Removing Private Key Generator in Cloud: A Survey on Registration-Based Encryption

***Abstract*—Registration-based encryption (RBE) is reviewed in this article. A taxonomy and comprehensive assessment criteria for RBE are first proposed. In the taxonomy, RBE schemes are assorted into registered identity-based encryption (RIBE) schemes, registered attribute-based encryption (RABE) schemes, and registered functional encryption (RFE). In accordance with cryptographically functional features, RBE is further divided into subcategories with regard to basic functionality, variability, accountability, efficient computation, and large scale. In addition, a systematical methodology for discussing and comparing existing ABE schemes is proposed. For each type of RBE, the corresponding scenario is presented and explained by concrete examples. Specifically, the syntax of RBE is given followed by the adversarial model and security goals. RBE schemes are discussed according to the design strategies and special features and are compared in the proposed assessment criteria with respect to security and performance. To our knowledge, this survey is the first one to make a comprehensive and holistic comparison. Finally, a number of open research challenges in ABE are pointed out.**

***Index Terms*—**

I. Introduction

Since the notion of registered identity-based encryption (RIBE) was proposed by [1], registration-based encryption (RBE) has attracted the interest of a number of researchers. Following Garg et al.'s work, a large number of RIBE schemes has been proposed [2]–[9]. Meanwhile, Hohenberger et. al. extended RBE to attribute-based encryption and proposed registered attribute-based encryption (RABE) in 2023 [10]. Right After that, numbers of researchers followed their work [11]–[13]. Later, Datta et. al. introduced the registered functional encryption (RFE), which presented the formal generic RBE with generalized functions [14]. This topic also attracts lots of researcher's interests [15]–[18].

In this work, we reviewed existing works on RBE, including RIBE, RABE, and RFE.

Registered Identity-Based Encryption. Registered identity-based encryption (RIBE) is proposed by [1]–[9] to address the key-escrow problem in the setting of identity-based encryption (IBE). In a RIBE scheme, private keys and ciphertexts are associated with identities and decryption succeeds if the identities associated with the private key and ciphertexts match, which is the exactly same as IBE. However, the IBE removes the private key generator (PKG) while involves a "key curator (KC)". The role of the KC is not to issue private decryption keys for users but instead to aggregate (register) the public keys and ids from registered users into public parameters.

In more detail, users in a RIBE scheme generate their own public/private key pairs (like in traditional public-key encryption) and then request the KC to register their public keys and their ids. The KC then registers them by implicitly embedding these public keys and ids in public parameters. Users encrypt data as it performing in IBE, i.e., the data is encrypted with public parameters and the recipient id. However, for the recipient, the decryption requires the corresponding updated helper key and private key. Therefore, before a decryption operation, the recipient must obtain the latest corresponding helper key. This helper key derives from the public parameters by the KC and also implicitly includes the recipient's id. Consequently, RIBE achieves the functionality of IBE, i.e., only the recipient whose id satisfies the encrypted data can decrypt it correctly.

Since the public parameters of the RIBE scheme changes whenever new users join the system, users must periodically refresh their helper key over the lifetime of the system. Note that the helper key for each user can be computed publicly, and importantly, in an RIBE system, the KC does not possess any secret information.

Registered Attribute-Based Encryption. A registered attribute-based encryption (RABE) [10]–[13], [19] applies the same idea as RIBE, which is removing the PKG. Similar to RIBE, in a RABE system, the KC registers users' self generated public keys and their attribute sets by updating the public parameters. The aggregated public key function as a public key for a standard ABE scheme. Since the key curator maintains no long-term secrets and can be publicly audited, RABE serves as a new paradigm for enabling the access-control capabilities of ABE without introducing a trusted key-issuing authority into the picture. Previously, the work of [10] showed how to construct RABE for an a prior bounded number of users using pairing-based assumptions in a model with a structured common reference string, as well as a scheme for an unbounded number of users in the common random string model.

Registered Functional Encryption. In registered functional encryption RFE [14]–[18] removes the PKG from the functional encryption (FE) and applies a KC instead. Different from either RIBE and RABE, the KC in RFE registers the public keys and a specific function for the registered users.

Conceptually, RFE covers the notion of RABE and RIBE. Specifically, in RABE, the registered function is a function that if attribute-set fulfills the ciphertext, then outputs data. While the registered function is a function that if identity fulfills encrypted identity, then outputs data.

