想.他观察到如果 f 是解密函数时能保证式(2)成立,就可以在不知道密钥的情况下更新密文,把扰动一直控制在较小的范围内,从而实现全同态加密.具体地说,如果满足:

$$Dec_{En_{pk_2}(sk_1)}(En_{pk_2}(En_{pk_1}(m)))=$$
$$Dec(En_{pk_2}(sk_1),(En_{pk_2}(En_{pk_1}(m))))=$$
$$En_{pk_2}(Dec(sk_2,En_{pk_1}(m)))=En_{pk_2}(m),$$

即可以用公钥 pk_2 加密的私钥 sk_1 和用公钥 pk_1 加密的明文 m 作为输入,输出用公钥 pk_2 加密的明文.实现了不知道私钥情况下的明文更新.满足这一条件的体制称作 Bootstrapping 的.

但遗憾的是对 2.3 节介绍的部分同态加密体制来说,解密函数表示成密钥比特的多项式次数仍然太高,不满足式(2).为了克服这个问题,Gentry 进一步引入了降低解密函数的次数的技巧,在文中称作 Squash.将原来的部分同态加密体制转化成一个新的体制,使得解密函数的次数降低,但对其他的性质没有影响.在原来的体制中秘密密钥是向量 $\boldsymbol{w}$,在新的体制中公钥包括一部分对 $\boldsymbol{w}$ 的提示信息,一个大的集合 $\mathcal{S}=\{\boldsymbol{x}_i,i=1,2,\cdots,S\}$ 存在一个稀疏的子集 T,其中的元素相加是 $\boldsymbol{w}$.用一个 0,1 比特串 $\boldsymbol{\sigma}=$

$[\sigma_1,\sigma_2,\cdots,\sigma_s]$表示,即 $\boldsymbol{w}=\sum_{i=1}^{s}\sigma_i\boldsymbol{x}_i$. 新的体制中秘密密钥是 $\boldsymbol{\sigma}$.

这样在原算法中需要计算 $\boldsymbol{m}\leftarrow\boldsymbol{c}-[\boldsymbol{w}\times\boldsymbol{c}] \bmod 2$ 解密,在新的算法中对密文 $\boldsymbol{c}$ 作一个处理,对所有的 $\boldsymbol{x}_i\in\mathcal{S}$,计算 $\boldsymbol{y}_i=\boldsymbol{x}_i\times\boldsymbol{c}$,解密过程转化成计算:

$$\boldsymbol{c}-\sum_j\sigma_j\boldsymbol{y}_j \bmod 2.$$

再利用一些加法的技巧,该式可以表示成次数大约是集合 T 的元素数量的 σ_j 的多项式. 合理地选择参数可以使得这里 T 足够小,得到一个 Bootstrapping 的体制.

2.5 Smart-Vercauteren 对 Gentry 体制的优化

2010 年 PKC 上 Smart 等人提出了第 1 个 Gentry 体制的优化[15]. 该体制定义在环 $R=\mathbb{Z}[x]/(f(x))$ 上,其中 $f_n(x)=x^n+1$,n 是 2 的幂次. 在一个 n 维方体里随机选择向量 $\boldsymbol{v}$,满足 $\boldsymbol{v}$ 生成的格行列式是一个素数,记 $J=(\boldsymbol{v})$,这样的 J 是一个主理想,这样的理想可以用 2 个参数(d,r)来表示:$d=\det(J)$,r 是 $f_n(x) \bmod d$ 的根. 注意到该理想格的 Hermite 形式具有如下的特征:

$$HNF(J)=\begin{pmatrix} d & 0 & 0 & \cdots & 0\\ -r & 1 & 0 & \cdots & 0\\ -[r^2]_d & 1 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & & \vdots\\ -[r^{n-1}]_d & 0 & 0 & \cdots & 1 \end{pmatrix}, \tag{3}$$

这里$[r]_d$ 指将 r 模到$(-d/2,d/2]$之间. 容易看出对一个向量 $\boldsymbol{a}$ 进行模 $HNF(J)$的运算相当于计算多项式 $a(x)$在点 r 处模 d 的取值,得到的向量是$([a(r)]_d,0,0,\cdots,0)$. 因此加密一个向量$(m,0,0,\cdots,0)$,其中 $m\in\{0,1\}$,即选择一个随机小的多项式 $u(x)$,计算在点 r 处的取值,输出密文 $c\leftarrow[2u(r)+m]_d$.

Smart 和 Vercauteren 的体制中,秘密密钥只是一个整数 w,计算 $m\leftarrow(c-\lfloor cw/d\rfloor) \bmod 2$ 即可解密. 该体制可以实现 Gentry 的部分同态加密方案,但是 Gentry 体制的 Squash 仍因为参数太大无法实现,从而实现不了 Bootstrapping,即无法实现全同态加密. Smart-Vercauteren 的体制很大的一个局限是生成部分同态体制的密钥非常复杂,由于找到一个行列式是素数的元素需要生成大约 $n^{1.5}$ 个随机元素. 计算秘密密钥的复杂度大约是 $n^{2.5}$. 所以生成 $n>2\,048$ 的密钥已不实际. 而它们的解密函数的次数高达几百,需要 n 达到 2^{27} 才可以进行 Squash 步骤,而这么大的 n 对密钥生成又是不可能的.

2.6 Gentry-Halevi 对 Gentry 体制的实现

Gentry-Halevi 第 1 次完全实现了全同态加密[16],对维数 2 048,8 192,32 768 公钥的大小大约为 70 MB 到 2.3 GB,运行 Bootstrpping 的时间大约是 30 s 到 30 min.

