脉冲星的随机数生成

Hayder Tirmazi

City College of New York.

Contributing authors: hayder.research@gmail.com;

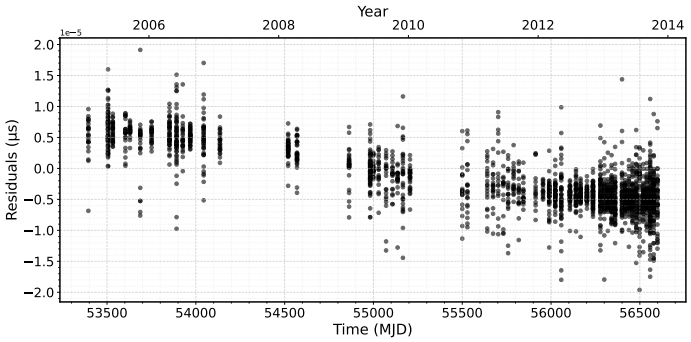
摘要

脉冲星显示出具有精确到达时间的信号，这些时间间隔在毫秒到秒之间，具体取决于具体的脉冲星。脉冲星信号的时间上存在微妙的变化。我们表明这些变化可以用作创建随机数生成器 (RNG) 的自然熵源。我们还探讨了使用随机性提取器来增加从脉冲星定时数据中提取的随机比特熵的效果。为了评估脉冲星 RNG 的质量，我们将它的熵建模为 k-源，并使用已知的密码学结果来展示它与理论上理想的均匀随机源的接近程度。为了保持与先前工作的连贯性，我们还展示了脉冲星 RNG 通过了诸如 NIST 测试套件等众所周知的统计测试。

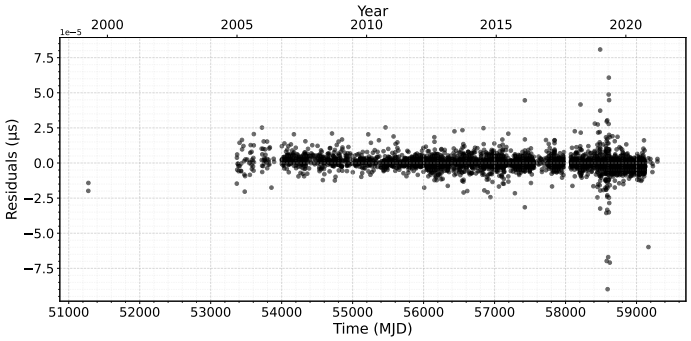
Keywords: 密码学随机性，随机数生成，真随机数生成器，天文学

1 介绍

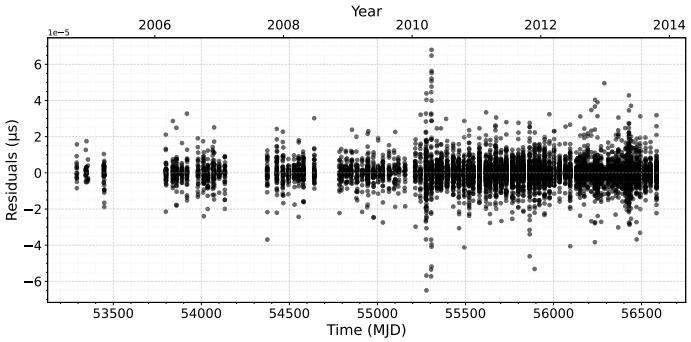
随机数生成器（RNGs）是现代密码学的基本组成部分 [1] 。它们可以用来实现可证明安全的密钥加密方案 [1, 2] 、数字签名方案 [1] 以及公钥加密方案如 RSA 等的关键生成步骤 [3] 和 [4] 。真随机数生成器（TRNGS）使用物理过程中的噪声作为随机性的来源。例如，Intel 的 TRNG 使用电阻中的约翰逊噪声 [5] 。伪随机数生成器（PRNGs）使用种子初始化，并利用算法产生对于不了解种子且仅限于执行概率多项式时间计算的对手而言看似随机的数字 [2]。PRNG 的初始种子可能源自 TRNG。从天体物理来源提取随机性的先前研究，按时间顺序包括：天文成像中的热点像素 [6]、射电天文学信号数据噪声 [7]、宇宙微波背景辐射光谱 [8]、宇宙光子到达时间 [9] 以及单个脉冲星的内在流量密度分布 [10]。



