$$\Delta=\frac{1}{2}\sqrt{|Y|/|X|}=\frac{1}{2}\sqrt{q^{(n+1)}/2^M}.$$

欲使$\Delta\leqslant 1/2^n=negl(n)$成立,则充分条件是:

$$M=(n+1)\lceil\log q\rceil+2n \tag{6}$$

最后,从方案的正确性考虑:

$$|error|=|e+\boldsymbol{e}_1^T\boldsymbol{r}-\boldsymbol{d}^T\boldsymbol{e}_2|\leqslant|e|+|\boldsymbol{e}_1^T\boldsymbol{r}|+|\boldsymbol{d}^T\boldsymbol{e}_2| \tag{7}$$

因为 $e\leftarrow\chi_B$,根据引理 2:

$$|e|\leqslant B=q\alpha\cdot\omega\left(\sqrt{\log n}\right) \tag{8}$$

由 $\boldsymbol{r}\leftarrow\{0,1\}^M$, $\boldsymbol{e}_1\leftarrow\chi_B^M$, $M=(n+1)\lceil\log q\rceil+2n$ 和文献[15]中命题 2.3 可知:

$$|\boldsymbol{e}_1^T\boldsymbol{r}|\leqslant\sqrt{M}q\alpha\cdot\omega\left(\sqrt{\log n}\right)=q\alpha\cdot O\left(\sqrt{n\log q}\right)\cdot\omega\left(\sqrt{\log n}\right) \tag{9}$$

由 $\boldsymbol{d}\leftarrow SampleD(\boldsymbol{R},\overline{\boldsymbol{A}},\boldsymbol{u},s_2),s_2=\sqrt{7(\mathcal{S}_1(\boldsymbol{R})^2+1)},\mathcal{S}_1(\boldsymbol{R})\leqslant O\left(\sqrt{n\log q}\right)\cdot\omega\left(\sqrt{\log n}\right)$ 可知:

$$s_2=O\left(\sqrt{n\log q}\right)\cdot\omega\left(\sqrt{\log n}\right) \tag{10}$$

根据引理 4,等价地有 $\boldsymbol{d}\leftarrow D_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}),s_2\cdot\omega\left(\sqrt{\log n}\right)}$. 又 $\boldsymbol{e}_2\leftarrow\chi_B^N$, 根据事实 1[29]、引理 2 和公式(5):

$$\begin{aligned}|\boldsymbol{e}_2^T\boldsymbol{d}|&\leqslant\|\boldsymbol{d}\|q\alpha\cdot\omega\left(\sqrt{\log n}\right)\\&\leqslant\sqrt{N}s_2\cdot\omega\left(\sqrt{\log n}\right)\cdot q\alpha\cdot\omega\left(\sqrt{\log n}\right)\\&=\sqrt{2n\lceil\log q\rceil}\cdot s_2q\alpha\cdot\omega\left(\sqrt{\log n}\right)^2\\&=q\alpha O(n\log q)\cdot\omega\left(\sqrt{\log n}\right)^3\\&=q\alpha O(n\cdot\log n)\cdot\omega\left(\sqrt{\log n}\right)^3\end{aligned} \tag{11}$$

由公式(7)~公式(9)和公式(11)可知:

$$\begin{aligned}|error|&\leqslant|e|+|\boldsymbol{e}_1^T\boldsymbol{r}|+|\boldsymbol{d}^T\boldsymbol{e}_2|\\&\leqslant q\alpha\left(\omega\left(\sqrt{\log n}\right)+O\left(\sqrt{n\log q}\right)\cdot\omega\left(\sqrt{\log n}\right)+O(n\log n)\cdot\omega\left(\sqrt{\log n}\right)^3\right)\\&=q\alpha O(n\log n)\cdot\omega\left(\sqrt{\log n}\right)^3.\end{aligned}$$

取 $\alpha=1\Big/\left(O(n\log n)\cdot\omega\left(\sqrt{\log n}\right)^3\right)$, 可满足 $2|error|<q/2$.又因为 $\sqrt{n}\geqslant\log n\geqslant 4$ 和 $q\alpha>2\sqrt{n}$, 所以可取素数:

$$q=O(n^2)\omega\left(\sqrt{\log n}\right)^3 \tag{12}$$

由公式(4)、公式(6)、公式(10)和公式(12),我们有如下定理:

