Bounded CCA2-secure Proxy Re-encryption from Lattices

Shingo Sato, Junji Shikata

Yokohama National University

August 15, 2025

Overview of Our Result

Background and Our Goal

Propose a bounded CCA2-secure post-quantum proxy re-encryption (PRE).

- PRE: Public key encryption that converts ciphertexts under a public key into ciphertexts under another public key.
- No existing CCA2-secure post-quantum PRE.

Overview of our Result

- Introduce the notion of bounded CCA2 security for PRE;
- Propose a generic construction of bounded CCA2-secure PRE starting from CPA-secure PRE with an additional property;
- Propose a lattice-based PRE with required security.

Proxy Re-encryption (PRE)

- Public key cryptosystem that allows a proxy to convert ciphertexts under pk_A into ciphertexts under pk_B.
- Applications: e-mail forwarding, encrypted data storage, etc.

$(\mathsf{pk}_A, \mathsf{sk}_A)$: User A's public/secret key-pair

$(\mathsf{pk}_B, \mathsf{sk}_B)$: User B's public/secret key-pair

$\mathsf{rk}_{A \to B}$: A re-encryption key from pk_A into pk_B

Proxy

Re-encryption procedure

$\mathsf{ct}_B \leftarrow \mathsf{ReEnc}(\mathsf{rk}_{A \to B}, \mathsf{ct}_A)$

ct_A s.t.
$\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}_A, \mathsf{ct}_A)$

ct_B s.t.
$\mathsf{m} \leftarrow \mathsf{Dec}(\mathsf{sk}_B, \mathsf{ct}_B)$

Classification of PRE

Focus on single-hop unidirectional PRE.

Unidirectional vs. Bidirectional

- Unidirectional: $\mathsf{rk}_{A \to B} \leftarrow \mathsf{ReKeyGen}(\mathsf{sk}_A, \mathsf{pk}_B)$ allows only re-encryption from pk_A into pk_B.
- Bidirectional: $\mathsf{rk}_{A \to B} \leftarrow \mathsf{ReKeyGen}(\mathsf{sk}_A, \mathsf{sk}_B)$ also allows re-encryption from pk_B into pk_A.

Single-hop vs. Multi-hop

- Single-hop: ct_B cannot be re-encrypted to other ciphertexts.
- Multi-hop: ct_B can be re-encrypted into ciphertexts under another public key.

Here, $\mathsf{ct}_B \leftarrow \mathsf{ReEnc}(\mathsf{rk}_{A \to B}, \mathsf{Enc}(\mathsf{pk}_A, \mathsf{m}))$.

Existing Post-Quantum PRE Schemes

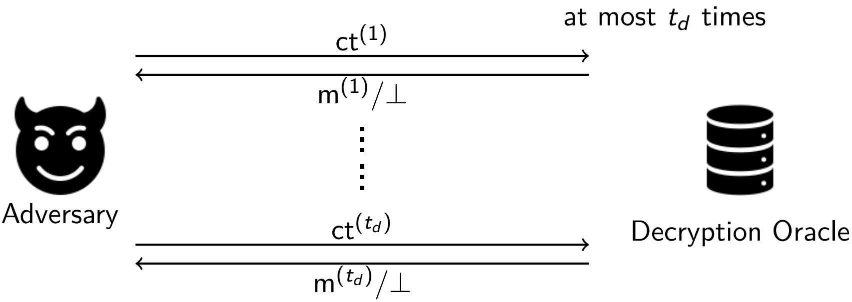
There is no CCA2-secure post-quantum PRE scheme.

Scheme	Security	Assumption	Dir.	# of Hops
[CCL+14]	CPA	LWE	Uni	Multi
[PRSV17]	CPA	Ring-LWE	Uni	Multi
[FKKP19]	(adaptive) HRA	LWE	Uni	Multi
[FL19]	CCA1	LWE	Uni	Multi
[ZLHZ23]	CPA	LWE	Uni	Single
[ZJZ24]	HRA	LWE	Uni	Multi
[WWXW25]	(adaptive) HRA	LWE	Uni	(unbounded) Multi

- CPA and CCA1 are strictly weaker than CCA2.
- The relationship between CCA2 and HRA is unknown:
  - HRA is strictly stronger than CPA.
  - But, the adversary is not given any access to the decryption oracle.

