NTRU Prime: Reducing Attack Surface at Low Cost

Daniel J. Bernstein, Chitchanok Chuengsatiansup,
Tanja Lange, and Christine van Vredendaal

Technische Universiteit Eindhoven

April 13th, 2018

Idea:

a field-based system that reduces (potential) attack surface, while still being fast and compact

Motivation

- **Tool 1:** Decryption failures in original NTRU

Motivation

- **Tool 1:** Decryption failures in original NTRU
- **Tool 2:** Evaluation-at-1 attack in original NTRU

Motivation

- **Tool 1:** Decryption failures in original NTRU
- **Tool 2:** Evaluation-at-1 attack in original NTRU
- **Tool 3:** mappings to quotient rings of $R_q = (\mathbf{Z}/q)[x]/(x^p - 1)$. Can possibly get more information on m from homomorphism $\psi : R_q \to T$, for some ring T.

Motivation

- **Tool 1:** Decryption failures in original NTRU
- **Tool 2:** Evaluation-at-1 attack in original NTRU
- **Tool 3:** mappings to quotient rings of $R_q = (\mathbf{Z}/q)[x]/(x^p - 1)$. Can possibly get more information on m from homomorphism $\psi : R_q \to T$, for some ring T.
- Unclear whether these can be exploited to get information on m. [Silverman-Smart-Vercauteren '04, Eisenträger-Hallgren-Lauter '14, Elias-Lauter-Ozman-Stange '15, Chen-Lauter-Stange '16, Castryck-Iliashenko-Vercauteren '16]

Motivation

- **Tool 1:** Decryption failures in original NTRU
- **Tool 2:** Evaluation-at-1 attack in original NTRU
- **Tool 3:** mappings to quotient rings of $R_q = (\mathbf{Z}/q)[x]/(x^p - 1)$. Can possibly get more information on m from homomorphism $\psi : R_q \to T$, for some ring T.
- Unclear whether these can be exploited to get information on m. [Silverman-Smart-Vercauteren '04, Eisenträger-Hallgren-Lauter '14, Elias-Lauter-Ozman-Stange '15, Chen-Lauter-Stange '16, Castryck-Iliashenko-Vercauteren '16]
- **Tool 4:** large proper subfields [Bernstein '14, Albrecht-Bai-Ducas '16, Bauch-Bernstein-Lange-de Valence-van Vredendaal '17]

Motivation

- **Tool 1:** Decryption failures in original NTRU
- **Tool 2:** Evaluation-at-1 attack in original NTRU
- **Tool 3:** mappings to quotient rings of $R_q = (\mathbf{Z}/q)[x]/(x^p - 1)$. Can possibly get more information on m from homomorphism $\psi : R_q \to T$, for some ring T.
- Unclear whether these can be exploited to get information on m. [Silverman-Smart-Vercauteren '04, Eisenträger-Hallgren-Lauter '14, Elias-Lauter-Ozman-Stange '15, Chen-Lauter-Stange '16, Castryck-Iliashenko-Vercauteren '16]
- **Tool 4:** large proper subfields [Bernstein '14, Albrecht-Bai-Ducas '16, Bauch-Bernstein-Lange-de Valence-van Vredendaal '17]
- **Tool 5:** many easily computable automorphisms [Campbell-Groves-Shepherd '14, Cramer-Ducas-Peikert-Regev '15]

Motivation

- **Tool 1:** Decryption failures in original NTRU
- **Tool 2:** Evaluation-at-1 attack in original NTRU
- **Tool 3:** mappings to quotient rings of $R_q = (\mathbf{Z}/q)[x]/(x^p - 1)$. Can possibly get more information on m from homomorphism $\psi : R_q \to T$, for some ring T.
- Unclear whether these can be exploited to get information on m. [Silverman-Smart-Vercauteren '04, Eisenträger-Hallgren-Lauter '14, Elias-Lauter-Ozman-Stange '15, Chen-Lauter-Stange '16, Castryck-Iliashenko-Vercauteren '16]
- **Tool 4:** large proper subfields [Bernstein '14, Albrecht-Bai-Ducas '16, Bauch-Bernstein-Lange-de Valence-van Vredendaal '17]
- **Tool 5:** many easily computable automorphisms [Campbell-Groves-Shepherd '14, Cramer-Ducas-Peikert-Regev '15]

Whether paranoia, or valid concern; what can we do about it?

