# 简单的连续工作证明

## Simple Proofs of Sequential Work

Bram Cohen 1 and Krzysztof Pietrzak 2

Eurocrypt 2018 最佳论文

**摘要**

在ITCS 2013年，Mahmoody、Moran和Vadhan [MMV 13]介绍并构建了可公开验证的连续工作证明，这是一种证明了对一个声明花费了连续计算工作的协议。这种证明的最初动机包括非交互式时间戳和可普遍验证的CPU工作台标记。最近的一个应用，也是我们的主要动机，是区块链设计，在这里，连续工作的证明可以结合使用空间证明作为一种更生态和经济的替代方法来替代目前用于保护比特币和其他加密货币的工作证明。

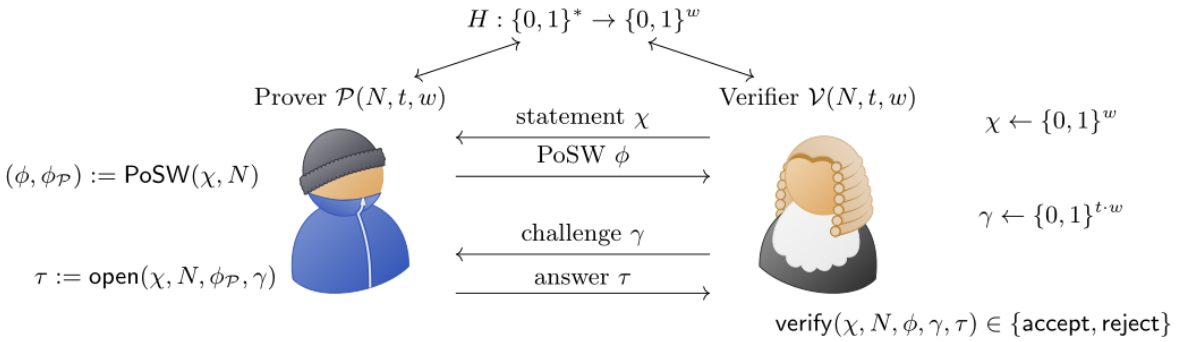
在连续工作的证明中，prover得到一个声明X，一个时间参数N和一个哈希函数H，H对于安全证明是一个随机预言机。

**正确性可靠性**

**正确性**要求，只要对H进行了N时间的运算，就能通过一个诚实的证人的验证

**可靠性**要求，任何验证器接受的内容必须是对H进行了(几乎)N次顺序查询。从而此解决方案能够证明收到X后经历了N时间的流逝。解决方案必须在最多n的对数的时间内公开可验证。

**验证流程**




- PoSW(χ,N)对哈希**函数Hx**进行了N次查询，得到了根节点φ与全部节点信息φp，任何欺骗者想要让验证者接受自己的证明，必须继续几乎N次顺序查询来计算φ。t是一个统计学的安全参数，t越大，健壮性越好：如果欺骗者只进行了（1-α）N次顺序查询，那么通过验证的可能是（1-α）^t（当t=21，α=0.8，那么通过验证的可能性<1%），w是Hash函数输出范围，用来抵御哈希碰撞和保持连续性，w=256是标准值。
- 验证者生成γ发送给证明者，证明者使用**open函数**计算出τ返回给验证者
- 验证者根据 γ ，τ，N，使用**verify函数**计算出根节点，验证与证明者给出的根节点φ是否相同