本文对 Gentry 体制的优化主要有以下 7 个方面:

1) 放松了 Smart-Vercauteren 体制的对格的行列式是素数的要求,只需要基的 HNF 形式具有式(3)的特征即可. 并且给出了一个非常容易的判别条件,判别这样的格.

2) 与 Smart-Vercauteren 体制类似,该体制也是使用一个秘密的逆多项式的一个系数来解密,但是为了简便用模计算代替了有理数的除法.

3) 在计算解密密钥时需要计算一个给定多项式模 $x^{2^m}\pm1$ 的逆,这在 Smart-Vercauteren 的体制中是非常费时间的操作. 给出了一个优化的算法可以高效地计算结式和逆多项式的一个系数,而不必计算整个多项式.

4) 使用了批处理技术加速加密,通过一起计算一些小系数的多项式在同一个点的值来有效计算. 计算 k 个多项式只是计算一个多项式复杂度的$\sqrt{k}$倍.

5) 秘密密钥是一个长度为 $S\approx1\,000$ 的二元向量,其中只有 15 个 1,其他是 0. 通过用 s 个长度为 S 的(每个向量只有一个 1)向量来表示秘密密钥提高算法的效率.

6) 公钥包含一个稀疏背包问题的实例,将其利用几何级数来表示,从而大大节省存储空间.

7) 全同态加密体制的公钥包含对秘密密钥比特的加密,利用时间和空间的平衡策略来优化存储空间而不增加过多的时间复杂度.

3 基于整数的全同态加密

2010 年的欧密会上,Dijk 等人[14]提出了一种基于整数的全同态加密体制. 该体制与 Gentry09 体制非常类似,首先构造一个部分同态的体制,再利用 Squash 降低解密函数次数,实现 Bootstrapping. 该体制的优势是它不需要理想格上的运算,但是公钥的长度仍然很长. 算法安全性基于近似最大公因子问题.

随后,在 2011 年美密会上,Coron 等人提出了该体制的一种降低密钥长度的版本[20],并且借鉴文

献[16]的方法进一步作了优化.实现了安全强度分别为 42 B,52 B,62 B,72 B 的几个实例.对安全强度为 72 B 的参数,加密和重加密分别需要 3 min 和 12 min,解密时间很短,公钥大小是 800 MB.同时证明了经过这些优化之后算法仍然是语义安全的,安全性基于一个变种的近似最大公因子问题.

3.1 DGHV 体制

利用$[z]_p$表示 z 模 p 到$(-p/2,p/2]$之间.生成一个 η 比特的奇数 p,$x_i \leftarrow D_{\gamma,p}(p)$,

$$D_{\gamma,p}(p)=\{q\in\mathbb{Z}\cap[0,2^{\gamma}/p],$$
$$r\leftarrow\mathbb{Z}\cap(-2^{\rho},2^{\rho}):x=pq+r\}.$$

选其中最大的记为 x_0,并且保证 x_0 是奇数,$[x_0]_p$ 是偶数.公钥 $pk=(x_0,x_1,\cdots,x_{\tau})$,私钥是 p.加密 1 B 的明文 m,选择一个随机子集 $S\subseteq\{1,2,\cdots,\tau\}$和 1 个在区间$(-2^{\rho'},2^{\rho'})$中的随机整数 r,输出密文 $c=[m+2r+2\sum_{i\in S}x_i]_{x_0}$.解密计算 $m\leftarrow(c \bmod p) \bmod 2$.由于 $c \bmod p=c-p\lfloor c/p\rfloor$,$p$ 是素数,因此只需计算 $m\leftarrow[c_2]\oplus[\lfloor c/p\rfloor]_2$.

在文献[14]中,证明了这是一个部分同态的体制,在近似 GCD 问题的困难性假设下是语义安全的.近似最大公因子问题,表述如下:参数(ρ,η,γ)近似 GCD 问题指对一个随机的 η 比特的奇数 p,给定多项式个 $D_{\gamma,p}(p)$中的取样,输出 p.这个问题目前还没有找到高效的算法解决,被认为是困难的.

将这个体制转化成全同态的,使用了与 Gentry09 类似的办法,通过增加公钥中部分私钥的信息,降低解密函数的系数从而实现 Bootstraping.具体地说,$x_p=\lfloor 2^{\kappa}/p\rfloor$,其中,$\kappa=\gamma\eta/\rho'$,选择一个随机的比特的 0,1 向量,只有 θ 比特为 1,

$$\boldsymbol{h}=[h_1,h_2,\cdots,h_{\theta}],\mathcal{H}=\{i:h_i=1\}.$$

选随机整数:$u_i\in\mathbb{Z}\cap[0,2^{\kappa+1}]$,$i=1,\cdots,\Theta$,满足$\sum_{i\in H}u_i=x_p \bmod 2^{\kappa+1}$.令:$y_i=u_i/2^{\kappa}$,$y=\{y_1,\cdots,y_{\Theta}\}$,因此 y_i 是一个小于 2 的正数,用二进制表示精度是 κ 比特,并且满足:$\left[\sum_{i\in H}y_i\right]_2=(1/p)-\Delta_p$,$\Delta_p<2^{-\kappa}$.经过这样的处理,私钥仍然是 h,公钥是 x 和 y.

加密过程转化:用部分加密算法计算密文 c^*,对 $i=1,\cdots,\Theta$,令 $z_i=[c^*y_i]_2$,仅保留 0,1 表示小数点后的$\lceil b(\theta+1)\rceil$位,输出 c^* 和 $z=\langle z_1,z_2,\cdots,z_{\Theta}\rangle$.解密输出 $m\leftarrow\left[c^*-\left\lceil\sum_i s_iz_i\right\rceil\right]_2$即可.