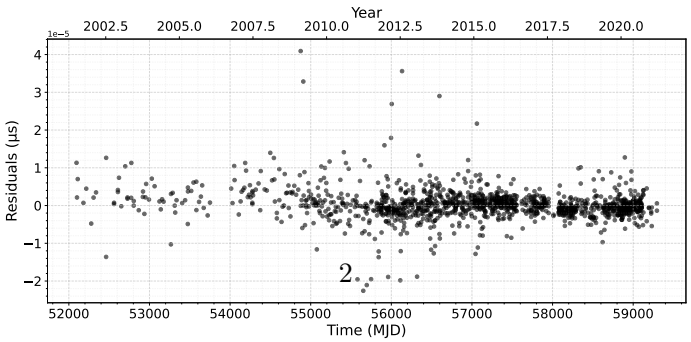
(a) J0030+0451 NANOGrav



(b) J0030+0451 EPTA



(c) J1918-0642 NANOGrav



(d) J1918-0642 EPTA

图 1: J0030+0451 和 J1918-0642 脉冲星的 μs 时间变化，修改后的儒略日（MJD）和年份绘制在 x 轴上

脉冲星定时变化提供了一个结构化但不可预测的替代熵源。据我们所知，本文是首次研究脉冲星信号到达时间间隔的变化作为密码学随机数生成的新熵源。之前来自天体物理源的随机数生成工作，显著包括 [10] 和 [6]，主要依赖于黑盒统计测试来评估随机性质量。仅依赖此类统计测试而不对熵源进行适当理论分析存在众所周知的问题 [11]。事实上，被 NIST 认可的统计测试甚至可以由弱 PRNGs 通过 [11]。与之前的工作不同，我们的工作还包括使用已知密码学技术进行的理论分析来补充我们经验性的发现。

本文的其余部分结构如下。在第 2 节中，我们从两个来源的观测数据创建了一个脉冲星随机数生成器：北美纳赫兹引力波天文台（NANOGrav）[12] 和欧洲脉冲星计时阵列（EPTA）[13]。第 3 节通过密码分析和统计测试来评估脉冲星随机数生成器。第 4 节提供了关于脉冲星随机数生成器可行性的相关讨论。

2 生成随机位

我们使用了两个脉冲星的测量数据，PSR J0030+0451 和 PSR J1918-0642。这两个脉冲星在 NANOGrav 9 年数据集发布 [5] 和 EPTA DR2 数据集发布 [13] 中均有出现。我们的脉冲星随机数生成器使用 PINT [14]v1.1.1 从这些数据集中提取计时残差。令 L 是脉冲星残差的列表，其中 L_i 是第 i 个元素。我们首先按照常规方式（$N_i = \frac{L_i - \min(L)}{\max(L) - \min(L)}$）将残差值标准化以创建列表 N。然后我们研究了三种量化技术将列表 N 转换为随机比特列表 R。

1. 一个简单的阈值：$R_i = 1$ 如果 $N_i \geq 0.5$，否则 $R_i = 0$
2. 8 位格雷编码 [15]
3. 使用 8 位格雷码值作为 SHA-512 哈希的种子 [16]

图 2 显示了这三种量化方法的测量数据集熵，单位为每字节比特。请注意，在本文中我们用熵表示信息熵，也称为香农熵。我们在本文中使用实体工具 [17] 测量所有数据集熵结果。

使用阈值作为量化方法需要谨慎选择在每个分布中放置阈值的位置。我们统一使用 $\tau = 0.5$ 作为阈值的方法，在对 EPTA 数据集中的 PSR J1918-0642 数据与 NANOGrav 数据集进行对比时，产生了截然不同的结果。这是由于 $\tau = 0.5$ 没有为 EPTA 数据提供相等的方向。这一点可以在图 3 中得到验证，该图显示了两个数据集的归一化残差（N）。请注意，虽然 NANOGrav 数据中的点大致被一条阈

