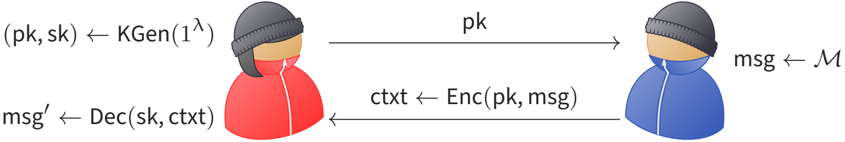
Hollow LWE: A New Spin — Unbounded Updatable Encryption from LWE and PCE

Martin R. Albrecht[1] (King's College London and SanboxAQ), Benjamin Benčina (Royal Holloway, Univesity of London) and Russell W. F. Lai (Aalto University)

Workshop On the Mathematics of Post-Quantum Cryptography, Zürich, 6 June 2025

[1] Slides heavily based on Benjamin's slides.

Public-Key Encryption (PKE)



Properties:

- Decryption Correctness: $\mathsf{msg}' = \mathsf{msg}$.
- IND-CPA Security:

$$\big(\mathsf{pk}, \mathsf{Enc}(\mathsf{pk}, \mathsf{msg}_0)\big) \underset{c}{\approx} \big(\mathsf{pk}, \mathsf{Enc}(\mathsf{pk}, \mathsf{msg}_1)\big).$$

Updatable Public-Key Encryption (UPKE)

Let $(\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ be a correct PKE scheme.

$(\mathsf{pk}', \mathsf{up}) \leftarrow \mathsf{UpdPk}(\mathsf{pk}; \rho)$

$\xleftarrow{\mathsf{up}}$

$\mathsf{sk}' \leftarrow \mathsf{UpdSk}(\mathsf{sk}, \mathsf{up})$

$\downarrow$ sk'

$\downarrow$ pk'

- Update correctness: Dec. cor. holds for updated keys $(\mathsf{pk}', \mathsf{sk}')$.

IND-CR-CPA Security Experiment

$\mathsf{IND\text{-}CR\text{-}CPA}_{\Pi,\mathcal{A}}(1^\lambda)$	Oracle $\mathsf{UpdO}(\rho)$
$i := 0; \quad b \leftarrow\!\!\$ \{0,1\}$	/ Update honestly using
$(\mathsf{pk}_0, \mathsf{sk}_0) \leftarrow \mathsf{KGen}(1^\lambda)$	/ potentially malicious randomness.
$(\mathsf{st}, \mathsf{msg}_0, \mathsf{msg}_1) \leftarrow \mathcal{A}^{\mathsf{UpdO}}(\mathsf{pk}_0)$	$(\mathsf{pk}_{i+1}, \mathsf{up}_i) \leftarrow \mathsf{UpdPk}(\mathsf{pk}_i; \rho)$
$\mathsf{ctxt} \leftarrow \mathsf{Enc}(\mathsf{pk}_i, \mathsf{msg}_b)$	$\mathsf{sk}_{i+1} \leftarrow \mathsf{UpdSk}(\mathsf{sk}_i, \mathsf{up}_i)$
$\mathsf{st} \leftarrow \mathcal{A}^{\mathsf{UpdO}}(\mathsf{ctxt}, \mathsf{st})$	$i := i + 1$
$j := i$	
$(\mathsf{pk}_{j+1}, \mathsf{up}_j) \leftarrow \mathsf{UpdPk}(\mathsf{pk}_j)$	
$\mathsf{sk}_{j+1} \leftarrow \mathsf{UpdSk}(\mathsf{sk}_j, \mathsf{up}_j)$	
$b' \leftarrow \mathcal{A}(\mathsf{pk}_{j+1}, \mathsf{sk}_{j+1}, \mathsf{up}_j, \mathsf{st})$	
return $b = b'$	

IND-CR-CPA Security

$$\big(\mathsf{pk}, \mathsf{Enc}(\mathsf{pk}, \mathsf{msg}_0), \mathsf{pk}', \mathsf{sk}', \mathsf{up}\big) \underset{c}{\approx} \big(\mathsf{pk}, \mathsf{Enc}(\mathsf{pk}, \mathsf{msg}_1), \mathsf{pk}', \mathsf{sk}', \mathsf{up}\big)$$

$\Rightarrow$ "forward secrecy."

Dual-Regev Encryption [Reg05, GPV08]

$\mathsf{KGen}(1^\lambda)$	$\mathsf{Enc}(\mathsf{pk}, \mathsf{msg} \in \{0,1\})$
$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times k}$	$\mathbf{x} \leftarrow\$ \mathbb{Z}_q^k; \quad \mathbf{e} \leftarrow\$ \chi^n; \quad e' \leftarrow\$ \chi$
$\mathbf{r} \leftarrow\$ \{\pm 1\}^n$	$\mathbf{c}_0 := \mathbf{A}\cdot\mathbf{x} + \mathbf{e} \bmod q$
$\mathbf{u}^{\mathrm{T}} := \mathbf{r}^{\mathrm{T}} \cdot \mathbf{A} \bmod q$	$c_1 := \langle \mathbf{u}, \mathbf{x}\rangle + e' + \lfloor \frac{q}{2} \rceil \cdot \mathsf{msg} \bmod q$
$\mathsf{pk} := (\mathbf{A}, \mathbf{u})$	**return** $\mathsf{ctxt} := (\mathbf{c}_0, c_1)$
$\mathsf{sk} := \mathbf{r}$	
return $(\mathsf{pk}, \mathsf{sk})$	$\mathsf{Dec}(\mathsf{sk}, \mathsf{ctxt})$
	return $\left\lfloor \frac{2}{q} \cdot (c_1 - \langle \mathbf{r}, \mathbf{c}_0\rangle \bmod q) \right\rceil$

- Correctness: $\mathbf{r}, \mathbf{e}, e'$ are short enough $\Rightarrow$ Dual-Regev has decryption correctness.
- Security: LWE assumption $\Rightarrow$ Dual-Regev is IND-CPA secure.

Prior LWE key-update mechanism [DKW21]

$\mathsf{UpdPk}(\mathsf{pk})$	$\mathsf{UpdSk}(\mathsf{sk}, \mathsf{up})$
$(\mathbf{A}, \mathbf{u}) \leftarrow \mathsf{pk}$	$\mathbf{r} \leftarrow \mathsf{sk}$
$\delta \leftarrow\!\!\$\ \chi_{\mathbf{r}}^{n}$	$\delta \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{up})$
$\mathsf{pk}' := (\mathbf{A}, \mathbf{u}^{\mathrm{T}} + \delta^{\mathrm{T}} \cdot \mathbf{A})$	$\mathsf{sk}' := \mathbf{r} + \delta$
$\mathsf{up} \leftarrow \mathsf{Enc}(\mathsf{pk}, \delta)$	**return** sk'
return $(\mathsf{pk}', \mathsf{up})$	

Issues:

- Updated secret key $\mathbf{r}' = \mathbf{r} + \delta$ has increased norm.
- To maintain correctness with many updates, either
  - restrict number of updates to be fixed a-priori, or
  - for $\mathsf{poly}(\lambda)$ many updates, set super-poly. modulus $q > \lambda^{\omega(1)} \implies$ large ctxt.

