一种基于LWE的BGN加密及门限加密方案

李菊雁[1]，马春光[1,2]，袁 琪[1,3]

(1. 哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001; 2. 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 西城区 100093;
3. 齐齐哈尔大学通信与电子工程学院 黑龙江 齐齐哈尔 161006)

【摘要】BGN加密方案是指允许密文任意次加法和一次乘法运算的加密方案，并且在密文的运算中，密文的规模没有增长。BGV12加密方案是基于(G)LWE的全同态加密方案，为了实现乘法同态，需要用到密钥交换、模转换等技术。该文在BGV12基础上构造了一种BGN加密方案。虽然只能支持密文的一次乘法运算，但不需要其他技术的支持，因而更快捷。与GVH10加密方案相比，有更好的参数规模。此外，将BGN加密方案扩展成一种门限加密方案，该门限加密方案同样允许所有参与者共同解密一个密文而没有泄露明文的任何信息，并且能抵抗密钥泄露攻击。

关 键 词 BGN加密； 密钥同态； LWE问题； 门限加密
中图分类号 TN918 **文献标志码** A doi:10.3969/j.issn.1001-0548.2018.01.014

A BGN-Type Encryption from LWE with a Threshold Encryption Scheme

LI Ju-yan[1], MA Chun-guang[1,2], and YUAN Qi[1,3]

(1. College of Computer Science and Technology, Harbin Engineering University Harbin 150001;
2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences Xicheng Beijing 100093;
3. College of Communication and Electronic Engineering, Qiqihar University Qiqihar Heilongjiang 161006)

Abstract The BGN (Boneh-Goh-Nissim) cryptosystem is a cryptosystem that permits arbitrary number of additions and one multiplication of ciphertext without growing the size of ciphertext. The scheme of BGV12 is a fully homomorphic encryption from (G)LWE which needs key switching, modulus switching and other technologies for the multiplicative homomorphism. This paper describes a BGN scheme based on BGV12. Although our constructed scheme only permits one multiplication, it does not need other technologies, so it is more efficient. Comparing with the scheme of GVH10, our scheme has better size of parameter. In addition, we extend our scheme to a threshold encryption scheme, which allows parties to cooperatively decrypt a ciphertext without learning anything but the plaintext, and can be protected from related-key attacks.

Key words BGN-type cryptosystem; key-homomorphic; learning with error problem; threshold encryption

基于容错学习(learning with error problem, LWE)的密码是一类备受关注的抗量子计算攻击的公钥密码体制[1]。BGN加密方案[2]描述了一种允许任意次加法和一次乘法的密文运算的加密系统，并且在密文的运算中，密文的规模没有增长。文献[3]基于LWE构造了一种简单的BGN加密方案GHV10，GHV10的解密算法需要用到陷门技术[4]。文献[5]构造了一种BGN加密方案，但是基于双线性配对和子集判定假设的。

加密方案BGV12[6]是一种全同态加密方案，加密的明文是比特，密文是向量。因为密文的乘法运算是向量的张量积，所以密文在运算后规模扩大。BGV12利用密钥交换、模转换等技术来控制噪音的增长和密文的规模，从而实现了全同态加密运算。如果为了实现密文的一次乘法运算仍然需要使用这些技术，那么BGV12就显得有些差强人意。本文利用BGV12的加密方案设计了一种变形的加密方案。加密的明文为矩阵(明文打包运算[7])，密文也为矩阵。因为密文的乘法运算是矩阵的乘法，而不是矩阵的张量积，所以密文的规模在运算后没有增大。

文献[8]基于RLWE构造了一种全同态加密算法ZXJXZ14，并扩展成一种门限加密方案。本文依据

收稿日期：2016 – 12 – 21；修回日期：2017 – 09 – 15
基金项目：国家自然科学基金(61472097)；信息安全国家重点实验室开放课题(2016-MS-10)
作者简介：李菊雁(1983 –)，男，博士生，主要从事密码学方面的研究.

