Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

6th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS

(PKIA 2025)

SEPTEMBER 3-4th, 2025

Lightweight and Efficient Module-LWE Identity-Based Encryption Scheme for Post-Quantum Security

Kamna Sahu, Srinivasa KG, Satyanarayana Vollala
IIIT Naya Raipur, India

C-DAC

https://pkiindia.in

Social Media
/pkiindia

IEEE BANGALORE SECTION

Contents

Introduction

- Traditional public-key crypto (RSA, ECC) broken by quantum (Shor's algorithm)
- Need for Post-Quantum Cryptography (PQC)
- Identity-Based Encryption (IBE): Keys derived from identity
- Problem: Existing LWE/Module-LWE IBE → huge MPK/MSK sizes

Motivation & Problem Statement

- IBE attractive for IoT, decentralized systems
- Existing schemes impractical (MBs of storage)
- Key storage critical bottleneck
- Goal: Lightweight, storage-efficient IBE

Related Work

- Shamir's IBE, Boneh–Franklin (pairings)
- GPV trapdoor lattice IBE
- Ducas et al. LWE-IBE → large keys
- Approx Trapdoor IBE (ACISP 2023)- Faster trapdoor gen but large keys[7]
- NTRU-based schemes (DLP-IBE)- still large keys[8]
- NTRU-based schemes (Latte) - Compact keys but lower security[13]
- **Gap:** No focus on drastic MPK/MSK compression

Proposed Scheme – Overview

- A Lightweight Modulo-LWE Identity-Based Encryption Scheme with Seed-Based Key Compression for Post-Quantum Security
- Standard IBE structure: Setup, Extract, Encrypt, Decrypt
- Two innovations:

1) Seed-based MPK/MSK compression

2) Dual-mode benchmarking

Contribution & IBE Flow

❑ **Contribution:**

- **Seed-based compression: Store only 32B seeds for MPK & MSK → regenerate using SHAKE-256.**
- **Dual-mode framework: Compare full-storage vs. compressed-storage performance.**
- **Exact byte-level key/cipher text sizes measured.**
- **Multi-parameter evaluation: 80-bit to 256-bit PQ security.**

❑ **IBE Flow:**

- **Setup: Generate MPK & MSK (full or compressed).**
- **Extract: Use MSK trapdoor to derive identity-specific secret key.**
- **Encrypt: Use MPK & identity to encrypt.**
- **Decrypt: Recover message using identity's secret key.**

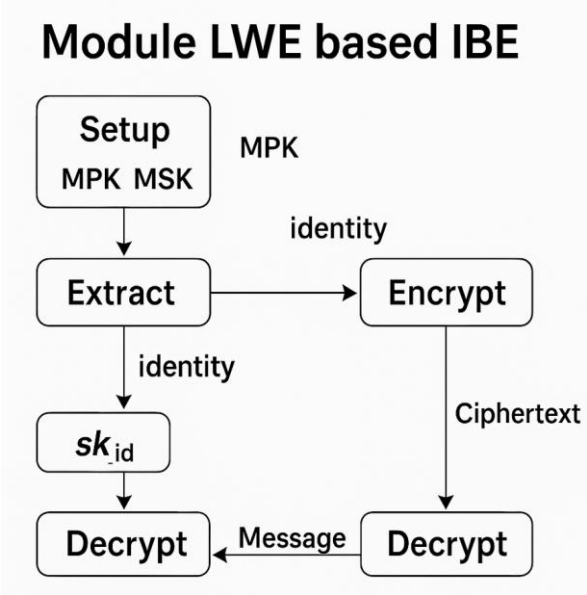

Fig 1. IBE Workflow

Proposed Scheme – Construction

❑ Algorithm 1: Setup

Input: (n, q), SEED_BYTES
If Full Mode:
  Generate full A ∈ Zq^(n×l), T ∈ Zq^(l×n)
Else (Compressed Mode):
  Generate seeds (seedA, seedT) of 32B
  Regenerate A, T via SHAKE-256 on demand
Output: mpk, msk

❑ Algorithm 2: Extract

Input: ID, msk, mpk
h = H(ID) ∈ Zq^n
Use trapdoor T to solve A·r ≡ h (mod q) for short r
Output: skID

❑ Algorithm 3: Encrypt

Input: mpk, ID, m ∈ {0,1}
Sample s, e1 ∈ Zq^n, e2 ∈ Zq from χ
h = H(ID)
u = A^T s + e1 (mod q)
v = ⟨h, s⟩ + e2 + m·(q/2) (mod q)
Output: CT = (u, v)