为了达到 2^{λ} 的安全强度,对参数有如下要求:抵抗对扰动变量的穷举搜索攻击 $\rho=\omega(\mathrm{lb}\lambda)$;为了 Squash 技术的实现 $\eta\geqslant\rho\Theta(\lambda\ \mathrm{lb}\lambda^2)$;抵抗格攻击 $\gamma=\omega(\eta^2\ \mathrm{lb}\lambda)$;保证安全性证明 $\tau\geqslant\gamma+\omega(\mathrm{lb}\lambda)$,$\rho'=\rho+\omega(\mathrm{lb}\lambda)$.在文献[14]中,建议参数:$\rho=\lambda$,$\rho'=2\lambda$,$\eta=\tilde{O}(\lambda^2)$,$\gamma=\tilde{O}(\lambda^5)$,$\tau=\gamma+\lambda$,公钥的长度是 $\tilde{O}(\lambda^{10})$.

3.2 优化版本的 DGHV 体制

2011 年的美密会上 Coron 等人提出的减少密钥长度的方案[20],主要创新点是 x_i 生成的方式为 $x'_{i,j}=x_{i_0}x_{i_1} \bmod x_0$,$1\leqslant i,j\leqslant\beta$,这样只需要存储 2β 个整数就可以生成 β^2 个整数 $x'_{i,j}$,公钥的大小从 τ 个 γ 比特的数降低到 $2\sqrt{\tau}$ 个.另外的不同还有 x_0 是无扰动的变量 $x_0=pq_0$,该要求使得体制的安全性基于一个变体的近似最大公因子问题.称为无扰动近似最大公因子问题,具体描述如下:

参数(ρ,η,γ)无扰动近似 GCD 问题指对一个随机的 η 比特的素数 p,给定 $x_0=pq_0$,其中 q_0 是一个属于$[0,2^{\gamma}/p]$的随机无小于 2^{λ} 因子的无平方数,多项式个 $D'_p(p,q_0)$中的取样输出 p.这个问题目前也还没有找到高效的算法解决,被认为是困难的.这里:

$$D'_p(p,q_0)=\{q\leftarrow\mathbb{Z}\cap[0,q],$$
$$r\leftarrow\mathbb{Z}\cap(-2^{\rho},2^{\rho}):x=pq+r\}.$$

密钥生成一个 η 比特的随机素数 p,q_0 是一个属于$[0,2^{\gamma}/p]$的随机无小于 2^{λ} 因子的无平方数,生成 $x_{i,b}=pq_{i,b}+r_{i,b}$,$1\leqslant i\leqslant\beta$,$b\in\{0,1\}$,其中 $q_{i,b}$是$[0,q)$的随机整数,$r_{i,b}\in(-2^{\rho},2^{\rho})$.私钥是 p,公钥是$(x_0,x_{1,0},x_{1,1},\cdots,x_{\beta,0},x_{\beta,1})$.加密对一个比特的明文 m 过程如下:生成一个随机大小为 $\tau=\beta^2$ 的向量 $\boldsymbol{b}=(b_{i,j})$元素均在$[0,2^{\alpha})$之间,生成一个$(-2^{\rho'},2^{\rho'})$中的随机整数 r,输出密文 $c=m+2r+2\sum_{1\leqslant i,j\leqslant\beta}b_{i,j}x_{i,0}x_{j,1} \bmod x_0$.解密过程与原算法相同.

在 Squash 的过程中,与原算法的不同之处就是为了节省存储,生成 $u_i\in\mathbb{Z}\cap[0,2^{\kappa+1}]$,$i=1,\cdots,\Theta$时,不再是随机选取而是通过一个伪随机生成函数 f 和种子 e 来生成,这样将这部分存储从 $\tilde{O}(\lambda^8)$降到 $\tilde{O}(\lambda^7)$.$z_i\leftarrow[c^*y_i]_2$,仅保留 0,1 表示小数点后的$\lceil\mathrm{lb}\theta\rceil+3$位.

为了达到 2^{λ} 的安全强度,对参数有如下要求:抵抗对扰动变量的穷举搜索攻击仍有 $\rho=\omega(\mathrm{lb}\lambda)$;抵抗格攻击 $\gamma=\omega(\eta^2\ \mathrm{lb}\lambda)$;为了 Squash 技术的实现 $\eta\geqslant(2\rho+\alpha)\Theta(\lambda\ \mathrm{lb}\lambda^2)$;保证安全性证明 $\alpha\beta^2\geqslant\gamma+\omega(\mathrm{lb}\lambda)$,$\rho'=2\rho+\alpha+\omega(\mathrm{lb}\lambda)$.在文献[20]中,建议参

数与原算法相同有 $\rho=\lambda,\eta=\tilde{O}(\lambda^2),\gamma=\tilde{O}(\lambda^5)$,另外还有 $\alpha=\lambda,\beta=\tilde{O}(\lambda^2),\rho'=4\lambda$,与原体制需要 $\tau=\tilde{O}(\lambda^5)$ 个 x_i 不同,这里只需要 $2\beta=\tilde{O}(\lambda^2)$ 个 x_i,公钥的长度从 $\tilde{O}(\lambda^{10})$ 降到 $\tilde{O}(\lambda^7)$.