Prior LWE key-update mechanism [DKW21]

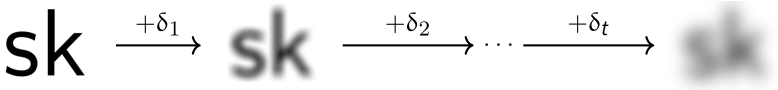
UpdPk(pk)	UpdSk(sk, up)
$(\mathbf{A}, \mathbf{u}) \leftarrow \mathsf{pk}$	$\mathbf{r} \leftarrow \mathsf{sk}$
$\delta \leftarrow\!\!\$\ \chi_{\mathbf{r}}^{n}$	$\delta \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{up})$
$\mathsf{pk}' := (\mathbf{A}, \mathbf{u}^{\mathrm{T}} + \delta^{\mathrm{T}} \cdot \mathbf{A})$	$\mathsf{sk}' := \mathbf{r} + \delta$
$\mathsf{up} \leftarrow \mathsf{Enc}(\mathsf{pk}, \delta)$	**return** sk'
return $(\mathsf{pk}', \mathsf{up})$	

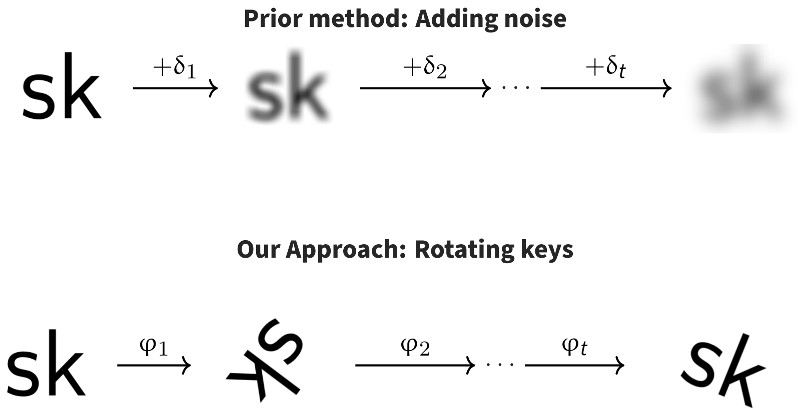
Issues:

- Updated secret key $\mathbf{r}' = \mathbf{r} + \delta$ has increased norm.
- To maintain correctness with many updates, either
  - restrict number of updates to be fixed a-priori, or
  - for poly(λ) many updates, set super-poly. modulus $q > \lambda^{\omega(1)} \implies$ large ctxt.

What if we rotate keys instead?

Prior method: Adding noise




Prior method: Adding noise
sk
$+\delta_1$
sk
$+\delta_2$
$\cdots$
$+\delta_t$
Our Approach: Rotating keys
sk
φ_1
sk
φ_2
$\cdots$
φ_t
sk

q-ARY LATTICES

A lattice $\Lambda \subseteq \mathbb{R}^n$ is a discrete additive subgroup of $\mathbb{R}^n$, i.e.

$$\Lambda = \mathbf{B} \cdot \mathbb{Z}^k$$

for some basis $\mathbf{B} \in \mathbb{R}^{n\times k}$ where $k \leq n$. All bases $\mathbf{B}, \mathbf{B}' \in \mathbb{R}^{n\times k}$ are related by unimodular $\mathbf{U} \in \mathbb{Z}^{k\times k}$ via $\mathbf{B}' = \mathbf{B} \cdot \mathbf{U}$.

Define the Construction A lattice of a full-rank $\mathbf{A} \in \mathbb{Z}_q^{n\times k}$ as

$$\Lambda_q(\mathbf{A}) = \mathbf{A} \cdot \mathbb{Z}^k + q \cdot \mathbb{Z}^n.$$

Note that $\Lambda_q(\mathbf{A})$ is q-ary, i.e.

$$q \cdot \mathbb{Z}^n \subseteq \Lambda_q(\mathbf{A}) \subseteq \mathbb{Z}^n.$$

LWE and Dual-Regev: Lattice point of view

For $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times k}$, $\mathbf{x} \xleftarrow{\$} \mathbb{Z}_q^{k}$, short noise $\mathbf{e} \xleftarrow{\$} \chi^n$, consider

$$\boxed{\mathbf{b}} = \boxed{\mathbf{A}}\,\boxed{\mathbf{x}} + \boxed{\mathbf{e}} \bmod q.$$

LWE assumption: for $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times k}$, $\mathbf{x} \xleftarrow{\$} \mathbb{Z}_q^{k}$, $\mathbf{e} \xleftarrow{\$} \chi^n$, $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^{n}$ we have $(\mathbf{A}, \mathbf{A}\cdot\mathbf{x} + \mathbf{e} \bmod q) \underset{c}{\approx} (\mathbf{A}, \mathbf{u})$.

Dual-Regev key-pair: $\left(\mathbf{A}, \mathbf{r}^{\mathrm{T}} \cdot \mathbf{A}\right) \underset{s}{\approx} \left(\mathbf{A}, \mathbf{u}^{\mathrm{T}} \xleftarrow{\$} \mathbb{Z}_q^{k}\right)$ for short $\mathbf{r}$ by LHL, or $\underset{c}{\approx}$ by LWE.

Lattice Isomorphism Problem (LIP)

Lattice Isomorphism: Lattices Λ, Λ' are isomorphic, denoted $\Lambda \sim \Lambda'$, if there exists an orthogonal matrix $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$, i.e.

$$\mathbf{O} \in \mathbb{R}^{n \times n} \qquad \text{with} \qquad \mathbf{O}^{\mathrm{T}} \cdot \mathbf{O} = \mathbf{I}_n,$$

such that

$$\Lambda' = \mathbf{O} \cdot \Lambda,$$

i.e. Λ' can be obtained by rotating and reflecting Λ. If $\mathbf{B}$ and $\mathbf{B}'$ are bases of Λ and Λ', then it means $\mathbf{B}' = \mathbf{O} \cdot \mathbf{B} \cdot \mathbf{U}$ for some unimodular $\mathbf{U} \in \mathbb{Z}^{k \times k}$.

