Cryptographic Foundations and Practical Applications for Cryptography-based Electronic Document Systems

Chenxu Wang

College of Safety Science and Engineering, Civil Aviation University of China, Tianjin, 300300, China
Sunny_cxw@outlook.com

Abstract. With the continuous development of digital technology, the application of electronic documents(e-document) has also penetrated into various industries. Electronic document is the best alternative for paper documents, and various industries can better assist in the storage and transmission of data through the digitization of documents. Cryptography uses mathematical techniques to transform data and prevent unauthorized parties from reading or changing it, enabling secure and efficient communications and transactions. This paper aims to introduce the key technologies and typical applications of electronic documents based on cryptography, such as symmetric cryptography, asymmetric cryptography, hash function, digital signature, and post-quantum cryptography. These technologies provide different levels of protection and functionality for e-document, such as authentication, integrity, confidentiality, non-repudiation, and scalability. Moreover, this paper surveys the current research and developments in this field, identifies the challenges and opportunities, and discusses emerging trends and future prospects. Finally, this paper puts forward feasible solutions and suggestions according to the problems existing in the current electronic document system analyzed.

Keywords: Cryptography, Electronic Document, Identity-based Encryption, Attribute-based Encryption, Blockchain

1 Introduction

The research of electronic documents(e-document) based on cryptography is to provide a foundation for secure and trustworthy communication and data exchange in the era of digital globalization. Cryptography can effectively ensure the confidentiality, integrity, and authenticity of document data, and support various applications such as e-government, e-health, e-learning, and e-business [1,2,3,4].

The development of cryptography-based e-document technologies is driven by the increasing demand for efficient, convenient, and cost-effective solutions for creating, storing, transmitting, and verifying e-document. Compared to paper document, e-document have many advantages, such as easy accessibility, portability, reusability, interoperability, and scalability [5]. However, electronic documents also face many challenges and risks, such as data breaches, identity theft, forgery, fraud,

P. Kar et al. (eds.), *Proceedings of the 2023 International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2023)*, Advances in Computer Science Research 108,
https://doi.org/10.2991/978-94-6463-300-9_78

and cyberattacks. Therefore, it is essential to adopt cryptographic techniques to ensure the security and trustworthiness of electronic documents and their associated processes.

With the study of the application of cryptography in e-documents, this paper will introduce the basic concepts and principles of cryptography and e-document systems, and discuss the main cryptography technologies used in e-document. This paper will also introduce some advanced cryptography technologies that can enhance the functionality and performance of electronic document systems, such as identity-based cryptography, attribute-based encryption, and blockchain. Additionally, this paper will survey the current state of research and development of cryptography-based e-document systems and identify challenges and opportunities for future work.

2 Electronic Document Technologies

2.1 Overview of E-document System

E-document systems are a digital platform that enables the creation, storage, management, and sharing of electronic documents. These systems are designed to ensure secure access, efficient workflow, and ease of collaboration among users. Key components of an e-document system include [6, 7, 8]:

Document creation: Tolol for generating electronic documents in various formats (PDF, Word, Html). Document storage: Secure repositories for storing and organizing electronic documents. Document management: Features for searching indexing, and version control of electronic documents. Access control and authentication: Mechanisms to ensure that only authorized users can access and modify electronic documents. Collaboration tools: Features for real-time collaboration and communication among users.

2.2 Cryptography in E-document

Cryptography plays a vital role in securing electronic documents by providing confidentiality, integrity, and authenticity. The following sections discuss the various cryptographic techniques used in electronic document systems.

Symmetric cryptography, an encryption technique employing a single key for data encryption and decryption, offers speed, efficiency, and suitability for safeguarding vast data quantities. Despite these advantages, challenges arise in key distribution and management, as both sender and receiver require the identical secret key, demanding secure exchange and storage. Should the key be compromised, attackers could effortlessly decrypt the data.

This eliminates the need for the sender and receiver to agree on a shared key beforehand. Asymmetric cryptography also allows digital signatures, which let the sender verify his identity and the message's integrity. Some examples of asymmetric encryption algorithms are Rivest-Shamir-Adleman (RSA), elliptic curve encryption (ECC), and lattice-based encryption.

A cryptographic hash function is a one-way function that produces a fixed-size output, also known as a hash value or sum, from any input. This output serves as a distinctive identifier for the input, verifying its integrity. Some examples of cryptographic hash functions are SM3, SHA, and MD. They are useful for various cryptographic purposes, such as creating digital signatures, message authentication codes, and key derivation functions.

A digital signature is a way of using cryptography to ensure that electronic documents are authentic and unaltered. It works by creating a unique signature with the sender's private key and adding it to the document. The recipient can then check the signature with the sender's public key. Digital signatures are widely used in e-document systems for signing contracts, legal documents, and financial transactions.

