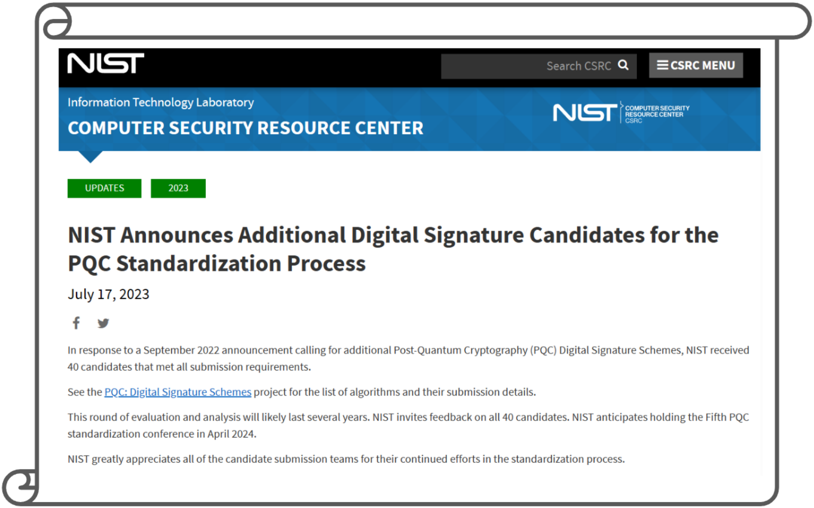
On the Quantum Security of HAWK

Serge Fehr[1,2] **Yu-Hsuan Huang**[1]

[1]Centrum Wiskunde & Informatica, The Netherlands

[2]Leiden University, The Netherlands

Background



NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

UPDATES 2023

NIST Announces Additional Digital Signature Candidates for the PQC Standardization Process

July 17, 2023

In response to a September 2022 announcement calling for additional Post-Quantum Cryptography (PQC) Digital Signature Schemes, NIST received 40 candidates that met all submission requirements.

See the PQC: Digital Signature Schemes project for the list of algorithms and their submission details.

This round of evaluation and analysis will likely last several years. NIST invites feedback on all 40 candidates. NIST anticipates holding the Fifth PQC standardization conference in April 2024.

NIST greatly appreciates all of the candidate submission teams for their continued efforts in the standardization process.

Figure: NIST Additional PQ Signature Competition

HAWK

A post-quantum signature using **probabilisitic hash and sign** based on the **Lattice Isomorphism Problem (LIP)**

HAWK

A post-quantum signature using **probabilisitic hash and sign** based on the **Lattice Isomorphism Problem (LIP)**

History of HAWK:

- LIP framework [DvW22]

On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography

Léo Ducas[1,2] and Wessel van Woerden[1]

[1] CWI, Cryptology Group, Amsterdam, The Netherlands
[2] Leiden University, Mathematical Institute, Leiden, The Netherlands

HAWK

A post-quantum signature using **probabilisitic hash and sign** based on the **Lattice Isomorphism Problem (LIP)**

History of HAWK:

- LIP framework [DvW22]
- HAWK [DPPvW22]

HAWK: Module LIP makes Lattice Signatures Fast, Compact and Simple

Léo Ducas[1,2], Eamonn W. Postlethwaite[1], Ludo N. Pulles[1], Wessel van Woerden[1]

[1] CWI, Cryptology Group, Amsterdam, the Netherlands
[2] Mathematical Institute, Leiden University, Leiden, The Netherlands
{ewp,lnp}@cwi.nl

HAWK

A post-quantum signature using **probabilisitic hash and sign** based on the **Lattice Isomorphism Problem (LIP)**

History of HAWK:

- LIP framework [DvW22]
- HAWK [DPPvW22]
- submitted to NIST

PQ Signatures Zoo Schemes Parameters Performance Wide screen version

Scheme	Status	Category
Dilithium	To be standardized	Lattices
EHTv3 / EHTv4 ⚠	On-ramp	Lattices
EagleSign ⚠	On-ramp	Lattices
Falcon	To be standardized	Lattices
HAETAE	On-ramp	Lattices
HAWK	On-ramp	Lattices
HuFu	On-ramp	Lattices
Raccoon	On-ramp	Lattices

