Computer Science and Application 计算机科学与应用, 2025, 15(4), 247-251
Published Online April 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.154096

Hans汉斯

时间门限代理签名方案

孙芳芳，岳笑含

沈阳工业大学信息科学与工程学院，辽宁 沈阳

收稿日期：2025年3月15日；录用日期：2025年4月14日；发布日期：2025年4月22日

摘　要

随着当前加密货币行业的发展，安全数字签名的必要性也成比例地增长。数字签名能够有效提高工作效率，降低交易成本，提升信息安全，因此在全球范围内得到了广泛的应用。数字签名是一种基于公钥密码学的技术，用于确认数字信息的完整性、身份认证和防伪造性。传统数字签名技术在应对多方协作、时间敏感任务等复杂场景时存在显著局限性，难以满足现代分布式系统对安全性、效率与灵活性的高要求。为此，研究者结合定时密码学与分布式签名技术，提出了基于时间锁谜题的门限代理签名方案。

关键词

时间锁谜题，门限签名，代理签名

Time-Bound Threshold Proxy Signature Scheme

Fangfang Sun, Xiaohan Yue

School of Information Science and Engineering, Shenyang University of Technology, Shenyang Liaoning

Received: Mar. 15th, 2025; accepted: Apr. 14th, 2025; published: Apr. 22nd, 2025

Abstract

With the current development of the cryptocurrency industry, the necessity of secure digital signatures has grown proportionally. Digital signatures can effectively enhance work efficiency, reduce transaction costs, and improve information security, thus being widely applied globally. Digital signatures are a technology based on public key cryptography, used to confirm the integrity of digital information, authenticate identities, and prevent forgery. Traditional digital signature technologies have significant limitations when dealing with complex scenarios such as multi-party collaboration and time-sensitive tasks, and are difficult to meet the high requirements of modern distributed

文章引用: 孙芳芳, 岳笑含. 时间门限代理签名方案[J]. 计算机科学与应用, 2025, 15(4): 247-251.
DOI: 10.12677/csa.2025.154096

systems for security, efficiency, and flexibility. Therefore, researchers have combined timed cryptography and distributed signature technology to propose a threshold proxy signature scheme based on time-lock puzzles.

Keywords

Time-Lock Puzzles, Threshold Signatures, Proxy Signature

1. 引言

数字签名[1]是一种基于公钥密码学的技术，用于确认数字信息的完整性、身份认证和防伪造性。它通过使用私钥对数据进行加密生成签名值，然后使用与私钥对应的公钥进行验证，确保接收者能够接收到完整、未被篡改的数据，并确认发送者的身份。数字签名[2] [3]广泛应用于电子商务、区块链、电子政务等领域。然而，传统的数字签名技术在某些复杂场景中(如多方协作、时间敏感任务[4] [5])存在局限性。这意味着，在数字交易中，各方的身份验证存在一些巨大的问题。

自 2015 年《电子签名法》颁布实施以来，我国电子签名行业得到了国家政策的大力支持。政府出台了一系列政策措施，旨在推动电子签名技术在各行业的广泛应用，中国《电子签名法》(2024 年修订)明确电子签名(含时间戳)的法律效力，国务院《关于在线政务服务的若干规定》进一步强化电子印章和签名的互通互认。

隐私保护型众筹项目的资金释放。众筹已成为创新项目、公益事业的重要融资方式，2022 年全球众筹市场规模超 300 亿美元。项目方募资由 10 名随机贡献者组成的监督组共同托管，资金按项目里程碑分阶段释放，每阶段需至少 $t=7$ 名监督者在里程碑达成时间 T_1 后签名授权。监督组无需平台介入，通过门限代理签名[6]自主控制资金。将 T_1 与里程碑时间挂钩，避免人为操作解谜时机。

