Computer Science and Application 计算机科学与应用, 2022, 12(8), 2028-2035
Published Online August 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.128205

Hans汉斯

比特币伪匿名性研究

李心雨

公安部第三研究所，上海

收稿日期：2022年7月20日；录用日期：2022年8月19日；发布日期：2022年8月24日

摘　要

随着互联网的发展，人类不单单局限于现实世界的购物，一种新颖的货币进入人们的视野，即数字货币。2008年，中本聪首次提出了比特币的概念，一种新的货币支付系统——去中心化的系统进入人们的视野，受到了广泛的关注。比特币的交易是通过地址进行的，利用公钥地址来代替用户的身份，从而实现匿名性。由于比特币具有匿名性，去中心化等特点，使得比特币成为世界上流通最广的数字货币。但是，这种采用公钥地址的方式，并不能很好地保护用户的隐私。比特币的匿名性，事实上是一种“伪匿名”，而是一种化名的方式。本文将从现实层面和加密算法方面对比特币的匿名性进行研究。

关键词

比特币，伪匿名性

Research on Pseudo Anonymity of Bitcoin

Xinyu Li

The Third Research Institute of the Ministry of Public Security, Shanghai

Received: Jul. 20th, 2022; accepted: Aug. 19th, 2022; published: Aug. 24th, 2022

Abstract

With the development of the Internet, human beings are not only limited to shopping in the real world, but a new currency has entered people's vision, that is, digital currency. In 2008, Nakamoto first proposed the concept of bitcoin. A new currency payment system, a decentralized system, entered people's vision and received extensive attention. Bitcoin transactions are carried out through addresses, using public key addresses to replace users' identities, so as to achieve anonymity. Due to its anonymity and decentralization, bitcoin has become the most widely circulated digital currency in the world. However, this way of using public key address can not well protect the privacy of users. The anonymity of bitcoin is actually a kind of "pseudo anonymity", but a way of pseudonym. This paper will study the anonymity of bitcoin from the aspects of reality and encryption

文章引用: 李心雨. 比特币伪匿名性研究[J]. 计算机科学与应用, 2022, 12(8): 2028-2035.
DOI: 10.12677/csa.2022.128205

algorithm.

Keywords

Bitcoin, Pseudo Anonymity

1. 研究背景

时代的进步，物品的增多，以物换物已不能满足人类的需求，货币也由此产生，用来衡量物质世界物品的“价值”。原始人类使用的货币是打磨后的兽骨贝壳等，用来表示价值的大小。进入文明社会，人类采用金属冶炼的技术进行铸币，使得金银、铜等作为货币，开始流通。时代不断发展，人类发明了纸币，相比较以往的货币，纸币的发明，减轻了人类外出的负担，促进了商业社会的形成。纸币因为其材质便宜，轻便携带等特点，被人类使用至今。

随着互联网的发展，人类不单单局限于现实世界的购物。一种新颖的货币进入人们的视野，即数字货币。2008 年，中本聪首次提出了比特币的概念[1]，一种新的货币支付系统-去中心化的系统进入人们的视野，受到了广泛的关注。2009 年 1 月 3 日，第一版比特币原型程序正式上线，次日，第一块区块生成，被称为“创世区块(The Genesis Block)”[2] (见图 1)。自此，比特币，区块链(Blockchain)给全世界带来了深远的影响[3]。比特币作为货币使用的第一笔交易在 2010 年 5 月，某一用户使用 10,000 个比特币购买了一块披萨[4]。2020 年 11 月 23 日，1 比特币等于 18,158.7005 美元。比特币的价格从最开始的低于十四美分，到现今已突破一万八美金，被越来越多的人接受和使用，迅速走向社会大众。

