A Thorough Treatment of Highly-Efficient NTRU Instantiations

Julien Duman[1], K. Hövelmanns[2], E. Kiltz[1], V. Lyubashevsky[3], G. Seiler[3] and D. Unruh[4]

Ruhr-University Bochum[1], TU Eindhoven[2], IBM Research Europe, Zurich[3], University of Tartu[4]

8. May 2023

NTRU

first practical lattice-based encryption scheme [HPS98]

$\mathcal{R} = \mathbb{Z}_q[X]/(f(X))$, $pk = \mathbf{g}/\mathbf{f}$, $sk = \mathbf{f}$, $c = \mathbf{r} \cdot pk + \vec{m}$, narrow distribution η

Oneway under $\mathcal{R}$-LWE$_\eta$ and NTRU$_\eta$ assumption

NTRU

first practical lattice-based encryption scheme [HPS98]

$\mathcal{R} = \mathbb{Z}_q[X]/(f(X))$, $pk = \mathbf{g}/\mathbf{f}$, $sk = \mathbf{f}$, $c = \mathbf{r} \cdot pk + \vec{m}$, narrow distribution η

Oneway under $\mathcal{R}$-LWE$_\eta$ and NTRU$_\eta$ assumption

NTRU$_\eta$ assumption: $pk \approx_c \mathbf{h} \leftarrow_\$ \mathcal{R}$

NTRU

first practical lattice-based encryption scheme [HPS98]

$\mathcal{R} = \mathbb{Z}_q[X]/(f(X))$, $pk = \mathbf{g}/\mathbf{f}$, $sk = \mathbf{f}$, $c = \mathbf{r} \cdot pk + \vec{m}$, narrow distribution η

Oneway under $\mathcal{R}$-LWE$_\eta$ and NTRU$_\eta$ assumption

NTRU$_\eta$ assumption: $pk \approx_c \mathbf{h} \leftarrow_\$ \mathcal{R}$

$\mathcal{R}$-LWE$_\eta$ assumption: difficult to compute $\vec{m}$ given $c = \mathbf{r} \cdot \mathbf{h} + \vec{m}$, where $\mathbf{h} \leftarrow_\$ \mathcal{R}$ and $\vec{m}, \mathbf{r} \leftarrow_\$ \eta$.

3 of 17 first round Lattice NIST PQC candidates used NTRU Variant

Decryption Errors and Compactness

$$\mathrm{Dec}(\mathbf{f}, \mathrm{Enc}(\mathbf{h}, \vec{m})) = (\mathbf{fc} \bmod {}^{\pm}q) \bmod {}^{\pm}3$$

$$= (\underbrace{3(\mathbf{gr} + \mathbf{f}'\vec{m})}_{\text{correctness term}} + \vec{m} \bmod {}^{\pm}q) \bmod {}^{\pm}3$$

Decryption Errors and Compactness

$$\text{Dec}(\mathbf{f}, \text{Enc}(\mathbf{h}, \vec{m})) = (\mathbf{fc} \bmod {}^{\pm}q) \bmod {}^{\pm}3$$

$$= (\underbrace{3(\mathbf{gr} + \mathbf{f}'\vec{m})}_{\text{correctness term}} + \vec{m} \bmod {}^{\pm}q) \bmod {}^{\pm}3$$

for correctness need all coefficients of $3(\mathbf{gr} + \mathbf{f}'\vec{m}) < q/2$

but can have larger coefficients for adversarially chosen $\vec{m}$

Decryption Errors and Compactness

$$\text{Dec}(\mathbf{f}, \text{Enc}(\mathbf{h}, \vec{m})) = (\mathbf{fc} \bmod {}^{\pm}q) \bmod {}^{\pm}3$$

$$= (\underbrace{3(\mathbf{gr} + \mathbf{f}'\vec{m})}_{\text{correctness term}} + \vec{m} \bmod {}^{\pm}q) \bmod {}^{\pm}3$$

for correctness need all coefficients of $3(\mathbf{gr} + \mathbf{f}'\vec{m}) < q/2$

but can have larger coefficients for adversarially chosen $\vec{m}$

$\implies$ only average-case correctness

$\implies$ can't directly obtain CCA-secure KEM

in fact adversary forcing decryption errors can leak the secret-key [HNP+03]

Decryption Errors and Compactness

$\text{Dec}(\mathbf{f}, \text{Enc}(\mathbf{h}, \vec{m})) = (\mathbf{fc} \bmod {}^{\pm}q) \bmod {}^{\pm}3$

$= (\underbrace{3(\mathbf{gr} + \mathbf{f}'\vec{m})}_{\text{correctness term}} + \vec{m} \bmod {}^{\pm}q) \bmod {}^{\pm}3$

for correctness need all coefficients of $3(\mathbf{gr} + \mathbf{f}'\vec{m}) < q/2$

but can have larger coefficients for adversarially chosen $\vec{m}$

$\implies$ only average-case correctness

$\implies$ can't directly obtain CCA-secure KEM

in fact adversary forcing decryption errors can leak the secret-key [HNP+03]

possible solution: increase q to obtain perfect correctness $\overset{\text{[SXY18]}}{\implies}$ CCA-KEM, but larger q decreases security of NTRU assumption and compactness

Decryption Errors and Compactness

$\mathsf{Dec}(\mathbf{f}, \mathsf{Enc}(\mathbf{h}, \vec{m})) = (\mathbf{fc} \bmod {}^{\pm}q) \bmod {}^{\pm}3$

