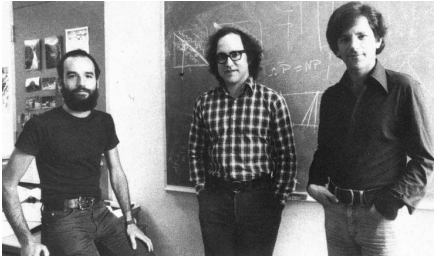
A Closer Look at Falcon

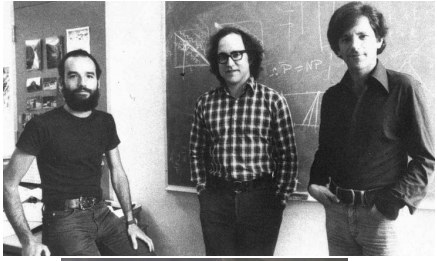
Pierre-Alain Fouque Hubert de Groote Eike Kiltz
Phillip Gajland Jonas Janneck

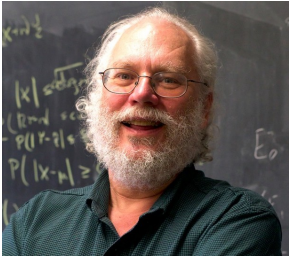
November 26, 2025

MOTIVATION: RSA, DH, SHOR AND QUANTUM

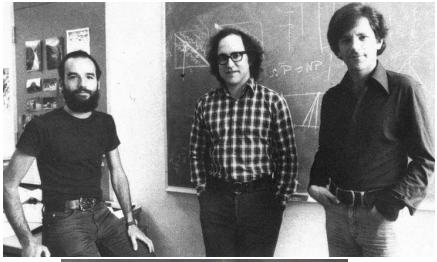


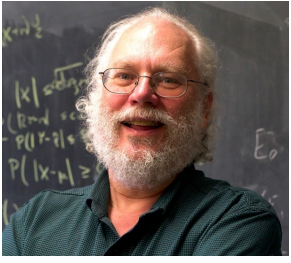
MOTIVATION: RSA, DH, SHOR AND QUANTUM

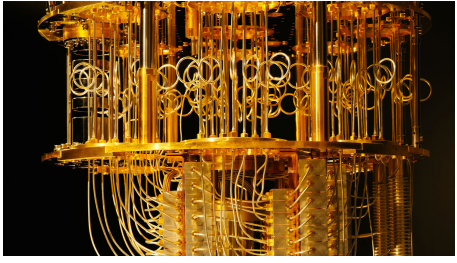


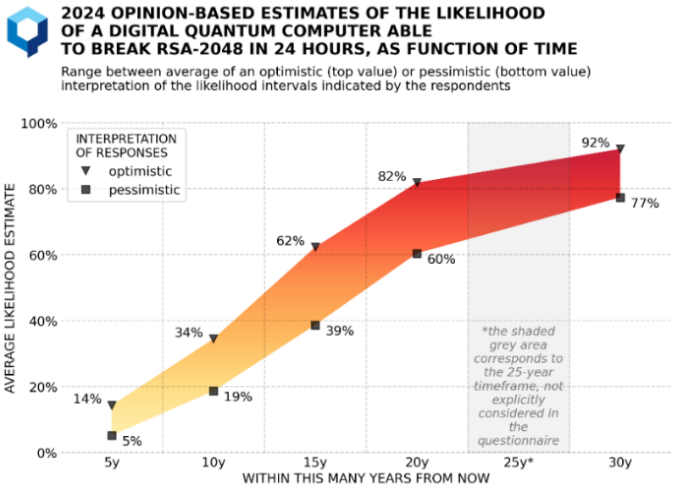


MOTIVATION: RSA, DH, SHOR AND QUANTUM








2024 OPINION-BASED ESTIMATES OF THE LIKELIHOOD OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIME
Range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the likelihood intervals indicated by the respondents
INTERPRETATION OF RESPONSES
optimistic
pessimistic
AVERAGE LIKELIHOOD ESTIMATE
100%
80%
60%
40%
20%
0%
14%
5%
34%
19%
62%
39%
82%
60%
92%
77%
*the shaded grey area corresponds to the 25-year timeframe, not explicitly considered in the questionnaire
5y
10y
15y
20y
25y*
30y
WITHIN THIS MANY YEARS FROM NOW

- Multi-year effort to standardise post-quantum cryptography
- After 4 rounds, 5 algorithms were selected for standardisation: 2 KEM, 3 Sig

- Multi-year effort to standardise post-quantum cryptography
- After 4 rounds, 5 algorithms were selected for standardisation: 2 KEM, 3 Sig

- Multi-year effort to standardise post-quantum cryptography
- After 4 rounds, 5 algorithms were selected for standardisation: 2 KEM, 3 Sig

Key Encapsulation Mechanism (KEM)	Signature Scheme (Sig)
`CRYSTALS-Kyber` [SAB+22] (`ML-KEM`)	`CRYSTALS-Dilithium` [LDK+22] (`ML-DSA`)
`HQC` [GMA+25]	`Falcon` [PFH+22] (`FN-DSA`)
	`SPHINCS+` [HBD+22] (`SLH-DSA`)

- Falcon is compact: small $|\sigma| + |pk|$

- Complicated implementation due to Gaussian Sampling
- Concrete Security?

- Falcon is compact: small $|\sigma| + |pk|$

Signature Scheme	NIST Level	$\lvert\sigma\rvert$	$\lvert pk\rvert$	$\lvert sk\rvert$	Security	Assumptions
CRYSTALS-Dilithium	II	2 420	1 312	32	**SUF-CMA**	**MLWE, SelfTargetMSIS, MSIS**
	III	3 293	1 952	32		
	V	4 595	2 592	32		
Falcon	I	666	897	1 281	**SUF-CMA**	**second-preimage multi-target NTRU-ISIS**
	V	1 280	1 793	2 305		
SPHINCS$^+$	I	7 856	32	64	**UF-CMA**	**PRF, ITSR, SM-TCR, SM-DSPR**
	III	16 224	48	96		
	V	29 792	64	128		

- Complicated implementation due to Gaussian Sampling
- Concrete Security?

- Falcon is compact: small $|\sigma| + |pk|$

Signature Scheme	NIST Level	$\lvert\sigma\rvert$	$\lvert pk\rvert$	$\lvert sk\rvert$	Security	Assumptions
CRYSTALS-Dilithium	II	2 420	1 312	32	**SUF-CMA**	**MLWE, SelfTargetMSIS, MSIS**
	III	3 293	1 952	32		
	V	4 595	2 592	32		
Falcon	I	666	897	1 281	**SUF-CMA**	**second-preimage multi-target NTRU-ISIS**
	V	1 280	1 793	2 305		
SPHINCS$^+$	I	7 856	32	64	**UF-CMA**	**PRF, ITSR, SM-TCR, SM-DSPR**
	III	16 224	48	96		
	V	29 792	64	128		

- Complicated implementation due to Gaussian Sampling
- Concrete Security?

- Falcon is compact: small $|\sigma| + |pk|$

Signature Scheme	NIST Level	$\lvert\sigma\rvert$	$\lvert pk\rvert$	$\lvert sk\rvert$	Security	Assumptions
CRYSTALS-Dilithium	II	2 420	1 312	32	**SUF-CMA**	**MLWE, SelfTargetMSIS, MSIS**
	III	3 293	1 952	32		
	V	4 595	2 592	32		
Falcon	I	666	897	1 281	**SUF-CMA**	**second-preimage multi-target NTRU-ISIS**
	V	1 280	1 793	2 305		
SPHINCS$^+$	I	7 856	32	64	**UF-CMA**	**PRF, ITSR, SM-TCR, SM-DSPR**
	III	16 224	48	96		
	V	29 792	64	128		

- Complicated implementation due to Gaussian Sampling
- Concrete Security?

- FALCON is based on [GPV08], which proves lattice-based *full domain hash*
- Security proof is not sufficient for FALCON
  - FALCON is defined over NTRU lattices, not plain lattices
  - Statistical distance arguments fail using FALCON parameters
  - FALCON avoids correctness error by repeated signing

- FALCON is based on [GPV08], which proves lattice-based *full domain hash*
- Security proof is not sufficient for FALCON
  - FALCON is defined over NTRU lattices, not plain lattices
  - Statistical distance arguments fail using FALCON parameters
  - FALCON avoids correctness error by repeated signing

- FALCON is based on [GPV08], which proves lattice-based *full domain hash*
- Security proof is not sufficient for FALCON
  - FALCON is defined over NTRU lattices, not plain lattices
  - Statistical distance arguments fail using FALCON parameters
  - FALCON avoids correctness error by repeated signing

- FALCON is based on [GPV08], which proves lattice-based *full domain hash*
- Security proof is not sufficient for FALCON
  - FALCON is defined over NTRU lattices, not plain lattices
  - Statistical distance arguments fail using FALCON parameters
  - FALCON avoids correctness error by repeated signing

- FALCON is based on [GPV08], which proves lattice-based *full domain hash*
- Security proof is not sufficient for FALCON
  - FALCON is defined over NTRU lattices, not plain lattices
  - Statistical distance arguments fail using FALCON parameters
  - FALCON avoids correctness error by repeated signing

- FALCON is based on [GPV08], which proves lattice-based *full domain hash*
- Security proof is not sufficient for FALCON
  - FALCON is defined over NTRU lattices, not plain lattices
  - Statistical distance arguments fail using FALCON parameters
  - FALCON avoids correctness error by repeated signing

Can Falcon be proven secure?
If so, what is its concrete security?

- Adaptation of [GPV08] uniformity results to Rényi divergence
- Proof for a modified generalisation of Falcon
  - Modification: Minor efficiency overhead due to salt resampling
  - Generalisation: Parametrised by Trapdoor Generation and Preimage Sampler
- Optimisation of the security bound and concrete bit security

- Adaptation of [GPV08] uniformity results to Rényi divergence
- Proof for a modified generalisation of Falcon
  - Modification: Minor efficiency overhead due to salt resampling
  - Generalisation: Parametrised by Trapdoor Generation and Preimage Sampler
- Optimisation of the security bound and concrete bit security

- Adaptation of [GPV08] uniformity results to Rényi divergence
- Proof for a modified generalisation of Falcon
  - Modification: Minor efficiency overhead due to salt resampling
  - Generalisation: Parametrised by Trapdoor Generation and Preimage Sampler
- Optimisation of the security bound and concrete bit security

- Adaptation of [GPV08] uniformity results to Rényi divergence
- Proof for a modified generalisation of Falcon
  - Modification: Minor efficiency overhead due to salt resampling
  - Generalisation: Parametrised by Trapdoor Generation and Preimage Sampler
- Optimisation of the security bound and concrete bit security

- Adaptation of [GPV08] uniformity results to Rényi divergence
- Proof for a modified generalisation of Falcon
  - Modification: Minor efficiency overhead due to salt resampling
  - Generalisation: Parametrised by Trapdoor Generation and Preimage Sampler
- Optimisation of the security bound and concrete bit security

- Adaptation of [GPV08] uniformity results to Rényi divergence
- Proof for a modified generalisation of Falcon
  - Modification: Minor efficiency overhead due to salt resampling
  - Generalisation: Parametrised by Trapdoor Generation and Preimage Sampler
- Optimisation of the security bound and concrete bit security

Scheme	**Notion**	**Bit Security**
Falcon$^+$-512 ($Q_s = 2^{64}$)	**UF-CMA** (Th. 1) **SUF-CMA** (Th. 2)	113
Falcon$^+$-512 ($Q_s = 2^{58}$)		119
Falcon$^+$-1024 ($Q_s = 2^{64}$)		256

Table: Provable bit security (Q_s = maximal signing queries).

