PQIE: Post-Quantum Identity Encryption

Data Tables — Supplementary for Manuscript Submission

Table 1: Comparison of did:pqie with Existing DID Methods

Feature	did:key	did:ethr	did:indy	did:peer	did:pqie (Ours)
Quantum-Safe Keys	NO	NO	NO	NO	**YES**
Encrypted DID Document	NO	NO	NO	NO	**YES**
Multi-Chain Anchoring	NO	NO	NO	NO	**YES**
ZKP Service Tokens	NO	NO	**YES**	NO	**YES**
Homomorphic Noise Filter	NO	NO	NO	NO	**YES**
W3C VC Support	NO	**YES**	**YES**	**YES**	**YES**
SPHINCS+ Signing	NO	NO	NO	NO	**YES**
Key Recovery	NO	**YES**	**YES**	NO	**YES**
Offline Resolution	**YES**	NO	NO	**YES**	**YES**

Table 2: PQIE Framework Block Summary

Block	Stage	Algorithm / Protocol	Output	Latency (ms)
O	User Input	Attribute Seeding	Raw Citizen Data	< 1
A	Key Generation	Ring-LWE / NTT	PK, SK, DID string	2.1
B	Noise Injection	Homomorphic Noise Filter	Obfuscated DID Document	0.8
C	Signing	SPHINCS+ / Ed25519-Hybrid	Signed VC Bundle	3.7
D	Encryption	AES-256-GCM (KEM-wrapped)	Ciphertext Payload	1.2
E	Anchoring	Indy / Ethereum / Polkadot	Ledger Tx Hash (3 chains)	18.4
F	Resolution	SDIS Resolver	Decrypted DID Document	4.9

Table 3: PQIE-Enc's Security Parameters

Parameter	Symbol	Value	Justification
Ring Dimension	n	1024	NIST Level 5 (256-bit PQ security)
Modulus	q	12289	NTT-friendly prime; minimizes noise growth

Parameter	Symbol	Value	Justification
Noise Distribution	χ	Gaussian $\sigma=3$	Balances correctness vs. security
Ciphertext Size	|ct|	~1.5 KB	Compact; suitable for HTTP headers
Public Key Size	|pk|	~1.3 KB	Standard Ring-LWE output
AES Wrapping Key	K_enc	256-bit AES	GCM mode; 96-bit random IV per session
SPHINCS+ Signature	σ_pq	~17 KB	SHA-256 instantiation; stateless
Hash Function	H	SHA3-512	Domain-separated for DID and VC contexts
Classical Security	λ_c	≥ 256 bits	Against Grover + lattice attacks
Quantum Security	λ_q	≥ 128 bits	Against Shor (inapplicable to Ring-LWE)

Table 4: Ring-LWE Cryptographic Parameters and Security Comparison

Scheme	Key Size	Sig. Size	Security Assumption	Quantum-Safe	NIST Level
RSA-2048	256 B	256 B	Factoring	NO	—
ECDSA (P-256)	64 B	64 B	ECDLP	NO	—
Ed25519	32 B	64 B	ECDLP	NO	—
Kyber-1024	1568 B	N/A	Ring-LWE	**YES**	5
SPHINCS+-256s	64 B	17 kB	Hash function	**YES**	5
Falcon-1024	1793 B	1280 B	NTRU Lattice	**YES**	5
PQIE Ring-LWE	~1.3 kB	~17 kB	Ring-LWE	**YES**	5

Table 5: Threat Model and Mitigations

Threat	Attack Vector	PQIE Mitigation	Residual Risk
Quantum Key Break	Shor's on EC keys	Ring-LWE (n=1024)	None (PQ-hard)
Grover Search	Brute-force on AES-128	AES-256-GCM enforced	Negligible
DID Correlation	Public ledger analysis	ZKP tokens + noise injection	Minimal
VC Forgery	Signature substitution	3-of-3 SPHINCS+ multi-sig	Minimal
Replay Attack	Token re-submission	Nonce + ledger anchoring	None
Man-in-the-Middle	TLS downgrade	Cert-pinned mTLS + DID auth	Minimal
Ledger Compromise	Single-chain attack	3-chain cross-anchoring	Low (2-of-3)
Side-Channel	Cache/branch profiling	Constant-time NTT impl.	Research area

Threat	Attack Vector	PQIE Mitigation	Residual Risk
Credential Leak	Wallet compromise	Selective disclosure (Merkle)	Low
Data Retention	PII on-chain	Encrypted payloads only	None

Table 6: PQIE Performance Benchmarks Across Platforms

Operation	Laptop (i7-12th)	Raspberry Pi 4	WebAssembly (Browser)	Target (≤)
DID Generation (Ring-LWE)	2.1 ms	11.3 ms	18.7 ms	20 ms
DID Document Encryption	1.2 ms	6.4 ms	9.1 ms	15 ms
Homomorphic Noise Injection	0.8 ms	4.1 ms	6.3 ms	10 ms
SPHINCS+ Signing	3.7 ms	19.2 ms	32.4 ms	40 ms
VC Issuance (full flow)	4.8 ms	24.7 ms	41.2 ms	50 ms
Multi-Chain Anchoring	18.4 ms	82.3 ms	—	100 ms
DID Resolution (SDIS)	4.9 ms	21.6 ms	38.5 ms	50 ms
ZKP Token Generation	6.2 ms	31.8 ms	52.1 ms	60 ms
End-to-End KYC Flow	41.1 ms	201 ms	—	250 ms

Table 9: Measured Performance Parameters (Averages over 100 iterations)

Operation	Mean (ms)	Median (ms)	Min (ms)	Max (ms)	±SD
Ring-LWE Transform (NTT+SHA3)	11.88	9.53	9.41	243.59	23.41
DID Generation (single chain)	0.06	0.01	0.01	4.74	0.47
DID Document Generation	12.37	11.76	10.75	18.18	1.61
Multi-Chain DID Generation (×3)	0.04	0.04	0.04	0.09	0.01
PQIE Keypair Generation	0.29	0.28	0.28	0.99	0.07
PQIE Signing (ML-DSA/FSA)	2.44	1.84	0.92	8.83	1.87
PQIE Signature Verification	0.60	0.60	0.59	0.69	0.02
Chain Detection from DID prefix	0.00	0.00	0.00	0.00	0.00
Universal DID Resolution	1.49	1.46	1.43	3.58	0.22
Cross-Chain Credential Lookup	0.75	0.72	0.70	2.16	0.15
Citizen Chain Summary	2.03	2.00	1.96	3.31	0.14
ZKP Service Token Generation	0.14	0.13	0.13	0.50	0.04

Operation	Mean (ms)	Median (ms)	Min (ms)	Max (ms)	±SD
DID Document Verification	0.61	0.60	0.59	0.73	0.02

* Measured on macOS 15.5 (Apple Silicon M-series), Python 3.13.3, 100 iterations, single-threaded, no concurrent load.

Tables 1–6 latency measurements are median values over 1,000 iterations. Table 9 values are from run_benchmarks.py (100 iterations on laptop CPU). WebAssembly benchmarks use WASM-compiled Ring-LWE (Emscripten 3.1.x). — indicates not applicable in browser context.