简明 zkSNARKs 分类手册（v1.1)

Kurt Pan

Cryptoland

Abstract. 通过本次作业对 zk-SNARKs 相关定义概念和相关工作进行简洁的整理和区分，希望在完善后能作为一个参考手册帮助 zk 研究者和从业者。

- 2023.06.20 v1.1
- 2022.07.21 v1.0

Keywords: zk-SNARKs

Table of Contents

1 总论

已知有五条路径可以构造一个论证系统，都是由一个信息论安全的协议和密码学方案一起组合而成：

1. 基于交互式证明系统 IP 的（GKR 协议）
2. 基于多证明者交互式证明系统 MIP 的
3. 基于常数轮多项式交互式谕示证明 PIOP 的（包括 MPC-in-the-Head）
4. 基于线性概率可检验证明系统 LPCP 的。
5. 基于承诺并证明技术的

已知有三条路径来构造一个多项式承诺方案：

1. 基于 IOP 和 Merkle 哈希组合：FRI [BBHR17] /Ligero [AHIV17] /Brakedown [GLS+21]

2. 基于透明 Σ 协议，离散对数假设：Hyrax [WTS+18], Bulletproof [BBB+18], Dory
3. 基于配对和可信设置：KZG [KZG10]

绝大多数 SNARK 设计三步走方法：

1. 设计一个对电路可满足性或 R1CS 可满足性问题的公开抛币 PIOP
2. 用多项式承诺方案替换 PIOP 中的每一条消息 h_i，得到一个公开抛币的交互式简洁论证系统
3. 用 Fiat-Shamir 去掉交互性

2 关键组件的定义

信息论证明系统

- **IP**：交互式证明系统
- **MIP** [BGKW88]：多证明者交互式证明系统，多个证明者分别和一个验证者进行交互式证明。
- **PCP** [AS98]：概率可验证证明系统，验证者查询访问证明者的消息字符串。
- **IOP** [BCS16]：交互式谕示证明系统，结合了 IP 和 PCP 的特点，验证者和证明者同时具有交互和查询访问消息。

理论模型

- **CRS**：所有参与方可以访问一个公共的参考串
- **ROM**：随机预言模型
- **AGM**：代数群模型
- **Fiat-Shamir 范式**：将任何公开抛币交互式论证系统转换为一个对同样语言的非交互论证系统。该转换在对常数轮协议，在随机预言模型中，是可靠的。[BR93]

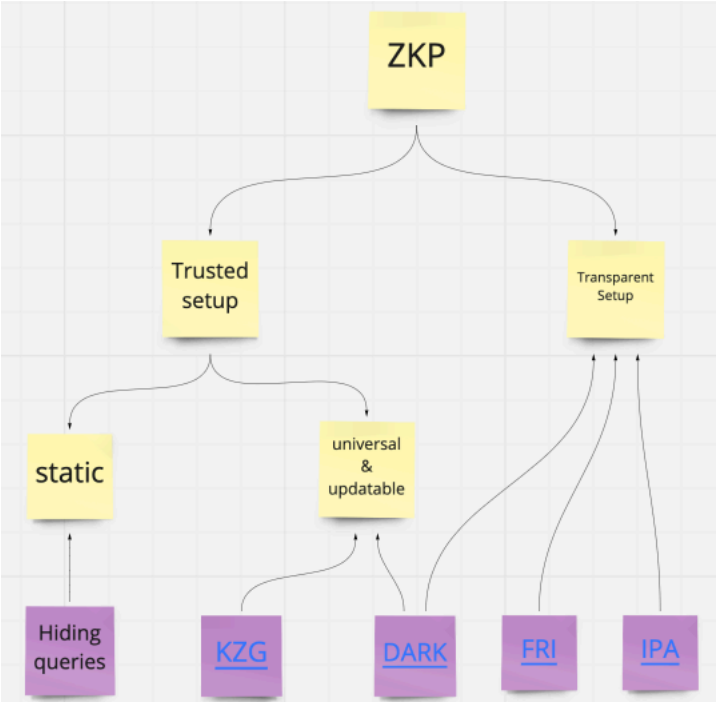
zk-SNARKs

- **零知识**：验证者除了陈述正确性不能获得任何其他知识增长
- **简洁**：验证者运行时间比进行计算更短
- **非交互**：协议通信只有证明者向验证者发送的一条消息
- **论证系统**：证明系统其中可靠性只对恶意的多项式时间证明者成立（依赖密码学假设）
- **知识证明**：证明者确实拥有知识