HAWK

A post-quantum signature using **probabilisitic hash and sign** based on the **Lattice Isomorphism Problem (LIP)**

History of HAWK:

- LIP framework [DvW22]
- HAWK [DPPvW22]
- submitted to NIST

Advantage:

- Discrete Gaussian sampling (DGS) on simple lattice

HAWK

A post-quantum signature using **probabilisitic hash and sign** based on the **Lattice Isomorphism Problem (LIP)**

History of HAWK:

- LIP framework [DvW22]
- HAWK [DPPvW22]
- submitted to NIST

Advantage:

- Discrete Gaussian sampling (DGS) on simple lattice
- fastest signing

Scheme	Parameterset	NIST level	Sign (cycles)	Verify (cycles)
HAWK	512	1	85,372	148,224
UOV	Ip-pkc	1	105,324	224,006
UOV	Ip-classic	1	105,324	90,336
UOV	Is-pkc	1	109,314	276,520
UOV	Is-classic	1	109,314	58,274
HAWK	1024	5	180,816	302,861
TUOV	Ip	1	220,792	491,120
TUOV	Is	1	272,394	570,194
UOV	III-pkc	3	299,316	917,402
UOV	III-classic	3	299,316	241,588
Dilithium	II	2	333,013	118,412

HAWK

A post-quantum signature using **probabilisitic hash and sign** based on the **Lattice Isomorphism Problem (LIP)**

History of HAWK:

- LIP framework [DvW22]
- HAWK [DPPvW22]
- submitted to NIST

Advantage:

- Discrete Gaussian sampling (DGS) on simple lattice
- fastest signing
- floating point free

Overview

- Background
- Security of HAWK
- More Details

Security of HAWK

Key recovery: lattice isomorphism problem

Security of HAWK

Key recovery: lattice isomorphism problem
What about unforgeability (EU-CMA)?

Security of HAWK

Key recovery: lattice isomorphism problem
What about unforgeability (EU-CMA)?

HAWK follows a non-standard variant of hash-and-sign:

- no "off-the-shelf" theorem to apply
- previous generic analyses do not apply

Security of HAWK

Key recovery: lattice isomorphism problem
What about unforgeability (EU-CMA)?

HAWK follows a non-standard variant of hash-and-sign:

- no "off-the-shelf" theorem to apply
- previous generic analyses do not apply

[DPPvW22]: Classical security in ROM $\geq$ one-more SVP

- does not carry over to the quantum setting

Security of HAWK

Key recovery: lattice isomorphism problem
What about unforgeability (EU-CMA)?

HAWK follows a non-standard variant of hash-and-sign:

- no "off-the-shelf" theorem to apply
- previous generic analyses do not apply

[DPPvW22]: Classical security in ROM $\geq$ one-more SVP

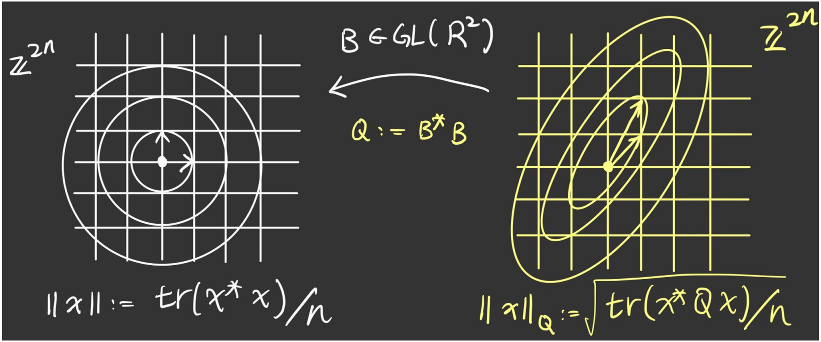
- does not carry over to the quantum setting

This work: Quantum security in QROM $\geq$ one-more SVP

- modular proof, accessible to non-quantum-experts
- replacing "quantum module" gives a classical proof