BACKGROUND AND FALCON

Rényi divergence [Rén61]

- Describes closeness of two distributions (generalisation of Kullback-Leibler)
- Used for better security bounds/parameters [LSS14, BLL+15, Pre17]
- Rényi divergence: $r = R_a(\mathcal{P} \mid\mid \mathcal{Q}) = 1 + \delta$ for $\delta \geq 0$
- Applied multiplicatively
- For Q queries to underlying distributions: r^Q loss

Rényi divergence [Rén61]

- Describes closeness of two distributions (generalisation of Kullback-Leibler)
- Used for better security bounds/parameters [LSS14, BLL+15, Pre17]
- Rényi divergence: $r = R_a(\mathcal{P} \mid\mid \mathcal{Q}) = 1 + \delta$ for $\delta \geq 0$
- Applied multiplicatively
- For Q queries to underlying distributions: r^Q loss

Rényi divergence [Rén61]

- Describes closeness of two distributions (generalisation of Kullback-Leibler)
- Used for better security bounds/parameters [LSS14, BLL+15, Pre17]
- Rényi divergence: $r = R_a(\mathcal{P} \mid\mid \mathcal{Q}) = 1 + \delta$ for $\delta \geq 0$
- Applied multiplicatively
- For Q queries to underlying distributions: r^Q loss

Rényi divergence [Rén61]

- Describes closeness of two distributions (generalisation of Kullback-Leibler)
- Used for better security bounds/parameters [LSS14, BLL+15, Pre17]
- Rényi divergence: $r = R_a(\mathcal{P} \mid\mid \mathcal{Q}) = 1 + \delta$ for $\delta \geq 0$
- Applied multiplicatively
- For Q queries to underlying distributions: r^Q loss

Rényi divergence [Rén61]

- Describes closeness of two distributions (generalisation of Kullback-Leibler)
- Used for better security bounds/parameters [LSS14, BLL+15, Pre17]
- Rényi divergence: $r = R_a(\mathcal{P} \mid\mid \mathcal{Q}) = 1 + \delta$ for $\delta \geq 0$
- Applied multiplicatively
- For Q queries to underlying distributions: r^Q loss

$$f_{\boldsymbol{h}} \colon \mathcal{R} \times \mathcal{R} \to \mathcal{R}_q$$
$$(\boldsymbol{s}_1, \boldsymbol{s}_2) \mapsto \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$$

$$\mathsf{PreSmp} \colon (sk, \boldsymbol{c}) \mapsto (\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2_{|f_{\boldsymbol{h}}(\boldsymbol{s}_1, \boldsymbol{s}_2) = \boldsymbol{c}}$$

$$f_{\boldsymbol{h}} \colon \mathcal{R} \times \mathcal{R} \to \mathcal{R}_q$$
$$(\boldsymbol{s}_1, \boldsymbol{s}_2) \mapsto \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$$

$$\mathsf{PreSmp} \colon (sk, \boldsymbol{c}) \mapsto (\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2_{|f_{\boldsymbol{h}}(\boldsymbol{s}_1, \boldsymbol{s}_2) = \boldsymbol{c}}$$

$\underline{\mathsf{Gen}}$

$(\boldsymbol{B}, \boldsymbol{h}) \xleftarrow{\$} \mathsf{TpdGen}(\mathcal{R}, \alpha, q)$

$(sk, pk) \coloneqq (\boldsymbol{B}, \boldsymbol{h}) \in \mathbb{Z}^{2n \times 2n} \times \mathcal{R}_q$

return (sk, pk)

$\underline{\mathsf{Sgn}(sk, m)}$

$r \xleftarrow{\$} \{0,1\}^k$

$\boldsymbol{c} \coloneqq \mathsf{H}(pk, r, m) \in \mathcal{R}_q$

repeat

$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$

until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$

$\sigma \coloneqq (r, \boldsymbol{s}_2) \in \{0,1\}^k \times \mathcal{R}$

return σ

$\underline{\mathsf{Ver}(pk = \boldsymbol{h}, m, \sigma = (r, \boldsymbol{s}_2))}$

$\boldsymbol{c} \coloneqq \mathsf{H}(pk, r, m)$

$\boldsymbol{s}_1 \coloneqq \boldsymbol{c} - \boldsymbol{s}_2 * \boldsymbol{h} \mod q$

return $[\![\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta]\!]$

$$f_{\boldsymbol{h}} \colon \mathcal{R} \times \mathcal{R} \to \mathcal{R}_q$$
$$(\boldsymbol{s}_1, \boldsymbol{s}_2) \mapsto \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$$

$$\mathsf{PreSmp} \colon (sk, \boldsymbol{c}) \mapsto (\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2_{|f_{\boldsymbol{h}}(\boldsymbol{s}_1, \boldsymbol{s}_2) = \boldsymbol{c}}$$

$\underline{\mathsf{Gen}}$

$(\boldsymbol{B}, \boldsymbol{h}) \xleftarrow{\$} \mathsf{TpdGen}(\mathcal{R}, \alpha, q)$
$(sk, pk) \coloneqq (\boldsymbol{B}, \boldsymbol{h}) \in \mathbb{Z}^{2n \times 2n} \times \mathcal{R}_q$
return (sk, pk)

$\underline{\mathsf{Sgn}(sk, m)}$

$r \xleftarrow{\$} \{0,1\}^k$
$\boldsymbol{c} \coloneqq \mathsf{H}(pk, r, m) \in \mathcal{R}_q$
repeat
  $(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$
$\sigma \coloneqq (r, \boldsymbol{s}_2) \in \{0,1\}^k \times \mathcal{R}$
return σ

$\underline{\mathsf{Ver}(pk = \boldsymbol{h}, m, \sigma = (r, \boldsymbol{s}_2))}$

$\boldsymbol{c} \coloneqq \mathsf{H}(pk, r, m)$
$\boldsymbol{s}_1 \coloneqq \boldsymbol{c} - \boldsymbol{s}_2 * \boldsymbol{h} \mod q$
return $[\![\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta]\!]$

$$f_{\boldsymbol{h}} \colon \mathcal{R} \times \mathcal{R} \to \mathcal{R}_q$$
$$(\boldsymbol{s}_1, \boldsymbol{s}_2) \mapsto \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$$

$$\mathsf{PreSmp} \colon (sk, \boldsymbol{c}) \mapsto (\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2_{|f_{\boldsymbol{h}}(\boldsymbol{s}_1, \boldsymbol{s}_2) = \boldsymbol{c}}$$

Gen

$(\boldsymbol{B}, \boldsymbol{h}) \xleftarrow{\$} \mathsf{TpdGen}(\mathcal{R}, \alpha, q)$
$(sk, pk) \coloneqq (\boldsymbol{B}, \boldsymbol{h}) \in \mathbb{Z}^{2n \times 2n} \times \mathcal{R}_q$
return (sk, pk)

Sgn(sk, m)

$r \xleftarrow{\$} \{0,1\}^k$
$\boldsymbol{c} \coloneqq \mathsf{H}(pk, r, m) \in \mathcal{R}_q$
repeat
  $(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$
$\sigma \coloneqq (r, \boldsymbol{s}_2) \in \{0,1\}^k \times \mathcal{R}$
return σ

Ver$(pk = \boldsymbol{h}, m, \sigma = (r, \boldsymbol{s}_2))$

$\boldsymbol{c} \coloneqq \mathsf{H}(pk, r, m)$
$\boldsymbol{s}_1 \coloneqq \boldsymbol{c} - \boldsymbol{s}_2 * \boldsymbol{h} \mod q$
return $[\![\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta]\!]$

Sgn$^+(sk, m)$

repeat
  $r \xleftarrow{\$} \{0,1\}^k$
  $\boldsymbol{c} \coloneqq \mathsf{H}(pk, r, m) \in \mathcal{R}_q$
  $(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$
$\sigma \coloneqq (r, \boldsymbol{s}_2) \in \{0,1\}^k \times \mathcal{R}$
return σ

PROOF IDEA OF [GPV08] FROM ONE-WAYNESS OF $f_{\boldsymbol{h}}$ [1]

$$f_{\boldsymbol{h}} \colon \mathcal{R} \times \mathcal{R} \to \mathcal{R}_q$$
$$(\boldsymbol{s}_1, \boldsymbol{s}_2) \mapsto \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$$

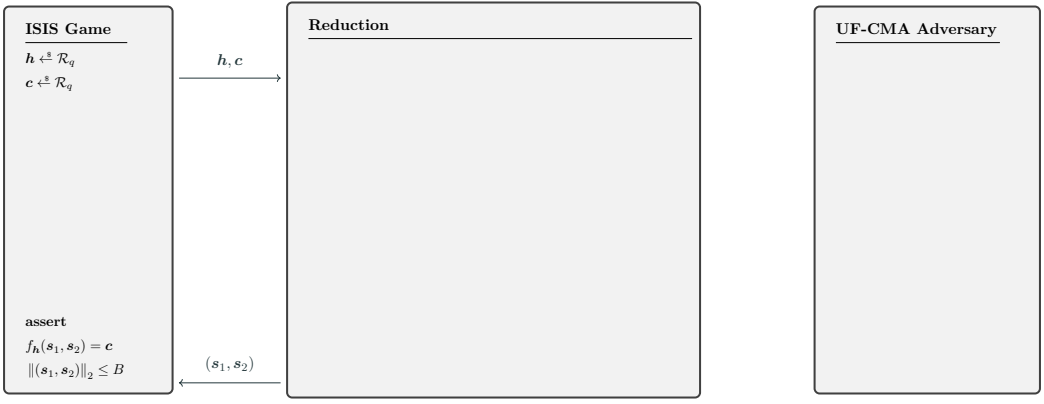
$$\mathsf{PreSmp} \colon (sk, \boldsymbol{c}) \mapsto (\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2_{|f_{\boldsymbol{h}}(\boldsymbol{s}_1, \boldsymbol{s}_2) = \boldsymbol{c}}$$

[1] We stick to the NTRU notation but [GPV08] uses plain (unstructured) lattices

PROOF IDEA OF [GPV08] FROM ONE-WAYNESS OF $f_{\boldsymbol{h}}$ [1]

$$f_{\boldsymbol{h}} \colon \mathcal{R} \times \mathcal{R} \to \mathcal{R}_q$$
$$(\boldsymbol{s}_1, \boldsymbol{s}_2) \mapsto \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$$

$$\mathsf{PreSmp} \colon (sk, \boldsymbol{c}) \mapsto (\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2_{|f_{\boldsymbol{h}}(\boldsymbol{s}_1, \boldsymbol{s}_2) = \boldsymbol{c}}$$

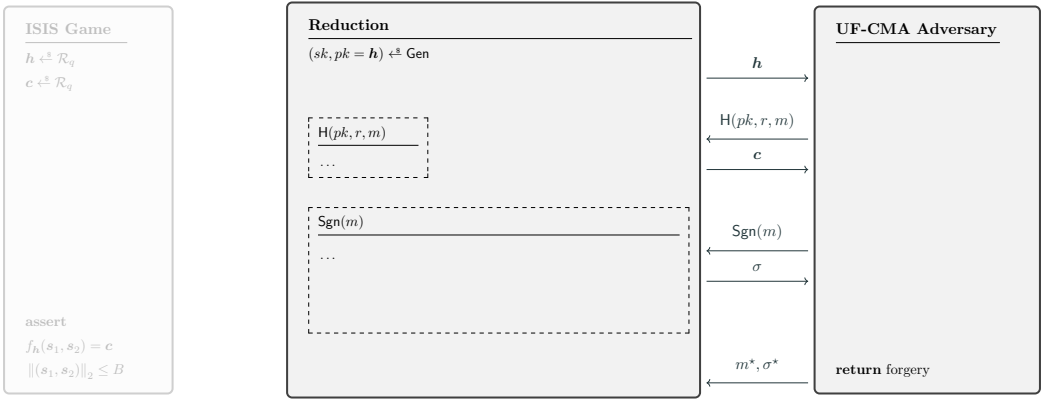


[1] We stick to the NTRU notation but [GPV08] uses plain (unstructured) lattices

PROOF IDEA OF [GPV08] FROM ONE-WAYNESS OF $f_{\boldsymbol{h}}$ [1]

$$f_{\boldsymbol{h}} \colon \mathcal{R} \times \mathcal{R} \to \mathcal{R}_q$$
$$(\boldsymbol{s}_1, \boldsymbol{s}_2) \mapsto \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$$

$$\mathsf{PreSmp} \colon (sk, \boldsymbol{c}) \mapsto (\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2_{|f_{\boldsymbol{h}}(\boldsymbol{s}_1, \boldsymbol{s}_2) = \boldsymbol{c}}$$



