Wireshark 进行分析，由于现场实践项目有限，本文对密评抓包取证仅分析了部分场景，方法仍需进一步实践和优化。

参考文献：

[1]唐明环，彭浩楠，王伟忠等.工业互联网领域商用密码应用安全性评估研究[J].通信世界，2023（07）：46-49.DOI：10.13571/j.cnki.cww.2023.07.015.

[2]李高磊，李建华，周志洪等.面向新型关键基础设施的密码应用安全性评估技术综述[J].网络与信息安全学报，2023，9（06）：1-19.

[3]黄晶晶，孙淑娴，周睿康等.商用密码应用安全性评估[J].信息安全与通信保密，2023（03）：113-121.

[4]蔡方博，荣志刚，李强.商用密码应用安全性评估方法研究[J].网络安全和信息化，2023（03）：101-103.

[5]张杨，张艳，彭华熹等.基础电信企业开展商用密码应用安全性评估工作的思考与建议[J].信息通信技术与政策，2023（01）：52-57.

[6]宫铭豪，丁森华.应急广播系统商用密码应用安全性评估研究[J].广播电视信息，2022，29（08）：97-100.DOI：10.16045/j.cnki.rti.2022.08.022.

[7]谢宗晓，董坤祥，甄杰.商用密码应用安全性评估及其相关标准[J].中国质量与标准导报，2022（02）：11-14.

[8]黎水林，陈广勇.《信息系统密码应用高风险判定指引》编制思路及要点解析[J].信息网络安全，2021（S1）：113-116.

[9]宋蒲斌，王奔，王昶等.网络安全等级保护下的门户网站设计与实现[J].长江科学院院报，2022，39（01）：155-159.

[10]栾庆武，岳蔚，周永华.基于 Wireshark 的智能变电站 SV 报文分析工具设计及实现[J].电力系统保护与控制，2019，47（24）：169-177.DOI：10.19783/j.cnki.pspc.190041.

[11]霍炜，郭启全，马原.商用密码应用与安全性评估[M].北京：电子工业出版社 ，2020：124.

[12]林沛满.Wireshark 网络分析就这么简单 [M]. 北京：人民邮电出版社 ，2014：17.

大数据背景下的伪随机数发生器研究

◆王景洪

（新乡市政务大数据中心　河南　453000）

摘要：大数据分析和模拟通常需要大量随机数，对于某些应用，如密码学或模拟研究，需要高质量的随机性，因此选择合适的 PRNG 算法变得至关重要。PRNG 的周期长度是指在生成的序列中重复出现的元素之间的距离。在大数据环境中，如果 PRNG 周期太短，可能导致生成的伪随机数序列在长时间内出现明显的重复模式。因此，选择具有足够长周期的 PRNG 算法是重要的。

关键词：大数据；伪随机数发生器；线性同余发生器

1　背景

在计算机科学和工程中，PRNG 被广泛用于模拟、加密、统计学应用、计算机图形学以及其他需要随机数的场景。为了提高伪随机数的质量，一些先进的 PRNG 算法如 Mersenne Twister 等被设计出来，以满足更高要求的随机性和统计性能。在一些应用中，对随机性要求较高的情况下，还可以使用硬件生成的真随机数或采用密码学安全的随机数生成算法。在大数据背景下，伪随机数发生器（PRNG）的重要性显著增加[1-5]。伪随机数发生器是计算机程序中常用的工具，用于生成看似随机但实际上是确定性的数值序列。在大数据环境中，PRNG 的应用广泛，涉及模拟、加密、数据掩码和其他领域。在大数据领域，有一些算法和应用场景可能需要使用伪随机数发生器。蒙特卡洛模拟是一种基于随机抽样的数值计算方法。在大数据环境中，蒙特卡洛方法通常用于估计复杂问题的数值解。这些问题包括金融风险评估、模拟实验、物理模拟等。伪随机数发生器用于生成模拟实验中的随机事件。随机化算法：随机化算法通过引入随机性来改善算法的性能。在大数据处理中，随机化算法被广泛应用于图算法、优化问题、机器学习等领域。伪随机数发生器用于产生算法中的随机选择或随机扰动。在大数据测试和性能评估过程中，可能需要生成大规模的测试数据。伪随机数发生器可以用于生成模拟真实数据的随机样本，以进行测试和验证。在一些大数据分析任务中，数据可能过于庞大，无法全部处理。随机采样是一种常见的方法，用于从大数据集中获取代表性的子样本。伪随机数发生器用于确定哪些数据点应该被选中。加在某些大数据场景中，可能涉及到需要生成安全的随机数，例如用于加密和解密操作。在这种情况下，需要使用密码学安全的伪随机数生成器。大数据中的模拟实验，如市场模拟、网络模拟等，通常需要引入随机性来模拟真实世界中的不确定性和变化。伪随机数发生器用于模拟这些随机事件[5-8]。

