International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

IDENTITY-BASED ENCRYPTION WITH CLOUD REVOCATION AUTHORITY AND ITS APPLICATIONS

[1]M.USHA,[2]K.R.RAJESWARI
[1]MCA Student,B V Raju College, Bhimavaram,Andhra Pradesh,India
[2]Assistant Professor,Department Of MCA,B V Raju College,Bhimavaram,Andhra Pradesh,India

ABSTRACT

Identity-Based Encryption (IBE) is a public key cryptosystem that eliminates the need for a Public Key Infrastructure (PKI) and certificate management in traditional public key settings. However, the lack of PKI introduces a significant challenge—revocation. Various revocable IBE schemes have been proposed to address this issue. Recently, Li et al. integrated an outsourcing computation technique into IBE, introducing a revocable IBE scheme with a Key-Update Cloud Service Provider (KU-CSP). However, their approach suffers from two major limitations: high computational and communication costs compared to previous revocable IBE schemes and poor scalability, as the KU-CSP must maintain a unique secret value for each user. To overcome these limitations, we propose a novel revocable IBE scheme incorporating a Cloud Revocation Authority (CRA). Our approach significantly enhances performance and improves scalability by requiring the CRA to store only a single system-wide secret for all users. Through security analysis, we demonstrate that our scheme achieves semantic security under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. Additionally, we extend our revocable IBE framework to develop a CRA-assisted authentication scheme with period-limited privileges, facilitating secure and efficient management of diverse cloud services.

Keywords: Identity-Based Encryption (IBE), Revocation, Cloud Revocation Authority (CRA), Key-Update Cloud Service Provider (KU-CSP), Semantic Security, Decisional Bilinear Diffie-Hellman (DBDH), Outsourced Computation, Cryptographic Scalability, Cloud Security, Authentication Scheme

I.INTRODUCTION

Identity-Based Public Key Systems (ID-PKS) [1], [2] present a compelling alternative to traditional public key cryptography by eliminating the need for a Public Key Infrastructure (PKI) and certificate management. In an ID-PKS setting, users rely on a trusted third party, known as the Private Key Generator (PKG), to generate their private keys based on an associated identity, such as an email address, name, or social security number. This eliminates the need for certificates and PKI-based validation processes. Identity-Based Encryption (IBE) allows a sender to encrypt messages using the recipient's identity as a public key, without requiring validation through a certificate authority. The recipient then decrypts the ciphertext using the private key linked to their identity. However, like conventional public key systems, ID-

PKS must incorporate a user revocation mechanism to address security concerns arising from compromised or misbehaving users. In traditional public key cryptography, Certificate Revocation Lists (CRLs) [3] are a well-known solution for revocation. When verifying a public key and its certificate, a party must check the CRL to ensure that the key has not been revoked. This process, however, introduces performance bottlenecks due to the continuous need for online validation within PKI frameworks. To mitigate these inefficiencies, various optimized revocation mechanisms [4], [5], [6], [7], [8] have been developed for PKI-based systems. Given the importance of revocation in secure communication, researchers have also focused on developing efficient revocation mechanisms tailored to ID-PKS settings. As a result, several revocable IBE schemes have been proposed to address the revocation challenge in identity-based cryptographic environments.

1.1 Related Work

The concept of Identity-Based Encryption (IBE) was first introduced by Boneh and Franklin [2] in 2001, leveraging the Weil pairing to create a practical IBE scheme. They also proposed a simple revocation mechanism in which the Private Key Generator (PKG) periodically issues new private keys to all non-revoked users. The sender encrypts messages using the recipient's identity along with the current time period, ensuring that only users with up-to-date keys can decrypt them. However, this approach requires a secure channel for key distribution, leading to significant overhead for the PKG.

To reduce the PKG's computational burden, Boneh et al. [9] introduced the **immediate revocation method**, which relies on an online semi-trusted mediator to assist users in decryption. This method prevents revoked users from decrypting messages by stopping their access to decryption assistance. However, as the number of users grows, this approach introduces a bottleneck due to the mediator's heavy decryption workload.

