

**“Preview Writeup”:** In anticipation of a package submission to the NIST Threshold Call

**Title:** Adamas: One-Round Lattice-Based Threshold KEM and PKE under Adaptive Corruptions

**Version:** Preview Writeup 0.1 (2026-10-08)<sup>1</sup>

**Team name:** Adamas

**Team members:** Shengli Liu, Shuai Han, Yunxin Zhang, Yunxiao Zhou

**Abstract:** This document previews Adamas, a family of one-round lattice-based  $(t, N)$ -threshold key encapsulation mechanism (TKEM) and public-key encryption (TPKE) schemes. In our Adamas family, the secret key is distributed among  $N$  parties, and any subset of at least  $t$  parties can jointly recover the encapsulated key/message from a ciphertext.

Our Adamas family comprises two TKEM schemes and one TPKE scheme with the following properties: (i) all schemes support *one-round* threshold decryption, requiring only a single round of message transmission; (ii) all schemes achieve CCA security (i.e., security against chosen-ciphertext attacks) and active security under *adaptive* corruptions, where the adversary may adaptively issue both partial decryption and corruption queries throughout the security experiment; (iii) all schemes are based on standard structured-lattice assumptions and enjoy *polynomial modulus*.

Technically speaking, the Adamas family consists of threshold variants of Regev-style encryption schemes augmented with non-interactive zero-knowledge (NIZK) proofs. The constructions leverage several techniques to achieve CCA security under adaptive corruptions in the threshold setting while maintaining efficiency. For active security, we use the Fujisaki-Okamoto (FO) transform to achieve security-with-abort in the threshold setting for our TKEM schemes and use NIZK proofs to achieve stronger robustness for our TPKE scheme. As a result, Adamas provides relatively efficient TKEM and TPKE schemes that support non-interactive decryption, CCA security and active security under adaptive corruptions.

**Proposed crypto-systems:** (I) Adamas.TKEM<sub>1</sub> (Categories S2); (II) Adamas.TKEM<sub>2</sub> (Categories S2); (III) Adamas.TPKE (Categories S2).

**Keywords:** Threshold Decryption; NIST Threshold Call; Dual-Regev Encryption; NIZK Proofs; Adaptive Corruptions



(Logo AI-generated with ChatGPT)

<sup>1</sup>Preliminary version submitted to NIST-MPTC for review

**Preview writeup.** This document is provided to NIST for online publication, to foster public awareness and support public discussion within the scope of the NIST First Call for Multi-Party Threshold Schemes [NIST-IR8214C]. This “preview writeup” represents a good-faith plan for a subsequent “package submission”. However, until the deadline for package submission, the team may still modify its own composition and the submission plan, including possible changes to the technical scope, and/or the used techniques or achieved results.

**Team members:** Shengli Liu <sup>i1,a1</sup>, Shuai Han <sup>i2,a1</sup>, Yunxin Zhang <sup>i3,a1\*</sup>, Yunxiao Zhou <sup>i4,a1\*</sup>

**Open Researcher and Contributor Identifiers (ORCID):**

i1 (0000-0003-1366-8256); i2 (0000-0002-8156-7089); i3 (0009-0004-2117-2693); i4 (0009-0009-0134-2874)

**Affiliations:**

<sup>a1</sup> Shanghai Jiao Tong University @ Shanghai, China

**Associateship clarifications:**

\* Ph.D student (non-employee).

**Main contacts:**

- **Team mailing list:** team-lhzz@googlegroups.com
- **Primary technical contact person:** Shengli Liu, slliu@sjtu.edu.cn
- **Secondary contact person 1:** Shuai Han, dalen17@sjtu.edu.cn
- **Secondary contact person 2:** Yuxin Zhang, yuxin.zhang@sjtu.edu.cn
- **Secondary contact person 3:** Yunxiao Zhou, cloudzhou@sjtu.edu.cn

**Produced by humans.** The team hereby confirms that the content in this preview writeup: (i) was produced by the team members, and (ii) was not produced by generative artificial intelligence (AI), with the possible exception of AI-proposed grammar improvements, minor integrated suggestions, or some well-identified and short localized portions of auxiliary content (e.g., some illustration); and (iii) was proofread by the team members.

# 1. Introduction

This preview writeup introduces Adamas, a family of one-round threshold key encapsulation mechanism (TKEM) and public-key encryption (TPKE) schemes achieving CCA security<sup>2</sup> and active security under adaptive corruptions from the MLWE and MSIS assumptions, based on a recent work [ZZHLH26]. Adamas comprises two TKEM schemes  $\text{TKEM}_1$ ,  $\text{TKEM}_2$  and one TPKE scheme, all built from Regev-style encryption schemes [Reg05; GPV08; LP11] and non-interactive zero-knowledge (NIZK) proofs. For thresholdization,  $\text{TKEM}_1$  uses the Shamir secret sharing (SSS) [Sha79] and supports *synchronous* decryption<sup>3</sup> for large-scale parties, while  $\text{TKEM}_2$  and TPKE use the replicated secret sharing (RSS) [SN87] and support *asynchronous* decryption for small-scale parties.