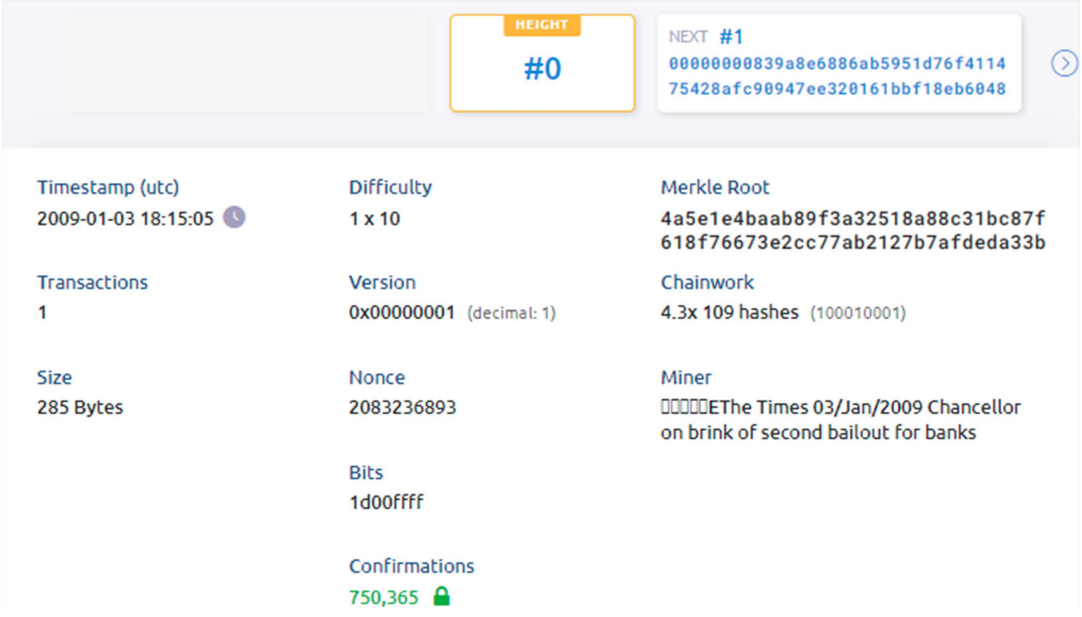

Figure 1. Chuangshi block
图 1. 创世区块

区块链技术是比特币的底层技术，比特币是区块链[5]技术的一个成功的应用，以比特币为代表的数字货币改变了全球范围内的支付方式。与传统货币不同，数字货币没有发行，流通的高昂成本，并且不受汇率的影响，交易时间，手续费都相对减少。同时，由于数字货币的成功，比特币的底层技术区块链，也成为继 20 世纪 70 年代大型机，20 世纪 80 年代个人电脑，近年来的因特网，移动互联网之后的“第五代计算范式”。区块链的研究逐渐延伸至金融、征信管理、资源共享、物联网等多个领域。区块链 1.0 比特币的成功，使得区块链 2.0 [6]，建立智能合约使用算法替代传统合同，以及区块链 3.0，将所有人和机器连接到一个全球性的网络中，超越货币、金融范围的去中心化应用等概念也应运而生[7]。

比特币的出现虽然大大改善了人类的交易方式，但是，比特币系统仍然存在许多问题。例如，比特币的交易效率低下[8]，为了避免发生二次交易的现象，需要花费较长的时间来等待确认区块的生成；比特币的交易平台仍然脆弱，比特币被盗的事件屡见不鲜，私钥容易被盗，保证比特币的密钥安全十分关键[9] [10]；区块链的不断增长，导致资源消耗的增加[7] [11] [12]，如何设计策略，调整策略，使得比特币的分布式计算网络同步的问题等[13]。

2. 概念与原理

比特币系统是一个基于 P2P 网络[14]的、开源的、去中心化[15]的货币交易系统。比特币使用遍布整个网络节点的分布式数据库来管理包括货币的交易发行，账户余额等，在比特币的系统中，任何一个节点都可以参与交易过程，确认其他交易的合法性并且将其他交易加入到分布式账本中。中本聪融合了密码学的基本原理，保证了每一个节点都可以按照协定，达成共识，比特币的交易安全性和用户身份的匿名性可以得到保证[16]。

中本聪在设计比特币时，对比特币的分发进行了详细的设计，将总共 2100 万枚比特币，按照一个递减的速率分发，每发现一个区块，奖励一定数量的比特币。2017 年，发现比特币的奖励已经从最开始的 50 个降低到 12.5 个。每个“矿工”，通过解决计算难题，来获得对公共账本的记账权，解决计算难题的过程就被称为“挖矿”，“挖矿”的过程也是一个竞争的过程。整个比特币支付系统的核心就是被称为“区块链”的公共账本[17]。区块链从本质上来讲，是一个共享数据库，由一系列相互关联的数据块(被称为“区块”)组成，每一个区块都是基于密码学方法产生的，记录了过去的 10 分钟内所有交易的信息[18]。