[1] We stick to the NTRU notation but [GPV08] uses plain (unstructured) lattices

PROOF IDEA OF [GPV08] FROM ONE-WAYNESS OF $f_{\boldsymbol{h}}$ [1]

$$f_{\boldsymbol{h}} \colon \mathcal{R} \times \mathcal{R} \to \mathcal{R}_q$$
$$(\boldsymbol{s}_1, \boldsymbol{s}_2) \mapsto \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$$

$$\mathsf{PreSmp} \colon (sk, \boldsymbol{c}) \mapsto (\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2_{|f_{\boldsymbol{h}}(\boldsymbol{s}_1, \boldsymbol{s}_2) = \boldsymbol{c}}$$

ISIS Game

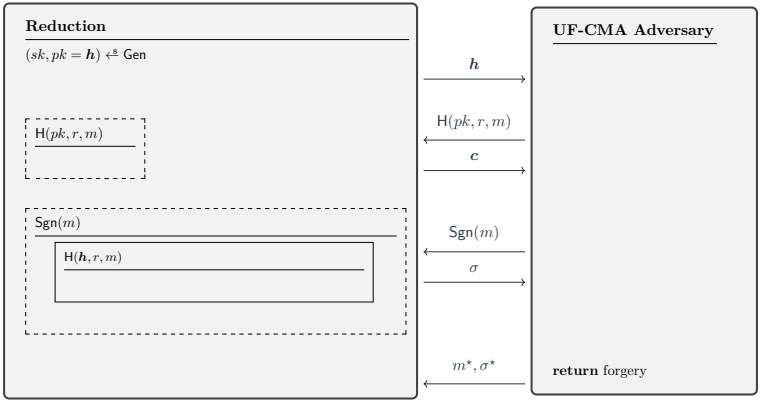
$h \xleftarrow{\$} \mathcal{R}_q$

$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$

assert

$f_h(s_1, s_2) = c$

$\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq B$

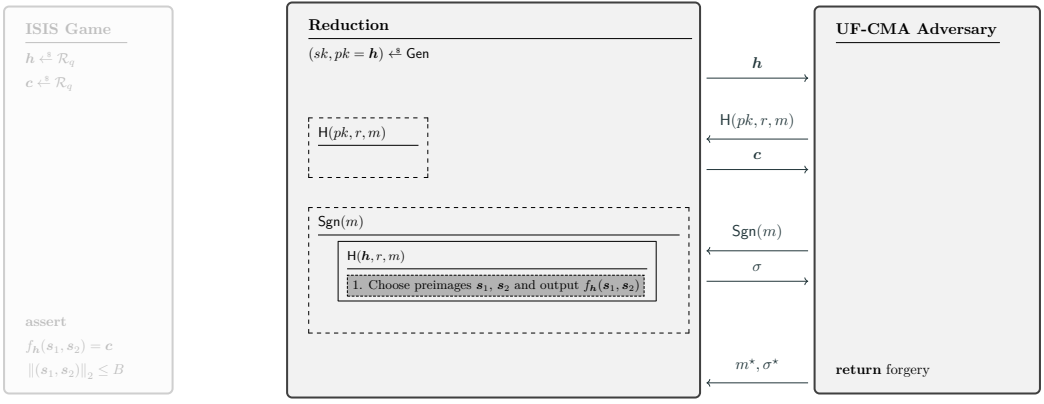


[1] We stick to the NTRU notation but [GPV08] uses plain (unstructured) lattices

PROOF IDEA OF [GPV08] FROM ONE-WAYNESS OF $f_{\boldsymbol{h}}$ [1]

$$f_{\boldsymbol{h}} \colon \mathcal{R} \times \mathcal{R} \to \mathcal{R}_q$$
$$(\boldsymbol{s}_1, \boldsymbol{s}_2) \mapsto \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$$

$$\mathsf{PreSmp} \colon (sk, \boldsymbol{c}) \mapsto (\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2_{|f_{\boldsymbol{h}}(\boldsymbol{s}_1, \boldsymbol{s}_2) = \boldsymbol{c}}$$

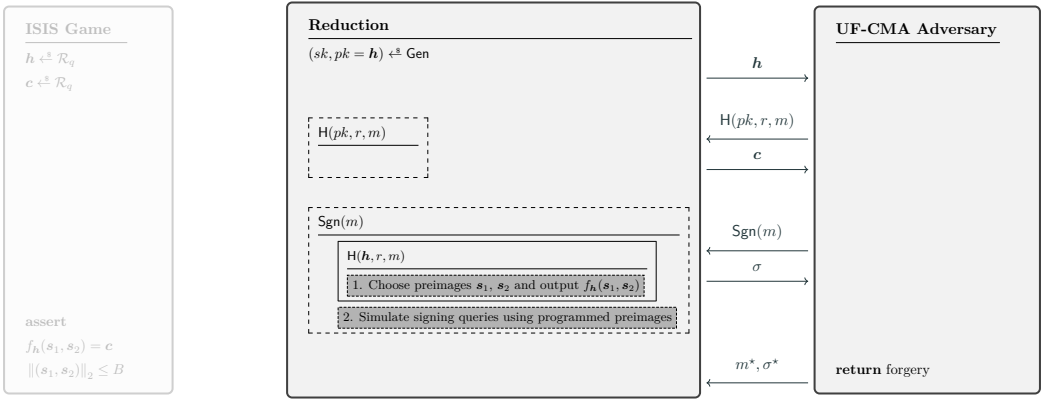


[1] We stick to the NTRU notation but [GPV08] uses plain (unstructured) lattices

PROOF IDEA OF [GPV08] FROM ONE-WAYNESS OF $f_{\boldsymbol{h}}$ [1]

$$f_{\boldsymbol{h}} \colon \mathcal{R} \times \mathcal{R} \to \mathcal{R}_q$$
$$(\boldsymbol{s}_1, \boldsymbol{s}_2) \mapsto \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$$

$$\mathsf{PreSmp} \colon (sk, \boldsymbol{c}) \mapsto (\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2_{|f_{\boldsymbol{h}}(\boldsymbol{s}_1, \boldsymbol{s}_2) = \boldsymbol{c}}$$

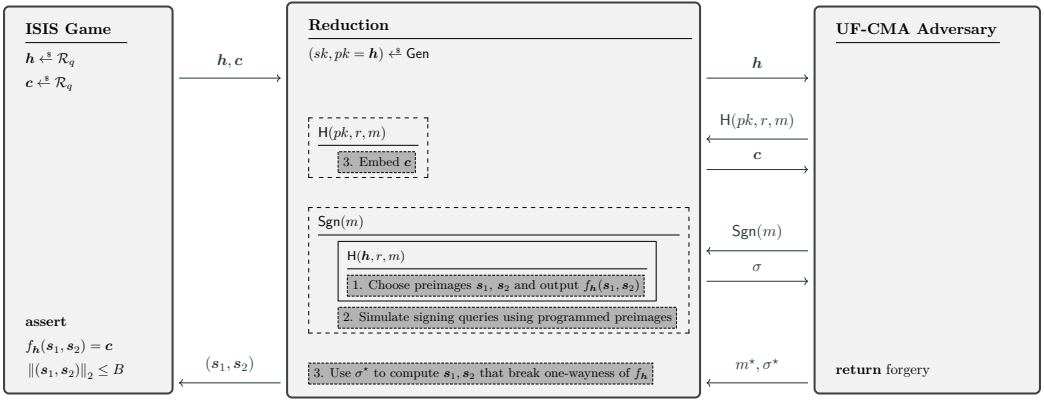


[1] We stick to the NTRU notation but [GPV08] uses plain (unstructured) lattices

PROOF IDEA OF [GPV08] FROM ONE-WAYNESS OF $f_{\boldsymbol{h}}$ [1]

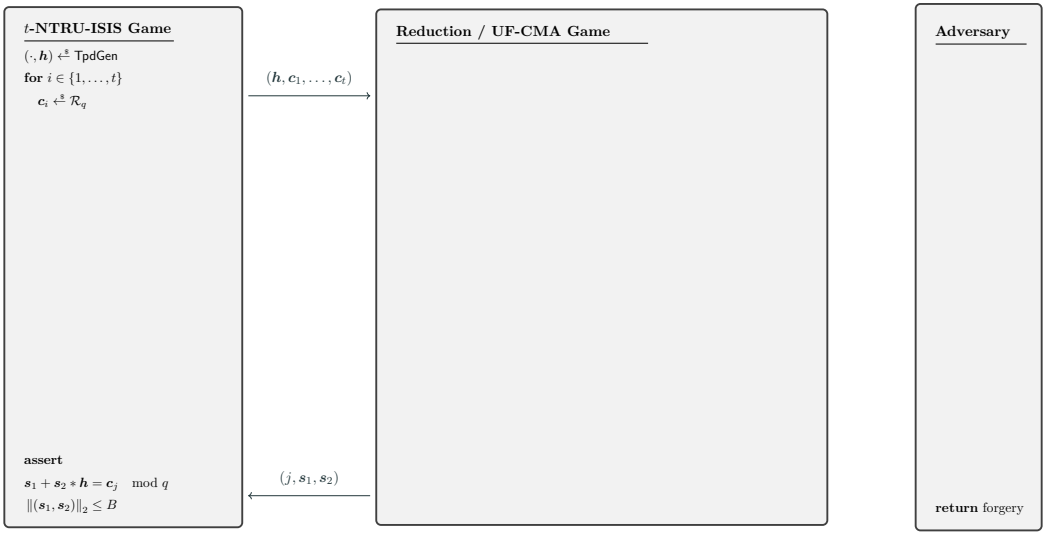
$$f_{\boldsymbol{h}} \colon \mathcal{R} \times \mathcal{R} \to \mathcal{R}_q$$
$$(\boldsymbol{s}_1, \boldsymbol{s}_2) \mapsto \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$$

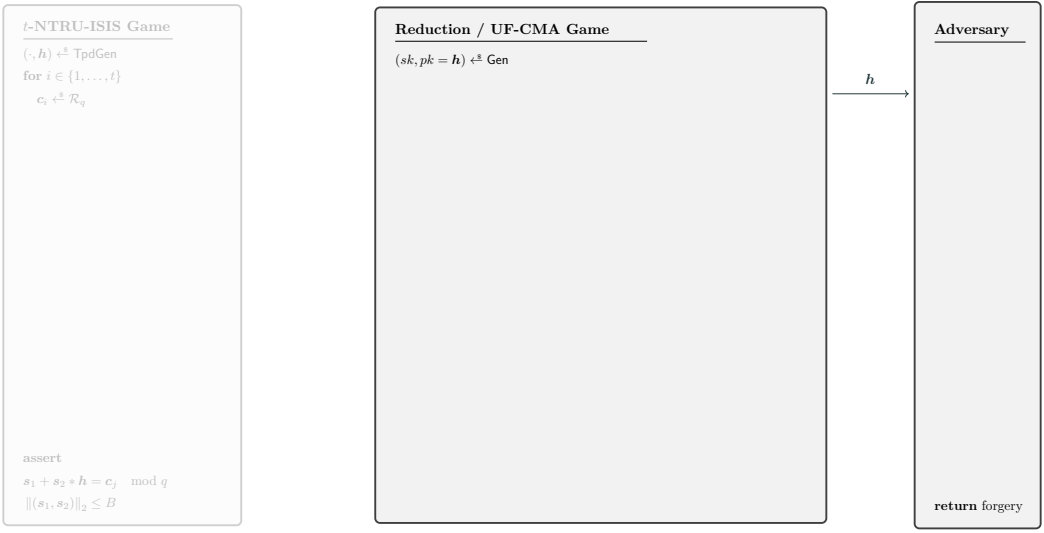
$$\mathsf{PreSmp} \colon (sk, \boldsymbol{c}) \mapsto (\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2_{|f_{\boldsymbol{h}}(\boldsymbol{s}_1, \boldsymbol{s}_2) = \boldsymbol{c}}$$