在这些应用中，伪随机数发生器的选择和性能对算法的准确性和效率都有很大的影响。因此，合适的伪随机数生成器需要根据具体的需求和算法特性进行选择。伪随机数发生器（Pseudo-Random Number Generator，PRNG）是一种通过算法生成数值序列的计算机程序或算法。这些生成的数列看似随机，但实际上是通过确定性的算法生成的，因此被称为“伪随机”，而不是真正的随机数[9]。

2　随机数发生器

PRNG 的工作原理基本上是从一个初始值（种子）开始，通过一系列的计算步骤生成一个数列。这个数列的生成是确定性的，相同的初始值和相同的算法会产生相同的数列。因此，PRNG 不具备真正的随机性，而是具有可重复性的特征[10-12]。

PRNG 的算法通常采用迭代的方式，通过前一个生成的数来计算下一个数。这样的算法在一定程度上能够模拟真实随机数的统计性质，例如均匀分布、独立性等。然而，由于其确定性特性，当使用相同的种子和算法时，PRNG 生成的数列是可预测的。大数据分析和模拟通常需要大量的随机数。虽然 PRNG 生成的数列是伪随机的，但其质量至关重要。对于某些应用，如密码学或模拟研究，需要高质量的随机性，因此选择合适的 PRNG 算法变得至关重要。PRNG 的周期长度是指在生成的序列中重复出现的元素之间的距离。在大数据环境中，如果 PRNG 的周期太短，可能导致生成的伪随机数序列在长时间内出现明显的重复模式。因此，选择具有足够

长周期的 PRNG 算法是重要的[13]。

2.1 线性同余发生器（Linear Congruential Generator，LCG）

线性同余发生器（Linear Congruential Generator，LCG）是一种简单的伪随机数发生器，其原理基于一个线性同余方程。其生成的伪随机数序列的下一个值依赖于当前值。具有简单、易于实现，计算效率高，但是周期性较短，容易出现线性相关性，不适合高度随机性要求的应用[14]。通过以下公式计算：

$$X_{n+1} = (a \cdot X_n + c) mod\ m \quad (2.1)$$

其中 X_n 是当前的伪随机数，a 是乘数（正整数），c 是增量（正整数或零），m 是模数（正整数），mod 表示取模运算。初始值 X_0 称为种子（或初始种子），它是用户提供的输入，接下来的伪随机数通过不断迭代计算得到。

LCG 的工作原理可以简要描述如下：

1. 选择适当的 a、c、m 和种子 X_0。

2. 计算 $X_1 = (a \cdot X_0 + c) \mod m$。

3. 将 X_1 作为下一次迭代的 X_0，重复上述步骤。

需要注意的是，LCG 的质量和随机性与所选参数 a、c、m 和种子 X_0 的选择密切相关。不同的参数可能导致不同的随机性质量和周期性。为了获得较好的性能，通常需要仔细选择这些参数。LCG 的一个缺点是在某些情况下可能出现周期性较短或线性相关性较强的问题，因此对于一些高要求的随机性应用，可能需要选择其他更复杂的伪随机数生成器。

2.2 Mersenne Twister

Mersenne Twister（MT）是一种流行的伪随机数生成器，其原理基于一个特殊的梅森素数。具有较长的周期（$2^{19937-1}$），在大多数情况下具有良好的统计性能。但其占用内存较多，可能不适用于资源受限的环境。在某些应用中可能存在线性相关性。