ZXJXZ14，也将设计BGN加密方案扩展成一种门限加密方案，并且同样能抵抗密钥泄露攻击。

1 预备知识

本文中的数、向量、矩阵分别记为 x、$\boldsymbol{x}$、$\boldsymbol{X}$，向量的内积记为 $<\boldsymbol{v},\boldsymbol{u}>$，$\boldsymbol{I}_k$ 表示k阶单位矩阵，$\boldsymbol{A}^{\mathrm{T}}$ 表示矩阵 $\boldsymbol{A}$ 的转置，$[k]$表示集合 $\{1,2,\cdots,k\}$。对于概率分布 D 而言，$x\leftarrow D$ 表示 x 依概率分布D选取，对于集合S，$x\leftarrow S$ 表示 x 在集合S上均匀随机选取。$\|\boldsymbol{v}\|_\infty$、$\|\boldsymbol{A}\|_\infty$ 分别表示向量 $\boldsymbol{v}$ 及矩阵$\boldsymbol{A}$中元素最大的量级。$\lfloor x\rfloor,\lceil x\rceil\ (x\geqslant 0)$表示对数$x$向下和向上取整，$[x]_q$ 表示 $x(\mathrm{mod}\,q)$，$[\boldsymbol{A}]_q$ 表示对矩阵$\boldsymbol{A}$的每一个元素分别模q。规定 $\mathbb{Z}_q=(-q/2,q/2]\cap\mathbb{Z}$。

定义 1 (LWE问题[9])对于整数 $q=q(n)$，向量 $\boldsymbol{s}\in\mathbb{Z}_q^n$ 及一个 $\mathbb{Z}_q$ 上的误差分布 $\chi=\chi(n)$，选取 $\boldsymbol{a}\leftarrow\mathbb{Z}_q^n$ 及 $x\leftarrow\chi$，输出 $(\boldsymbol{a},<\boldsymbol{a},\boldsymbol{s}>+x)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$，该分布记为 $A_{\boldsymbol{s},\chi}$。$\mathrm{LWE}_{n,m,q,\chi}$ 的判定问题为：以不可忽略的优势来区分 m 个来自 $A_{\boldsymbol{s},\chi}$ 的取样和 m 个 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的均匀随机取样。文献[9]在2005年证明了在量子归约下，LWE问题至少与worst-case的近似因子为 $\widetilde{O}(n/\alpha)$ 的SVP、SIVP 的变体一样困难，其中 α 是LWE实例中与扰动分布的方差有关的参数。文献[10-11]分别给出了从GapSVP到LWE一个经典归约。

定义 2 (B界分布[12])对于一个定义在整数上的分布全体 $\{\chi_n\}_{n\in N}$，如果 $\Pr\limits_{\boldsymbol{e}\leftarrow\chi^n}[|\boldsymbol{e}|>B]$ 是可忽略的，则 $\{\chi_n\}_{n\in N}$ 称为B界的。

定理 1[12] 设 $q=q(n)\in\mathbb{N}$ 为素数的幂或者为不同poly(n)大小的素数的乘积，$B\geqslant\omega(\log n)\sqrt{n}$。那么存在一个有效的取样$B$界分布 χ，使得如果存在一个有效的算法解决参数为 n,q,χ 的一般情况的LWE困难问题，那么：

1) 存在一个有效的量子算法在 n 维格上解决 $\mathrm{GapSVP}_{\widetilde{O}(nq/B)}$；

2) 如果 $q\geqslant\widetilde{O}(2^{n/2})$，那么存在一个有效的经典算法在 n 维格上解决 $\mathrm{GapSVP}_{\widetilde{O}(nq/B)}$。

对于这两种情况，如果考虑以亚多项式的优势来区分，那么需要 $B\geqslant\widetilde{O}(n)$，并且最后的近似因子比 $\widetilde{O}(n^{1.5}q/B)$ 略大。

2 BGN加密方案

本节利用BGV12的加密方案设计了一种变形的加密方案。加密的明文为矩阵，密文也为矩阵。因为密文的乘法运算是矩阵的乘法，所以密文的规模在运算后没有增大。又因为该加密方案也支持任意次密文加法运算，所以为BGN加密方案。

2.1 BGN加密方案

BGN 加密方案由五元组(E.Setup , E.SecretKeygen, E.PublicKeygen, E.Enc, E.Enc, E.Dec)构成。

初始化阶段 $\mathrm{E.Setup}(1^\lambda,1^\mu)$：适应性地选择 μ 比特的模q，及参数 $n=n(\lambda,\mu)$，$m=\lceil(2n+1)\log q\rceil$，$\chi=\chi(\lambda,\mu)$。

密钥生成算法 $\mathrm{E.SecretKeygen}(1^n)$：选取 $\boldsymbol{S}\leftarrow\mathbb{Z}_q^{n\times m}$，输出 $\mathrm{sk}=\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\in\mathbb{Z}_q^{(n+m)\times(n+m)}$。