4 全同态加密体制的新进展

虽然在全同态体制的实用化方面做了很多工作,但其实现效率还远达不到应用的要求.主要有下面 2 点原因:1)Bootstrapping 的复杂性至少是解密的复杂度乘以用来加密密钥比特的密文的比特长度.这是因为 Bootstrapping 需要同态计算解密函数,而解密密钥需要经过加密处理.而解密复杂度和密钥长度均为 $\Omega(\lambda)$,因此 Bootstrapping 的复杂度至少是二次的.2)可以计算次数为 d 的函数部分同态加密体制,需要 2^d 近似最短向量问题在 2^λ 时间内不可解.格的维数需要达到 $\Omega(d\lambda)$,向量的系数需要达到 $\Omega(d)$(单位 B),因此更新后的密文长度至少是 $\Omega(d\lambda^2)$.但是部分同态体制要达到 Bootstrapping 必须可以对自身的解密函数进行同态运算,即 d 必须大于解密函数的次数 $\Omega(\lambda)$,因此更新后密文的长度为 $\tilde{\Omega}(\lambda^2)$.这样即使假设这些更新的密文解密只需要 $\Theta(\lambda)$ 的时间,总的时间仍然需要 $\tilde{\Omega}(\lambda^4)$.

由于全同态加密体制在实际中的重要应用前景,对其研究和优化不断有新的进展,很多文章[21-22]发表在顶级密码学会议上,由于篇幅所限,这里不再做详细介绍.

4.1 不带 Squash 的全同态加密体制

最近 Gentry 等人[18]和 Brakerski 等人[23]分别独立提出了不用 Squash 步骤的同态加密体制.这样使得体制的安全性不再需要稀疏背包问题的困难性假设.这 2 个体制仍需要 Bootstraping 步骤,没有从根本上提高算法的效率.但这 2 种算法都提出了很有意义的思想.

Gentry 等人[18]通过将解密函数表示成不同的形式实现了 Bootstrapping.他们观察到基于格的密码体制的解密函数可以表示成一种特殊类型的对称多项式,这种多项式可以利用大域上的深度为 3 的算术电路表示.尽管这个多项式的次数较高,他们证明了可以将其转化成乘同态的体制(如 ElGamal)进行同态计算,再将结果转化回去.这里的乘同态体制可以用加同态体制来代替,比如通过加上离散对数.该体制的安全性依赖于最坏情况的理想格上的困难问题.

Brakerski 等人设计的体制[23]基于 LWE 问题,该体制的创新性主要有 2 点:1)基于 LWE 构造了一个部分同态加密体制,主要的技术是重线性化,突破了之前的体制都基于理想格上的困难问题的缺陷;2)利用维数约化和模约化的技术来减少密文的长度,降低解密复杂度.从而在不用 Squash 的情况下实现 Bootstrapping.在基于 LWE 的体制中,解密通过计算密文和密钥的内积 $m=(\langle \boldsymbol{c},\boldsymbol{s}\rangle \bmod q) \bmod 2$.维数约化技术将明文 m 在密钥 s 下的密文 c 转化成在一个不同的密钥 s' 加密下的密文 c',$m=(\langle \boldsymbol{c}',\boldsymbol{s}'\rangle \bmod q) \bmod 2$.这里 c' 和 s' 的维数都比 c,s 小.为了实现这个步骤需要在公钥中包括 s 在 s' 下的加密,但是这里 s 不是按比特加密的.模约化步骤将 m 在密钥 s 下的密文 c 转化成一个在不同的模下的密钥 s' 下的密文 c',$m=(\langle \boldsymbol{c}',\boldsymbol{s}'\rangle \bmod q) \bmod 2$.在部分同态加密的更新密文过程中,扰动会变得很大,利用维数约化和模约化得到同一个明文的小得多的密文,对这个小的密文执行解密过程,最终实现了不需要 Squash 的 Bootstrapping.

4.2 不带 Bootstrapping 的全同态加密体制

Gentry 借鉴 Brakerski 等人的设计中模约化的技术控制扰动变量的大小,提出了不需要 Bootstrapping 的全同态加密体制[17].

模约化的核心是如下的引理:p,q 是 2 个奇数,$\boldsymbol{c}$ 是一个整数向量,$\boldsymbol{c}'$ 是一个与 $(p/q)\boldsymbol{c}$ 接近的向量且 $\boldsymbol{c}'=\boldsymbol{c} \bmod 2$.对任意 s,$\|\langle \boldsymbol{c},\boldsymbol{s}\rangle \bmod q\|<q/2-(q/p)l_1(\boldsymbol{s})$,有 $\langle \boldsymbol{c}',\boldsymbol{s}\rangle \bmod p=\langle \boldsymbol{c},\boldsymbol{s}\rangle \bmod p \bmod 2$,且 $\|\langle \boldsymbol{c}',\boldsymbol{s}\rangle \bmod p\|<(p/q)\|\langle \boldsymbol{c},\boldsymbol{s}\rangle \bmod p\|+l_1(\boldsymbol{s})$,其中,$l_1(\boldsymbol{s})$ 是 $\boldsymbol{s}$ 的 l_1 范数.

该引理表明在不知道密钥 s 的情况下,只需要知道 s 长度的界,即可把一个模 q 下的密文转化为一个模 p 的密文仍可以正确解密,即 $\langle \boldsymbol{c}',\boldsymbol{s}\rangle \bmod p=\langle \boldsymbol{c},\boldsymbol{s}\rangle \bmod p \bmod 2$,这个转化只涉及到一个数乘和取整.如果 s 比较短,p 比 q 小,该转化达到了减小密文中扰动的目的,即 $\|\langle \boldsymbol{c}',\boldsymbol{s}\rangle \bmod p\|<\|\langle \boldsymbol{c},\boldsymbol{s}\rangle \bmod p\|$.在不知道密钥的情况下减少扰动是 Bootstrapping 希望达到的目的,而模约化的步骤显然比 Bootstrapping 要简洁很多.