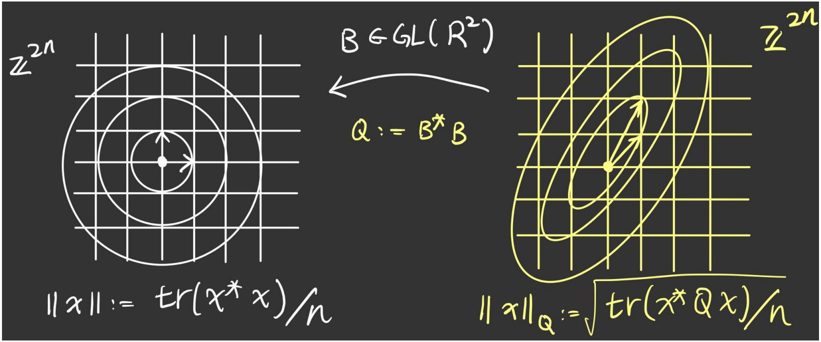
One-more SVP (omSVP)

DGS on $\mathbb{Z}^{2n} \cong \mathcal{R}^2$ in $\|x\| := \sqrt{\mathrm{tr}(x^* x)/n}$ is easy



One-more SVP (omSVP)

DGS on $\mathbb{Z}^{2n} \cong \mathcal{R}^2$ in $\|x\| := \sqrt{\mathrm{tr}(x^* x)/n}$ is easy

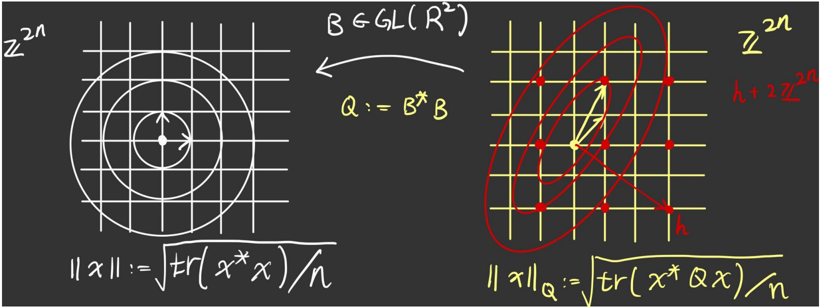


For $B \in \mathrm{GL}(\mathcal{R}^2)$ and $Q := B^* B$

- Given B: DGS in $\|x\|_Q := \sqrt{\mathrm{tr}(x^* Q x)/n}$ is (very) easy
- Given Q but not B: (believed) hard to find x with small $\|x\|_Q > 0$, even given Discrete Gaussian samples in $\|x\|_Q$ (one-more SVP)

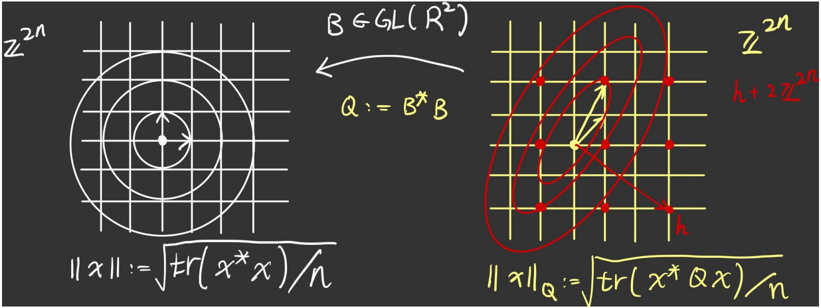
(Over simplified) HAWK

$\tilde{D}_B\,[\,h\,]$: discrete Gaussian on $h + 2\mathbb{Z}^{2n}$ in $\|x\|_Q := \mathrm{tr}(x^* x)/n$



(Over simplified) HAWK

$\tilde{D}_B\,[\,h\,]$: discrete Gaussian on $h + 2\mathbb{Z}^{2n}$ in $\|x\|_Q := \mathrm{tr}(x^* x)/n$



$Sign_B(m)$:

$r \leftarrow \{0,1\}^{\text{saltlen}}$

$h := H(m, r)$

$v \leftarrow \tilde{D}_B\,[\,h\,]$

$s := \frac{1}{2}(h + v)$

return $sig := (r, s)$

$Vrfy_Q(m, (r, s))$:

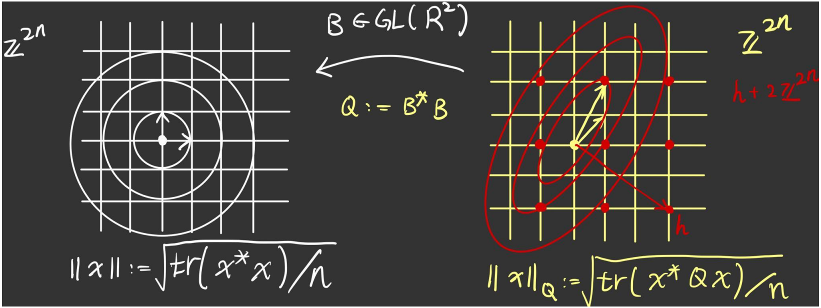
$v := 2s - H(m, r)$

check $s \in \mathbb{Z}^{2n}$

check $\|v\|_Q > 0$ is small

(Over simplified) HAWK

$\tilde{D}_B[h]$: discrete Gaussian on $h + 2\mathbb{Z}^{2n}$ in $\|x\|_Q := \mathrm{tr}(x^* x)/n$



$Sign_B(m)$:

$r \leftarrow \{0,1\}^{\text{saltlen}}$
$h := H(m, r)$
$v \leftarrow \widetilde{D}_B[h]$
$s := \frac{1}{2}(h + v)$
return $sig := (r, s)$

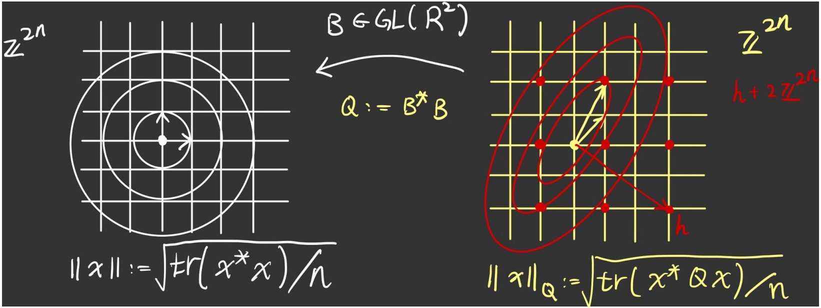
$Vrfy_Q(m, (r, s))$:

$v := 2s - H(m, r)$
check $s \in \mathbb{Z}^{2n}$
check $\|v\|_Q > 0$ is small

If $Vrfy_Q(m, sig) = 1$ then $\|v\|_Q > 0$ is already small.

(Over simplified) HAWK

$\tilde{D}_B[h]$: discrete Gaussian on $h + 2\mathbb{Z}^{2n}$ in $\|x\|_Q := \mathrm{tr}(x^* x)/n$



$Sign_B(m)$:

$r \leftarrow \{0,1\}^{\text{saltlen}}$
$h := H(m, r)$
$v \leftarrow \widetilde{D}_B[h]$
$s := \frac{1}{2}(h + v)$
return $sig := (r, s)$

$Vrfy_Q(m, (r, s))$:

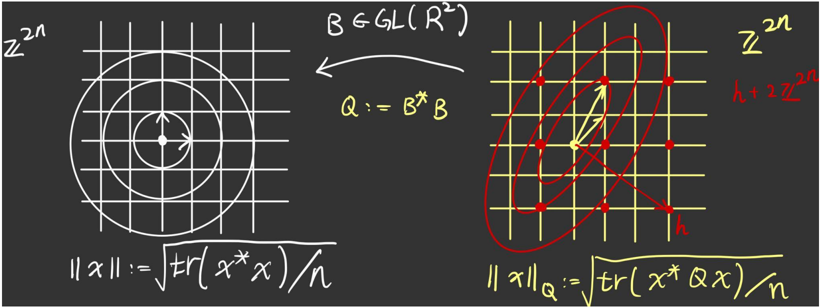
$v := 2s - H(m, r)$
check $s \in \mathbb{Z}^{2n}$
check $\|v\|_Q > 0$ is small

If $Vrfy_Q(m, sig) = 1$ then $\|v\|_Q > 0$ is already small.