NTRU Prime

- **NTRU Prime**: Switch to Prime degree, large Galois group, inert modulus cryptography.

NTRU Prime

- **NTRU Prime**: Switch to Prime degree, large Galois group, inert modulus cryptography.
- Choose prime p, set $F = x^p - x - 1$ (tool 4).
- Choose prime q such that F is irreducible mod q (tools 2, 3)
- NTRU Prime works over the field

$$(\mathbb{Z}/q)[x]/(x^p - x - 1),$$

- with Galois group S_p of size $p!$ (tool 5).

Streamlined NTRU Prime

System parameters (p, q, t), p, q prime, $q \geq 32t + 1$ (tool 1).

Streamlined NTRU Prime

System parameters (p, q, t), p, q prime, $q \geq 32t + 1$ (tool 1).

- Pick g small in $\mathcal{R}$

$$g = g_0 + \cdots + g_{p-1}x^{p-1} \text{ with } g_i \in \{-1, 0, 1\}$$

  No weight restriction on g, only size restriction on coefficients; g required to be invertible in $\mathcal{R}/3$.

- Pick t-small $f \in \mathcal{R}$

$$f = f_0 + \cdots + f_{p-1}x^{p-1} \text{ with } f_i \in \{-1, 0, 1\} \text{ and } \sum |f_i| = 2t$$

  Since $\mathcal{R}/q$ is a field, f is invertible.

- Compute public key $h = g/(3f)$ in $\mathcal{R}/q$.
- Private key is f and $1/g \in \mathcal{R}/3$.

Streamlined NTRU Prime

System parameters (p, q, t), p, q prime, $q \geq 32t + 1$ (tool 1).

- Pick g small in $\mathcal{R}$

$$g = g_0 + \cdots + g_{p-1}x^{p-1} \text{ with } g_i \in \{-1, 0, 1\}$$

  No weight restriction on g, only size restriction on coefficients; g required to be invertible in $\mathcal{R}/3$.