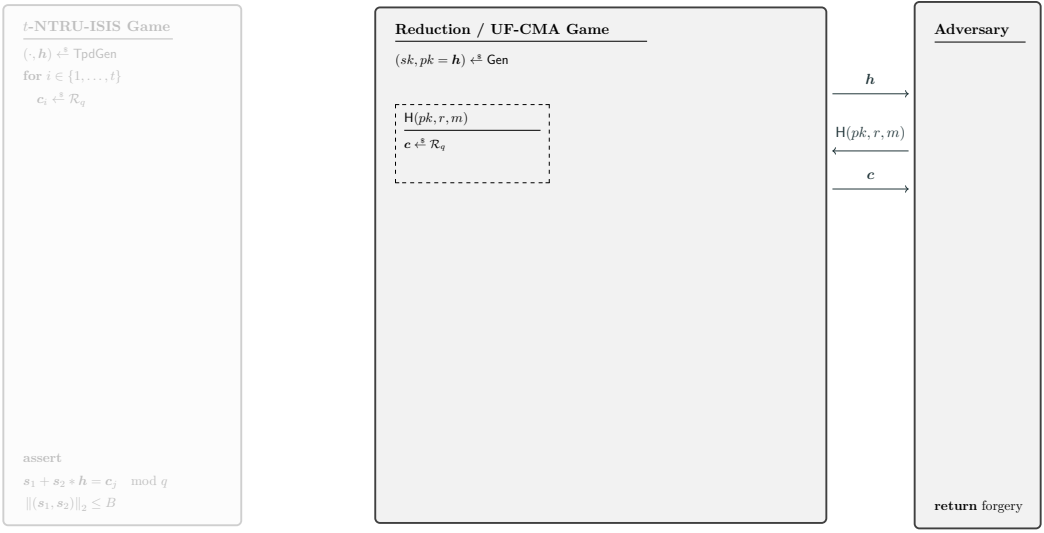


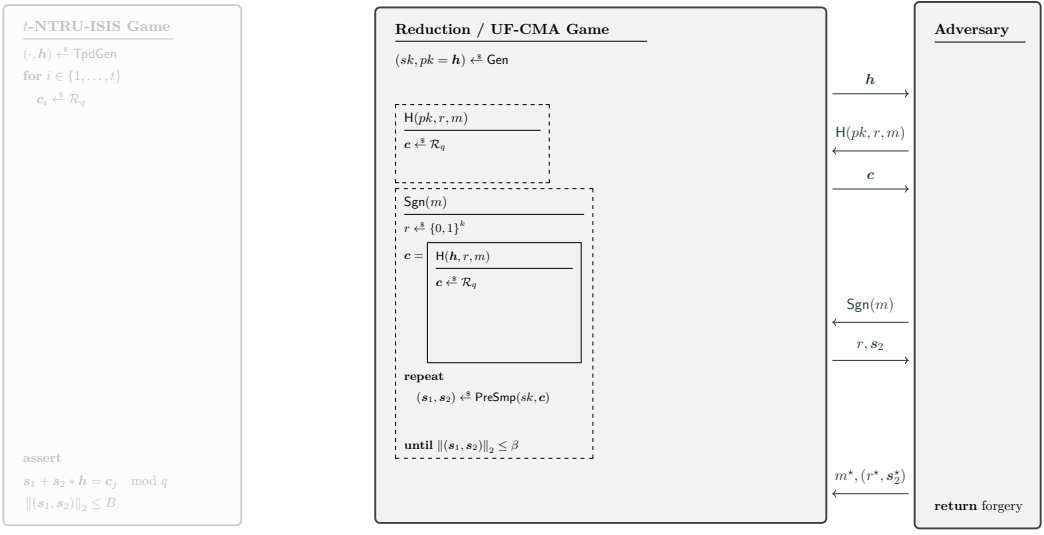
[1] We stick to the NTRU notation but [GPV08] uses plain (unstructured) lattices

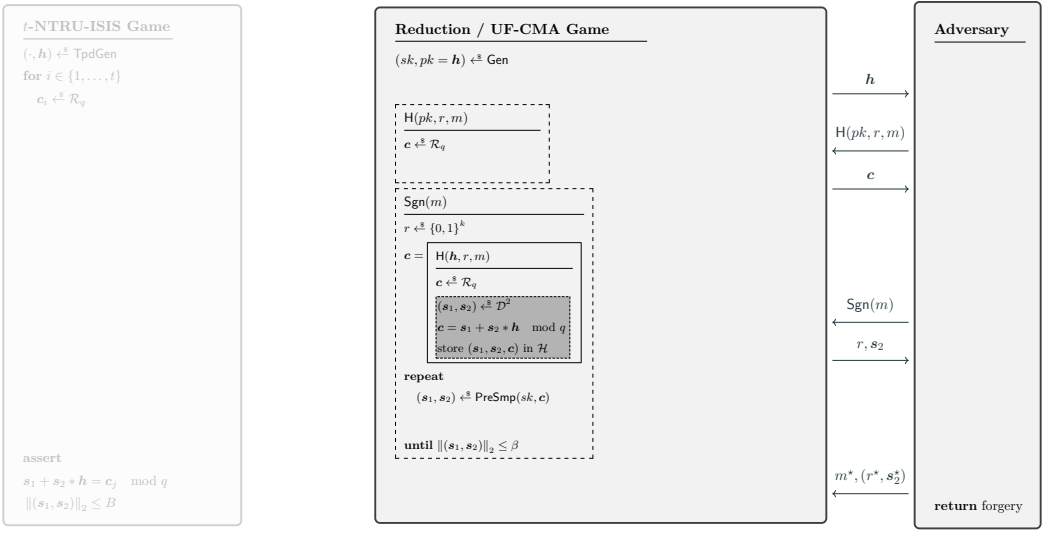
PROOF


t-NTRU-ISIS Game
$(\cdot, \boldsymbol{h}) \xleftarrow{s} \mathsf{TpdGen}$
for $i \in \{1, \ldots, t\}$
$\boldsymbol{c}_i \xleftarrow{s} \mathcal{R}_q$
$(\boldsymbol{h}, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_t)$
Reduction / UF-CMA Game
Adversary
assert
$\boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} = \boldsymbol{c}_j \mod q$
$\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq B$
$(j, \boldsymbol{s}_1, \boldsymbol{s}_2)$
return forgery


t-NTRU-ISIS Game
$(\cdot, \boldsymbol{h}) \xleftarrow{s}$ TpdGen
for $i \in \{1, \ldots, t\}$
$\boldsymbol{c}_i \xleftarrow{s} \mathcal{R}_q$
assert
$\boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} = \boldsymbol{c}_j \mod q$
$\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq B$
Reduction / UF-CMA Game
$(sk, pk = \boldsymbol{h}) \xleftarrow{s}$ Gen
$\boldsymbol{h}$
Adversary
return forgery


t-NTRU-ISIS Game
$(\cdot, \boldsymbol{h}) \xleftarrow{s}$ TpdGen
for $i \in \{1, \ldots, t\}$
$\boldsymbol{c}_i \xleftarrow{s} \mathcal{R}_q$
assert
$\boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} = \boldsymbol{c}_j \mod q$
$\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq B$
Reduction / UF-CMA Game
$(sk, pk = \boldsymbol{h}) \xleftarrow{s}$ Gen
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c} \xleftarrow{s} \mathcal{R}_q$
$\boldsymbol{h}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c}$
Adversary
return forgery


t-NTRU-ISIS Game
$(\cdot, \boldsymbol{h}) \xleftarrow{\$} \mathsf{TpdGen}$
for $i \in \{1, \ldots, t\}$
$\boldsymbol{c}_i \xleftarrow{\$} \mathcal{R}_q$
assert
$\boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} = \boldsymbol{c}_j \mod q$
$\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq B$
Reduction / UF-CMA Game
$(sk, pk = \boldsymbol{h}) \xleftarrow{\$} \mathsf{Gen}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$\mathsf{Sgn}(m)$
$r \xleftarrow{\$} \{0,1\}^k$
$\boldsymbol{c} =$
$\mathsf{H}(\boldsymbol{h}, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
repeat
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$
$\boldsymbol{h}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c}$
$\mathsf{Sgn}(m)$
$r, \boldsymbol{s}_2$
$m^\star, (r^\star, \boldsymbol{s}_2^\star)$
Adversary
return forgery


t-NTRU-ISIS Game
$(\cdot, \boldsymbol{h}) \xleftarrow{\$} \mathsf{TpdGen}$
for $i \in \{1, \ldots, t\}$
$\boldsymbol{c}_i \xleftarrow{\$} \mathcal{R}_q$
assert
$\boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} = \boldsymbol{c}_j \mod q$
$\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq B$
Reduction / UF-CMA Game
$(sk, pk = \boldsymbol{h}) \xleftarrow{\$} \mathsf{Gen}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$\mathsf{Sgn}(m)$
$r \xleftarrow{\$} \{0,1\}^k$
$\boldsymbol{c} =$
$\mathsf{H}(\boldsymbol{h}, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$
$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$
store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$
repeat
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$
$\boldsymbol{h}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c}$
$\mathsf{Sgn}(m)$
$r, \boldsymbol{s}_2$
$m^\star, (r^\star, \boldsymbol{s}_2^\star)$
Adversary
return forgery

- Is the distribution of $\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$ for $(\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2$ close to uniform?
- What does close mean?
- Statistical distance: **No** ($\approx 2^{-35}$)
- Rényi divergence: **Yes** (actually "maybe")

$\mathsf{H}(pk, r, m)$

$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$

$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$

$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$

store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$

- Is the distribution of $\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$ for $(\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2$ close to uniform?
- What does close mean?
- Statistical distance: **No** ($\approx 2^{-35}$)
- Rényi divergence: **Yes** (actually "maybe")

$\mathsf{H}(pk, r, m)$

$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$

$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$

$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$

store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$

- Is the distribution of $\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$ for $(\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2$ close to uniform?
- What does close mean?
- Statistical distance: **No** ($\approx 2^{-35}$)
- Rényi divergence: **Yes** (actually "maybe")

$\mathsf{H}(pk, r, m)$

$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$

$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$

$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$

store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$

- Is the distribution of $\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$ for $(\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2$ close to uniform?
- What does close mean?
- Statistical distance: **No** ($\approx 2^{-35}$)
- Rényi divergence: **Yes** (actually "maybe")

$\mathsf{H}(pk, r, m)$

$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$

$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$

$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$

store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$

- Is the distribution of $\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$ for $(\boldsymbol{s}_1, \boldsymbol{s}_2) \sim \mathcal{D}^2$ close to uniform?
- What does close mean?
- Statistical distance: **No** ($\approx 2^{-35}$)
- Rényi divergence: **Yes** (actually "maybe")