In 2008, Boldyreva et al. [14] improved key update efficiency by employing the **complete subtree method** from Fuzzy IBE [35]. This approach reduced the number of key updates from linear to logarithmic in the number of users. While this method alleviated some of the PKG's workload, it introduced other inefficiencies:

1. Each user's private key size was proportional to 3log⁡f0n3\log n elliptic curve points, where nn is the number of users.
2. The encryption and decryption processes were computationally intensive.
3. The PKG still bore the burden of maintaining a binary tree structure for large user bases.

Libert and Vergnaud [16] enhanced the security of Boldyreva et al.'s revocable IBE scheme by introducing an **adaptive-ID secure scheme**. Later, Seo and Emura [17] identified **decryption key exposure attacks** and modified the revocation mechanism accordingly. To further optimize key sizes, Park et al. [18] employed **multilinear maps**, but this approach caused the size of public parameters to scale with the number of users. Wang et al. [19] sought to maintain constant public parameter size by integrating the **dual system encryption methodology** [20] with the complete subtree method.

Seo and Emura [21] extended these ideas into the **Hierarchical IBE (HIBE) model**, where each user generates a secret key by combining partial keys from their hierarchical ancestors. However, this scheme suffered from quadratic growth in key size as users moved deeper into the hierarchy. Seo and Emura later proposed a **history-free update mechanism** [22] to simplify the key update process, though their method still relied on a secure channel for periodic key transmission.

Tseng and Tsai [23] addressed this issue in 2012 by removing the need for a secure In 2015, Li et al. [24] introduced outsourcing computation to reduce the PKG's workload by delegating key updates to a Key-Update Cloud Service Provider (KU-CSP). They adopted Tseng and Tsai's two-key structure, with the PKG generating a random secret value (time key) for each user and sending it to the KU-CSP. The KU-CSP then generated the user's time update key and transmitted it via a public channel. Revocation was managed by instructing the KU-CSP to stop issuing updates for specific users.

While Li et al.'s approach alleviated the PKG's burden, it had two critical drawbacks:

1. **High computational and communication costs** compared to previous revocable IBE schemes [2], [23].
2. **Lack of scalability**, as the KU-CSP needed to maintain a separate time key for each user, resulting in high management overhead.

Given these limitations, there remains a need for a more **efficient and scalable** revocable IBE scheme that minimizes computational costs while improving security and usability.

channel, instead splitting each user's private key into two components:

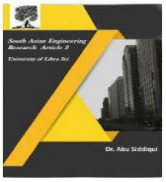
- An identity key, which remains fixed and is securely transmitted once.
- A time update key, which is periodically updated and sent over a public channel.

To revoke a user, the PKG simply stops issuing new time update keys. However, the computational overhead for the PKG remained high due to the linear nature of the update process.

1.2 Our Contributions

To address the scalability and efficiency limitations in Li et al.'s scheme [24], we propose a new revocable Identity-Based Encryption (IBE) scheme that introduces a **Cloud Revocation Authority (CRA)**. Our approach integrates the advantages of both Tseng and Tsai's revocable IBE scheme [23] and Li et al.'s scheme [24] while overcoming their shortcomings.

In our proposed scheme, each user's private key is still composed of an identity key and a time update key, as in previous schemes. However, instead of relying on a Key-Update Cloud Service Provider (KU-CSP), we introduce a Cloud Revocation Authority (CRA) to handle key updates and revocation. Unlike the KU-CSP, which requires storing a unique secret key for each user, the CRA only maintains a single master time key for all users. The CRA periodically generates current time update keys for non-revoked users and transmits them via a public channel. This approach significantly



improves scalability, reducing both storage and management overhead.

In this article, we first present the **framework** of our revocable IBE scheme with CRA, defining its security properties and comparing it with existing schemes, including Tseng and Tsai's revocable IBE scheme [23] and Li et al.'s KU-CSP-based scheme [24]. Our analysis considers multiple factors such as:

- The key update mechanism and channel requirements
- The size of each user's private key
- The computational load for key updates
- The extent of outsourced computation
- The workload distribution between the PKG and cloud entities
- The overall scalability of the revocation mechanism

Subtree-based IBE schemes [14], [16], [17], [18], [19] and HIBE schemes [21], [22] have leveraged the **complete subtree method** to reduce the number of key updates from **linear to logarithmic** in the number of users. However, these schemes still suffer from key size issues, with each user's private key being **O(log n)**, where **n** is the total number of users. Furthermore, these approaches rely on secure channels for private key distribution, with no additional authority to assist in user revocation.