公钥生成算法 $\mathrm{E.PublicKeygen}(\boldsymbol{S})$：选取 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{m\times n}$ 及 $\boldsymbol{X}\leftarrow\chi^{n\times n}$，计算 $\boldsymbol{B}=[\boldsymbol{SA}+2\boldsymbol{X}]_q$。输出 $\mathrm{pk}=\begin{pmatrix}\boldsymbol{B}\\ -\boldsymbol{A}\end{pmatrix}\in\mathbb{Z}_q^{(n+m)\times n}$。

加密算法 $\mathrm{E.Enc}(\mathrm{pk},\mathrm{M})$：对于明文 $\boldsymbol{M}\in\{0,1\}^{n\times n}$，$\mathrm{pk}=\begin{pmatrix}\boldsymbol{B}\\ -\boldsymbol{A}\end{pmatrix}$，选取 $\boldsymbol{R}\in\{0,1\}^{n\times n}$，并输出密文 $\boldsymbol{C}=\left[\begin{pmatrix}\boldsymbol{BR}+\boldsymbol{M} & \boldsymbol{0}\\ -\boldsymbol{AR} & \boldsymbol{0}\end{pmatrix}\right]_q\in\mathbb{Z}_q^{(n+m)\times(n+m)}$。

解密算法 $\mathrm{E.Dec}(\mathrm{sk},\boldsymbol{C})$：对于密文 $\boldsymbol{C}$，$\mathrm{sk}=\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}$，令 $\boldsymbol{E}=\left[\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\boldsymbol{C}\right]_q$，然后输出 $m_{(i,j)}=\left[\left[<\boldsymbol{e}_i,\boldsymbol{s}_j>\right]_q\right]_2$，这里 $\boldsymbol{e}_i$ 是 $\boldsymbol{E}$ 的第i行，$\boldsymbol{s}_j$ 是 $\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}^{\mathrm{T}}$ 的第j列，$i,j\in[n]$。

注：解密算法中的右乘 $\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}^{\mathrm{T}}$ 是多余的，仅在乘积密文的解密中会用到。

命题 1 (正确性)设 $q,n,m,|\chi|\leqslant B$ 为上述加密方案E所需的参数，$\boldsymbol{S}\in\mathbb{Z}_q^{n\times m}$ 为任意矩阵，$\boldsymbol{M}\in\{0,1\}^{n\times n}$。令 $\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\leftarrow\mathrm{E.PublicKeygen}(\boldsymbol{S})$，$\boldsymbol{C}\leftarrow\mathrm{E.Enc}(\mathrm{pk},\boldsymbol{M})$，如果 $[\boldsymbol{M}+2\boldsymbol{XR}]_q=\boldsymbol{M}+2\boldsymbol{XR}$，那么 $\mathrm{E.Decs}(\mathrm{sk},\boldsymbol{C})=\boldsymbol{M}$。

证明：由定义可知 $\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\boldsymbol{C}\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}^{\mathrm{T}}=\begin{pmatrix}\boldsymbol{M}+2\boldsymbol{XR} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}(\mathrm{mod}q)$，因而解密正确。

引理 1 (安全性)[5]：设参数 m,n,q,χ，使得 $\mathrm{LWE}_{m,n,q,\chi}$ 成立，那么对任意的 $\boldsymbol{M}\in\mathbb{Z}_2^{n\times n}$，如果 $\begin{pmatrix}\boldsymbol{B}\\ -\boldsymbol{A}\end{pmatrix}\leftarrow \mathrm{E.PublicKeygen}(\boldsymbol{S})$，$\boldsymbol{R}\in\{0,1\}^{n\times n}$，则 $(\boldsymbol{BR},\boldsymbol{AR})$ 与 $\mathbb{Z}_q^{m\times n}\times\mathbb{Z}_q^{m\times n}$ 上的均匀分布计算不可区分。

2.2 同态性

设密文：

$$\boldsymbol{C}_1=\left[\begin{pmatrix}\boldsymbol{BR}_1+\boldsymbol{M}_1 & \boldsymbol{0}\\ -\boldsymbol{AR}_1 & \boldsymbol{0}\end{pmatrix}\right]_q$$

$$\boldsymbol{C}_2=\left[\begin{pmatrix}\boldsymbol{BR}_2+\boldsymbol{M}_2 & \boldsymbol{0}\\ -\boldsymbol{AR}_2 & \boldsymbol{0}\end{pmatrix}\right]_q$$