多项式承诺方案

多项式承诺方案是输入对象为多项式的密码学承诺方案，满足隐藏性和绑定性。此外还满足部分打开部分点处的求值，不用全部打开整个多项式。常见多项式承诺方案有如下分类：

- KZG [KZG10] 基于配对椭圆曲线，结构化公共字符串
- IPA [BBB+18] 内积论证系统
- FRI [BBHR17] 快速里德所罗门交互式谕示证明系统



可信设置

- 计算特定可信设置：SRS 中包含 power-of-tau，以及表示电路连线模式或 R1CS 矩阵项的多项式求值的编码。
- 通用（universal）可信设置：一个 SRS 可以对任意 R1CS/电路可满足性实例使用，直到某个固定的大小界。只包含 power-of-tau，电路无关。
- 可更新（updatable）可信设置：SRS 可以在任意时间由任何参与方更新，只要至少有一个参与方诚实，证明就不可以被伪造。

算术化和中间表示

- 算术化：将通用陈述或问题转换为可验证的方程组的过程。
- 算术电路：线路为有限域中的元素，门为加法门和乘法门的电路
- **R1CS/QAP**：一种用一系列算术方程编码算术电路的方法

3 组合为不同方案: SNARKS 菜谱

- Virgo [ZXZS20] = IP + FRI
- Hyrax [WTS+18] = IP + IPA
- Libra [XZZ+19] = IP + KZG
- Spartan [Set20], Quarks [SL20] = MIP + IPA
- Brakedown, Shockwave [GLS+21] = MIP + Brakedown/Ligero-承诺
- Aurora [BCR+19], Fractal [COS20], Redshift [KPV19], STARK[BBHR19], Plonky2 [1] = PIOP + FRI
- Ligero [AHIV17] = PIOP + Ligero-承诺
- Ligero++ [BFH+20]= PIOP + Ligero-承诺 + FRI
- Sonic [MBKM19] , Marlin [CHM+20] , PlonK [GWC19] = PIOP + KZG
- Halo 2 [2] = Plonk PIOP + IPA
- Pinocchio [PHGR13], Groth16 [Gro16] = LPCP + 配对

[1] https://github.com/mir-protocol/plonky2/blob/main/plonky2/plonky2.pdf
[2] https://zcash.github.io/halo2/

4 各个因素的权衡

4.1 常数证明大小

有两条路径可以达到「证明大小只包含常数个群元素」：常数轮 PIOP+KZG 多项式承诺，LPCP+ 双线性配对。前者的代表 Marlin 证明大小大约是后者代表 Groth16（只要 3 个群元素）的 4 倍，Plonk 的证明大小大约是 Groth16 的 2.5 倍。所以在「最小证明大小」这个目标上后者完胜。

这两条路径都有如下两个缺点都用了 SRS，都需要可信设置。但前者使用 SRS 的缺点没有后者严重：前者的 SRS 是通用的且可更新的，后者的 SRS 是计算特定的。证明者计算开销都很大。证明者要进行多个 FFT/多项式除法/多指数运算，时间和空间开销都很大且不易并行化和分布化。