- Pick t-small $f \in \mathcal{R}$

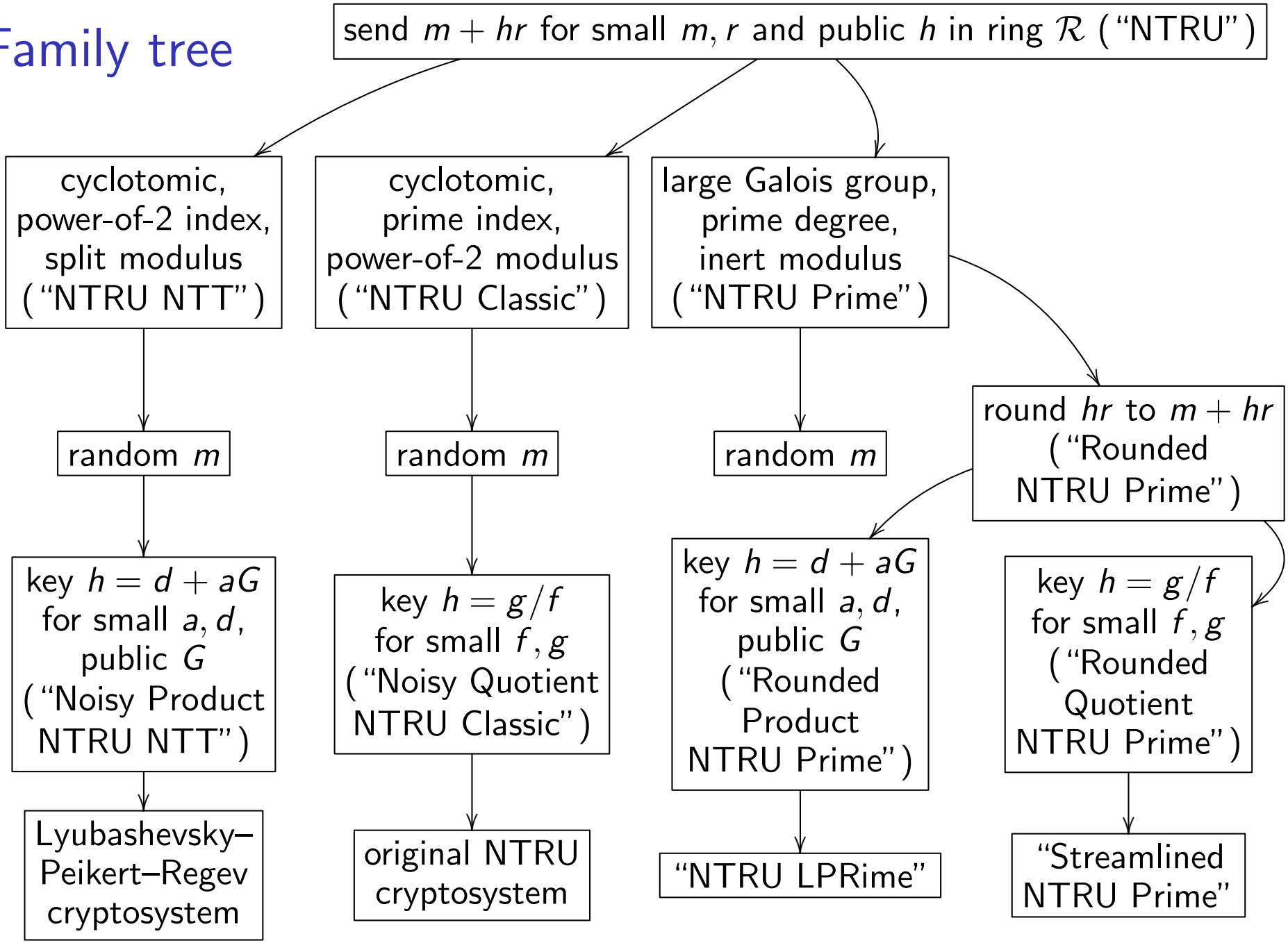
$$f = f_0 + \cdots + f_{p-1}x^{p-1} \text{ with } f_i \in \{-1, 0, 1\} \text{ and } \sum |f_i| = 2t$$

  Since $\mathcal{R}/q$ is a field, f is invertible.

- Compute public key $h = g/(3f)$ in $\mathcal{R}/q$.
- Private key is f and $1/g \in \mathcal{R}/3$.

Streamlined NTRU Prime is a Key Encapsulation Mechanism (KEM), combine with Data Encapsulation Mechanism (DEM) to send messages.

Family tree


send $m + hr$ for small m, r and public h in ring $\mathcal{R}$ ("NTRU")
cyclotomic, power-of-2 index, split modulus ("NTRU NTT")
cyclotomic, prime index, power-of-2 modulus ("NTRU Classic")
large Galois group, prime degree, inert modulus ("NTRU Prime")
round hr to $m + hr$ ("Rounded NTRU Prime")
random m
random m
random m
key $h = d + aG$ for small a, d, public G ("Noisy Product NTRU NTT")
key $h = g/f$ for small f, g ("Noisy Quotient NTRU Classic")
key $h = d + aG$ for small a, d, public G ("Rounded Product NTRU Prime")
key $h = g/f$ for small f, g ("Rounded Quotient NTRU Prime")
Lyubashevsky–Peikert–Regev cryptosystem
original NTRU cryptosystem
"NTRU LPRime"
"Streamlined NTRU Prime"

Streamlined NTRU Prime Security I

- What we know so far:

	original NTRU	**New Hope**	**Streamlined NTRU Prime**
Polynomial P	$x^p - 1$	$x^p + 1$	$x^p - x - 1$
Degree p	prime	power of 2	prime
Modulus q	2^d	prime	prime
# factors of P in $\mathcal{R}/q$	> 1	p	1
# proper subfields	> 1	many	1
Every m encryptable	✗	✓	✓
No decryption failures	✗	✗	✓

Streamlined NTRU Prime Security I

- What we know so far:

	original NTRU	**New Hope**	**Streamlined NTRU Prime**
Polynomial P	$x^p - 1$	$x^p + 1$	$x^p - x - 1$
Degree p	prime	power of 2	prime
Modulus q	2^d	prime	prime
# factors of P in $\mathcal{R}/q$	> 1	p	1
# proper subfields	> 1	many	1
Every m encryptable	✗	✓	✓
No decryption failures	✗	✗	✓

- Because of the last 2 ✓'s the analysis is simpler than that of original NTRU.