Bounded CCA2 Security for Public Key Encryption

- A weak variant of CCA2 security for public key encryption (PKE)
- The number of decryption queries is at most a-priori parameter $t_d = O(1)$ (called a collusion parameter).



Generic constructions from CPA-secure PKE have been proposed so far. There are several practical applications.

Our Contribution

Goal

Propose a bounded CCA2-secure post-quantum PRE with compact ciphertexts.

- Bounded CCA2 security: provides a sufficiently wide range of applications.
- Compact ciphertexts: ciphertext-size does not depend on collusion parameters, linearly.

Contribution

- Formalize the notion of bounded CCA2 security for PRE;
- Propose a generic construction of bounded CCA2-secure PRE with compact ciphertexts starting from CPA-secure PRE with our introduced property;
- Propose a lattice-based PRE with required properties;

Definition of PRE

Definition (Syntax of PRE (informal))

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$;
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{m}) \to \mathsf{ct}$;
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to \mathsf{m}/\bot$;
- $\mathsf{ReKeyGen}(\mathsf{sk}_A, \mathsf{pk}_B) \to \mathsf{rk}_{A\to B}$;
- $\mathsf{ReEnc}(\mathsf{rk}_{A\to B}, \mathsf{ct}_A) \to \mathsf{ct}_B$.

$\mathsf{pk}, \mathsf{pk}_A, \mathsf{pk}_B$: public keys; $\mathsf{sk}, \mathsf{sk}_A, \mathsf{sk}_B$: secret keys; m: message; ct: ciphertext; $\bot$: rejection symbol; $\mathsf{rk}_{A\to B}$: a re-encryption key.

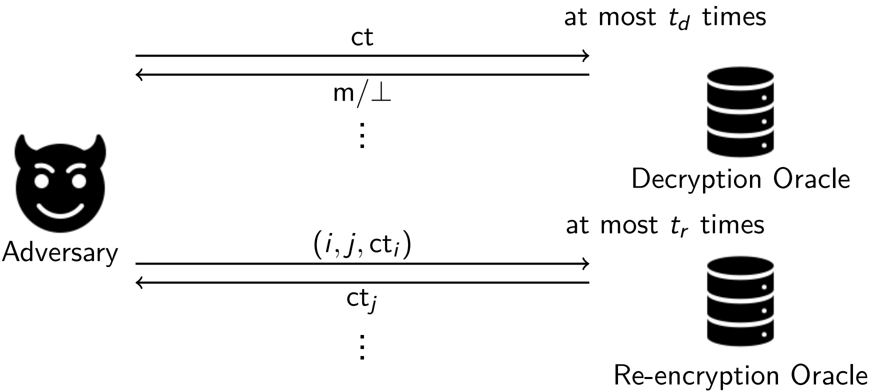
Re-encryption correctness

$$\mathsf{Dec}(\mathsf{sk}_B, \mathsf{ReEnc}(\mathsf{rk}_{A\to B}, \mathsf{ct}_A)) = \mathsf{m}$$

holds for all $\mathsf{ct}_A \leftarrow \mathsf{Enc}(\mathsf{pk}_A, \mathsf{m})$ and $\mathsf{rk}_{A\to B} \leftarrow \mathsf{ReKeyGen}(\mathsf{sk}_A, \mathsf{pk}_B)$.

Bounded CCA2 Security for PRE

- The numbers of decryption queries and re-encryption queries are at most a-priori parameters $t_d = O(1)$ and $t_r = O(1)$, respectively.



The CCA2 security in the game above is called (t_d, t_r)-CCA2 security.

Building Blocks of Our Basic PRE

Building blocks

- CPA-secure PRE $\mathsf{PRE}_{\mathsf{CPA}}$;
- Strongly unforgeable one-time signatures OTS;
- Cover-free families (CFFs)

Definition (($\bar{n}, u, t$)-CFF)

$\exists$ a function $\phi : \{1, \ldots, \bar{n}\}$(an identity space) $\to$ (a subset of $\{1, \ldots, u\}$) (where $u \ll \bar{n}$) s.t.

$$\phi(\mathsf{id}^*) \notin \phi(\mathsf{id}^{(1)}) \cup \ldots \cup \phi(\mathsf{id}^{(t)})$$

for all

- $\mathsf{id}^{(1)}, \ldots, \mathsf{id}^{(t)} \in \{1, \ldots, \bar{n}\}$ and
- $\mathsf{id}^* \notin \{1, \ldots, \bar{n}\} \backslash \{\mathsf{id}^{(1)}, \ldots, \mathsf{id}^{(t)}\}$.

