A Probabilistic Analysis of Legal Risks in Digital Signatures: Balancing Technical, Legal, and Evidentiary Challenges for Enhanced Security and Validity

Bingxin Dong

East China University of Science and Technology, Shanghai, China

bingxind2024@163.com

Abstract. The widespread adoption of digital signatures in various electronic transactions and communications has brought increased attention to their associated legal risks. This study systematically analyzes technical, legal, and evidence admissibility risks to uncover the key legal challenges digital signatures face under different probability scenarios. The findings indicate a significant increase in technical risk within high-probability scenarios, underscoring the need for robust technical safeguards in high-risk transactions. Legal risk remains consistently high across all scenarios, particularly in high-probability ones, highlighting the necessity for a sound legal framework. In addition, evidence admissibility risk peaks in medium to high probability scenarios, indicating the need to bolster the evidentiary effectiveness of digital signatures in these situations. This study's conclusions offer valuable insights into the legal risk management of digital signatures, emphasizing the importance of implementing targeted risk prevention measures tailored to specific scenarios.

Keywords: Digital signature, Legal risk, Technical risk, Evidence admissibility

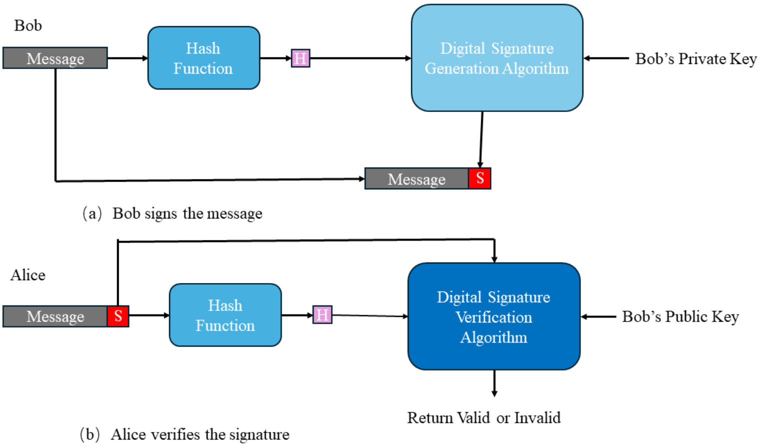
1 Introduction

In the current digital landscape, the necessity for secure and trustworthy methods to validate the authenticity and integrity of electronic communications and transactions has become increasingly crucial [1, 2]. Digital signatures, serving as a fundamental element of modern cryptography, present a solution that ensures both the identity of the sender and the integrity of the message.

This technology has been widely adopted across various sectors, encompassing e-commerce, financial services, legal documents, and government operations, all of which necessitate trust and security. Functionally, a digital signature can be likened to an electronic counterpart of a handwritten signature or a stamped seal, yet it offers a significantly higher level of inherent security. It operates based on the principles of asymmetric cryptography, which employs a pair of keys—one public and one private.

C. Lin et al. (eds.), *Proceedings of the 2024 9th International Conference on Modern Management, Education and Social Sciences (MMET 2024)*, Advances in Social Science, Education and Humanities Research 880,
https://doi.org/10.2991/978-2-38476-309-2_99

The signer utilizes their private key to generate a signature on a digital document. Subsequently, any individual possessing the corresponding public key can verify the signature's authenticity. This procedure not only confirms the document's origin but also ensures its integrity since signing [3, 4]. A visual representation of the digital signature and verification process is depicted in Fig. 1 [5, 6, 7].



(a) Bob signs the message

(b) Alice verifies the signature

Fig. 1. Digital signature generation and verification process

Notwithstanding its substantial benefits, the utilization of digital signatures entails certain legal risks that necessitate careful management. These risks encompass technical vulnerabilities, including the potential compromise of cryptographic algorithms [8, 9, 10], as well as legal uncertainties concerning the recognition and enforcement of digital signatures across different jurisdictions. Moreover, evidentiary challenges can arise when establishing the validity of digital signatures in legal proceedings.