定理 4(存在性). 设安全参数 $n\geqslant 16$,若取:

$q=O(n^2)\omega\left(\sqrt{\log n}\right)^3$, $M=(n+1)\lceil\log q\rceil+2n$,$N=2n\lceil\log q\rceil$, $\alpha=1\Big/\left(O(n\log n)\cdot\omega\left(\sqrt{\log n}\right)^3\right)$,$s_2=O\left(\sqrt{n\log q}\right)\omega\left(\sqrt{\log n}\right)$,

则存在一个语义安全的无证书加密方案.

4.4 效 率

下面把本文的 CLPKE 与目前现存的格上无证书加密方案[25,26]作效率比较.为此,设 n 为安全参数,q 为模数,m 为系统所生成格的维数,$k=\lceil\log q\rceil$,尺寸以数据的比特长度来计.为方便比较,典型地取 $\omega\left(\sqrt{\log n}\right)=\log n$, 如文献[2,30].考虑到文献[25]可能为多比特加密方案,故比较密文尺寸和加(解)密计算量时,我们采用每比特真正消息的平均密文尺寸和加(解)密平均计算量,如平均密文尺寸等于 ℓ 比特消息被加密为密文的总长度除以消息的比特个数 ℓ.类似地定义加(解)密平均计算量.这样,我们选择了 13 项指标.

首先,文献[25]中方案的参数 $m,q,\tilde{O}(n/\alpha)$ 的取值同文献[26],分别大于我们方案对应的参数取值(见表 1).引入参数 ℓ 和 d,其中,ℓ 表示真正被加密的消息长度 $x\in\{0,1\}^{\ell}$,d 表示多比特版本的 HIBE 和 IBE 加密方案每次可处

理的最大比特串长度.当使用 d 比特版本的 HIBE 和 IBE 方案加密 $\{0,1\}^{\ell+\bar{m}}$ 时,不妨假定这 $\ell+\bar{m}$ 个比特恰好分成 t 组,每组含 d 个比特,即 $dt=\ell+\bar{m}$.系统私钥 $\boldsymbol{T}_0\in\mathbb{Z}^{m\times m}$ 满足 $\|\boldsymbol{T}_0\|\leqslant\sigma_0\sqrt{m}\leqslant O(n\log q)$ 且 $m=O(n\log q)$,故取 $\sigma_0=\sqrt{n\log q}$ 为矩阵 $\boldsymbol{T}_0$ 中元素绝对值的上界.用户的部分私钥 $\boldsymbol{T}_{id}\in\mathbb{Z}^{2m\times 2m}$ 矩阵是利用 $\boldsymbol{T}_0\in\mathbb{Z}^{m\times m}$ 为陷门基抽样后再随机化所得,所以 $\boldsymbol{T}_{id}$ 中元素绝对值的上界不小于 $\boldsymbol{T}_0$ 中元素绝对值的上界,所以用户私钥的尺寸至少为 $180n^2k^2\log\sqrt{n\log q}$. 生成用户部分私钥需要 $O((2m)^2)$次格上离散高斯抽样,每次抽样的复杂度[2]为 $O((2m)^2)$,所以生成用户部分私钥需要计算量为 $O((2m^2))\cdot O((2m^2))=O(n^4k^4)$.