$\mathsf{H}(pk, r, m)$

$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$

$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$

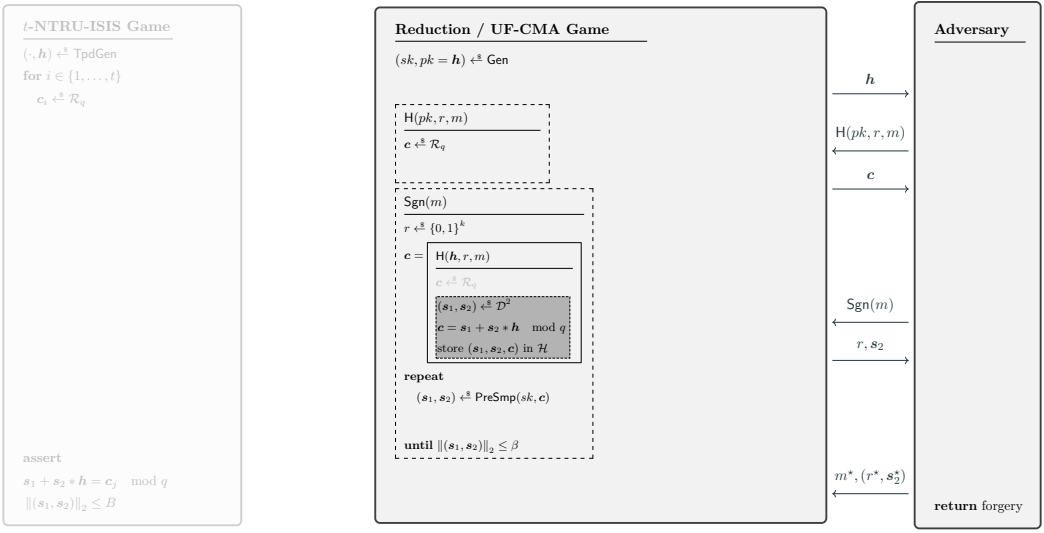
$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$

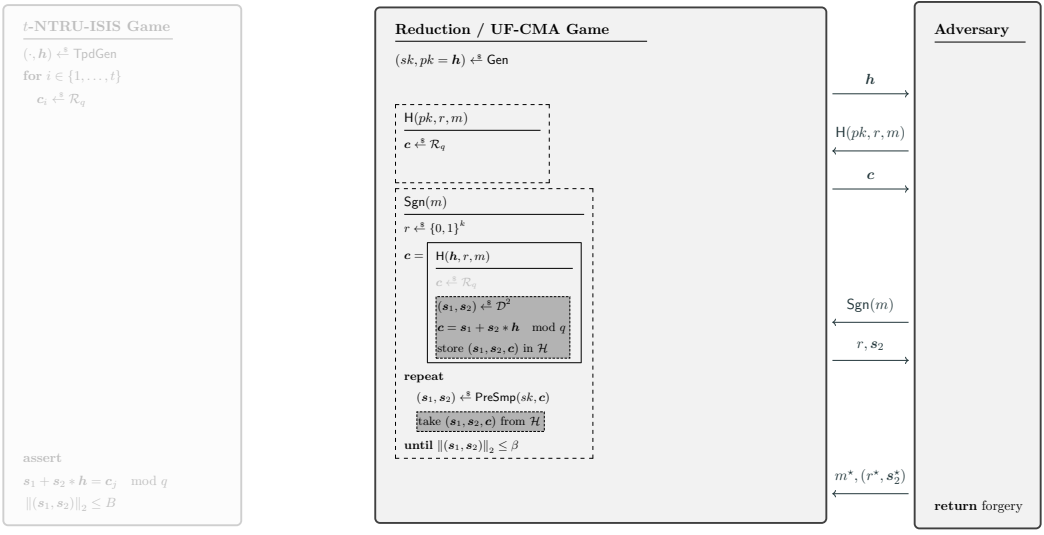
store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$

Corollary: Rényi Uniformity for NTRU

Let q be prime, $\boldsymbol{h} \in \mathcal{R}_q \setminus \{\boldsymbol{0}\}$, $a \in (1, \infty)$, $\epsilon \in (0, \frac{1}{2})$, $s \geq \eta_\epsilon(\boldsymbol{\Lambda}_{\boldsymbol{h},q})$, $\mathcal{P} = \mathcal{U}(\mathcal{R}_q)$, and $\mathcal{Q}$ the distribution of $\boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$ where $\boldsymbol{s}_1, \boldsymbol{s}_2 \sim \mathcal{D}_{\mathcal{R},s}$. Then,

$$R_a(\mathcal{P} \,||\, \mathcal{Q}) \lesssim 1 + \frac{2a\epsilon^2}{(1-\epsilon)^2}.$$


t-NTRU-ISIS Game
$(\cdot, \boldsymbol{h}) \xleftarrow{\$} \mathsf{TpdGen}$
for $i \in \{1, \ldots, t\}$
$\boldsymbol{c}_i \xleftarrow{\$} \mathcal{R}_q$
assert
$\boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} = \boldsymbol{c}_j \mod q$
$\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq B$
Reduction / UF-CMA Game
$(sk, pk = \boldsymbol{h}) \xleftarrow{\$} \mathsf{Gen}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$\mathsf{Sgn}(m)$
$r \xleftarrow{\$} \{0,1\}^k$
$\boldsymbol{c} =$
$\mathsf{H}(\boldsymbol{h}, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$
$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$
store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$
repeat
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$
$\boldsymbol{h}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c}$
$\mathsf{Sgn}(m)$
$r, \boldsymbol{s}_2$
$m^\star, (r^\star, \boldsymbol{s}_2^\star)$
Adversary
return forgery


t-NTRU-ISIS Game
$(\cdot, \boldsymbol{h}) \xleftarrow{\$} \mathsf{TpdGen}$
for $i \in \{1, \ldots, t\}$
$\boldsymbol{c}_i \xleftarrow{\$} \mathcal{R}_q$
assert
$\boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} = \boldsymbol{c}_j \mod q$
$\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq B$
Reduction / UF-CMA Game
$(sk, pk = \boldsymbol{h}) \xleftarrow{\$} \mathsf{Gen}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$\mathsf{Sgn}(m)$
$r \xleftarrow{\$} \{0,1\}^k$
$\boldsymbol{c} =$
$\mathsf{H}(\boldsymbol{h}, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$
$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$
store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$
repeat
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$
take $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ from $\mathcal{H}$
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$
$\boldsymbol{h}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c}$
$\mathsf{Sgn}(m)$
$r, \boldsymbol{s}_2$
$m^\star, (r^\star, \boldsymbol{s}_2^\star)$
Adversary
return forgery

- $(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$ must be Rényi close to conditional Gaussian [Kle00, Pre17]
- Is it short enough: $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$?
- For FALCON, probability is $\approx 1 - 2^{-14}$
- Program RO with a conditional (on being small) Gaussian? Uniformity Corollary does not apply anymore!
- Salt to the rescue! $\rightarrow$ Get new preimage by sampling new salt

$\mathsf{Sgn}(m)$

$r \xleftarrow{\$} \{0,1\}^k$

$\boldsymbol{c} = \mathsf{H}(\boldsymbol{h}, r, m)$

repeat

$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$

take $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ from $\mathcal{H}$

until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$

- $(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$ must be Rényi close to conditional Gaussian [Kle00, Pre17]
- Is it short enough: $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$?
- For FALCON, probability is $\approx 1 - 2^{-14}$
- Program RO with a conditional (on being small) Gaussian? Uniformity Corollary does not apply anymore!
- Salt to the rescue! $\rightarrow$ Get new preimage by sampling new salt

$\mathsf{Sgn}(m)$

$r \xleftarrow{\$} \{0,1\}^k$

$\boldsymbol{c} = \mathsf{H}(\boldsymbol{h}, r, m)$

repeat

$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$

take $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ from $\mathcal{H}$

until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$

- $(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$ must be Rényi close to conditional Gaussian [Kle00, Pre17]
- Is it short enough: $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$?
- For FALCON, probability is $\approx 1 - 2^{-14}$
- Program RO with a conditional (on being small) Gaussian? Uniformity Corollary does not apply anymore!
- Salt to the rescue! $\rightarrow$ Get new preimage by sampling new salt

$\mathsf{Sgn}(m)$

$r \xleftarrow{\$} \{0,1\}^k$

$\boldsymbol{c} = \mathsf{H}(\boldsymbol{h}, r, m)$

repeat

$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$

take $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ from $\mathcal{H}$

until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$

- $(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$ must be Rényi close to conditional Gaussian [Kle00, Pre17]
- Is it short enough: $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$?
- For FALCON, probability is $\approx 1 - 2^{-14}$
- Program RO with a conditional (on being small) Gaussian? Uniformity Corollary does not apply anymore!
- Salt to the rescue! $\rightarrow$ Get new preimage by sampling new salt

$\mathsf{Sgn}(m)$

$r \xleftarrow{\$} \{0,1\}^k$

$\boldsymbol{c} = \mathsf{H}(\boldsymbol{h}, r, m)$

repeat

$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$

take $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ from $\mathcal{H}$

until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$

- $(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$ must be Rényi close to conditional Gaussian [Kle00, Pre17]
- Is it short enough: $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$?
- For FALCON, probability is $\approx 1 - 2^{-14}$
- Program RO with a conditional (on being small) Gaussian? Uniformity Corollary does not apply anymore!
- Salt to the rescue! $\rightarrow$ Get new preimage by sampling new salt

$\mathsf{Sgn}(m)$

$r \xleftarrow{\$} \{0,1\}^k$

$\boldsymbol{c} = \mathsf{H}(\boldsymbol{h}, r, m)$

repeat

$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$

take $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ from $\mathcal{H}$

until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$

$\mathsf{Sgn}^+(m)$

repeat

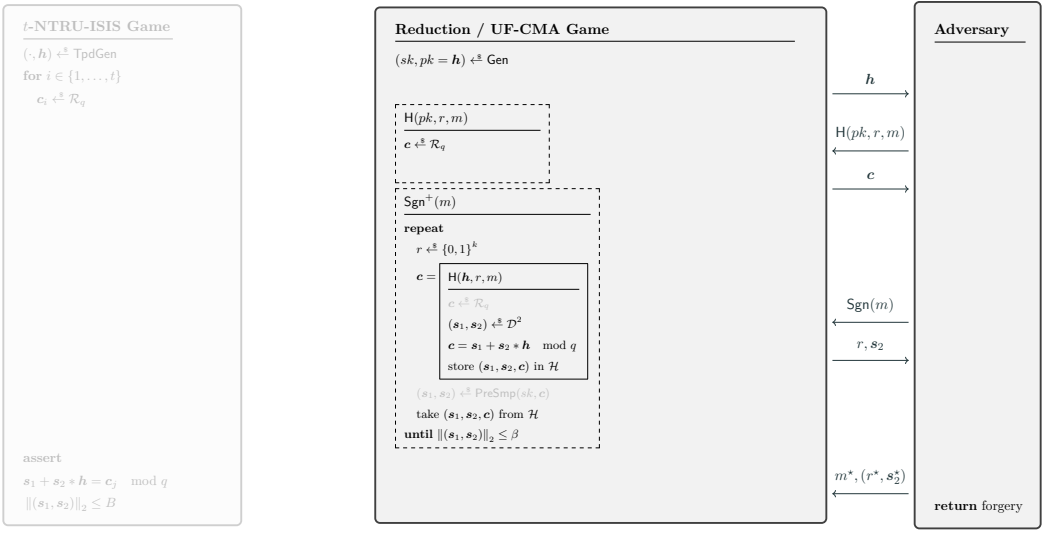
$r \xleftarrow{\$} \{0,1\}^k$

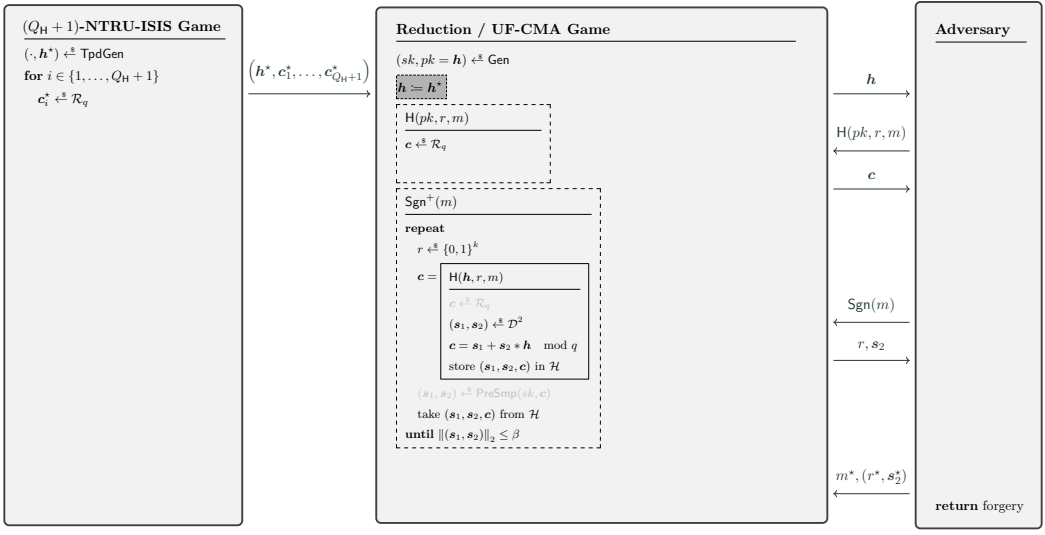
$\boldsymbol{c} = \mathsf{H}(\boldsymbol{h}, r, m)$