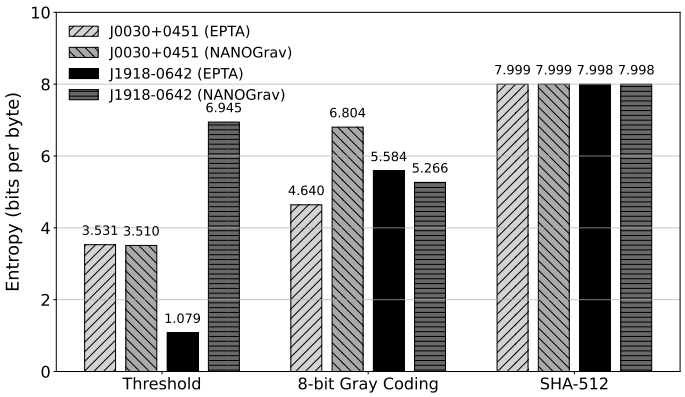


图 2: 不同量化方法对两个脉冲星在 EPTA 和 NANOGrav 数据中的熵

值线在 0.5 处划分为两部分（如图中虚线所示），但在 EPTA 数据集中，大多数点都位于 0.5 之下。

我们接下来研究三种不同的随机性提取器对我们结果的影响。随机性提取器是一种函数，其输入包括 1) 一个相对较小的均匀随机种子和 2) 一个相对较弱的熵源，例如放射性衰变 [18] 或在我们的例子中脉冲星时间变化。随机性提取器输出看起来对计算能力有限的对手而言独立于输入熵源且均匀随机分布的随机位。请注意，之前的基于天体物理学的 RNG 论文包括 [6] 将随机性提取器称为去偏或去歪斜算法。我们测试了两种简单的 *专设的*随机性提取器，即异或几个连续比特 [19] 和 [20]。我们还测试了一个基于 SHA-3 系列加密哈希函数的 SHAKE-256 的随机性提取器。图 4 显示了我们的结果。虽然使用加密哈希能产生最高的熵，但值得注意的是，即使是像冯 · 诺依曼这样的临时随机性提取器也能提供显著的熵增益。

3 评估

一个严格的数学证明表明绝对随机性被认为是不可能的 [19] 。为了分析 TRNGs，我们必须依赖于基于物理学基本假设 [19] 以及我们的数学分析相结合的假设。我们使用标准密码学定义来定义随机性提取器和 k-源（详情见 A）。我们利用这些定义来展示在合理的物理假设下 Pulsar RNG 的适用性。我们假设脉冲星定时变化表现出非平凡熵，并可以被建模为 k 源（假设 1）。从理论角度来看，这一假设与脉冲星定时变化的现有随机模型 [21] 相一致，这些变化是由诸如突变 [22] 等非确定性现象引起的，同时也存在引力波 [23] 。

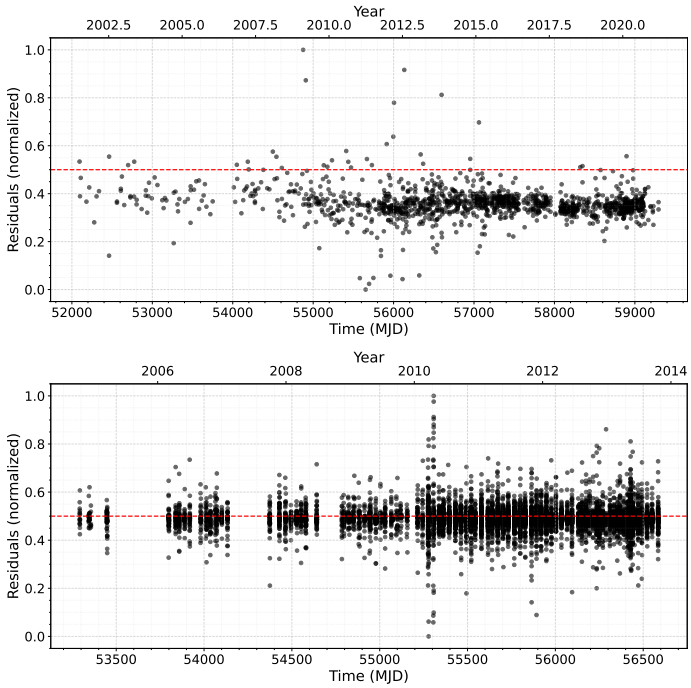


图 3: 标准化的 PSR J1918-0642 残差在 EPTA 数据（上方）和 NANOGrav 数据（下方）。

我们也基于 NANOGrav 和 EPTA 的脉冲星数据实证验证了我们的假设。我们在表 1 中展示了我们的实证结果。我们从 10 个不同的脉冲星生成二进制数组，其中 NANOGrav 数据集中有 5 个，在 EPTA 数据集中有 5 个。然后我们以每比特为单位测量生成的二进制数组的最小熵（定义 3）。通过一个非平凡的最小熵，我们的意思是其值显著大于 0。根据定义，二进制数组上的最小熵将在每比特 $[0, 1]$ 范围内。我们依赖于第 2 节中讨论的 8 位格雷编码方法进行量化。

3.1 加密保证

我们证明了我们的脉冲星随机数生成器满足剩余哈希引理中的强提取器条件。随机性提取器是加密原语，可以将有偏的熵源转换为（在实践中）均匀分布的随机分布。剩余哈希引理由形式上证明了一个通用哈希函数族可以从 k-源中提取近似均匀的比特。对于脉冲星随机数生成器中执行这一去偏操作的哈希函数，我们使用 SHA-3 加密哈希函数家族中的 SHAKE-256。正式的证明见于 A。非形式地讲，这一结果意味着由脉冲星随机数生成器产生的随机比特在统计上接近从某