则：

1) 加法

对于适合的参数有：

$$\boldsymbol{C}^+=\boldsymbol{C}_1+\boldsymbol{C}_2=\left[\begin{pmatrix}\boldsymbol{B}(\boldsymbol{R}_1+\boldsymbol{R}_2)+(\boldsymbol{M}_1+\boldsymbol{M}_2) & \boldsymbol{0}\\ -\boldsymbol{A}(\boldsymbol{R}_1+\boldsymbol{R}_2) & \boldsymbol{0}\end{pmatrix}\right]_q$$

是 $[\boldsymbol{M}_1+\boldsymbol{M}_2]_2$ 的密文。

2) 乘法

规定密文乘积为 $\boldsymbol{C}^*=\boldsymbol{C}_1\boldsymbol{C}_2^{\mathrm{T}}\bmod q$。因此

$$\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\boldsymbol{C}^*\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}^{\mathrm{T}}=$$

$$\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\begin{pmatrix}\boldsymbol{BR}_1+\boldsymbol{M}_1 & \boldsymbol{0}\\ -\boldsymbol{AR}_1 & \boldsymbol{0}\end{pmatrix}\times$$

$$\left(\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\begin{pmatrix}\boldsymbol{BR}_2+\boldsymbol{M}_2 & \boldsymbol{0}\\ -\boldsymbol{AR}_2 & \boldsymbol{0}\end{pmatrix}\right)^{\mathrm{T}}\bmod q=$$

$$\begin{pmatrix}\boldsymbol{M}_1\boldsymbol{M}_2^{\mathrm{T}}+\boldsymbol{X}^* & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\bmod q$$

式中，$\boldsymbol{X}^*=2\boldsymbol{M}_1\boldsymbol{R}_2^{\mathrm{T}}\boldsymbol{X}_2^{\mathrm{T}}+2\boldsymbol{X}_1\boldsymbol{R}_1\boldsymbol{M}_2^{\mathrm{T}}+4X_1\boldsymbol{R}_1\boldsymbol{R}_2^{\mathrm{T}}\boldsymbol{X}_2^{\mathrm{T}}$，那么对于适合的参数 $\boldsymbol{C}^*=\boldsymbol{C}_1\boldsymbol{C}_2^{\mathrm{T}}\bmod q$ 为 $[\boldsymbol{M}_1\boldsymbol{M}_2^{\mathrm{T}}]_2$ 的密文。

2.3 参数设定

定理 2 令 n 为安全参数，任意的 $c=c(n)\geq 0$。设 $q>6n^{2c+6}$ 为素数，$m=\lceil(2n+1)\log q\rceil$，$B=n^{\frac{3}{2}}$。那么上述加密方案支持密文的 n^c 次加法和一次乘法运算。

证明：先考虑密文 $\boldsymbol{C}$ 为 $l\leqslant n^c$ 个密文的和，记

$$\boldsymbol{C}=\left[\begin{pmatrix}\boldsymbol{B}\sum_{i=1}^{l}\boldsymbol{R}_i+\sum_{i=1}^{l}\boldsymbol{M}_i & \boldsymbol{0}\\ -\boldsymbol{A}\sum_{i=1}^{l}\boldsymbol{R}_i & \boldsymbol{0}\end{pmatrix}\right]_q。$$

因为

$$\left\|\boldsymbol{B}\sum_{i=1}^{l}\boldsymbol{R}_i+\sum_{i=1}^{l}\boldsymbol{M}_i\right\|_\infty=l+2nBl<$$

$$n^c(1+2n^{5/2})<3n^{c+\frac{5}{2}}<\frac{q}{2}$$

所以 $\left[\sum_{i=1}^{l}\boldsymbol{M}_i+2\sum_{i=1}^{l}\boldsymbol{X}_i\boldsymbol{R}_i\right]_q=\sum_{i=1}^{l}\boldsymbol{M}_i+2\sum_{i=1}^{l}\boldsymbol{X}_i\boldsymbol{R}_i$，故 $\mathrm{E.Dec}(\mathrm{sk},\boldsymbol{C})=\left[\sum_{i=1}^{l}\boldsymbol{M}_i\right]_2$。

