(Verifiable) Delay Functions from Lucas Sequences

Charlotte Hoffmann[1] Chethan Kamath[4]

Pavel Hubáček[2,3] Tomáš Krňák[3]

[1] Institute of Science and Technology Austria

[2] Institute of Mathematics, Czech Academy of Sciences

[3] Charles University, Faculty of Mathematics and Physics

[4] Indian Institute of Technology Bombay

Verifiable Delay Functions

- $f_T : X \to Y$

Verifiable Delay Functions

- $f_T : X \to Y$
- sequentiality: evaluation of f_T requires T sequential steps
  - usually $f_T = \underbrace{f \circ \ldots \circ f}_{T}$

Verifiable Delay Functions

- $f_T : X \to Y$
- sequentiality: evaluation of f_T requires T sequential steps
  - usually $f_T = \underbrace{f \circ \ldots \circ f}_{T}$
- public verifiability: $P(x, T) = (y, \pi)$ $\pi : f_T(x) = y$

Verifiable Delay Functions

- $f_T : X \to Y$
- sequentiality: evaluation of f_T requires T sequential steps
  - usually $f_T = \underbrace{f \circ \dots \circ f}_{T}$
- public verifiability: $P(x, T) = (y, \pi)$ $\pi : f_T(x) = y$

- applications:
  - resource-efficient blockchains [CP19]
  - randomness beacons [Rab83, Sch+21]
  - short-lived proofs and signatures [ABC22]
  - proof of data replication [Bon+18]
  - ...

Verifiable Delay Functions

- $f_T : X \to Y$
- sequentiality: evaluation of f_T requires T sequential steps
  - usually $f_T = \underbrace{f \circ \dots \circ f}_{T}$
- public verifiability: $P(x, T) = (y, \pi)$ $\pi : f_T(x) = y$

- applications:
  - resource-efficient blockchains [CP19]
  - randomness beacons [Rab83, Sch+21]
  - short-lived proofs and signatures [ABC22]
  - proof of data replication [Bon+18]
  - ...
- constructions:
  - hidden order groups [Pie19, Wes20]
  - SNARKs [Bon+18]
  - isogenies [Feo+19, Sha19, CRT21]
  - lattices [LM23, CLM23]
  - squaring in a finite field [KMT22]

(Modular) Lucas Sequences

- $U(P,Q)$: $U_0 = 0,\ U_1 = 1,\ U_i = PU_{i-1} - QU_{i-2}$
- $V(P,Q)$: $V_0 = 2,\ V_1 = P,\ V_i = PV_{i-1} - QV_{i-2}$

(Modular) Lucas Sequences

- $U(P,Q)$: $U_0 = 0,\ U_1 = 1,\ U_i = PU_{i-1} - QU_{i-2}$
- $V(P,Q)$: $V_0 = 2,\ V_1 = P,\ V_i = PV_{i-1} - QV_{i-2}$
- $U(1,-1)$ ... Fibonacci numbers
- $U(2,-1)$ ... Pell numbers

(Modular) Lucas Sequences

- $U(P,Q)$: $U_0 = 0,\ U_1 = 1,\ U_i = PU_{i-1} - QU_{i-2}$
- $V(P,Q)$: $V_0 = 2,\ V_1 = P,\ V_i = PV_{i-1} - QV_{i-2}$
- $U(1,-1)$ ... Fibonacci numbers
- $U(2,-1)$ ... Pell numbers
- primality tests, factorization [Rie85, Wil82]
- LUC cryptosystems [LS93, MN81, BBL85]

Construction

- $g_T(P,Q) = (U_{2^T}(P,Q) \bmod N, V_{2^T}(P,Q) \bmod N)$

Construction

- $g_T(P,Q) = (U_{2^T}(P,Q) \bmod N, V_{2^T}(P,Q) \bmod N)$
- well known fact:

  let $\omega, \bar{\omega} \in \mathbb{Z}_N[\sqrt{P^2-4Q}]$ be roots of $x^2 - Px + Q$

  then $U_n = \frac{\omega^n - \bar{\omega}^n}{\omega - \bar{\omega}}$ and $V_n = \omega^n + \bar{\omega}^n$