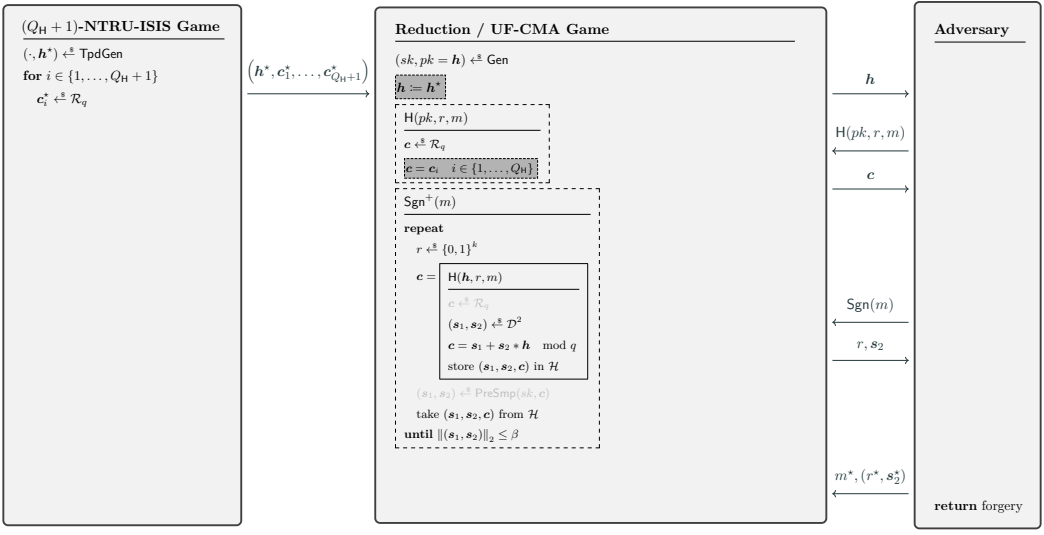
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$

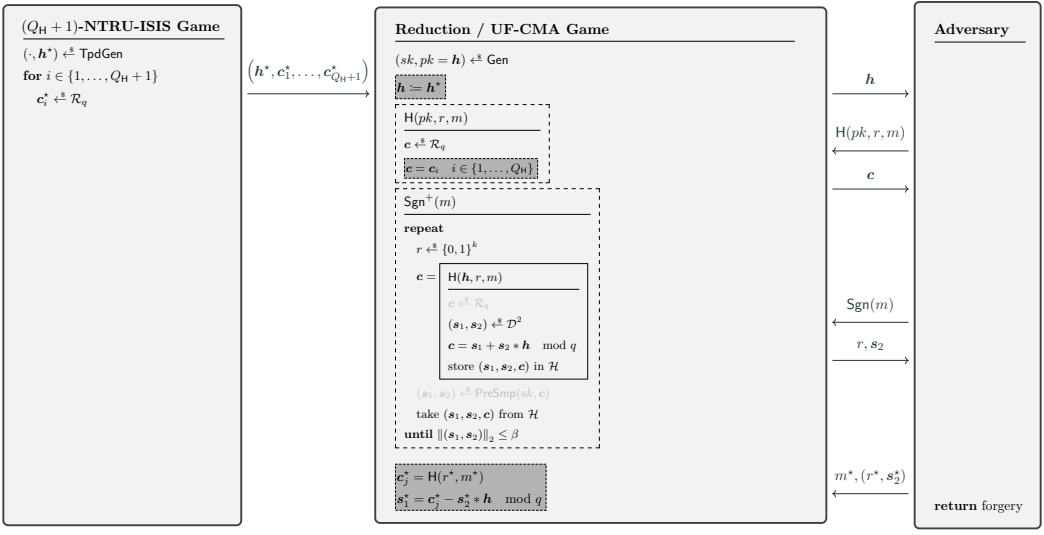
take $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ from $\mathcal{H}$

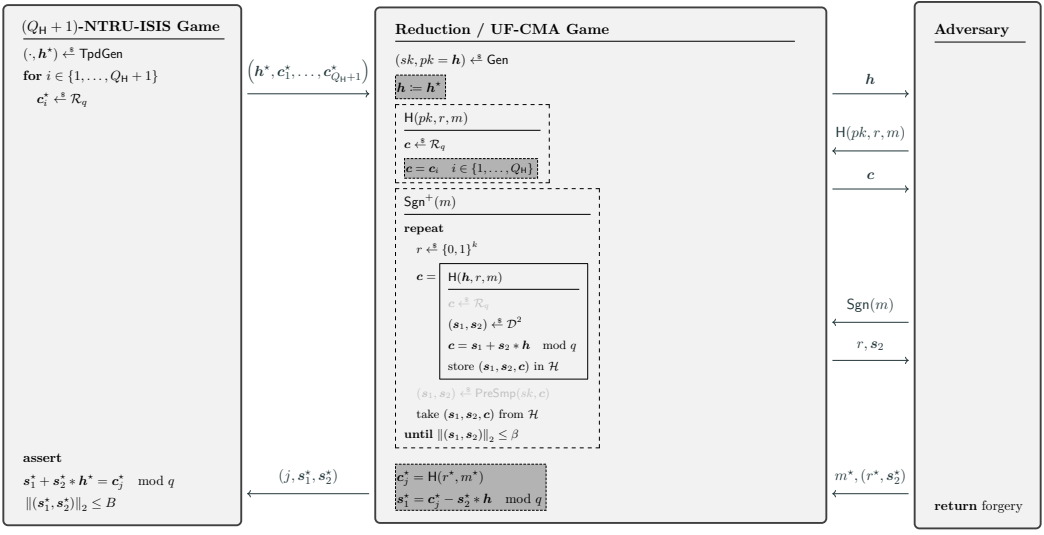
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$


t-NTRU-ISIS Game
$(\cdot, \boldsymbol{h}) \xleftarrow{\$} \mathsf{TpdGen}$
for $i \in \{1, \ldots, t\}$
$\boldsymbol{c}_i \xleftarrow{\$} \mathcal{R}_q$
assert
$\boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} = \boldsymbol{c}_j \mod q$
$\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq B$
Reduction / UF-CMA Game
$(sk, pk = \boldsymbol{h}) \xleftarrow{\$} \mathsf{Gen}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$\mathsf{Sgn}^{+}(m)$
repeat
$r \xleftarrow{\$} \{0,1\}^k$
$\boldsymbol{c} =$
$\mathsf{H}(\boldsymbol{h}, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$
$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$
store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$
$(s_1, s_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, c)$
take $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ from $\mathcal{H}$
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$
$\boldsymbol{h}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c}$
$\mathsf{Sgn}(m)$
r, s_2
$m^\star, (r^\star, \boldsymbol{s}_2^\star)$
Adversary
return forgery


$(Q_{\mathsf{H}}+1)$-NTRU-ISIS Game
$(\cdot, \boldsymbol{h}^\star) \xleftarrow{\$} \mathsf{TpdGen}$
for $i \in \{1, \ldots, Q_{\mathsf{H}}+1\}$
$\boldsymbol{c}_i^\star \xleftarrow{\$} \mathcal{R}_q$
$\left(\boldsymbol{h}^\star, \boldsymbol{c}_1^\star, \ldots, \boldsymbol{c}_{Q_{\mathsf{H}}+1}^\star\right)$
Reduction / UF-CMA Game
$(sk, pk = \boldsymbol{h}) \xleftarrow{\$} \mathsf{Gen}$
$\boldsymbol{h} := \boldsymbol{h}^\star$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$\mathsf{Sgn}^+(m)$
repeat
$r \xleftarrow{\$} \{0,1\}^k$
$\boldsymbol{c} =$
$\mathsf{H}(\boldsymbol{h}, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$
$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$
store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$
take $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ from $\mathcal{H}$
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$
$\boldsymbol{h}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c}$
$\mathsf{Sgn}(m)$
r, s_2
$m^\star, (r^\star, \boldsymbol{s}_2^\star)$
Adversary
return forgery


$(Q_{\mathsf{H}}+1)$-NTRU-ISIS Game
$(\cdot, \boldsymbol{h}^\star) \xleftarrow{\$} \mathsf{TpdGen}$
for $i \in \{1, \ldots, Q_{\mathsf{H}}+1\}$
$\boldsymbol{c}_i^\star \xleftarrow{\$} \mathcal{R}_q$
$\left(\boldsymbol{h}^\star, \boldsymbol{c}_1^\star, \ldots, \boldsymbol{c}_{Q_{\mathsf{H}}+1}^\star\right)$
Reduction / UF-CMA Game
$(sk, pk = \boldsymbol{h}) \xleftarrow{\$} \mathsf{Gen}$
$\boldsymbol{h} := \boldsymbol{h}^\star$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$\boldsymbol{c} = \boldsymbol{c}_i \quad i \in \{1, \ldots, Q_{\mathsf{H}}\}$
$\mathsf{Sgn}^+(m)$
repeat
$r \xleftarrow{\$} \{0,1\}^k$
$\boldsymbol{c} =$
$\mathsf{H}(\boldsymbol{h}, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$
$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$
store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$
take $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ from $\mathcal{H}$
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$
$\boldsymbol{h}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c}$
$\mathsf{Sgn}(m)$
r, s_2
$m^\star, (r^\star, \boldsymbol{s}_2^\star)$
Adversary
return forgery


$(Q_{\mathsf{H}}+1)$-NTRU-ISIS Game
$(\cdot, \boldsymbol{h}^\star) \xleftarrow{\$} \mathsf{TpdGen}$
for $i \in \{1, \ldots, Q_{\mathsf{H}}+1\}$
$\boldsymbol{c}_i^\star \xleftarrow{\$} \mathcal{R}_q$
$\left(\boldsymbol{h}^\star, \boldsymbol{c}_1^\star, \ldots, \boldsymbol{c}_{Q_{\mathsf{H}}+1}^\star\right)$
Reduction / UF-CMA Game
$(sk, pk = \boldsymbol{h}) \xleftarrow{\$} \mathsf{Gen}$
$\boldsymbol{h} := \boldsymbol{h}^\star$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$\boldsymbol{c} = \boldsymbol{c}_i \quad i \in \{1, \ldots, Q_{\mathsf{H}}\}$
$\mathsf{Sgn}^+(m)$
repeat
$r \xleftarrow{\$} \{0,1\}^k$
$\boldsymbol{c} =$
$\mathsf{H}(\boldsymbol{h}, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$
$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$
store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$
take $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ from $\mathcal{H}$
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$
$\boldsymbol{c}_j^\star = \mathsf{H}(r^\star, m^\star)$
$\boldsymbol{s}_1^\star = \boldsymbol{c}_j^\star - \boldsymbol{s}_2^\star * \boldsymbol{h} \mod q$
$\boldsymbol{h}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c}$
$\mathsf{Sgn}(m)$
r, s_2
$m^\star, (r^\star, \boldsymbol{s}_2^\star)$
Adversary
return forgery