Lattice Isomorphism Problem (ΔLIP) [DvW22]: Given lattices $\Lambda_0, \Lambda_1, \Lambda \subseteq \mathbb{R}^n$, decide if

$$\Lambda \sim \Lambda_0 \qquad \text{or} \qquad \Lambda \sim \Lambda_1.$$

Lattice Isomorphism Problem (LIP)

Lattice Isomorphism: Lattices Λ, Λ' are isomorphic, denoted $\Lambda \sim \Lambda'$, if there exists an orthogonal matrix $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$, i.e.

$$\mathbf{O} \in \mathbb{R}^{n \times n} \qquad \text{with} \qquad \mathbf{O}^{\mathrm{T}} \cdot \mathbf{O} = \mathbf{I}_n,$$

such that

$$\Lambda' = \mathbf{O} \cdot \Lambda,$$

i.e. Λ' can be obtained by rotating and reflecting Λ. If $\mathbf{B}$ and $\mathbf{B}'$ are bases of Λ and Λ', then it means $\mathbf{B}' = \mathbf{O} \cdot \mathbf{B} \cdot \mathbf{U}$ for some unimodular $\mathbf{U} \in \mathbb{Z}^{k \times k}$.

Lattice Isomorphism Problem (ΔLIP) [DvW22]: Given lattices $\Lambda_0, \Lambda_1, \Lambda \subseteq \mathbb{R}^n$, decide if

$$\Lambda \sim \Lambda_0 \qquad \text{or} \qquad \Lambda \sim \Lambda_1.$$

Rotate Keys with LIP?

The idea, more concretely:

- Rotate the lattice: $\mathbf{A} \mapsto \mathbf{A}' := \mathbf{O} \cdot \mathbf{A} \cdot \mathbf{U} \bmod q$.
- Rotate the key: $\mathbf{r} \mapsto \mathbf{r}' := \mathbf{O} \cdot \mathbf{r} \bmod q$.
- Update the syndrome: $\mathbf{u} \mapsto \mathbf{u}' := \mathbf{U}^{\mathrm{T}} \cdot \mathbf{u} \bmod q$, so that:

$$\mathbf{r}^{\mathrm{T}} \cdot \mathbf{A} = \mathbf{u}^{\mathrm{T}} \qquad \Rightarrow \qquad \mathbf{r}'^{\mathrm{T}} \cdot \mathbf{A}' = \mathbf{u}'^{\mathrm{T}}$$

One can think of it as re-randomising a SIS commitment.

Upshot: $\|\mathbf{r}'\|_2 = \sqrt{\langle \mathbf{O} \cdot \mathbf{r}, \mathbf{O} \cdot \mathbf{r} \rangle} = \sqrt{\langle \mathbf{r}, \mathbf{r} \rangle} = \|\mathbf{r}\|_2$.

Issue: Orthogonal $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ are real-valued $\Rightarrow$ $\mathbf{O} \cdot \mathbf{A} \cdot \mathbf{U}$ and $\mathbf{O} \cdot \mathbf{r}$ may not be integral.

Rotate Keys with LIP?

The idea, more concretely:

- Rotate the lattice: $\mathbf{A} \mapsto \mathbf{A}' := \mathbf{O} \cdot \mathbf{A} \cdot \mathbf{U} \bmod q$.
- Rotate the key: $\mathbf{r} \mapsto \mathbf{r}' := \mathbf{O} \cdot \mathbf{r} \bmod q$.
- Update the syndrome: $\mathbf{u} \mapsto \mathbf{u}' := \mathbf{U}^{\mathrm{T}} \cdot \mathbf{u} \bmod q$, so that:

$$\mathbf{r}^{\mathrm{T}} \cdot \mathbf{A} = \mathbf{u}^{\mathrm{T}} \qquad \Rightarrow \qquad \mathbf{r}'^{\mathrm{T}} \cdot \mathbf{A}' = \mathbf{u}'^{\mathrm{T}}$$

One can think of it as re-randomising a SIS commitment.

Upshot: $\left\|\mathbf{r}'\right\|_2 = \sqrt{\langle \mathbf{O} \cdot \mathbf{r}, \mathbf{O} \cdot \mathbf{r} \rangle} = \sqrt{\langle \mathbf{r}, \mathbf{r} \rangle} = \|\mathbf{r}\|_2$.

Issue: Orthogonal $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ are real-valued $\Rightarrow$ $\mathbf{O} \cdot \mathbf{A} \cdot \mathbf{U}$ and $\mathbf{O} \cdot \mathbf{r}$ may not be integral.

ROTATE KEYS WITH LIP?

The idea, more concretely:

- Rotate the lattice: $\mathbf{A} \mapsto \mathbf{A}' := \mathbf{O} \cdot \mathbf{A} \cdot \mathbf{U} \bmod q$.
- Rotate the key: $\mathbf{r} \mapsto \mathbf{r}' := \mathbf{O} \cdot \mathbf{r} \bmod q$.
- Update the syndrome: $\mathbf{u} \mapsto \mathbf{u}' := \mathbf{U}^{\mathrm{T}} \cdot \mathbf{u} \bmod q$, so that:

$$\mathbf{r}^{\mathrm{T}} \cdot \mathbf{A} = \mathbf{u}^{\mathrm{T}} \qquad \Rightarrow \qquad \mathbf{r}'^{\mathrm{T}} \cdot \mathbf{A}' = \mathbf{u}'^{\mathrm{T}}$$

One can think of it as re-randomising a SIS commitment.

Upshot: $\left\|\mathbf{r}'\right\|_2 = \sqrt{\langle \mathbf{O} \cdot \mathbf{r}, \mathbf{O} \cdot \mathbf{r} \rangle} = \sqrt{\langle \mathbf{r}, \mathbf{r} \rangle} = \|\mathbf{r}\|_2$.

Issue: Orthogonal $\mathbf{O} \in \mathcal{O}_n(\mathbb{R})$ are real-valued $\Rightarrow$ $\mathbf{O} \cdot \mathbf{A} \cdot \mathbf{U}$ and $\mathbf{O} \cdot \mathbf{r}$ may not be integral.

Lattice Automorphism of $\mathbb{Z}^n$

- The automorphism group $\mathrm{Aut}(\Lambda)$ of a lattice Λ is the group of all isomorphisms from Λ to itself.

