The Evolution of Digital Signature Technologies in Mobile Devices

Jinhan Mao
Software Engineering, Wuhan University, Wuhan, China

Keywords: Digital Signature Technologies, Mobile Devices, Cryptography.

Abstract: Due to the popularity of mobile devices and the development of the digital society, digital signatures, as a technical means of security authentication and data integrity protection, have gradually received widespread attention. Therefore, it is very meaningful to review and explore digital signatures. This article will review the research on mobile devices and digital signatures, discuss the implementation principles, application scenarios, and challenges faced by mobile device digital signatures. More specifically, this review first discuss the aspect of digital signature frameworks on mobile devices. In this regard, two aspects are listed: trusted execution environment, certificate revocation mechanism, and secure transport layer security to demonstrate that this comprehensive framework provides a detailed perspective on the complex elements involved in establishing a robust digital signature system on mobile devices. Secondly, a review of past research on asymmetric cryptography was also conducted, in which it can be found that although Rivest–Shamir–Adleman (RSA) algorithm is currently the best algorithm, other studies have also shown that ECC method has better efficiency and security compared to RSA algorithm. In addition, this review also discussed the application of hash functions in digital signatures and concluded that a robust hash function like SHA-256 is crucial for the reliability and security of digital signatures on mobile devices, and can protect transactions and sensitive information in an increasingly mobile centric digital environment.

1 INTRODUCTION

With the proliferation of mobile devices and the development of digital society, digital signature, as a technical means of security authentication and data integrity protection, has gradually received widespread attention. The portability and intelligent characteristics of mobile devices provide more possibilities for the application of digital signatures, making digital signatures a research hotspot in the field of mobile device security. With the popularity of mobile devices and the development of digital society, there is an increasing demand for digital signature technology on mobile devices. Digital signature technology can ensure the authenticity and integrity of data on mobile devices and effectively prevent the risk of information tampering and identity forgery.

Currently, researchers have proposed a series of digital signature schemes on mobile devices through continuous improvement and innovation. Asokan et al. (Asokan et al. 1997) proposed Server-Supported Signature scheme for mobile communication. Their work employed a one-way function traditional digital signature scheme. Signature servers were responsible for generating signature tokens and certification authorities to verify these tokens. Therefore, the scheme's robustness depends on the reliability of those servers. Besides, Yu Lei et al. (Lei et al. 2004) also proposed a server based signature (SBS) scheme for mobile devices based on asymmetric cryptographic algorithms are not suitable for mobile devices These schemes mainly include digital signature based on asymmetric encryption algorithm, digital signature based on hash function and digital signature based on biometric identification.

Digital signature schemes based on asymmetric cryptographic algorithms make use of the pairing of public and private keys to achieve verification of digital signatures through the process of encrypting and decrypting data. This scheme has high security, but due to its high computational complexity, it consumes more resources for mobile devices. The hash function based digital signature scheme is to process the data through the hash function to obtain a unique hash value, and then encrypt the hash value to achieve the verification of the digital signature. This scheme is relatively low computational complexity, but due to the characteristics of the hash function,

Mao, J.
The Evolution of Digital Signature Technologies in Mobile Devices.
DOI: 10.5220/0012818300004547

In *Proceedings of the 1st International Conference on Data Science and Engineering (ICDSE 2024)*, pages 248-252
ISBN: 978-989-758-690-3

there may be a problem of hash collision. The biometric-based digital signature scheme, on the other hand, uses the biometric information on the mobile device, such as fingerprints, facial recognition, etc., to verify the digital signature. This scheme has high convenience and user experience but is limited by the accuracy and security of biometric identification technology. Pawan K. Janbandhu, M. Y. Siyal (Janbandhu & Siyal 2018) proposed a new biometric-based signature system that integrates biometrics with public key infrastructure (PKI) using iris recognition. This biometric signature approach embodys plenty of advantages, including accurate identification of individuals, no storage or transmission of biometric templates, and convenience in signing documents.