Table 1 Efficiency comparison

表 1 效率对比

方案	Ref.[25]	Ref.[26]	本文
维数m	$6nk$	$6nk$	$2nk$
模数q	$O(n^4k^{3.5})\omega(\log n)^3$	$O(n^4k^{3.5})\omega(\log n)^3$	$O(n^2)\omega\left(\sqrt{\log n}\right)^3$
近似因子 $\tilde{O}(n/\alpha)$	$\tilde{O}(n^{4.5})$	$\tilde{O}(n^{4.5})$	$\tilde{O}(n^2)$
系统公钥尺寸	$24n^2k\log q+dn\log q$	$6n^2k\log q$	$2n^2k\log q$
系统私钥尺寸	$36n^2k^2\log\left(\sqrt{n\log q}\right)$	$36n^2k^2\log\left(\sqrt{n\log q}\right)$	$n^2k^2\log\left(4\sqrt{n}\right)$
用户公钥尺寸	$28nk\log q+dn\log q$	$(6n^2k+n)\log q$	$(n^2k+2nk+k+2n^2+2n)\log q$
用户私钥尺寸	$\geqslant 180n^2k^2\log\sqrt{n\log q}$	$\geqslant 15nk\log(6nk)$	$\leqslant(1.5n+5.5nk)\log n$
平均密文尺寸	$\left(2+\frac{30nk(\ell+10nk)}{\ell d}+\frac{20nk+n}{\ell}\right)\log q$	$(12nk+1)\log q$	$(2nk+n+1)\log q$
生成用户公钥计算量	不需要计算	$O(n^2\log^2 q\log n)$	$O(n^2\log^2 q\log n)$
生成用户部分私钥计算量	$O(n^4k^4)$	$O(n^2k^2)$	$O(n\log n)$
生成用户私钥计算量	不需要计算	$O(n^2\log^2 q\log^2 n)$	不需要计算
加密平均计算量	$\frac{1}{\ell}[O(n^3k\log^2 q)+O(tn^2k\log q\log n)+O(tdn\log q\log n)]$	$O(n^2\log^3 q)$	$O(n^2\log^2 q\log n)$
解密平均计算量	$\frac{1}{\ell}[O(n^3k\log^2 q)+O(dn^2k^2)+O(tdnk\log q\log n))]$	$O(n\log^2 q\log n)$	$O(n\log^2 q\log n)$

在文献[26]中,用户私钥$(\boldsymbol{t},\boldsymbol{e})\in\mathbb{Z}^m\times\mathbb{Z}^m$ 且 $\boldsymbol{t}\leftarrow D_{\mathbb{Z}^m,\sigma_1}$,$\boldsymbol{e}\leftarrow D_{\mathbb{Z}^m,\sigma_2}$,其中,

$$\sigma_1=m\omega(\log m),\sigma_2=\|\boldsymbol{t}\|\sigma_s,\sigma_s=\sqrt{m}O\left(\sqrt{n\log q}\right)\omega(\log m).$$

这样,$\sigma_1>m,\sigma_2=\|\boldsymbol{t}\|\sigma_s>\sqrt{m}\sigma_s=mO\left(\sqrt{n\log q}\right)\omega(\log m)>\sqrt{m^3}$.

所以,用户私钥尺寸至少为 $2.5m\log m=15nk\log(6nk)$.生成用户的部分私钥需要做一次 m 维格上的离散高斯抽样,所以生成用户部分私钥需要计算量为 $O(m^2)=O(n^2k^2)$.

在本文中,系统私钥 $\boldsymbol{R}\leftarrow D_{\mathbb{Z},s_1}^{nk\times nk}$,$s_1=4\omega\left(\sqrt{\log n}\right)\leqslant 4\sqrt{n}$,系统私钥尺寸不大于 $n^2k^2\log\left(4\sqrt{n}\right)$.用户私钥$(\boldsymbol{x},\boldsymbol{d})\in\mathbb{Z}^n\times\mathbb{Z}^N$ 且 $\boldsymbol{x}\leftarrow D_{\mathbb{Z}^m,q\alpha}$,$\boldsymbol{d}\leftarrow SampleD(\boldsymbol{R},\bar{\boldsymbol{A}},\boldsymbol{u},s_2)$. 根据参数设置,可以 $1-negl(n)$概率保证 $0<q<n^{2.5}\omega\left(\sqrt{\log n}\right)^2$,$0<\alpha<1\Big/\left(n\omega\left(\sqrt{\log n}\right)^3\right)$,则有 $2\sqrt{n}<q\alpha\cdot\omega\left(\sqrt{\log n}\right)<n^{1.5}$,即$\|\boldsymbol{x}\|_\infty<n^{1.5}$.