- It is well-known that $\mathrm{Aut}(\mathbb{Z}^n) = \mathcal{O}_n(\mathbb{Z})$, i.e. the group of signed permutations

$$\mathcal{O}_n(\mathbb{Z}) = \left\{ \mathbf{D} \cdot \mathbf{P} \ ; \ \mathbf{D} \in \mathrm{diag}(\{\pm 1\}^n), \ \mathbf{P} \in \mathcal{P}_n \right\}.$$

- Since

$$q \cdot \mathbb{Z}^n \subseteq \Lambda_q(\mathbf{A}) \subseteq \mathbb{Z}^n,$$

we have

$$q \cdot \mathbb{Z}^n \subseteq \mathbf{O} \cdot \Lambda_q(\mathbf{A}) = \Lambda_q(\mathbf{O} \cdot \mathbf{A}) \subseteq \mathbb{Z}^n,$$

i.e. rotating $\Lambda_q(\mathbf{A})$ by $\mathbf{O} \in \mathcal{O}_n(\mathbb{Z})$ gives another q-ary lattice.

Lattice Automorphism of $\mathbb{Z}^n$

- The automorphism group $\text{Aut}(\Lambda)$ of a lattice Λ is the group of all isomorphisms from Λ to itself.

- It is well-known that $\text{Aut}(\mathbb{Z}^n) = \mathcal{O}_n(\mathbb{Z})$, i.e. the group of signed permutations

$$\mathcal{O}_n(\mathbb{Z}) = \left\{\mathbf{D} \cdot \mathbf{P} \; ; \; \mathbf{D} \in \text{diag}(\{\pm 1\}^n), \, \mathbf{P} \in \mathcal{P}_n\right\}.$$

- Since

$$q \cdot \mathbb{Z}^n \subseteq \Lambda_q(\mathbf{A}) \subseteq \mathbb{Z}^n,$$

  we have

$$q \cdot \mathbb{Z}^n \subseteq \mathbf{O} \cdot \Lambda_q(\mathbf{A}) = \Lambda_q(\mathbf{O} \cdot \mathbf{A}) \subseteq \mathbb{Z}^n,$$

  i.e. rotating $\Lambda_q(\mathbf{A})$ by $\mathbf{O} \in \mathcal{O}_n(\mathbb{Z})$ gives another q-ary lattice.

Coding theory point of view

- The Construction A lattice of $\mathbf{A} \in \mathbb{Z}_q^{n\times k}$ defined by $\Lambda_q(\mathbf{A}) = \mathbf{A} \cdot \mathbb{Z}^k + q \cdot \mathbb{Z}^n$ is isomorphic to the $[n, k]$-linear code $\mathfrak{C} = \mathbf{A} \cdot \mathbb{Z}_q^k$ over $\mathbb{Z}_q$ generated by $\mathbf{A}$.
- The (Signed) Permutation Code Equivalence ((S)PCE) problem is to decide if two codes $\mathfrak{C}$ and $\mathfrak{C}'$ are (signed) permutation equivalent, i.e. whether

$$\mathfrak{C}' = \mathbf{O} \cdot \mathfrak{C}$$

  for some (signed) permutation matrix $\mathbf{O} \in \mathcal{O}_n(\mathbb{Z})$.
- SPCE is essentially decision LIP with Λ's restricted to q-ary lattices and $\mathbf{O}$'s restricted to signed permutations.

Coding theory point of view

- The Construction A lattice of $\mathbf{A} \in \mathbb{Z}_q^{n \times k}$ defined by $\Lambda_q(\mathbf{A}) = \mathbf{A} \cdot \mathbb{Z}^k + q \cdot \mathbb{Z}^n$ is isomorphic to the $[n, k]$-linear code $\mathfrak{C} = \mathbf{A} \cdot \mathbb{Z}_q^k$ over $\mathbb{Z}_q$ generated by $\mathbf{A}$.

- The (Signed) Permutation Code Equivalence ((S)PCE) problem is to decide if two codes $\mathfrak{C}$ and $\mathfrak{C}'$ are (signed) permutation equivalent, i.e. whether

$$\mathfrak{C}' = \mathbf{O} \cdot \mathfrak{C}$$

for some (signed) permutation matrix $\mathbf{O} \in \mathcal{O}_n(\mathbb{Z})$.

- SPCE is essentially decision LIP with Λ's restricted to q-ary lattices and $\mathbf{O}$'s restricted to signed permutations.

CODING THEORY POINT OF VIEW

- The Construction A lattice of $\mathbf{A} \in \mathbb{Z}_q^{n \times k}$ defined by $\Lambda_q(\mathbf{A}) = \mathbf{A} \cdot \mathbb{Z}^k + q \cdot \mathbb{Z}^n$ is isomorphic to the $[n, k]$-linear code $\mathfrak{C} = \mathbf{A} \cdot \mathbb{Z}_q^k$ over $\mathbb{Z}_q$ generated by $\mathbf{A}$.

- The (Signed) Permutation Code Equivalence ((S)PCE) problem is to decide if two codes $\mathfrak{C}$ and $\mathfrak{C}'$ are (signed) permutation equivalent, i.e. whether

$$\mathfrak{C}' = \mathbf{O} \cdot \mathfrak{C}$$

  for some (signed) permutation matrix $\mathbf{O} \in \mathcal{O}_n(\mathbb{Z})$.

- SPCE is essentially decision LIP with Λ's restricted to q-ary lattices and $\mathbf{O}$'s restricted to signed permutations.

PCE-BASED KEY-UPDATE MECHANISM

$\mathsf{UpdPk}(\mathsf{pk})$	$\mathsf{UpdSk}(\mathsf{sk}, \mathsf{up})$
$(\mathbf{A}, \mathbf{u}) \leftarrow \mathsf{pk}$	$\mathbf{r} \leftarrow \mathsf{sk}$
$\mathbf{O} \leftarrow\$ \mathcal{O}_n(\mathbb{Z})$	$\mathbf{O} \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{up})$
$\mathbf{A}', \mathbf{U} := \mathsf{SF}(\mathbf{O} \cdot \mathbf{A})$	$\mathsf{sk}' := \mathbf{O} \cdot \mathbf{r}$
$\mathsf{pk}' := (\mathbf{A}', \mathbf{u}^{\mathrm{T}} \cdot \mathbf{U})$	**return** sk'
$\mathsf{up} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathbf{O})$	
return $(\mathsf{pk}', \mathsf{up})$	

Update correctness:

$$\mathbf{r}'^{\mathrm{T}} \cdot \mathbf{A}' = \mathbf{r}^{\mathrm{T}} \cdot \underbrace{\mathbf{O}^{\mathrm{T}} \cdot \mathbf{O}}_{\mathbf{I}_n} \cdot \mathbf{A} \cdot \mathbf{U} = \underbrace{\mathbf{r}^{\mathrm{T}} \cdot \mathbf{A}}_{\mathbf{u}^{\mathrm{T}}} \cdot \mathbf{U} = \mathbf{u}^{\mathrm{T}} \cdot \mathbf{U} = \mathbf{u}'^{\mathrm{T}} \pmod{q}.$$

