LINEture 后量子数字签名方案的安全参数分析

Yevgen Kotukh[2][0000-0003-4997-620X] 和 Gennady Khalimov[1][0000-0002-2054-9186]

[1] 哈尔科夫国立无线电电子大学，乌克兰哈尔科夫[2] 叶夫亨尼·别列兹尼亚克军事学院，基辅，乌克兰 yevgenkotukh@gmail.com

摘要。 本文对 *LINEture* 后量子数字签名方案的安全参数进行了全面的密码学分析。该方案基于初等阿贝尔 *2*-群上的矩阵代数构造。我们研究了三个主要参数对密码强度的影响：字长 m（呈二次影响）、向量维度 l，以及会话密钥中的子矩阵数量 q（呈线性影响）。分析揭示了参数 l 的双重性质：根据原作者的分析，它不会影响方案抵抗猜测攻击的能力；然而，对验证机制的深入考察表明，l 确立了一个大小为 $l \cdot m$ 比特的“验证屏障”。我们确定了阈值关系 $l < (q-1) \cdot m$，低于该阈值时，参数 l 将成为安全性的关键因素。为实现最高密码学效率，本文提出了最优选择规则 $l \approx (q-1) \cdot m$。文中还提供了与 *NIST* 后量子密码标准的比较分析及实用参数建议。

关键词：后量子密码学、数字签名、基于矩阵的密码学、阿贝尔群、安全性分析、参数优化。

I. 引言

量子计算的进步对现有密码系统构成了根本性威胁，因为这些系统依赖整数分解和离散对数问题的计算困难性。Shor 算法能够在量子计算机上高效求解这些问题，因此有必要开发能够抵御量子攻击的替代性密码原语 [1]。

美国国家标准与技术研究院（NIST）于2024年结束了后量子密码标准化进程，选定基于格的方案（CRYSTALS-Dilithium、Falcon）和基于哈希的签名（SPHINCS+）作为主要标准 [2]。尽管如此，探索其他构造仍然十分重要，因为密码学多样性不可或缺，而且在资源受限环境中可能存在效率更高的解决方案。

LINEture 密码系统是一种新颖的后量子数字签名方案，基于阶为 2m 的初等阿贝尔 2-群上的线性矩阵代数构建。该系统在 Fiat-Shamir 范式中采用零知识证明机制 [3]。该系统的一个显著优势是密钥紧凑性：密钥大小约为 300–500 字节，而 Dilithium 的密钥大小为 2–3 KB。

尽管这一构造在理论上颇具吸引力，但对 LINEture 的安全参数进行严格论证的研究仍不充分。特别是，参数 l——即替换向量的维数——在确保密码强度方面所发挥的作用尚不明确，值得进一步深入分析。

本文旨在全面分析参数 (m, l, q) 对 LINEture 密码系统安全性的影响，识别潜在的依赖关系，并为最优参数选择提出建议。

II. 数学基础

A. 参数结构

LINEture 密码系统由三个主要参数定义，详见表I。

表I。主要密码系统参数

参数	值	函数
m	8 或 16 比特	字长（替换元素）
l	8 或 16	向量维度（m 位字的数量）
q	3 或 4	会话密钥 K 中子矩阵的数量

B. 会话密钥结构

会话密钥 K 由 q 个子矩阵拼接而成，每个子矩阵的维度为 m×m：

$$K = [H_1 \mid H_2 \mid R_1 \mid R_2 \mid \ldots \mid R_{q-2}] \qquad (1)$$

其中，H1 和 H2 是由消息哈希 h(r1, msg) 和 h(r2, msg) 确定性导出的子矩阵，而 R_i 是随机秘密子矩阵。密钥空间的基数为：

$$|K_{secret}| = 2^{m^2 \cdot (q-l)} \qquad (2)$$

C. 共享密钥与替换向量

共享密钥 S = (S1, S2, ..., Sl)由一个包含*l*个双射替换的向量 S_i: $\{0,1\}^m \to \{0,1\}^m$构成。一个关键特性是，针对*l*个分量中的每个分量，秘密都是**独立地**计算的，但使用的是一个**共用的**会话密钥 K:

$$S_i = f(B_i, K), \quad i = 1, \ldots, l \qquad (3)$$

D. 密码原语大小

B基于对密码系统的结构分析，已确定以下大小关系 ed:

公钥：pk = 6·l·m2/8 字节 私钥：sk = l·m2/8 + 辅助参数 签名：sign = l·m/8 + 2(q−l)·m2/8 + 64 字节

III. 安全性分析

A. 会话密钥猜测攻击

根据该密码系统作者给出的原始安全性分析，主要攻击途径是猜测会话密钥。安全级别由以下因素表征:

$$S_{guessing} = 2 \cdot (q-l) \cdot m^2 \text{ bits} \qquad (4)$$

作者的重要观察：参数 *l* 在方程（4）中**缺失**。原始研究中的安全性表（表 II）也证实了这一点。

表 II. 安全级别

(m, l, q)	$S_{guessing}$	$S_{collision}$
(8, 8, 3)	256 比特	~224 比特
(8, 16, 3)	256 比特	~224 比特
(16, 8, 3)	1024 比特	~896 比特
(16, 16, 3)	1024 比特	~896 比特

如表 II 所示，配置 (8,8,3) 和 (8,16,3) 的猜测安全性相同（256 比特），尽管 l 的取值不同。

B. 碰撞攻击

碰撞攻击与参数 l 和 q 无关，仅由字长 m 决定:

$$S_{collision} \approx 3.5 \cdot m^2 \text{ bits} \qquad (5)$$

对于 m=8，这约为 224 比特；无论 q 如何增加，这都是 m 较小时的**限制因素**。

C. 作者分析中的参数影响

根据原始分析，参数对安全性的影响如下：***m* - 严重** （二次影响，m2）：安全性的基本单位
***q* - 显著** （线性影响）：q 每增加一个单位，安全性增加 2m2 比特 ***l* - 辅助**：仅决定哈希大小（l×m 比特）和密钥维度

A. 签名验证机制

对验证过程的详细分析揭示了参数 l 的潜在作用。在验证过程中，需要验证 **l 个独立方程**是否成立:

$$S_i(z_i) = h_i, \quad \forall i = 1, \ldots, l \qquad (6)$$

在猜测攻击中，攻击者生成候选 K'，并计算 S' = (S'1, ..., S'l)。要使攻击成功，**所有 l 个方程**必须同时成立。

B. 概率分析

如果 K' 猜测错误，那么 $S'_i \neq S_i$ 以高概率成立。单个方程发生偶然巧合的概率为:

$$P(S'_i(z_i) = h_i \mid S'_i \neq S_i) = 2^{-m} \qquad (7)$$

对于所有 *l* 个方程同时成立:

$$P_{success} = (2^{-m})^{l} = 2^{-l \cdot m} \qquad (8)$$

基本结论：参数 l 建立了一个额外的**l·m 比特**“验证屏障”，将可行攻击的空间限制为原来的 $2^{l \cdot m}$ 分之一。

C. 线性代数分析

对于身份验证证明，两个会话密钥 K1 和 K2 必须产生相同的共享密钥：

$$A \cdot K_1 \cdot B = A \cdot K_2 \cdot B = S \qquad (9)$$

This 该条件会生成一个由 l·m 个 GF(2) 上的线性方程组成的方程组。有效攻击空间变为 es:

$$2^{2(q-1)m^2 - l \cdot m} \qquad (10)$$

D. 参数 *l* 的阈值

当 l·m < (q−1)·m2 时，参数 l 会影响安全性，即：

$$\boldsymbol{l < (q-1) \cdot m} \qquad (11)$$

这定义了参数 l 的阈值（表 III）。

表 III. 参数 l 的阈值

m	q	阈值 l	l=8 状态
8	3	16	严重
8	4	24	严重
16	3	32	严重

为直观展示各项参数对安全性和密码系统效率的影响，我们绘制了全面的图形分析（图 1 和图 2）。

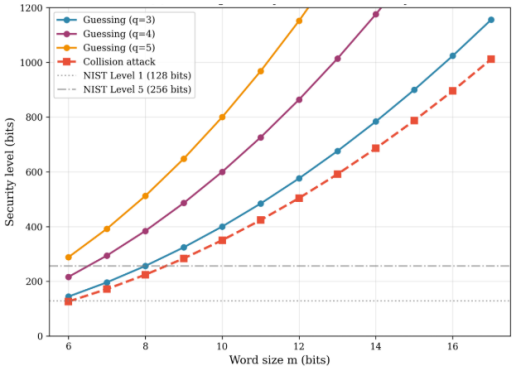

图1 – 猜测安全性与碰撞安全性

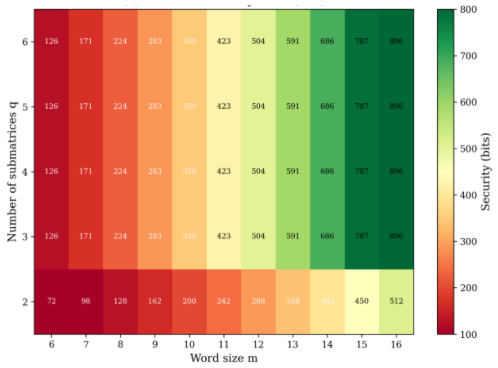

图2 – 最低安全级别的安全性热图

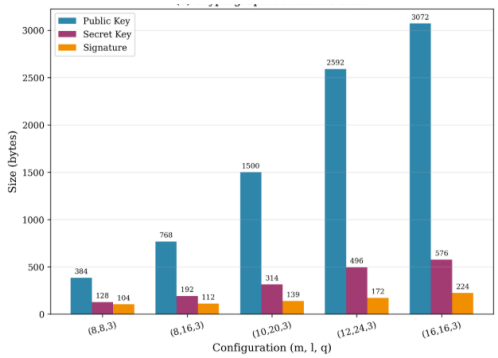

图 3 – 秘密密钥、公钥和数字签名的大小

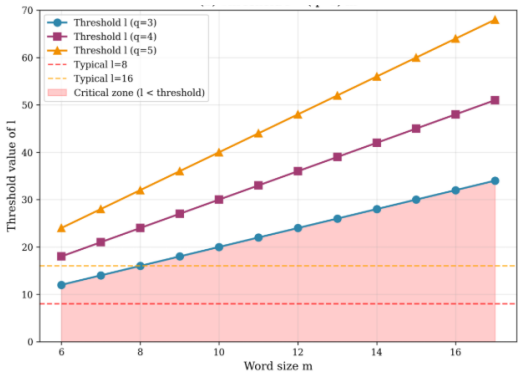

图 4 – 阈值 l=(q-1)m

IV. 最优参数选择

A. 结果综合

结合作者的分析以及我们对验证屏障的深入分析，我们构建了一个更完善的安全模型：$S_{effective} = min(2(q-1)m2, 3.5m2, l \cdot m + (q-1)m2/2)$ (12)

其中，第三项计入了当 $l < (q-1)\cdot m$ 时的验证屏障。

B. 最优选择规则

基于所进行的分析，我们提出以下选择规则：

规则1（最优 l）：$l_{opt} = (q-1)\cdot m$。低于此阈值的取值会因验证屏障不足而导致安全性下降；nt 验证屏障；价值 上述方案会增大尺寸，但不会带来安全性提升。

规则2（m 的选择）：为抵御碰撞攻击，建议使用 $m \geq 10$。当 m=8 时，无论其他参数如何，抗碰撞性都仅约为 224 比特。

规则 3（q 缩放）：增大 q 可有效增强抗猜测性（每增加一个单位的 q，可提升 +2m2 比特），且不会显著增大密钥大小。

表 IV. 推荐配置

级别	(m, l, q)	安全性	Size	效率
基础	(8, 16, 3)	224 比特	~800 B	0.28
标准	(10, 20, 3)	350 比特	~1.2 KB	0.29
High	(12, 24, 3)	504 比特	~1.8 KB	0.28