In contrast, Tseng and Tsai's revocable IBE scheme [23] introduced a division of keys into **identity keys and time update keys**, both issued by the PKG. While this reduces the key management burden, the PKG still handles all user revocations. To further distribute the workload, Li et al. [24] introduced a **KU-CSP**, allowing an external entity to manage time update keys. However, Li et al.'s scheme lacks **scalability**, as the KU-CSP must store and manage **n individual time keys** for **n users**, leading to increased overhead.

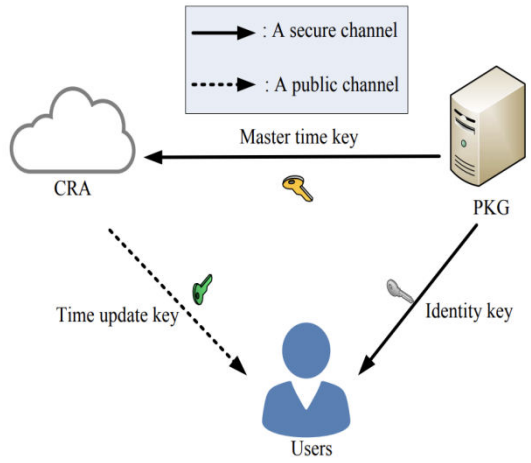
Our proposed scheme enhances scalability by employing a **CRA** instead of a KU-CSP. The key advantages of our approach include:

1. **Single Master Time Key**: The CRA maintains only **one master time key** for all users, eliminating the need for per-user secret values.
2. **Improved Scalability**: Unlike Li et al.'s scheme, where the KU-CSP requires storage for **n different time keys**, our scheme enables a **single CRA** to handle all users efficiently.
3. **Flexible Expansion**: When the number of users **n** grows significantly, multiple CRAs can be deployed to **distribute the revocation workload**, with each CRA holding the same master time key.
4. **Cloud Integration**: Since cloud computing provides a scalable and distributed environment, deploying multiple CRAs enhances **efficiency** and **fault tolerance**, reducing the burden on a single PKG.

In the later sections, we provide a detailed security analysis of our scheme. We formally prove that our approach is semantically secure against adaptive-ID and chosen-ciphertext attacks (CCA) in the random oracle model, relying on the bilinear decision Diffie-Hellman (DBDH) problem

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

[2].



Additionally, leveraging our **revocable IBE scheme with CRA**, we construct a **CRA-aided authentication scheme** that enables **period-limited privileges** for efficiently managing a **large number of cloud services**.

To illustrate the performance improvements of our approach, **Table 1** presents a comparative analysis of subtree-based IBE schemes [14], [16], [17], [18], [19], HIBE schemes [21], [22], and Tseng-Tsai's scheme [23]. The comparison focuses on computational efficiency, communication overhead, and scalability, highlighting the advantages of our proposed CRA-based revocable IBE scheme.

Operation Overview

The PKG selects a master secret key (α) and a master time key (β) and determines the total number of time periods (z). The master time key (β) is securely transmitted to the CRA.

User Identity Key Distribution:

The PKG generates an identity key (D_ID) for each user based on their identity (ID).This key is securely shared with the user.

Security Considerations

The proposed scheme is **IND-ID-CCA-secure** (identity-based encryption secure against chosen-ciphertext attacks), which will be formally proven in the next section.

Additionally, by omitting **W** from the ciphertext **C = (U, V, W)** and using only **C = (U, V)**, we obtain a simpler **IND-ID-CPA-secure** (chosen-plaintext secure) version of the scheme.

Notably, previous schemes such as those by Tseng and Tsai [23] and Li et al. [24] are only **IND-ID-CPA-secure**. To achieve **IND-ID-CCA** security, they require additional transformation techniques [26, 27], which involve adding a hash value **W** to the ciphertext—an approach already integrated into our proposed scheme.

