RESEARCH ARTICLE OPEN ACCESS

Proxy Re-Encryption Enhanced Envelope Encryption for Fast Data Revocation

Naman Jain
Senior Software Development Engineer Seattle, Washington, USA

Abstract:

This study analyzes the use of proxy re-encryption integrated with enhanced envelope encryption to enable rapid and iterative data revocation in an enterprise-scale environment. The need for such analysis is dictated by the fact that in modern large-scale enterprise and provider-independent platforms, especially those focused on the financial sector, lifecycle management of cryptographic keys and flexible control of data access rights have become critically important. The traditional envelope encryption approach, which dominates most infrastructures, encounters operational difficulties when simultaneous mass key rotation or revocation of permissions is required. Each instance of such an operation necessitates re-encryption (re-packing) of individual Data Encryption Keys (DEK) for every object resource, inevitably resulting in significant computational overhead and increased latency. The methodological foundation of this work includes a systematic review of existing encryption models, analysis of contemporary proxy re-encryption (PRE) schemes, as well as comparative performance measurements. The proposed proxy re-encryption enhanced envelope (PRE-EE) architecture envisages delegating to a trusted proxy the task of transforming encrypted keys, thereby enabling key rotation and access revocation without the need to alter the state of each ciphertext in storage, and achieving the operation in constant time from the perspective of the Key Management Infrastructure (KMI). The results obtained demonstrate that PRE-EE represents a scalable and cost-effective solution that eliminates the primary bottlenecks of traditional envelope encryption systems, while minimizing compute, storage, and network overhead to reduce the operational costs of large-scale key management. Furthermore, the approach is aligned with emerging post-quantum threats, where faster and more frequent rotations reduce risk compared to big-bang re-encryption events. The benefits of adopting this model will be of value to secure-system architects, enterprise-platform engineers, and cybersecurity specialists who aim to develop adaptive and reliable mechanisms for protecting confidential data.

Keywords: proxy re-encryption, envelope encryption, access revocation, key management, interactive renewal, cloud security, enterprise security, cryptography, PRE, fintech, scalability, post-quantum resilience.

Introduction:

Enterprise platforms serve as the primary means of deploying a wide spectrum of digital services - from retail applications to high-load financial systems processing trillions of transactions. At the same time, the volume of information created and stored in a business lifecycle continues to grow exponentially and is estimated to reach approximately 175 ZB by 2025 [1]. Ensuring the confidentiality and integrity of such vast data arrays requires not only highly reliable cryptographic schemes but also adaptive access control mechanisms. In strictly regulated industries - financial (PCI DSS) and healthcare (HIPAA) - key lifecycle management, including periodic replacement and immediate revocation in the event of a compromise risk or changes in internal policies, is not a recommendation but a requirement of both legislation and industry standards [12].

The relevance of the research is determined by the limitations of the classical envelope encryption model. In this scheme each fragment of data is protected by a unique Data Encryption Key (DEK), which is then wrapped using a centralized master key, or key encryption key (KEK), stored in a secure Key Management Infrastructure (KMI) [2]. When security policies change, for example during master key rotation or revocation of user privileges, all DEKs encrypted under the previous KEK must be decrypted and re-encrypted using the new one. In large-scale systems with billions of objects such an operation becomes a “re-encryption storm” - a resource-intensive procedure capable of causing performance degradation, escalating infrastructure costs, and elevating operational risks during the transition period.

The objective of the study is to conduct a comprehensive analysis of the architecture of PRE-Enhanced Envelope Encryption, which employs proxy re-encryption to enable efficient, cost-conscious and scalable key rotation as well as instantaneous revocation of data access in enterprise environments.

The scientific novelty resides in the integration of proxy re-encryption with the traditional envelope encryption model, which allows the primary workload for transforming ciphertexts to be offloaded onto a semi-trusted proxy server, thereby achieving policy updates in constant time from the standpoint of the KMS.

The author's hypothesis is that the use of PRE for re-wrapping DEKs decouples the lifecycle of the data from the lifecycle of the master keys. This separation enables iterative renewal of keys instead of disruptive big-bang rotations, enabling revocation and rotation operations independently of the number of objects. Furthermore, PRE-EE establishes a foundation for post-quantum resilience, as faster and more frequent rotations reduce the operational risk stemming from the vulnerabilities of traditional algorithms to quantum computing attacks. Collectively, these capabilities substantially enhance the scalability, cost-efficiency, and security of the enterprise systems.