This paper makes a significant technical contribution by conducting a probabilistic risk analysis of digital signatures, particularly focusing on the vulnerabilities of cryptographic algorithms and key management practices. By applying a systematic framework, this study highlights how the severity of these risks fluctuates under different probability scenarios, providing actionable insights into improving encryption methods and key management strategies. Additionally, this paper bridges the gap between the technical aspects of digital signatures and their legal and evidentiary implications, offering a comprehensive approach to managing these intertwined risks.

2 Digital Signature Risks

The widespread adoption of digital signatures has brought forth a range of legal risks that demand meticulous management to guarantee their reliability and enforceability across diverse legal contexts. These risks can be broadly classified into technical risks, legal risks, and evidentiary risks, each presenting distinct challenges under varying probability scenarios. The following section provides a detailed examination of these risks, emphasizing the contributing factors to their severity and the potential consequences for the legal validity of digital signatures.

2.1 Technical Risks

Technical risks pertain to vulnerabilities inherent in the underlying cryptographic algorithms and key management practices that constitute the basis of digital signatures. As the complexity and sophistication of cyberattacks continue to evolve, the robustness of these technical measures becomes increasingly critical.

- **Cryptographic Algorithm Vulnerabilities**: The security of digital signatures is fundamentally reliant on the strength of the employed cryptographic algorithms. With the continuous advancement in computational power, certain algorithms may become susceptible to attacks, thereby jeopardizing the authenticity and integrity of the signatures. This risk becomes particularly acute in high-probability scenarios where the likelihood of targeted attacks is heightened.
- **Key Management Issues**: The proper management of cryptographic keys is imperative to prevent unauthorized access or misuse. Deficiencies in key generation, storage, or distribution can result in the compromise of digital signatures, rendering them vulnerable to forgery or unauthorized alteration. While this technical risk persists across all probability scenarios, its severity escalates with the increasing likelihood of such vulnerabilities being exploited.

2.2 Legal Risks

Legal risks are associated with the recognition and enforceability of digital signatures across different jurisdictions. As the adoption of digital signatures continues to expand, inconsistencies in legal frameworks and standards present significant challenges to their validity.

- **Jurisdictional Variations**: Different countries have diverse regulations governing the use and recognition of digital signatures. The absence of a unified global legal framework can lead to situations where a signature deemed valid in one jurisdiction may not be acknowledged in another. This risk is particularly pronounced in high-probability scenarios where cross-border transactions are prevalent.
- **Legal Framework Gaps** While many countries have enacted legal provisions for digital signatures, there remain gaps in areas such as the recognition of certain types of digital signatures or the requirement for additional verification measures. These gaps can undermine the legal standing of digital signatures, especially in legal proceedings where stringent evidentiary standards are enforced.

2.3 Evidentiary Risks

Evidentiary risks encompass the challenges in establishing the validity and authenticity of digital signatures within a legal context. These risks are pivotal in determining whether a digital signature can serve as reliable evidence in court.

- **Authenticity Verification**: Ensuring that a digital signature is genuinely connected to the signer is fundamental to its evidentiary value. However, the process of verifying authenticity can be intricate, particularly in cases where the technology used to create the signature is called into question. This risk is amplified in medium to high probability scenarios where the authenticity of the signature may be contested.
- **Integrity and Non-Repudiation**: A digital signature must guarantee that the signed document has not been tampered with after signing and that the signer cannot deny having signed it. Failures in maintaining document integrity or ensuring non-repudiation can significantly diminish the evidentiary strength of a digital signature, making it susceptible to legal challenges.

2.4 Risk Assessment

Fig. 2 presents a comparative analysis of the technical, legal, and evidentiary risks associated with digital signatures across varying probability scenarios. The risk severity scores in Fig. 2 are derived from a qualitative risk assessment approach, which synthesizes insights from global research and theoretical frameworks on digital signature systems. This method allows for a comprehensive evaluation of risk levels based on well-established findings in the field.