C. 与 *NIST* 后量子密码标准的比较

表 V. 与 NIST 后量子密码标准的比较

方案	安全性	签名	PK
LINEture (10,20,3)	~350 比特	~450 B	~750 B
Dilithium-II	~128 比特	~2420 B	~1312 B
Falcon-512	~128 比特	~666 B	~897 B

LINEture 在签名紧凑性方面具有显著优势（小 3-5× ），同时提供更高的安全级别。不过需要注意的是，美国国家标准与技术研究院的标准已经过严格的密码分析，而 LINEture 仍需接受更多独立审查。

V. 讨论

A. 参数 l 的双重性质

从直接猜测攻击的角度来看（公式 4），安全性表达式中确实没有 l——作者的表格也证实了这一点。然而，深入考察验证机制（公式 8）会发现一个潜在的“验证屏障”。

要调和这两种观点，关键在于认识到，当 $l \geq (q-1)\cdot m$ 时，验证屏障会变得冗余，不会影响有效安全性。然而，对于典型取值 $l=8$ 、$m=8$ 和 $q=3$，条件 $l < (q-1)\cdot m = 16$ 成立，因此参数 l 对安全性至关重要。

B. 对密码系统的关键观察

尽管具有吸引人的特性，LINEture 仍存在若干显著局限：

1. **缺乏形式化安全证明**——该系统未能归约到公认的计算困难问题。2. **线性代数结构**——可能易受原文未讨论的代数攻击。3. **抗量子性尚未得到严格确立**——所声称的后量子安全性仍需正式证明。4. **缺乏独立密码分析**——该系统尚未经历类似美国国家标准与技术研究院 NIST 后量子密码标准化项目的公开竞赛。