$(Q_{\mathsf{H}}+1)$-NTRU-ISIS Game
$(\cdot, \boldsymbol{h}^\star) \xleftarrow{\$} \mathsf{TpdGen}$
for $i \in \{1, \ldots, Q_{\mathsf{H}}+1\}$
$\boldsymbol{c}_i^\star \xleftarrow{\$} \mathcal{R}_q$
assert
$\boldsymbol{s}_1^\star + \boldsymbol{s}_2^\star * \boldsymbol{h}^\star = \boldsymbol{c}_j^\star \mod q$
$\|(\boldsymbol{s}_1^\star, \boldsymbol{s}_2^\star)\|_2 \leq B$
$\left(\boldsymbol{h}^\star, \boldsymbol{c}_1^\star, \ldots, \boldsymbol{c}_{Q_{\mathsf{H}}+1}^\star\right)$
$(j, \boldsymbol{s}_1^\star, \boldsymbol{s}_2^\star)$
Reduction / UF-CMA Game
$(sk, pk = \boldsymbol{h}) \xleftarrow{\$} \mathsf{Gen}$
$\boldsymbol{h} := \boldsymbol{h}^\star$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$\boldsymbol{c} = \boldsymbol{c}_i \quad i \in \{1, \ldots, Q_{\mathsf{H}}\}$
$\mathsf{Sgn}^+(m)$
repeat
$r \xleftarrow{\$} \{0,1\}^k$
$\boldsymbol{c} =$
$\mathsf{H}(\boldsymbol{h}, r, m)$
$\boldsymbol{c} \xleftarrow{\$} \mathcal{R}_q$
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathcal{D}^2$
$\boldsymbol{c} = \boldsymbol{s}_1 + \boldsymbol{s}_2 * \boldsymbol{h} \mod q$
store $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ in $\mathcal{H}$
$(\boldsymbol{s}_1, \boldsymbol{s}_2) \xleftarrow{\$} \mathsf{PreSmp}(sk, \boldsymbol{c})$
take $(\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{c})$ from $\mathcal{H}$
until $\|(\boldsymbol{s}_1, \boldsymbol{s}_2)\|_2 \leq \beta$
$\boldsymbol{c}_j^\star = \mathsf{H}(r^\star, m^\star)$
$\boldsymbol{s}_1^\star = \boldsymbol{c}_j^\star - \boldsymbol{s}_2^\star * \boldsymbol{h} \mod q$
Adversary
$\boldsymbol{h}$
$\mathsf{H}(pk, r, m)$
$\boldsymbol{c}$
$\mathsf{Sgn}(m)$
r, s_2
$m^\star, (r^\star, \boldsymbol{s}_2^\star)$
return forgery

Assumption

Property of $f_{\boldsymbol{A}}$

Security Notion

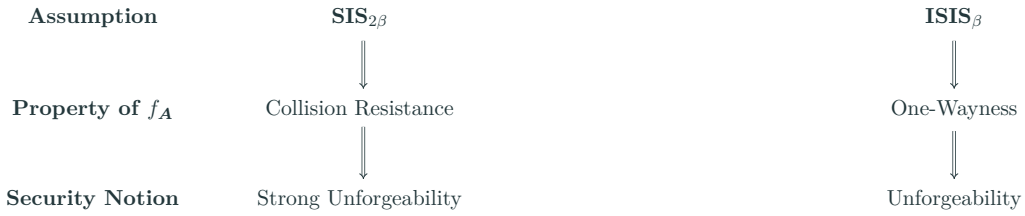
ISIS$_\beta$

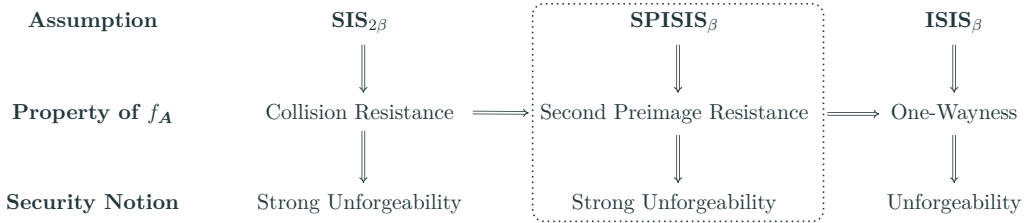
$\Downarrow$

One-Wayness

$\Downarrow$

Unforgeability


Assumption
SIS$_{2\beta}$
ISIS$_{\beta}$
Property of $f_{\boldsymbol{A}}$
Collision Resistance
One-Wayness
Security Notion
Strong Unforgeability
Unforgeability


Assumption
SIS$_{2\beta}$
SPISIS$_{\beta}$
ISIS$_{\beta}$
Property of $f_{\boldsymbol{A}}$
Collision Resistance
Second Preimage Resistance
One-Wayness
Security Notion
Strong Unforgeability
Strong Unforgeability
Unforgeability

SECURITY BOUNDS

Q_s	Maximum Signing Queries
Q_{H}	Maximum Random Oracle Queries
r_u	Rényi Loss Uniformity
r_p	Rényi Loss Preimage Sampler

$$\mathrm{Adv}^{\textbf{UF-CMA}} \leq r_u^{Q_s} \cdot r_p^{Q_s} \cdot \mathrm{Adv}^{\mathsf{Q_H}\text{-}\mathcal{R}\text{-}\textbf{ISIS}}_{B=\beta} + \ldots$$

Q_s	Maximum Signing Queries
Q_{H}	Maximum Random Oracle Queries
r_u	Rényi Loss Uniformity
r_p	Rényi Loss Preimage Sampler

$$\mathrm{Adv}^{\textbf{UF-CMA}} \leq r_u^{Q_s} \cdot r_p^{Q_s} \cdot \mathrm{Adv}^{\mathsf{Q_H}\text{-}\mathcal{R}\text{-}\textbf{ISIS}}_{B=\beta} + \ldots$$

$$\mathrm{Adv}^{\textbf{SUF-CMA}} \leq \mathrm{Adv}^{\textbf{UF-CMA}} + r_p^{Q_s} \cdot \left(\mathrm{Adv}^{Q_s\text{-}\mathcal{R}\text{-}\textbf{SPISIS}}_{B=\beta} + \ldots\right) + \ldots$$

OLD SECURITY BOUND: STRONG UNFORGEABILITY

Q_s	Maximum Signing Queries
Q_{H}	Maximum Random Oracle Queries
r_u	Rényi Loss Uniformity
r_p	Rényi Loss Preimage Sampler

$$\mathrm{Adv}^{\textbf{SUF-CMA}} \leq r_u^{Q_{\mathsf{H}}} \cdot r_p^{Q_s} \cdot \mathrm{Adv}^{\mathcal{R}\textbf{-SIS}}_{B=2\beta} + \ldots$$

- Rényi arguments rely on ϵ (error of smoothing parameter η_ϵ), with $\epsilon = 1/\sqrt{Q_s \cdot \lambda}$ and $Q_s = 2^{64}$
- $\implies$ Loss stays small for $\approx Q_s$ queries, but $r_u^{Q_{\mathsf{H}}}$ explodes for $Q_{\mathsf{H}} = 2^{96}$
- Can be solved using proof technique from [BRTZ24], but results in a significant tightness loss
- More problematic: The **SIS** bound is large. For Falcon-512, it provides only 95 bits, and for Falcon-1024, it becomes trivial since $2\beta = 16765 > 12289 = q$.

Q_s	Maximum Signing Queries
Q_{H}	Maximum Random Oracle Queries
r_u	Rényi Loss Uniformity
r_p	Rényi Loss Preimage Sampler

$$\mathrm{Adv}^{\textbf{SUF-CMA}} \leq r_u^{Q_{\mathsf{H}}} \cdot r_p^{Q_s} \cdot \mathrm{Adv}^{\mathcal{R}\textbf{-SIS}}_{B=2\beta} + \ldots$$

- Rényi arguments rely on ϵ (error of smoothing parameter η_ϵ), with $\epsilon = 1/\sqrt{Q_s \cdot \lambda}$ and $Q_s = 2^{64}$
- $\implies$ Loss stays small for $\approx Q_s$ queries, but $r_u^{Q_{\mathsf{H}}}$ explodes for $Q_{\mathsf{H}} = 2^{96}$
- Can be solved using proof technique from [BRTZ24], but results in a significant tightness loss
- More problematic: The **SIS** bound is large. For Falcon-512, it provides only 95 bits, and for Falcon-1024, it becomes trivial since $2\beta = 16765 > 12289 = q$.

Q_s	Maximum Signing Queries
Q_{H}	Maximum Random Oracle Queries
r_u	Rényi Loss Uniformity
r_p	Rényi Loss Preimage Sampler

$$\mathrm{Adv}^{\textbf{SUF-CMA}} \leq r_u^{Q_{\mathsf{H}}} \cdot r_p^{Q_s} \cdot \mathrm{Adv}^{\mathcal{R}\text{-}\textbf{SIS}}_{B=2\beta} + \ldots$$

- Rényi arguments rely on ϵ (error of smoothing parameter η_ϵ), with $\epsilon = 1/\sqrt{Q_s \cdot \lambda}$ and $Q_s = 2^{64}$
- $\implies$ Loss stays small for $\approx Q_s$ queries, but $r_u^{Q_{\mathsf{H}}}$ explodes for $Q_{\mathsf{H}} = 2^{96}$
- Can be solved using proof technique from [BRTZ24], but results in a significant tightness loss
- More problematic: The **SIS** bound is large. For Falcon-512, it provides only 95 bits, and for Falcon-1024, it becomes trivial since $2\beta = 16765 > 12289 = q$.

Q_s	Maximum Signing Queries
Q_{H}	Maximum Random Oracle Queries
r_u	Rényi Loss Uniformity
r_p	Rényi Loss Preimage Sampler

$$\mathrm{Adv}^{\textbf{SUF-CMA}} \leq r_u^{Q_{\mathsf{H}}} \cdot r_p^{Q_s} \cdot \mathrm{Adv}^{\mathcal{R}\textbf{-SIS}}_{B=2\beta} + \ldots$$

- Rényi arguments rely on ϵ (error of smoothing parameter η_ϵ), with $\epsilon = 1/\sqrt{Q_s \cdot \lambda}$ and $Q_s = 2^{64}$
- $\implies$ Loss stays small for $\approx Q_s$ queries, but $r_u^{Q_{\mathsf{H}}}$ explodes for $Q_{\mathsf{H}} = 2^{96}$
- Can be solved using proof technique from [BRTZ24], but results in a significant tightness loss
- More problematic: The **SIS** bound is large. For Falcon-512, it provides only 95 bits, and for Falcon-1024, it becomes trivial since $2\beta = 16765 > 12289 = q$.

Q_s	Maximum Signing Queries
Q_{H}	Maximum Random Oracle Queries
r_u	Rényi Loss Uniformity
r_p	Rényi Loss Preimage Sampler

$$\mathrm{Adv}^{\textbf{SUF-CMA}} \leq r_u^{Q_{\mathsf{H}}} \cdot r_p^{Q_s} \cdot \mathrm{Adv}^{\mathcal{R}\textbf{-SIS}}_{B=2\beta} + \ldots$$

- Rényi arguments rely on ϵ (error of smoothing parameter η_ϵ), with $\epsilon = 1/\sqrt{Q_s \cdot \lambda}$ and $Q_s = 2^{64}$
- $\implies$ Loss stays small for $\approx Q_s$ queries, but $r_u^{Q_{\mathsf{H}}}$ explodes for $Q_{\mathsf{H}} = 2^{96}$
- Can be solved using proof technique from [BRTZ24], but results in a significant tightness loss
- More problematic: The **SIS** bound is large. For Falcon-512, it provides only 95 bits, and for Falcon-1024, it becomes trivial since $2\beta = 16765 > 12289 = q$.