$= (\underbrace{3(\mathbf{gr} + \mathbf{f}'\vec{m})}_{\text{correctness term}} + \vec{m} \bmod {}^{\pm}q) \bmod {}^{\pm}3$

for correctness need all coefficients of $3(\mathbf{gr} + \mathbf{f}'\vec{m}) < q/2$

but can have larger coefficients for adversarially chosen $\vec{m}$

$\implies$ only average-case correctness

$\implies$ can't directly obtain CCA-secure KEM

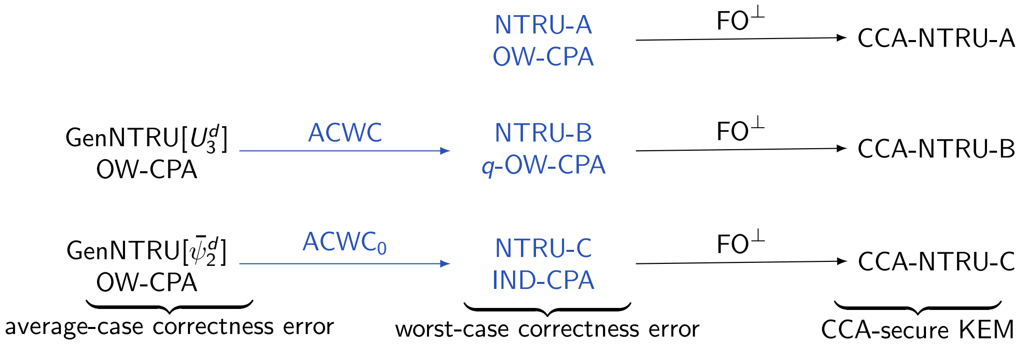
in fact adversary forcing decryption errors can leak the secret-key [HNP$^+$03]

possible solution: increase q to obtain perfect correctness $\overset{\text{[SXY18]}}{\implies}$ CCA-KEM, but larger q decreases security of NTRU assumption and compactness

our solution: apply error-reducing transform $\overset{\text{FO}}{\implies}$ CCA-KEM

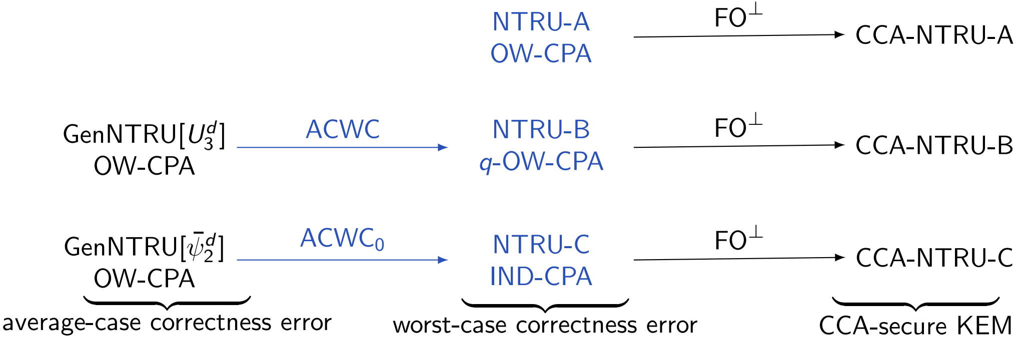
Advantage: smaller $q \implies$ better security for NTRU assumption + more compact

This work



3 NTRU variants

This work

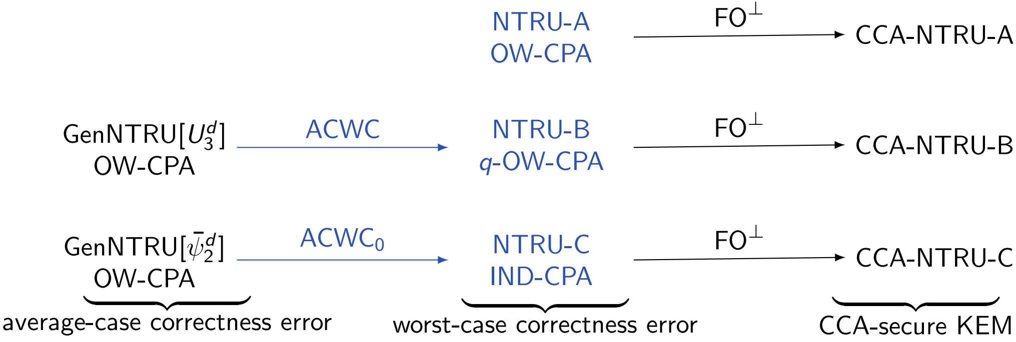


3 NTRU variants

NTRU-A with worst-case correctness

2 error-reducing transformations, analyzed in (Q)ROM

This work



- 3 NTRU variants
- NTRU-A with worst-case correctness
- 2 error-reducing transformations, analyzed in (Q)ROM
- analysis of the worst-case correctness
- obtain CCA-KEMs through FO

