

Applying a cryptographic metric to Dilithium and Falcon

Authors Markus Rautell, Outi-Marja Latvala, Visa Vallivaara, Kimmo Halunen
(kimmo.halunen@oulu.fi)

Introduction

- Quantum computers are becoming a real threat to classical public key cryptography
- NIST has launched a process to standardize quantum-resistant public key encapsulation and digital signature algorithms
- Measuring the security of cryptographic systems is a difficult problem and there are many metrics that can be applied
- The purpose of a metric is to help one to choose between all different cryptosystems when buying or designing a new product or service
- It would be convenient to have a taxonomy of metrics that measures the overall sustainability

Challenges

- Security parameters of examined algorithms have changed along the way of NIST standardization process
- Algorithms are still under development and used taxonomy is designed to measure fully developed systems
- Algorithms aim at different security levels
- Many similarities due to the demands of NIST and lattice-based nature of examined algorithms

Results

Cat.	Subcategory	Metric	Falcon	Dilithium
AM	Degrees of freedom	Observe, choose, choose adaptively	choose adaptively	choose adaptively
		Security game compliance	Game, generic	Game, generic
Adversarial available information	Pre-crypto		public key	public key
		Post-crypto	2 ⁶⁴ signatures of chosen messages	2 ⁶⁴ signatures of chosen messages
		Secret key material	no material	no material
Adversarial goal	Goal	Semantic deduction, forgery	Semantic deduction, forgery	
Adversarial resources	Computation power, instantiated		quantum computer	quantum computer
			BQP	BQP
	Memory, instantiated		quantum computer	quantum computer
		Memory, non-instantiated	unlimited	unlimited
PF	Security assumptions	Mathematical complexity	computational/search	computational/search
		Abstraction assumptions	Type	ROM, QROM
		Tightness	tight reduction	non-tight reduction

Cat.	Subcategory	Metric	Falcon	Dilithium
VF	Vulnerabilities	Number	1	1
		Number of classified	1	1
	Side-channels	Existence	known side-channel attacks	known side-channel attacks
	Evaluator acceptance & reputation	Reviews	12	19
	Evaluator experience	Academic publications	1873	3763
		Experience in years	348	696
Verification time		Time since released for evaluation	Released 30.11.2017	Released 30.11.2017
		Size and efforts of evaluation community	Cryptography II, Authentication	Cryptography II, Authentication
Openness of target	Software/design	open source	open source	
Readiness level	Technology Readiness Level		TRL 4 - TRL 6	TRL 4 - TRL 6
		Integration Readiness Level	IRL 4 - IRL 6	IRL 4 - IRL 6
		System Readiness Level	SRL 2 - SRL 3	SRL 2 - SRL 3
	PETS maturity model	Prototype ^(+ /++)	Prototype ^(+ /++)	
Key length	Bits for criteria compliance	1 998 - 3 840 (B)	2 032 - 3 920 (B)	
Memory and transmission costs	Run-time memory		4 300, 2 708 (kB)	5 524, 3 048 (kB)
		Storage capacity	3 561 - 6 913 (B)	5 764 - 11 107 (B)
		Communication bandwidth	1 536 - 3 073 (B)	3 732 - 7 187 (B)
Implementation complexity	Size of software		356 532 - 1 112 295 (B)	165 478 - 281 698 (B)
		Dedicated hardware requirements	no special hardware needed	no special hardware needed

Conclusion

- Used metric taxonomy can recognize differences between examined algorithms
- Used metric taxonomy misses valuable information and needs improvement
- Lower subcategories should be more flexible, but at the same time allow deeper analysis
- Used metrics indicate that Falcon is more compact and safe from theoretical security perspective, but less studied than Dilithium