2008 年，Satoshi Nakamoto 首次发布其关于比特币和区块链的构想[19]，Satoshi Nakamoto 认为，这是一个不受信任的系统，但是在该系统中，发送方可以安全且匿名地将数字信息发送给不受信任且匿名的接收方。目前，比特币已经成为几十年来(从 1982 年开始)最成功，且被广泛应用的数字货币系统[1]。

3. 伪匿名性

比特币的交易是通过地址(见图 2)进行的，利用公钥地址[20]来代替用户的身份，从而实现匿名性[21]。由于比特币具有匿名性，去中心化(见图 3)等特点，使得比特币成为世界上流通最广的数字货币。但是，这种采用公钥地址的方式，并不能很好的保护用户的隐私。比特币的匿名性，事实上是一种“伪匿名”，而是一种化名的方式。匿名指一个人的身份是无法被其他的人所识别，而非实名是指通过假名的方式进行相关交易，用户的信息不完整，不准确。在区块链中，每一个用户都有一个和真实身份无关的虚拟身份，通过这个虚拟身份进行交易，但是这个虚拟身份做的所有事情都是透明的，也就是区块链上的每一笔交易数据都是公开透明的，如果存在一种方式，能够将地址和现实身份信息对应起来，由于区块链的所有交易信息都是公开的数据，那与该身份进行的所有交易信息都可以被查询。区块链实际上就是一个公共总账，所有人都可以进行访问，不同交易之间的关联性对所有人都是可见的。如果一个用户的其中一个公钥地址暴露，那么这个用户所有相关公钥地址均可能出现泄露的情况，甚至与该用户相关的其他

用户地址也存在泄露的风险。

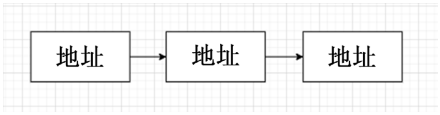

Figure 2. Whereabouts of bitcoins
图 2. 比特币去向

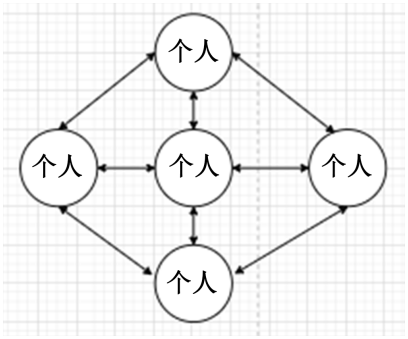

Figure 3. Decentralization
图 3. 去中心化

比特币的匿名性依赖于三个措施进行保护：

1) 任何人都可以利用虚拟的身份创建比特币的地址，进行交易。

2) 通过比特币的地址无法与实体进行关联。

3) 创建比特币地址的数量不受限制，使用者可以没进行一次交易创建一个地址，并且这些地址之间没有任何关系。

相比较银行卡等电子现金的使用，首先就需要使用者通过身份证等能够证明身份的证件进行注册，获取银行卡账号，进行交易。而比特币地址的创建则不需要进行实名认证，很多比特币的网站都提供了一键生成比特币地址的功能。

由于没有通过实名认证进行比特币地址的创建，每一个地址的交易都是独立的，实际上就无法将地址与实体进行关联。也就是可以查看一个地址进行了哪些数额的交易，却无法得知进行交易的实体是谁。

比特币地址创建的数量是不受限制的，使用者甚至可以每进行一次交易，就创建一个新的比特币地址，最大程度的保证了用户本身的信息。同时，这些地址之间没有任何的关联性，即使在某一次交易中，泄露了该地址的用户信息，也可以直接舍弃这个地址，使用其他的地址进行交易，而其他人无法通过已知的地址找到其他的地址。

通过这些措施，看似比特币似乎很好地保证了匿名性，但是仍然存在很多问题，可能导致比特币的匿名性受到破坏。

比特币的底层技术是区块链。区块链是一种特殊的分布式账本。比特币的所有交易都是记录在公共区块链上，任何人都可以看到。通过某一个地址，可以在链上找到与这个地址相关联的一系列地址。利用数据分析工具，就可以将这些地址进行分析，找到某个特定的地址。

同时，现在主要的交易所都是中心化(见图 4)的交易所。中心化的特点是中心掌握分布节点的信息，分布节点之间不掌握其他节点的信息。在中心化的交易所进行交易，就需要账户信息的注册，也就是需要完成最基本的 KYC 认证[22]。KYC 认证(见图 5)是 Know Your Custome 的简称，是一种实名认证机制。当使用者完成 KYC 认证，也就是实名认证后，转账地址和个人身份也就完全对应起来，甚至当从交易所