Registration-Based Encryption. In this work, we introduce the notion of Registration-Based Encryption (RBE), which is the abstract of RIBE, RABE, and RFE.

Two crucial features are applied for all types of RBE: 1) all actions performed by the KC are deterministic and transparent for audition; and 2) public parameters and helper keys should be compact and update procedure must be efficient; ideally, objective sizes and algorithm costs are poly-logarithmic in the number of registered users in the system.

Specifically, if n users registered, then each user only needs to update their helper keys at most $O(\log n)$ times over the lifetime of the system. The size of helper keys and public parameters should also be short (i.e., poly$(\lambda, \log n)$, where λ is a security parameter).

The contributions of this work includes:

- Taxonomy and Assessment criteria: a clear taxonomy and comprehensive assessment criteria of RBE are proposed. According to the taxonomy, RBE is categorized into RIBE, RABE, and RFE.
- Comprehensive Analysis: a systematical methodology for analysis existing RBE schemes is proposed. Specifically, application scenario of RBE is demonstrated with detailed examples. Next, the syntax of RBE is introduced and is followed by thread model and security goals. Moreover, the state-of-the-art for RBE is analysis in terms of design strategies, dependent cryptography tools, and special features in detail. Finally, a comprehensive comparison is illustrated in terms of the proposed assessment criteria with respect to security and performance.
- Research Challenges: a number of open research challenges are highlighted from the analysis of the state-of-the-art of RBE.W

II. Taxonomy And Assessment Criteria Of RE

A. Taxonomy Of RBE

According to the functionality, the proposed taxonomy of RBE includes three main categories: RIBE, RABE, and RFE. Besides, according to the use of dependent cryptography prototypes, basic schemes of RBE fall in non-black-box and black-box. Furthermore, enhanced RBE schemes further realizes other cryptography functional features, including variability, efficient computation, accountability, and large scale.

- Verifiable RBE. Verifiable RBE allows any third party to verify the pre-registration and post-registration of the KC.
- Accountable RBE. The accountable CP-ABE involves the KC accountability.
- Efficient RBE. The efficient RBE explores efficient computation in the algorithms in KC and efficient storage of master pubic keys and common reference string structures.
- Large Scale RBE. Large scale RBE enables the scheme to register large amount of users efficiently without the setup of a bounder.

B. Assessment Criteria of RBE

For a systematic comparison of existing RBE schemes, we present the assessment criteria with respect to security and performance. It is noted that the assessment criteria are proposed for fairly evaluating the properties claimed in different RBE schemes.

1) Security Assessment Criteria:

- Type of Adversaries. Since the registration algorithm is deterministic, there are only selective adversaries considered in RBE.
- Security Model. According to whether random oracles are used in the security analysis, the security models are categorized into the standard mode (STM) and the random oracle model (ROM). the ROM means that random oracles are involved in the model. A random oracle is a black box that responds to each query by giving a random value chosen uniformly from its output domain. If a query is repeated, it returns the same value as before.
- Complexity Assumption. An RBE scheme's security is usually reduced to the adopted complexity assumptions. It is more desirable to prove the security under the recognized assumptions, of which the form is concise and the complexity is proved. The security proofs under complexity assumptions of concise forms are technically challenging, because fewer parameters are provided by the assumption instance and used by the challengers.

2) Performance Assessment Criteria:

- Common Reference String Size. This parameter is relevant to the storage overhead.
- Master Public Key Size. This parameter is relevant to the communication and storage overhead.
- Ciphertext Size. This parameter is relevant to the communication and storage overhead.
- Helper Decryption Key Size. This parameter is relevant to the communication and storage overhead.
- Setup Computation Cost.
- Registration Computation Cost.
- Update Computation Cost.
- Encryption Computation Cost.
- Decryption Computation Cost.
- Group. The groups involved in black-box RBE are divided into prime-order groups and composite order groups according to the group order. It is noted that the prime-order ABE construction is more desirable than the composite-order ABE construction from the viewpoint of efficiencies. However, if full security is required, the design of prime-order ABE is technically more challenging than that of composite-order ABE, because the methodology for full security proofs usually relies on composite-order groups.

III. RIBE

A. Application Scenario

RIBE removes the PKG from IBE and enables users to generate theirs own public keys and private keys.