梅森素数是具有 2^{p-1} 形式的质数，其中 p 也是一个质数。MT 以这样的梅森素数作为周期，并采用了梅森素数的一些数学性质，以提供长周期和良好的统计性能。Mersenne Twister 的原理如下：

1. 初始化：使用一个 32 比特的种子（或数组）初始化生成器。MT 使用一个 624 元素的状态数组来存储中间值。

2. 状态更新：当需要生成新的随机数时，MT 使用状态数组中的元素进行运算，更新状态。具体而言，MT 使用递推式：

$$Y_k = (Y_{k-1} \oplus (Y_{k-1} >> 30)) \cdot 1812433253 + k \quad (2.2)$$

其中 $\oplus$ 表示按位异或，>> 表示右移操作，乘法和加法操作都是模 2^{32} 的。这一步骤将状态数组的每个元素都更新为一个新的值。

3. 提取随机数：从更新后的状态数组中提取随机数。MT 使用状态数组中的元素，进行一系列的位操作和算术运算，最终生成一个 32 比特的伪随机数。

4. 重复：上述步骤循环执行，每次需要生成新的随机数时，都进行状态更新和随机数提取。

Mersenne Twister 具有较长的周期 $2^{19937}-1$，并且在统计性能上通常表现良好。然而，需要注意的是，由于其状态数组较大，MT 在内存占用上相对较大，可能不适用于资源受限的环境。在一些密码学安全性要求较高的场景下，可能需要选择专门设计的密码学安全的伪随机数生成器。

2.3 SecureRandom（Java）

SecureRandom 是 Java 中用于生成安全随机数的类。它是 java.security 包中的一部分，提供了一种安全的方式来生成伪随机数，适用于密码学和其他安全敏感的场景。其提供高度安全的随机数，适用于安全敏感的应用。但是在某些情况下可能比一些非密码学安全的算法慢，适用性受到一些限制。

以下是 SecureRandom 的一些关键特点：

1. 强密码学安全性：SecureRandom 使用强密码学安全的伪随机数生成算法，通常基于安全哈希函数或其他密码学原理。这确保生成的随机数在密码学上是安全的，不容易被预测。

2. 自维护内部状态：SecureRandom 会自动维护内部的状态，以确保生成的随机数不可预测且具有足够的安全性。

3. 系统提供的实现：SecureRandom 尽可能地利用操作系统提供的安全随机性。

4. 支持多种算法：SecureRandom 提供了多个安全随机数生成算法的实现，包括 SHA1PRNG、NativePRNG、Windows-PRNG 等。可以通过构造函数或系统属性进行选择。

3 总结

大数据处理需要高效的计算，因此 PRNG 的性能也是一个考虑因素。选择一个既能提供高质量随机性又能满足性能需求的 PRNG 算法是至关重要的。大数据处理通常涉及并行计算，因此 PRNG 的并行性能也需要考虑。一些 PRNG 算法具有较好的并行性，可以更好地适应大规模并行计算的需求。如果伪随机数用于加密或其他安全敏感的应用，安全性变得至关重要。在这种情况下，需要选择经过充分验证和认可的密码学安全的 PRNG 算法。生成的伪随机数应当具有良好的分布特性，以确保在不同的应用场景中得到合理的结果。一些 PRNG 算法可能在特定范围内产生偏差，需要谨慎选择。在实际应用场景中，可以根据具体的场景和性能要求选择合适的 PRNG 算法。一些常见的 PRNG 算法包括线性同余发生器、Mersenne Twister 等。对于特定需求，可能需要使用更先进的密码学安全的 PRNG 算法。选择合适的 PRNG 取决于具体的应用场景和随机性要求。对于一般应用，像 Mersenne Twister 或 XORshift 可能足够，而对于需要高安全性的场景，应使用专门设计的密码学安全的 PRNG。在实际应用中，还可以通过混合多个 PRNG 或者使用硬件随机数生成器来提高随机性。

参考文献：

[1]孙福玉，曹万苍.伪随机数发生器[J].赤峰学院学报：自然科学版，2013（24）：2.DOI：10.3969/j.issn.1673-260X.2013.24.014.