The NIST Threshold Call [NIST-IR8214C, § 9.2.4.2] expresses a strong preference for provable security under adaptive corruptions w.r.t. critical safety properties. Security under adaptive corruptions is also particularly relevant to real-world TKEM/TPKE deployments, as practical adversaries are more likely to choose corruption targets dynamically based on observed ciphertexts, partial decryptions and system behavior, rather than fixing them before the protocol begins.

Our main design goal is to achieve CCA security under adaptive corruptions for TKEM/TPKE, while supporting one-round decryption and maintaining efficiency. All our schemes are threshold variants of Regev-style encryption augmented with NIZK proofs. To achieve CCA security under adaptive corruptions efficiently, we leverage polynomial flooding techniques and develop refined security analysis, which enable our schemes to use polynomial-sized smudging noise (rather than exponential ones) to limit the leakage of secret-key shares, thus enjoying polynomial modulus. To further improve efficiency,  $\text{TKEM}_1$  uses the optimized Regev encryption variant [LP11]. For active security,  $\text{TKEM}_1$  and  $\text{TKEM}_2$  achieve security-with-abort based on the Fujisaki-Okamoto (FO) transform [FO99; FO13], and TPKE achieves stronger robustness based on NIZK proofs.

Our submission focus on TKEM/TPKE from lattices, aligning with Category S2 of NIST Threshold call [NIST-IR8214C]: threshold post-quantum KEM/PKE that are not standardized by NIST.

## 2. Specification

### 2.1. Organization

This specification presents three candidate schemes  $\text{TKEM}_1$ ,  $\text{TKEM}_2$  and TPKE for S2, which cover threshold constructions for conventional primitives that have not been standardized by NIST. All schemes follow a common design framework, achieving one-round threshold decryption, CCA security and active security under adaptive corruptions, but they differ substantially in their efficiency, supported party scale, decryption setting and achieved active security, as summarized in Table 1. The first candidate  $\text{TKEM}_1$  uses Shamir secret sharing (SSS) for thresholdization,

<sup>2</sup>“CCA security” means CCA2 security, where the adversary can make decryption queries throughout the experiment.

<sup>3</sup>For simplicity, we use “decryption” to denote both decapsulation for TKEM and decryption for TPKE.

whereas TKEM<sub>2</sub> and TPKE use replicated secret sharing (RSS). By submitting all three schemes, we seek feedback from the community to determine which design offers a more compelling balance of security, performance and scalability for further consideration.

**SSS-based Scheme TKEM<sub>1</sub>.** The SSS-based TKEM<sub>1</sub> achieves CCA security and security-with-abort under adaptive corruptions, and supports synchronous decryption for large-scale parties.

**RSS-based Schemes TKEM<sub>2</sub> and TPKE.** The RSS-based TKEM<sub>2</sub> and TPKE achieve CCA security under adaptive corruptions and asynchronous decryption, but are practical only for small party number  $N$  since the number of shares per party is  $\binom{N-1}{t-1}$ . For active security, TKEM<sub>2</sub> achieves security-with-abort while TPKE achieves robustness, both under adaptive corruptions.

Table 1: Properties of our three schemes.

| Scheme            | Secret Sharing | Security | Corruptions | Supported Parties | #Shares per Party  | Decryption Setting | Active Security     |
|-------------------|----------------|----------|-------------|-------------------|--------------------|--------------------|---------------------|
| TKEM <sub>1</sub> | SSS            | CCA      | Adaptive    | Large-scale       | 1                  | Synchronous        | Security-with-abort |
| TKEM <sub>2</sub> | RSS            | CCA      | Adaptive    | Small-scale       | $\binom{N-1}{t-1}$ | Asynchronous       | Security-with-abort |
| TPKE              | RSS            | CCA      | Adaptive    | Small-scale       | $\binom{N-1}{t-1}$ | Asynchronous       | Robustness          |

The specification is organized as follows. We first introduce the syntax and concrete instantiations of the required building blocks. We then provide intuition for how these components are combined to obtain the complete constructions of TKEM<sub>1</sub>, TKEM<sub>2</sub> and TPKE, together with intuitions of how they achieve CCA security and active security under adaptive corruptions.

