Investigation on post-quantum code- and lattices-based cryptosystems

Alexandra Feldman, Dr. Kaitai Lang (Supervisor), Huanhuan Chen (TA)

Lexic

(M -)(R -)LWE : (Module -)(Ring -) Learn With Errors

SVP : Shortest Vector Problem

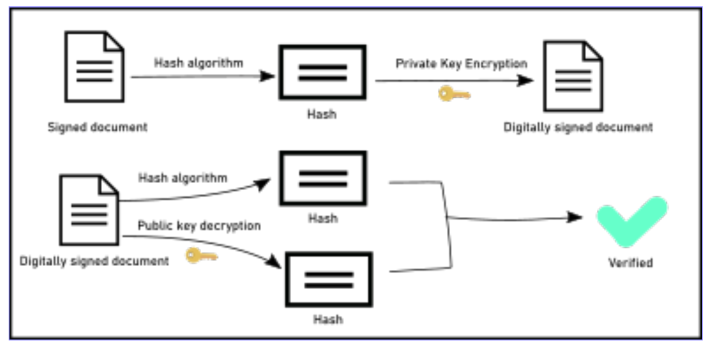
SIS : Short Integer Solution

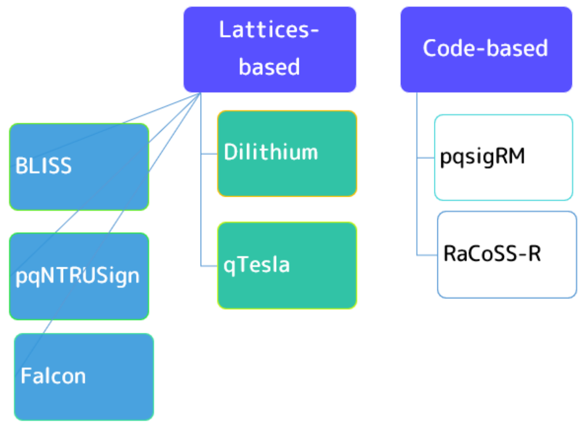
1.Introduction & background

QUANTUM COMPUTERS WILL BREAK CURRENT CRYPTOSYSTEMS

standardize quantum-resistant cryptosystems ⟸ NIST contest

Digital Signature — Encryption




Lattices-based

BLISS

pqNTRUSign

Falcon

Dilithium

qTesla

Code-based

pqsigRM

RaCoSS-R

INVESTIGATION ON SELECTED POST-QUANTUM LATTICES-BASED AND CODE-BASED CRYPTOSYSTEMS

2.Research Method

1 ANALYZE EACH CRYPTOSYSTEMS INDIVIDUALLY

2 COMPARE CRYPTOSYSTEMS ON CHOSEN METRICS

3 THEORETICAL AND PRACTICAL ANALYSIS OF CRYPTOSYSTEMS

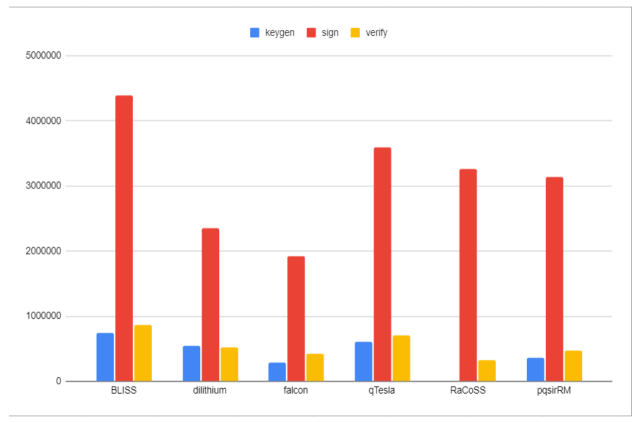
4 COMPARISON AMONG CODE- AND LATTICES-BASED CRYPTOSYSTEMS

1. Practical level of cost
2. Theoritical level of cost
3. Security attack resilience
4. Efficiency
5. Distinguishable feature
6. Potential Vulnerabilities

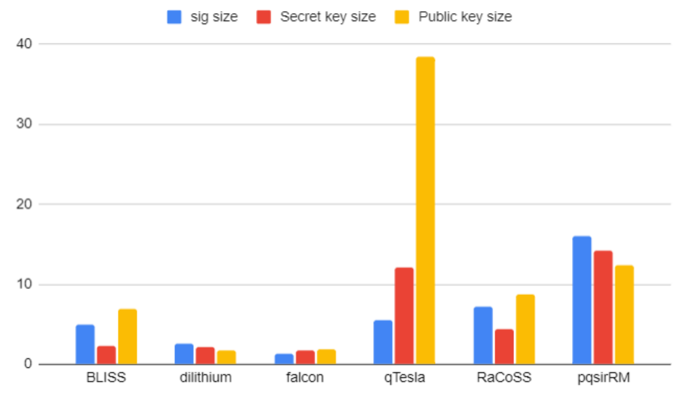
3.Results

Lattices-based		pqNTRUSign	BLISS	Falcon	Dilithium	qTesla
Underlying Hard Problem		CVP	R-LWE	SIS	LWE	R-LWE
Features	Sampler	• Uniform distribution • Use of rejection sampling	• Based on Bi modal gaussian distribution • Bernoulli-based rejection sampling	• Variant of GPV using fast fourier sampling • Non-constant time • Use of a recursive datastructure	• Uniform distribution • Constant-time	• Simplified gaussian sampler • Constant-time
	Construction principle	• NTRU lattices			• Fiat-Shamir with Aborts	
Attack resilience		• Proven secure,	• Broken by a cache-side channel attack	• Fix issues with constant-time sampler slowing down	• Fault attacks are potentially dangerous, an be solved by inducing randomness	

Performance



Security



Code-based	pqsigRM	RaCoSS-R
Underlying Problem	Variant of reed-muller code	Syndrome decoding problem
Features	• Variant of CFS	
Security resilliency	Secure under EUF-CMA	Broken

4.Conclusion

- Falcon and Dilithium are the most promising lattices-based cryptosystem
- pqsigRM is the most promising code-based cryptosystem
- Hash-and-sign cryptosytems fits for compactness need
- Fiat-Shamir with aborts are more secure as they are vulnerable from an underlying algebraic structure
- Lattices-based cryptosystems are generally more flexible and secure for standardization
- The choice of a cryptosystem should be more context-dependent

@
a.n.feldman@student.tudelft.nl