4.2 透明性 Transparency

除了上述两条为了极小化证明大小的路径，只要不使用基于 KZG 的多项式承诺，其他的路径构造出的 SNARK 都是透明的。使用 URS 而非 SRS。

4.3 后量子安全

IOP 是可能后量子的,所以基于 IOP 的多项式承诺方案(FRI/Ligero/Brakedown)(包括 MPC-in-the-Head 方法构造的 IOP）都是后量子的，另外两类多项式承诺方案因为依赖离散对数问题的困难性非后量子的。

4.4 域选择的限制

比如关于加密和签名方案的证明，很多加密和签名方案是定义在非 FFT 友好的有限域上的椭圆曲线群中的，如果 SNARKs 系统证明者需要进行 FFT, 则就不能用。

来自可靠性保证 域大小必须足够大以确保达到想要的可靠性安全级别。

来自零散对数或 KZG 多项式承诺 使用基于零散对数或 KZG 多项式承诺的 SNARKs，以及 LPCP+ 配对的方法，都必须使用和多项式承诺定义的群阶数相等的域。

来自 FFT 来自 IOP 和线性 PCP 的 SNARKs 要求证明者在大向量上进行 FFT 运算，而不同的有限域对 FFT 算法的支持具有不同的复杂度。部分常数轮 PIOP [CHM+20; GWC19] 要求有限域具有特定乘法或加法子群。

来自程序-电路转译 在一些基于 IOP 的 SNARKS 中（比如 STARKs [BBHR19]），从计算机程序（RAMs) 到电路或其他中间表示的转换过程只适用于特征为 2 的域。

4.5 不同操作的相对效率

证明者的瓶颈可能是在域上 FFT，可能是群操作（多指数），也可能是构造 Merkle 树中的哈希求值。哪个操作成为瓶颈也依赖于要处理的计算的大小。

4.6 中间表示（IR）

除了上述的算术电路和 R1CS，还可以支持更通用的中间表示。比如扩展门，支持大于 2 的门的扇入，从而产生更快的证明者。比如“类 Plonk 算术化”指对 Plonk [GWC19] 的修改以支持一种电路门的度数可以达到 9 的中间表示。

References

[AHIV17] Scott Ames et al. “Ligero: Lightweight Sublinear Arguments Without a Trusted Setup”. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (2017) (Cited on pages 2, 5).

[AS98] Sanjeev Arora and Shmuel Safra. “Probabilistic checking of proofs: a new characterization of NP”. In: *J. ACM* 45 (1998), pp. 70–122 (Cited on page 3).

[BBB+18] Benedikt Bünz et al. “Bulletproofs: Short Proofs for Confidential Transactions and More”. In: *2018 IEEE Symposium on Security and Privacy (SP)* (2018), pp. 315–334 (Cited on pages 3, 4).

[BBHR17] Eli Ben-Sasson et al. “Fast Reed-Solomon Interactive Oracle Proofs of Proximity”. In: *Electron. Colloquium Comput. Complex.* 2017 (Cited on pages 2, 4).

[BBHR19] Eli Ben-Sasson et al. “Scalable Zero Knowledge with No Trusted Setup”. In: *Advances in Cryptology – CRYPTO 2019*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Cham: Springer International Publishing, 2019, pp. 701–732. ISBN: 978-3-030-26954-8 (Cited on pages 5, 7).

[BCR+19] Eli Ben-Sasson et al. “Aurora: Transparent Succinct Arguments for R1CS”. In: *Advances in Cryptology – EUROCRYPT 2019*. Ed. by Yuval Ishai and Vincent Rijmen. Cham: Springer International Publishing, 2019, pp. 103–128. ISBN: 978-3-030-17653-2 (Cited on page 5).

[BCS16] Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner. “Interactive Oracle Proofs”. In: *TCC*. 2016 (Cited on page 3).

[BFH+20] Rishabh Bhadauria et al. “Ligero++: A New Optimized Sublinear IOP”. In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (2020) (Cited on page 5).

[BGKW88] Michael Ben-Or et al. “Multi-prover interactive proofs: how to remove intractability assumptions”. In: *STOC ’88*. 1988 (Cited on page 3).