### 2.1.1. Regev-Style Encryption

Our TKEM and TPKE schemes are based on the Regev-style PKE scheme [Reg05; GPV08; LP11].

In the basic dual Regev scheme [Reg05; GPV08], encrypting a message  $\mu$  under the public key  $\text{pk} = \mathbf{A}\mathbf{k}$  yields a ciphertext  $\text{ct} = (\mathbf{c}^\top = \mathbf{s}^\top \mathbf{A} + \mathbf{e}^\top, d = \mathbf{s}^\top \text{pk} + e' + \text{Encode}(\mu))$ , where  $\mathbf{c}$  is an MLWE instance,  $\mathbf{e}, e'$  are MLWE noises, and  $\text{Encode}(\mu)$  is an encoding of the message  $\mu$  which enables correct recovery in the presence of noises.

The optimized Regev variant in [LP11] (the LP11 variant thereafter) replaces  $\text{pk} = \mathbf{A}\mathbf{k}$  with an MLWE instance  $\mathbf{A}\mathbf{k} + \mathbf{f}$ , allowing smaller dimensions for  $\mathbf{A}$  and improving concrete efficiency.

### 2.1.2. Non-Interactive Zero-Knowledge Proof

To upgrade the Regev-style schemes to CCA-secure ones, we augment their ciphertexts with NIZK proofs. Specifically, the encryption algorithm appends a NIZK proof  $\pi$  to the original  $\text{ct} = (\mathbf{c}, d)$  to prove its well-formedness, and the decryption algorithm verifies  $\pi$  before decrypting  $(\mathbf{c}, d)$  to  $\mu$ .

We use NIZK proofs with different properties for the dual Regev scheme and the LP11 variant.

- For the LP11 variant, we use a simulation-extractable NIZK [Gro06] to prove that  $(c, d)$  is a valid LP11 ciphertext, i.e., there exists witness  $(\mu, s, e, e')$ , s.t.  $c^\top = s^\top A + e^\top$  and  $d = s^\top pk + e' + \text{Encode}(\mu)$ .
- For the dual Regev scheme, we use a one-time simulation-sound NIZK [Sah99; DDOPS01] to prove that  $c$  is an MLWE instance, i.e., there exists witness  $(s, e)$ , s.t.  $c^\top = s^\top A + e^\top$ .

Note that the above relations are linear (with small-norm witness), so we can efficiently instantiate these NIZK proofs using Lantern [LNP22], together with standard transformations based on strongly unforgeable signatures and public-key encryption.

### 2.1.3. Secret Sharing

Observe that the decryption of the Regev-style schemes is just a linear operation with  $sk = k$ , so it is friendly to be thresholdized via applying a linear secret sharing scheme like SSS or RSS.

- **Shamir secret sharing.** SSS [Sha79] is based on Lagrange interpolation, and has excellent efficiency properties, i.e., each party holds 1 evaluation of the secret polynomial as the secret share. Since both the secret shares and Lagrange coefficients have large values, we further incorporate the zero-sum mask technique [PKMMPS24; KRT24] when using SSS.
- **Replicated secret sharing.** For RSS [ISN87], both the secret shares and the reconstruction coefficients have small values, so it is particularly suitable for the lattice setting. However, each party must hold  $\binom{N-1}{t-1}$  secret shares, so it is practical only for small party number  $N$ .

### 2.1.4. TKEM<sub>1</sub> in Large-Scale Synchronous Setting

Our TKEM<sub>1</sub> is designed in the synchronous setting and its construction goes with two steps. Firstly, we use SSS to thresholdize the LP11 variant of Regev encryption augmented with NIZK, and equip it with polynomial flooding and zero-sum mask techniques, to achieve CCA security under adaptive corruptions. Then, we apply the FO transform to achieve security-with-abort under adaptive corruptions. We refer to Figure 1 (the upper part) for an overview of our TKEM<sub>1</sub>.

More precisely, in the first step, we construct an intermediate threshold PKE scheme as follows.

- **Key Generation.** This is executed by a trusted dealer. The public key  $pk = Ak + f$  is an MLWE instance. The secret key share of party  $i \in [N]$  includes an SSS secret share  $k_i$  of  $k$ .
- **Encryption.** Given message  $\mu \in \mathcal{R}_p$ , we use a simple encoding algorithm  $\text{Encode}(\mu) = \lceil \frac{q}{p} \rceil \cdot \mu$ . The ciphertext  $ct$  includes the ciphertext  $(c, d)$  of LP11 variant, augmented with a NIZK proof  $\pi$  showing the well-formness of  $(c, d)$ .
- **Partial Decryption.** Given  $ct = (c, d, \pi)$  and a decryption set  $S$ , each party  $i$  verifies  $\pi$ , and then computes partial decryption  $h_{i,S} := \lambda_{i,S} c^\top k_i + y_{i,S} + \Delta_{i,S}$ , where  $\lambda_{i,S}$  is Lagrange coefficient,  $y_{i,S}$  is a polynomial-sized smudging noise and  $\Delta_{i,S}$  is a zero-sum mask.