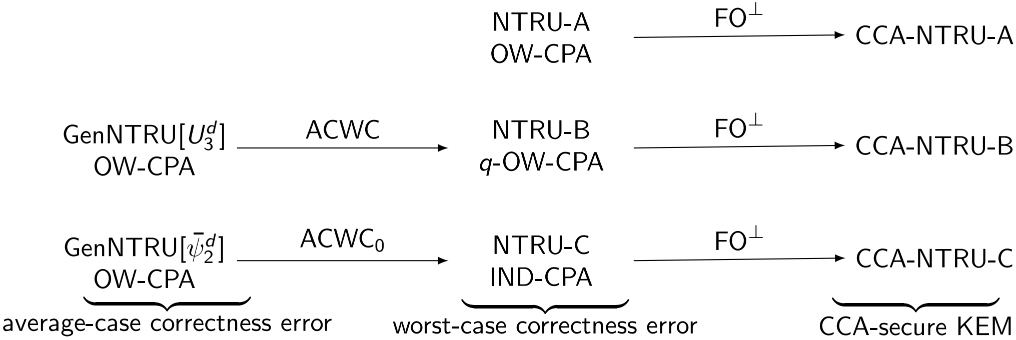
Practical application

Instantiated with NTT-friendly Rings $\mathbb{Z}_q[X]/(X^d - X^{d/2} + 1)$ [LS19], our scheme is

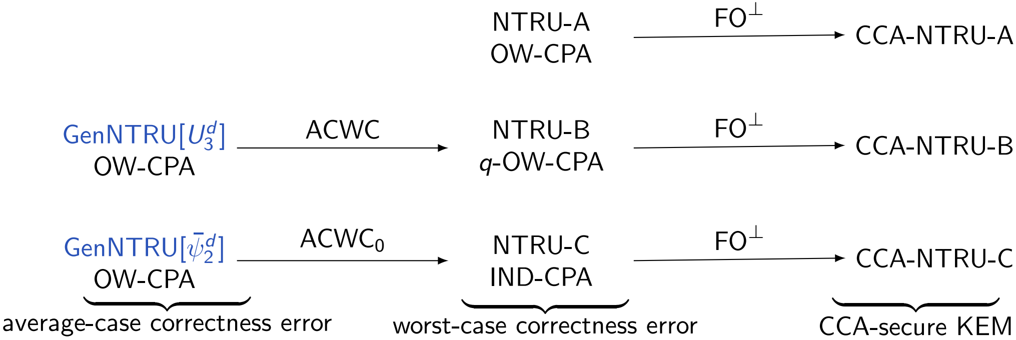
- 15% more compact
- 15x improvement in ephemeral round-trip time
- 35x faster key-generation
- 6x faster key-encapsulation
- 9x faster key-decapsulation

than NIST-Finalist NTRU-HRSS-701 [HRSS17]

Overview


NTRU-A
OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-A
GenNTRU$[U_3^d]$
OW-CPA
ACWC
NTRU-B
q-OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-B
GenNTRU$[\bar{\psi}_2^d]$
OW-CPA
ACWC_0
NTRU-C
IND-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-C
average-case correctness error
worst-case correctness error
CCA-secure KEM

Overview


NTRU-A
OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-A
GenNTRU$[U_3^d]$
OW-CPA
ACWC
NTRU-B
q-OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-B
GenNTRU$[\bar{\psi}_2^d]$
OW-CPA
ACWC_0
NTRU-C
IND-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-C
average-case correctness error
worst-case correctness error
CCA-secure KEM

GenNTRU[η]

$\underline{\text{KeyGen}()}$

$\mathbf{f}', \mathbf{g} \leftarrow \eta$

$\mathbf{f} := 3\mathbf{f}' + 1$

if $\mathbf{f}$ or $\mathbf{g} \notin \mathcal{R}^\times$, restart

return $(pk, sk) = (3\mathbf{g}\mathbf{f}^{-1}, \mathbf{f})$

$\underline{\text{Enc}(\mathbf{h} \in \mathcal{R}, \vec{m} \in \{-1, 0, 1\}^d)}$

$\mathbf{r} \leftarrow \eta$

return $\mathbf{c} := \mathbf{h}\mathbf{r} + \vec{m}$

$\underline{\text{Dec}(\mathbf{f} \in \mathcal{R}, \mathbf{c} \in \mathcal{R})}$

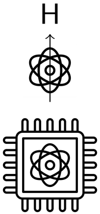
return $\vec{m} := (\mathbf{c}\mathbf{f} \bmod^{\pm} q) \bmod^{\pm} 3$

$h \bmod^{\pm} q$ to mean the integer from the set $\left\{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\right\}$ which is congruent to h modulo q

Randomness Recoverable: $\mathbf{r} = \mathbf{h}^{-1}(\mathbf{c} - \vec{m})$

Quantum Random Oracle Model [BDF+11]

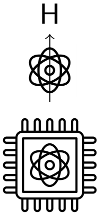
$$\mathsf{H}\left(\frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle\right)$$



Quantum computers can execute hash functions in quantum superposition

Quantum Random Oracle Model [BDF+11]

$$\mathsf{H}\left(\frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle\right)$$

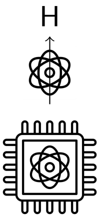


Quantum computers can execute hash functions in quantum superposition

therefore need to extend this in the ROM by allowing quantum access

Quantum Random Oracle Model [BDF+11]

$$\mathsf{H}\left(\frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle\right)$$

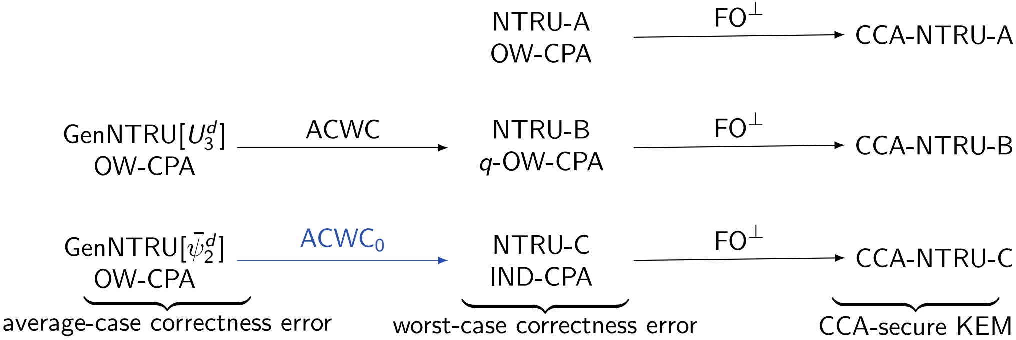


Quantum computers can execute hash functions in quantum superposition

therefore need to extend this in the ROM by allowing quantum access

common lemma: Oneway-to-hiding [AHU19]