B. Syntax

Definition (Syntax of RIBE). A registration-based encryption (RIBE) scheme consists of PPT of PPT algorithms (Gen, Reg,Enc, Upd, Dec) working as follows. The Reg and Upd algorithms are performed by the KC.

- Setup. $Setup(\lambda) \rightarrow crs$. Some of the subroutines below will need a common random string crs, which could be sampled publicly using some public randomness beacon.
- Key generation. $Gen(\lambda) \rightarrow (pk, sk)$. The randomized algorithm Gen takes as input the security parameter λ and outputs a pair of public/secret keys (pk, sk). Note that these are only public and secret keys, not the encryption or decryption keys. The key generation algorithm is run by any honest party locally who wants to register itself into the system.
- Registration. $Reg(crs, pp, id, pk) \rightarrow pp'$. The deterministic4 algorithm Reg takes as input the common random sting crs, current public parameters pp, a registering identity id and a public key pk (supposedly for the identity id), and it outputs pp' as the updated public parameters.
- Encryption. $Enc(crs, pp, id, m) \rightarrow ct$. The randomized algorithm Enc takes as input the common random sting crs, the current public parameters pp, a recipient identity id and a plaintext message m and outputs a ciphertext ct.
- Update. $Upd(pp, id) \rightarrow hpk$. The deterministic algorithm Upd takes as input the current public parameters pp and an identity id, and generates an update helper key hpk that can help user id to decrypt its messages.
- Decryption. $Dec(sk, hpk, ct) \rightarrow m$: The deterministic decryption algorithm Dec takes as input a secret key sk, an helper key hpk, and a ciphertext ct, and it outputs a message m.

C. Adversarial Model and Security Goals

All KCs in RBEs are falled into semi-trusted and transparent. Semi-trusted stands for that the KC is honestly performing the protocols but curious about the sensitive information from users, including private keys and shared data among users. Transparent stands for that the KC keeps no secret and operates deterministically. In such a way, KC is easy to be audited by any party.

All RBEs should satisfy Data Confidentiality and Collusion Resistance.

- Data Confidentiality: in a RBE system, if a user is unauthorized user, it should be blocked from decrypting the ciphertext. In addition, the KC should not be allowed to decrypt ciphertexts without authorization.
- Collusion Resistance: a RBE system should prevent collusion attacks from unauthorized users and the KC.

D. Research Status

This section aims to analyze the state-of-the-art schemes of RIBEs [1]–[9] in terms of design strategies, dependent cryptography tools, and special feature.

E. Comparison

The comparison is carried out from the proposed security assessment criteria and performance assessment criteria and comes with a clear table.

IV. RABE

RABE removes private key generator from ABE, particular ciphertext-policy ABE (CP-ABE), and enables users to generate theirs own public keys and private keys.

A. Syntax

Definition (Syntax of RABE). A registered identity-based encryption (RABE) scheme consists of PPT of PPT algorithms (Gen, Reg,Enc, Upd, Dec) working as follows. The Reg and Upd algorithms are performed by the KC.

- Setup. $Setup(\lambda) \rightarrow crs$. Some of the subroutines below will need a common random string crs, which could be sampled publicly using some public randomness beacon.
- Key generation. $Gen(\lambda) \rightarrow (pk, sk)$. The randomized algorithm Gen takes as input the security parameter λ and outputs a pair of public/secret keys (pk, sk). Note that these are only public and secret keys, not the encryption or decryption keys. The key generation algorithm is run by any honest party locally who wants to register itself into the system.
- Registration. $Reg(crs, pp, S, pk) \rightarrow pp'$. The deterministic4 algorithm Reg takes as input the common random sting crs, current public parameters pp, a set of user attributes S and a public key pk (supposedly for the identity id), and it outputs pp' as the updated public parameters.
- Encryption. $Enc(crs, pp, \mathbb{A}, m) \rightarrow ct$. The randomized algorithm Enc takes as input the common random sting crs, the public parameters pp, an access policy structure $\mathbb{A}$ and a plaintext message m and outputs a ciphertext ct.
- Update. $Upd(pp, pk) \rightarrow hpk$. The deterministic algorithm Upd takes as input the current public parameters pp and a user public key pk, and generates a helper key hpk that can help the user to decrypt its messages.
- Decryption. $Dec(sk, hpk, ct) \rightarrow m$: The deterministic decryption algorithm Dec takes as input a secret key sk, a helper key hpk, and a ciphertext ct, and it outputs a message m.