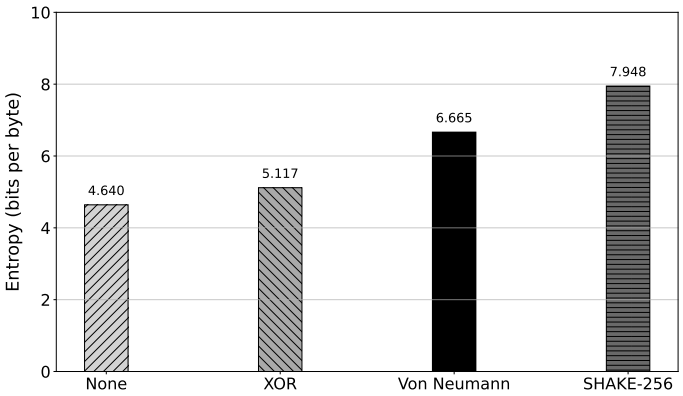


图 4: 来自 PSR J0030+0451（EPTA）数据的不同随机性提取器的熵。

Pulsar	Dataset	Min Entropy (bits per bit)
PSR J0030+0451	EPTA	0.974
PSR J1918-0642	EPTA	0.826
PSR J2124-3358	EPTA	0.801
PSR J1843-1113	EPTA	0.911
PSR J2322+2057	EPTA	0.699
PSR J1832-0836	NANOGrav	0.679
PSR J2302+4442	NANOGrav	0.909
PSR J0030+0451	NANOGrav	0.882
PSR J1918-0642	NANOGrav	0.739
PSR J1012+5307	NANOGrav	0.798

表 1: 实验证据验证了对于 10 颗脉冲星（其中 5 颗来自 NANOGrav，5 颗来自 EPTA）非平凡（显著大于 0）的最小熵。请注意，最大可能的最小熵是 1。

个理想的均匀分布中采样的随机比特。更精确地说，脉冲星随机数生成器输出与一个均匀分布之间的统计距离被限定在一个合适的 ε 内。

3.2 统计检验

之前对来自天体物理源的 RNGs 的分析依赖于黑盒统计测试，如 NIST SP800-22b 测试 [24]，实体 [17]，铁杆支持者和 `dieharder` [25]。在第 3.2 节中，我们展示了使用此类统计测试评估时我们的脉冲星 RNG 表现良好，并提供了关于去偏和混合方法的讨论。然而，我们将这些黑盒统计测试的结果作为密码学随机数生成

NIST test	Proportion	P-value	Pass
Frequency	10/10	0.911413	Y
BlockFrequency	10/10	0.911413	Y
CumulativeSums	10/10	0.534146	Y
Runs	10/10	0.213309	Y
LongestRun	10/10	0.534146	Y
Rank	10/10	0.534146	Y
FFT	10/10	0.534146	Y
ApproximateEntropy	10/10	0.122325	Y
Serial	10/10	0.017912	Y
LinearComplexity	10/10	0.004301	Y

表 2: PSR J0030+0451（EPTA）脉冲星随机数生成器的统计测试结果。

器适用性的唯一证据是不准确的 [11]. 即使是弱（不安全）的伪随机数生成器也可以通过这些测试 [11]. 因此，我们建议仅将我们的统计测试结果用作对我们理论主张的补充证据。我们在 NIST 统计测试套件上展示了我们 Pulsar RNG 完整版本的 NIST SP800-22b 结果，包括 SHA-512 量化和 SHAKE-256 随机性提取。我们测试了生成的 1 百万比特，将其评估为每个 10 万比特的 10 个位流。表 2 显示了 PST J0030+0451 在 EPTA 数据上的结果。

脉冲星随机数生成器通过了 NIST SP800-22b 中的所有测试。NIST SP800-22b 将给定的比特流与二进制位均匀随机分布的零假设 [10] 进行比较。频率测试检查比特流中 0 和 1 的比例。块频率测试检查相同的比例，但针对的是比特流的段或块。累积和测试检查比特流中的比特累计和是否遵循随机游走。连续性测试检查连续 0 或 1 的最大长度。最长连续 1 测试检查比特流区块中连续 1 的最大长度。快速傅里叶变换 [26] 测试，简称 FFT，检查比特流中是否存在任何重复模式。近似熵测试检查所有可能的重叠 m 位模式在整个序列中的频率。序列测试侧重于比特流中所有可能的重叠 m 位模式的频率。最后，线性复杂度测试侧重于线性反馈移位寄存器（LFSR）的长度以确定该序列是否足够复杂以被认为是随机的 [24]。