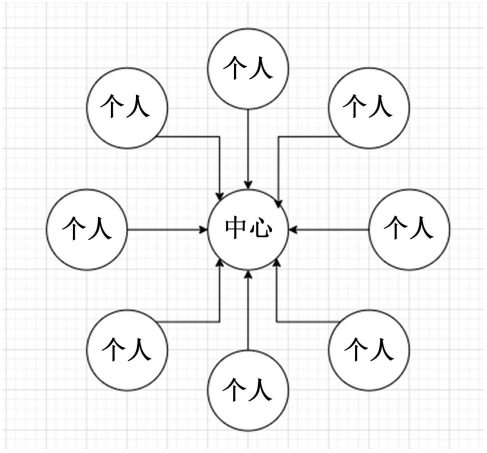

Figure 4. Centralization
图 4. 中心化

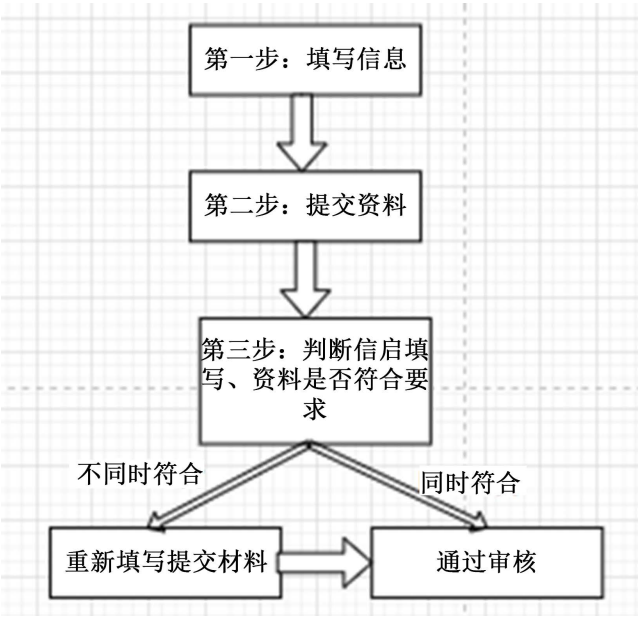

Figure 5. Simple KYC certification
图 5. 简单 KYC 认证

提现的时候，交易所也会知道你的个人钱包地址。用户的信息被存放在一个很大的数据库中，一旦该数据库被破解，所有的信息都会暴露。

比特币支持一个用户创建多个比特币钱包。虽然，我们现在没有办法把哪些地址对应同一个用户，但是，可以利用大数据，人工智能等方式，通过交易比特币的特点，推断出哪些地址是属于同一个用户的。假设一个用户想要购买某一样物品，而他拥有多个比特币钱包，每一个钱包的钱都不足以支付这件商品的价格。当他使用多个钱包对同一个账户发送一些比特币，那么，很大程度上，可以推测这些地址属于同一个用户。也就是同一个交易中的多个输入地址可能属于同一个用户。如图 6，地址 1，地址 2 等多个地址，同时向一个地址发送比特币，则这多个地址可能属于同一个比特币用户。一旦将多个比特币地址匹配到了同一个用户，并且该用户曾今用任何一个地址通过交易所进行过交易的话，那么，该用户的所有信息都可以被查询。

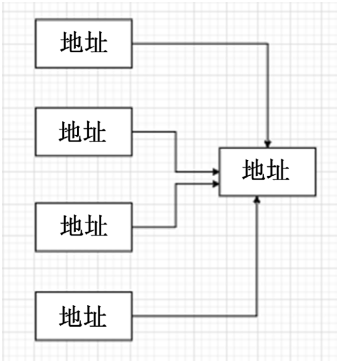

Figure 6. Send bitcoin from different addresses to the same address
图 6. 不同地址向同一个地址发送比特币