The process of creating a digital signature involves two steps: hashing and signing. Hashing is the process of generating a fixed-length string that represents the content of the document using a hashing algorithm. Signing is the process of encrypting the hash value with the sender's private key, producing the signature. The signature is attached to the document and sent to the recipient. The process of verifying a digital signature involves two steps: separating and comparing. Separating is the process of detaching the signature from the document and decrypting it with the sender's public key. This reveals the original hash value of the document. Comparing is the process of generating a new hash value of the document using the same hashing algorithm as the sender and matching it with the original hash value. If they match, it means that the document is authentic and unaltered and that it was signed by the sender.

Quantum computers pose a serious threat to many of the current cryptographic schemes that protect communication and data. These schemes, such as RSA and ECC, belong to the category of asymmetric or public-key cryptography, and they use mathematical problems that are hard for classical computers but easy for quantum computers. For example, quantum computers can factor large numbers or find discrete logarithms much faster than classical computers using Shor's algorithm and Grover's algorithm, respectively [9, 10].

3 Key Technologies in Cryptography-based Electronic Document Systems

Cryptography-based electronic document systems rely on various key technologies to ensure the security and integrity of their documents. In this section, this paper will discuss some of the key technologies that are commonly used in these systems.

3.1 Identity-based Encryption

Identity-based Encryption (IBE) is a type of asymmetric cryptography that uses a user's identity as their public key [11]. Unlike traditional public key cryptography, which requires the use of a certificate authority to issue public keys, IBE allows any trusted third party to issue public keys based on a user's identity. This makes IBE a more flexible and scalable solution for cryptography-based electronic document systems.

One of the key advantages of IBE is that it simplifies the key management process. Because users can use their identity as their public key, they do not need to go through the cumbersome process of obtaining a certificate from a certificate authority. This makes it easier for users to securely exchange documents and information [12]. Another advantage of IBE is that it can be used to implement fine-grained access control for electronic documents. With IBE, access to documents can be controlled based on the identity of the user, rather than a pre-defined set of permissions [13]. This makes it easier to implement complex access control policies that can change dynamically over time.

3.2 Attribute-based Encryptions

Attribute-based Encryptions (ABE) can be used to implement a wide range of access control policies for electronic documents. For example, a document could be encrypted so that only users with a specific job title or security clearance can access it. ABE can also be used to implement dynamic access control policies that can change in response to changes in the user's attributes. One of the key advantages of ABE is that it can reduce the complexity of access control policies. Because access control is based on attributes rather than specific keys or passwords, it can be easier to manage and enforce complex access control policies.

3.3 Blockchain-based Solutions

Blockchain technology is a novel approach for cryptography-based electronic document systems. It consists of a distributed ledger that records and validates transactions in a secure and transparent way. Blockchain technology can offer several benefits for electronic document management, such as tamper-proof and auditable records, transparency and accountability, and security and immutability [13].

One benefit of blockchain technology is that it can create a tamper-proof and auditable record of all document transactions [14, 15]. Since all transactions are stored on a public ledger, the history and authenticity of a document can be easily traced and verified. This can enhance trust in scenarios where it is crucial, such as in financial transactions or legal proceedings [16].

Another benefit of blockchain technology is that it can provide a high level of security. The ledger is distributed across a network of nodes, making it hard for an attacker to compromise the system. Moreover, the ledger is designed to be immutable, making it hard to alter or erase records once they are added to the ledger.

4 Research and Developments in Cryptography-based Electronic Document Systems

This section will review some of the current research and developments in cryptography-based electronic document systems. And will also identify some of the challenges and opportunities that exist in this field, and discuss emerging trends and future prospects.

4.1 Review of Current Research and Developments

Cryptography-based electronic document systems represent a dynamic and rapidly evolving research field. Some of the most notable areas of current investigation include: Post-Quantum Cryptography: Quantum computing threatens the security of conventional cryptographic schemes. To counter this, the field of post-quantum cryptography is dedicated to developing algorithms capable of withstanding quantum attacks. The National Institute of Standards and Technology (NIST) launched the Post-Quantum Cryptography (PQC) project in 2016 and issued the Report on Post-Quantum Cryptography (NISTIR 8105) [10]. Secure Multi-Party Computation: Secure Multi-Party Computation (MPC) is a cryptographic technique that allows multiple parties to jointly compute a function without revealing their individual inputs to one another [17]. MPC has a wide array of applications in domains where privacy and security are paramount, such as secure electronic voting systems and secure auctions. Furthermore, MPC can contribute to machine learning applications by allowing parties to train models on private datasets and evaluate private models using private data, as demonstrated by the CrypTen framework proposed by Brian Knott et al. [18]. MPC also supports privacy-preserving data mining, private information retrieval, and threshold cryptography. MPC is a robust research area aimed at designing efficient and secure protocols for various computing scenarios and adversarial models, and is also closely linked to the burgeoning field of federated machine learning [19]. Privacy-Enhancing Technologies: Privacy-Enhancing Technologies (PETs) are cryptographic methods designed to safeguard user privacy in electronic document systems. PETs encompass techniques such as anonymous credentials, private information retrieval, and privacy-preserving data mining. At present, PETs have found applications in a variety of fields, including e-health [20].