[2]杨威，吴国凤.几种伪随机数发生器及其在 WEB 中的应用[J]. 微型电脑应用，2007.DOI：JournalArticle/5aea382bc095d713d8a5252c.

[3]魏公毅，刘擎宇.并行机上的伪随机数发生器[J].计算机系统应用，1994（10）：2.DOI：CNKI：SUN：XTYY.0.1994-10-011.

[4]谢海宝，吕磊.基于伪随机数发生器的双向认证协议[J].计算机技术与发展，2022，32（1）：6.

[5]蒋文明，盛利元，李锋.Rijndael 分组密码的伪随机数发生器[J].计算机工程与应用，2012（06）：100-102+132.DOI：CNKI：11-2127/TP.20110302.1101.013.

[6]万武南，王晓京，刘旸.基于复合离散混沌动力系统的伪随机数发生器[C]//中国科协第五届青年学术年会，2023-12-18.

[7]MIN Le-quan，闵乐泉，HAO Long-ji，等.关于 2d 词伪随机数发生器随机性检测研究[C]//中国密码学会 2016 混沌保密通信专委会第二届学术会议，2016.

[8]刘沛华.基于 FPGA 的高速伪随机数发生器设计[J].半导体人工神经网络实验室，2012.

[9]李培.混沌伪随机数发生器设计与分析及其在比特承诺中的应用[J]. 2012.

[10]Xuelong Z，Qingmei W，Manwu X U，et al.Pseudo

Random Numbers Generator Based on One-Dimensional Extended Cellular Automata 基于一维扩展元胞自动机的伪随机数发生器研究[J].计算机，2005，32（4）：137-139.DOI：10.3969/j.issn.1002-137X.2005.04.043.

[11]朱峰.高速随机数的产生与应用[D].东南大学，2014.DOI：10.7666/d.Y2781819.

[12]刘传明.基于交叉置乱和 DNA 编码的混沌图像加密算法[D].大连理工大学[2023-12-18].DOI：CNKI：CDMD：2.1017.821840.

[13]杨忠昊.多种密码序列的变值测量图示研究[D].云南大学，2018.

[14]郭永宁，孙树亮.基于真随机数和伪随机数相结合的图像加密算法[J].陕西师范大学学报：自然科学版，2020，48（2）：6.

[15]药国莉.基于混沌的随机数生成器[D].西安电子科技大学，2023.DOI：CNKI：CDMD：2.1017.276129.

基于区块链的可审计密码货币方案

◆高乐　张竣哲　余佳鑫　唐胤

（五邑大学（江门）　广东　529020）

摘要：在区块链交易的背景下，保护个人隐私至关重要。现有的解决方案强调实现匿名性以确保用户的身份安全，然而，仅仅实现交易的匿名性无法满足政府陆续颁布的审计政策要求。针对上述问题，提出了一种实现部分匿名性、保密性、可审计性和可追溯性的解决方案。通过结合佩德森承诺变体和随机化签名实现密码货币的部分匿名性以及审计性，从而在符合审计条件的前提下保护用户的隐私；基于 Twisted Elgamal 加密算法以及专门构造的零知识证明，在符合法律法规的前提下实现交易金额的保密性。系统测试结果表明，该方案能够有效地实现上述要求，通过系统测试、对比分析以及安全性分析证实该方案的可行性。

关键词：区块链；隐私保护；可审计；密码货币

基金项目：科技部国家重点研发计划（2022YFC3303200）；广东省教学质量与教改（GDJX2020009）

随着区块链的兴起，密码货币引起全球 IT 行业、金融机构以及学术界的巨大兴趣。尽管它具有许多吸引人的特性，但交易隐私一直是其在实际应用时最具挑战性的问题之一[1]。为了解决这一问题，比特币选择引入假名来保护用户的身份。然而，各种去匿名化攻击的出现已经表明，仅仅依赖假名不足以提供足够的匿名性。此后，研究人员提出了一些强大的匿名方案，这些方案采用环签名、零知识证明和混合机制等技术来掩盖交易各方的身份和交易金额，有助于增强匿名性和保密性，减轻了去匿名化攻击所带来的风险。