比特币的加密算法[23]一共有两类，非对称加密算法(椭圆曲线加密算法)和哈希算法。公钥和私钥由椭圆曲线加密算法生成，私钥可推出公钥而反之不能。哈希函数的概念最早在文献[24]中被提出，可以把任意长度的输入通过 Hash 运算，变成长度固定的输出。它在信息安全方面的使用较为广泛，可以应用在文本校验，消息承诺，数字签名，鉴权协议，消息认证等算法中。经典的密码学哈希函数有 RIPEMD 算法、SHA 算法、MD 算法等[25]。在安全应用中使用的哈希函数被称为密码学哈希函数，一个密码学哈希函数 H()需要满足如下条件[9]：

1) 抗碰撞性(Collision-resistance)。输入不同的值，产生不同的结果，也被称为抗冲突性。

2) 隐匿性(Hiding)。如果知道了哈希函数的输出，不存在一种方式，能够逆向推导出输入的值。

3) 难题友好性(Puzzle friendliness)。如果希望哈希函数的输出是一个特定的值，只要输入的部分足够随机，那么在一定的时间内，都是不可被破解的。

比特币系统采用椭圆曲线[26]数字签名算法(ECDSA)实现数字签名，是 ECC 和 DSA 的结合，椭圆曲线数字签名算法[27]是基于椭圆曲线密码，椭圆曲线上的离散对数(ECDLP)这个困难问题而设计的，该算法的安全性主要是依赖所选椭圆曲线的安全性，比特币系统中选用的是参数记为 secp256k1 的 Koblitz 曲线。

比特币密码学目前是坚不可摧的。但是，量子计算机有超越传统计算机的潜力，并且这种情况随时都可能发生。如果发生这种情况，也就是被称为“量子优势”[28]，这可能最终导致比特比密码学的破坏。如果量子计算机技术得到完善，估计需要 1500 个量子位元才有足够的处理能力破解比特币私钥。不到半年时间，量子计算机从 50 量子比特发展到 72 量子比特，每增加一个量子比特处理能力都会快两倍。也就是说半年不到量子计算机处理能力已经翻了 4 百万倍了。现在的数字货币技术因为大量计算机参与进记账而变得当前技术无法破解。但是当现在的计算机队伍中出现一个量子计算机的时候，整个算力将会都被这个量子计算机控制，量子计算机可以随意更改账本使得整个区块链变得不再可信。

4. 总结

区块链的去中心化和不可篡改属性，使其受到了广泛的关注，同时存在很多问题。基于区块链的比特币也因此存在问题，需要对比特币进行深入研究。其中，最重要的问题就是比特币的匿名性。本文主要论证了比特币的匿名性实际上是一种伪匿名，很多方式都会导致用户信息的泄露，为后续对比特币的去匿名化提供参考。

本文从现实层面，加密算法角度，较为清晰地论证了比特币的匿名性是伪匿名，对于之后，比特币的去匿名化的研究提供基础。由于资料匮乏，本人能力有限，还有很多方式可以论证比特币匿名性不是

完全匿名，在本文论述之后，仍会继续探索比特币的匿名性，同时，思索具体方式实现比特币的去匿名化，使比特币真正做到可监管，防止比特币在经济领域的犯罪行为。

参考文献

[1] Satoshi, N. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] 程洁. 知识产权交易创新系统研究——对“区块链知识产权交易平台”的构想[J]. 技术与市场, 2020, 27(12): 85-86.

[3] 蔡霖翔. 区块链数字货币资金流追溯研究[D]: [硕士学位论文]. 北京: 中国人民公安大学, 2019.

[4] Bonneau, J., Miller, A., Clark, J., *et al*. (2015) SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In: *Security and Privacy*, IEEE, San Jose, 104-121. https://doi.org/10.1109/SP.2015.14

[5] 周福礼, 海盼盼, 陈天赋, 何彦东, 陈山. 区块链技术与跨境电子商务的融合机理与实现路径研究[J/OL]. 世界科技研究与发展, 1-10. https://doi.org/10.16507/j.issn.1006-6055.2022.05.004, 2022-07-18.

[6] 任航, 谢昭宇. 区块链 2.0 时代智能合约的犯罪风险及其应对——以 The DAO 黑客事件为例[J]. 犯罪与改造研究, 2020(3): 2-7.

[7] Swan, M. (2015) Blockchain: Blueprint for a New Economy. O’Reilly Media, Sebastopol.

[8] Andreas, M.A. (2014) Mastering Bitcoin. O’Reilly Media, Sebastopol.