Materials and Methods

In recent years the rapid growth of data volumes and the tightening of regulatory requirements for their protection have necessitated the development of efficient encryption mechanisms with the capability for prompt revocation of access. Among the fundamental works analyzing the overall landscape of digital assets and leakage risks are the IDC report The Digitization of the World - From Edge to Core Reinsel D., Gantz J., Rydning J. [1] and the Cost of a Data Breach Report 2024 [12]. These studies demonstrate that the global volume of data being generated exceeds 175 ZB and that the average cost of a data breach globally in 2024 is 4.9 million USD, underscoring the relevance of developing solutions capable of minimizing potential losses by swift invalidation of access rights.

The second group comprises studies devoted to the practice of envelope encryption and enterprise key management. Documentation from the AWS Key Management Service (KMS) describes an architecture in which symmetric encryption keys are locally protected using master keys stored in hardware security modules (HSM) [2]. A similar approach is presented in Google Cloud KMS, where the authors emphasize the advantages of a multilayer model: separate storage of data keys and master keys reduces the attack surface and simplifies management of key rotation [6]. These principles are consistent with the recommendations of the NIST SP 800-57 Part 1 Rev. 5 guideline, which defines hierarchical key-management infrastructures based on envelope encryption, where data-encryption keys (DEKs) are wrapped under key-encrypting keys (KEKs) and securely controlled through cryptographic modules [7]. In parallel, the OASIS Key Management Interoperability Protocol (KMIP) [8] defines a vendor-neutral framework for interoperable key management across hardware security modules, enterprise KMIs, and hybrid environments. It standardizes operations for key creation, wrapping, rotation, and deletion, ensuring consistent lifecycle control across heterogeneous systems. Its practical adoption has been demonstrated through interoperability testing by leading vendors - Thales, IBM, Micro Focus, and Cryptsoft, during the RSA Conference 2020 [9]. Paidy P., Chaganti K. [10] propose scenarios for dynamic operation of KMI in a fault-tolerant architecture without significant performance loss. Finally, Somasundaram P. [13] synthesizes methods of unified secret management in multi-cloud scenarios, focusing on a consistent access policy and centralized audit of key operations.

The third category encompasses cryptographic methods of proxy re-encryption (PRE) aimed to produce secure and flexible delegation of access rights without revealing user's secret keys. For example, Luo F., Al-Kuwari S. [4] propose an attribute-based PRE scheme with attribute-based revocation of rights, enabling finely tuned access policies without the need for direct interaction between the data owner and each recipient. Ren C., et al. [5] advance the concept of certificateless PRE, eliminating the need for a certificate infrastructure and automating the construction of encryption routes for cloud data exchange (Clap-PRE). Chen Y., et al. [14] propose a threshold PRE scheme for IoT environments, combining threshold encryption mechanisms and blockchain to guarantee immutability and decentralized key management. Park H. A. [3] highlights the resilience of a PRE protocol to chosen-ciphertext attacks in critical unmanned networks (FANETs), minimizing computational overhead in the generation of transformation keys and ensuring low latency in data transmission.

Separate attention in the literature is devoted to the integration of PRE with blockchain technology to enhance transparency and manageability of access. Liu G., et al. [11] developed a scheme for exchanging electronic medical records in which blockchain is used to store proofs of authorization and the PRE mechanism for delegating access to encrypted documents without disclosing patients' medical keys. Such a hybrid approach demonstrates potential for increasing trust among network participants but raises questions of scalability, operational efficiency and performance when operating with large blockchains.

Also, within the framework of this study, it is worth paying attention to and reviewing the works of the following authors: Eltayieb N. et al. [15] propose the CLPRE CRF (Certificateless Proxy Reencryption with Cryptographic Reverse Firewall) scheme, combining certificateless PRE and Cryptographic Reverse Firewalls. Ge C. et al. [16] introduce the direct revocation mechanism (ABPRE DR), whereby a proxy server can deactivate re-encryption keys associated with specific attributes without regenerating the master key or re-encrypt the original data, improving the responsiveness of access control.

Thus, contemporary science identifies several key approaches: envelope encryption combined with enterprise-scale Key Management Infrastructures (KMI); various types of PRE schemes (attribute-based, certificateless, threshold) for flexible delegation of access rights; and hybrid architectures combining PRE and blockchain aim to ensure immutability and auditable operations. Despite these advances, the literature reveals the following contradictions and gaps. First, most works on envelope encryption emphasize key management but do not explore integrating PRE for instant revocation of access without the high compute and storage cost of full re-encryption across large data volumes. Second, proposed PRE schemes are typically evaluated only in terms of cryptographic reliability but insufficiently study real-world performance metrics, latency and cost implications in enterprise-scale environments. Third, hybrid PRE-blockchain solutions currently lack a unified interaction standard and require further study of consensus mechanisms with respect for confidentiality requirements. Ultimately, the weakest aspect of existing publications is the comprehensive analysis of end-to-end systems combining envelope encryption, proxy re-encryption, and blockchain while simultaneously addressing performance, cost-efficiency, scalability, and manageability of revocation policies.