Caution – Mind the Hull

- The hardness of (S)PCE, depends on the hull of the code $\mathfrak{C} = \mathbf{A} \cdot \mathbb{Z}_q^k$.
- The hull $\mathcal{H}(\mathfrak{C}) := \mathfrak{C} \cap \mathfrak{C}^\perp = \left\{\mathbf{x} \in \mathfrak{C} \,;\, \mathbf{x}^\mathrm{T} \cdot \mathfrak{C} = \mathbf{0}\right\}$ is a subcode of $\mathfrak{C}$.
- Random codes have small hull dimension [Sen97], most likely 0.
- Existing attacks against (S)PCE run in time $\mathcal{O}\left(q^h \cdot \mathrm{poly}(n,k)\right)$ or $\mathcal{O}\left(n^h \cdot \mathrm{poly}(n,k,q)\right)$, i.e. efficient when h is small [Sen00, BOST19].
- Up to now, only LCD ($h = 0$) and self-orthogonal ($h = k$) codes have been treated in the literature, and not algorithmically.

SampCode(n, k, h, q)

We give an algorithm SampCode(n, k, h, q) that samples $\mathbf{A}$ generating a uniformly random $[n, k]$-linear code over $\mathbb{Z}_q$ with hull dimension h. We call such codes and matrices "h-hollow".

Sample Sell-Dual Vectors

Definition: A vector $\mathbf{v} \in \mathfrak{C}$ is *self-orthogonal* if $\langle \mathbf{v}, \mathbf{v} \rangle = 0$.

Observation: $\mathbf{v} = \mathbf{A} \cdot \mathbf{x} \in \text{Span}(\mathbf{A})$ is self-orthogonal iff $\mathbf{x}^{\mathrm{T}} \cdot \mathbf{A}^{\mathrm{T}} \cdot \mathbf{A} \cdot \mathbf{x} = 0$.

Warning's Second Theorem [CW35] implies there are at least q^{k-2} self-orthogonal vectors in any code.

Algorithm idea:

- Sample $\mathbf{x}_i \leftarrow\$ \mathbb{Z}_q$ for $i = 1, \ldots, k-2$.
- Solve the conic equation $\mathbf{x}^{\mathrm{T}} \cdot \mathbf{A}^{\mathrm{T}} \cdot \mathbf{A} \cdot \mathbf{x} = 0$ for $(\mathbf{x}_{k-1}, \mathbf{x}_k)$.
- Complete $\mathbf{x}$ with a random solution (and adjust the probability).

Solving Conics over Finite Fields

Definition: A smooth affine conic is an equations of the form

$$A \cdot x^2 + B \cdot xy + C \cdot y^2 + D \cdot x + E \cdot y + F = 0,$$

where $\Delta = B^2 - 4 \cdot A \cdot C \neq 0$.

A conic over a finite field $\mathbb{F}$ of odd characteristic always has a solution. If $\Delta \in \mathrm{QR}(\mathbb{Z}_q)$ then the number of solutions $S \in \{q - 1, 2 \cdot q - 1\}$ and if $\Delta \notin \mathrm{QR}(\mathbb{Z}_q)$ then $S \in \{1, q + 1\}$.

Adjusting Probabilities with Rejection Sampling

Discriminant Δ depends on $\mathbf{A}$ and is fixed at the beginning of execution. So we know the maximal number of solutions $M(\Delta)$ is either $2 \cdot q - 1$ or $q + 1$.

If the conic has S solutions, we have to accept $\mathbf{v}$ with probability $\frac{S}{M}$, since

$$\Pr[\mathbf{v} = \mathbf{A} \cdot \mathbf{x} \text{ sampled}] = \frac{1}{q^{k-2}} \cdot \frac{1}{S} \cdot \Pr\left[u \leq \frac{S}{M}\right] = \frac{1}{q^{k-2}} \cdot \frac{1}{M},$$

is then independent of S, hence the distribution is uniform.

STEALING FROM THE DUAL

Algorithm:

- Sample a 0-hollow matrix $\mathbf{A}_0$ from $\mathbb{Z}_q^{n\times(k-h)}$.
- Sample $\mathbf{y} \leftarrow\$ \mathsf{SSO}(\mathsf{Span}(\mathbf{A}_0)^{\perp})$ and define $\mathbf{A}_1 = [\mathbf{A}_0, \mathbf{y}]$.
- …
- Sample $\mathbf{y} \leftarrow\$ \mathsf{SSO}(\mathsf{Span}(\mathbf{A}_{h-1})^{\perp})$ and return $\mathbf{A}_h = [\mathbf{A}_{h-1}, \mathbf{y}] \in \mathbb{Z}_q^{n\times k}$.

The output distribution of this algorithm is negligibly close to the uniform distribution on $[n, k]$-linear h-hollow codes over $\mathbb{Z}_q$. It succeeds with prob.

$$\varepsilon \geq \left(1 - \frac{1}{q} - \frac{1}{q^2}\right) \cdot (1 - \mathsf{negl}(n))$$

if $2 \cdot k \leq n$ and $2 \cdot h \leq k$.

Hollow Lattice Problems

Upshot: Now that we know how to sample h-hollow codes, we can rely on PCE for h-hollow codes with $n^h \geq 2^\lambda$ and $q^h \geq 2^\lambda$ (+ other conditions), which should now be hard.

Question: Does this somehow make LWE easy?