又根据引理 2 和引理 4,$\|\boldsymbol{d}\|_\infty\leqslant s_2\cdot\omega\left(\sqrt{\log n}\right)^2=O\left(\sqrt{n\log q}\right)\omega\left(\sqrt{\log n}\right)^3<n^{2.75}$.这样,用户私钥的尺寸至多为 $n\log n^{1.5}+N\log n^{2.75}=(1.5n+5.5nk)\log n$.因为采用文献[6]中陷门生成算法,所以本文生成用户部分私钥需要计算量为 $O(n\log n)$.

表 1 给出了 3 个方案在相同安全参数 n 下的比较结果.结果显示:

(1) 与文献[25]中单比特版本方案相比(即 $d=1$),除了生成用户公/私钥计算量这两项指标(其中,在生成用户私钥计算量上二者持平)以外,本文方案在表 1 中所列的其他各项指标上均有明显优势.

(2) 与文献[25]中多比特版本方案相比(即 $d>1$ 且 $d|(\ell+10nk)$),在生成用户公钥计算量上我们的方案处于劣

势.在平均密文尺寸上,当 $1<d\leqslant 15$ 且ℓ为满足 $d|(\ell+10nk)$条件的任意正整数,或者当 $15<d\leqslant \ell+10nk$ 且ℓ为满足 $d|(\ell+10nk)$和 $1\leqslant \ell<25$ 的正整数时,我们的方案占优势;但是当 $k\leqslant d\leqslant \ell+10nk$ 且ℓ为满足 $d|(\ell+10nk)$和$\ell\geqslant 30nk$ 的正整数时,文献[25]中的方案占优势(这里给出各个方案占优的充分条件,下同).在加密平均计算量方面,当$\ell\leqslant O(n)$且 d 为满足 $d|\ell+10nk,d>1$ 的任意正整数,或者当$\ell>O(n)$且 d 为满足 $d|\ell+10nk,1<d\leqslant 1+10nk/\ell$的任意正整数时,都是我们的方案占优;当$\ell>O(n)$且 d 为满足 $d|\ell+10nk,d\geqslant O(nk)$的任意正整数时,文献[25]中的方案占优势.另外,在生成用户私钥计算量上二者持平.因此,除了上述 4 个指标以外,本文方案在所列的其余 9 项指标上均有显著的优势(与参数ℓ和 d 的取值无关).

(3) 与文献[26]相比,本文方案在表 1 中所列的各项指标上均有明显优势.

5 结 论

本文在格上借助于文献[6]中陷门生成方法提出一个单比特的无证书加密方案.该方案在随机预言模型下被证明是语义安全的.与文献[25,26]中的方案相比,我们的方案具有更短的公/私钥和更低的解密平均计算量,尤其是比文献[26]有更短的密文及更简单、自然的用户公/私钥生成算法.这种简单的算法也有力地促成了把单比特变为多比特的无证书加密方案,而且在单比特方案安全情况下选择的参数,如 m,q,N,M,α,s_2,可以不变地直接应用到后者,并使后者具有与前者同样的安全性.另外,我们的方案可根据实际情况对明文空间做 $\mathbb{Z}_2\to\mathbb{Z}_2^t\to\mathbb{Z}_p^t$ 的扩展,还可以方便地把它移植到多项式环上,以获得更小的参数和更好的效率.

致谢 我们向给予支持和提出宝贵建议的评审专家深表感谢.

References:

[1] Regev O. On lattices, learning with errors, random linear codes, and cryptography. In: Proc. of the STOC. New York, ACM, 2005. 84−93. [doi: 10.1145/1060590.1060603]

[2] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Proc. of the STOC. New York, ACM, 2008. 197−206. [doi: 10.1145/1374376.1374407]

[3] Gentry C. Fully homomorphic encryption using ideal lattices. In: Mitzenmacher M, ed. Proc. of the STOC. New York, ACM, 2009. 169−178. [doi: 10.1145/1536414.1536440]

[4] Agrawal S, Boneh D, Boyen X. Efficient lattice (H)IBE in the standard model. In: Gilbert H, ed. Proc. of the EUROCRYPT 2010. LNCS 6110, Berlin, Heidelberg: Springer-Verlag, 2010. 553−572. [doi: 10.1007/978-3-642-13190-5_28]