[BR93] Mihir Bellare and Phillip Rogaway. “Random oracles are practical: a paradigm for designing efficient protocols”. In: *CCS ’93*. 1993 (Cited on page 3).

[CHM+20] Alessandro Chiesa et al. “Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS”. In: *Advances in Cryptology – EUROCRYPT 2020*. Ed. by Anne Canteaut and Yuval Ishai. Cham: Springer International Publishing, 2020, pp. 738–768. ISBN: 978-3-030-45721-1 (Cited on pages 5, 7).

[COS20] Alessandro Chiesa, Dev Ojha, and Nicholas Spooner. "Fractal: Post-quantum and Transparent Recursive Proofs from Holography". In: *Advances in Cryptology – EUROCRYPT 2020*. Ed. by Anne Canteaut and Yuval Ishai. Cham: Springer International Publishing, 2020, pp. 769–793. ISBN: 978-3-030-45721-1 (Cited on page 5).

[GLS+21] Alexander Golovnev et al. "Brakedown: Linear-time and post-quantum SNARKs for R1CS". In: *IACR Cryptol. ePrint Arch.* 2021 (2021), p. 1043 (Cited on pages 2, 5).

[Gro16] Jens Groth. "On the Size of Pairing-Based Non-interactive Arguments". In: *Advances in Cryptology – EUROCRYPT 2016*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 305–326. ISBN: 978-3-662-49896-5 (Cited on page 5).

[GWC19] Ariel Gabizon, Zachary J. Williamson, and Oana-Madalina Ciobotaru. "PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge". In: *IACR Cryptol. ePrint Arch.* 2019 (2019), p. 953 (Cited on pages 5, 7).

[KPV19] Assimakis A. Kattis, Konstantin Panarin, and Alexander Yu. Vlasov. "RedShift: Transparent SNARKs from List Polynomial Commitment IOPs". In: *IACR Cryptol. ePrint Arch.* 2019 (2019), p. 1400 (Cited on page 5).

[KZG10] Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg. "Constant-Size Commitments to Polynomials and Their Applications". In: *ASIACRYPT*. 2010 (Cited on pages 3, 4).

[MBKM19] Mary Maller et al. "Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updatable Structured Reference Strings". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (2019) (Cited on page 5).

[PHGR13] Bryan Parno et al. “Pinocchio: Nearly Practical Verifiable Computation”. In: *2013 IEEE Symposium on Security and Privacy* (2013), pp. 238–252 (Cited on page 5).

[Set20] Srinath Setty. “Spartan: Efficient and General-Purpose zkSNARKs Without Trusted Setup”. In: *Advances in Cryptology – CRYPTO 2020*. Ed. by Daniele Micciancio and Thomas Ristenpart. Cham: Springer International Publishing, 2020, pp. 704–737. ISBN: 978-3-030-56877-1 (Cited on page 5).

[SL20] Srinath T. V. Setty and Jonathan Lee. “Quarks: Quadruple-efficient transparent zkSNARKs”. In: *IACR Cryptol. ePrint Arch.* 2020 (2020), p. 1275 (Cited on page 5).

[WTS+18] Riad S. Wahby et al. “Doubly-Efficient zkSNARKs Without Trusted Setup”. In: *2018 IEEE Symposium on Security and Privacy (SP)* (2018), pp. 926–943 (Cited on pages 3, 5).

[XZZ+19] Tiacheng Xie et al. “Libra: Succinct Zero-Knowledge Proofs with Optimal Prover Computation”. In: *Advances in Cryptology – CRYPTO 2019*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Cham: Springer International Publishing, 2019, pp. 733–764. ISBN: 978-3-030-26954-8 (Cited on page 5).

[ZXZS20] Jiaheng Zhang et al. “Transparent Polynomial Delegation and Its Applications to Zero Knowledge Proof”. In: *2020 IEEE Symposium on Security and Privacy (SP)* (2020), pp. 859–876 (Cited on page 5).