ZkpComRef 2021

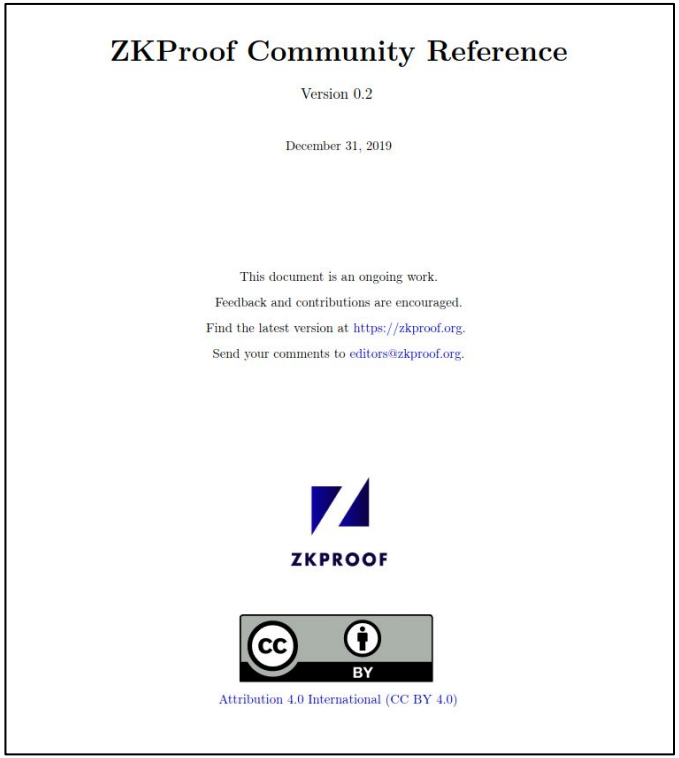
Daniel Benarroch (QEDIT), Luís Brandão (NIST/Strativia), Eran Tromer (Columbia & TAU)
editors@zkproof.org

Presented at the 4th ZKProof Workshop — Home Edition
April 26, 2021

Outline

1. Intro to the ZkpComRef
2. Current State and Process
3. Writathon!

1. Have you looked at the ZKProof Community Reference before today?



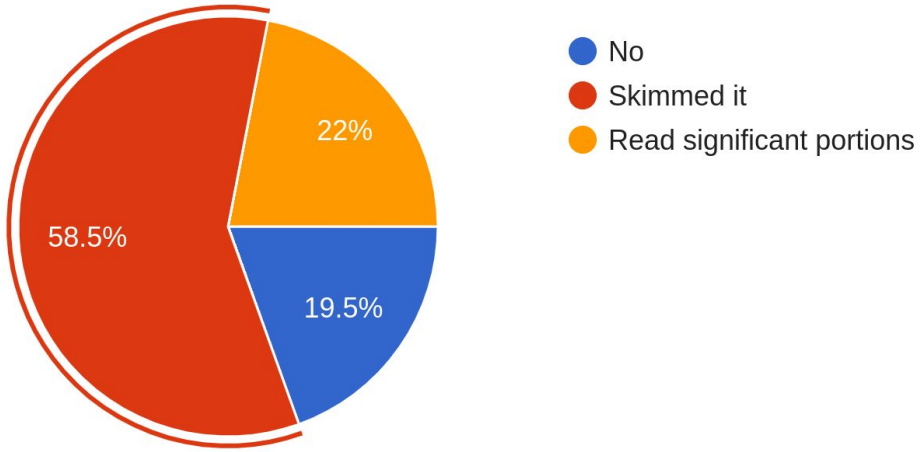
ZKProof Community Reference

Version 0.2

December 31, 2019

This document is an ongoing work.
Feedback and contributions are encouraged.
Find the latest version at https://zkproof.org.
Send your comments to editors@zkproof.org.

ZKPROOF



41 first participants by 18 May 2020

1. Intro to the ZkpComRef

What is the ZkpComRef?

1. A Collaborative document to serve as a reference for the development of zero-knowledge proof technology
2. Covers theoretical aspects such as definitions and security, as well as practical aspects of implementations and applications
3. A live document to be continuously updated by the community

IT IS NOT A STANDARD DOCUMENT!