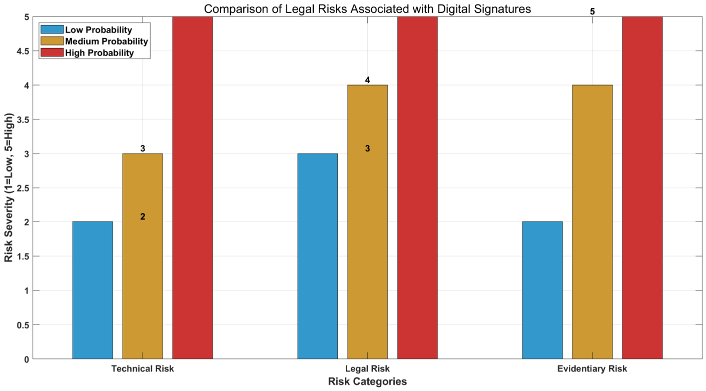


Fig. 2. Comparative analysis of technical, legal, and evidentiary risks associated with digital signatures under different probability scenarios.

Technical Risk Assessment. Research across the globe highlights the increasing vulnerabilities in cryptographic systems, particularly as computational capabilities advance. Studies on widely used cryptographic algorithms such as RSA and elliptic curve cryptography emphasize the growing risk these systems face from emerging technologies and sophisticated attack strategies. The global consensus points to a significant escalation of technical risks in high-probability scenarios, where targeted cyberattacks become more prevalent and effective.

Key concerns include:

- The continuous evolution of attack methods, which are becoming more sophisticated and capable of exploiting weaknesses in even advanced cryptographic systems.
- The ongoing challenges in managing cryptographic keys securely, as improper key management remains a leading cause of digital signature compromises.

As such, the technical risks are assigned higher severity scores in high-probability scenarios, reflecting the widespread recognition of these issues in the field.

Legal Risk Assessment. On a global scale, legal risks stem primarily from the lack of a unified international framework for digital signatures. Different countries and regions maintain varying standards and regulations, leading to legal uncertainty when digital signatures are used in cross-border transactions. Research in legal studies consistently highlights the challenges posed by jurisdictional discrepancies, which create significant obstacles to the recognition and enforceability of digital signatures.

These legal risks are particularly prominent in high-probability scenarios, where the use of digital signatures in international contexts is more frequent, increasing the likelihood of legal disputes. The global legal landscape underscores the need for harmonization, as legal risks remain consistently high across all probability scenarios due to the fragmented regulatory environment.

Evidentiary Risk Assessment. Globally, the evidentiary risks associated with digital signatures revolve around the challenges in verifying their authenticity and integrity in legal settings. Courts and legal systems across the world face difficulties in accepting digital signatures as valid and reliable evidence, especially when the underlying technology is contested or when the process of signature creation is questioned.

The consensus in legal and forensic research indicates that evidentiary risks are most severe in medium to high-probability scenarios. This is due to the increased scrutiny that digital signatures face in legal disputes, where proving non-repudiation and maintaining document integrity are critical. The evidentiary risks are exacerbated by the complexity of verifying digital signatures, particularly when technology or standards vary between jurisdictions.

3 Risk Mitigation and Legal Safeguards

In the rapidly evolving landscape of digital signatures, implementing effective risk mitigation strategies and establishing robust legal safeguards is paramount to ensure the security, reliability, and legal enforceability of these signatures. This section delves into the various approaches to mitigating the risks associated with digital signatures, focusing on technical, legal, and evidentiary facets. The effectiveness of each approach in addressing specific risks will be analyzed, as illustrated in Fig. 3.