Results and Discussion

To address the identified shortcomings of access revocation in classical envelope encryption schemes, an architectural model PRE-Enhanced Envelope Encryption (PRE-EE) is proposed [16]. It integrates the proxy re-encryption mechanism directly into the key management lifecycle, minimizing computational overhead and transforming a traditionally heavy, resource-intensive operation into a fast, scalable and cost-efficient process [3, 11].

The PRE-EE system includes 4 foundational components (see Figure 1):

1. Client - the user or service initiating data read and write requests.
2. Key Management Infrastructure (KMI) - responsible for generation and secure storage of key encryption keys (KEKs), creation of re-encryption keys and administration of access policies
3. Proxy server (Proxy) - a semi-trusted intermediary (for example, an intelligent gateway to the storage) that performs re-encryption of encrypted data encryption keys (DEKs) upon request without having access to either the KEK or plaintext data.
4. Data Store - the persistent repository where encrypted data objects are stored together with their corresponding encrypted DEK [3, 5].

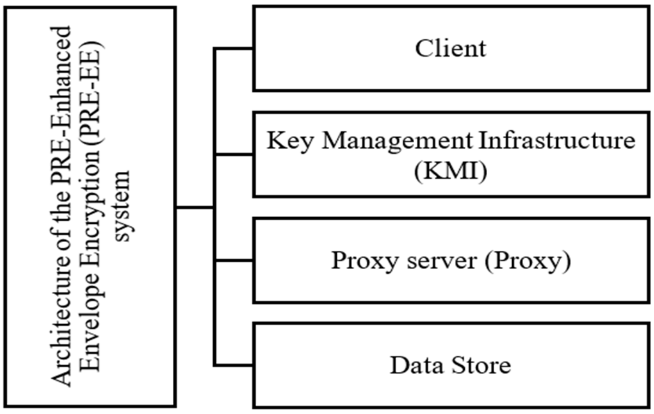

Fig. 1. Architecture of the PRE-Enhanced Envelope Encryption (PRE-EE) system [3, 5, 11, 15].

The procedure for key rotation or access revocation in the proposed architecture comprises the following steps (Fig.2):

- Initial state: All data is protected by a data encryption key container (DEK), and the DEK itself is wrapped by the master key KEK_A corresponding to access policy A.

- Rotation initiation: The administrator defines the task to switch from policy A to policy B (that is, replacing KEK_A with KEK_B) and issues the corresponding command to the key management infrastructure (KMI) [6, 8, 10].

- Generation of the transformation key: Instead of directly re-encrypting each instance of the DEK, the KMI creates a specialized re-encryption key rk_AtoB, intended to convert the existing DEK ciphertext from KEK_A format to KEK_B format. This step removes the need for decrypt and re-encrypt operations on every data object.

- Delegation to the proxy: The rk_AtoB key is securely transferred from the KMI to the proxy server over an authenticated and encrypted channel, preserving channel confidentiality and preventing leakage of key material.

- On the fly transformation: Upon a client request, the proxy server intercepts the wrapped DEK, applies rk_AtoB to generate a new DEK ciphertext wrapped under KEK_B. The updated DEK is returned to the client, which then contacts the KMI for final decryption using KEK_B [4, 13].

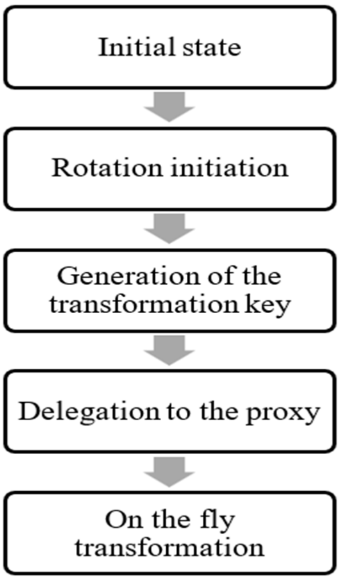

Fig.2. Stages of the procedure for changing the key or revoking access rights in the architecture [4, 6, 10, 13]

Management of the DEK lifecycle in the PRE-EE model acquires an adaptive and policy-driven character. The container key may exist in several encryption states corresponding to different access policies (distinct KEKs), and transitions between these states are executed dynamically by the proxy server.

