小马随机信标

（第一章工作原理）

欢迎您进入小马随机信标网站 www.sjxb.com.cn。我公司致力于区块链和商用密码的新技术创新和工程实现。第 1 章先解释小马随机信标的工作原理，未来章节将陆续公布，编码器解码器代码和试运行的随机信标结果。欢迎对无偏随机信标有需求的客户、学术界和集成电路芯片厂关注本网站。

将为公众提供一种基于 VDF32 算法的可证无偏随机信标，以下简称小马随机信标。小马随机信标拟解决人类对公开摇号、公证公开随机数需求，服务对象为智能合约、射幸合同、游戏开盲盒、稀缺资源公平抽签、合议庭抽签等场景。其中，实现无偏功能的核心组件为 VDF32 算法（一种可解码的可验证延迟函数）。

广告语:并不是所有的随机信标都是无偏的。

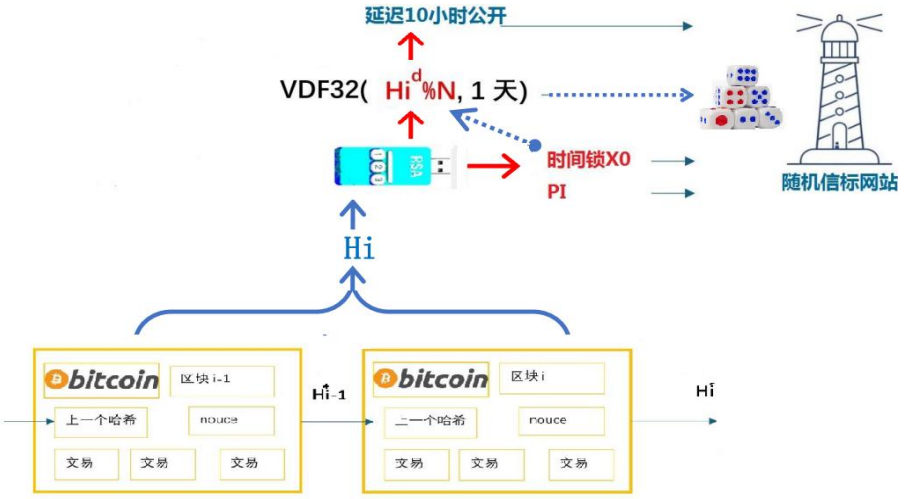
一、工作原理

生产者：VDF32（Hi^d%N，1天）作为随机信标，其中Hi相当于比特币第i区块hash。

验证者：用RSA验签脚本modexp（Hi^d，0x10001，N）-Hi？=0，验算时间戳及熵源正确性，用VDF32解码电路验算VDF32编码正确性，耗时21.1秒/255个解码电路。

质押者：Hi年龄的半小时至1小时内，为安全质押期。

图1,小马随机信标的原理图



公众可以这样理解小马随机信标的工作原理和安全性假设。即使比特币矿工+生产者+攻击者联盟为共谋复合体，其中，攻击者具备设计生产高性能ASIC的能力（假定人类不存在48倍-24倍算速电路）。所述共谋复合体也不能在半小时-1小时内，看到VDF32（Hi^d%N，1天）的计算结果；所以，没办法对小马随机信标作弊。

可以形象理解：全世界人都可以通过比特币矿工角色参加抽签游戏，每个签的结果至少1小时后才能看到，又因为每10分钟必须公告本轮抽签的结果，所以，来不及作弊。

即使比特币矿工依靠51%算力回滚区块1小时剔除Hi；Hi虽然在链上被剔除了，但质押协议和回滚比特币长链的新闻事件可以证明Hi真实存在过。

为了阻击攻击者同步计算VDF32编码，Hi生成10小时后由生成者公布Hi^d。

本设计还包括改良时间锁设计组件，模 RSA 模数连续立方 t2 的结果恰恰等于 Hi^d%N，由 PI 证明时间锁断言正确性，技术优势，断言证明不需要计算结果；时间锁及其 PI 可以防止生产者拒绝服务或故意作恶的功能。改良时间锁组件设计:

验证者获得 Hi^d，可以由生成者公开，也可以通过 X0 连续立方 t2 次获得。

改良时间锁是随机信标的辅助组件，功能和用途是，通过时间锁原语阻击攻击者同步计算 VDF32，不需要计算结果即可验证生产者是否虚假承诺。改良的理由是，我们发现已有 Wesolowski-VDF 类型的时间锁的技术不足，必须等到计算结果完成，才可以实施验证。从 VDF32 信标设计功能看，希望时间锁计算结果恰恰为 Hi^d，希望在时间锁计算前能用零知识证明时间锁的结果恰恰等于 Hi^d。为了实现既定功能并且解决已有时间锁技术不足创设了改良时间锁方案。通过方程式推演和验算器程序验证，如图 1 所示，攻击者必须先计算时间锁，再计算 VDF32，生成者只需计算 VDF32。