- Need $C_s > Q_s$ queries needed due to repetition:

- Rényi arguments are very sensitive
- Decreasing maximum signing queries can compensate it

- Need $C_s > Q_s$ queries needed due to repetition:

$$\mathrm{Adv}^{\textbf{UF-CMA}} \leq r_u^{C_s} \cdot r_p^{C_s} \cdot \mathrm{Adv}^{\mathsf{Q_H}\text{-}\mathcal{R}\text{-}\textbf{ISIS}}_{B=\beta} + \dots$$

- Rényi arguments are very sensitive
- Decreasing maximum signing queries can compensate it

- Need $C_s > Q_s$ queries needed due to repetition:

$$\mathrm{Adv}^{\textbf{UF-CMA}} \leq r_u^{C_s} \cdot r_p^{C_s} \cdot \mathrm{Adv}^{\mathsf{Q_H}\text{-}\mathcal{R}\text{-}\textbf{ISIS}}_{B=\beta} + \dots$$

- Rényi arguments are very sensitive
- Decreasing maximum signing queries can compensate it

- Need $C_s > Q_s$ queries needed due to repetition:

$$\mathrm{Adv}^{\textbf{UF-CMA}} \leq r_u^{C_s} \cdot r_p^{C_s} \cdot \mathrm{Adv}^{\mathsf{Q_H}\text{-}\mathcal{R}\text{-}\textbf{ISIS}}_{B=\beta} + \dots$$

- Rényi arguments are very sensitive
- Decreasing maximum signing queries can compensate it

- Optimise Rényi order a_p, a_u for Rényi terms r_p, r_u

Parameters	UF-CMA (Thm. 1)		
	FALCON$^+$-512		FALCON$^+$-1024
Bit security (core-SVP), t-$\mathcal{R}$-**ISIS**$_{q=q,\alpha=1.17,B=\beta}$	120		
Max Signing queries Q_s	2^{64}		
Max repetitions C_s	$2^{64} + 2^{50}$		
Rényi Order a_p	72.96		
Rényi Order a_u	71.73		
Bits lost from Rényi a_p	3.5		
Bits lost from Rényi a_u	3.5		
Final bit security	**113**		

- There might be better attacks against multi-target **ISIS** [2]
- Similar for **SUF-CMA**, as **UF-CMA** term dominates

[2] The * symbol at 270 bits refers to the bit security of the computational term.

- Optimise Rényi order a_p, a_u for Rényi terms r_p, r_u

Parameters	**UF-CMA** (Thm. 1)	
	FALCON$^+$-512	FALCON$^+$-1024
Bit security (core-SVP), t-$\mathcal{R}$-**ISIS**$_{q=q,\alpha=1.17,B=\beta}$	120	
Max Signing queries Q_s	2^{64}	
Max repetitions C_s	$2^{64} + 2^{50}$	
Rényi Order a_p	72.96	
Rényi Order a_u	71.73	
Bits lost from Rényi a_p	3.5	
Bits lost from Rényi a_u	3.5	
Final bit security	**113**	

- There might be better attacks against multi-target **ISIS** [2]
- Similar for **SUF-CMA**, as **UF-CMA** term dominates

[2] The * symbol at 270 bits refers to the bit security of the computational term.

- Optimise Rényi order a_p, a_u for Rényi terms r_p, r_u

Parameters	**UF-CMA** (Thm. 1)		
	Falcon$^+$-512		Falcon$^+$-1024
Bit security (core-SVP), t-$\mathcal{R}$-**ISIS**$_{q=q,\alpha=1.17,B=\beta}$	120		
Max Signing queries Q_s	2^{64}	2^{58}	
Max repetitions C_s	$2^{64}+2^{50}$	$2^{58}+2^{44}$	
Rényi Order a_p	72.96	583.67	
Rényi Order a_u	71.73	582.46	
Bits lost from Rényi a_p	3.5	0.5	
Bits lost from Rényi a_u	3.5	0.5	
Final bit security	**113**	**119**	

- There might be better attacks against multi-target **ISIS** [2]
- Similar for **SUF-CMA**, as **UF-CMA** term dominates

[2] The * symbol at 270 bits refers to the bit security of the computational term.

- Optimise Rényi order a_p, a_u for Rényi terms r_p, r_u

Parameters	**UF-CMA** (Thm. 1)		
	Falcon$^+$-512		Falcon$^+$-1024
Bit security (core-SVP), t-$\mathcal{R}$-**ISIS**$_{q=q,\alpha=1.17,B=\beta}$	120		278
Max Signing queries Q_s	2^{64}	2^{58}	2^{64}
Max repetitions C_s	$2^{64}+2^{50}$	$2^{58}+2^{44}$	$2^{64}+2^{36}$
Rényi Order a_p	72.96	583.67	157.05
Rényi Order a_u	71.73	582.46	155.92
Bits lost from Rényi a_p	3.5	0.5	4
Bits lost from Rényi a_u	3.5	0.5	4
Final bit security	**113**	**119**	**256 (270)***

- There might be better attacks against multi-target **ISIS** [2]
- Similar for **SUF-CMA**, as **UF-CMA** term dominates

[2] The * symbol at 270 bits refers to the bit security of the computational term.

- Optimise Rényi order a_p, a_u for Rényi terms r_p, r_u

Parameters	**UF-CMA** (Thm. 1)		
	Falcon$^+$-512		Falcon$^+$-1024
Bit security (core-SVP), t-$\mathcal{R}$-**ISIS**$_{q=q,\alpha=1.17,B=\beta}$	120		278
Max Signing queries Q_s	2^{64}	2^{58}	2^{64}
Max repetitions C_s	$2^{64}+2^{50}$	$2^{58}+2^{44}$	$2^{64}+2^{36}$
Rényi Order a_p	72.96	583.67	157.05
Rényi Order a_u	71.73	582.46	155.92
Bits lost from Rényi a_p	3.5	0.5	4
Bits lost from Rényi a_u	3.5	0.5	4
Final bit security	**113**	**119**	**256 (270)***

- There might be better attacks against multi-target **ISIS** [2]
- Similar for **SUF-CMA**, as **UF-CMA** term dominates

[2] The * symbol at 270 bits refers to the bit security of the computational term.

- Optimise Rényi order a_p, a_u for Rényi terms r_p, r_u

Parameters	**UF-CMA** (Thm. 1)		
	Falcon$^+$-512		Falcon$^+$-1024
Bit security (core-SVP), t-$\mathcal{R}$-**ISIS**$_{q=q,\alpha=1.17,B=\beta}$	120		278
Max Signing queries Q_s	2^{64}	2^{58}	2^{64}
Max repetitions C_s	$2^{64}+2^{50}$	$2^{58}+2^{44}$	$2^{64}+2^{36}$
Rényi Order a_p	72.96	583.67	157.05
Rényi Order a_u	71.73	582.46	155.92
Bits lost from Rényi a_p	3.5	0.5	4
Bits lost from Rényi a_u	3.5	0.5	4
Final bit security	**113**	**119**	**256 (270)***

- There might be better attacks against multi-target **ISIS** [2]
- Similar for **SUF-CMA**, as **UF-CMA** term dominates

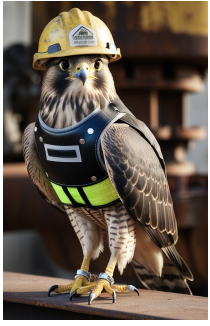
[2] The * symbol at 270 bits refers to the bit security of the computational term.

- QROM proof
- Cryptanalysis of t-$\mathcal{R}$-**ISIS** and t-$\mathcal{R}$-**SPISIS** problems

- QROM proof
- Cryptanalysis of t-$\mathcal{R}$-**ISIS** and t-$\mathcal{R}$-**SPISIS** problems

SUMMARY

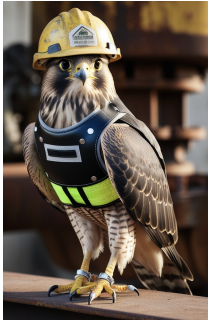
- Minor, conservative modification allows for the *first concrete proof* of FALCON
- Adaptation of [GPV08] to work with Rényi divergence
- Optimisation of the security bound and concrete bit security (for FFO sampler)



ia.cr/2024/1769

phillip.gajland@ibm.com

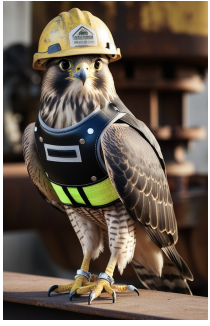
- Minor, conservative modification allows for the *first concrete proof* of FALCON
- Adaptation of [GPV08] to work with Rényi divergence
- Optimisation of the security bound and concrete bit security (for FFO sampler)



ia.cr/2024/1769

phillip.gajland@ibm.com

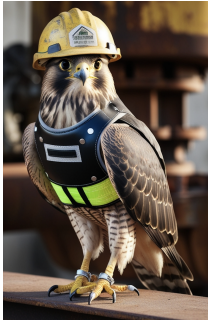
- Minor, conservative modification allows for the *first concrete proof* of FALCON
- Adaptation of [GPV08] to work with Rényi divergence
- Optimisation of the security bound and concrete bit security (for FFO sampler)



ia.cr/2024/1769

phillip.gajland@ibm.com

- Minor, conservative modification allows for the *first concrete proof* of FALCON
- Adaptation of [GPV08] to work with Rényi divergence
- Optimisation of the security bound and concrete bit security (for FFO sampler)



ia.cr/2024/1769

phillip.gajland@ibm.com

REFERENCES I

[BLL+15] Shi Bai, Adeline Langlois, Tancrède Lepoint, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 3–24, Auckland, New Zealand, November 30 – December 3, 2015. Springer, Berlin, Heidelberg, Germany. (Cited on slide 9.)

[BRTZ24] Mihir Bellare, Doreen Riepel, Stefano Tessaro, and Yizhao Zhang. Count Corruptions, Not Users: Improved Tightness for Signatures, Encryption and Authenticated Key Exchange. In *ASIACRYPT 2024*, LNCS. Springer, Heidelberg, 2024. (Cited on slide 21.)

[GMA+25] Philippe Gaborit, Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Edoardo Persichetti, Gilles Zémor, Jurjen Bos, Arnaud Dion, Jerome Lacan, Jean-Marc Robert, Pascal Veron, Paulo Barreto, Shay Gueron, Tim Guneysu, Rafael Misoczki, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur, Santosh Ghosh, and Jan Richter-Brokmann. HQC. Technical report, National Institute of Standards and Technology, available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms, 2025. (Cited on slide 4.)

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th Annual ACM Symposium on Theory of Computing*, pages 197–206, Victoria, BC, Canada, May 17–20, 2008. ACM Press. (Cited on slide 6, 7, 7, 7, 1, 1, 1, 1, 1, 1, 1, and 26.)

[HBD+22] Andreas Hülsing, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Jean-Philippe Aumasson, Bas Westerbaan, and Ward Beullens. SPHINCS+. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. (Cited on slide 4.)

REFERENCES II

[Kle00] Philip N. Klein. Finding the closest lattice vector when it's unusually close. In David B. Shmoys, editor, *11th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 937–941, San Francisco, CA, USA, January 9–11, 2000. ACM-SIAM. (Cited on slide 16, 16, 16, 16, and 16.)

[LDK+22] Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé, and Shi Bai. CRYSTALS-DILITHIUM. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. (Cited on slide 4.)

[LSS14] Adeline Langlois, Damien Stehlé, and Ron Steinfeld. GGHLite: More efficient multilinear maps from ideal lattices. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 239–256, Copenhagen, Denmark, May 11–15, 2014. Springer, Berlin, Heidelberg, Germany. (Cited on slide 9.)

[MP24] Michele Mosca and Marco Piani. Quantum threat timeline report 2024. Technical report, Global Risk Institute, December 2024. (Cited on slide (document).)

[PFH+22] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. (Cited on slide 4.)

[Pre17] Thomas Prest. Sharper bounds in lattice-based cryptography using the Rényi divergence. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 347–374, Hong Kong, China, December 3–7, 2017. Springer, Cham, Switzerland. (Cited on slide 9, 16, 16, 16, 16, and 16.)

[Rén61] Alfréd Rényi. On measures of entropy and information. Proc. 4th Berkeley Symp. Math. Stat. Probab. 1, 547-561 (1961)., 1961. (Cited on slide 1.)

REFERENCES III

[SAB+22] Peter Schwabe, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehlé, and Jintai Ding. CRYSTALS-KYBER. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. (Cited on slide 4.)