Overview


NTRU-A
OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-A
GenNTRU[U_3^d]
OW-CPA
ACWC
NTRU-B
q-OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-B
GenNTRU[$\bar{\psi}_2^d$]
OW-CPA
ACWC$_0$
NTRU-C
IND-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-C
average-case correctness error
worst-case correctness error
CCA-secure KEM

$\mathsf{ACWC}_0[\mathsf{PKE}]$

$\underline{\mathsf{Enc}'(pk, m \in \{0,1\}^\lambda)}$	$\underline{\mathsf{Dec}'(sk, (c, u))}$
pick random r	$r := \mathsf{Dec}(sk, c)$
return $(\mathsf{Enc}(pk, r), \mathsf{F}(r) \oplus m)$	**return** $\mathsf{F}(r) \oplus u$

Intuition: Correctness independent of $m \implies$ worst-case correct

$\mathsf{ACWC}_0[\mathsf{PKE}]$

$\underline{\mathsf{Enc}'(pk, m \in \{0,1\}^\lambda)}$

pick random r

return $(\mathsf{Enc}(pk, r), \mathsf{F}(r) \oplus m)$

$\underline{\mathsf{Dec}'(sk, (c, u))}$

$r := \mathsf{Dec}(sk, c)$

return $\mathsf{F}(r) \oplus u$

Intuition: Correctness independent of $m \implies$ worst-case correct

Thm: If PKE is δ average-case correct, then $\mathsf{ACWC}_0[\mathsf{PKE}]$ is δ worst-case correct.

$\mathsf{ACWC}_0[\mathsf{PKE}]$

$\underline{\mathsf{Enc}'(pk, m \in \{0,1\}^\lambda)}$

pick random r

return $(\mathsf{Enc}(pk, r), \mathsf{F}(r) \oplus m)$

$\underline{\mathsf{Dec}'(sk, (c, u))}$

$r := \mathsf{Dec}(sk, c)$

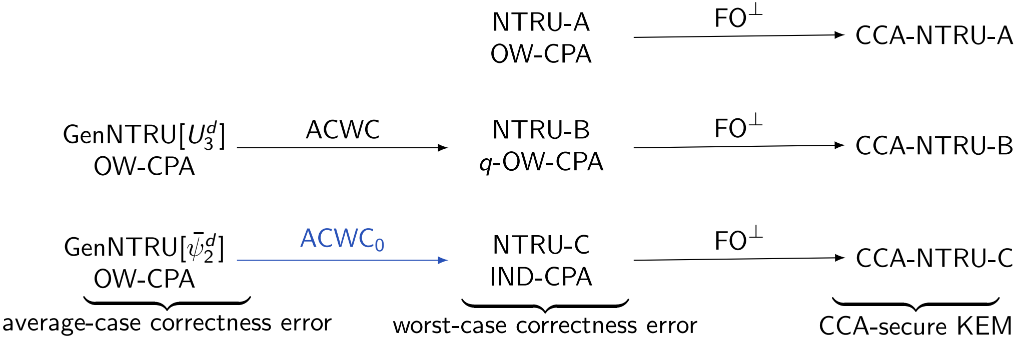
return $\mathsf{F}(r) \oplus u$

Intuition: Correctness independent of $m \implies$ worst-case correct

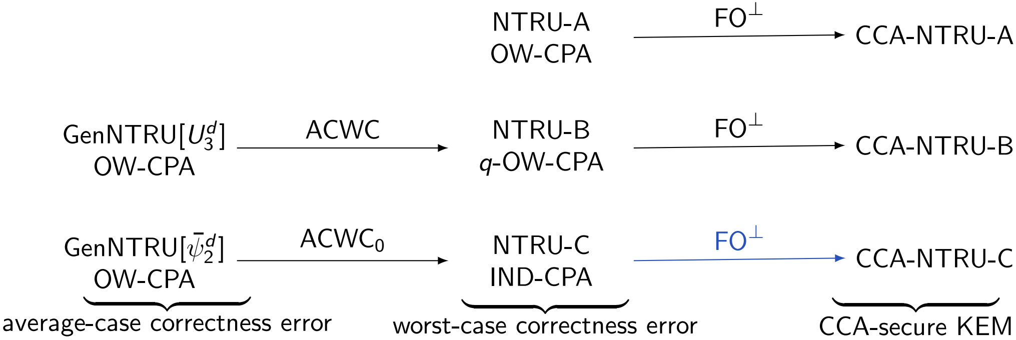
Thm: If PKE is δ average-case correct, then $\mathsf{ACWC}_0[\mathsf{PKE}]$ is δ worst-case correct.

Thm: If PKE is oneway, then $\mathsf{ACWC}_0[\mathsf{PKE}]$ is IND-CPA secure in the (Q)ROM.