CMA attack: pick (r, s') where $s' := \frac{1}{2}(h - v)$

Vanilla HAWK

$\tilde{D}_B[h]$: discrete Gaussian on $h + 2\mathbb{Z}^{2n}$ in $\|x\|_Q := \mathrm{tr}(x^* x)/n$



$Sign_B(m)$:

1: $r \leftarrow \{0,1\}^{\text{saltlen}}$
2: $h := H(m, r)$
3: $v \leftarrow \widetilde{D}_B[h]$
4: $s := \frac{1}{2}(h + \langle v \rangle)$
5: **return** $sig := (r, s)$

$Vrfy_Q(m, (r, s))$:

1: $v := 2s - H(m, r)$
2: **check** $s \in \mathbb{Z}^{2n}$
3: **check** $\|v\|_Q > 0$ is small

unique representation:

$\langle v \rangle = \langle -v \rangle \in \{\pm v\}$

If $Vrfy_Q(m, sig) = 1$ then $\|v\|_{\mathrm{pk}} > 0$ is already small.

~~CMA attack: pick (r, s') where $s' := \frac{1}{2}(h - v)$~~

Overview

- Background
- Security of HAWK
- More Details

Proof Sketch

Goal: simulate $Sign_B$ while preserving freshness of v.

Proof Sketch

Goal: simulate $Sign_B$ while preserving freshness of v.

$Sign_B(m)$:

$r \leftarrow \{0,1\}^{\text{saltlen}}$
$h := H(m, r)$
$v \leftarrow \widetilde{D}_B\,[\,h\,]$
$s := \frac{1}{2}\,(h + \langle v \rangle)$
return $sig := (r, s)$

$Sim^{\text{DGS in } \|x\|_Q}(m)$:

$r \leftarrow \{0,1\}^{\text{saltlen}}$
$v \leftarrow \text{DGS in } \|x\|_Q$
$H(m, r) := h := v \mod 2$
$s := \frac{1}{2}\,(h + \langle v \rangle)$
return $sig := (r, s)$

Proof Sketch

Goal: simulate $Sign_B$ while preserving freshness of v.

$Sign_B(m)$:

$r \leftarrow \{0,1\}^{\text{saltlen}}$
$h := H(m,r)$
$v \leftarrow \widetilde{D}_B[\,h\,]$
$s := \frac{1}{2}(h + \langle v \rangle)$
return $sig := (r,s)$

$Sim^{\text{DGS in } \|x\|_Q}(m)$:

$r \leftarrow \{0,1\}^{\text{saltlen}}$
$v \leftarrow \text{DGS in } \|x\|_Q$
$H(m,r) := h := v \mod 2$
$s := \frac{1}{2}(h + \langle v \rangle)$
return $sig := (r,s)$

Two steps:

- Closeness $Sign_B \approx Sim$
- A fresh and valid forgery $(m^*, sig^* := (r^*, s^*)) \leftarrow \mathcal{A}^{H,Sim}$ yields a fresh vector $v^* := 2s^* - H(m^*, r^*)$.

Proof Sketch

Goal: simulate $Sign_B$ while preserving freshness of v.

$Sign_B(m)$:

- $r \leftarrow \{0,1\}^{\text{saltlen}}$
- $h := H(m, r)$
- $v \leftarrow \widetilde{D}_B\,[\,h\,]$
- $s := \frac{1}{2}\left(h + \langle v \rangle\right)$
- **return** $sig := (r, s)$

$Sim^{\text{DGS in } \|x\|_Q}(m)$:

- $r \leftarrow \{0,1\}^{\text{saltlen}}$
- $v \leftarrow \text{DGS in } \|x\|_Q$
- $H(m, r) := h := v \mod 2$
- $s := \frac{1}{2}\left(h + \langle v \rangle\right)$
- **return** $sig := (r, s)$

Two steps:

- Closeness $Sign_B \approx Sim$
- A fresh and valid forgery $(m^*, sig^* := (r^*, s^*)) \leftarrow \mathcal{A}^{H,Sim}$ yields a fresh vector $v^* := 2s^* - H(m^*, r^*)$.

Both require quantum reasoning.

Closeness $Sign_{sk} \approx Sim$

Introduce an intermediate oracle *Trans*.