❑ Algorithm 4: Decrypt

Input: skID, (u, v)
m' = v − ⟨u, r⟩ (mod q)
If m' closer to 0 → output 0, else 1

❑ **Correctness:** Decrypt(Extract(ID,msk),Encrypt(ID,m)) = m

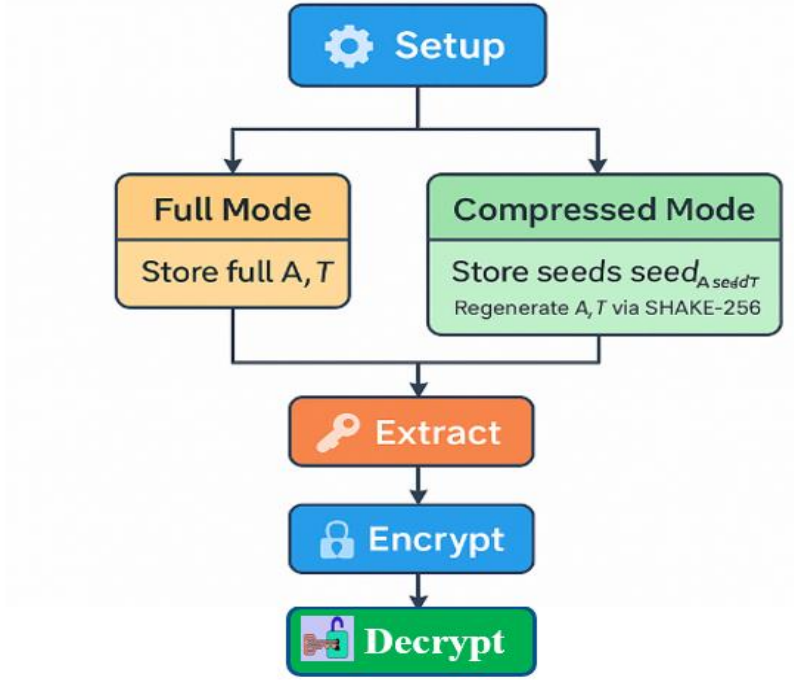

Fig. 2. Proposed Module LWE based IBE

Performance Evaluation

Metric	Full Mode	Compressed Mode
MPK (B)	1,179,648	32
MSK (B)	1,179,648	32
Reduction (%)	–	99.997
SKID (B)	1,536	1,536
CT (B)	1,538	1,538
Setup (ms)	215.16	0.01
Extract (ms)	1.96	380.33
Enc (ms)	2.45	2.57
Dec (ms)	0.01	0.01

Table I :Performance results for proposed work under the default parameter set

n	$\log_2(q)$	Security Parameter	Mode	MPK (B)	MSK (B)	SK (B)	CT (B)	Setup (ms)	Extract (ms)	Enc (ms)	Dec (ms)
512	23	<80	Full	2,097,152	2,097,152	2,048	2,050	345.10	2.10	2.90	0.01
512	23	<80	Compressed	32	32	2,048	2,050	0.01	600.55	2.85	0.01
768	~12	192	Full	1,179,648	1,179,648	1,536	1,538	215.16	1.96	2.45	0.01
768	~12	192	Compressed	32	32	1,536	1,538	0.01	380.33	2.57	0.01
1024	25	>128	Full	8,388,608	8,388,608	8,192	8,196	1,250.33	4.80	4.52	0.01
1024	25	>128	Compressed	32	32	8,192	8,196	0.01	1,050.44	4.50	0.01
2048	25	>256	Full	33,554,432	33,554,432	16,384	16,388	4,950.11	8.52	46.59	0.02
2048	25	>256	Compressed	32	32	16,384	16,388	0.01	2,200.88	46.55	0.02

Table II : Performance results for proposed across multiple parameter sets

Default Parameters (NIST L3, n=768):
- MPK/MSK: **1.18 MB → 32B** (99.997% reduction)
- Extract: 1.96 ms → 380 ms
- Enc/Dec ~unchanged (~2.5 ms / 0.01 ms)

Multi-parameter sets:
- **n=512: <80 bits → testing**
- **n=1024: >128 bits → high security**
- **n=2048: >256 bits → over kill**

- **Full Mode** – stores full A, T → fast performance
- **Compressed Mode** – stores seeds → extreme size reduction

Results and Comparison

Metric	Prop. Work	Trapdoor IBE2 [7]	Trapdoor IBE1 [7]	Latte [13]
Sec. (bits)	**192**	≈192	≈80	128
MPK (KB)	**0.03**	31.25	14.38	3.00
MSK (KB)	**0.03**	34.38	15.81	12.00
SK (KB)	**1.50**	34.38	15.81	3.00
CT (KB)	**1.50**	34.38	15.81	6.03
Enc (ms)	**2.57**	1.10	1.05	0.06
Dec (ms)	**0.01**	0.07	0.05	0.06