模约化从表面来看并不是一个好的处理扰动的方法,因为对于比 q 小的 p,模约化虽然降低了扰动变量的绝对值,但也相应减少了模的长度,即扰动和模的比值没有减少.对体制的同态能力来说,扰动的绝对值更重要.特别是对乘法.比如取 $q\approx x^k$,2 个模

q 的部分同态加密体制的密文如果扰动大小都是 x,相乘之后扰动变成 x^2,经过 4 轮的乘法,扰动变成 x^{16},即只能进行 $\mathrm{lb}\,k$ 层的乘法.如果选择一系列递减的模 $\{q_i \approx q/x^i\}$,$i<k$.2 个模 q 的密文相乘之后,把密文转化成在一个小的模 $q_1 \approx q/x$ 下,这样对应的扰动从 x^2 降到 x(这里假设 $l_1(s)$ 很小可以忽略).再在模 q_1 的情况下做 2 个密文的乘法,扰动仍是 x^2,再利用模约化技术将模降到 q_2,扰动仍可保持在 x.以此类推,利用这种技术可以进行 k 层的乘法,大大提高了之前的 $\mathrm{lb}\,k$.

这样通过模约化得到了噪声的减少,利用逐渐减少模,可以保持噪声一直比较小.实现了对任意多项式保持同态性质而不需要 Bootstrapping,从而提高了算法的效率.关于该体制具体的优化可参见文献[17],在这里不再详述.

5 全同态加密的应用

现实生活中的实际应用往往会大幅推动科学理论的发展.随着互联网的发展,尤其是云计算概念的诞生,人们在加密数据搜索与处理等方面的需求日益增加,大大推动了全同态加密方向的科学研究.与此同时,自 Gentry 的创新性工作发表以来,关于全同态加密的研究工作开始出现了新的高潮,被广泛应用于多种实际环境.本节将对全同态加密的一些典型应用作简要介绍.

5.1 全同态加密一般性应用框架

密码协议是大多数安全模块中必备的环节,从广义上讲,所有的密码协议都是安全多方计算的一个特例.它们广泛应用于金融交易、社交网络、实时监控、信息管理等多个领域.常见的密码协议中,通常包括多个参与者,他们可能是可信方(例如用户自己、经过认证的参与者)或不可信方(未经认证的参与者).理论上,凡是存在不可信方的协议都具备全同态加密应用的可能.因此,全同态加密的大部分应用都可视作安全多方计算的范畴.

当不可信方需要对敏感数据进行搜索、分析、处理等操作时,协议的其他参与者不希望不可信方掌握明文数据,因此可以采用全同态加密方案,让不可信方直接对密文进行操作,实现等同于对原始数据直接进行处理的效果,从而完成用户的需求.我们给出全同态加密的一般性应用框架,如图 1 所示:

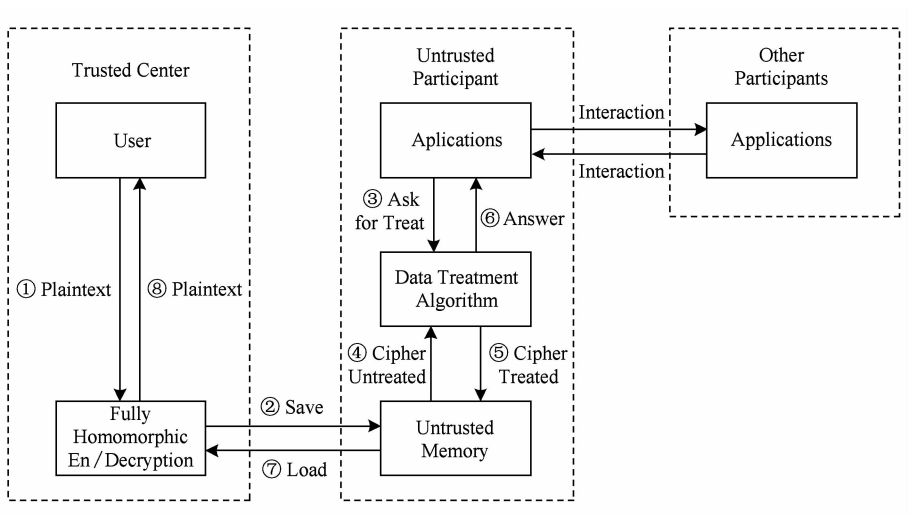

Fig. 1 General application framework of fully homomorphic scheme.

图 1 全同态加密的一般性应用框架

加密数据处理方法简述如下:假设存在全同态加密函数 $Enc_k(x)$,首先用户用自己的私钥 k 对需要处理的数据 m 进行同态加密 $c=Enc_k(m)$,然后将加密数据 c 上传到云端服务器.服务器能够对加密数据 c 直接进行处理,得到 $c'=f(c)=f(Enc_k(m))$,然后将处理后的密文 c' 返回给用户.用户收到 $c'=f(c)=f(Enc_k(m))=Enc_k(f(m))$ 后,利用自己的私钥 k 对其进行同态解密,得到已经处理好的明文数据 $f(m)$.

5.2 云计算中的全同态加密

云存储安全是云计算领域的重要安全问题之一.为解决数据隐私保护的问题,常见的方法是由用户对数据进行加密,把加密后的密文信息存储在服务端.然而,当用户需要服务器提供数据搜索、分析、处理等功能时,传统加密方案难以实现,但全同态加密为之提供了实现的可能.