下面考虑密文 $\boldsymbol{C}'$ 为两个密文的乘积，这两个密文分别为 l_1,l_2 个密文的和，其中 $l_1+l_2\leqslant n^c$，记

$$\boldsymbol{C}'=\left[\begin{pmatrix}\boldsymbol{B}\sum_{i=1}^{l_1}\boldsymbol{R}_i+\sum_{i=1}^{l_1}\boldsymbol{M}_i & \boldsymbol{0}\\ -\boldsymbol{A}\sum_{i=1}^{l_1}\boldsymbol{R}_i & \boldsymbol{0}\end{pmatrix}\begin{pmatrix}\boldsymbol{B}\sum_{i=1}^{l_2}\boldsymbol{R}_i+\sum_{i=1}^{l_2}\boldsymbol{M}_i' & \boldsymbol{0}\\ -\boldsymbol{A}\sum_{i=1}^{l_2}\boldsymbol{R}_i & \boldsymbol{0}\end{pmatrix}^{\mathrm{T}}\right]_q。$$

因为：

$$\left\|\left(\sum_{i=1}^{l_1}\boldsymbol{M}_i+2\sum_{i=1}^{l_1}\boldsymbol{X}_i\boldsymbol{R}_i\right)\left(\sum_{i=1}^{l_2}\boldsymbol{M}_i'+2\sum_{i=1}^{l_2}\boldsymbol{X}_i\boldsymbol{R}_i\right)^{\mathrm{T}}\right\|_\infty=$$

$$n(l_1+2nBl_1)(l_2+2nBl_2)\leqslant$$

$$n(1+2nB)^2l_1(n^c-l_1)<$$

$$\frac{n^{2c+1}}{4}\left(1+4n^{\frac{5}{2}}+4n^5\right)<\frac{5}{4}n^{2c+6}<\frac{q}{2}$$

所以 $\mathrm{E.Dec}(\mathrm{sk},C')=\left[\left(\sum_{i=1}^{l_1}\boldsymbol{M}_i\right)\left(\sum_{i=1}^{l_2}\boldsymbol{M}_i\right)^{\mathrm{T}}\right]_2$。

注：本方案与GHV10[3]相比较，对于任意的 $c=c(n)>0$，仅要求 $q>6n^{2c+6}$ 为素数，而GHV10要求 $q>2^{20}(c+4)^3n^{3c+4}\log^5 n$ 为素数。这意味着如果 q 的范围扩大，则能支持比 $c=c(n)>0$ 更大的运算。

3 扩展成门限加密方案

本节首先介绍密钥同态，然后构造门限加密方案，最后证明该方案能抵抗密钥泄露攻击。

3.1 密钥同态

假设密钥 $\mathrm{sk}_i=\begin{pmatrix}\boldsymbol{I} & \boldsymbol{S}_i\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}=\mathrm{E.SecretKeygen}(1^n)$，选取 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{m\times n}$，$\boldsymbol{X}_i\leftarrow\chi^{n\times n}$，令：

$$\boldsymbol{B}_i=[\boldsymbol{S}_i\boldsymbol{A}+2\boldsymbol{X}_i]_q\in\mathbb{Z}_q^{n\times n}$$

那么 $\mathrm{pk}_i=\begin{pmatrix}\boldsymbol{B}_i\\ -\boldsymbol{A}\end{pmatrix}=\mathrm{E.PublicKeygen}(\boldsymbol{S}_i)$，$i=1,2$。

因为：

$$\begin{pmatrix}\boldsymbol{B}_1+\boldsymbol{B}_2\\ -\boldsymbol{A}\end{pmatrix}=\begin{pmatrix}(\boldsymbol{S}_1+\boldsymbol{S}_2)\boldsymbol{A}+2(\boldsymbol{X}_1+\boldsymbol{X}_2)\\ -\boldsymbol{A}\end{pmatrix}=$$
$$\text{E.PublicKeygen}(\boldsymbol{S}_1+\boldsymbol{S}_2)$$

所以得到了对应于结合密钥 $\text{sk}=\begin{pmatrix}\boldsymbol{I} & \boldsymbol{S}_1+\boldsymbol{S}_2\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}$ 的结合公钥 $\text{pk}=\begin{pmatrix}\boldsymbol{B}_1+\boldsymbol{B}_2\\ -\boldsymbol{A}\end{pmatrix}$，这就是密钥同态。