Overview


NTRU-A
OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-A
GenNTRU[U_3^d]
OW-CPA
ACWC
NTRU-B
q-OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-B
GenNTRU[$\bar{\psi}_2^d$]
OW-CPA
ACWC_0
NTRU-C
IND-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-C
average-case correctness error
worst-case correctness error
CCA-secure KEM

Overview


NTRU-A
OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-A
GenNTRU$[U_3^d]$
OW-CPA
ACWC
NTRU-B
q-OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-B
GenNTRU$[\bar{\psi}_2^d]$
OW-CPA
ACWC_0
NTRU-C
IND-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-C
average-case correctness error
worst-case correctness error
CCA-secure KEM

Fujisaki-Okamoto Transform with Explicit Rejection

$$\mathsf{Encaps}_{pk}(;r) = (\underbrace{\mathsf{Enc}_{pk}(r;\mathsf{G}(r))}_{\text{ciphertext}}, \underbrace{\mathsf{H}(r)}_{\text{key}})$$

$$\mathsf{Decaps}_{sk}(c) = \begin{cases} \mathsf{H}(r') & \text{if } \mathsf{Enc}_{pk}(r';\mathsf{G}(r')) \stackrel{?}{=} c \\ & \qquad \text{where } r' := \mathsf{Dec}_{sk}(c) \\ \perp & \text{else} \end{cases}$$

Fujisaki-Okamoto Transform with Explicit Rejection

$$\mathsf{Encaps}_{pk}(;r) = (\underbrace{\mathsf{Enc}_{pk}(r;\mathsf{G}(r))}_{\text{ciphertext}}, \underbrace{\mathsf{H}(r)}_{\text{key}})$$

$$\mathsf{Decaps}_{sk}(c) = \begin{cases} \mathsf{H}(r') & \text{if } \mathsf{Enc}_{pk}(r';\mathsf{G}(r')) \stackrel{?}{=} c \\ & \qquad \text{where } r' := \mathsf{Dec}_{sk}(c) \\ \perp & \text{else} \end{cases}$$

transform *worst-case correct* OW/IND-CPA PKE into IND-CCA-secure KEM

Re-Encryption Check gives the KEM its CCA-security

Fujisaki-Okamoto Transform with Explicit Rejection

$$\mathsf{Encaps}_{pk}(;r) = (\underbrace{\mathsf{Enc}_{pk}(r;\mathsf{G}(r))}_{\text{ciphertext}}, \underbrace{\mathsf{H}(r)}_{\text{key}})$$

$$\mathsf{Decaps}_{sk}(c) = \begin{cases} \mathsf{H}(r') & \text{if } \mathsf{Enc}_{pk}(r';\mathsf{G}(r')) \stackrel{?}{=} c \\ & \qquad \text{where } r' := \mathsf{Dec}_{sk}(c) \\ \bot & \text{else} \end{cases}$$

transform *worst-case correct* OW/IND-CPA PKE into IND-CCA-secure KEM

Re-Encryption Check gives the KEM its CCA-security

Fujisaki-Okamoto Transform with Explicit Rejection

$$\mathsf{Encaps}_{pk}(;r) = (\underbrace{\mathsf{Enc}_{pk}(r;\mathsf{G}(r))}_{\text{ciphertext}}, \underbrace{\mathsf{H}(r)}_{\text{key}})$$

$$\mathsf{Decaps}_{sk}(c) = \begin{cases} \mathsf{H}(r') & \text{if } \mathsf{Enc}_{pk}(r';\mathsf{G}(r')) \stackrel{?}{=} c \\ & \qquad \text{where } r' := \mathsf{Dec}_{sk}(c) \\ \bot & \text{else} \end{cases}$$

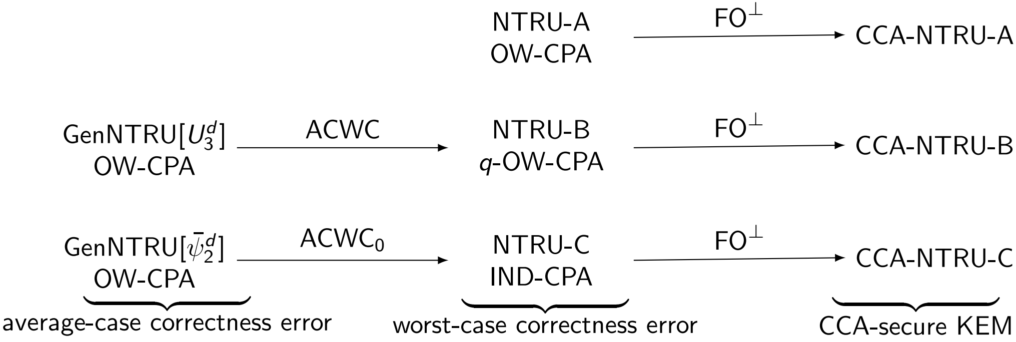
transform *worst-case correct* OW/IND-CPA PKE into IND-CCA-secure KEM