Basic Generic Construction from CPA-secure PRE (1/2)

We consider the following trivial construction which is based on the existing bounded CCA2-secure PKE [CHH+07]:

- $\mathsf{pk} = (\mathsf{PRE}_{\mathsf{CPA}}.\mathsf{pk}_1, \ldots, \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{pk}_u)$;
- $\mathsf{sk} = (\mathsf{PRE}_{\mathsf{CPA}}.\mathsf{sk}_1, \ldots, \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{sk}_u)$;
- $\mathsf{ct} = (\mathsf{OTS.vk}, \mathsf{ct}_{\mathsf{vk}}, \mathsf{OTS}.\sigma)$:
    1. $(\mathsf{OTS.vk}, \mathsf{OTS.sigk}) \leftarrow \mathsf{OTS.KeyGen}$;
    2. $\mathsf{ct}_{\mathsf{vk}} = (\mathsf{PRE}_{\mathsf{CPA}}.\mathsf{ct}_1, \ldots, \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{ct}_v)$: Enc, associated with OTS.vk.
        1. $\phi(\mathsf{OTS.vk}) := \{\tau_1, \ldots, \tau_v\} \subseteq \{1, \ldots, u\}$;
        2. Sample random values $(x_1 \ldots, x_v)$ s.t. $x_1 \oplus \cdots \oplus x_v = \mathsf{m}$;
        3. $\forall i \in \{1, \ldots, v\}$, $\mathsf{PRE}_{\mathsf{CPA}}.\mathsf{ct}_i \leftarrow \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{Enc}(\mathsf{PRE}_{\mathsf{CPA}}.\mathsf{pk}_{\tau_i}, x_i)$;
    3. $\mathsf{OTS}.\sigma \leftarrow \mathsf{OTS.Sign}(\mathsf{OTS.sigk}, \mathsf{ct}_{\mathsf{vk}})$;

Basic Generic Construction from CPA-secure PRE (2/2)

Re-encryption key generation (ReKeyGen)

- $\mathsf{rk}_{A\to B} = (\mathsf{rk}_{i\to j})_{i,j\in\{1,\ldots,u\}}$:
  - $\mathsf{rk}_{i\to j} \leftarrow \mathsf{PRE_{CPA}.ReKeyGen}(\mathsf{PRE_{CPA}.sk}_{A,i}, \mathsf{PRE_{CPA}.pk}_{B,j})$.

  for $\mathsf{sk}_A = (\mathsf{PRE_{CPA}.sk}_{A,1}, \ldots, \mathsf{PRE_{CPA}.sk}_{A,u})$ and $\mathsf{pk}_B = (\mathsf{PRE_{CPA}.pk}_{B,1}, \ldots, \mathsf{PRE_{CPA}.pk}_{B,u})$.

Re-encryption (ReEnc):

$\mathsf{ct}_A = (\mathsf{OTS.vk}_A, \mathsf{ct}_{\mathsf{vk}_A}, \mathsf{OTS}.\sigma_A) \Rightarrow \mathsf{ct}_B = (\mathsf{OTS.vk}_B, \mathsf{ct}_{\mathsf{vk}_B}, \mathsf{OTS}.\sigma_B)$

1. $(\mathsf{OTS.vk}_B, \mathsf{OTS.sigk}_B) \leftarrow \mathsf{OTS.KeyGen}$;
2. $\mathsf{ct}_{\mathsf{vk}_B} = (\mathsf{PRE_{CPA}.ct}_{B,1}, \ldots, \mathsf{PRE_{CPA}.ct}_{B,v})$:
   1. $\phi(\mathsf{OTS.vk}_A) := \{\alpha_1, \ldots, \alpha_v\}$ and $\phi(\mathsf{OTS.vk}_B) := \{\beta_1, \ldots, \beta_v\}$;
   2. $\forall i \in \{1, \ldots, v\}$,
      $\mathsf{PRE_{CPA}.ct}_{B,i} \leftarrow \mathsf{PRE_{CPA}.ReEnc}(\mathsf{rk}_{\alpha_i\to\beta_i}, \mathsf{PRE_{CPA}.ct}_{A,i})$.
3. $\mathsf{OTS}.\sigma_B \leftarrow \mathsf{OTS.Sign}(\mathsf{OTS.sigk}_B, \mathsf{ct}_{\mathsf{vk}_B})$.