4 讨论

我们已经证明了脉冲星定时变化作为 RNG 熵源的可行性。理论上，基于合理的物理假设，我们证明了存在基于脉冲星的强大随机性提取器。实验上，我们使

用各种标准统计测试验证了我们的脉冲星 RNG 的质量。与基于电子设备噪声的 TRNG 相比，例如电阻中的约翰逊噪声 [27]，脉冲星 RNG 不受局部温度波动和其他局部环境因素的影响。脉冲星定时变化数据也可从多个来源公开获得，包括北美纳米赫兹引力波天文台 [23]、欧洲脉冲星计时阵列 [13]、中国脉冲星计时阵列 [28] 和澳大利亚的帕克斯脉冲星计时阵列 [29]。与大多数量子 RNG [30] 不同，我们的脉冲星 RNG 不需要专用硬件，并使用这些公开数据。

除了密码学之外，我们的 Pulsar RNG 还适用于许多其他应用。RNGs 在蒙特卡罗模拟中用于从输入变量的基本分布生成随机变数 [31]。这个随机变数生成过程实际上是蒙特卡罗模拟的核心。RNGs 也用于实现概率数据结构，如布隆过滤器 [32]、跳表 [33] 和草图 [34]。RNG 的其他用途包括机器学习算法 [35] 甚至艺术作品 [36]。我们发布了一个完全开源的 Python 实现，用于我们的 Pulsar RNG。我们的实现在多种配置下使用脉冲星数据生成随机数时包含一个可用工具。该工具目前支持 NANOGrav 和 EPTA 数据，但我们的模块化实现使得该工具容易扩展到其他公共数据集。除了我们的工具外，我们还开源了所有数据处理脚本、随机性提取方法和评估代码。最后，我们也公开发布了生成的原始比特流，以便独立验证我们的结果。我们将讨论的所有工件都已发布在 github.com/jadidbourbaki/pulsar_rng。

许多开放性问题由此工作产生。我们观察到（表 1）不同的脉冲星会产生不同的熵。已知有超过 3000 颗脉冲星，全面的研究将有助于更好地理解脉冲星定时变化中的最小熵和熵分布生成情况。在实际应用中部署基于脉冲星的随机数生成器也将展示实践优势或我们分析未涉及的挑战。

附录 A　形式定义与证明

给定集合 S，我们用 $x \leftarrow\!\!\$\ S$ 表示 x 是从 S 中均匀随机采样的。对于集合 S，我们用 $|S|$ 表示 S 中元素的数量。相同的符号用于列表 $\mathcal{L}$。我们使用 $\leftarrow$ 来表示变量赋值。如果输出是随机化算法的值，我们将使用 $\leftarrow\!\!\$$。对于随机化算法 A，我们写作 $\text{output} \leftarrow \text{A}_r(\text{input}_1, \text{input}_2, \cdots, \text{input}_l)$，其中 $r \in \mathcal{R}$ 是 A 使用的随机硬币，$\mathcal{R}$ 是可能硬币的集合。我们认为字符串 $\{0,1\}^n$ 是伽罗瓦域 $\text{GF}(2^n)$ 的元素。我们将随机变量简写为 r.v。我们假设所有对手都是计算受限的。更准确地说，我们假设对手被限制在非均匀概率多项式时间 [2]。

定义 1 (统计距离 Δ)**.** 令 X, Y 是取值范围为 U 的随机变量。

$$\Delta(X,Y) = \frac{1}{2}\Sigma_{u\in U}|P[X=u] - P[Y=u]|$$

。

定义 2 (ε-关闭)**.** 令 X, Y 为取值范围为 U 的随机变量。

$$X \approx_\varepsilon Y \equiv \Delta(X, Y) \leq \varepsilon$$

定义 3 (最小熵)**.** 令 X 为一个取值范围为 U 的随机变量。

$$H_\infty(X) = -\log_2(\max_{u \in U} P[X = u])$$

定义 4 (k 源)**.** *R.vX* 是一个 k-源如果 $H_\infty(X) \geq k$

我们基于以下关于脉冲星定时变化的假设进行分析。

假设 1. 令 P_X 表示脉冲星 P 在宇宙 U 中信号时序变化的随机变量。我们假设 P_X 是一个 k-源（定义 *4*）且具有非平凡的 k。

我们现在可以精确地在密码学意义上定义一个随机性提取器 [37]。

定义 5 (随机性提取器)**.** 令种子 U_d 在 $\{0,1\}^d$ 上均匀分布。$\mathcal{E} : \{0,1\}^n \times \{0,1\}^d \mapsto \{0,1\}^m$ 是一个 *(k,ε)*-抽取器，如果对于所有 k-源 X 在 $\{0,1\}^n$ 上独立于 U_d 的情况中，

