Comparing Lattices and Bilinear Parings in CP-ABE

Lorenzo Gasparini[1], Elia Onofri[2], Martina Palmucci[3], and Marco Pedicini[1]

[1] Department of Mathematics and Physics, Roma Tre University, Rome, Italy
[2] Istituto per le Applicazioni del Calcolo (IAC), National Research Council of Italy (CNR), Naples, Italy
[3] NTT DATA Italia S.p.a., Rome, Italy

Abstract. Ciphertext-Policy Attribute-Based Encryption enables fine-grained access control by binding ciphertext decryption to user attributes. While most practical schemes are pairing-based and rely on assumptions vulnerable to quantum attacks, lattice-based approaches offer post-quantum security at the cost of reduced expressiveness. In this work, we present the first direct benchmark of open-source implementations from both families across diverse hardware, assessing their performance toward the design of practical quantum-resilient access control systems.

Keywords: CP-ABE · Benchmarking · OpenABE · Palisade.

In recent years, *Attribute-Based Encryption* (ABE, [22]) has gained significant traction as a versatile cryptographic primitive for securing data in distributed and untrusted environments, generalising the more classical notion of Identity Based Encryption (IBE, see [23]). Its main appeal lies in enabling *fine-grained access control* over encrypted information by binding decryption capabilities to descriptive attributes rather than to specific user identities. Among the various ABE paradigms, the *Ciphertext-Policy* variant (CP-ABE, [3]) embeds access policies directly into the ciphertext, allowing data owners to specify, at the time of encryption, the exact set of attributes required for decryption.

More formally, a CP-ABE system typically involves three roles: a *central authority* (CA) responsible for setup and key issuance, *data owners* who encrypt under a chosen policy, and *users* who can decrypt only if their attributes match the policy requirements. CP-ABE schemes are built on four core algorithms:

Setup run by the CA to generate public parameters and a master secret
KeyGen run by the CA to issue a private key bound to a user's attributes
Encryption run by data owners to produce a ciphertext under a chosen policy
Decryption run by users to recover the plaintext if attributes allows

De Cifris Koine – FCiR25 ACTA https://doi.org/10.69091/koine/vol-8-P10

Table 1. Overview of CP-ABE schemes implemented in major open-source libraries.

Algorithm	Primitive	Library (Language)						Ref.
		OpenABE (C++) [28]	Charm (Python) [2]	Rabe (Rust) [11]	CiFer (C) [8]	GoFe (Go) [12]	PALISADE (C++) [18, 20]	
WATERS	Pairing	■	■					[25]
JYJGXD	Pairing		■					[15]
RW	Pairing		■					[21]
YAHK	Pairing		■					[26]
CGW	Pairing		■					[6]
FAME	Pairing		■		■	■		[1]
AR	Pairing		■					[14]
TBPRE	Pairing		■					[16]
YLLC	Pairing		■					[27]
AW	Pairing		■	■				[13]
BSW	Pairing		■	■				[3]
BDABE	Pairing			■				[5]
ZZ	Lattices						■	[29]

For completeness, we note that extensions to the classical CP-ABE model address challenges such as key escrow and recovery [30], key revocation [7], and multi-authority settings [9]. A further relevant distinction is between *small-universe* schemes, where the attribute set is fixed at setup, and *large-universe* schemes, where attributes may be drawn from an unbounded domain.

Since the seminal work of Bethencourt, Sahai, and Waters [3], most practical CP-ABE schemes were designed around *pairing-based cryptography*: this approach offers efficient algorithms, mature implementations, and a well-established security model [17]. However, it depends on number-theoretic assumptions (like *e.g.* Decisional Diffie–Hellman [4, 10]) which are known vulnerable to polynomial-time quantum attacks via Shor's algorithm [24]. This vulnerability has motivated interest in other primitives, including *lattice-based cryptography*, and in particular Learning With Errors-based schemes, which offer strong post-quantum security guarantees and favourable asymptotic efficiency in some settings [19].