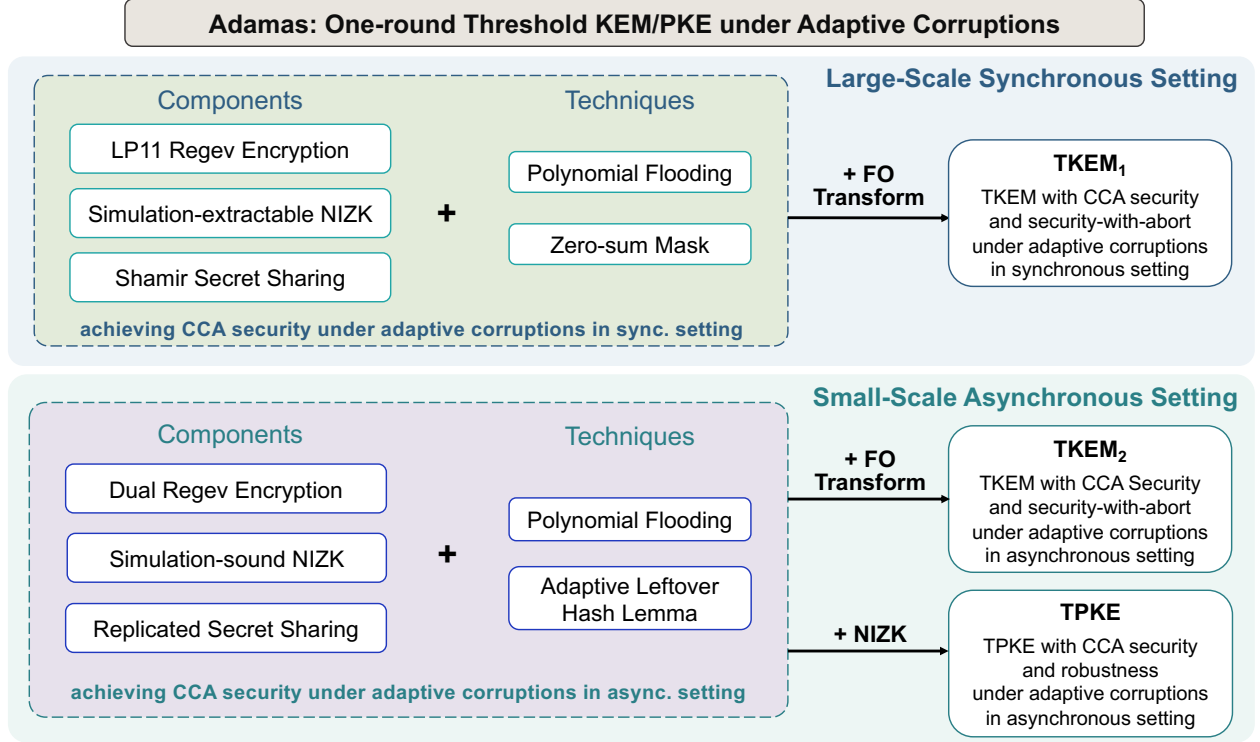


Figure 1: Modular Architecture of the Proposed TKEM<sub>1</sub>, TKEM<sub>2</sub> and TPKE.

- **Combination.** Given  $ct = (c, d, \pi)$  and  $\{h_{i,S}\}_{i \in S}$ , the combiner recovers the message by computing  $\mu := \lceil \frac{p}{q} \cdot (d - \sum_{i \in S} h_{i,S}) \rceil$ . The correctness follows from the correctness of the LP11 variant, the completeness of the NIZK and the fact that  $\sum_{i \in S} \Delta_{i,S} = 0$ .

Both polynomial flooding and zero-sum mask technique are essential to the security. In particular, the smudging noise  $y_{i,S}$  limits the leakage of the secret key from the term  $d - \sum_{i \in S} h_{i,S}$  when combining, and the zero-sum mask  $\Delta_{i,S}$  avoids the leakage from the partial decryption  $h_{i,S}$ .