[5] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In: Rogaway P, ed. Proc. of the CRYPTO 2011. LNCS 6841, Berlin, Heidelberg: Springer-Verlag, 2011. 505−524. [doi: 10.1007/978-3-642-22792-9_29]

[6] Micciancio D, Peikert C. Trapdoor for lattices: Simpler, tighter, faster, smaller. In: Pointcheval D, Johansson T, eds. Proc. of the EUROCRYPT 2012. LNCS 6223, Berlin, Heidelberg: Springer-Verlag, 2012. 191−208. [doi: 10.1007/978-3-642-29011-4_41]

[7] Micciancio M, Peikert C. Hardness of SIS and LWE with small parameters. In: Canetti R, Garay JA, eds. Proc. of the CRYPTO 2013. Part I. LNCS 8042, Berlin, Heidelberg: Springer-Verlag, 2013. 21−39. [doi: 10.1007/978-3-642-40041-4_2]

[8] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. Journal of the ACM, 2013,60(6): 1−35. [doi: 10.1145/2535925]

[9] Boneh D, Gentry C, Gorbunov S, Halevi S, Nikolaenko V, Segev G, Vaikuntanathan V, Vinavagamurthy D. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In: Nguyen PQ, Oswald EE, eds. Proc. of EUROCRYPT 2014. LNCS 8441, Berlin, Heidelberg: Springer-Verlag, 2014. 533−556. [doi: 10.1007/978-3-642-55220-5_30]

[10] Ducas L, Lyubashevsky V, Prest T. Efficient identity-based encryption over NTRU lattices. In: Sarkar P, Iwata T, eds. Proc. of ASIACRYPT 2014. Part II. LNCS 8874, Berlin, Heidelberg: Springer-Verlag, 2014. 22−41. [doi: 10.1007/978-3-662-45608-8_2]

[11] Nguyen PQ, Zhang J, Zhang ZF. Simpler efficient group signatures from lattices. In: Kate J, ed. Proc. of the PKC 2015. LNCS 9020, Berlin, Heidelberg: Springer-Verlag, 2015. 401−426. [doi: 10.1007/978-3-662-46447-2_18]

[12] Brakerski Z, Gentry C, Vaikuntanathan V. Fully homomorphic encryption without Bootstrapping. In: Goldwasser S, ed. Proc. of the Innovations in Theoretical Computer Science. 2012. 309−325. [doi: 10.1145/2090236.2090262]

[13] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-Simpler, asymptotically-faster, attribute-based. In: Canetti R, Garay JA, eds. Proc. of the CRYPTO 2013. Part I. LNCS 8042, Berlin, Heidelberg: Springer-Verlag, 2013. 75−92. [doi: 10.1007/978-3- 642-40041-4_5]

[14] Alperin-Sheriff J, Peikert C. Faster bootstrapping with polynomial error. In: Garay JA, Gennaro R, eds. Proc. of the CRYPTO 2014. LNCS 8616, Berlin, Heidelberg: Springer-Verlag, 2014. 297−314. [doi: 10.1007/978-3-662-44371-2_17]

[15] Brakerski Z, Vaikuntanathan V. Lattice-Based FHE as secure as PKE. In: Proc. of the ITCS. 2014. 1−12. http://eprint.iacr.org/2013/541

[16] Gorbunov S, Vaikuntanathan V, Wichs D. Leveled fully homomorphic signatures from standard lattices. In: Proc. of the STOC. New York, ACM, 2015. 469−477. http://eprint.iacr.org/2014/897 [doi: 10.1145/2746539.2746576]

[17] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Laih CS, ed. Proc. of the ASIACRYPT 2003. LNCS 2894, Berlin, Heidelberg: Springer-Verlag, 2003. 452−473. [doi: 10.1007/978-3-540-40061-5_29]

[18] Dent A. A survey of certificateless encryption schemes and security models. Int'l Journal of Information Security, 2008,7(5): 347−377. [doi: 10.1007/s10207-008-0055-0]

[19] Zhou CX, Zhou W, Dong XW. Provable certificateless generalized signcryption scheme. Designs, Codes and Cryptography, 2014, 71(2):331−346. [doi: 10.1007/s10623-012-9734-y]

[20] Chen H, Zhang FT, Song RS. Certificateless proxy signature scheme with provable security. Ruan Jian Xue Bao/Journal of Software, 2009,20(3):692−701 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/574.htm [doi: 10.3724/SP.J.1001.2009.00574]

[21] Chen H, Zhu CJ, Song RS. Efficient certificateless signature and group signature schemes. Journal of Computer Research and Development, 2010,47(2):231−237 (in Chinese with English abstract).