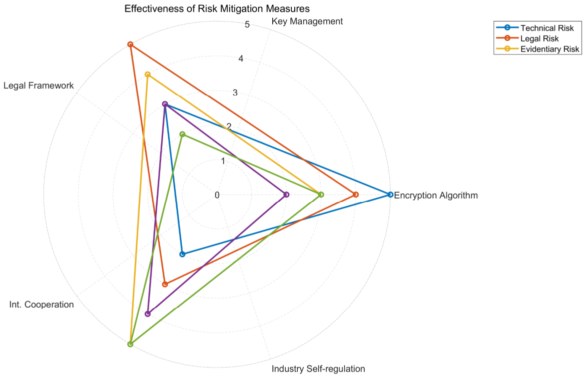


Fig. 3. Comparative analysis of risk mitigation strategies for digital signatures under different probability scenarios

3.1 Risks Technical Risk Mitigation

Technical risks, particularly those stemming from cryptographic vulnerabilities and key management issues, can be substantially mitigated through the implementation of advanced cryptographic algorithms and the enforcement of stringent key management practices.

- **Encryption Algorithm Improvement**: The ongoing evolution of cryptographic techniques is indispensable to address the increasing sophistication of cyberattacks. The utilization of stronger encryption algorithms capable of withstanding current and emerging threats can enhance the security of digital signatures, particularly in high-risk environments. This measure is vital for diminishing the probability of successful attacks on digital signature systems.
- **Key Management Enhancement**: Robust key management practices are indispensable to preserving the integrity and confidentiality of cryptographic keys. These practices encompass secure procedures for key generation, storage, distribution, and disposal. Enhancing key management mitigates the risk of key compromise, a critical concern in both high and medium-risk scenarios.

3.2 Legal Safeguards

Legal risks concerning the recognition and enforceability of digital signatures can be addressed through the development and harmonization of legal frameworks that furnish clear guidelines and standards for their utilization.

- **Legal Framework Improvement**: Strengthening and harmonizing legal frameworks across jurisdictions is essential to ensure that digital signatures are universally recognized and enforceable. This involves updating existing laws to accommodate technological advancements and establishing unambiguous standards for digital signature usage. Improvements in legal frameworks are particularly effective in mitigating legal risks, as they provide the necessary legal certainty and consistency.
- **International Cooperation**: Cross-border transactions often involve multiple legal systems, thus making international cooperation crucial for the recognition and enforcement of digital signatures. Collaborative endeavors between countries, such as the establishment of international treaties and agreements, can help align legal standards and reduce jurisdictional discrepancies. This, in turn, mitigates legal risks in the context of global transactions.

3.3 Evidentiary Risk Mitigation

Evidentiary risks, which relate to the ability to demonstrate the validity and authenticity of digital signatures in legal proceedings, can be mitigated through industry self-regulation and adherence to best practices.

- **Industry Self-regulation**: The establishment of industry standards and best practices can significantly bolster the reliability of digital signatures as evidence in legal disputes. By adhering to these standards, organizations can showcase their due diligence and ensure that their digital signature processes are robust and legally defensible. This approach is particularly effective in reducing evidentiary risks by providing clear guidelines for the creation and management of digital signatures.
- **Traceability and Auditability**: Ensuring that digital signatures are traceable and auditable is essential for their acceptance as evidence in court. Implementing processes that furnish a clear audit trail for each digital signature, encompassing details about the signing process and the signer’s identity, enhances the credibility and reliability of the evidence.

4 Conclusion

The legal validity of digital signatures is a critical concern that encompasses various technical, legal, and evidentiary challenges. This study has presented a comprehensive analysis of these challenges, revealing that digital signatures, while offering substantial benefits in securing electronic transactions and communications, are not devoid of risks. These risks are multi-faceted and vary depending on the probability of their occurrence, necessitating targeted mitigation strategies and robust legal safeguards.