Requirement to satisfy Compact Ciphertexts (1/2)

Purpose

For a ciphertext $\mathsf{ct} = (\mathsf{OTS.vk}, \mathsf{ct}_{\mathsf{vk}}, \mathsf{OTS}.\sigma)$, compress $\mathsf{ct}_{\mathsf{vk}} = (\mathsf{PRE}_{\mathsf{CPA}}.\mathsf{ct}_1, \ldots, \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{ct}_v)$ into a single ciphertext.

We consider the following compression:

$$\mathsf{pk}_{\mathsf{vk}} \leftarrow \sum_{i \in \{1,\ldots,v\}} \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{pk}_{\tau_i};$$

$$\mathsf{ct}_{\mathsf{vk}} \leftarrow \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{Enc}(\mathsf{pk}_{\mathsf{vk}}, \mathsf{m}).$$

The first attempt

Require for $\mathsf{PRE}_{\mathsf{CPA}}$ to satisfy public-to-secret key homomorphism [TW14]:

$$\mathsf{Dec}(\mathsf{sk}_{\mathsf{vk}}, \mathsf{ct}_{\mathsf{vk}}) = \mathsf{m}$$

holds for $\mathsf{sk}_{\mathsf{vk}} = \sum_{i \in \{1,\ldots,v\}} \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{sk}_{\tau_i}$.

Requirement to satisfy Compact Ciphertexts (2/2)

The algorithm Dec works for original ciphertexts in the same way as the bounded CCA2-secure PKE [TW14].

However, such homomorphism is not enough for generating or decrypting re-encrypted ciphertexts.

- Consider re-encrypting a ciphertext $\mathsf{ct}_A = (\mathsf{OTS.vk}_A, \mathsf{ct}_{\mathsf{vk}_A}, \mathsf{OTS}.\sigma_A)$ by using re-encryption keys $\mathsf{rk}_{\alpha_i \to \beta_i}$.
- But $\mathsf{ct}_{\mathsf{vk}_A} \leftarrow \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{Enc}(\mathsf{pk}_{\mathsf{vk}_A}, \mathsf{m})$ is compressed into a single ciphertext.
  $\Rightarrow$ Cannot run $\mathsf{PRE}_{\mathsf{CPA}}.\mathsf{ReEnc}(\mathsf{rk}_{\alpha_i \to \beta_i}, \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{ct}_{A,i})$.

Key-homomorphism for PRE

We introduce a new notion of PRE so that we can compute compact re-encrypted ciphertexts.

Re-encryption key homomorphism (informal)

$$\mathsf{rk}_{\mathsf{vk}_A \to \mathsf{vk}_B} = \sum_{i \in \{1,\dots,v\}} \mathsf{rk}_{\alpha_i \to \beta_i}; \text{ and}$$

$$\mathsf{Dec}(\mathsf{sk}_{\mathsf{vk}_B}, \mathsf{ReEnc}(\mathsf{rk}_{\mathsf{vk}_A \to \mathsf{vk}_B}, \mathsf{ct}_{\mathsf{vk}_A})) = \mathsf{m}$$

hold for

- $\mathsf{ct}_{\mathsf{vk}_A} \leftarrow \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{Enc}(\mathsf{pk}_{\mathsf{vk}_A}, \mathsf{m})$;
- $\mathsf{pk}_{\mathsf{vk}_A} \leftarrow \sum_{i \in \{1,\dots,v\}} \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{pk}_{\alpha_i}$;
- $\mathsf{sk}_{\mathsf{vk}_B} \leftarrow \sum_{i \in \{1,\dots,v\}} \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{sk}_{\beta_i}$.