Re-Encryption Check gives the KEM its CCA-security

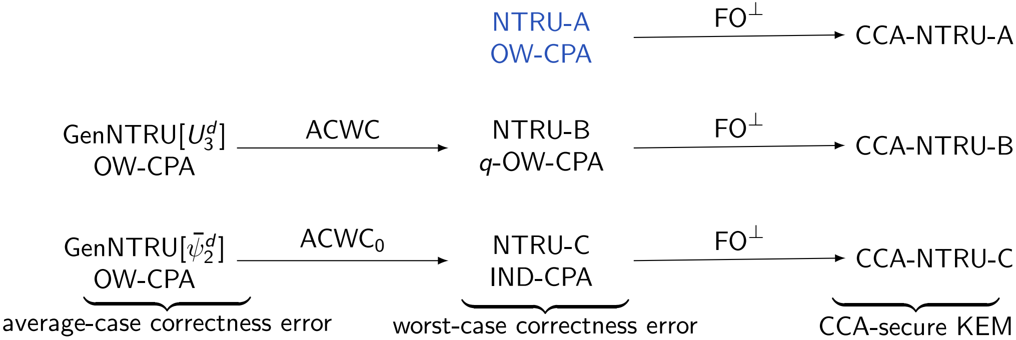
Explicit Rejection has been proven secure in the QROM [DFMS21]

more efficient decapsulation than implicit rejection

Overview


NTRU-A
OW-CPA
FO$^{\perp}$
CCA-NTRU-A
GenNTRU[U_3^d]
OW-CPA
ACWC
NTRU-B
q-OW-CPA
FO$^{\perp}$
CCA-NTRU-B
GenNTRU[$\bar{\psi}_2^d$]
OW-CPA
ACWC$_0$
NTRU-C
IND-CPA
FO$^{\perp}$
CCA-NTRU-C
average-case correctness error
worst-case correctness error
CCA-secure KEM

Overview


NTRU-A
OW-CPA
FO$^{\perp}$
CCA-NTRU-A
GenNTRU[U_3^d]
OW-CPA
ACWC
NTRU-B
q-OW-CPA
FO$^{\perp}$
CCA-NTRU-B
GenNTRU[$\bar{\psi}_2^d$]
OW-CPA
ACWC$_0$
NTRU-C
IND-CPA
FO$^{\perp}$
CCA-NTRU-C
average-case correctness error
worst-case correctness error
CCA-secure KEM

Distribution used in NTRU-A

define distribution ψ_2^d over $\mathbb{Z}^d$ as $\vec{b_1} + \vec{b_2} - \vec{b_3} - \vec{b_4}$, for $\vec{b_i} \leftarrow_\$ \{0,1\}^d$

alternative generation of ψ_2^d

$$\vec{b} = (\vec{b_1} \underbrace{-2\vec{b_2} \odot \vec{b_3}}_{0 \mod 2}) \odot (1 \underbrace{-2\vec{b_4}}_{0 \mod 2}),$$

Distribution used in NTRU-A

define distribution ψ_2^d over $\mathbb{Z}^d$ as $\vec{b_1} + \vec{b_2} - \vec{b_3} - \vec{b_4}$, for $\vec{b_i} \leftarrow_\$ \{0,1\}^d$

alternative generation of ψ_2^d

$$\vec{b} = (\vec{b_1} \underbrace{-2\vec{b_2} \odot \vec{b_3}}_{0 \mod 2}) \odot (1 \underbrace{-2\vec{b_4}}_{0 \mod 2}),$$

$\implies \vec{b} \bmod 2 = \vec{b_1}$

Distribution used in NTRU-A

define distribution ψ_2^d over $\mathbb{Z}^d$ as $\vec{b_1} + \vec{b_2} - \vec{b_3} - \vec{b_4}$, for $\vec{b_i} \leftarrow_\$ \{0,1\}^d$

alternative generation of ψ_2^d

$$\vec{b} = (\vec{b_1} \underbrace{-2\vec{b_2} \odot \vec{b_3}}_{0 \mod 2}) \odot (1 \underbrace{-2\vec{b_4}}_{0 \mod 2}),$$

$\implies \vec{b} \bmod 2 = \vec{b_1}$

Idea of NTRU-A: use message m as $\vec{b_1} = \vec{b} \mod 2$, and sample $\vec{b_2}, \vec{b_3}, \vec{b_4}$ random

$\implies$ adversary only controls $\mathbf{e} \mod 2$ in $\mathbf{c} = \mathbf{hr} + \mathbf{e}$

Distribution used in NTRU-A

define distribution ψ_2^d over $\mathbb{Z}^d$ as $\vec{b_1} + \vec{b_2} - \vec{b_3} - \vec{b_4}$, for $\vec{b_i} \leftarrow_\$ \{0,1\}^d$

alternative generation of ψ_2^d

$$\vec{b} = (\vec{b_1} \underbrace{-2\vec{b_2} \odot \vec{b_3}}_{0 \mod 2}) \odot (1 \underbrace{-2\vec{b_4}}_{0 \mod 2}),$$

$\implies$ $\vec{b} \bmod 2 = \vec{b_1}$

Idea of NTRU-A: use message m as $\vec{b_1} = \vec{b} \mod 2$, and sample $\vec{b_2}, \vec{b_3}, \vec{b_4}$ random

$\implies$ adversary only controls $\mathbf{e} \mod 2$ in $\mathbf{c} = \mathbf{hr} + \mathbf{e}$