Construction

- $g_T(P,Q) = (U_{2^T}(P,Q) \bmod N, V_{2^T}(P,Q) \bmod N)$
- well known fact:

  let $\omega, \bar{\omega} \in \mathbb{Z}_N[\sqrt{P^2-4Q}]$ be roots of $x^2 - Px + Q$

  then $U_n = \dfrac{\omega^n - \bar{\omega}^n}{\omega - \bar{\omega}}$ and $V_n = \omega^n + \bar{\omega}^n$

- $g_T(P,Q) = \omega^{2^T}$

Sequentiality

$$f_T : \mathbb{Z}_N \to \mathbb{Z}_N$$
$$x \mapsto x^{2^T}$$

- RSW: f_T is sequential [RSW96]

Sequentiality

$f_T : \mathbb{Z}_N \to \mathbb{Z}_N$

$x \mapsto x^{2^T}$

- RSW: f_T is sequential [RSW96]

$g_T : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$

$(P, Q) \mapsto (U_{2^T}, V_{2^T})$

- LCS: g_T is sequential

Sequentiality

$f_T : \mathbb{Z}_N \to \mathbb{Z}_N$

$x \mapsto x^{2^T}$

$g_T : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$

$(P, Q) \mapsto (U_{2^T}, V_{2^T})$

- RSW: f_T is sequential [RSW96]
- LCS: g_T is sequential

- proven: RSW $\leq$ LCS

Sequentiality

$f_T : \mathbb{Z}_N \to \mathbb{Z}_N$

$x \mapsto x^{2^T}$

$g_T : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$

$(P, Q) \mapsto (U_{2^T}, V_{2^T})$

- RSW: f_T is sequential [RSW96]
- LCS: g_T is sequential
- proven: RSW $\leq$ LCS

$$\frac{U_{2^T}^2 - D V_{2^T}^2}{4} = Q^{2^T} \quad [PB91]$$

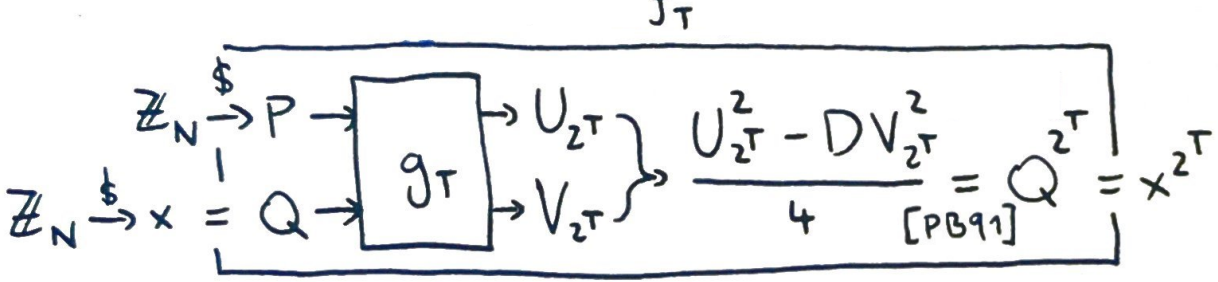
Sequentiality

$f_T : \mathbb{Z}_N \to \mathbb{Z}_N$
$x \mapsto x^{2^T}$

$g_T : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$
$(P, Q) \mapsto (U_{2^T}, V_{2^T})$