[9] Sarah, M., Marjori, P., Grant, J., *et al*. (2013) A Fistful of Bitcoins: Characterizing Payments among Men with No Names. In: *Proceedings of the* 2013 *Conference on Internet Measurement Conference*, ACM, New York, 127-140.

[10] Fergal, R. and Martin, H. (2012) An Analysis of Anonymity in the Bitcoin System. In: Altshuler, Y., *et al*., Eds., *Security and Privacy in Social Networks*, Springer, Berlin, 197-223. https://doi.org/10.1007/978-1-4614-4139-7_10

[11] Arvind, N., Joseph, B., Edward, F., *et al*. (2016) Bitcoin and Cryptocurrency Technologies. Princeton University Press, Princeton.

[12] Eskandari, S., Barrera, D., Stobert, E., *et al*. (2015) A First Look at the Usability of Bitcoin Key Management. *The* 2015 *Network and Distributed System Security* (*NDSS*) *Symposium*, San Diego, 8-11 February 2015, 1-10. https://doi.org/10.14722/usec.2015.23015

[13] Gervais, A., Capkun, S., Karame, G.O., *et al*. (2014) On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients. *Computer Security Applications Conference*, New Orleans, 8-12 December 2014, 326-335. https://doi.org/10.1145/2664243.2664267

[14] 张杨. 基于 P2P 网络资源传输管理的排队系统研究[D]: [硕士学位论文]. 秦皇岛: 燕山大学, 2021. https://doi.org/10.27440/d.cnki.gysdu.2021.001891

[15] Popescu, G.H. (2014) The Economics of the Bitcoin System. *Psychosociological Issues in Human Resource Management*, **2**, 57-62.

[16] 张弛. 一种数字货币系统 P2P 消息传输机制的设计与实现[D]: [硕士学位论文]. 呼和浩特: 内蒙古大学, 2016.

[17] O’Dwyer, K.J. and Malone, D. (2014) Bitcoin Mining and Its Energy Footprint. 25*th IET Irish Signals & Systems Conference* 2014 *and* 2014 *China-Ireland International Conference on Information and Communities Technologies*, Limerick, 26-27 June 2014, 280-285. https://doi.org/10.1049/cp.2014.0699

[18] 黎江, 何京汉. 区块链的“进击”——区块链、分布式账本技术解读[J]. 金融电子化, 2016(3): 55-58.

[19] Eyal, I., Gencer, A.E., Sirer, E.G., *et al*. (2016) Bitcoin-ng: A Scaleable Blockchain Protocol. 13*th USENIX Symposium on Networked Systems Design and Implementation* (*NSDI*16), Santa Clara, 16-18 March 2016, 46-49.

[20] 余梁. 比特币的安全性到底有多高[J]. 计算机与网络, 2022, 48(2): 45.

[21] 于七龙, 鲁宁, 史闻博. 一种可追溯的比特币混淆方案[J]. 计算机科学, 2021, 48(11): 72-78.

[22] 肖旻. 区块链技术在金融业 KYC 监管中的应用[J]. 上海立信会计金融学院学报, 2017(2): 40-46. https://doi.org/10.13230/j.cnki.jrsh.2017.02.005

[23] 钟晔. 比特币混币服务地址识别研究[D]: [硕士学位论文]. 广州: 广州大学, 2022.

[24] Chaum, D. (1983) Blind Signatures for Untraceable Payments. In: Chaum, D., Rivest, R.L. and Sherman, A.T., Eds., *Advances in Cryptology*, Springer, Berlin, 199-203. https://doi.org/10.1007/978-1-4757-0602-4_18

[25] Diffie, W. and Hellman, M.E. (1976) New Directions in Cryptography. *Transactions on Information Theory*, **22**, 644-654. https://doi.org/10.1109/TIT.1976.1055638

[26] 杨国强. 椭圆曲线及双线性对密码的快速实现算法与关键技术研究[D]: [博士学位论文]. 济南: 山东大学, 2021.

https://doi.org/10.27272/d.cnki.gshdu.2021.000393

[27] Preneel, B. (2010) Cryptographic Hash Functions: Theory and Practice. 12*th International Conference, ICICS* 2010, Barcelona, 15-17 December 2010, 1-3. https://doi.org/10.1007/978-3-642-17650-0_1

[28] 刘雍. 量子优势的基准评估与实现技术研究[D]: [博士学位论文]. 长沙: 国防科技大学, 2020. https://doi.org/10.27052/d.cnki.gzjgu.2020.000057