In the second step, we further apply FO transform to the above threshold PKE, to achieve active security and get our TKEM<sub>1</sub>. Concretely, let  $G, H$  be random oracles. The key generation and partial decryption algorithms remain the same. The encapsulation algorithm encrypts a random message  $\mu$  as above, but using randomness  $G(\mu)$ . The ciphertext is  $ct$  and the encapsulated key is  $K := H(\mu, ct)$ . The combination algorithm first recovers  $\mu$  from  $ct$  as above, then verifies if  $ct$  is an encryption of  $\mu$  with randomness  $G(\mu)$ , and finally outputs  $K := H(\mu, ct)$ . The re-encryption step ensures the combiner either recover the correct encapsulated key  $K := H(\mu, ct)$  or abort, thus achieving security-with-abort.

As such, we obtain TKEM<sub>1</sub> with CCA security and security-with-abort under adaptive corruptions.

### 2.1.5. TKEM<sub>2</sub> and TPKE in Small-Scale Asynchronous Setting

Our TKEM<sub>2</sub> and TPKE are designed in the asynchronous setting and their constructions also go with two steps. We refer to Figure 1 (the lower part) for an overview of our TKEM<sub>2</sub> and TPKE.

The first step (i.e., constructing an intermediate threshold PKE with CCA security under adptive corruption) is similar to the first step of TKEM<sub>1</sub>, except with the following main differences.

- The threshold PKE scheme is based on dual Regev encryption augmented with NIZK proofs, and uses RSS to share the secret key.
- As both the secret shares and reconstruction coefficients of RSS have small values, a single polynomial-sized smudging noise  $y_i$  (without the zero-sum masks) suffices for the CCA security under adaptive corruptions, with the help of our adaptive leftover hash lemma.

The second step include two routes to achieve active security. We can either apply the FO transform to get TKEM<sub>2</sub> achieving security-with-abort under adaptive corruptions, similar to TKEM<sub>1</sub>, or augment the partial decryption with NIZK proofs to get TPKE achieving robustness.

As such, we obtain TKEM<sub>2</sub> with CCA security and security-with-abort under adaptive corruptions, and obtain TPKE with CCA security and robustness under adaptive corruptions.

## 2.2. System Model

For all our schemes, we assume a trusted dealer for key generation and secret-share distribution, i.e., the dealer shares the secret key among  $N$  parties using secret sharing scheme and securely distributes the corresponding share to each party. For TKEM<sub>1</sub>, parties are connected with synchronous and authenticated channels with guaranteed message delivery. For TKEM<sub>2</sub> and TPKE, parties are connected with asynchronous and authenticated channels.

To decrypt a ciphertext, each participating party independently runs the partial decryption algorithm to generate its decryption share  $h_i$ . The shares  $\{h_i\}_{i \in S}$  are sent to a designated combiner, which invokes the combination algorithm to recover the message or encapsulated key.

## 2.3. Security

We consider security against active adversaries, offering either security-with-abort or the stronger guarantee of robustness. Security-with-abort ensures that an honest combiner can either recover the correct message (resp. encapsulated key) or return  $\perp$ . Robustness additionally enables the combiner to verify individual partial decryptions to detect and reject invalid ones.

For all our schemes, we consider game-based CCA security under adaptive corruptions without secure erasures. It requires the hardness for a probabilistic polynomial-time adversary to distinguish the encryption of  $\mu_0$  and  $\mu_1$  (resp. the real key encapsulated in the challenge ciphertext or a uniformly random one) with non-negligible advantage, even if the adversary can adaptively obtain (1) the partial decryptions of any ciphertexts including the challenge ciphertext, and (2) secret key

shares and the randomness used in previous partial decryption queries. To avoid trivial attacks, the total number of corrupted parties and obtained partial decryptions of the challenge ciphertext must be less than the threshold  $t$ .

All our schemes achieve CCA security and active security under adaptive corruptions based on the MLWE and MSIS assumptions in the random oracle model. We refer to [ZZHLH26] for more details of the security analysis of our submissions.

### 3. Open-Source Implementation

Our submission builds on our very recent work [ZZHLH26], so no open-source implementation is currently available. For the final submission, we plan to develop an optimized open-source implementation. Since our constructions rely on well-studied and highly optimized components, including Regev-style encryption schemes and NIZK proofs, we do not anticipate significant implementation, testing, or reproducibility challenges.

### 4. Experimental Performance Evaluation

In Table 2, we present estimated efficiency including the ciphertext size  $|\text{ct}|$  and the partial decryption size  $|h_i|$  per user of all our submitted schemes for 128-bit security levels under different settings of party number  $N$  and threshold  $t$ .