- RSW: f_T is sequential [RSW96]
- LCS: g_T is sequential

- proven: RSW $\leq$ LCS



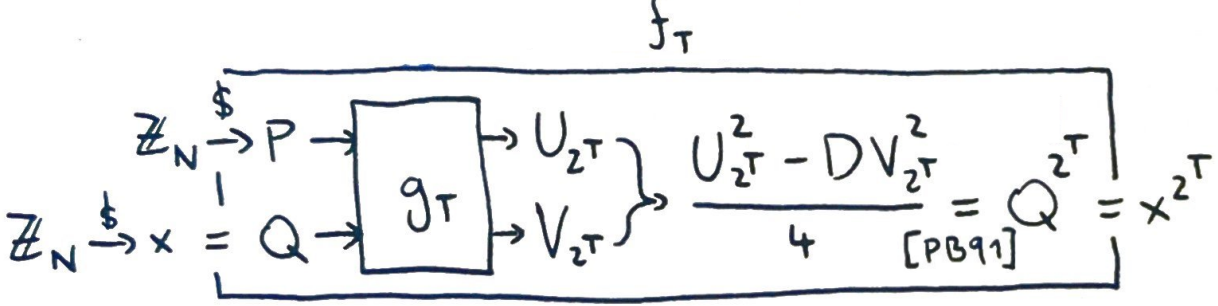
Sequentiality

$f_T : \mathbb{Z}_N \to \mathbb{Z}_N$
$x \mapsto x^{2^T}$

$g_T : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N \times \mathbb{Z}_N$
$(P, Q) \mapsto (U_{2^T}, V_{2^T})$

- RSW: f_T is sequential [RSW96]
- LCS: g_T is sequential

- proven: RSW $\leq$ LCS



- conjectured: RSW $<$ LCS

Verifiability

Pietrzak's protocol [Pie19]

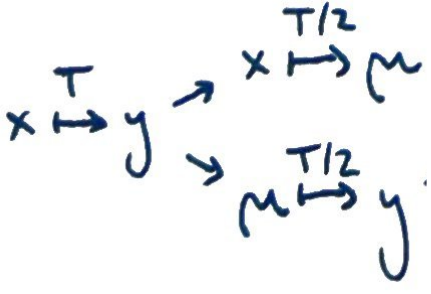
Verifiability

Pietrzak's protocol [Pie19]

$x \overset{T}{\mapsto} y$

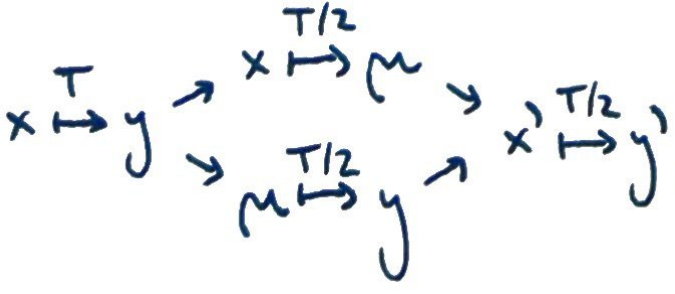
Verifiability

Pietrzak's protocol [Pie19]



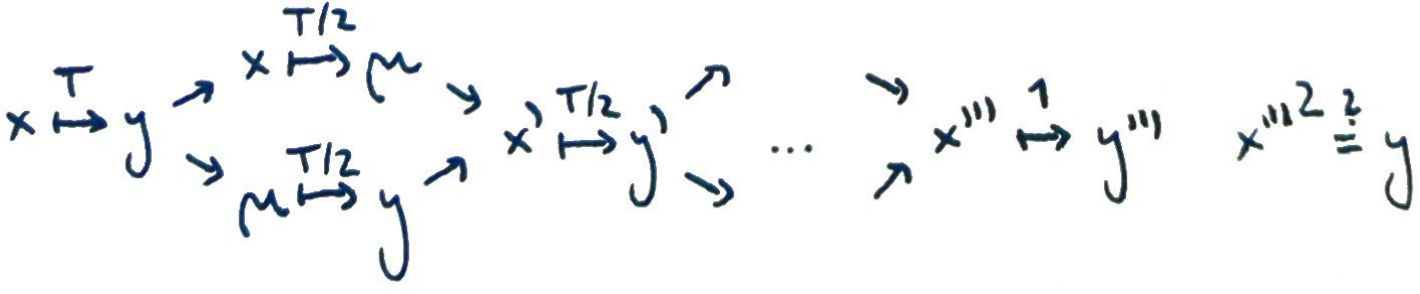
Verifiability

Pietrzak's protocol [Pie19]



Verifiability

Pietrzak's protocol [Pie19]



Verifiability

Pietrzak's protocol [Pie19]

This work

Verifiability

	Pietrzak's protocol [Pie19]	This work
base group	$\mathbb{Z}_N^{(2)}(\cdot)$	$\mathbb{Z}_N^{(a)}[\sqrt{D}](\cdot)$
function	$x \mapsto x^{2^T}$	$\omega \mapsto \omega^{2^T}$