Despite the availability of benchmarks comparing CP-ABE schemes within the same cryptographic family, no prior work has directly compared pairing-based and lattice-based CP-ABE in a unified setting. Such a comparison is challenging due to differences in parameter domains, security levels, and algorithmic bottlenecks, as well as the scarcity of open-source lattice-based implementations (see Table 1). Nonetheless, this analysis is valuable for practitioners seeking to balance performance, security, and implementation complexity, particularly for deployment in quantum-resilient systems; in this work we aim filling this gap.

Methodology

For our analysis, we select two representative CP-ABE implementations: the Waters' scheme [25] (OpenABE, [28]) as pairing-based representative and Zhang and Zhang's LWE-based scheme [29] (PALISADE-ABE, [20]) as lattice-based contestant. The first features a mature and actively maintained library, representative of classical CP-ABE deployments, while the latter is a state-of-the-art post-quantum secure approach. Both implementations are open source, tested by the research community, and configured to provide comparable expressiveness.

For the benchmark setup, we performed 1000 repetitions per configuration, on two distinct hardware platforms. The first consists in a high-end cloud virtual machine (VM), hosted on the CloudShare platform provided by the NTT Innovation Lab, with a 16-core Intel Xeon E5-2660v4 CPU and 400GB of RAM. The second is a low-end setup built on a Raspberry Pi 4B (RPi), equipped with a quad-core ARM Cortex-A72 and 4GB of SDRAM. A dual-platform setup aims at capturing performance both in server-class deployments and in resource-limited edge devices.

In details, to assess scalability we measured the timing for each fundamental function at the varying of the universe size (attribute numbers ranging from 6 to 32), with an all-and fixed policy. Both schemes were run at equivalent target security levels (128-bit classical security).

Results

In what follows, we discuss the results of our experiments (see also Figure 1).

On both platforms, the pairing-based scheme consistently outperformed the lattice-based one in setup phase by a factor of 3.2×; as expected, OpenABE exhibits constant timings, independent of the number of attributes, while PALISADE shows a clear linear growth, reaching a maximum difference of approximately 276 ms at 32 attributes on the high-end VM. It is worth noting, however, that in most deployment scenarios, the setup phase is performed only once during the system's initialisation. As such, even a considerable difference in execution time may have limited practical impact.

The gap widen for Key Generation phase, reaching an average multiplicative factor of 8.3× for the VM and of 7.1× for the RPi. To provide a concrete comparison, for 32 attributes, OpenABE completes the operation in roughly 85 ms against the 799 ms taken by PALISADE on the VM, clearly demonstrating the computational weight of the lattice-based approach. Overall, the impact of the high-end device over the RPi is between 3× and 4×. Such an impact is more relevant in practice, as the operation is to be carried out each time a novel user sign in the system; however, the computational burden might be mitigated in part by the deployment context. Furthermore, the most costly operation in PALISADE consists in trapdoored-randomness generation, which can be inherently carried out off-line w.r.t. the actual keygen phase.

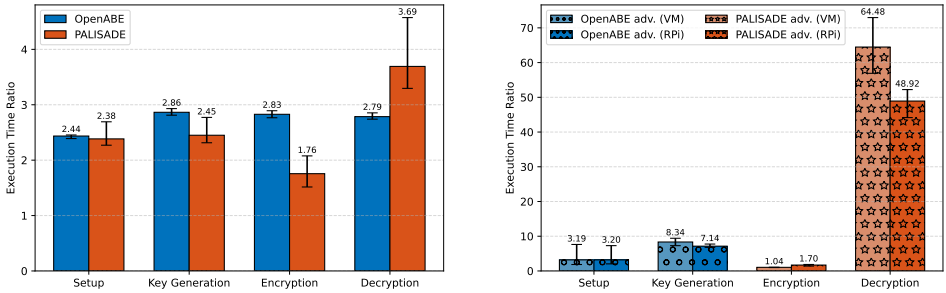

Fig. 1. Summary of the performance gain (ratios) amongst the different hardware platforms and cryptographic schemes. Annotated bars indicate average speed-up ratios, while grey error bars represent the minimum and maximum observed values. (left) Relative advantage of executing each library on the VM with respect to the RPi. (right) Comparative advantage between OpenABE and PALISADE on both platforms: bars denote either an OpenABE advantage (blue, circles) or a PALISADE advantage (orange, stars), depending on which library performs better for a given operation.