5.2.1 云计算中的加密数据检索

随着云计算技术的广泛应用,服务器端存储的加密数据必将成爆炸式增加,对加密数据的检索成为一个迫切需要解决的问题.现有的加密数据检索算法包括线性搜索、公钥搜索和安全索引等[24],这些算法可以快速地检索出所需信息,但是它们只适用于小规模数据的检索,而且代价很高.基于全同态加密技术的数据检索方法可以直接对加密的数据进行检索,不但能保证被检索的数据不被统计分析,还能对被检索的数据进行简单的运算,同时保持对应的明文顺序.目前一些公司已经准备提供云搜索服务,例如2010年5月Google宣布将计划开始提供加密搜索服务[25],但技术细节尚未公开.

数据检索有多种方法,如向量空间模型[26]等.首先对文档进行分词和词干化,即从文档中抽取出能表征文档主要内容特征和形式特征的检索词,以形成文档的向量表示.然后将得到的检索词和待检索文档进行加密,并储存至云服务器.采用了全同态加密方案后,当服务器需要检索加密文档时,可直接提交加密后的检索词.此时每个文档都可根据所提交的关键词进行权重向量表示,对用全同态加密后的词频和倒排文档频率进行操作可以得到权重:

$$W_{i,k}=\frac{(\mathrm{lb}\, f_{ik}+1.0)\times \mathrm{lb}\,\dfrac{N}{n_k}}{\sqrt{\sum_{k=1}^{l}\left[(\mathrm{lb}\, f_{ik}+1.0)\times \mathrm{lb}\,\dfrac{N}{n_k}\right]^2}},$$

其中,$f_{i,k}$为检索词T_k在文档D_i中出现的频率,N为整个文档集包含的文档数,n_k为整个文档集中含检索词T_k的文档数.该权重反映了关键词与文档的相关度,因而可以根据大小进行排序,筛选出用户需要的文档.用户得到加密文档后,用私钥对文档解密即可得到原始文档,整个过程如图2所示[24]:

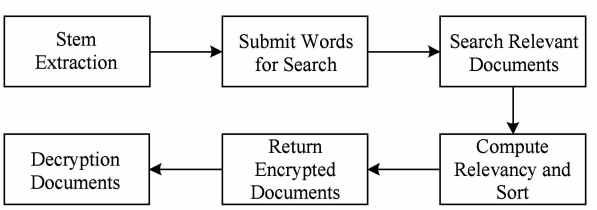

Fig. 2 Data retrieval system based on fully homomorphic.

图2 基于全同态加密的数据检索过程

5.2.2 云计算中的加密数据处理

云计算中的加密数据处理和5.2.1节所述加密数据检索的思路类似.首先对待处理的关键数据进行加密和特殊标记,以与普通加密数据区分开来,然后再上传到服务器.服务器会直接对密文数据进行操作来完成用户的需求,并将处理后的密文返回给用户.目前人们对加密数据处理已经开始了一定的应用研究.

在医疗应用中,人们提出了一种医疗记录云存储系统(病人控制加密)[27],医疗服务提供者先对病人的医疗记录进行加密,然后传输到云存储系统.病人通过与某个服务提供者分享私钥,共享其医疗记录.然而,该系统只提供云搜索服务(关键词匹配或者其他的一些搜索方法),并没有提供云计算服务.利用全同态加密体制,该系统可以对加密的医疗记录进行计算,为病人提供云计算服务[28].随着科技的发展,基于无线体域网的监视器或者其他设备将能够代替病人连续不断地向云端服务器传输加密数据.利用全同态加密体制,云端服务器可以对加密数据进行计算,并根据具体的计算结果,返回给病人一些警告或者建议等.在这个方案中,可能需要计算平均值、标准差、最小二乘法等统计函数.加密输入可能包括血压、心率等实时信息以及体重、性别等病人的基本信息,而加密用的函数则可以是公开的.

在金融行业,全同态加密有着潜在的应用,一些数据和进行加密的函数是需要保密的.例如公司的数据、股票价格、绩效、存货清单等信息都与投资决策有关,是制定交易策略的关键信息.全同态加密体制可以使一些函数能够被秘密地计算[28].1)用户可以将函数的加密形式、敏感数据的密文分别上传到云端服务器(或许它们分别来自不同的用户);2)第三方的管理者可利用这些函数的加密形式对加密数据进行处理.在处理完成后,云端服务器把处理的结果以密文的形式发送给用户,用户解密后则可得到处理后的敏感数据.

此外,文献[28]以一个化妆品公司为例描述了全同态加密的一个应用.假设该公司希望根据顾客的相关信息把特定的广告发送给目标顾客.若每个顾客的移动电话能够连续不断地上传自己的信息,包括实时方位、邮件、浏览器等,则该化妆品公司可以用相关函数进行计算,决定发送什么样的化妆品信息给顾客.由于顾客不希望私人信息泄露,因而可用全同态加密体制对数据进行加密.所有的顾客信息加密后上传到服务器,同时广告商也上传加密的广告到服务器,服务器对加密数据进行相关的计算,决定哪一个加密广告发送给顾客.顾客收到加密的

广告后用私钥对其进行解密即可获得广告.由于顾客的个人信息与广告均为加密传输的,因此不会泄露顾客的任何隐私.

5.3 电子投票

电子投票在计票的快捷准确、人力和开支的节省、投票的便利性等方面有着传统投票方式无法企及的优越性.而设计安全的电子选举系统是全同态加密的一个典型应用.

文献[29]描述了一个简单的电子选举方案:1)若有同态函数 $Enc_k(x_1+x_2)=Enc_k(x_1)\times Enc_k(x_2)$,选民将自己的选票进行加密 $C_i=Enc_k(M_i)$,其中 $M_i\in\{0,1\}$;2)投票中心收集同态加密后的选民选票 C_i;投票中心基于全同态加密方案的同态性质对加密后的选票 C_i 进行计票 $C=C_1\times C_2\times\cdots\times C_n$,得到经过同态加密后的选举结果 $C=Enc_k(M_1+M_2+\cdots+M_n)$;3)只有拥有解密密钥的某个可信机构才能够对加密后的选举结果进行解密,公布选举结果.在上述过程中,选票收集与计票完全对加密后的选票数据进行操作,不需要使用任何解密密钥.因此,任何一个主体或机构都可以完成计票员的职责,无论其是否可信.