3.2 门限加密方案

类似于文献[8]，本文也假设存在一个可信第三方F，F计算结合公钥、密钥，然后把计算后的结果发送给各个参与者(假设共k个参与者)，并同时保证密钥的安全性。为了保证语义安全，本文同样加入了干扰噪音。

密钥生成算法TE.SecretKeygen(1^n)：取 $\boldsymbol{S}_i\leftarrow\mathbb{Z}_q^{n\times m}$，输出 $\text{sk}_i=\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}_i\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\in\mathbb{Z}_q^{(n+m)\times(n+m)}, i\in[k]$。

公钥生成算法 TE.PublicKeygen($\boldsymbol{S}$)：取 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{m\times n}$，$\boldsymbol{X}_i\leftarrow\chi^{n\times n}$，计算 $\boldsymbol{B}_i=[\boldsymbol{S}_i\boldsymbol{A}+2\boldsymbol{X}_i]_q$，输出 $\text{pk}_i=\begin{pmatrix}\boldsymbol{B}_i\\ -\boldsymbol{A}\end{pmatrix}\in\mathbb{Z}_q^{(n+m)\times n}$，$i\in[k]$。

当F从k个参与者中接收到 pk_i 后诚实地计算 $\boldsymbol{B}=\sum_{i=1}^{k}\boldsymbol{B}_i$。故结合公钥为：$\text{pk}=\begin{pmatrix}\boldsymbol{B}\\ -\boldsymbol{A}\end{pmatrix}$。

加密算法TE.Enc(pk，$\boldsymbol{M}$)：对于明文 $\boldsymbol{M}\in\{0,1\}^{n\times n}$ 及公钥 $\text{pk}=\begin{pmatrix}\boldsymbol{B}\\ -\boldsymbol{A}\end{pmatrix}$，均匀取 $\boldsymbol{R}\in\{0,1\}^{n\times n}$ 及干扰噪音 $\boldsymbol{X}^*$，输出密文 $\boldsymbol{C}=\left[\begin{pmatrix}\boldsymbol{BR}+\boldsymbol{M}+2\boldsymbol{X}^* & \boldsymbol{0}\\ -\boldsymbol{AR} & \boldsymbol{0}\end{pmatrix}\right]_q$。

解密算法TE.Dec$(\text{sk},\boldsymbol{C})$：各参与者把解密共享 $\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}_i\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\boldsymbol{C}\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}_i\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}^{\mathrm{T}}$ 发送给F，F诚实地计算 $\left[\sum_{i=1}^{k}\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}_i\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\boldsymbol{C}\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}_i\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}^{\mathrm{T}}\right]_q \bmod 2$。并输出明文$\boldsymbol{M}$。

正确性可由以下运算得出。

$$\left[\sum_{i=1}^{k}\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}_i\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\boldsymbol{C}\begin{pmatrix}\boldsymbol{I}_n & \boldsymbol{S}_i\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}^{\mathrm{T}}\right]_q \bmod 2=$$
$$\left[\begin{pmatrix}\boldsymbol{BR}+\boldsymbol{M}+2\boldsymbol{X}^*-\sum_{i=1}^{k}\boldsymbol{S}_i\boldsymbol{AR} & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\right]_q \bmod 2=$$
$$\left[\begin{pmatrix}\boldsymbol{M}+2\left(\boldsymbol{X}^*+\sum_{i=1}^{k}\boldsymbol{X}_i\boldsymbol{R}\right) & \boldsymbol{0}\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\right]_q \bmod 2$$

3.3 结合密钥的安全性

可以仿照文献[8]的游戏来证明结合密钥的安全性，即攻击者不能以显著优势区分在诚实公钥下的加密密文与均匀选取的假密文，证明省略。

4 结 束 语

本文基于BGV12，设计了一种基于LWE的BGN加密方案。与GHV10比较，有较好的参数规模，即对于任意的 $c=c(n)>0$，GHV10要求 $q>2^{20}(c+4)^3n^{3c+4}\log^5 n$ 为素数，而本文仅要求 $q>6n^{2c+6}$ 为素数。与BGV12比较，因为不再需要用到密钥交换、模转换等技术，一次乘法同态运算更高效。与ZXJXZ14类似，将BGN加密也扩展成一种门限加密方案，允许所有参与者共同解密一个密文而没有泄露明文的任何信息，并且能抵抗密钥泄露攻击。最后值得注意的是，类似于GHV10中的扩展及应用，同样可以把本文的加密方案扩展成身份基加密(也需要利用陷门T)、Two-Out-of-Two加密等。

本文得到信息安全国家重点实验室开放课题(2016-MS-10)的资助，在此表示感谢。

参 考 文 献

[1] 王小云, 刘明洁. 格密码学研究[J]. 密码学报, 2014, 1(1): 13-27.
WANG Xiao-yun, LIU Ming-jie. Survey of lattice-based cryptography[J]. Journal of Cryptologic Research, 2014, 1(1): 13-27.