Amongst the four main functions, Encryption is the one showing the more competitive times in both environments, aligning almost perfectly on the VM and presenting only minimal advantage (1.7×) for the lattice-based scheme on the RPi. This is notable given that encryption is performed by data owners often using mid- to low-end devices, making PALISADE particularly appealing for edge-centric deployments. This is further confirmed as the VM gain w.r.t. the RPi is the overall less impacting, being generally lower than 2× on PALISADE.

The most notable trade-off is, however, in Decryption. Here, the lattice-based scheme consistently outperforms the counterpart, with speedups of 57–73× on the VM and 44–52× on the RPi. While OpenABE's pairing-based scheme scales linearly with the number of attributes, reaching up to 1.3 s, PALISADE maintains near-constant times due to its lightweight matrix–vector operations and rounding steps. Being less expressive, PALISADE's efficient decryption cost is particularly attractive for constrained environments, where decryption is frequent and often performed by resource-limited end users.

Conclusions

This study presents the first direct performance benchmark of CP-ABE schemes built on pairing- and lattice-based primitives, comparing OpenABE's implementation of Waters' scheme with PALISADE-ABE's Zhang–Zhang construction. Tests on both a high-end virtual machine and a resource-constrained Raspberry Pi reveal complementary strengths: from one side, the lattice-based approach present

outstanding decryption performance in a quantum-safe environment, maintaining near-constant times as attribute count grows and outperforming the pairing-based counterpart; on the other hand, the pairing-based implementation achieves better results in setup and key generation, while also offering greater policy expressiveness and universe size support.

Overall, the results indicate that lattice-based CP-ABE is highly promising for constrained or decryption-intensive scenarios, while pairing-based schemes remain preferable when complex policies and large universes are required. Bridging this gap will require advancing lattice-based designs to support richer policy structures, large-universe settings, and auxiliary features such as key delegation. Future research should also investigate implementation-level optimisations and hardware acceleration to further reduce the performance gaps.

Acknowledgements E. Onofri is a member of the "Gruppo Nazionale Calcolo Scientifico – Istituto Nazionale di Alta Matematica" (GNCS–INdAM), Italy.

M. Pedicini is a member of the "Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni – Istituto Nazionale di Alta Matematica" (GNSAGA–INdAM), Italy.

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

1. Agrawal, S., Chase, M.: FAME: Fast Attribute-based Message Encryption. In: Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D. (eds.) ACM CCS 2017, pp. 665–682. ACM Press (2017). https://doi.org/10.1145/3133956.3134014
2. Akinyele, J.A., Garman, C., Miers, I., Pagano, M.W., Rushanan, M., Green, M., Rubin, A.D.: Charm: a framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering **3**(2), 111–128 (2013). https://doi.org/10.1007/s13389-013-0057-3
3. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-Policy Attribute-Based Encryption. In: 2007 IEEE Symposium on Security and Privacy, pp. 321–334. IEEE Computer Society Press (2007). https://doi.org/10.1109/SP.2007.11
4. Boneh, D.: The decision Diffie-Hellman problem. In: Third Algorithmic Number Theory Symposium (ANTS). LNCS. Springer (1998)
5. Bramm, G., Gall, M., Schütte, J.: BDABE - Blockchain-based Distributed Attribute based Encryption. In: Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, 99–110. SCITEPRESS - Science and Technology Publications (2018). https://doi.org/10.5220/0006852600990110
6. Chen, J., Gay, R., Wee, H.: Improved Dual System ABE in Prime-Order Groups via Predicate Encodings. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, pp. 595–624. Springer, Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_20