Our Generic Construction with Compact Ciphertexts (1/2)

- $\mathsf{pk} = (\mathsf{PRE}_{\mathsf{CPA}}.\mathsf{pk}_1, \ldots, \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{pk}_u)$;
- $\mathsf{sk} = (\mathsf{PRE}_{\mathsf{CPA}}.\mathsf{sk}_1, \ldots, \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{sk}_u)$;
- $\mathsf{ct} = (\mathsf{OTS.vk}, \mathsf{ct}_{\mathsf{vk}}, \mathsf{OTS}.\sigma)$:
  1. $(\mathsf{OTS.vk}, \mathsf{OTS.sigk}) \leftarrow \mathsf{OTS.KeyGen}$;
  2. Compute $\mathsf{ct}_{\mathsf{vk}}$: Enc of a message m.
     1. $\phi(\mathsf{OTS.vk}) := \{\tau_1, \ldots, \tau_v\}$;
     2. $\mathsf{pk}_{\mathsf{vk}} \leftarrow \sum_{i \in \{1,\ldots,v\}} \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{pk}_{\tau_i}$.
     3. $\mathsf{ct}_{\mathsf{vk}} \leftarrow \mathsf{PRE.Enc}(\mathsf{pk}_{\mathsf{vk}}, \mathsf{m})$;
  3. $\mathsf{OTS}.\sigma \leftarrow \mathsf{OTS.Sign}(\mathsf{OTS.sigk}, \mathsf{ct}_{\mathsf{vk}})$;

Re-encryption key generation

- $\mathsf{rk}_{A \to B} = (\mathsf{rk}_{i \to j})_{i,j \in \{1,\ldots,u\}}$:
  - $\mathsf{rk}_{i \to j} \leftarrow \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{ReKeyGen}(\mathsf{PRE}_{\mathsf{CPA}}.\mathsf{sk}_{A,i}, \mathsf{PRE}_{\mathsf{CPA}}.\mathsf{sk}_{B,j})$.

Our Generic Construction with Compact Ciphertexts (2/2)

Re-encryption:

$\mathsf{ct}_A = (\mathsf{OTS.vk}_A, \mathsf{ct}_{\mathsf{vk}_A}, \mathsf{OTS}.\sigma_A) \Rightarrow \mathsf{ct}_B = (\mathsf{OTS.vk}_B, \mathsf{ct}_{\mathsf{vk}_B}, \mathsf{OTS}.\sigma_B)$

1. $(\mathsf{OTS.vk}_B, \mathsf{OTS.sigk}_B) \leftarrow \mathsf{OTS.KeyGen}$;
2. Generation of $\mathsf{ct}_{\mathsf{vk}_B}$:
   1. $\phi(\mathsf{OTS.vk}_A) := \{\alpha_1, \ldots, \alpha_v\}$ and $\phi(\mathsf{OTS.vk}_B) := \{\beta_1, \ldots, \beta_v\}$;
   2. $\mathsf{rk}_{\mathsf{vk}_A \to \mathsf{vk}_B} \leftarrow \sum_{i \in \{1,\ldots,v\}} \mathsf{rk}_{\alpha_i \to \beta_i}$;
   3. $\mathsf{ct}_{\mathsf{vk}_B} \leftarrow \mathsf{PRE_{CPA}.ReEnc}(\mathsf{rk}_{\mathsf{vk}_A \to \mathsf{vk}_B}, \mathsf{ct}_{\mathsf{vk}_A})$;
3. $\mathsf{OTS}.\sigma_B \leftarrow \mathsf{OTS.Sign}(\mathsf{OTS.sigk}_B, \mathsf{PRE_{CPA}.ct}_{\mathsf{vk}_B})$.

Theorem (Security of the proposed PRE)

Assume that

- $\mathsf{PRE_{CPA}}$ *is* CPA *secure and* re-encryption key homomorphic*;*
- OTS *is* strongly unforgeable*; and*
- ϕ *is* $(\bar{n}, u, t)$*-CFF.*

Then the proposed PRE scheme is (t, t)-CCA2*-secure.*

Lattice-based PRE with CPA Security and Re-encryption Key homomorphism

- KeyGen, Enc and Dec of our PRE scheme L-PRE are the same as those of ML-KEM.K-PKE (except for using compression functions).
- ReKeyGen and ReEnc are constructed so that L-PRE is re-encryption key homomorphic.