$$\mathcal{E}(X, U_d), U_d) \approx_\varepsilon (U_m, U_d)$$

其中 U_m 均匀分布于 $\{0,1\}^m$ 独立于 X 和 U_d。

如上定义的提取器在文献中也被称为**强**提取器。

定义 6 (通用哈希族)**.** 一组大小为 2^d 的从 $\{0,1\}^n$ 到 $\{0,1\}^m$ 的哈希函数族 $\mathcal{H}$ 被称为是通用的，如果对于每一个 $x, y \in \{0,1\}^n$ 满足 $x \neq y$，

$$P_{h \in \mathcal{H}}[h(x) = h(y)] \leq 2^{-m}.$$

我们将 Pulsar RNG 算法表示为 $\mathcal{E}_p$。$\mathcal{E}_p$ 依赖于一个通用哈希族。$\mathcal{E}_p$ 从 Pulsar 熵源 $x_p \leftarrow\!\!\$\ P_X$ 获取量化数据。然后使用来自大小为 2^d 的通用哈希族 $h_p \leftarrow\!\!\$\ \mathcal{H}$ 中的哈希函数。在我们的默认实现中，这是 SHA-3 哈希家族中的 SHAKE-256 哈希函数。$\mathcal{E}_p$ 然后使用 p_x 作为 h_p 的种子。

$$\mathcal{E}_p(p_x, h) = h_p(p_x)$$

在密码学中有一个著名的称为剩余哈希引理 [37] 的结果，最初由 [38] 证明。剩余哈希引理证明了一个通用哈希族可以用来从一个 k-source 构造一个强提取器。

定理 1 (剩余哈希引理)**.** 令 X 为一个 k-源，其宇宙集合为 U。固定 $\varepsilon > 0$。令 $\mathcal{H}$ 为一个大小为 2^d 的通用哈希族，输出长度为 $m = k - 2\log_2(\frac{1}{\varepsilon})$。定义

$$\mathcal{E}(x, h) = h(x)$$

然后 $\mathcal{E}$ 是一个强 $(k, \varepsilon/2)$ 提取器，种子长度为 d，输出长度为 m。

我们现在准备证明我们的主要结果，即我们的脉冲星随机数生成器 $\mathcal{E}_p$ 是一个强提取器。

定理 2. 令 P_X 表示脉冲星 P 的信号定时变化，其宇宙为 U。固定 $\varepsilon > 0$。脉冲星随机数生成器，$\mathcal{E}_p$ 是一个强大的 $(m + 2\log_2(\frac{1}{\varepsilon}))$-抽取器，其种子长度为 d，输出长度为 m。

证明 证明直接来自于假设 1 和剩余哈希引理。 □

References

[1] Katz, J., Lindell, Y.: Introduction to Modern Cryptography, Second Edition, 2nd edn. Chapman & Hall/CRC, n/a (2014)

[2] Pass, R., Shelat, A.: A Course in Cryptography. Lecture Notes. Available at: https://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf (2010)

[3] Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978) https://doi.org/10.1145/359340.359342

[4] ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: Blakley, G.R., Chaum, D. (eds.) Advances in Cryptology, pp. 10–18. Springer, Berlin, Heidelberg (1985)

[5] Jun, B., Kocher, P.: The intel random number generator. Cryptography Research Inc. white paper **27**(1-8), 66 (1999)

[6] Pimbblet, K.A., Bulmer, M.: Random numbers from astronomical imaging. Publications of the Astronomical Society of Australia **22**(1), 1–5 (2005) https://doi.org/10.1071/AS04043

[7] Chapman, E., Grewar, J., Natusch, T.: Celestial sources for random number generation. Australian Information Security Management Conference (2016)

[8] Lee, J.S., Cleaver, G.B.: The cosmic microwave background radiation power spectrum as a random bit generator for symmetric- and asymmetric-key cryptography. Heliyon **3**(10), 00422 (2017) https://doi.org/10.1016/j.heliyon.2017.e00422

[9] Wu, C., Bai, B., Liu, Y., Zhang, X., Yang, M., Cao, Y., Wang, J., Zhang, S., Zhou, H., Shi, X., Ma, X., Ren, J.-G., Zhang, J., Peng, C.-Z., Fan, J., Zhang, Q., Pan, J.-W.: Random number generation with cosmic photons. Phys. Rev. Lett. **118**, 140402 (2017) https://doi.org/10.1103/PhysRevLett.118.140402

[10] Dawson, J.R., Hobbs, G., Gao, Y., Camtepe, S., Pieprzyk, J., Feng, Y., Tranfa, L., Bradbury, S., Zhu, W., Li, D.: Physical publicly verifiable randomness from pulsars. Astronomy and Computing **38**, 100549 (2022) https://doi.org/10.1016/j.ascom.2022.100549

