NTRU Prime: Security and Performance Analysis

Chitchanok Chuengsatiansup & Christine van Vredendaal

Technische Universiteit Eindhoven

February 26, 2016

Joint work with Daniel J. Bernstein & Tanja Lange

What is NTRU Prime?

- Public key is small/small $\in (\mathbb{Z}/q)[x]/\text{poly}$

	NTRU	**NTRU Prime**
poly	$x^N - 1$	$x^p - x - 1$
Modulus q	2^d	prime
# of factors of poly mod q	> 1	1
# of proper subfields	> 1	1
Every m encryptable	✗	✓
No decryption failures	✗	✓

What is NTRU Prime?

- Public key is small/small $\in (\mathbb{Z}/q)[x]/\text{poly}$

	NTRU	**NTRU Prime**
poly	$x^N - 1$	$x^p - x - 1$
Modulus q	2^d	prime
# of factors of poly mod q	> 1	1
# of proper subfields	> 1	1
Every m encryptable	✗	✓
No decryption failures	✗	✓

- We investigated security against the strongest known attacks; hybrid attack of BKZ and MitM, and lattice sieving

p	**q**	**t**	**Key size**	**Security**
881	7673	159	11.4 Kb	257

What is NTRU Prime?

- Public key is small/small $\in (\mathbb{Z}/q)[x]/\text{poly}$

	NTRU	NTRU Prime
poly	$x^N - 1$	$x^p - x - 1$
Modulus q	2^d	prime
# of factors of poly mod q	> 1	1
# of proper subfields	> 1	1
Every m encryptable	✗	✓
No decryption failures	✗	✓

- We investigated security against the strongest known attacks; hybrid attack of BKZ and MitM, and lattice sieving

p	q	t	Key size	Security
881	7673	159	11.4 Kb	257

But, is it still fast?

Polynomial Multiplication

- Main bottleneck is polynomial multiplication
- Multiplication algorithms considered:
  - Toom (3-7)
  - refined Karatsuba
  - arbitrary degree variant of Karatsuba (3-7)
- Best operation count found so far for 896×896:
  - 5-level refined Karatsuba up to 128×128
  - Toom7: evaluated at $0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, 6, \infty$
- Performance
  - vectorized Haswell implementation in progress
  - ≥ 0.125 cycles per floating-point operation

	mul	con mult	add	shift	total
op.	50544	16083	121248	7407	195282
cycles$\geq$	6318	2011	15156	926	24411