Hollow Lattice Problems

Hollow-LWE: $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times k}$ h-hollow, $\mathbf{x} \leftarrow\$ \mathbb{Z}_q^{k}$, $\mathbf{e} \leftarrow\$ \chi^n$, $\mathbf{u} \leftarrow\$ \mathbb{Z}_q^{n}$, distinguish

$$(\mathbf{A}, \mathbf{A}\cdot\mathbf{x}+\mathbf{e}) \qquad \text{from} \qquad (\mathbf{A}, \mathbf{u})\,.$$

Theorem (LWE $\to$ Hollow-LWE)

If there exists a (t,ε)-algorithm $\mathcal{A}$ for $\mathrm{LWE}^{h}_{k,n,q,\chi}$ then there exists a $(t+\mathrm{poly}(\lambda), \varepsilon')$-algorithm $\mathcal{B}$ for $\mathrm{LWE}_{k-h,n,q,\chi}$ where

$$\epsilon' \geq \varepsilon \cdot \underbrace{\left(1-\frac{1}{q}-\frac{1}{q^2}\right)}_{\textit{triv. hull}} \cdot \underbrace{\left(1-\frac{h}{e^n}\right)}_{\textit{sub-sampler}} \cdot \underbrace{\prod_{i=0}^{k-h}\left(1-q^{i-n}\right)}_{\textit{full rank}} \cdot \underbrace{\prod_{i=1}^{h}\left(1-q^{k+i-n}\right)}_{\textit{lin. dep. in hull}}.$$

Hollow Lattice Problems

Theorem (Hollow-LHL)

Let n, k, h, q integers with

$$n \geq \underbrace{(1+c) \cdot k \cdot \log_2(q)}_{\text{LHL}} + \underbrace{k + h}_{\text{extra}}$$

for a positive real constant $c > 0$, $h \leq \frac{k}{2}$, and q an odd prime. Let $\mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_q^{n \times k}$ h-hollow matrix, $\mathbf{r} \leftarrow\!\!\$\ \{\pm 1\}^n$, and $\mathbf{u} \leftarrow\!\!\$\ \mathbb{Z}_q^k$. Then the pairs

$$(\mathbf{A}, \mathbf{r}^{\mathrm{T}} \cdot \mathbf{A}) \qquad \text{and} \qquad (\mathbf{A}, \mathbf{u}^{\mathrm{T}})$$

are statistically close in k.

Our Construction

$\underline{\mathsf{KGen}(1^\lambda)}$

$\mathbf{A} \leftarrow\!\!\$\ \mathsf{SampCode}(n, k, h, q)$

$\mathbf{r} \leftarrow\!\!\$\ \{\pm 1\}^n$

$\mathbf{u}^{\mathrm{T}} := \mathbf{r}^{\mathrm{T}} \cdot \mathbf{A} \bmod q$

$\mathsf{pk} := (\mathbf{A}, \mathbf{u})$

$\mathsf{sk} := \mathbf{r}$

return $(\mathsf{pk}, \mathsf{sk})$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{msg} \in \mathbb{Z} \cap [-p/2, p/2))}$

$\mathbf{x} \leftarrow\!\!\$\ \mathbb{Z}_q^k; \quad \mathbf{e} \leftarrow\!\!\$\ \chi^n; \quad e' \leftarrow\!\!\$\ \chi$

$\mathbf{c}_0 := \mathbf{A} \cdot \mathbf{x} + \mathbf{e} \bmod q$

$c_1 := \langle \mathbf{u}, \mathbf{x} \rangle + e' + \left\lfloor \frac{q}{p} \right\rceil \cdot \mathsf{msg} \bmod q$

return $\mathsf{ctxt} := (\mathbf{c}_0, c_1)$

$\underline{\mathsf{Dec}(\mathsf{sk}, \mathsf{ctxt})}$

return $\left\lfloor \frac{p}{q} \cdot (c_1 - \langle \mathbf{r}, \mathbf{c}_0 \rangle \bmod q) \right\rceil$

$\underline{\mathsf{UpdPk}(\mathsf{pk})}$

$\rho \leftarrow\!\!\$\ \{0,1\}^\lambda$

$\mathbf{O} := \mathsf{H}(\rho)$

$(\mathbf{A}', \mathbf{U}) := \mathsf{SF}(\mathbf{O} \cdot \mathbf{A})$

$\mathbf{u}'^{\mathrm{T}} := \mathbf{u}^{\mathrm{T}} \cdot \mathbf{U} \bmod q$

$\mathsf{pk}' := (\mathbf{A}', \mathbf{u}')$

$\mathsf{up} \leftarrow \mathsf{Enc}(\mathsf{pk}, \rho)$

return $(\mathsf{pk}', \mathsf{up})$

$\underline{\mathsf{UpdSk}(\mathsf{sk}, \mathsf{up})}$

$\rho \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{up})$

$\mathbf{O} := \mathsf{H}(\rho)$

$\mathbf{r}' := \mathbf{O} \cdot \mathbf{r}$

return $\mathsf{sk}' := \mathbf{r}'$

Security Theorem

Our construction is the Dual-Regev PKE with

- $\mathbf{A} \leftarrow\$ \mathsf{SampCode}(n, k, h, q)$,
- $\mathbf{r} \leftarrow\$ \{\pm 1\}^n$, and
- the above PCE-based update mechanism.

Theorem

Let n, k, h, q be positive integers parametrised by λ with $n \geq (1 + c) \cdot k \cdot \log_2(q) + k + h$ for a positive real constant $c > 0$, $2 \cdot h \leq k$ and q prime.
Assuming the advantage of any PPT *adversary in distinguishing $\mathsf{LWE}^h_{k,n,q,\chi}$ and in distinguishing $\mathsf{PCE}^h_{n,k,q}$ is negligible in λ, our construction is IND-CR-CPA secure in the ROM.*

$\textsc{Game}_4 \overset{?}{\approx} \textsc{Game}_5$

$$\begin{aligned}
\mathsf{pk}_0 &= (\mathbf{A}, \mathbf{u}), \\
\mathsf{pk} &= (\mathbf{O} \cdot \mathbf{A} \cdot \mathbf{U},\ \mathbf{U}^{\mathrm{T}} \cdot \mathbf{u}), \\
\mathsf{sk} &= \mathbf{O} \cdot \mathbf{r}, \\
\mathsf{ctxt} &\leftarrow \mathsf{Enc}((\mathbf{A}, \mathbf{u}), \mathsf{msg}_b), \\
\mathsf{up} &= \mathsf{Enc}((\mathbf{A}, \mathbf{u}), \rho^*);
\end{aligned}$$

$$\begin{aligned}
\mathbf{r} &\leftarrow\!\!\$\ \{\pm 1\}^n, \\
\mathbf{u}^{\mathrm{T}} &= \mathbf{r}^{\mathrm{T}} \cdot \mathbf{A}, \\
\mathbf{O} &\leftarrow\!\!\$\ \mathcal{O}_n(\mathbb{Z})
\end{aligned}$$

$$\begin{aligned}
\mathsf{pk}_0 &= (\mathbf{A}, \mathbf{u}), \\
\mathsf{pk} &= (\mathbf{B}, \mathbf{v}), \\
\mathsf{sk} &= \mathbf{r}', \\
\mathsf{ctxt} &\leftarrow \mathsf{Enc}((\mathbf{A}, \mathbf{u}), \mathsf{msg}_b), \\
\mathsf{up} &= \mathsf{Enc}((\mathbf{A}, \mathbf{u}), \rho^*);
\end{aligned}$$

$$\begin{aligned}
\mathbf{r}, \mathbf{r}' &\leftarrow\!\!\$\ \{\pm 1\}^n, \\
\mathbf{u}^{\mathrm{T}} &= \mathbf{r}^{\mathrm{T}} \cdot \mathbf{A}, \\
\mathbf{v}^{\mathrm{T}} &= \mathbf{r}'^{\mathrm{T}} \cdot \mathbf{B}
\end{aligned}$$