B. Adversarial Model and Security Goals

As mentioned in section III.C, the adversarial model of ABE also follows the semi-trusted and transparent KC.

RABE should also satisfy Data Confidentiality and Collusion Resistance.

C. Research Status

This section aims to analyze the state-of-the-art schemes of RABEs [10]–[13], [19] in terms of design strategies, dependent cryptography tools, and special feature.

D. Comparison

The comparison is carried out from the proposed security assessment criteria and performance assessment criteria and comes with a clear table.

V. RFE

RFE removes private key generator from FE and enables users to generate theirs own public keys and private keys.

A. Syntax

Definition (Syntax of RFE). A registered functional encryption (RABE) scheme consists of PPT of PPT algorithms (Gen, Reg,Enc, Upd, Dec) working as follows. The Reg and Upd algorithms are performed by the KC.

- Setup. $Setup(\lambda) \rightarrow crs$. Some of the subroutines below will need a common random string crs, which could be sampled publicly using some public randomness beacon.
- Key generation. $Gen(\lambda) \rightarrow (pk, sk)$. The randomized algorithm Gen takes as input the security parameter λ and outputs a pair of public/secret keys (pk, sk). Note that these are only public and secret keys, not the encryption or decryption keys. The key generation algorithm is run by any honest party locally who wants to register itself into the system.
- Registration. $Reg(crs, pp, f, pk) \rightarrow pp'$. The deterministic4 algorithm Reg takes as input the common random sting crs, current public parameters pp, a function $f \in \mathcal{F}$ and a public key pk (supposedly for the identity id), and it outputs pp' as the updated public parameters.
- Encryption. $Enc(crs, pp, m) \rightarrow ct$. The randomized algorithm Enc takes as input the common random sting crs, the public parameters pp and a plaintext message m and outputs a ciphertext ct.
- Update. $Upd(pp, pk) \rightarrow hpk$. The deterministic algorithm Upd takes as input the current public parameters pp stored at the KC and a user pubic key pk, and generates an helper key hpk that can help the user to decrypt its messages.
- Decryption. $Dec(sk, hpk, ct) \rightarrow m$: The deterministic decryption algorithm Dec takes as input a secret key sk, a helper key hpk, and a ciphertext ct, and it outputs a message m.

B. Adversarial Model and Security Goals

As mentioned in section III.C, the adversarial model of RFE also follows the semi-trusted and transparent KC.

RFE should also satisfy Data Confidentiality and Collusion Resistance.

- Data Confidentiality in RFE: in a RFE system, if a user is unauthorized user, it should be blocked from decrypting the ciphertext. In addition, the KC should not be allowed to decrypt ciphertexts without authorization. Furthermore, in a RFE system, an authorized user should only gain the function value $f(m)$ from the ciphertext and nothing else about the message m.
- Collusion Resistance in RFE: a RFE system should prevent collusion attacks from unauthorized users and the KC.

C. Research Status

This section aims to analyze the state-of-the-art schemes of RFE [14]–[18] in terms of design strategies, dependent cryptography tools, and special feature.

D. Comparison

The comparison is carried out from the proposed security assessment criteria and performance assessment criteria and comes with a clear table.

VI. Conclusion and Future Directions

As data security regulations from governments become increasingly stringent and the demand for robust data protection grows, RBE is poised to play a crucial role in securing cloud environments.

This paper presents a comprehensive overview of the state-of-the-art in RBE. First, we propose a taxonomy that classifies RBE into RIBE, RABE (Registration-Based Attribute-Based Encryption), RFE, as well as non-black-box and black-box RBE.

We then introduce a thorough and holistic assessment framework for evaluating RBE schemes. Each type of RBE is systematically analyzed in terms of application scenarios, adversarial models, security goals, design strategies, and key features. Furthermore, comparisons between RBE schemes are conducted with respect to the proposed assessment criteria.

On the top of the presented comprehensive overview, there are a lot of challenging and interesting problem existing on RBE research.