[2] BONEH D, GOHE J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts[C]//Proceedings of Second Theory of Cryptography Conference, TCC 2005. Cambridge, MA, USA: Springer, 2005: 325-341.

[3] GENTRY C, HALEVI S, VAIKUNTANATHAN V. A simple bgn-type cryptosystem from LWE[C]//Proceedings of Advances in Cryptology-EUROCRYPT 2010. Riviera, French: Springer, 2010: 506-522.

[4] MICCIANCIO D, PEIKERT C. Trapdoors for lattices: Simpler, tighter, faster, smaller[C]//Proceedings of Advances in Cryptology-EUROCRYPT 2012. Cambridge, UK: Springer, 2012: 700-718.

(下转第111页)

WU Ying. Improved brightness preserving bi-histogram equalization algorithm[J]. Journal of Computer Applications, 2010, 30(6): 1632-1634.

[14] 吕宗伟. 基于亮度保持的子图像加权对比度增强[J]. 电子学报, 2013, 41(2): 282-287.
LÜ Zong-wei. Brightness preservation based weighted sub-images for contrast enhancement[J]. Acta Electronica Sinica, 2013, 41(2): 282-287.

[15] 余权, 马胜前, 马冬梅. 保持图像亮度的自适应局部对比度增强[J]. 计算机工程与应用, 2015, 51(7): 160-164.
YU Quan, MA Sheng-qian, MA Dong-mei. Adaptive local contrast enhancement with brightness preservation[J]. Computer Engineering and Applications, 2015, 51(7): 160-164.

[16] 曾磊, 童莉, 李中国, 等. 基于直方图峰值的 PCB 三维 CT 图像双直方图均衡算法[J]. 信息工程大学学报, 2014, 15(3): 319-324.
ZENG Lei, TONG Li, LI Zhong-guo, et al. PCB three dimensional CT image enhancement based on maximum histogram coefficient bi-histogram equalization[J]. Journal of Information Engineering University, 2014, 15(3): 319-324.

[17] THIEN H T, THUONG L T. Brightness preserving weighted dynamic range histogram equalization for image contrast enhancement[C]//IEEE International Conference on Advanced Technologies for Communications. Ho Chi Minh, Vietnam: 2013: 386-391.

编 辑 叶 芳

(上接第98页)

[5] ZHANG Wei. A BGN-type multiuser homomorphic encryption scheme[C]//Proceedings of 2015 International Conference on Intelligent Networking and Collaborative Systems. Taipei, Taiwan, China: IEEE, 2005: 268-271.

[6] BRAKERSHI Z, GENTRY C, VAIKUNTANATHAN V. (Leveled) fully homomorphic ncryption without bootstrapping[C]//Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. Cambridge, Massachusetts: ACM. 2012: 309-325.

[7] HIROMASA R, ABE M, OKAMATO T. Packing messages and optimizing bootstrapping in GSW-FHE[C]// Proceedings of Public-Key Cryptography-PKC 2015. Gaithersburg, MD, USA: Springer, 2015: 699-715.

[8] ZHANG Xiao-jun, XU Chun-xiang, JIN Chun-hua, et al. Efficient fully homomorphic encryption from RLWE with an extension to a threshold encryption scheme[J]. Future Generation Computer Systems, 2014(36): 180-186.

[9] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]//Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing. Baltimore, MD, USA: ACM, 2005: 84-93.

[10] PEIKERT C. Public-key cryptosystems from the worst-case shortest vector problem[C]//Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM, 2009: 333-342.

[11] BRAKERSKI Z, LANGLOIS A, PEIKERT C, et al. Classical hardness of learning with errors[C]//Proceedings of the 45th Annual ACM Symposium on Symposium on Theory of Computing. New York: ACM, 2013: 575-584.

[12] GENTRY C, SAHAIY A, WATERS B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based[C]//Proceedings of Advances in Cryptology-CRYPTO 2013. Santa Barbara, CA, USA: Springer, 2013: 75-92.

编 辑 蒋 晓