Table 2: The estimated efficiency of schemes  $\text{TKEM}_1$ ,  $\text{TKEM}_2$  and TPKE. The sizes are estimated assuming that the CCA adversary makes at most  $2^{60}$  partial decryption queries. The efficiency of TPKE is estimated in the semi-honest setting, i.e., without the NIZK proofs for robustness.

| Scheme                 | Party Number $N$ | Threshold $t$ | Ciphertext Size $ \text{ct} $ | Partial Decryption Size $ h_i $ |
|------------------------|------------------|---------------|-------------------------------|---------------------------------|
| $\text{TKEM}_1$        | 1024             | $\leq 1024$   | 101 KB                        | 1.87 KB                         |
| $\text{TKEM}_2$ & TPKE | 8                | 4             | 170 KB                        | 86 KB                           |
|                        | 16               | 2             | 158 KB                        | 38 KB                           |
|                        | 16               | 8             | 178 KB                        | 16.4 MB                         |

### 5. Licensing, Patent Claims, and Funding

**License.** We intend to release our future reference implementation under the Apache License.

**Patents.** None.

**Funding.** National Cyber Security-National Science and Technology Major Project (2026ZD1500900), National Cryptologic Science Fund of China (2025NCSF01009), National Natural Science Foundation of China (62572295, 62522212), and National Key R&D Program of China (2025YFA1017100).

## 6. Comparison with Other Submissions

In this section, we compare our Adamas with [DLNPY21] and other submissions of Categories S2.

**Comparison with [DLNPY21].** To our best knowledge, the construction in [DLNPY21] is the only prior lattice-based TPKE scheme that achieves CCA security under adaptive corruptions. However, its security proof requires a super-polynomial modulus-to-noise ratio, which weakens the hardness of the LWE assumption and reduces efficiency. Their work is theory-oriented and only provides an asymptotic estimation. They [DLNPY21] leave the construction of an LWE-based TPKE scheme that is secure under adaptive corruptions with a polynomial modulus as an open problem. This open problem is resolved by our recent work [ZZHLH26] and our Adamas family.

**Comparison with Amber.** Amber [BPLP26a] is a lattice-based TKEM based on the BCHK+ transformation [LP25] and has compact ciphertext sizes. BCHK+ transformation compiles a threshold identity-based encryption (TIBE) and an one-time signature to a CCA-secure TKEM. Due to the underlying three-round TIBE, Amber’s decryption process also requires three rounds. Our Adamas has relatively larger ciphertext sizes but only requires a single round interaction for decryption. Regarding security, the latest ePrint version of [BPLP26b, Footnote 5] notes that its prior version wrongly stated that the SSS-based TPKE scheme in Amber [BPLP26a] can be proven secure against adaptive corruptions. Thus, Amber only achieves CCA security under static corruptions. In comparison, all our schemes achieve CCA security under adaptive corruptions.

**Comparison with SplitKey.** The Split-decryption protocol of the SplitKey submission [LPSVM+26] is a quantum-vulnerable, two-party, server-assisted TPKE scheme based on the threshold ElGamal encryption and NIZK proofs. It proves security in the universal composability framework under static corruptions based on the one-more computational Diffie-Hellman assumption. In comparison, our Adamas targets lattice-based  $(t, N)$ -TPKE and TKEM with post-quantum security.

**Comparison with PQarrots.** The Kea protocol of the PQarrots submission [AABBB+26] is a post-quantum secure TPKE scheme. It proves restricted CCA security and identifiable-with-abort under static corruptions in an idealized group-action model. Their decryption requires  $O(t)$  interaction rounds. In comparison, our Adamas achieves CCA security under adaptive corruptions with only one-round decryption.