[11] Saarinen, M.-J.O.: SP 800 – 22 and GM/T 0005 – 2012 Tests: Clearly Obsolete, Possibly Harmful . In: 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 31–37. IEEE Computer Society, Los Alamitos, CA, USA (2022). https://doi.org/10.1109/EuroSPW55150.2022.00011 . https://doi.ieeecomputersociety.org/10.1109/EuroSPW55150.2022.00011

[12] Matthews, A.M., Nice, D.J., Fonseca, E., Arzoumanian, Z., Crowter, K., Demorest, P.B., Dolch, T., Ellis, J.A., Ferdman, R.D., Gonzalez, M.E., *et al.*: The nanograv nine-year data set: astrometric measurements of 37 millisecond pulsars. The Astrophysical Journal **818**(1), 92 (2016)

[13] EPTA, InPTA, *et al.*: The second data release from the european pulsar timing array: V. search for continuous gravitational wave signals. Astronomy and Astrophysics **690**, 118 (2024)

[14] Luo, J., Ransom, S., Demorest, P., Ray, P.S., Archibald, A., Kerr, M., Jennings, R.J., Bachetti, M., van Haasteren, R., Champagne, C.A., Colen, J., Phillips,

C., Zimmerman, J., Stovall, K., Lam, M.T., Jenet, F.A.: PINT: A Modern Software Package for Pulsar Timing. The Astrophysical Journal **911**(1), 45 (2021) https://doi.org/10.3847/1538-4357/abe62f arXiv:2012.00074 [astro-ph.IM]

[15] Doran, R.W.: The gray code. Technical report, Citeseer (2007)

[16] Penard, W., Van Werkhoven, T.: On the secure hash algorithm family. Cryptography in context, 1–18 (2008)

[17] Walker, J.: ENT: A Pseudorandom Number Sequence Test Program. Fourmilab: Switzerland, 2008 (2008)

[18] Walker, J.: Hotbits: Genuine random numbers, generated by radioactive decay. Online: http://www. fourmilab. ch/hotbits (2001)

[19] Stipčević, M., Koç, Ç.K.: True random number generators. In: Open Problems in Mathematics and Computational Science, pp. 275–315. Springer, ??? (2014)

[20] Von Neumann, J.: Various techniques used in connection with random digits. John von Neumann, Collected Works **5**, 768–770 (1963)

[21] Antonelli, M., Basu, A., Haskell, B.: Stochastic processes for pulsar timing noise: fluctuations in the internal and external torques. Monthly Notices of the Royal Astronomical Society **520**(2), 2813–2828 (2023) https://doi.org/10.1093/mnras/stad256

[22] Zubieta, E., García, F., del Palacio, S., Araujo Furlan, S. B., Gancio, G., Lousto, C. O., Combi, J. A., Espinoza, C. M.: Timing irregularities and glitches from the pulsar monitoring campaign at iar. A&A **689**, 191 (2024) https://doi.org/10.1051/0004-6361/202450441

[23] Agazie, G., Anumarlapudi, A., Archibald, A.M., Arzoumanian, Z., Baker, P.T., Bécsy, B., Blecha, L., Brazier, A., Brook, P.R., Burke-Spolaor, S., Burnette, R., Case, R., Charisi, M., Chatterjee, S., Chatziioannou, K., Cheeseboro, B.D., Chen, S., Cohen, T., Cordes, J.M., Cornish, N.J., Crawford, F., Cromartie, H.T., Crowter, K., Cutler, C.J., DeCesar, M.E., DeGan, D., Demorest, P.B.,

Deng, H., Dolch, T., Drachler, B., Ellis, J.A., Ferrara, E.C., Fiore, W., Fonseca, E., Freedman, G.E., Garver-Daniels, N., Gentile, P.A., Gersbach, K.A., Glaser, J., Good, D.C., Gültekin, K., Hazboun, J.S., Hourihane, S., Islo, K., Jennings, R.J., Johnson, A.D., Jones, M.L., Kaiser, A.R., Kaplan, D.L., Kelley, L.Z., Kerr, M., Key, J.S., Klein, T.C., Laal, N., Lam, M.T., Lamb, W.G., W. Lazio, T.J., Lewandowska, N., Littenberg, T.B., Liu, T., Lommen, A., Lorimer, D.R., Luo, J., Lynch, R.S., Ma, C.-P., Madison, D.R., Mattson, M.A., McEwen, A., McKee, J.W., McLaughlin, M.A., McMann, N., Meyers, B.W., Meyers, P.M., Mingarelli, C.M.F., Mitridate, A., Natarajan, P., Ng, C., Nice, D.J., Ocker, S.K., Olum, K.D., Pennucci, T.T., Perera, B.B.P., Petrov, P., Pol, N.S., Radovan, H.A., Ransom, S.M., Ray, P.S., Romano, J.D., Sardesai, S.C., Schmiedekamp, A., Schmiedekamp, C., Schmitz, K., Schult, L., Shapiro-Albert, B.J., Siemens, X., Simon, J., Siwek, M.S., Stairs, I.H., Stinebring, D.R., Stovall, K., Sun, J.P., Susobhanan, A., Swiggum, J.K., Taylor, J., Taylor, S.R., Turner, J.E., Unal, C., Vallisneri, M., Haasteren, R., Vigeland, S.J., Wahl, H.M., Wang, Q., Witt, C.A., Young, O., Collaboration, T.N.: The nanograv 15 yr data set: Evidence for a gravitational-wave background. The Astrophysical Journal Letters **951**(1), 8 (2023) https://doi.org/10.3847/2041-8213/acdac6