The key security element in PRE solutions is the proxy component, to which the task of correctly performing the re-encryption operation is delegated; however, its privileges are strictly regulated and constrained, specifically excluding the following capabilities:

- decrypt the data encryption key (DEK) or the original content;
- independently generate re-encryption keys;
- perform reverse re-encryption (from B to A) when using unidirectional schemes;
- collude with a client holding access rights under policy B in order to gain access to data protected under policy A (the non-collusion property) [3, 5].

This restriction of proxy rights allows embedding PRE-EE into architectures built on Zero Trust principles, where each component operates under the assumption of minimal and verifiable trust.

The principal advantage of PRE-EE is the radical reduction of computational and operational resources required for access-right revocation. Consider a system in which N encrypted data objects are stored:

- Traditional approach. Revocation of access requires performing N decryption and N encryption operations on the KMI, resulting in an overall computational complexity of O(N).

- PRE-EE. The revocation procedure is reduced to a single re-encryption key generation operation in the KMI (O(1)), after which the proxy performs on-the-fly re-encryption during each data access. Consequently, for the KMI, the costs of initiating revocation remain constant and do not depend on the number of objects N [3, 8, 10].

Advantages, limitations and future development trends of the proposed architecture are summarized in Table 1.

Table 1. Advantages, Limitations and Future Development Trends of Proxy Re-Encryption Enhanced Envelope Encryption (PRE-EE) for Fast Data Revocation [3, 5, 10, 14]

Category	Key points
Advantages	• High efficiency of access revocation (re-encryption of only the DEK without re-processing the entire ciphertext) • Reduced client, compute and network load (minimal volumes of transmitted data) • Granular access control (attribute-based and conditional policies) • Seamless integration with KMI and envelope encryption workflows.
Limitations	• Requires a semi-trusted proxy (necessity of HSM/TEE and auditing) • Potential exponential growth in the number of re-encryption keys with a large number of users or attributes • Risk of collusion attacks in transitive schemes • Dependence on proxy availability (redundancy and fault tolerance complicate the infrastructure)
Future trends	• Post-quantum PRE schemes based on lattices and LWE • Key-aggregate Proxy Re-Encryption for group keys • Integration with Attribute-Based (ABE-PRE) and Conditional PRE for fine-grained policy enforcement • Homomorphic PRE for secure computation and analysis over encrypted data • Decentralized blockchain-based KMI architectures • Embedding PRE within Trusted Execution Environments (TEE) and hardware security modules

As a practical scenario, consider company N, which grants its partner temporary access to anonymized transactional data for analytical purposes. Access management is implemented through the PartnerX policy associated with the key KEK_PartnerX. Upon expiration of the contract, immediate revocation of the partner's privileges is required to maintain compliance and data confidentiality.

In a traditional architecture, this would necessitate initiating a background task to locate all DEK encrypted with KEK_PartnerX and rewrap them under a new internal key, such as KEK_Internal. This process is labor-intensive, time-consuming, cost-inefficient and increases operational risks during the transition.

By contrast, under the PRE-EE model, the administrator only needs to generate the re-encryption key rk_PartnerXtoInternal and deploy it to the proxy service. From that point forward, any attempt by the partner to decrypt the data with KEK_PartnerX proves futile, as the previous key is effectively obsolete. Meanwhile, internal personnel continue to access resources seamlessly: the proxy performs DEK transformation on the fly. As a result, access revocation occurs instantly and with minimal overhead, which is critical for ensuring information security and potentially meeting regulatory compliance requirements [4, 13].

Thus, the proposed PRE-EE architecture not only eliminates the theoretical limitations of traditional schemes but also provides a powerful tool for constructing flexible, scalable and reliable enterprise key management infrastructures.

Conclusion

Within the scope of the study an architectural model of enhanced envelope encryption with proxy re-encryption (PRE-EE) was proposed. This concept is aimed at eliminating the fundamental limitation of traditional key management systems - the excessive operational costs and latency associated with revoking access to encrypted data and replacing keys.

The strength of the PRE-EE model lies in offloading the cryptographic work of key transformation to a semi-trusted proxy server. This enables the revocation or rotation of access rights for an arbitrary number of resources in constant time from the perspective of the central key management infrastructure (KMI), fundamentally surpassing existing solutions that exhibit linear time complexity.

Thus PRE-EE serves not merely as a theoretical model but also as a practice-oriented engineering solution. The resource-intensive batch procedure of mass re-encryption is transformed into a lightweight, rapid and reliable operation, significantly improving both scalability and resilience. Furthermore, by supporting iterative key renewal and enabling faster rotation cycles, PRE-EE provides a foundation for post-quantum-ready enterprise key-management architectures.