Technical risks primarily involve vulnerabilities associated with cryptographic algorithms and key management practices. As this study underscores, these risks become particularly pronounced in high-probability scenarios where the likelihood of targeted cyberattacks is elevated. Consequently, the continuous improvement of encryption algorithms and the enhancement of key management practices are essential measures to fortify the technical foundations of digital signatures.

Legal risks are equally significant, particularly considering the diverse legal frameworks across jurisdictions. The study emphasizes that a consistent and harmonized legal framework is crucial for the universal recognition and enforceability of digital signatures. This is especially pertinent in high-probability scenarios, such as cross-border transactions, where legal discrepancies can undermine the validity of digital signatures. The study identifies improvements in legal frameworks and international cooperation as key strategies to mitigate these risks.

Evidentiary risks pertain to the challenges of establishing the validity and authenticity of digital signatures in legal proceedings. These risks are most acute in medium to high-probability scenarios, where the evidentiary strength of digital signatures may be contested. The study underscores the importance of industry self-regulation and the adoption of best practices to enhance the traceability and auditability of digital signatures, thereby strengthening their admissibility as evidence in court.

In conclusion, the findings of this study furnish a clear roadmap for managing the legal risks associated with digital signatures. The study emphasizes the necessity of adopting a multi-faceted approach that encompasses technical improvements, legal harmonization, and evidentiary safeguards. By proactively addressing these risks, stakeholders can ensure that digital signatures continue to serve as a reliable and legally valid tool in the digital economy. As digital signatures become increasingly integral to various aspects of modern life, it is imperative that these strategies be implemented and continuously refined to keep pace with the evolving technological and legal landscapes.

References

1. Joshi, K., et al.: Exploring the Connectivity Between Education 4.0 and Classroom 4.0: Technologies, Student Perspectives, and Engagement in the Digital Era. IEEE Access 12, 24179–24204 (2024).
2. Bhardwaj, S., Dave, M.: Secure Electronic Transaction Based Framework for Evidence Transportation in Network Forensics. In: IEEE 7th Conference on Information and Communication Technology (CICT), pp. 1–6. Jabalpur, India (2023).
3. Abbes, M., Julien, A., Hao, S., Touzani, M.: Adopting Digital Signatures for Complex Financial Products in the French Banking Sector: How Technology Acceptance and User Literacy Matter. IEEE Trans. Eng. Manag. 71, 5536–5546 (2024).
4. Mosanaei-Boorani, H., Bayat-Sarmadi, S.: A Digital Signature Architecture Suitable for V2V Applications. IEEE Trans. Circuits Syst. I: Reg. Pap. 71(2), 731–739 (2024).
5. Li, S., Feng, Y., Dang, F., Li, D., Wang, R.: Algorithm Improvement for Elliptic Curve Digital Signature. In: 3rd International Conference on Computer Science and Blockchain (CCSB), pp. 64–68. Shenzhen, China (2023).
6. Akar AlKfari, B. H., Ajeena, R. K. K.: On Applying the BRH Curve in Digital Signature Scheme. In: Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), pp. 1–3. Trichirappalli, India (2023).

7. Rakhra, M., Singh, A., Singh, D., Shruti: Digital Signature Verification In Cloud Computing. In: 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 1–6. Noida, India (2024).
8. Shichun, Y., et al.: Essential Technics of Cybersecurity for Intelligent Connected Vehicles: Comprehensive Review and Perspective. IEEE Internet Things J. 10(24), 21787–21810 (2023).
9. Baldi, M., Deneuville, J.-C., Persichetti, E., Santini, P.: Cryptanalysis of a Code-Based Signature Scheme Based on the Schnorr-Lyubashevsky Framework. IEEE Commun. Lett. 25(9), 2829–2833 (2021).
10. Zhan, Y., Wang, B., Lu, R.: Cryptanalysis and Improvement of a Pairing-Free Certificateless Aggregate Signature in Healthcare Wireless Medical Sensor Networks. IEEE Internet Things J. 8(7), 5973–5984 (2021).