This paper will review the research related to mobile devices and digital signatures, and discuss the implementation principle, application scenarios, as well as the problems and challenges of digital signatures in mobile devices. Firstly, introduce the basic concepts and principles of digital signatures, including related technologies such as digital certificates, public key cryptography and hash functions will be introduced. Then, this paper will focus on the application scenarios of digital signatures in mobile devices, such as mobile payment, e-contract and e-ticket, and analyse the advantages and limitations of digital signatures in these scenarios. At the same time, this review will explore the security issues of digital signatures in mobile devices, such as the challenges of private key protection, authentication, and data integrity, and introduce the solutions and techniques in current research.

2 METHOD

2.1 The Framework of Digital Signatures on Mobile Devices

A general procedure of digital signatures is provided in Fig. 1. The framework for implementing digital signatures on mobile devices is multifaceted, involving various indispensable components and processes, in order to ensure a secure and streamlined digital transaction environment. Firstly, it is necessary to establish a powerful PKI to manage the creation and distribution of encryption key pairs, which consist of public and private keys. These keys are mostly used by users and entities participating in the digital signature process and are securely stored on mobile devices. These keys typically utilize hardware-based security features, such as Trusted Execution Environment (TEE), to prevent unauthorized access. The signature generation process includes using a secure password hash function for data hash search and applying the user's private key. At the same time, signature verification also includes retrieving the corresponding public key from a trusted source, hashing the received data, and verifying the digital signature. X. The use of 509 certificates helps to bind public keys to user identities and integrates the advantages of secure communication protocols such as certificate revocation mechanism and Transport Layer Security (TLS), thereby enhancing overall system security. Expanding the security aspect of mobile devices to biometric authentication and implementing user-friendly interfaces to ensure secure user interaction. In addition, the server supports a range of optional features such as timestamp and revocation checking. Adhering to legal standards and continuous improvement strategies, such as algorithm flexibility and instant security patches, ensures adaptability to evolving encryption standards and mitigates potential vulnerabilities in mobile security dynamic environments. This comprehensive framework provides a detailed perspective on the complex elements involved in establishing a powerful digital signature system on mobile devices.

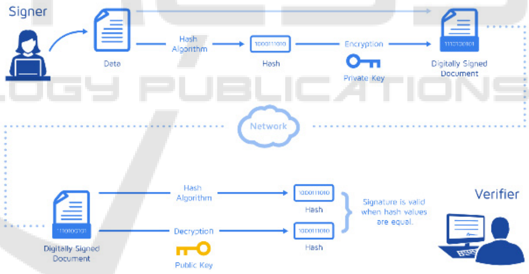

Figure 1: The general procedure of digital signatures (DocuSign, https://www.docusign.com/how-it-works/ electronic-signature/digital-signature/digital-signature-faq).

2.2 Asymmetric Cryptographic Algorithms

Asymmetric cryptography shown in Fig. 2, also known as public key cryptography, plays an unparalleled role in ensuring the security of communication and data storage. It involves two different types of keys - public key and private key. Public keys are widely distributed and can be freely accessed by anyone. The public key is used for encryption, and the sender encrypts the message using the recipient's public key. Once encrypted, only the recipient with the corresponding private key can decrypt and read the encrypted information. And the private key is confidential, only the owner knows. It is used for decryption, and the receiver uses its private key to decrypt the encrypted message received from the sender. So as to obtain the information contained in the encrypted information.

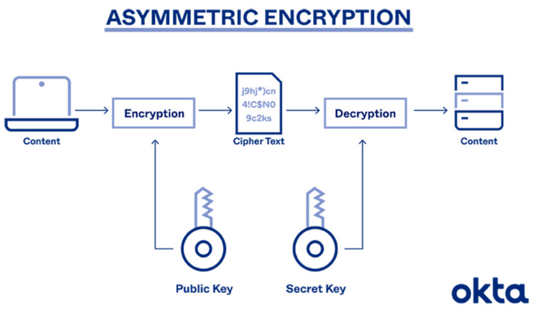

Figure 2: The schematic diagram of asymmetric cryptography (Okta, https://www.okta.com/identity-101/asymmetric-encryption/).