Future Work

The PRE-EE architecture introduced in this study establishes a foundation for scalable, cost-efficient, and policy-driven key management in enterprise environments. Building upon these outcomes, future work can focus on extending the architecture toward broader operational and cryptographic maturity.

A promising direction lies in the scalable deployment of PRE-EE across distributed Key Management Infrastructures (KMI). Investigating optimizations for proxy placement, policy synchronization, and performance under multi-region and multi-tenant workloads will help refine the operational models that govern proxy coordination and its lifecycle automation.

Further advancement may focus on enhancement of security assurance. Incorporating formal verification techniques of proxy operations and hardware-based attestation through Trusted Execution Environments (TEE) can reinforce the guarantees of non-collusion, correctness, and unidirectionality that form the security foundation of PRE-EE deployments.

Finally, another area of exploration involves extending PRE-EE with post-quantum cryptographic capabilities. Implementing lattice and LWE based proxy re-encryption schemes, would ensure long-term resilience against quantum threats while preserving cost efficiency and operational performance.

References

1. Reinsel, D., Gantz, J., Rydning, J. (2018). *The Digitization of the World From Edge to Core*. Retrieved from: https://www.seagate.com/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf (date of access: 10.06.2025).
2. Amazon Web Services. *AWS Key Management Service*. Retrieved from: https://docs.aws.amazon.com/pdfs/kms/latest/cryptographic-details/kms-crypto-details.pdf (date of access: 13.06.2025).
3. Park, H. A. (2024). Secure Proxy Re-Encryption Protocol for FANETs Resistant to Chosen-Ciphertext Attacks. *Applied Sciences, 14*(2), 1–16. https://doi.org/10.3390/app14020761.
4. Luo, F., & Al-Kuwari, S. (2021). Revocable attribute-based proxy re-encryption. *Journal of Mathematical Cryptology, 15*(1), 465–482.
5. Ren, C., et al. (2022). CLAP-PRE: Certificateless Autonomous Path Proxy Re-Encryption for Data Sharing in the Cloud. *Applied Sciences, 12*(9), 1–13. https://doi.org/10.3390/app12094353.
6. Envelope encryption. Retrieved from: https://cloud.google.com/kms/docs/envelope-encryption (date of access: 16.06.2025).
7. NIST SP 800-57 Part 1 Rev. 5 – Recommendation for Key Management (General). National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-57 Part 1 Rev. 5, 1–95. https://doi.org/10.6028/NIST.SP.800-57pt1r5
8. OASIS. (2020). Key Management Interoperability Protocol Specification Version 2.1. Retrieved from: https://docs.oasis-open.org/kmip/kmip-spec/v2.1/os/kmip-spec-v2.1-os.html (date of access: 18.06.2025).
9. OASIS Key Management Interoperability Protocol (KMIP) Technical

Committee. (2020). Interoperability between leading key management vendors demonstrates continued strength of OASIS KMIP standard at RSA 2020. Retrieved from: https://www.prweb.com/releases/interoperability-between-leading-key-management-vendors-demonstrates-continued-strength-of-oasis-kmip-standard-at-rsa-2020-892789938.html (date of access: 18.06.2025)

10. Paidy, P., & Chaganti, K. (2024). Resilient Cloud Architecture: Automating Security Across Multi-Region AWS Deployments. *International Journal of Emerging Trends in Computer Science and Information Technology, 5*(2), 82-93.

11. Liu, G., et al. (2024). A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. *Journal of Cloud Computing, 13*,1-13 .

12. *Cost of a Data Breach Report 2024*. Retrieved from: https://www.ibm.com/reports/data-breach (date of access: 20.06.2025).

13. Somasundaram, P. (2024). Unified secret management across cloud platforms: A strategy for secure credential storage and access. *International Journal of Computer Engineering and Technology (IJCET),*15 (2), 5-12.

14. Chen, Y., et al. (2021). A Threshold Proxy Re-Encryption Scheme for Secure IoT Data Sharing Based on Blockchain. *Electronics, 10*(19), 1–18. https://doi.org/10.3390/electronics10192359.

15. Eltayieb, N. et al. (2025). Certificateless proxy re-encryption with cryptographic reverse firewalls for secure cloud data sharing. *Future Generation Computer Systems*,162. https://doi.org/10.1016/j.future.2024.08.002.

16. Ge, C. et al. (2023). Attribute-based proxy re-encryption with direct revocation mechanism for data sharing in clouds. *ACM TURC '23: Proceedings of the ACM Turing Award Celebration Conference - China 2023*, 164-165. https://doi.org/10.1145/3603165.3607460.