Verifiability

	Pietrzak's protocol [Pie19]	This work
base group	$\mathbb{Z}_N^{(2)}(\cdot)$	$\mathbb{Z}_N^{(a)}[\sqrt{D}](\cdot)$
function	$x \mapsto x^{2^T}$	$\omega \mapsto \omega^{2^T}$
factors of N	safe primes $\mathbb{Z}_{p-1}^{(2)}(\cdot)$ is a prime order group	strong primes $\mathbb{Z}_{p-1}^{(a)}(\cdot)$ and $\mathbb{Z}_{p+1}^{(a)}(\cdot)$ have no subgroups of small order

Verifiability

	Pietrzak's protocol [Pie19]	This work
base group	$\mathbb{Z}_N^{(2)}(\cdot)$	$\mathbb{Z}_N^{(a)}[\sqrt{D}](\cdot)$
function	$x \mapsto x^{2^T}$	$\omega \mapsto \omega^{2^T}$
factors of N	safe primes $\mathbb{Z}_{p-1}^{(2)}(\cdot)$ is a prime order group	strong primes $\mathbb{Z}_{p-1}^{(a)}(\cdot)$ and $\mathbb{Z}_{p+1}^{(a)}(\cdot)$ have no subgroups of small order
cofactor	2	$a \in O(1)$

Verifiability

	Pietrzak's protocol [Pie19]	This work
base group	$\mathbb{Z}_N^{(2)}(\cdot)$	$\mathbb{Z}_N^{(a)}[\sqrt{D}](\cdot)$
function	$x \mapsto x^{2^T}$	$\omega \mapsto \omega^{2^T}$
factors of N	safe primes $\mathbb{Z}_{p-1}^{(2)}(\cdot)$ is a prime order group	strong primes $\mathbb{Z}_{p-1}^{(a)}(\cdot)$ and $\mathbb{Z}_{p+1}^{(a)}(\cdot)$ have no subgroups of small order
cofactor	2	$a \in O(1)$
group membership verifiability	$\sqrt[2]{\mu}$ is a previous member of the sequence	prover gets $\sqrt[a]{\mu}$ by delaying cofactor clearing

Summary and Open Problems

- a new VDF candidate based on new hardness assumption

Summary and Open Problems

- a new VDF candidate based on new hardness assumption
- RSW ≤ LCS proven

Summary and Open Problems

- a new VDF candidate based on new hardness assumption
- RSW ≤ LCS proven
- generalization of the Pietrzak's protocol

Summary and Open Problems

- a new VDF candidate based on new hardness assumption
- RSW $\leq$ LCS proven
- generalization of the Pietrzak's protocol
- open problems
  - RSW $<$ LCS conjecture

Summary and Open Problems

- a new VDF candidate based on new hardness assumption
- $RSW \leq LCS$ proven
- generalization of the Pietrzak's protocol
- open problems
  - $RSW < LCS$ conjecture
  - verifiability of primality of Mersenne numbers
    - non-primality of certificates for Proth's numbers [Hof+23]

$2^{82,589,933} - 1$ Mersenne

$10223 \cdot 2^{31,172,165} + 1$ Proth

Summary and Open Problems

- a new VDF candidate based on new hardness assumption
- RSW ≤ LCS proven
- generalization of the Pietrzak's protocol
- open problems
  - RSW < LCS conjecture
  - verifiability of primality of Mersenne numbers
    - non-primality of certificates for Proth's numbers [Hof+23]

$2^{82,589,933} - 1$ Mersenne $10223 \cdot 2^{31,172,165} + 1$ Proth

Thank you for your attention!

References

[ABC22] Arasu Arun, Joseph Bonneau, and Jeremy Clark. *Short-lived zero-knowledge proofs and signatures*. Cryptology ePrint Archive, Paper 2022/190. https://eprint.iacr.org/2022/190. 2022. URL: https://eprint.iacr.org/2022/190.

[BBL95] Daniel Bleichenbacher, Wieb Bosma, and Arjen K. Lenstra. "Some Remarks on Lucas-Based Cryptosystems". In: *CRYPTO*. Vol. 963. Lecture Notes in Computer Science. Springer, 1995, pp. 386–396.