但过分强调匿名性也引入新的挑战。由于密码货币不被承认为合法货币，也不受政府监管，执法机构难以确认交易的目的地和交易金额。这种不透明性妨碍了监管机构有效监管和调查密码货币市场的能力，进而损害金融机构的声誉并对经济系统构成重大威胁。在学术界，一些人主张将可审计性纳入区块链系统，中央银行数字货币由此诞生。这种货币的优势在于它由政府发行并受法律保护，有助于促进金融稳定和政府监管，但由于其过于强调审计，使得用户隐私可能遭到泄露，从而降低用户的使用信心。为解决上述问题，本文提出一种平衡隐私与监管的交易方案，主要贡献如下：

（1）给出一种实现用户身份的隐私保护、交易双方的交易金额保密、监管方对违法交易的身份追踪的密码货币方案实现框架。

（2）将佩德森承诺变体技术与重随机化签名算法改进结合，在确保用户隐私安全的同时实现了对违法用户的身份追踪，在符合区块链账户模型的运行模式下保证了交易的匿名性。

（3）基于 Twisted Elgamal 加密算法以及专门构造的零知识证明技术实现了交易金额保密性，确保交易的实际金额不被暴露的同时，通过零知识证明使得每笔交易均在规定范围内，从而符合政府监管需求。

1　相关工作

Saberhagen 提出了 CryptoNote，它使用可追踪的环签名[2]来隐藏交易参与者，使用一次性密钥来防止货币的双重花费。Zerocoin[3]是 Ian Miers 提出的方案，它使用累加器和非交互式零知识证明[4]来确保用户的交易匿名性。Zerocash[5]是由 Sasson 等人开发的方案，通过嵌套承诺、简洁非交互式零知识证明和默克尔树来隐藏交易流动和金额。针对隐私保护技术的发展带来的监管问题，学者们提出了以下解决方案：Solidus[6]采用了类似银行的结构，但没有隐藏交易参与者的身份。Li 等人[7]提出了可追踪门罗币，通过可验证的加密技术平衡了用户的匿名性和问责制。Zkledger[8]是一个分布式分类账系统，为多次审计提供了强大的隐私和审计支持，但受到高存储成本的阻碍。PGC[9]是一种基于账户模型的可审计机密支付方案。它使用 Twisted Elgamal 加密来隐藏交易金额，并通过 Bulletproof[10]实现范围证明。Zether[11]是一种在以太坊上基于账户模型的智能合约方案，实现 K 次匿名性并提供金额的保密性。BlockMaze[12]采用双余额模型和两步转账机制来隐藏用户余额、转账金额和交易身份。最近，Liang 等人[13]提出了一种基于 UTXO 模型的可监管匿名支付方案。它计算转账总金额和转账数量，而不暴露交易之间的关联，允许监管机构在用户违反规定时恢复其身份。然而，这暴露了交易金额。MD. MAINUL Islam 等人[14]通过动态分散标识符在链上实现了可自我管理的身份验证，但仍然暴露了用户的交易金额。Lin 等人[15]基于 UTXO 模型，通过累加器和同态加密实现了匿名性、保密性和可审计性。管理者可以为用户生成可追踪的匿名公钥和交易密文，他们有能力打开交易密文并跟踪用户的长期公钥。然而，这也赋予了管理者相当大的权力。

2　系统方案

2.1 系统采用的技术手段

2.1.1 佩德森承诺变体

佩德森承诺方案是一种由三个多项式时间算法组成的两方协议，变体在原有基础上增加了重随机化功能，其构造如下所示：

（1）初始化算法 $(pp) \leftarrow \mathrm{Setup}(1^{\lambda})$。输入安全参数 λ，输出公共参数 pp。

（2）承诺生成算法 $(cm_1, cm_2) \leftarrow \mathrm{Com}(m; r)$。输入承诺