5.4 数字水印

数字水印技术是指用信号处理的方法在数字化的多媒体数据中嵌入隐蔽的标记,这种标记通常是不可见的,只有通过专用的检测器或阅读器才能提取.如何应对复杂网络环境下数据隐藏与数字水印系统的安全挑战,是目前需要迫切解决的问题.针对数字水印的一种主要的安全性攻击手段是非授权检测攻击,即攻击者在未经授权的情况下对含有水印的载体进行检测,以确定水印是否存在,进而猜测或破译水印的含义,甚至去除载体中的水印并嵌入一个伪造的水印.文献[30]提出的基于全同态加密的数字水印方案可以有效地抵抗这种攻击.该方案首先利用全同态加密体制对水印信号与原始载体进行加密,然后将加密后的水印嵌入到原始载体中.在用户检测水印之前,必须首先对含有水印的载体进行同态解密,从而保证解密后的水印信号与含水印的载体之间没有明显的相关性.在解密含水印的载体之后,可以通过计算解密后的载体与水印信号之间的相关度,判断水印的存在性进而提取水印.图3描述了传统的数字水印方案与基于全同态加密的数字水印方案的区别:

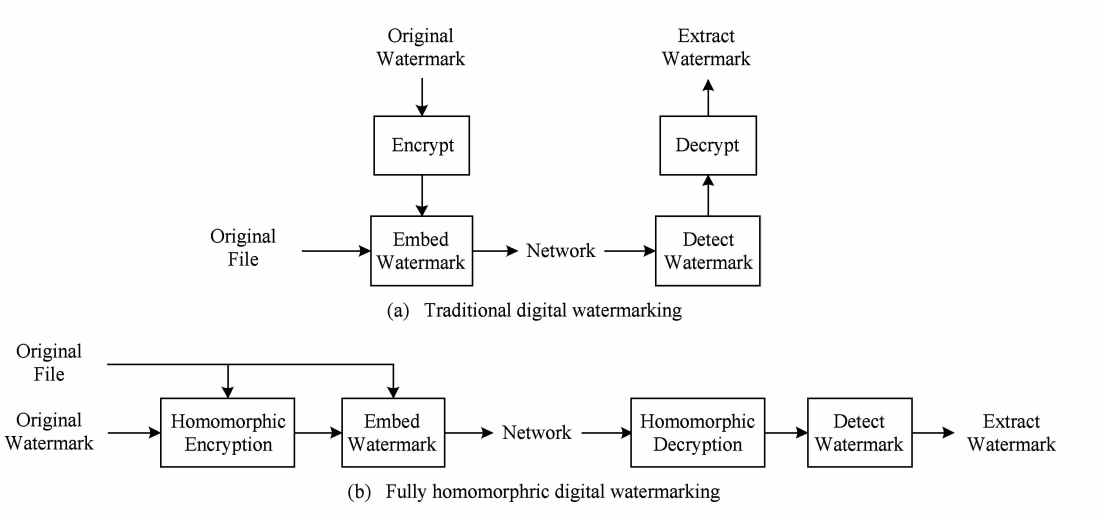

Fig. 3 Difference between traditional and fully homomorphic digital watermarkings.

图3 传统数字水印与基于全同态加密的数字水印的区别

6 总 结

全同态加密在云计算、电子商务等实际中的重要应用使其受到密码学家越来越多的关注.一方面,全同态加密研究方面的突破,不断满足互联网上加密数据搜索与处理等方面的需求,另一方面应用的需要又反过来促进了理论的发展.2009年第1个全同态加密方案被提出,但由于实现效率、密钥存储等方面的局限,该方案远达不到实用化的要求.随后,研究人员为了突破这些局限,在该方向不断作出新的工作.特别是不用 Bootstrapping,Squash 等技术的全同态加密方案大大提高了算法的效率,使得全同态加密逐步向实用化靠近.但是全同态加密方案的安全性和实用性方面的研究还有很长的路要走.

参 考 文 献

[1] Rivest R, Adleman L, Dertouzos M. On data banks and privacy homomorphisms [M] Foundations of Secure Computation. New York: Academic Press, 1978: 169-180

[2] Cohen J, Fischer M. A robust and verifiable cryptographically secure election scheme (Extended Abstract) [C] // Proc of the 26th Annual Symp on Foundations of Computer Science (FOCS1985). Piscataway, NJ: IEEE, 1985: 372-382

[3] Damgard I, Jurik M. A generalization, a simplification and some applications of Paillier probabilistic public-key system [G] //LNCS 1992: Proc of Public Key Cryptography (PKC 2001). Berlin: Springer, 2001: 119-136

[4] Paillier P. Public-key cryptosystems based on composite degree residuosity classes [G] //LNCS 1592: Proc of Eurocrypt 1999. Berlin: Springer, 1999: 223-238

[5] Melchor C, Gaborit P. A lattice-based computationally efficient private information retrieval protocol [EB/OL]. 2007 [2012-12-09]. http://eprint.iacr.org/2007/446

[6] Lipmaa H. An Oblivious transfer protocol with log-squared communication [G] //LNCS 3650: Proc of ISC 2005. Berlin: Springer, 2005: 314-328