$\implies$ worst-case decryption errors $\approx$ average-case errors

$\implies$ no additional error-reducing transform necessary

NTRU-A

$\text{Enc}(\mathbf{h} \in \mathcal{R}, \vec{m} \in \{0,1\}^d)$

$\mathbf{r} := \text{Gen1}()$

$\vec{b}_2, \vec{b}_3, \vec{b}_4 \leftarrow \{0,1\}^d$

$\mathbf{e} := (\vec{m} - 2\vec{b}_2 \odot \vec{b}_3) \odot (1 - 2\vec{b}_4)$

return $\mathbf{hr} + \mathbf{e}$

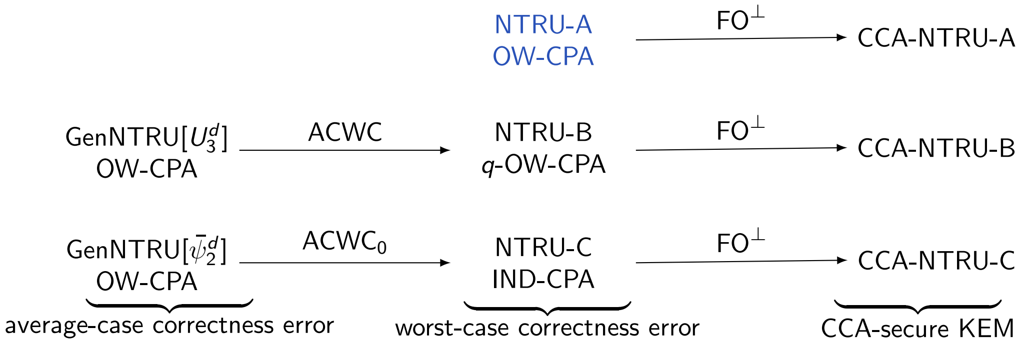
$\text{Dec}(\mathbf{f} \in \mathcal{R}, \mathbf{c} \in \mathcal{R})$

return $(\mathbf{cf} \bmod {}^{\pm} q) \bmod 2$

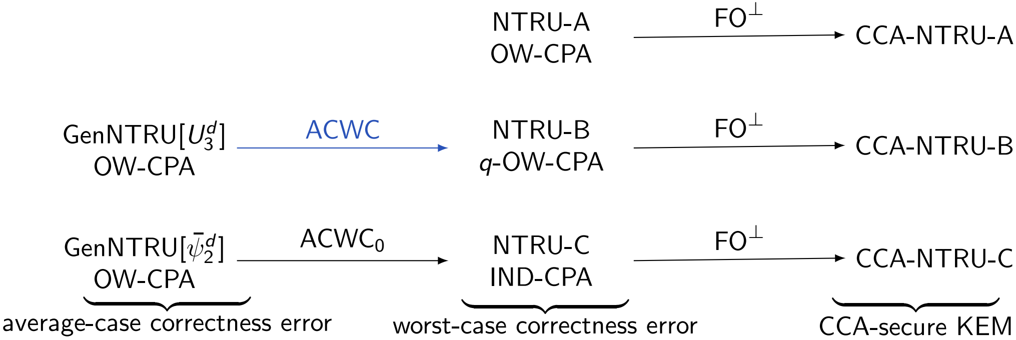
OW-CPA secure based on $\text{NTRU}_{\psi_2^d}$ and $\mathcal{R}\text{-LWE2}_{\psi_2^d}$ assumption

$\mathcal{R}\text{-LWE2}_{\psi_2^d}$ assumption: given $(\mathbf{h}, \mathbf{hr} + \mathbf{e})$ for $\mathbf{h} \leftarrow \mathcal{R}$ and $\mathbf{r}, \mathbf{e} \leftarrow_\$ \psi_2^d$ difficult to compute $\mathbf{e} \bmod 2$

Overview


NTRU-A
OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-A
GenNTRU$[U_3^d]$
OW-CPA
ACWC
NTRU-B
q-OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-B
GenNTRU$[\bar{\psi}_2^d]$
OW-CPA
ACWC_0
NTRU-C
IND-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-C
average-case correctness error
worst-case correctness error
CCA-secure KEM

Overview


NTRU-A
OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-A
$\mathsf{GenNTRU}[U_3^d]$
OW-CPA
ACWC
NTRU-B
q-OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-B
$\mathsf{GenNTRU}[\bar{\psi}_2^d]$
OW-CPA
ACWC_0
NTRU-C
IND-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-C
average-case correctness error
worst-case correctness error
CCA-secure KEM

Size-preserving ACWC

similar to ACWC_0 but size-preserving

needs different proof techniques

Size-preserving ACWC

similar to ACWC_0 but size-preserving

needs different proof techniques

OW-CPA proof uses Measure-and-Reprogram Theorem [DFM20]

worst-case error bound uses Hoeffding Bound

Size-preserving ACWC

similar to ACWC_0 but size-preserving

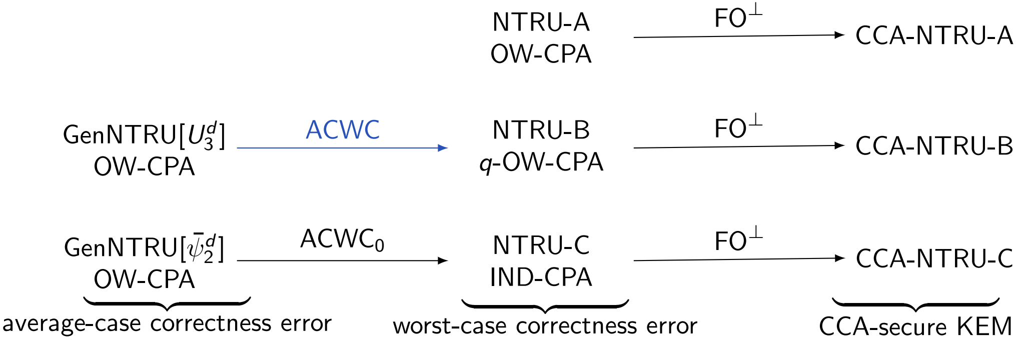
needs different proof techniques

OW-CPA proof uses Measure-and-Reprogram Theorem [DFM20]