7. Cianfriglia, M., Onofri, E., Pedicini, M.: mRLWE-CP-ABE: A revocable CP-ABE for post-quantum cryptography. Journal of Mathematical Cryptology **18**(1) (2024). https://doi.org/10.1515/jmc-2023-0026
8. CiFer, https://github.com/fentec-project/CiFEr.
9. Das, S., Namasudra, S.: Multiauthority CP-ABE-based Access Control Model for IoT-enabled Healthcare Infrastructure. IEEE Transactions on Industrial Informatics **19**(1), 821–829 (2023). https://doi.org/10.1109/tii.2022.3167842
10. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Transactions on Information Theory **22**(6), 644–654 (1976). https://doi.org/10.1109/tit.1976.1055638
11. Fraunhofer AISEC, Rabe: Rust Attribute Based Encryption Library, https://github.com/Fraunhofer-AISEC/rabe (2023).
12. GoFe, https://github.com/fentec-project/gofe.
13. Lewko, A.B., Waters, B.: Decentralizing Attribute-Based Encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, pp. 568–588. Springer, Berlin, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_31
14. Li, J., Yao, W., Han, J., Zhang, Y., Shen, J.: User Collusion Avoidance CP-ABE With Efficient Attribute Revocation for Cloud Storage. IEEE Systems Journal **12**(2), 1767–1777 (2018). https://doi.org/10.1109/jsyst.2017.2667679
15. Li, J., Zhang, Y., Ning, J., Huang, X., Poh, G.S., Wang, D.: Attribute Based Encryption with Privacy Protection and Accountability for CloudIoT. IEEE Transactions on Cloud Computing **10**(2), 762–773 (2022). https://doi.org/10.1109/tcc.2020.2975184
16. Liu, Q., Wang, G., Wu, J.: Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. Information Sciences **258**, 355–370 (2014). https://doi.org/10.1016/j.ins.2012.09.034
17. Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., Urbieta, A.: All Cryptolibraries Are Beautiful, But Some Are More Beautiful Than Others: A Survey of CP-ABE Libraries. In: 3rd URSI Atlantic / Asia-Pacific Radio Science Meeting - 2022 (2022). https://researchgate.net/publication/363098622
18. PALISADE Cryptography Library, (2023). https://palisade-crypto.org. Accessed: 2023-04-10.
19. Peikert, C.: A Decade of Lattice Cryptography, Cryptology ePrint Archive, Report 2015/939 (2015). https://eprint.iacr.org/2015/939.
20. Rohloff, K., Polyakov, Y., Cousins, D.: PALISADE-ABE, (2022). https://gitlab.com/palisade/palisade-abe. GITLAB: `palisade/palisade-abe`.
21. Rouselakis, Y., Waters, B.: Efficient Statically-Secure Large-Universe Multi-Authority Attribute-Based Encryption. In: Böhme, R., Okamoto, T. (eds.) FC 2015. LNCS, pp. 315–332. Springer, Berlin, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47854-7_19
22. Sahai, A., Waters, B.R.: Fuzzy Identity-Based Encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, pp. 457–473. Springer, Berlin, Heidelberg (2005). https://doi.org/10.1007/11426639_27
23. Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO'84. LNCS, pp. 47–53. Springer, Berlin, Heidelberg (1984). https://doi.org/10.1007/3-540-39568-7_5

24. Shor, P.W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Review **41**(2), 303–332 (1999). https://doi.org/10.1137/s0036144598347011
25. Waters, B.: Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, pp. 53–70. Springer, Berlin, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_4
26. Yamada, S., Attrapadung, N., Hanaoka, G., Kunihiro, N.: A Framework and Compact Constructions for Non-monotonic Attribute-Based Encryption. In: Krawczyk, H. (ed.) PKC 2014. LNCS, pp. 275–292. Springer, Berlin, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54631-0_16
27. Yang, Y., Liu, J.K., Liang, K., Choo, K.-K.R., Zhou, J.: Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Encryption of Cloud Data. In: Pernul, G., Ryan, P.Y.A., Weippl, E.R. (eds.) ESORICS 2015, Part II. LNCS, pp. 146–166. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-24177-7_8
28. Zeutro, Zeutro/openabe: The openabe library - open source cryptographic library with attribute-based encryption implementations in C/C++, https://github.com/zeutro/openabe.
29. Zhang, J., Zhang, Z.: "A Ciphertext Policy Attribute-Based Encryption Scheme without Pairings". In: Information Security and Cryptology. Springer Berlin Heidelberg, 2012, 324–340. ISBN: 9783642347047. https://doi.org/10.1007/978-3-642-34704-7_23.
30. Zhang, R., Li, J., Lu, Y., Han, J., Zhang, Y.: Key escrow-free attribute based encryption with user revocation. Information Sciences **600**, 59–72 (2022). https://doi.org/10.1016/j.ins.2022.03.081