Streamlined NTRU Prime Security II

- We investigated security against the strongest known attacks; meet-in-the-middle (mitm), hybrid attack of BKZ and mitm, and lattice sieving

Streamlined NTRU Prime Security II

- We investigated security against the strongest known attacks; meet-in-the-middle (mitm), hybrid attack of BKZ and mitm, and lattice sieving
- Streamlined NTRU Prime 4591^{761} and NTRU LPRime 4591^{761} both use $p = 761$ and $q = 4591$.
- These parameters lead to respectively 248 bits and 225 bits of pre-quantum security. Quantum computers will speed up by less than squareroot.

Performance

- The resulting sizes and Haswell speeds show that reducing the attack surface has very low cost:

Metric	**Streamlined NTRU Prime** 4591^{761}	**NTRU LPRime** 4591^{761}
Public-key size	1218 bytes	1047 bytes
Ciphertext size	1047 bytes	1175 bytes
Encapsulation time	59456 cycles	94508 cycles
Decapsulation time	97684 cycles	128316 cycles

Performance

- The resulting sizes and Haswell speeds show that reducing the attack surface has very low cost:

Metric	**Streamlined NTRU Prime** 4591^{761}	**NTRU LPRime** 4591^{761}
Public-key size	1218 bytes	1047 bytes
Ciphertext size	1047 bytes	1175 bytes
Encapsulation time	59456 cycles	94508 cycles
Decapsulation time	97684 cycles	128316 cycles

- This beats cycle counts of New Hope, Kyber and Curve25519
- It does not outperform NTRU KEM (HRSS '17) (48646 cycles enc, 67338 cycles dec)
- NTRU KEM ciphertexts are longer (1281 bytes vs. 1047 bytes)

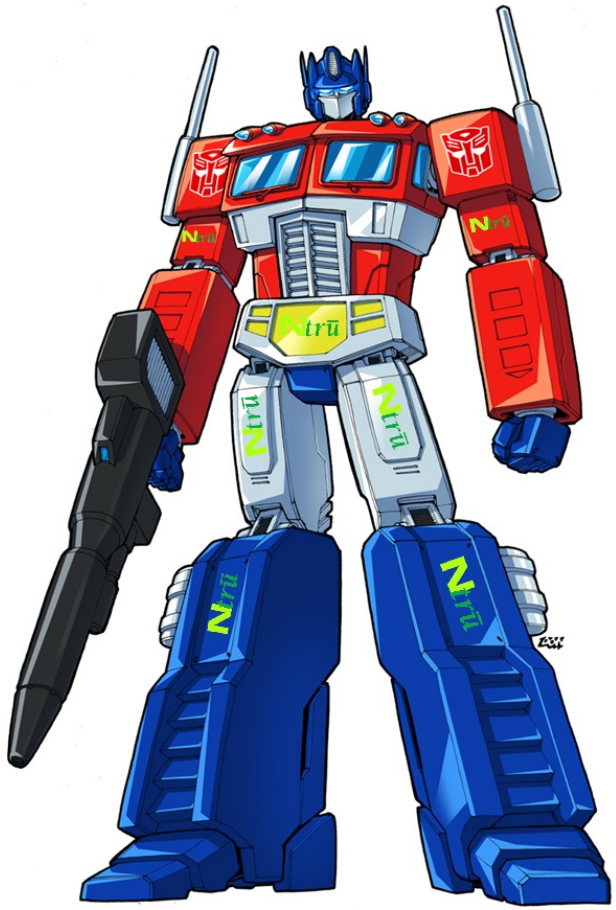


Figure: (Optimus) NTRU Prime.

Thank you!