## References

- [BPLP26a]** Katharina Boudgoust, Rafael del Pino, Oleksandra Lapiha, and Thomas Prest. *Amber: a Family of Efficient Lattice-Based IND-CCA Threshold KEMs*. National Institute of Standards and Technology (NIST), Multi-Party Threshold Cryptography. January 2026. URL: <https://csrc.nist.gov/csrc/media/Projects/threshold-cryptography/documents/TCall-1/Amber-PW01.pdf>.
- [AABBB+26]** Marius A. Aardal, Shahla Atapoor, Karim Bagheri, Andrea Basso, Xavier Bonnetain, Giacomo Borin, Daniele Cozzo, Pierrick Dartois, Luca De Feo, Max Duparc, Jonathan K. Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Samuel Jaques, Yi-Fu Lai, Dania Lazzarini, Jason T. LeGrow, Chloe Martindale, Luciano Maino, Jonas Meers, Michael Meyer, Sikhar Patranabis, Robi Pedersen, Giacomo Pope, Doreen Riepel, Damien Robert, Ryan Rueger, Sina Schaeffler, André Schrottenloher, and Frederik Vercauteren. *PQarrots: Macaw, Kea and Kakapo—Threshold primitives from (isogeny-based) group actions*. NIST Threshold Call Preview Writeup. Version 0.3, dated 2026-01-30. January 2026. URL: <https://csrc.nist.gov/csrc/media/Projects/threshold-cryptography/documents/TCall-1/PQarrots-PW01.pdf>.
- [BPLP26b]** Katharina Boudgoust, Rafaël del Pino, Oleksandra Lapiha, and Thomas Prest. “IND-CCA Lattice Threshold KEM Under 30 KiB”. In: *Public-Key Cryptography - PKC 2026 - 29th IACR International Conference on Practice and Theory of Public-Key Cryptography, West Palm Beach, FL, USA, May 25-28, 2026, Proceedings, Part I*. Ed. by Shi Bai and Edoardo Persichetti. Vol. 16551. Lecture Notes in Computer Science. Springer, 2026, pp. 38–69. DOI: [10.1007/978-3-032-26731-3\\_2](https://doi.org/10.1007/978-3-032-26731-3_2). URL: [https://doi.org/10.1007/978-3-032-26731-3\\_2](https://doi.org/10.1007/978-3-032-26731-3_2). Also at [ia.cr/2026/021](https://ia.cr/2026/021).
- [DDOPS01]** Alfredo De Santis, Giovanni Di Crescenzo, Rafail Ostrovsky, Giuseppe Persiano, and Amit Sahai. “Robust Non-interactive Zero Knowledge”. In: *CRYPTO 2001*. Ed. by Joe Kilian. Vol. 2139. LNCS. Springer, 2001, pp. 566–598. URL: [https://doi.org/10.1007/3-540-44647-8\\_33](https://doi.org/10.1007/3-540-44647-8_33).
- [DLNPY21]** Julien Devevey, Benoît Libert, Khoa Nguyen, Thomas Peters, and Moti Yung. “Non-interactive CCA2-Secure Threshold Cryptosystems: Achieving Adaptive Security in the Standard Model Without Pairings”. In: *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part I*. Ed. by Juan A. Garay. Vol. 12710. Lecture Notes in Computer Science. Springer, 2021, pp. 659–690. DOI: [10.1007/978-3-030-75245-3\\_24](https://doi.org/10.1007/978-3-030-75245-3_24). URL: [https://doi.org/10.1007/978-3-030-75245-3\\_24](https://doi.org/10.1007/978-3-030-75245-3_24). Also at [ia.cr/2021/630](https://ia.cr/2021/630).
- [FO13]** Eiichiro Fujisaki and Tatsuaki Okamoto. “Secure Integration of Asymmetric and Symmetric Encryption Schemes”. In: *Journal of Cryptology* 26.1 (January 2013), pp. 80–101. DOI: [10.1007/s00145-011-9114-1](https://doi.org/10.1007/s00145-011-9114-1). URL: <https://doi.org/10.1007/s00145-011-9114-1>.
- [FO99]** Eiichiro Fujisaki and Tatsuaki Okamoto. “Secure Integration of Asymmetric and Symmetric Encryption Schemes”. In: *Advances in Cryptology – CRYPTO ’99*. Ed. by Michael J. Wiener. Vol. 1666.

Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, August 1999, pp. 537–554. DOI: [10.1007/3-540-48405-1\\_34](https://doi.org/10.1007/3-540-48405-1_34). URL: [https://doi.org/10.1007/3-540-48405-1\\_34](https://doi.org/10.1007/3-540-48405-1_34).

**[GPV08]** Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. “Trapdoors for hard lattices and new cryptographic constructions”. In: *STOC 2008*. Ed. by Cynthia Dwork. ACM, 2008, pp. 197–206. URL: <https://doi.org/10.1145/1374376.1374407>. Also at [ia.cr/2007/432](https://ia.cr/2007/432).

**[Gro06]** Jens Groth. “Simulation-Sound NIZK Proofs for a Practical Language and Constant Size Group Signatures”. In: *Advances in Cryptology - ASIACRYPT 2006, 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, December 3-7, 2006, Proceedings*. Ed. by Xuejia Lai and Kefei Chen. Vol. 4284. Lecture Notes in Computer Science. Springer, 2006, pp. 444–459. DOI: [10.1007/11935230\\_29](https://doi.org/10.1007/11935230_29). URL: [https://doi.org/10.1007/11935230\\_29](https://doi.org/10.1007/11935230_29).

**[ISN87]** Mitsuru Ito, Akira Saito, and Takao Nishizeki. “Secret Sharing Scheme Realizing General Access Structure”. In: *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '87)*. IEEE, 1987, pp. 99–102. URL: <https://archiv.infsec.ethz.ch/education/fs08/secsem/itsani87.pdf>.