给出 X0 和 PI 的简明结果，令 $X0^{3^{\wedge}t}=Hi^d$;

得到时间锁 X0 为：$Hi^{d*3^{\wedge}-t}$;

改良方法:令 g=X0，$y=Hi^d$，连续平方改成连续立方;

所以，$\mathrm{PI}=X0^{e*(3^{-t2}-r)}\cdot l^{-1}$

验证方程式为$\mathbf{PI}^{l}*(\mathbf{x0}^{\mathbf{e}})^{\mathbf{r}}=\mathbf{Hi}$。

二、VDF32 算法

针对 VDF 竞品不足，首次提出适用随机信标的 VDF32 设计。工作原理：编码器相当于宽度为 1、深度为 13 层 g 逻辑的串行电路，解码器相当于宽度为 13、深度为 1 层 g^{-1}逻辑的并行电路。采用 4 种电路评估方法评估解码器和编码器的关键路径，结果显示：编码器理论时延大约是解码器时延 34.6 倍，NanGate 15nm 手工评估增益 35.53，TSMC90nm 综合软件评估增益为 35.6，在 EP3C25Q240 实际增益 16。

VDF32 输入输出为 32 字节，迭代逻辑是 VDF32({A15，A14，..A0},1)={g(~(~A15&A14)&A13)⊕A0⊕轮常数），A14 ，…，A1}，其中 g^{-1}为稀疏抽头设计。竞品包括连续 SHA2、Wesolowski-VDF 和 minroot/Nova。技术优势，除因极长时间计算导致验证阶段的综合开销较大，以下指标全面领先：1.不需要初始化 setup 和零知识证明，2.可解码型 VDF，3.电路热点 16bit，因此特别省电，4.易于 ASIC 实现，5.抗量子设计，其中在能量消耗和抗特殊硬件加速表现最优。

salt 为 16 字节，生成多项式 X128+X40+X24+X16+1，周期 524280；每个周期迭代 24 个子轮，每个子轮迭代 13 次 g 逻辑。

参照当前最高性能 FPGA 表现定义**第一代算速标准，VDF32 编码每个子轮 75Mhz**，由 xczu2cg 电路实现。由此定义 1 天颗粒为，2000*255 个大颗粒 VDF32 编码，更具体时间推导如下。

方程式：2000*255*24*524280*75Mhz^{-1}=8556.25 秒=0.9903 天。

图 2　VDF32 编码器的整体结构图

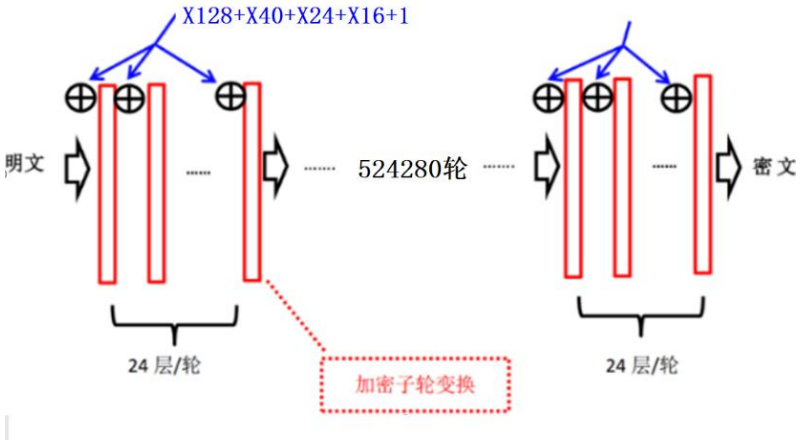
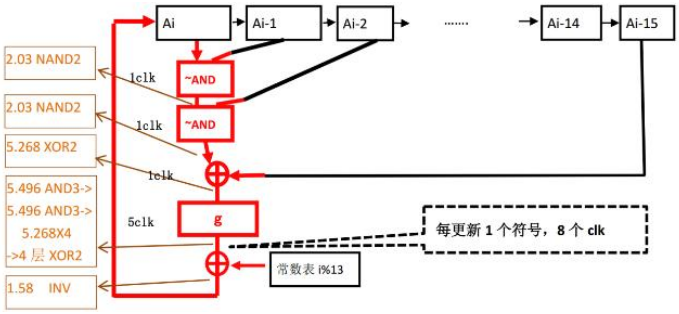