Theorem (Security of L-PRE)

- L-PRE *is* CPA *secure under the module-LWE assumption, and* re-encryption key homomorphic*.*
- *In particular, assuming the adversary* $\mathcal{A}$ *against* L-PRE*, there exists a reduction algorithm* $\mathcal{B}$ *against module-LWE such that*

$$\mathsf{Adv}^{\text{ind-cpa}}_{\text{L-PRE},\mathcal{A},n}(\lambda) \leq O(n_h \cdot q_{rk}) \cdot \mathsf{Adv}^{\text{mlwe}}_{\mathcal{B}}(\lambda),$$

where n_h *is the number of honest users and* q_{rk} *is the number of re-encryption key queries.*

Conclusion

- Proposed a generic construction of bounded CCA2-secure PRE with compact ciphertexts:
  - Introduced the notion of bounded CCA2 security for PRE;
  - Proposed a generic construction from CPA-secure PRE with our introduced key-homomorphism, and OTS;
- Presented lattice-based PRE with required properties;
- As a result, we can obtain a bounded CCA2-secure post-quantum PRE with compact ciphertexts by using
  - our proposed lattice-based PRE; and
  - a lattice-based OTS scheme [LM08, LM18].

Conclusion

- Proposed a generic construction of bounded CCA2-secure PRE with compact ciphertexts:
  - Introduced the notion of bounded CCA2 security for PRE;
  - Proposed a generic construction from CPA-secure PRE with our introduced key-homomorphism, and OTS;
- Presented lattice-based PRE with required properties;
- As a result, we can obtain a bounded CCA2-secure post-quantum PRE with compact ciphertexts by using
  - our proposed lattice-based PRE; and
  - a lattice-based OTS scheme [LM08, LM18].

Thank you!

References I

[CCL+14] Nishanth Chandran, Melissa Chase, Feng-Hao Liu, Ryo Nishimaki, and Keita Xagawa, *Re-encryption, functional re-encryption, and multi-hop re-encryption: A framework for achieving obfuscation-based security and instantiations from lattices*, Public Key Cryptography, LNCS, vol. 8383, Springer, 2014, pp. 95–112.

[CHH+07] Ronald Cramer, Goichiro Hanaoka, Dennis Hofheinz, Hideki Imai, Eike Kiltz, Rafael Pass, Abhi Shelat, and Vinod Vaikuntanathan, *Bounded cca2-secure encryption*, ASIACRYPT, LNCS, vol. 4833, Springer, 2007, pp. 502–518.

[FKKP19] Georg Fuchsbauer, Chethan Kamath, Karen Klein, and Krzysztof Pietrzak, *Adaptively secure proxy re-encryption*, Public Key Cryptography (2), LNCS, vol. 11443, Springer, 2019, pp. 317–346.

[FL19] Xiong Fan and Feng-Hao Liu, *Proxy re-encryption and re-signatures from lattices*, ACNS, LNCS, vol. 11464, Springer, 2019, pp. 363–382.

[LM08] Vadim Lyubashevsky and Daniele Micciancio, *Asymptotically efficient lattice-based digital signatures*, TCC, LNCS, vol. 4948, Springer, 2008, pp. 37–54.

[LM18] ———, *Asymptotically efficient lattice-based digital signatures*, J. Cryptol. **31** (2018), no. 3, 774–797.

[PRSV17] Yuriy Polyakov, Kurt Rohloff, Gyana Sahu, and Vinod Vaikuntanathan, *Fast proxy re-encryption for publish/subscribe systems*, ACM Trans. Priv. Secur. **20** (2017), no. 4, 14:1–14:31.

References II

[TW14] Stefano Tessaro and David A. Wilson, *Bounded-collusion identity-based encryption from semantically-secure public-key encryption: Generic constructions with short ciphertexts*, Public Key Cryptography, LNCS, vol. 8383, Springer, 2014, pp. 257–274.

[WWXW25] Xiaohan Wan, Yang Wang, Haiyang Xue, and Mingqiang Wang, *Unbounded multi-hop proxy re-encryption with HRA security: An lwe-based optimization*, ACISP (2), LNCS, vol. 15659, Springer, 2025, pp. 124–144.

[ZJZ24] Biming Zhou, Haodong Jiang, and Yunlei Zhao, *Cpa-secure kems are also sufficient for post-quantum TLS 1.3*, ASIACRYPT (3), LNCS, vol. 15486, Springer, 2024, pp. 433–464.

[ZLHZ23] Yunxiao Zhou, Shengli Liu, Shuai Han, and Haibin Zhang, *Fine-grained proxy re-encryption: Definitions and constructions from LWE*, ASIACRYPT (6), LNCS, vol. 14443, Springer, 2023, pp. 199–231.