- *Stronger security*. RBE should ensure both data confidentiality and data integrity.
- *Robust Feature Adoption*. Existing robust features from IBE, ABE, and FE schemes can potentially be integrated into RBE. For instance, revocable RBE allows the Key Curator (KC) to revoke registered users. In this scenario, RBE must ensure both forward and backward security—preventing revoked users from accessing future encrypted data and ensuring that past data remains inaccessible to newly registered users.
- *Efficiency*. There remains significant potential for enhancing the efficiency of RBE schemes, especially in scenarios involving large-scale user bases. Optimizing computation and communication overhead is critical to ensure practical deployment in large systems.
- *Anti-Quantum*. As quantum computing technology progresses, it is widely recognized that many public-key encryption schemes, including RBE, require security enhancements to withstand potential quantum attacks.

ACKNOWLEDGMENT

REFERENCES

[1] S. Garg, M. Hajiabadi, M. Mahmoody, and A. Rahimi, "Registration-based encryption: removing private-key generator from ibe," in *Theory of Cryptography: 16th International Conference, TCC 2018, Panaji, India, November 11–14, 2018, Proceedings, Part I 16*. Springer, 2018, pp. 689–718.

[2] S. Garg, M. Hajiabadi, M. Mahmoody, A. Rahimi, and S. Sekar, "Registration-based encryption from standard assumptions," in *IACR international workshop on public key cryptography*. Springer, 2019, pp. 63–93.

[3] R. Goyal and S. Vusirikala, "Verifiable registration-based encryption," in *Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part I 40*. Springer, 2020, pp. 621–651.

[4] K. Cong, K. Eldefrawy, and N. P. Smart, "Optimizing registration based encryption," in *IMA International Conference on Cryptography and Coding*. Springer, 2021, pp. 129–157.

[5] N. Glaeser, D. Kolonelos, G. Malavolta, and A. Rahimi, "Efficient registration-based encryption," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 1065–1079.

[6] M. Mahmoody, W. Qi, and A. Rahimi, "Lower bounds for the number of decryption updates in registration-based encryption," in *Theory of Cryptography Conference*. Springer, 2022, pp. 559–587.

[7] M. Hajiabadi, M. Mahmoody, W. Qi, and S. Sarfaraz, "Lower bounds on assumptions behind registration-based encryption," in *Theory of Cryptography Conference*. Springer, 2023, pp. 306–334.

[8] D. Fiore, D. Kolonelos, and P. d. Perthuis, "Cuckoo commitments: registration-based encryption and key-value map commitments for large spaces," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2023, pp. 166–200.

[9] Q. Wang, R. Li, Q. Wang, D. Galindo, S. Chen, and Y. Xiang, "Transparent registration-based encryption through blockchain," *Distributed Ledger Technologies: Research and Practice*, vol. 2, no. 1, pp. 1–14, 2023.

[10] S. Hohenberger, G. Lu, B. Waters, and D. J. Wu, "Registered attribute-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2023, pp. 511–542.

[11] Z. Zhu, K. Zhang, J. Gong, and H. Qian, "Registered abe via predicate encodings," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2023, pp. 66–97.

[12] Y. Zhang, J. Zhao, Z. Zhu, J. Gong, and J. Chen, "Registered attribute-based signature," in *IACR International Conference on Public-Key Cryptography*. Springer, 2024, pp. 133–162.

[13] C. Freitag, B. Waters, and D. J. Wu, "How to use (plain) witness encryption: Registered abe, flexible broadcast, and more," in *Annual International Cryptology Conference*. Springer, 2023, pp. 498–531.

[14] P. Datta and T. Pal, "Registration-based functional encryption." *IACR Cryptol. ePrint Arch.*, vol. 2023, p. 457, 2023.

[15] D. Francati, D. Friolo, M. Maitra, G. Malavolta, A. Rahimi, and D. Venturi, "Registered (inner-product) functional encryption," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2023, pp. 98–133.

[16] P. Branco, R. W. Lai, M. Maitra, G. Malavolta, A. Rahimi, and I. K. Woo, "Traitor tracing without trusted authority from registered functional encryption," *Cryptology ePrint Archive*, 2024.

[17] Z. Zhu, J. Li, K. Zhang, J. Gong, and H. Qian, "Registered functional encryptions from pairings," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2024, pp. 373–402.

[18] Q. Chu, L. Lin, C. Qian, and J. Chen, "Registered functional encryption for quadratic functions from mddh," *Cryptology ePrint Archive*, 2024.

[19] R. Garg, G. Lu, B. Waters, and D. J. Wu, "Reducing the crs size in registered abe systems," in *Annual International Cryptology Conference*. Springer, 2024, pp. 143–177.

APPENDIX