The security of asymmetric cryptography depends on mathematical complexity, such as factoring large numbers or solving discrete logarithms. These problems are computationally difficult, which means there is currently no effective algorithm to solve them at the appropriate time.

The Rivest–Shamir–Adleman (RSA) algorithm is one of the most widely used asymmetric encryption algorithms. It generates public and private keys based on the mathematical properties of large prime numbers. Its security is based on the difficulty of decomposing large numbers. Another popular asymmetric encryption algorithm is the Elgamal algorithm. Unlike the RSA algorithm, it is based on the Diffie Hellman key exchange scheme, built on the difficulty of calculating logarithms over finite fields. Elgamal can be used for encryption and digital signatures. However, some researchers have also proposed that elliptic curve cryptography (ECC) is better than RSA. Yifan Shen et al. (Shen et al. 2021) proposed ECC, a new public key cryptography method based on elliptic curve algebraic structures over finite fields. Compared to RSA, it provides better efficiency and security, and is considered the next generation of public key cryptography.2.3 hash function.

2.3 Hash Function

In the realm of digital signatures on mobile devices, the choice of a suitable hash function is paramount for ensuring the integrity and security of the signed data. Hash functions are cryptographic algorithms that transform variable-length input data into a fixed-length hash value, often represented as a sequence of characters. One commonly employed hash function is Secure Hash Algorithm 256-bit (SHA-256), which is part of the SHA-2 family. SHA-256 produces a 256-bit (32-byte) hash output, providing a robust balance between security and computational efficiency. This hash value is unique to the input data, and even a small change in the input results in a significantly different hash, contributing to collision resistance.

On mobile devices, where computational resources are often constrained, the efficiency of the hash function is crucial. SHA-256 strikes a balance by offering a high level of security while being computationally feasible for mobile platforms. This hash value becomes a crucial component in the digital signature process. During signature generation, the hash function is applied to the data being signed, producing a digest. The private key is then used to encrypt this digest, forming the digital signature. During signature verification, the corresponding public key decrypts the signature, and the hash function is reapplied to the received data, ensuring that it matches the decrypted digest. The use of a robust hash function like SHA-256 is fundamental to the reliability and security of digital signatures on mobile devices, safeguarding transactions and sensitive information in an increasingly mobile-centric digital landscape. Based on the importance of hash functions in digital signatures, Sebastian Rohde et al (Rohde et al. 2008) proposed Fast Hash-Based Signatures on Constrained Devices named Merkle signature scheme, the signature scheme provides comparable timings and maintains a smaller code size compared to state of the art implementations of RSA and ECDSA.

3 DISCUSSION

The progress and application of digital signatures in mobile devices represents a significant milestone in the realm of cybersecurity and electronic authentication. Digital signatures have emerged as a secure and efficient means of verifying the authenticity and integrity of digital documents or transactions. In the context of mobile devices, the adoption of digital signatures has been fueled by the increasing reliance on mobile platforms for communication, financial transactions, and various business processes.

The application of digital signatures in mobile devices simplifies and strengthens processes that traditionally require physical signatures or complex authentication mechanisms. Mobile users can now sign contracts, approve transactions, and verify the authenticity of documents directly from their smartphones or tablets. This convenience not only speeds up workflow, but also helps to reduce paper usage and align with broader environmental sustainability goals.

However, the implementation of digital signatures in mobile devices is not without its limitations and challenges. One notable limitation is the varying legal recognition of digital signatures across jurisdictions. While many countries have enacted legislation to recognize the validity of digital signatures, the lack of global standardization poses challenges for cross-border transactions and collaborations. Harmonizing legal frameworks to ensure the universal acceptance of digital signatures remains an ongoing challenge.