[24] Bassham III, L.E., Rukhin, A.L., Soto, J., Nechvatal, J.R., Smid, M.E., Barker, E.B., Leigh, S.D., Levenson, M., Vangel, M., Banks, D.L., et al.: Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards & Technology (2010)

[25] Brown, R.G., Eddelbuettel, D., Bauer, D.: Dieharder. Duke University Physics Department Durham, NC, 27708–0305 (2018)

[26] Heideman, M., Johnson, D., Burrus, C.: Gauss and the history of the fast fourier transform. IEEE Assp Magazine **1**(4), 14–21 (1984)

[27] Tyson, T.: Thermal Johnson Noise Generated by a Resistor. https://123.physics.ucdavis.edu/week_2_files/Johnson_noise_intro.pdf (2013)

[28] Xu, H., Chen, S., Guo, Y., Jiang, J., Wang, B., Xu, J., Xue, Z., Nicolas Caballero, R., Yuan, J., Xu, Y., Wang, J., Hao, L., Luo, J., Lee, K., Han, J., Jiang, P., Shen, Z., Wang, M., Wang, N., Xu, R., Wu, X., Manchester, R., Qian, L., Guan, X., Huang, M., Sun, C., Zhu, Y.: Searching for the nano-hertz stochastic gravitational wave background with the chinese pulsar timing array data release i. Research in Astronomy and Astrophysics **23**(7), 075024 (2023) https://doi.org/10.1088/1674-4527/acdfa5

[29] Manchester, R.N., Hobbs, G., Bailes, M., Coles, W.A., van Straten, W., Keith, M.J., Shannon, R.M., Bhat, N.D.R., Brown, A., Burke-Spolaor, S.G., Champion, D.J., Chaudhary, A., Edwards, R.T., Hampson, G., Hotan, A.W., Jameson, A., Jenet, F.A., Kesteven, M.J., Khoo, J., Kocz, J., Maciesiak, K., Oslowski, S., Ravi, V., Reynolds, J.R., Sarkissian, J.M., Verbiest, J.P.W., Wen, Z.L., Wilson, W.E., Yardley, D., Yan, W.M., You, X.P.: The Parkes Pulsar Timing Array Project. Publications of the Astronomical Society of Australia **30**, 017 (2013) https://doi.org/10.1017/pasa.2012.017 arXiv:1210.6130 [astro-ph.IM]

[30] Ma, X., Yuan, X., Cao, Z., Qi, B., Zhang, Z.: Quantum random number generation. npj Quantum Information **2**(1), 1–9 (2016)

[31] Raychaudhuri, S.: Introduction to monte carlo simulation. In: 2008 Winter Simulation Conference, pp. 91–100 (2008). IEEE

[32] Bloom, B.H.: Space/time trade-offs in hash coding with allowable errors. Commun. ACM **13**(7), 422–426 (1970) https://doi.org/10.1145/362686.362692

[33] Pugh, W.: Skip lists: a probabilistic alternative to balanced trees. Commun. ACM **33**(6), 668–676 (1990) https://doi.org/10.1145/78973.78977

[34] Cormode, G., Muthukrishnan, S.: An improved data stream summary: the count-min sketch and its applications. Journal of Algorithms **55**(1), 58–75 (2005) https://doi.org/10.1016/j.jalgor.2003.12.001

[35] Mitchell, T.: Introduction to machine learning. Machine learning **7**, 2–5 (1997)

[36] Bauer, A.: Gallery of random art. https://www.random-art.org/ (1998)

[37] Reyzin, L.: Lecture Notes for CS 937: Advanced Topics in Cryptography. Spring 2011. Available online: https://www.cs.bu.edu/~reyzin/teaching/s11cs937/notes-leo-1.pdf (2011)

[38] Impagliazzo, R., Levin, L.A., Luby, M.: Pseudo-random generation from one-way functions. In: Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing. STOC '89, pp. 12–24. Association for Computing Machinery, New York, NY, USA (1989). https://doi.org/10.1145/73007.73009 . https://doi.org/10.1145/73007.73009