**[KRT24]** Shuichi Katsumata, Michael Reichle, and Kaoru Takemure. “Adaptively Secure 5 Round Threshold Signatures from MLWE/MSIS and DL with Rewinding”. In: *CRYPTO 2024, Part VII*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14926. LNCS. Springer, 2024, pp. 459–491. URL: [https://doi.org/10.1007/978-3-031-68394-7\\_15](https://doi.org/10.1007/978-3-031-68394-7_15). Also at [ia.cr/2024/1033](https://ia.cr/2024/1033).

**[LNP22]** Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plançon. “Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General”. In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13508. Lecture Notes in Computer Science. Springer, 2022, pp. 71–101. DOI: [10.1007/978-3-031-15979-4\\_3](https://doi.org/10.1007/978-3-031-15979-4_3). URL: [https://doi.org/10.1007/978-3-031-15979-4\\_3](https://doi.org/10.1007/978-3-031-15979-4_3). Also at [ia.cr/2022/284](https://ia.cr/2022/284).

**[LP11]** Richard Lindner and Chris Peikert. “Better Key Sizes (and Attacks) for LWE-Based Encryption”. In: *Topics in Cryptology - CT-RSA 2011 - The Cryptographers’ Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*. Ed. by Aggelos Kiayias. Vol. 6558. Lecture Notes in Computer Science. Springer, 2011, pp. 319–339. DOI: [10.1007/978-3-642-19074-2\\_21](https://doi.org/10.1007/978-3-642-19074-2_21). URL: [https://doi.org/10.1007/978-3-642-19074-2\\_21](https://doi.org/10.1007/978-3-642-19074-2_21). Also at [ia.cr/2010/613](https://ia.cr/2010/613).

**[LP25]** Oleksandra Lapiha and Thomas Prest. “A Lattice-Based IND-CCA Threshold KEM from the BCHK+ Transform”. In: *ASIACRYPT 2025*. December 2025. URL: [https://doi.org/10.1007/978-981-95-5099-9\\_15](https://doi.org/10.1007/978-981-95-5099-9_15). Also at [ia.cr/2025/1958](https://ia.cr/2025/1958).

**[LPSVM+26]** Peeter Laud, Alisa Pankova, Nikita Snetkov, Jelizaveta Vakarjuk, Petr Muzikant, Aivo Kalu, Burak Can Kus, Semjon/Sona Kravtšenko, Raul-Martin Rebane, and Mart Oruaas. *SplitKey: Two-party signing and decryption with extra features*. NIST Threshold Call Preview Writeup. Version 0.1, dated 2026-01-12. Team: SplitForge. January 2026. URL: <https://csrc.nist.gov/csrc/media/Projects/threshold-cryptography/documents/TCall-1/SplitForge-PW01.pdf>.

**[PKMMPS24]** Rafaël Del Pino, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, and Markku-Juhani O. Saarinen. “Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumptions”. In: *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part II*. Ed. by Marc Joye and Gregor Leander. Vol. 14652. Lecture Notes in Computer Science. Springer, 2024, pp. 219–248. DOI: [10.1007/978-3-031-58723-8\\_8](https://doi.org/10.1007/978-3-031-58723-8_8). URL: [https://doi.org/10.1007/978-3-031-58723-8\\_8](https://doi.org/10.1007/978-3-031-58723-8_8). Also at [ia.cr/2024/184](https://ia.cr/2024/184).

**[Reg05]** Oded Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *STOC 2005*. Ed. by Harold N. Gabow and Ronald Fagin. ACM, 2005, pp. 84–93. URL: <https://doi.org/10.1145/1060590.1060603>.

**[Sah99]** Amit Sahai. “Non-Malleable Non-Interactive Zero Knowledge and Adaptive Chosen-Ciphertext Security”. In: *FOCS 1999*. IEEE Computer Society, 1999, pp. 543–553. URL: <https://doi.org/10.1109/SFFCS.1999.814628>.

**[Sha79]** Adi Shamir. “How to Share a Secret”. In: *Commun. ACM* 22.11 (1979), pp. 612–613. URL: <https://doi.org/10.1145/359168.359176>.

**[ZZHLH26]** Yuxin Zhang, Yunxiao Zhou, Shuai Han, Shengli Liu, and Xinyi Huang. *Adaptively CCA-Secure Threshold Decryption from Lattices with Polynomial Modulus*. Cryptology ePrint Archive, Paper 2026/1627. 2026. URL: <https://eprint.iacr.org/2026/1627>.

**[NIST-IR8214C]** Luís T. A. N. Brandão and René Peralta. *NIST First Call for Multi-Party Threshold Schemes*. (National Institute of Standards and Technology) NIST Internal Report (NISTIR) 8214C. 2026. DOI: [10.6028/NIST.IR.8214C](https://doi.org/10.6028/NIST.IR.8214C).