VI. 结论

本文对 LINEture 后量子数字签名密码系统的安全参数进行了全面的密码学分析。主要发现如下：

1. 根据公式 $S = 2(q-1)\ m2$ 比特，确定了参数 m 对抵御猜测攻击的能力的二次影响，以及参数 q 的线性影响。

2. 揭示了参数 l 的双重性质：根据作者的评估，它不会影响安全性；然而，对验证过程的深入分析表明，会形成一个大小为 $l\cdot m$ 比特的“验证屏障”。

3. 确定了阈值关系 $l < (q-1)\cdot m$，低于该阈值时，参数 l 会成为严重的安全因素。

4. T已提出最优选择规则 $l_{opt} = (q-1)\cdot m$，以实现最高的密码学效率 y.

5. 已针对三个安全级别提出建议，并考虑了安全性与尺寸权衡。

我们考虑以下进一步研究方向。首先，在随机预言机模型下给出形式化安全性证明；其次，分析其抵抗量子代数攻击的能力，并比较软件和硬件实现的效率。

参考文献

[1] Khalimov, G., Kotukh, Y., Kolisnyk, M., Khalimova, S., Sievierinov, O., & Volkov, O. (2024年, November). SIGNLINE：基于线性方程密码系统的数字签名方案。载于*2024*年第四届电气、计算机、通信与机电一体化工程国际会议（*ICECCME*）（第1-9页）。IEEE。[2] Khalimov, G., Kotukh, Y., Kolisnyk, M., Khalimova, S., Sievierinov, O., & Korobchynskyi, M. (2025年, March). 基于线性方程的数字签名方案。载于未来信息与通信会议（第711-728页）。Cham：Springer Nature Switzerland。[3] Gennady Khalimov, Yevgen Kotukh, Maksym Kolisnyk, Svitlana Khalimova, Oleksandr Sievierinov。LINE：基于线性方程的对数签名密码系统。https://eprint.iacr.org/2024/697.pdf，论文2024/697。[4] Khalimov, G., Kotukh, Y., & Khalimova, S. (2020年, December). 基于Ree函数域自同构群的加密方案。载于*2020*年第七届物联网：系统、管理与安全国际会议（*IOTSMS*）（第1-8页）。IEEE。[5] Khalimov, G., Sun, X., Kotukh, Y., & Dzhura, I. 新型密钥封装方法。载于*IEMTRONICS 2025*论文集：国际物联网、电子与机电一体化会议，第*2*卷（第55页）。Springer Nature。[6] Khalimov, G., Kotukh, Y., Shonia, O., Didmanidze, I., Sievierinov, O., & Khalimova, S. (2020年, October). 基于Suzuki函数域自同构群的加密方案。载于*2020*年*IEEE*信息通信问题科学与技术国际会议（*PIC S&T*）（第383-387页）。IEEE。[7] G. Khalimov, Y. Kotukh, S. Khalimova, M. Korobchynskyi, V. Podlipaiev, O. Zaitsev。LINE密码系统的密码分析。2025年第五届电气、计算机、通信与机电一体化工程国际会议（ICECCME），桑给巴尔，坦桑尼亚联合共和国，2025年，第1-7页，doi: 10.1109/ICECCME64568.2025.11277439[8] Khalimov, G., Kotukh, Y., Didmanidze, I., & Khalimova, S. (2021年, July). 基于小Ree群的加密方案。载于*2021*年第七届计算机技术应用国际会议论文集（第33-37页）。[9] Khalimov, G., & Kotukh, Y. (2025). 基于Ree群的安全加密方案。*arXiv*预印本 *arXiv:2504.17919*。[10] Khalimov, G., & Kotukh, Y. (2025). 采用Hermitian函数域三参数群的MST3加密改进。*arXiv*预印本 *arXiv:2504.15391*。

[11] Khalimov, G., & Kotukh, Y. (2025). 基于小Ree群的改进MST3加密方案。arXiv预印本 arXiv:2504.10947。[12] Khalimov, G., & Kotukh, Y. (2025). 基于广义Suzuki 2-群的高级MST3加密方案。arXiv预印本 arXiv:2504.11804。[13] Khalimov, G., & Kotukh, Y. (2025). 通过Suzuki函数域自同构群强化MST3密码系统的密码强度。arXiv预印本 arXiv:2504.07318。[14] G. Khalimov, Y. Kotukh, Yu. Serhiychuk, O. Marukhnenko.《基于Suzuki群的密码系统实现复杂度分析》。《电信与无线电工程杂志》，第78卷，第5期，2019年，419 427 10 1615 78 540 21 期，页码 -。DOI：。/TelecomRadEng.v .i . .[15] Y. Kotukh.《通用哈希在电信系统中实现可证明抗攻击认证方案中的应用》。《电信与无线电工程杂志》，第75卷，第7期，2016年，第 595 605 10 1615 75 7 30 -页。[16] 2025 DOI：。/TelecomRadEng.v .i . Kotukh, Y. V., Khalimov, G. Z., & Dzhura, I. Y. ( ). 基于非交换群的密码系统的密码学竞争力。《Radiotekhnika》，（221），72-82。[17] Котух, Є., Марухненко, О., Халімов, Г., & Коробчинський, M. (2023). 以基于广义Suzuki 2-群的MST3密码系统为例，制定密码变换库的测试方法。《网络安全：教育、科学、技术》电子专业科学刊物，2(22)，113-121。[18] Kotukh, E. ., Severinov, O. ., Vlasov, A. ., Kozina, L. ., Tenytska, A. ., & Zarudna , E. . (2021). 对数签名的构造方法与性质。《Radiotekhnika》，2(205), 94–99。https://doi.org/ 10 30837 2021 2 205 09 . /rt. . . . Kotukh, Y., & Khalimov, H. ( ). 对数签名[19] 2024 在密码原语实现中的优势。《现代科学的挑战与问题》，*2*, 296 299 119 -。[20] 2021 https://cims.fti.dp.ua/j/article/view/ Kotukh, E., Severinov, O., Vlasov, A., Kozina, L., Tenytska, A., & Zarudna, E. ( ). 对数签名的构造方法与性质。《Radiotekhnika》，2(205)，94-99。