[7] Goldwasser S, Kharchenko D. Proof of plaintext knowledge for the Ajtai-Dwork cryptosystem [G] //LNCS 3378: Proc of Second Theory of Cryptography Conference (TCC 2005). Berlin: Springer, 2005: 529-555

[8] Goldwasser S, Micali S. Probabilistic encryption and how to play mental poker keeping secret all partial information [C] // Proc of the 14th Annual ACM Symp on Theory of Computing (STOC 1982). New York: ACM, 1982: 365-377

[9] Kawachi A, Tanaka K, Xagawa K. Multi-bit cryptosystems based on lattice problems [G] //LNCS 4450: Proc of PKC 2007. Berlin: Springer, 2007: 315-329

[10] Naccache D, Stern J. A new public-key cryptosystem based on higher residues [C] //Proc of the 5th ACM Conf on Computer and Communications Security (ACM CCS'98). New York: ACM, 1998: 59-66

[11] El-Gamal T. A public key cryptosystem and a signature scheme based on discrete logarithms [G] //LNCS 196: Proc of CRYPTO 1984. Berlin: Springer, 1984: 10-18

[12] Boneh D, Goh E, Nissim K. Evaluating 2-DNF formulas on ciphertexts [G] //LNCS 3378: Proc of the 2nd Theory of Cryptography Conf (TCC 2005). Berlin: Springer, 2005: 325-341

[13] Gentry C. Fully homomorphic encryption using ideal lattices [C] //Proc of the 41st Annual ACM Symp on Theory of Computing (STOC 2009). New York: ACM, 2009: 169-178

[14] Dijk M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers [G] //LNCS 6110: Proc of EUROCRYPT'2010. Berlin: Springer, 2010: 24-43

[15] Smart N P, Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes [G] //LNCS 6056: Proc of PKC 2010. Berlin: Springer, 2010: 420-443

[16] Gentry C, Halevi S. Implementing Gentry's fully-homomorphic encryption scheme [G] //LNCS 6632: Proc of EUROCRYPT 2011. Berlin: Springer, 2011: 129-148

[17] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping [C] //Proc of Innovations in Theoretical Computer Science 2012 (ITCS 2012). New York: ACM, 2012: 309-325

[18] Gentry C, Halevi S. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits [C] //Proc of the 52nd IEEE Annual Symp on Foundations of Computer Science (FOCS 2011). Piscataway, NJ: IEEE, 2011: 107-109

[19] Goldreich O, Goldwasser S, Halevi S. Public-key cryptosystems from lattice reduction problems [G] //LNCS 1294: Proc of CRYPTO 1997. Berlin: Springer, 1997: 112-131

[20] Coron S, Mandal A, Naccache D, et al. Fully homomorphic encryption over the integers with shorter public keys [G] // LNCS 6841: Proc of CRYPTO2011. Berlin: Springer, 2011: 487-504

[21] Gentry C, Halevi S, Smart P. Fully homomorphic encryption with polylog overhead [G] //LNCS 7237: Proc of EUROCRYPT 2012. Berlin: Springer, 2012: 465-482

[22] Gentry C, Halevi S, Smart P. Better bootstrapping in fully homomorphic encryption [G] //LNCS 7293: Proc of PKC 2012. Berlin: Springer, 2012: 1-16

[23] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from(standard) Lwe [C] //Proc of the 52nd IEEE Annual Symp on Foundations of Computer Science (FOCS 2011). Piscataway, NJ: IEEE, 2011: 97-106

[24] Liu Gen, Jiang Tianfa. Research on homomorphic encryption technology and the applications of it in IOT [J]. Information Network Security, 2011(5): 61-64 (in Chinese)
(刘艮, 蒋天发. 同态加密技术及其在物联网中的应用研究[J]. 信息网络安全, 2011(5): 61-64)

[25] ZDNet. Google to begin offering encrypted search [OL]. [2013-08-20]. http://www.zdnet.co.uk

[26] Wu Guangyuan, He Pilian, Cao Guihong, et al. Research on word co-occurrence based on vector space model and its application in doucuments [J]. Computer Applications, 2003, 23(6): 138-145 (in Chinese)
(吴光远, 何丕廉, 曹桂宏, 等. 基于向量空间模型的词共现研究及其在文本分类中的应用[J]. 计算机应用, 2003, 23(6): 138-145)

[27] Chase M, Lauter K, Benaloh J, et al. Patient controlled encryption: Patient privacy in electronic medical records [C] //Proc of the 1st Cloud Computing Security Workshop, 2009. New York: ACM, 2009: 103-114

[28] Lauter K, Naehrig M, Vaikuntanathan V. Can homomorphic encryption be practical? [C] //Proc of the 3rd ACM Cloud Computing Security Workshop (CCSW 2011). New York: ACM, 2011: 113-124

[29] Zhou Yongbin. A survey of homomorphic cryptography [G] //The Development Report of the Chinese Cryptology 2010. Beijing: Electronic Industry Press, 2011: 160-184 (in Chinese)
(周永彬. 同态密码学研究进展[G] //中国密码学发展报告2010. 北京: 电子工业出版社, 2011: 160-184)

[30] Li Zhi, Zhu Xinglei, Lian Yong, et al. Constructing secure content dependent watermarking scheme using homomorphic encryption [C] //Proc of the 2007 IEEE Int Conf on Multimedia and Exposition (ICME 2007). Piscataway, NJ: IEEE, 2007: 627-630

Liu Mingjie, born in 1985. Received her PhD from Tsinghua University in 2012. Postdoctor in Peking university. Her main research interest is lattice-based cryptography.

Wang An, born in 1983. Received his PhD degree in Shandong University in 2011. Currently postdoctor in Tsinghua University. His main research interests include side-channel attack, embedded system, and cryptography engineering.