[22] Zhang L, Wu QH, Domingo-Fener J, Qin B, Zeng P. Signatures in hierarchical certificateless cryptography: Efficient constructions and provable security. Information Sciences, 2014,272:223−237. [doi: 10.1016/j.ins.2014.02.085]

[23] Chin JJ, Behnia R, Heng SH, Phan RCW. Cryptanalysis of a certificateless identification scheme. Security and Communication Networks, 2015,8(2):122−125. [doi: 10.1002/sec.963]

[24] Zhang FT, Sun YX, Zhang L, Geng MM, Li SJ. Research on certificateless public key cryptography. Ruan Jian Xue Bao/Journal of Software, 2011,22(6):1316−1332 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4007.htm [doi: 10.3724/SP.J.1001.2011.04007]

[25] Sepahi R, Steinfeld R, Pieprzyk J. Lattice-Based certificateless public-key encryption in the standard model. Int'l Journal of Information Security, 2014,13(4):315−333. [doi: 10.1007/s10207-013-0215-8]

[26] Jiang MM, Hu YP, Lei H, Wang BC, Lai QQ. Lattice-Based certificateless encryption scheme. Frontiers of Computer Science, 2014,8(5):828−836. [doi: 10.1007/s11704-014-3187-6]

[27] Lindner R, Peikert C. Better key sizes (and attacks) for LWE-based encryption. In: Kiayias A, ed. Proc. of the CT-RSA 2011. LNCS 6558, Berlin, Heidelberg: Springer-Verlag, 2011. 319−339. [doi: 10.1007/978-3-642-19074-2_21]

[28] Alwen J, Peikert C. Generating shorter bases for hard random lattices. In: Proc. of the Symp. on Theoretical Aspects of Computer Science. 2009. 75−86. [doi: 10.1007/s00224-010-9278-3]

[29] Peikert C, Vaikuntanathan V, Waters B. A framework for efficient and composable oblivious transfer. In: Wagner D, ed. Proc. of the CRYPTO 2008. LNCS 5157, Berlin, Heidelberg: Springer-Verlag, 2008. 554−571. [doi: 10.1007/978-3-540-85174-5_31]

[30] Gentry C, Halevi S, Vaikuntanathan V. A simple BGN-type cryptosystem from LWE. In: Gilbert H, ed. Proc. of the EUROCRYPT 2010. LNCS 6110, Berlin, Heidelberg: Springer-Verlag, 2010. 506−522. [doi: 10.1007/978-3-642-13190-5_26]

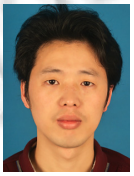
附中文参考文献:

[20] 陈虎,张福泰,宋如顺.可证安全的无证书代理签名方案.软件学报,2009,20(3):692−701. http://www.jos.org.cn/1000-9825/574.htm [doi: 10.3724/SP.J.1001.2009.00574]

[21] 陈虎,朱昌杰,宋如顺.高效的无证书签名和群签名方案.计算机研究与发展,2010,47(2):231−237.

[24] 张福泰,孙银霞,张磊,耿曼曼,李素娟.无证书公钥密码体制研究.软件学报,2011,22(6):1316−1332. http://www.jos.org.cn/1000-9825/4007.htm [doi: 10.3724/SP.J.1001.2011.04007]

陈虎(1975－),男,江苏睢宁人,博士,副教授,主要研究领域为密码学.



连至助(1986－),男,博士生,主要研究领域为密码学.

胡予濮(1955－),男,博士,教授,博士生导师,主要研究领域为密码学.

贾惠文(1990－),男,博士生,主要研究领域为密码学.