**DAG图**

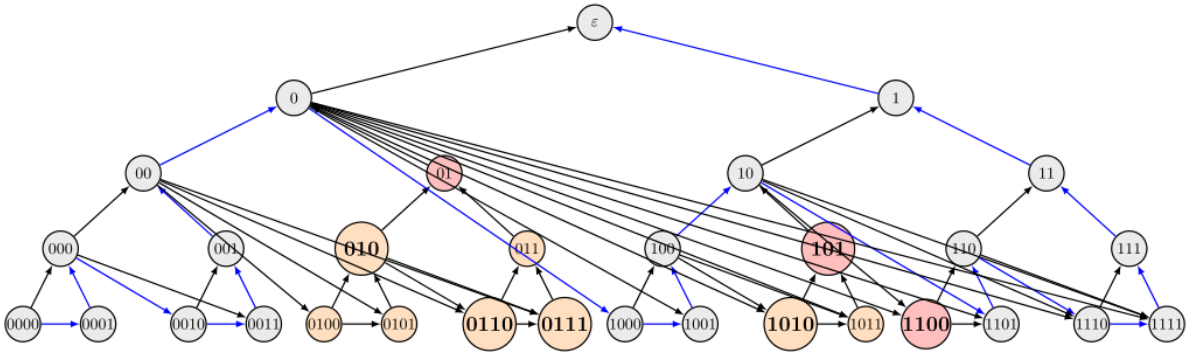



**Fig. 3.** Illustration of $G_4^{\mathsf{PoSW}}$. The set $S^* = \{01, 101, 1100\}$ – which e.g. could be derived from $S = \{010, 0110, 0111, 101, 1010, 1100\}$ – is shown in red. $D_{S^*}$ is the union of red and orange nodes. $\hat{S} = \hat{S}^*$ are the orange or red leaves. The path of length $2N - 1 - |B_S| = 32 - 1 - 11 = 19$ (as constructed in the proof of Lemma 4) is shown in blue.

## Hx函数

**使用Hx函数计算了DAG图的标签，标签保存在φp，φ保存根节点的标签lε**

$(\phi, \phi_{\mathcal{P}}) := \mathsf{PoSW}^{\mathsf{H}_\chi}(N)$ : computes the labels $\{\ell_i\}_{i\in\{0,1\}^{\leq n}}$ (cf. Def. 1) of the graph $G_n^{\mathsf{PoSW}}$ (as defined in §4) using $\mathsf{H}_\chi$. It stores the labels $\phi_{\mathcal{P}} = \{\ell_i\}_{i\in\{0,1\}^{\leq m}}$ of the $m$ highest layers, and sends the root label $\phi = \ell_\varepsilon$ to $\mathcal{V}$.

## open函数

**验证者发送γ给证明者，证明者返回返回γ到root路径上的兄弟节点的label**

$\tau := \mathsf{open}^{\mathsf{H}_\chi}(N, \phi_{\mathcal{P}}, \gamma)$ : on challenge $\gamma = (\gamma_1 \ldots, \gamma_t)$, $\tau$ contains – for every $i, 1 \leq i \leq t$ – the label $\ell_{\gamma_i}$ of node $\gamma_i \in \{0,1\}^n$ and the labels of all siblings of the nodes on the path from $\gamma_i$ to the root (as in an opening of a Merkle tree commitment), i.e.,

$$\{\ell_k\}_{k\in\mathcal{S}_{\gamma_i}} \text{ where } \mathcal{S}_{\gamma_i} \stackrel{\text{def}}{=} \{\gamma_i[1\ldots j-1] \| (1-\gamma_i[j])\}_{j=1\ldots n}$$

and

$$\tau \stackrel{\text{def}}{=} \{\ell_{\gamma_i}, \{\ell_k\}_{k\in\mathcal{S}_{\gamma_i}}\}_{i=1\ldots t} .$$

E.g., for $\gamma_i = 0101$ (cf. Figure 3) $\tau$ contains the labels of 0101, 0100, 011, 00 and 1.

## verify函数

**验证者根据 γ ，τ，N，计算出根节点，验证与证明者给出的根节点是否相同**

$\mathsf{verify}^{\grave{\mathsf{H}}_\chi}(N, \phi, \gamma, \tau)$ : Using that the graphs $G_n^{\mathsf{PoSW}}$ have the property that all the parents of a leaf $\gamma_i$ are in $\mathcal{S}_{\gamma_i}$, for every $i, 1 \leq i \leq t$, one first checks that $\ell_{\gamma_i}$ was correctly computed from its parent labels (i.e., as in Eq.1)

$$\ell_{\gamma_i} \stackrel{?}{=} \mathsf{H}_\chi(i, \ell_{p_1}, \ldots, \ell_{p_d}) \text{ where } (p_1, \ldots, p_d) = \mathsf{parents}(\gamma_i) \ .$$


[DN93] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In Ernest F. Brickell, editor, CRYPTO' 92, volume 740 of LNCS, pages 139–147. Springer, Heidelberg, August 1993.

[DFKP15] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof
Pietrzak. Proofs of space. In Rosario Gennaro and Matthew J. B. Robshaw, editors, CRYPTO 2015, Part II, volume 9216 of LNCS, pages 585–605. Springer, Heidelberg, August 2015.

Hamza Abusalah, Joël Alwen, Bram Cohen, Danylo Khilko, Krzysztof Pietrzak, Leonid Reyzin:
**Beyond Hellman's Time-Memory Trade-Offs with Applications to Proofs of Space.** ASIACRYPT (2) 2017: 357-379

[MMV13] Mohammad Mahmoody, Tal Moran, and Salil P. Vadhan. Publicly verifiable
proofs of sequential work. In Robert D. Kleinberg, editor, ITCS 2013, pages 373–388. ACM, January 2013