由上述场景[7]可知，存在权力集中，签名时间限制不明确仅通过自身约束来实现，因此需要将签名时间固定在一个范围内，并将签名密钥或者部分签名定时发放。在定时发放之前，我们需要一个证明，用来证明签名密钥或者部分签名的正确性。

2. 技术背景

2.1. 离散对数

离散对数问题[8]，也称为离散对数难题，是计算机科学和数学领域中的一个著名问题。它涉及到对于给定的两个整数 x 和 y，以及一个素数 p，找到一个整数 n，使得 $x^n = y\left(mod\ p\right)$ 成立。这是一个非常困难的问题，因为在当前的数学和计算能力下，没有已知的有效算法可以在多项式时间内解决它。

离散对数难题是密码学中的一个核心数学问题，主要应用于公钥密码系统。其定义如下：给定一个有限循环群 G，生成元素 g 和群中的一个元素 h，离散对数难题要求找到一个整数 x，使得 $g^x = h$。这个问题之所以困难，是因为在适当的群中，计算 g^x 是高效的，但从 h 反推 x 却极其困难。

离散对数难题的难度依赖于所选择的群。常见的群包括模素数 pp 的乘法群和椭圆曲线群。椭圆曲线群因其更高的安全性而广泛应用于现代密码学中，如椭圆曲线数字签名算法和密钥交换协议。

2.2. 时间锁谜题

时间锁谜题(Time-Lock Puzzles，简称 TLP)的概念最早由 Rivest、Shamir 和 Wagner 等人于 1996 年提出来，该概念源自 May 的定时释放密码学[9]。时间锁谜题是一种向“未来”发送消息的机制，他们的协议允许发送者生成一个谜题，该谜题的答案在特定时间过去之前保持隐藏。时间锁谜题实现时间延迟和秘密的安全存储是依赖于顺序平方假设，具体来说，TLP 允许一个参与方在未来的某个时间点才能获得秘密信息，而其他参与方无法在该时间之前获取该信息。

3. 方案构建

3.1. 方案系统模型

如图 1 所示为可验证定时门限代理签名方案[7] [8]的系统模型，其中包含以下实体：原始签名者，代理签名者，签名接收者，验证者。各实体的具体职责如下：

1) 原始签名者：原始签名者是文件签署的最终负责人，他负责生成代理签名密钥并将其分发给代理签名者。

2) 代理签名者：用代理签名密钥对文件进行签署生成部分签名。

3) 接收者：验证代理签名者生成的部分签名的正确性并聚合部分签名生成最终签名。

4) 验证者：接收最终签名并验证最终签名的正确性。

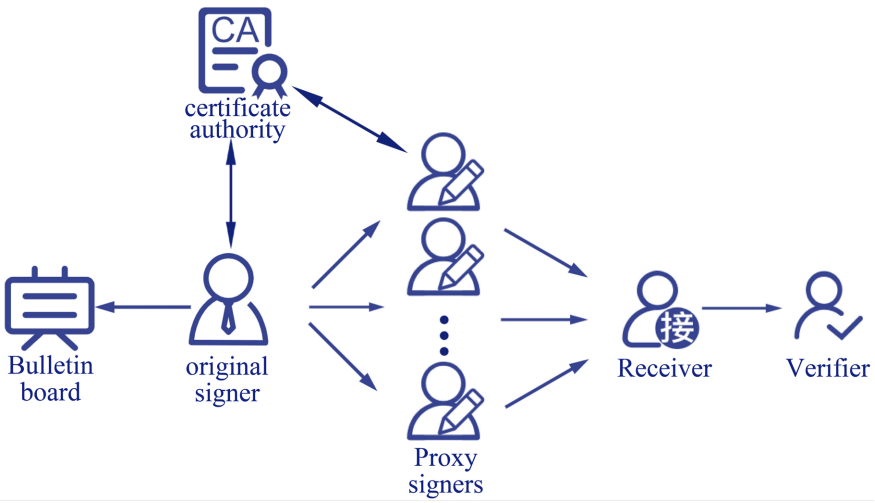

Figure 1. System model diagram
图 1. 系统模型图

3.2. 方案形式化定义

1) 密钥生成阶段

原始签名者和代理签名者分别生成各自的公私钥对$\left(pk_i, sk_i\right)$，并有证书颁发机构对密钥对进行验证。该过程的形式化定义为：$KeyGen\left(1^{\lambda}\right)\to\left(pk_i, sk_i\right)$。