Proof Sketch:
Assume that an adversary EEE can break the proposed CRA-aided authentication scheme with period-limited privileges. We will use EEE to construct an algorithm FFF that can win the IND-ID-CPA security games (Games 1 and 2) of the revocable IBE scheme with CRA.

II.LITERATURE SURVEY

1. Identity-Based Cryptosystems and Signature Schemes (A. Shamir, 1984)

Shamir introduced the concept of Identity-Based Cryptography (IBC), which eliminates the need for traditional Public Key Infrastructure (PKI). In IBC, a user's public key is derived from an easily

recognizable identity, such as an email address, while a trusted authority issues the corresponding private key. This innovation significantly reduces key management complexities and laid the foundation for further research in Identity-Based Encryption (IBE) and digital signatures.

2. Identity-Based Encryption from the Weil Pairing (Boneh & Franklin, 2001)

Boneh and Franklin proposed the first practical Identity-Based Encryption (IBE) scheme based on bilinear pairings, specifically the Weil pairing. Their scheme provided semantic security under the random oracle model and supported public key encryption without requiring digital certificates. This work became a cornerstone in the field of cryptographic applications, particularly for secure email and digital identity management.

3. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (Housley et al., 2002)

This work defined the X.509 certificate standard and the associated Certificate Revocation List (CRL) framework, which is used for managing public key infrastructure (PKI). The X.509 standard is widely adopted in securing network communications, including SSL/TLS, and addresses key issues such as key distribution, authentication, and certificate validity.

4. Fast Digital Identity Revocation (Aiello et al., 1998)

Aiello et al. proposed a cryptographic approach for efficiently revoking digital identities. Their work improved the efficiency of certificate revocation mechanisms by optimizing CRL distribution and lookup times. This was a crucial advancement in ensuring timely and scalable revocation of compromised or expired digital identities.

5. Certificate Revocation and Certificate Update (Naor & Nissim, 2000)

Naor and Nissim presented efficient data structures and cryptographic techniques for certificate revocation and update processes. Their methods significantly reduced the computational and communication overhead associated with verifying certificate status, improving the performance of PKI systems.

III.CONCLUSION

In this article, we introduced a novel revocable identity-based encryption (IBE) scheme incorporating a cloud revocation authority (CRA). The CRA is responsible for handling the revocation process, thereby reducing the computational burden on the private key generator (PKG). While Li et al.'s revocable IBE scheme with a key-update cloud service provider (KU-CSP) also employs an outsourced computation approach, their scheme incurs higher computational and communication costs compared to existing IBE schemes. Additionally, their KU-CSP must maintain a secret value for each user during the time key update process, limiting scalability.

In contrast, our proposed revocable IBE scheme with CRA enhances efficiency by allowing the CRA to manage time key updates using a single master time key for all users without compromising security. This design significantly improves computational and communication performance compared to Li et al.'s scheme. Through experimental evaluation and

performance analysis, we have demonstrated that our scheme is highly efficient and well-suited for mobile devices.

From a security standpoint, we have proven that our scheme is semantically secure against adaptive identity-based attacks under the decisional bilinear Diffie-Hellman assumption. Furthermore, leveraging the proposed revocable IBE scheme with CRA, we developed a CRA-aided authentication scheme with period-limited privileges, designed to efficiently manage access across multiple cloud services.

IV.REFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," Proceedings of Crypto'84, LNCS, vol. 196, pp. 47–53, 1984.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Proceedings of Crypto'01, LNCS, vol. 2139, pp. 213–229, 2001.

[3] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," IETF, RFC 3280, 2002.

[4] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," Proceedings of Crypto'98, LNCS, vol. 1462, pp. 137–152, 1998.

[5] M. Naor and K. Nissim, "Certificate revocation and certificate update," IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, pp. 561–570, 2000.

[6] S. Micali, "Novomodo: Scalable certificate validation and simplified PKI management," Proceedings of the 1st Annual PKI Research Workshop, pp. 15–25, 2002.

[7] F. F. Elwailly, C. Gentry, and Z. Ramzan, "QuasiModo: Efficient certificate validation and revocation," Proceedings of PKC'04, LNCS, vol. 2947, pp. 375–388, 2004.