$\text{Game}_4 \approx \text{Game}_5$: The stars just about align

- Take a h-hollow PCE instance $(\mathbf{A}, \mathbf{B})$. Compute $\mathbf{a}^{\mathrm{T}} = \sum_{i=1}^{n} \mathbf{A}_i$ and $\mathbf{b}^{\mathrm{T}} = \sum_{i=1}^{n} \mathbf{B}_i$. Then $[1]^n$ is a valid secret for $(\mathbf{A}, \mathbf{a})$ and $(\mathbf{B}, \mathbf{b})$.

- Sample $\mathbf{O}_{\mathbf{A}}, \mathbf{O}_{\mathbf{B}} \leftarrow\$ \mathcal{O}_n(\mathbb{Z})$, $\mathbf{U}_{\mathbf{A}}, \mathbf{U}_{\mathbf{B}} \leftarrow\$ \mathcal{GL}_k(\mathbb{Z}_q)$, and compute

$$\begin{aligned} \mathbf{A}' &= \mathbf{O}_{\mathbf{A}} \cdot \mathbf{A} \cdot \mathbf{U}_{\mathbf{A}} & \mathbf{a}'^{\mathrm{T}} &= \mathbf{a}^{\mathrm{T}} \cdot \mathbf{U}_{\mathbf{A}} & \mathbf{r}_{\mathbf{A}} &= \mathbf{O}_{\mathbf{A}} \cdot [1]^n \\ \mathbf{B}' &= \mathbf{O}_{\mathbf{B}} \cdot \mathbf{B} \cdot \mathbf{U}_{\mathbf{B}} & \mathbf{b}'^{\mathrm{T}} &= \mathbf{b}^{\mathrm{T}} \cdot \mathbf{U}_{\mathbf{B}} & \mathbf{r}_{\mathbf{B}} &= \mathbf{O}_{\mathbf{B}} \cdot [1]^n \end{aligned}$$

- If $\mathbf{B} = \mathrm{SF}(\mathbf{P} \cdot \mathbf{A})$, then $\mathbf{O}_{\mathbf{B}} \cdot \mathbf{P} \cdot \mathbf{O}_{\mathbf{A}}^{-1}$ updates $((\mathbf{A}', \mathbf{a}'), \mathbf{r}_{\mathbf{A}})$ to $((\mathbf{B}', \mathbf{b}'), \mathbf{r}_{\mathbf{B}})$, since for any $\mathbf{P}$ we have $[1]^n = \mathbf{P} \cdot [1]^n$, otherwise random.

- Thus any distinguisher $\mathcal{D}_{4,5}$ also distinguishes PCE.

$\textsc{Game}_4 \approx \textsc{Game}_5$: The stars just about align

- Take a h-hollow PCE instance $(\mathbf{A}, \mathbf{B})$. Compute $\mathbf{a}^{\mathrm{T}} = \sum_{i=1}^{n} \mathbf{A}_i$ and $\mathbf{b}^{\mathrm{T}} = \sum_{i=1}^{n} \mathbf{B}_i$. Then $[1]^n$ is a valid secret for $(\mathbf{A}, \mathbf{a})$ and $(\mathbf{B}, \mathbf{b})$.

- Sample $\mathbf{O}_{\mathbf{A}}, \mathbf{O}_{\mathbf{B}} \leftarrow\!\!\$\ \mathcal{O}_n(\mathbb{Z})$, $\mathbf{U}_{\mathbf{A}}, \mathbf{U}_{\mathbf{B}} \leftarrow\!\!\$\ \mathcal{GL}_k(\mathbb{Z}_q)$, and compute

$$
\begin{aligned}
\mathbf{A}' &= \mathbf{O}_{\mathbf{A}} \cdot \mathbf{A} \cdot \mathbf{U}_{\mathbf{A}} & \mathbf{a}'^{\mathrm{T}} &= \mathbf{a}^{\mathrm{T}} \cdot \mathbf{U}_{\mathbf{A}} & \mathbf{r}_{\mathbf{A}} &= \mathbf{O}_{\mathbf{A}} \cdot [1]^n \\
\mathbf{B}' &= \mathbf{O}_{\mathbf{B}} \cdot \mathbf{B} \cdot \mathbf{U}_{\mathbf{B}} & \mathbf{b}'^{\mathrm{T}} &= \mathbf{b}^{\mathrm{T}} \cdot \mathbf{U}_{\mathbf{B}} & \mathbf{r}_{\mathbf{B}} &= \mathbf{O}_{\mathbf{B}} \cdot [1]^n
\end{aligned}
$$

- If $\mathbf{B} = \mathrm{SF}(\mathbf{P} \cdot \mathbf{A})$, then $\mathbf{O}_{\mathbf{B}} \cdot \mathbf{P} \cdot \mathbf{O}_{\mathbf{A}}^{-1}$ updates $((\mathbf{A}', \mathbf{a}'), \mathbf{r}_{\mathbf{A}})$ to $((\mathbf{B}', \mathbf{b}'), \mathbf{r}_{\mathbf{B}})$, since for any $\mathbf{P}$ we have $[1]^n = \mathbf{P} \cdot [1]^n$, otherwise random.

- Thus any distinguisher $\mathcal{D}_{4,5}$ also distinguishes PCE.

$\textsc{Game}_4 \approx \textsc{Game}_5$: The stars just about align

- Take a h-hollow PCE instance $(\mathbf{A}, \mathbf{B})$. Compute $\mathbf{a}^{\mathrm{T}} = \sum_{i=1}^{n} \mathbf{A}_i$ and $\mathbf{b}^{\mathrm{T}} = \sum_{i=1}^{n} \mathbf{B}_i$. Then $[1]^n$ is a valid secret for $(\mathbf{A}, \mathbf{a})$ and $(\mathbf{B}, \mathbf{b})$.