2) 代理密钥生成阶段

原始签名者P_0输入其私钥x_0和权证m_w，输出签名σ作为代理群组的签名私钥。原始签名者P_0通过利用插值法计算出代理签名者P_i的代理签名私钥R_i和公钥Q_i。该过程的形式化定义为：$PKGen\left(sk_0, m_w\right)\to\left(R_i, Q_i\right)$。

3) 定时委托阶段

原始签名者 P_0 执行算法，输入代理签名私钥 R_i，输出承诺 C_i。并利用证明系统证明谜题中的签名密钥的正确性和有效性。该过程的形式化定义为：$TimeDel\left(1^{\lambda}, R_i\right) \rightarrow \left(crs, pk, C_i\right)$。

4) 代理签名生成阶段

每个代理签名者 P_i 输入 $\left(crs, pk, C_i\right)$，执行 VTC 的验证算法验证 C_i 的正确性。当验证正确时，每个代理签名者 P_i 解密获得谜题中的签名密钥，对 m 进行签名 S_i。该过程的形式化定义为：$PrSign\left(crs, pk, C_i\right) \rightarrow \left(R_i, S_i\right)$。

接收者 B 接收每个代理签名者 P_i 的部分签名 S_i，并验证部分签名的正确性，之后将其聚合到成一个签名 S。该过程的形式化定义为：$PrSignAg\left(S_i\right) \rightarrow \left(R, S, K, m_w\right)$。

5) 代理签名验证阶段

验证者接收 $\left(R, S, K\right)$ 时，验证签名 S 是否正确。该过程的形式化定义为：$PrSignVery\left(R, S, K\right) \rightarrow 0/1$。

3.3. 安全及隐私需求

1) 机密性(隐私性)

原始签名者的私钥不能从任何信息派生，例如发送给代理签名者的参数。即使攻击者破坏了所有代理签名者，他也无法获得原始签名者私钥。

2) 代理保护性

部分代理签名不能由代理签名者以外的其他人生成。即使攻击者破坏了原始签名者和 t 个代理签名者，他无法生成他未破坏的代理签名者的有效部分代理签名。

3) 不可伪造性

有效的代理签名只能由 t 个或 t 个以上委托代理签名者协作生成。即使攻击者破坏了原始签名者和 t − 1 个代理签名者，他也无法生成有效的代理签名。

4) 不可否认性

代理组不能拒绝它们创建的代理签名，并且原始签名者不能否认已将签名消息的权力委托给代理组。

5) 时间约束性

代理签名密钥只能在授权的时间内使用。

6) 已知签名者

通过代理签名，可以确定实际签名者的身份。

4. 性能分析和安全性证明

机密性方面，基于离散对数难题确保原始签名者私钥无法泄露，代理组密钥无法逆向推导；代理保护性通过时间锁谜题封装代理密钥，敌手在阈值时间前破解概率可忽略；不可伪造性要求至少 t 个代理签名者协作生成有效签名，可抵抗框架攻击(需解决离散对数难题)、公钥替换攻击(依赖零知识证明约束)、合谋攻击(t − 1 个代理无法重构多项式密钥)及权证攻击(哈希抗碰撞与公告板不可篡改性)；不可否认性由私钥与权证绑定实现，签名者无法否认委托或签名行为；时间约束性通过权证时效与谜题)严格限制签名有效期；已知签名者特性利用 ASID 标识与单向哈希确保实际签名者身份可验证且不可伪造。综上，方案在离散对数、哈希函数与时间锁机制的综合防护下，实现了动态代理场景下的强安全性。