[8] V. Goyal, "Certificate revocation using fine-grained certificate space partitioning," Proceedings of Financial Cryptography, LNCS, vol. 4886, pp. 247–259, 2007.

[9] D. Boneh, X. Ding, G. Tsudik, and C.-M. Wong, "A method for fast revocation of public key certificates and security capabilities," Proceedings of the 10th USENIX Security Symposium, pp. 297–310, 2001.

[10] X. Ding and G. Tsudik, "Simple identity-based cryptography with mediated RSA," Proceedings of CT-RSA'03, LNCS, vol. 2612, pp. 193–210, 2003.

[11] B. Libert and J. J. Quisquater, "Efficient revocation and threshold pairing-based cryptosystems," Proceedings of PODC 2003, pp. 163–171, 2003.

[12] J. Baek and Y. Zheng, "Identity-based threshold decryption," Proceedings of PKC'04, LNCS, vol. 2947, pp. 262–276, 2004.

[13] H.-S. Ju, D.-Y. Kim, D.-H. Lee, H. Park, and K. Chun, "Modified ID-based threshold decryption and its application to mediated ID-based encryption," Proceedings of APWeb 2006, LNCS, vol. 3841, pp. 720–725, 2006.

[14] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," Proceedings of CCS'08, pp. 417–426, 2008.

[15] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Proceedings of Eurocrypt'05, LNCS, vol. 3494, pp. 557–557, 2005.

[16] B. Libert and D. Vergnaud, "Adaptive-ID secure revocable identity-based

encryption," Proceedings of CT-RSA'09, LNCS, vol. 5473, pp. 1–15, 2009.
[17] J.-H. Seo and K. Emura, "Revocable identity-based encryption revisited: security model and construction," Proceedings of PKC'13, LNCS, vol. 7778, pp. 216–234, 2013.
[18] S. Park, K. Lee, and D.H. Lee, "New constructions of revocable identity-based encryption from multilinear maps," IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1564–1577, 2015.
[19] C. Wang, Y. Li, X. Xia, and K. Zheng, "An efficient and provably secure revocable identity-based encryption scheme," PLOS ONE, vol. 9, no. 9, article e106925, 2014.
[20] A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts," Proceedings of TCC'10, LNCS, vol. 5978, pp. 455–479, 2010.
[21] J.-H. Seo and K. Emura, "Efficient delegation of key generation and revocation functionalities in identity-based encryption," Proceedings of CT-RSA'13, LNCS, vol. 7779, pp. 343–358, 2013.
[22] J.-H. Seo and K. Emura, "Revocable hierarchical identity-based encryption: history-free update, security against insiders, and short ciphertexts," Proceedings of CT-RSA'15, LNCS, vol. 9048, pp. 106–123, 2015.
[23] Y.-M. Tseng and T.-T. Tsai, "Efficient revocable ID-based encryption with a public channel," The Computer Journal, vol. 55, no. 4, pp. 475–486, 2012.
[24] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," IEEE Transactions on Computers, vol. 64, no. 2, pp. 425–437, 2015.
[25] S. Galbraith, K. Paterson, and N. P. Smart, "Pairings for cryptographers," Discrete Applied Mathematics, vol. 156, no. 16, pp. 3113–3121, 2008.
[26] E. Fujisaki and T. Okamoto, "How to enhance the security of public-key encryption at minimum cost," Proceedings of PKC'99, LNCS, vol. 1560, pp. 53–68, 1999.
[27] T. Kitagawa, P. Yang, G. Hanaoka, R. Zhang, K. Matsuura, and H. Imai, "Generic transforms to acquire CCA-security for identity-based encryption: The cases of FOPKC and REACT," Proceedings of ACISP'06, LNCS, vol. 4058, pp. 348–359, 2006.
[28] J. S. Coron, "On the exact security of full domain hash," Proceedings of Crypto'00, LNCS, vol. 1880, pp. 229–235, 2000.
[29] M. Scott, "Computing the Tate pairing," Proceedings of CT-RSA'05, LNCS, vol. 3376, pp. 293–304, 2005.