Table III : Comparison with prior lattice-based IBE schemes

Gap Filled by Proposed Work:

- MPK/MSK much smaller than:
  - Approx Trapdoor IBE (31–34 KB)
  - Latte (3–12 KB)
- First IBE with **seed-based MPK/MSK compression**
- Maintains strong PQ security with drastic **>99.99% storage reduction**

Feature	Our Work	[7]	[8]	[13]
Lattice Basis	**Mod-LWE**	Mod-LWE/iNTRU	NTRU	NTRU
Trapdoor Type	**Std. LWE + mod opt.**	Approx. gadget	NTRU trap.	NTRU trap.
Seed MPK Comp.	**✓ 32B**	✗	✗	✗
Seed MSK Comp.	**✓ 32B**	✗	✗	✗
Dual Mode Eval.	✓	✗	✗	✗
Exact Byte / q	✓	✗	✗	✗
Multi-Param Test	✓	✗	✗	✗
CT Size Opt.	✓	✗	✗	✗
Embedded Impl.	✓	✗	✗	✗
PQ Security	✓	✓	✓	✓

Table IV: Feature Comparison Of Identity-based Encryption Schemes

Conclusion & Future Work

- Proposed lightweight Module-LWE IBE with seed-based compression
- Reduces MPK/MSK from MB → 32B (99.99% reduction)
- Negligible impact on encryption/decryption
- Strong candidate for PQC in resource-constrained systems
- Future work:
  - Hierarchical, Attribute-based , Revocable IBE
  - Hardware optimization
  - Side-channel resistance
  - Extend to other lattice primitives

References

[1] R.L.Rivest, “Cryptography,” in Algorithms and complexity, pp. 717 755,Elsevier,1990.

[2] P.W.Shor, “Algorithms for quantum computation : discrete logarithms and factoring,” inProceedings35thannual symposiumon foundations ofcomputerscience,pp.124–134, Ieee,1994.

[3] D. J. Bernstein and T. Lange, “Post-quantum cryptography ” Nature, vol.549,no.7671,pp.188–194,2017.

[4] NIST, “Post-quantum cryptography,” csrc.nist.gov/projects/post quantum-cryptography,May09,2024.

[5] K.deBoer and W.van Woerden,“Lattice-based cryptography: Asurvey on the security of the lattice-based nist finalists,” Cryptology ePrint Archive,2025. [6] L.Martin,“Identity-basedencryptioncomesofage,”Computer,vol.41, no.8,pp.93–95,2008.

[7] M. Izabach`ene, L. Prabel, and A. Roux-Langlois, “Identity-based encryption from lattices using approximate trapdoors,” inAustralasian ConferenceonInformationSecurityandPrivacy,pp.270–290,Springer, 2023.

[8] L. Ducas, V. Lyubashevsky, and T. Prest, “Efficient identity-based encryption over ntru lattices,” in International Conference on the Theory and Application of Cryptology and Information Security, pp. 22–41, Springer,2014.

[9] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Workshop on the theory and application of cryptographic techniques, pp.47–53,Springer,1984.

[10] D. Boneh and M. Franklin, “An efficient public key traitor tracing scheme,”in Annual International Cryptology Conference,pp.338–353, Springer,1999.

[11] C. Gentry, C. Peikert, andV. Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions,” in Proceedings of the fortiethannualACMsymposiumonTheoryofcomputing,pp.197–206, 2008.

[12] L. Ducas, V. Lyubashevsky, and T. Prest, “Efficient identity-based encryption over ntru lattices,”in Advances in Cryptology–ASIACRYPT 2014(P.SarkarandT. Iwata, eds.),2014.

[13] R.K. Zhao, S. McCarthy, R. Steinfeld,A. Sakzad, andM.O’Neill, “Quantum-safe hibe: does it cost a latte?,” IEEE Transactions on InformationForensicsandSecurity,vol.19,pp.2680–2695,2023.

[14] S. Agrawal, D. Boneh, and X. Boyen, “Efficient lattice (h) ibe in the standard model,” in Advances in Cryptology–EUROCRYPT2010: 29thAnnual International Conference on the Theory and Applications of Cryptographic Techniques, FrenchRiviera,May30–June 3, 2010. Proceedings29,pp.553–572,Springer,2010.

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

THANK YOU

C-DAC

https://pkiindia.in

Social Media
/pkiindia

IEEE BANGALORE SECTION