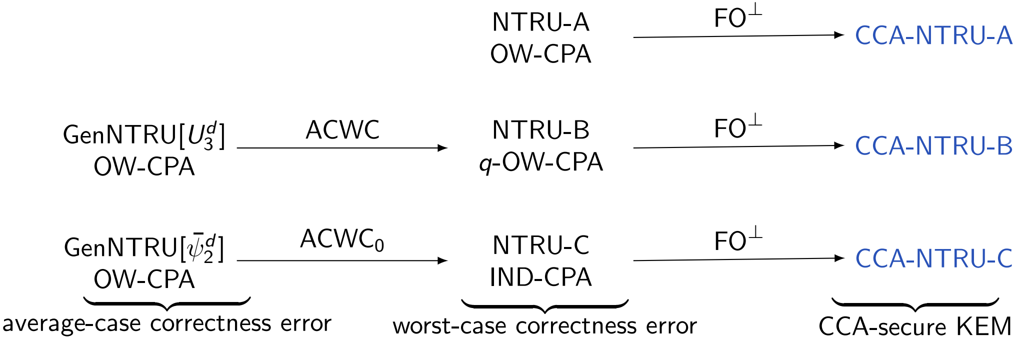
worst-case error bound uses Hoeffding Bound

see Paper for details

Overview


NTRU-A
OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-A
GenNTRU[U_3^d]
OW-CPA
ACWC
NTRU-B
q-OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-B
GenNTRU[$\bar{\psi}_2^d$]
OW-CPA
ACWC_0
NTRU-C
IND-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-C
average-case correctness error
worst-case correctness error
CCA-secure KEM

Overview


NTRU-A
OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-A
GenNTRU$[U_3^d]$
OW-CPA
ACWC
NTRU-B
q-OW-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-B
GenNTRU$[\bar{\psi}_2^d]$
OW-CPA
ACWC$_0$
NTRU-C
IND-CPA
$\mathsf{FO}^{\perp}$
CCA-NTRU-C
average-case correctness error
worst-case correctness error
CCA-secure KEM

Results

Scheme	KeyGen	Encaps	Decaps	pk (B)	c (B)	security
CCA-NTRU-A_{2917}^{648}	6.2K	5.6K	7.3K	972	972	180
NTRU-HRSS-701	220.3K	34.6K	65K	1138	1138	166
NTTRU	6.4K	6.1K	7.9K	1248	1248	183
Kyber-512 (90's)	6.2K	7.9K	9.2K	800	768	148
Kyber-768 (90's)	11K	13.1K	14.8K	1184	1088	212

Table: Number of cycles (on a Skylake machine) for various operations of a CCA-secure KEM.

Conclusion

We showed

- different ways to obtain worst-case correctness for NTRU
- proven them secure in the ROM and QROM

Conclusion

We showed

- different ways to obtain worst-case correctness for NTRU
- proven them secure in the ROM and QROM
- allows us to apply FO to obtain CCA security
- allows for smaller modulus $q \implies$ better security and compactness

Conclusion

We showed

- different ways to obtain worst-case correctness for NTRU
- proven them secure in the ROM and QROM
- allows us to apply FO to obtain CCA security
- allows for smaller modulus $q \implies$ better security and compactness

using NTT-friendly Rings obtain three efficient CCA-secure NTRU Designs, with flexible parameter choice

Conclusion

We showed

- different ways to obtain worst-case correctness for NTRU
- proven them secure in the ROM and QROM
- allows us to apply FO to obtain CCA security
- allows for smaller modulus $q \implies$ better security and compactness

using NTT-friendly Rings obtain three efficient CCA-secure NTRU Designs, with flexible parameter choice

Thank you!

Andris Ambainis, Mike Hamburg, and Dominique Unruh.
Quantum security proofs using semi-classical oracles.
In *Advances in Cryptology – CRYPTO 2019*, volume 11693 of *Lecture Notes in Computer Science*, pages 269–295. Springer, 2019.
https://ia.cr/2018/904.

Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry.
Random oracles in a quantum world.
In *International conference on the theory and application of cryptology and information security*, pages 41–69. Springer, 2011.

Jelle Don, Serge Fehr, and Christian Majenz.
The measure-and-reprogram technique 2.0: Multi-round Fiat-Shamir and more.
In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III*, volume 12172 of *Lecture Notes in Computer Science*, pages 602–631. Springer, 2020.

Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner.
Online-extractability in the quantum random-oracle model.
Cryptology ePrint Archive, Report 2021/280, 2021.
https://ia.cr/2021/280.

Nick Howgrave-Graham, Phong Q. Nguyen, David Pointcheval, John Proos, Joseph H. Silverman, Ari Singer, and William Whyte.
The impact of decryption failures on the security of NTRU encryption.
In *CRYPTO*, pages 226–246, 2003.

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman.
NTRU: A ring-based public key cryptosystem.
In *ANTS*, pages 267–288, 1998.

Andreas Hülsing, Joost Rijneveld, John M. Schanck, and Peter Schwabe.
High-speed key encapsulation from NTRU.
In *CHES*, volume 10529 of *Lecture Notes in Computer Science*, pages 232–252. Springer, 2017.

Vadim Lyubashevsky and Gregor Seiler.

NTTRU: truly fast NTRU using NTT.
IACR Trans. Cryptogr. Hardw. Embed. Syst., 2019(3):180–201, 2019.

Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa.
Tightly-secure key-encapsulation mechanism in the quantum random oracle model.

In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 520–551. Springer, Heidelberg, April / May 2018.
http://eprint.iacr.org/2017/1004.