In addition, the security of digital signatures on mobile devices is an important issue. Mobile platforms are susceptible to malicious software and phishing attacks, which may compromise the private keys associated with digital signatures. Developers and security experts must continuously enhance encryption protocols, develop powerful authentication mechanisms, and introduce users to the best solutions to mitigate these risks. In addition, the challenge of implementing secure storage and managing encryption keys on mobile devices requires continuous innovation in both hardware and software. The future prospects of the application of digital signatures in mobile devices are very promising, with the possibility of further development and widespread adoption. A key area for future development is to combine biometric authentication with digital signatures. The use of fingerprint recognition, facial recognition, or other biometric markers enhances the security of digital signatures and reduces reliance on traditional password-based authentication methods. In addition, artificial intelligence methods can be also introduced due to their excellent performance in many tasks (Kayalibay et al. 2017, Qiu et al. 2022, Mohassel & Zhang 2017). At the same time, the development of blockchain technology has also provided opportunities to enhance the integrity of digital signatures. The decentralized and tamper proof features of blockchain can be used to create immutable records of digital signatures, providing additional layers of trust and responsibility. Smart contracts driven by blockchain technology can automatically execute protocols after digital signatures are verified, further simplifying business processes. As the Internet of Things (IoT) continues to proliferate, the application of digital signatures in securing communication between interconnected devices becomes increasingly relevant. Mobile devices, serving as gateways to the IoT ecosystem, can play a pivotal role in ensuring the integrity and authenticity of data exchanged between devices. The expansion of digital signature capabilities to encompass IoT environments may pave the way for more secure and reliable interconnected systems.

4 CONCLUSION

This work mainly discussed the basic concepts and principles of digital signatures on mobile devices, including related technologies such as digital certificates, public key cryptography, and hash functions. Among these methods, this paper mainly discusses asymmetric cryptographic algorithms and hash functions in detail. Meanwhile, after discussion, it can be also found that the Digital signatures have emerged as a secure and efficient means of verifying the authenticity and integrity of digital documents or transactions. Though the application of digital signatures on mobile devices has advantages, the security of digital signatures on mobile devices is still a top priority. In the future, further studies will address this security issue.

REFERENCES

B. Kayalibay, G. Jensen, P. van der Smagt. CNN-based segmentation of medical imaging data, 2017. https://arxiv.org/abs/1701.03056

DocuSign, Understanding digital signatures, https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq

N. Asokan, G. Tsudik, M. Waidner, JCS, **5**, 1, 91-108 (1997)

Okta, Asymmetric Encryption: Definition, Architecture, Usage, https://www.okta.com/identity-101/asymmetric-encryption/

P. K. Janbandhu, M. Y. Siyal, *A new biometric based Signature system.* in Proceedings of 3rd International Conference on Information, Communication and Signal Processing, ICICS (2018)

P. Mohassel, Y. Zhang. *Secureml: A system for scalable privacy-preserving machine learning.* in Proceedings of 2017 IEEE symposium on security and privacy (SP) 22, 19-38 (2017)

S. Rohde, T. Eisenbarth, E. Dahmen, J. Buchmann, C. Paar. *Fast hash-based signatures on constrained devices.* in Proceedings of InSmart Card Research and Advanced Applications: 8th IFIP WG 8.8/11.2 International Conference, CARDIS (2008)

Y. Lei, D. Chen, Z. Jiang. *Generating digital signatures on mobile devices,* in Proceedings of 18th International Conference on Advanced Information Networking and Applications, ICAINA, 2, 532-535 IEEE (2004)

Y. Qiu, J. Wang, Z. Jin, H. Chen, M. Zhang, L. Guo, BSPC (2022)

Y. Shen, Z. Sun, T. Zhou. *Survey on asymmetric cryptography algorithms,* in Proceedings of 2021 International Conf. on Electronic Information Engineering and Computer Science, EIECS (2021)