图 3.编码器子轮 1/13 逻辑及关键路径分析（8clk/**42.972**）



			TMSC90nm			
	理论	NateGate15nm	TSMC90nm	XCZU2CG	EP3C25Q240	AMD9700
编码延迟	8*13	42.972ps*13	500Mhz/24	75Mhz/24	33Mhz/24(34.9 秒 *20)	24.43Mhz/24
解码延迟	3	15.696 ps	333Mhz	50Mhz	24Mhz(40.0 秒)	6.97Mhz
增益	34.6	35.53	35.9	16	17.5	6.45

表 1.编码器/解码器性能评估及其增益

当前的第一代算速由Xczu2cg支撑，编码1子轮75Mhz，解码24子轮50Mhz，所以，255*2000个颗粒编码0.99天，验证者可用255个解码器21.1秒验证编码正确性；

参照当前最高性能 FPGA 表现定义第一代算速标准，VDF32 编码每个子轮 75Mhz，由 xczu2cg 电路实现。由此定义 1 天颗粒为，2000*255 个大颗粒 VDF32 编码。

方程式：**2000*255*24*524280*75Mhz^{-1}=8556.25 秒=0.9903 天。**

下面，是 VDF32 的编码器和解码器在各平台的性能表现。

VDF32编码1子轮　75Mzh 第一代算速

VDf32解码24子轮 50Mhz

实体或评估	VDF32 编码 1 子轮	VDF32 解码 24 子轮	增益	2000*255 个大颗粒编码	2000*255 个大颗粒解码
TMSC90nm	333Mhz （synopsys 评估）	500Mhz （synopsys 评估）	36.0	0.223 天	2.11 秒
XCZU2cg （16nm 工艺）	**75Mhz** **(实测 2000 个颗粒 335.5 秒）** 被定义第 1 代算速	50Mhz (实测 200 个颗粒 2.1 秒）	16.0	0.99 天	21.1 秒
AMD9700X 睿频 5.5G	~~24.43Mhz~~ 31. 66Mhz （实测 2000 个大颗粒 ~~1029~~ 秒） 794. 0	6.97Mhz (实测 2000 个颗粒 150 秒）	~~6.85~~ 5. 29	~~3.04~~ 2. 35 天	150.3 秒

表 2.VDF32 编码速度表现和电路评估

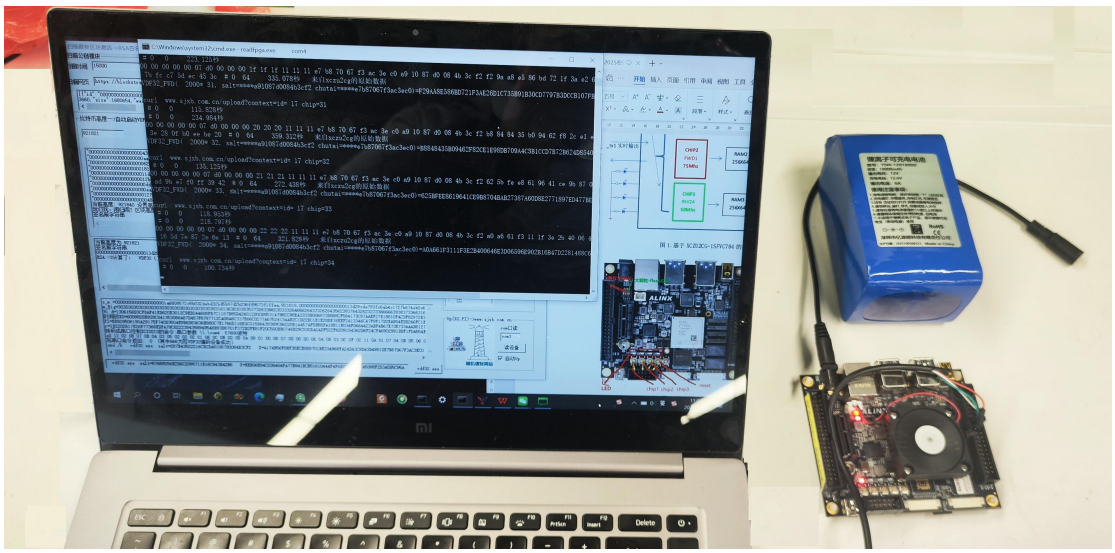


图 4.xczu2cg 器件编码器实际工作状态

解码器数量/线程	2000 颗粒运行时间	编码核心的 clk 数	备注
2	150.3 秒	32.7	128 核全速/性能优先
4	158.0 秒	34.4	
6	167.5 秒	36.5	
8	186.5 秒	40.5	32 核全速/资源优先