Blockchain-Based Solutions: Researchers are actively exploring the application of blockchain technology to electronic document systems. Investigations are underway into a range of blockchain-based solutions, including smart contracts, decentralized file storage systems, and blockchain-based identity management systems [21, 22]. Blockchain technology has the potential to significantly enhance current electronic document systems in terms of data integrity, tracking, immutability, security, trustability, and accountability.

4.2 Identification of Challenges and Opportunities in the Field

While the field of cryptography-based electronic document systems presents myriad opportunities, it is not without its challenges. Some of the key issues in this area include [8, 23, 24]:

Usability: One major hurdle for cryptography-based electronic document systems lies in their usability. The complexity of cryptographic techniques often renders them hard for the average user to comprehend, posing significant barriers to widespread adoption. Scalability is another critical issue. As these systems gain more traction, they will need to efficiently handle an enormous volume of transactions and users, a task that can be daunting, especially for systems that rely on intricate cryptographic techniques. Interoperability: The ability to work seamlessly with other systems and platforms is crucial as cryptography-based electronic document systems become more prevalent. However, achieving interoperability can be a formidable challenge, particularly when different systems employ diverse cryptographic techniques. Trust: Gaining users' trust is paramount in cryptography-based electronic document systems. Users need to have faith that their documents are secure and their privacy is safeguarded. Building such trust can be particularly challenging for new and untested systems. Despite these challenges, the field also abounds with opportunities. These include [7,11,13,20,23]: Increased Security: Cryptography-based electronic document systems have the potential to significantly enhance the security of electronic documents. With robust cryptographic techniques, these systems can ensure that documents are tamper-proof and access is strictly controlled. Improved Privacy: Cryptography-based electronic document systems also offer opportunities for enhancing privacy. By employing techniques such as attribute-based encryption and privacy-enhancing technologies, it is possible to protect users' privacy while simultaneously enabling secure information sharing. Greater Efficiency: Cryptography-based electronic document systems can significantly increase efficiency in document management and sharing. Blockchain-based solutions, for example, can create a secure and transparent record of all document transactions, which can streamline document management and mitigate the risk of errors and fraud.

4.3 Discussion of Emerging Trends and Future Prospects

Looking to the future, there are several emerging trends in the field of cryptography-based electronic document systems. These include: Blockchain technology can enhance the reliability, efficiency and transparency of electronic document systems that rely on cryptography. As the technology evolves and improves, it is expected that more organizations and individuals will adopt blockchain-based platforms for their document-related needs. Greater focus on usability: One of the main challenges facing cryptography-based electronic document systems is usability. In the future, there is likely to be a greater focus on developing user-friendly interfaces and tools that make it easier for users to understand and use these systems. The growing importance of privacy: With increasing concerns about data privacy, it is likely that I will see a growing emphasis on privacy-enhancing technologies in cryptography-based electronic document systems.

With the emergence of quantum computing, there is a growing need for post-quantum cryptography solutions that can resist quantum attacks. In the future, I can expect to see continued development and refinement of post-quantum cryptography techniques.

5 Conclusion

This paper explores the integral role of cryptographic techniques in promoting secure and dependable communication within the landscape of digital globalization. It addresses the growing need for the application of these techniques to electronic documents (e-documents), crucial to the fields of e-government, e-health, e-learning, and e-business. As the demand for e-document solutions that are efficient, user-friendly, and cost-effective continues to grow, cryptographic technologies have become key players in confronting inherent challenges such as data breaches, forgery, and cyberattacks. For a well-rounded understanding, this paper begins with an introduction to the fundamental concepts of cryptography and e-document systems. It delves into primary cryptographic technologies used in e-documents, such as symmetric and asymmetric cryptography, hash functions, digital signatures, and the emerging field of post-quantum cryptography. Moreover, the paper explores sophisticated cryptographic technologies like identity-based encryption, attribute-based encryption, and blockchain technology, which enhance the functionality and performance of e-document systems.

The study further investigates critical technologies used in cryptographic-based e-document systems. Identity-based Encryption, for instance, streamlines key management by utilizing a user's identity as their public key. Attribute-based Encryption offers a more nuanced approach to data sharing and security, providing access control based on user attributes. The decentralization and tamper-proof nature of blockchain-based solutions are also examined for their potential to bolster the security and credibility of e-document systems. The paper presents a comprehensive review of the current research and advancements in the field of cryptography-based e-document systems, highlighting the challenges, opportunities, and emerging trends. With the ever-increasing volume of digital data and the escalating complexity of security threats, this research underscores the importance of continuous exploration and innovation in cryptographic-based e-document technologies. By doing so, it contributes significantly to strengthening the security and reliability of e-documents and associated processes. This study ultimately emphasizes the realization of the full potential of e-documents - accessibility, portability, and scalability - in the age of digital globalization, thus shaping the future of digital communication and data exchange.