[Bon+18] Dan Boneh et al. "Verifiable Delay Functions". In: *CRYPTO (1)*. Vol. 10991. Lecture Notes in Computer Science. Springer, 2018, pp. 757–788.

[CLM23] Valerio Cini, Russell W. F. Lai, and Giulio Malavolta. "Lattice-Based Succinct Arguments from Vanishing Polynomials". In: *Advances in Cryptology – CRYPTO 2023*. Ed. by Helena Handschuh and Anna Lysyanskaya. Cham: Springer Nature Switzerland, 2023, pp. 72–105. ISBN: 978-3-031-38545-2.

[CP19] Bram Cohen and Krzysztof Pietrzak. *The Chia Network Blockchain*. Tech. rep. https://www.chia.net/assets/ChiaGreenPaper.pdf, Accessed: 2022-07-29. Chia Network, 2019.

[CRT21] Jorge Chávez-Saab, Francisco Rodríguez-Henríquez, and Mehdi Tibouchi. "Verifiable Isogeny Walks: Towards an Isogeny-Based Postquantum VDF". In: *SAC*. Vol. 13203. Lecture Notes in Computer Science. Springer, 2021, pp. 441–460.

[Feo+19] Luca De Feo et al. "Verifiable Delay Functions from Supersingular Isogenies and Pairings". In: *ASIACRYPT (1)*. Vol. 11921. Lecture Notes in Computer Science. Springer, 2019, pp. 248–277.

[Hof+23] Charlotte Hoffmann et al. *Certifying Giant Nonprimes*. Cryptology ePrint Archive, Paper 2023/238. https://eprint.iacr.org/2023/238. 2023. URL: https://eprint.iacr.org/2023/238.

[KMT22] Dmitry Khovratovich, Mary Maller, and Pratyush Ranjan Tiwari. *MinRoot: Candidate Sequential Function for Ethereum VDF*. Cryptology ePrint Archive, Paper 2022/1626. https://eprint.iacr.org/2022/1626. 2022. URL: https://eprint.iacr.org/2022/1626.

[LM23] Russell W. F. Lai and Giulio Malavolta. "Lattice-Based Timed Cryptography". In: *Advances in Cryptology – CRYPTO 2023*. Ed. by Helena Handschuh and Anna Lysyanskaya. Cham: Springer Nature Switzerland, 2023, pp. 782–804. ISBN: 978-3-031-38554-4.

[LS93] M. J. J. Lennon and P. J. Smith. "LUC: A new public key system". In: *Ninth IFIP Symposium on Computer Security*. Ed. by E. G. Douglas. Elsevier Science Publishers, 1993, pp. 103–117.

[MN81] W. B. Müller and W. Nöbauer. "Some remarks on public-key cryptosystems". In: *Studia Sci. Math. Hungar.* 16 (1981), pp. 71–76.

[PB91] C. P. and David M. Bressoud. "Factorization and Primality Testing." In: *Mathematics of Computation* 56.193 (1991), p. 400. ISSN: 00255718.

[Pie19] Krzysztof Pietrzak. "Simple Verifiable Delay Functions". In: *ITCS*. Vol. 124. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019, 60:1–60:15.

[Rab83] Michael O. Rabin. "Transaction Protection by Beacons". In: *J. Comput. Syst. Sci.* 27.2 (1983), pp. 256–267.

[Rie85] Hans Riesel. *Prime numbers and computer methods for factorization*. Vol. 57. Progress in Mathematics. Birkhäuser, 1985.

[Sch+21] Philipp Schindler et al. "RandRunner: Distributed Randomness from Trapdoor VDFs with Strong Uniqueness". In: *28th Annual Network and Distributed System Security Symposium, NDSS 2021, virtually, February 21-25, 2021*. The Internet Society, 2021.

[Sha19] Barak Shani. "A note on isogeny-based hybrid verifiable delay functions". In: *IACR Cryptology ePrint Archive* 2019 (2019), p. 205.

[Wes20] Benjamin Wesolowski. "Efficient Verifiable Delay Functions". In: *J. Cryptol.* 33.4 (2020), pp. 2113–2147. URL: https://doi.org/10.1007/s00145-020-09364-x.

[Wil82] Hugh C. Williams. "A $p+1$ method of factoring". In: *Math. Comput.* 39.159 (1982), pp. 225–234.