本方案的时间代价核心集中于时间锁谜题(Time-Lock Puzzle, TLP) [10] [11]的生成与解谜操作，其设计目标为确保时序安全性(即操作需经特定时间延迟后生效)，但同时也引入显著计算开销。各阶段性能特征如下：固定开销、主要源于同态时间锁谜题的全局参数生成与证明系统初始化。此类操作涉及大素数

生成、双线性对预计算等密码学基元，虽为一次性开销，但在资源受限环境中需预计算优化。TLP 的生成与解谜依赖不可并行的模幂链计算，计算量随安全参数 τ 指数增长。

5. 结论

本文提出了一种基于时间锁谜题与门限签名的动态代理签名方案，在离散对数难题、抗碰撞哈希函数及多项式秘密共享机制的多层防护下，实现了以下核心贡献。未来工作将聚焦于方案在量子计算威胁下的适应性改进，探索基于后量子密码(如格密码)的代理签名构造，并优化时间锁谜题的计算效率以适配大规模应用场景。

参考文献

[1] Rivest, R.L., Shamir, A. and Wagner, D.A. (1996) Time-Lock Puzzles and Timed-Release Crypto.

[2] Boneh, D. and Naor, M. (2000) Timed Commitments. In: *Lecture Notes in Computer Science*, Springer, 236-254. https://doi.org/10.1007/3-540-44598-6_15

[3] Boneh, D. and Komlo, C. (2022) Threshold Signatures with Private Accountability. In: *Lecture Notes in Computer Science*, Springer, 551-581. https://doi.org/10.1007/978-3-031-15985-5_19

[4] Shoup, V. (2000) Practical Threshold Signatures. *Advances in Cryptology—EUROCRYPT* 2000: *International Conference on the Theory and Application of Cryptographic Techniques Bruges*, Belgium, 14-18 May 2000, 207-220.

[5] Desmedt, Y. and Frankel, Y. (1991) Shared Generation of Authenticators and Signatures. In: *Lecture Notes in Computer Science*, Springer, 457-469. https://doi.org/10.1007/3-540-46766-1_37

[6] Yu, J. and Zhang, J. (2022) Quantum (t, n) Threshold Proxy Blind Signature Scheme Based on Bell States. *International Journal of Theoretical Physics*, **61**, Article No. 207. https://doi.org/10.1007/s10773-022-05112-y

[7] Tang, F., Xu, T., Peng, J. and Gan, N. (2024) TP-PBFT: A Scalable PBFT Based on Threshold Proxy Signature for IoT-Blockchain Applications. *IEEE Internet of Things Journal*, **11**, 15434-15449. https://doi.org/10.1109/jiot.2023.3347232

[8] Hsu, C., Wu, T. and Wu, T. (2001) New Nonrepudiable Threshold Proxy Signature Scheme with Known Signers. *Journal of Systems and Software*, **58**, 119-124. https://doi.org/10.1016/s0164-1212(01)00032-2

[9] Hwang, M.S., Lu, E.J. and Lin, I.-C. (2003) A Practical (t, n) Threshold Proxy Signature Scheme Based on the RSA Cryptosystem. *IEEE Transactions on Knowledge and Data Engineering*, **15**, 1552-1560. https://doi.org/10.1109/tkde.2003.1245292

[10] Damgård, I.B. (1995) Practical and Provably Secure Release of a Secret and Exchange of Signatures. *Journal of Cryptology*, **8**, 201-222. https://doi.org/10.1007/bf00191356

[11] Garay, J.A. and Pomerance, C. (2003) Timed Fair Exchange of Standard Signatures. In: *Lecture Notes in Computer Science*, Springer, 190-207. https://doi.org/10.1007/978-3-540-45126-6_14