References

1. Karunia, R. L. (2023). Implementation of e-Government for Better Public Service at Lombok Barat. KSS, 8(11), 379-390.
2. Eşiyok, A., Divanoğlu, S. U., & Çelik, R. (2023). Digitalization in Healthcare - Mobile Health (M-Health) Applications. Aksaray Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 15(2), 165-174. https://doi.org/10.52791/aksarayiibd.1241287
3. Md Zin, Z. (2023). Canvas LMS Course Design: Create and Deliver Interactive Online Course on the Canvas Learning Management System: A Book Review. AJEE, 7(1), 20–23.
4. Dašić, D., Ratković, M., Marčetić, A., & Tošić, M. (2023). PROMOTION ON THE INTERNET AS A FUNCTION OF AGRIBUSINESS DEVELOPMENT IN CENTRAL SERBIA. EA, 70(2), 479–491.
5. Suban, A. L., & Reja, I. D. (2022). Developing Beru Subdistrict's Population Data Service Application towards Paperless Office and Good IT Governance. Indonesian Journal of Multidisciplinary Science, 2(2), 1928-1938.
6. Olena, H., & Irina, S. (2018). Analysis of e-document management systems in Ukraine and criteria for their selection. Технологический аудит и резервы производства, 3(2), 18-24.
7. Heryandi, A., Finandhita, A., & Atin, S. (2020). Prototype of e-document application based on digital signatures to support digital document authentication. In IOP Conference Series: Materials Science and Engineering (pp. 012042).
8. Adam, A., Nuke Puji Lestari, S., Wahyu Yustika, P., & Betari Ayu Almadania, L. (2022). Saas platform for blockchain based e-document authentication applications. In 2022 International Conference on Science and Technology (ICOSTECH) (pp. 1-7).
9. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194.
10. Chen, L. et al. (2016). Report on Post-Quantum Cryptography.
11. Boneh, D., & Franklin, M. (2001). Identity-based encryption from the Weil pairing. In Annual international cryptology conference (pp. 213-229).
12. Zhang, L., Han, W., Zhang, R., Wang, L., & Meng, X. (2023). Identity-Based Key Management Scheme for Secure Discussion Group Establishment in DOSNs. IEEE Transactions on Information Forensics and Security, 18, 3706-3719.
13. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 89-98).
14. Hohenberger, S., Lu, G., Waters, B., & Wu, D. J. (2023). Registered attribute-based encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 511-542).
15. Meirobie, I., Irawan, A. P., Sukmana, H. T., Lazirkha, D. P., & Santoso, N. P. L. (2022). Framework Authentication e-document using Blockchain Technology on the Government system. International Journal of Artificial Intelligence Research, 6(2).
16. Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C. Z., Li, H., & Tan, Y. A. (2019). Secure multi-party computation: theory, practice and applications. Information Sciences, 476, 357-372.
17. Knott, B., Venkataraman, S., Hannun, A., Sengupta, S., Ibrahim, M., & van der Maaten, L. (2021). Crypten: Secure multi-party computation meets machine learning. Advances in Neural Information Processing Systems, 34, 4961-4973.
18. Mugunthan, V., Polychroniadou, A., Byrd, D., & Balch, T. H. (2019). Smpai: Secure multi-party computation for federated learning. In Proceedings of the NeurIPS 2019 Workshop on Robust AI in Financial Services (pp. 1-9).

19. Becher, S., Gerl, A., Meier, B., & Bölz, F. (2020). Big picture on privacy enhancing technologies in e-health: a holistic personal privacy workflow. Information, 11(7), 356.
20. Javed, I. T., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N., & Qureshi, K. N. (2021). Health-ID: A blockchain-based decentralized identity management for remote healthcare. In Healthcare (pp. 712).
21. Garg, R. (2022). Decentralized transaction mechanism based on smart contracts. 3rd International Conference on Blockchain and IoT, Sydney Australia.
22. Ziyadullayev, S. (2023). INTEGRATION OF ELECTRONIC DOCUMENT CIRCULATION INTO THE HEALTHCARE SYSTEM. PEDAGOGICAL SCIENCES AND TEACHING METHODS, 2(22), 73-76.
23. Ali, A. M., & Farhan, A. K. (2020). Enhancement of QR code capacity by encrypted lossless compression technology for verification of secure E-Document. IEEE Access, 8, 27448-27458.