~~$Sign_B$~~ $Trans(m)$:

$r \leftarrow \{0,1\}^{\text{saltlen}}$
~~$h := H(m, r)$~~
$H(m, r) := h \leftarrow \{0,1\}^{2n}$
$v \leftarrow \widetilde{D}_B\,[\,h\,]$
$s := \frac{1}{2}\left(h + \langle v \rangle\right)$
return $sig := (r, s)$

$Sim^{\text{DGS in } \|x\|_Q}(m)$:

$r \leftarrow \{0,1\}^{\text{saltlen}}$
$v \leftarrow \text{DGS in } \|x\|_Q$
$H(m, r) := h := v \mod 2$
$s := \frac{1}{2}\left(h + \langle v \rangle\right)$
return $sig := (r, s)$

Closeness $Sign_{sk} \approx Sim$

Introduce an intermediate oracle *Trans*.

~~$Sign_B$~~ $Trans(m)$:

```
r ← {0,1}^saltlen
~~h := H(m, r)~~
H(m, r) := h ← {0,1}^{2n}
v ← D̃_B[h]
s := 1/2 (h + ⟨v⟩)
return sig := (r, s)
```

$r \leftarrow \{0,1\}^{\text{saltlen}}$

~~$h := H(m,r)$~~

$H(m,r) := h \leftarrow \{0,1\}^{2n}$

$v \leftarrow \widetilde{D}_B[h]$

$s := \frac{1}{2}(h + \langle v \rangle)$

return $sig := (r, s)$

$Sim^{\text{DGS in } \|x\|_Q}(m)$:

$r \leftarrow \{0,1\}^{\text{saltlen}}$

$v \leftarrow \text{DGS in } \|x\|_Q$

$H(m,r) := h := v \mod 2$

$s := \frac{1}{2}(h + \langle v \rangle)$

return $sig := (r, s)$

Two (sub)steps:

- $Sign_B \approx Trans$ by adaptive reprogramming lemma [GHHM21].
- $Trans \approx Sim$ by bounding statistical distance.

Closeness $\mathit{Sign}_{\mathsf{sk}} \approx \mathit{Sim}$

Introduce an intermediate oracle *Trans*.

~~Sign_B~~ $\mathit{Trans}(m)$:

$r \leftarrow \{0,1\}^{\mathsf{saltlen}}$
~~$h := H(m, r)$~~
$H(m, r) := h \leftarrow \{0,1\}^{2n}$
$v \leftarrow \widetilde{D}_B\,[\,h\,]$
$s := \frac{1}{2}\left(h + \langle v \rangle\right)$
return $\mathit{sig} := (r, s)$

$\mathit{Sim}^{\mathsf{DGS\ in}\ \|x\|_Q}(m)$:

$r \leftarrow \{0,1\}^{\mathsf{saltlen}}$
$v \leftarrow \mathsf{DGS\ in}\ \|x\|_Q$
$H(m, r) := h := v \mod 2$
$s := \frac{1}{2}\left(h + \langle v \rangle\right)$
return $\mathit{sig} := (r, s)$

Two (sub)steps:

- $\mathit{Sign}_B \approx \mathit{Trans}$ by adaptive reprogramming lemma [GHHM21].
- $\mathit{Trans} \approx \mathit{Sim}$ by bounding statistical distance.

Improvable: replace statistical distance by Rényi's divergence, see HAWK spec.

Classical Proof

To obtain classical proof:

- replace adaptive reprogramming lemma [GHHM21] to classical reprogramming
- replace quantum preimage bound to classical one

That's It

HAWK is quantum secure.

Eprint: `ia.cr/2023/711`

References I

[DPPvW22] Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel van Woerden. Hawk: Module LIP makes lattice signatures fast, compact and simple. In Shweta Agrawal and Dongdai Lin, editors, Advances in Cryptology – ASIACRYPT 2022, pages 65–94, Cham, 2022. Springer Nature Switzerland.

[DvW22] Léo Ducas and Wessel van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In Orr Dunkelman and Stefan Dziembowski, editors, Advances in Cryptology – EUROCRYPT 2022, pages 643–673, Cham, 2022. Springer International Publishing.

References II

[GHHM21] Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Tight adaptive reprogramming in the QROM. In Mehdi Tibouchi and Huaxiong Wang, editors, Advances in Cryptology – ASIACRYPT 2021, pages 637–667, Cham, 2021. Springer International Publishing.