- Sample $\mathbf{O_A}, \mathbf{O_B} \leftarrow\$ \mathcal{O}_n(\mathbb{Z})$, $\mathbf{U_A}, \mathbf{U_B} \leftarrow\$ \mathcal{GL}_k(\mathbb{Z}_q)$, and compute

$$\begin{aligned} \mathbf{A}' &= \mathbf{O_A} \cdot \mathbf{A} \cdot \mathbf{U_A} & \quad \mathbf{a}'^{\mathrm{T}} &= \mathbf{a}^{\mathrm{T}} \cdot \mathbf{U_A} & \quad \mathbf{r_A} &= \mathbf{O_A} \cdot [1]^n \\ \mathbf{B}' &= \mathbf{O_B} \cdot \mathbf{B} \cdot \mathbf{U_B} & \quad \mathbf{b}'^{\mathrm{T}} &= \mathbf{b}^{\mathrm{T}} \cdot \mathbf{U_B} & \quad \mathbf{r_B} &= \mathbf{O_B} \cdot [1]^n \end{aligned}$$

- If $\mathbf{B} = \mathrm{SF}(\mathbf{P} \cdot \mathbf{A})$, then $\mathbf{O_B} \cdot \mathbf{P} \cdot \mathbf{O_A}^{-1}$ updates $((\mathbf{A}', \mathbf{a}'), \mathbf{r_A})$ to $((\mathbf{B}', \mathbf{b}'), \mathbf{r_B})$, since for any $\mathbf{P}$ we have $[1]^n = \mathbf{P} \cdot [1]^n$, otherwise random.

- Thus any distinguisher $\mathcal{D}_{4,5}$ also distinguishes PCE.

$\textsc{Game}_4 \approx \textsc{Game}_5$: THE STARS JUST ABOUT ALIGN

- Take a h-hollow PCE instance $(\mathbf{A}, \mathbf{B})$. Compute $\mathbf{a}^{\mathrm{T}} = \sum_{i=1}^{n} \mathbf{A}_i$ and $\mathbf{b}^{\mathrm{T}} = \sum_{i=1}^{n} \mathbf{B}_i$. Then $[1]^n$ is a valid secret for $(\mathbf{A}, \mathbf{a})$ and $(\mathbf{B}, \mathbf{b})$.

- Sample $\mathbf{O}_{\mathbf{A}}, \mathbf{O}_{\mathbf{B}} \leftarrow\$ \mathcal{O}_n(\mathbb{Z})$, $\mathbf{U}_{\mathbf{A}}, \mathbf{U}_{\mathbf{B}} \leftarrow\$ \mathcal{GL}_k(\mathbb{Z}_q)$, and compute

$$\begin{aligned} \mathbf{A}' &= \mathbf{O}_{\mathbf{A}} \cdot \mathbf{A} \cdot \mathbf{U}_{\mathbf{A}} & \mathbf{a}'^{\mathrm{T}} &= \mathbf{a}^{\mathrm{T}} \cdot \mathbf{U}_{\mathbf{A}} & \mathbf{r}_{\mathbf{A}} &= \mathbf{O}_{\mathbf{A}} \cdot [1]^n \\ \mathbf{B}' &= \mathbf{O}_{\mathbf{B}} \cdot \mathbf{B} \cdot \mathbf{U}_{\mathbf{B}} & \mathbf{b}'^{\mathrm{T}} &= \mathbf{b}^{\mathrm{T}} \cdot \mathbf{U}_{\mathbf{B}} & \mathbf{r}_{\mathbf{B}} &= \mathbf{O}_{\mathbf{B}} \cdot [1]^n \end{aligned}$$

- If $\mathbf{B} = \mathrm{SF}(\mathbf{P} \cdot \mathbf{A})$, then $\mathbf{O}_{\mathbf{B}} \cdot \mathbf{P} \cdot \mathbf{O}_{\mathbf{A}}^{-1}$ updates $((\mathbf{A}', \mathbf{a}'), \mathbf{r}_{\mathbf{A}})$ to $((\mathbf{B}', \mathbf{b}'), \mathbf{r}_{\mathbf{B}})$, since for any $\mathbf{P}$ we have $[1]^n = \mathbf{P} \cdot [1]^n$, otherwise random.

- Thus any distinguisher $\mathcal{D}_{4,5}$ also distinguishes PCE.

Some Parameters and Sizes

Table 1: Parameters for the given λ and p with $c = 0.25$ and $s = 8$.

λ	p	n	k	$\log_2(q)$	h	$\|\text{ctxt}\|$	$\|\text{up}\|$
128	2	7313	450	13	27	11.6 KiB	1485.7 KiB
128	16	11000	550	16	26	21.5 KiB	687.6 KiB
192	32	20250	900	18	37	44.5 KiB	1708.7 KiB
256	32	29688	1250	19	48	68.9 KiB	3525.6 KiB
[HPS23] with 2^{20} updates							
128	–	–	–	36	–	9.1 KiB	27 KiB

Future Work

- Replace the Hollow LHL with a computational assumption.
- Switch from LWE to MLWE.
- Consider the model from [AFM24].
- …

Thank you! Read the full version at ia.cr/2025/340:

Bibliography I

Joël Alwen, Georg Fuchsbauer, and Marta Mularczyk.
Updatable public-key encryption, revisited.
In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part VII*, volume 14657 of *LNCS*, pages 346–376. Springer, Cham, May 2024.

Magali Bardet, Ayoub Otmani, and Mohamed Saeed-Taha.
Permutation Code Equivalence is Not Harder Than Graph Isomorphism When Hulls Are Trivial.
In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 2464–2468. IEEE, 2019.

Herrn Chevalley and Ewald Warning.
Bemerkung zur vorstehenden Arbeit von Herrn Chevalley.
Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, 11(1):76–83, 1935.

Bibliography II

- Yevgeniy Dodis, Harish Karthikeyan, and Daniel Wichs.
  Updatable public key encryption in the standard model.
  In Kobbi Nissim and Brent Waters, editors, *TCC 2021, Part III*, volume 13044 of *LNCS*, pages 254–285. Springer, Cham, November 2021.
- Léo Ducas and Wessel P. J. van Woerden.
  On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography.
  In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part III*, volume 13277 of *LNCS*, pages 643–673. Springer, Cham, May / June 2022.
- Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan.
  Trapdoors for hard lattices and new cryptographic constructions.
  In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.

Bibliography III

Calvin Abou Haidar, Alain Passelègue, and Damien Stehlé.
Efficient updatable public-key encryption from lattices.
In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part V*, volume 14442 of *LNCS*, pages 342–373. Springer, Singapore, December 2023.

Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.
In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.

Nicolas Sendrier.
On the Dimension of the Hull.
SIAM Journal on Discrete Mathematics, 10(2):282–293, 1997.

Bibliography IV

Nicolas Sendrier.
Finding the permutation between equivalent linear codes: the support splitting algorithm.
IEEE Transactions on Information Theory, 46(4):1193–1203, 2000.