表 3.AMD9700X-解码器性能评估

对 AMD9700X 型 cpu 而言，VDF32 编码不能被加速，但多路的 VDF32 解码可以被显著加速。其中 AVX512 指令更贡献 2 倍，超标量贡献 1-4 倍，多核多线程可以继续贡献。我们认为 32 个 AVX512 物理核 186.5 秒验算完第一算速 1 天的 VDF32 编码结果是可以被公众接受的成果。

三、竞品分析

我们认为，无偏性是最难的，任何带私钥的设计先天存在不能无偏的缺陷，比如基于 VRF 组件的以太坊随机信标，我们还认为，VDF（可验证延迟函数）是构造无偏随机信标的必要组件。下面是，搜集的 VDF 竞品及竞品分析，由此证明本题目在功能上的技术优势。

随机信标竞品	时间戳	无偏性	对接区块链/元宇宙	备注
比特币区块 hash	可以证明(好)	矿工发现随机信标对己方不利，不要奖励也不记账。(较差)	适用	区块链浏览器 blockstream.info Blockstream EXPLORER
以太坊随	可以证明	矿工发现	适用	区块链浏览器

机信标链	(好)	随机信标对己方不利，宁可被惩罚，也不记账。（较差）		www.oklink.com/zh-hans/ethereum
联盟链	先天熵源质量差，不是公众参与？被腐化和共谋作恶成本极低。	重放作恶成本极低。	不适用	联盟共谋情况，欺骗公众成本极低，存在重放欺骗可能。所以，构造不非偏性的成本很低。
基于VDF32随机信标（本作品）	唯一熵源为最新鲜比特币区块hash。	生产新区块的时间远小于随机信标计算时间（逻辑自洽）	适用	**独立站：**www.sjxb.com.cn 

表 2.随机信标竞品分析表

相比 Wesolowski-VDF 和 Minroot，VDF32 编码器热点只有 16bit，所以特别省电、容易电路评估的电路实现。Wesolowski-VDF 编码器热点高达 8192 比特，所以特别费电，极难评估和高性能电路实现。可以这样认为，VDF32 编码器是“滴漏”特别省资源，其他是竞品是小溪或瀑布，特别费资源。

示意图 1:VDF32->铜壶滴漏

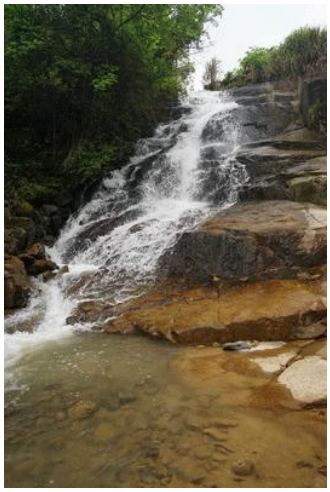


示意图 2:其他竞品->小溪瀑布

分析内容\竞品		**本论文 VDF32/vdf32-1**	连续 SHA2 方案	**Wesolowski-VDF**	Minroot/nova
工作原理		**编码为 1 个串行电路；解码优选 255 个并行电路，比如 128 个或 64 个 AVX512 物理核**	编码为 1 个 SHA2 单元，验证为 160KB 数据，4000 核 GPU。	**理论上，RSA 的 N 群阶必须不能被任何人获知，基于时间谜题。**	理论上，椭圆曲线群阶不能被任何人获知，类似时间谜题。
1.Setup 阶段		**无（好）**	无（好）	**必须的（差）**	必须的（差）
2 计算阶段	面积消耗	**最小**	较小	**极大**	较大
	能量消耗	**最小**	中	**极大**	中
	抗特殊硬件加速	**最好评估**	较容易评估	**极难评估**	极难评估
3.验证阶段	时间复杂度	**t/空间复杂度字节数**	约本案的 34.6 倍	**很短，Log（t）**	很短，但零知识启动时间很大+log（t）
	空间复杂度	**参考 8192 字节/8823 倍增益**	参考 160K 字节/4000 倍增益	**参考：2048 字节/RSA8192**	参考：8k -16k,跟 log(t)有关
量子攻击		**免疫（好）**	免疫（好）	**不免疫（差）**	不免疫（差）
可解码性		**是（好）**	否（差）	**否（差）**	否（差）
参考资料		**本作品**	Solana 白皮书	**参考资料[3]，CSDN 网站**	参考资料[4] [5]，CSDN 网站

表 3.4 种 VDF 竞品对照方表

很快将公开 VDF32 的编码器解码器源程序和随机信标试运行成果，敬请关注。欢迎用户和工业界垂询。欢迎区块链和密码学专家公开评议。

网址：www.sjxb.com.cn

邮箱：ma_zs73@sina.com

知识产权归小马随机信标

2025 年 11 月 2 日