All she wanted was

- ***Educational*** tutorial to enter the field
- Agreed-upon ***guidelines*** built around an inclusive ***community***
- ***Dynamic*** document to ensure up-to-date and able to update

Who are you?

CONSUMER

- ***Learner:*** onboarding, usage in applications, start research
- ***Mentor:*** professor / manager suggest material w/t guidance
- ***Evaluator:*** check a system is secure and state-of-the-art

CONTRIBUTOR

- ***Innovator:*** integrate own research / experience
- ***Sage:*** convey knowledge, recomm. & warnings

The Upbringing

ZKProof Standards
Security Track Proceedings

ZKProof Standards
Implementation Track Proceedings

ZKProof Standards
Applications Track Proceedings

1 August 2018 + subsequent revisions

This document is an ongoing work in progress.
Feedback and contributions are encouraged.

Track Chairs:
Daniel Benarroch, Ran Canetti and Andrew Miller

Track Participants:
Shashank Agrawal, Tony Arcieri, Vipin Bharathan, Josh Cincinnati, Joshua Daniel, Anuj Das Gupta, Angelo De Caro, Michael Dixon, Maria Dubovitskaya, Nathan George, Brett Hemenway Falk, Hugo Krawczyk, Jason Law, Anna Lysyanskaya, Zaki Manian, Eduardo Morais, Neha Narula, Gavin Pacini, Jonathan Rouach, Kartheek Solipuram, Mayank Varia, Douglas Wikstrom and Aviv Zohar

ZKProof Community Reference

Version 0.1

(Draft 2019-04-11)

ZKProof Community Reference

Version 0.2

December 31, 2019

This document is an ongoing work.
Feedback and contributions are encouraged.
Find the latest version at https://zkproof.org.
Send your comments to editors@zkproof.org.

ZKPROOF

Over 60 contributors

1. Jens Groth
2. Yael Kalai
3. Muthu Venkitasubramaniam
4. Nir Bitansky
5. Ran Canetti
6. Henry Corrigan-Gibbs
7. Shafi Goldwasser
8. Charanjit Jutla
9. Yuval Ishai
10. Rafail Ostrovsky
11. Omer Paneth
12. Tal Rabin
13. Maryana Raykova
14. Ron Rothblum
15. Alessandra Scafuro
16. Eran Tromer
17. Douglas Wikström
18. Sean Bowe
19. Kobi Gurkan
20. Benedikt Bünz
21. Konstantinos Chalkias
22. Daniel Genkin
23. Jack Grigg
24. Daira Hopwood
25. Andrew Poelstra
26. abhi shelat
27. Madars Virza
28. Riad S. Wahby
29. Pieter Wuille
30. Shashank Agrawal
31. Tony Arcieri
32. Vipin Bharathan
33. Josh Cincinnati
34. Joshua Daniel
35. Anuj Das Gupta
36. Angelo De Caro
37. Michael Dixon
38. Maria Dubovitskaya
39. Nathan George
40. Brett Hemenway Falk
41. Hugo Krawczyk
42. Jason Law
43. Anna Lysyanskaya
44. Zaki Manian
45. Eduardo Morais
46. NehaNarula
47. Gavin Pacini
48. Jonathan Rouach
49. Kartheek Solipuram
50. Daniel Benarroch
51. Andrew Miller
52. Aviv Zohar
53. Luís Brandão
54. Angela Robinson
55. Rene Peralta
56. Justin Thaler
57. Jason Law
58. Mayank Varia
59. Ivan Visconti
60. Yupeng Zhang
61. Yu Hang
62. ???

ARE YOU NEXT?

TODAY YOU WILL HAVE THE CHANCE!

CURRENT EDITORS

- Luís Brandão
- Eran Tromer
- Daniel Benarroch

1. What do you think about the ZkpComRef?

1. Love It! And have recommended it to many others
2. I checked it out a few times
3. Meh, not so useful
4. Do not have the time for that
5. There is a lot to improve
6. Other?

WRITE YOUR ANSWER ON THE CHAT --- GO!

2. Current State and Process

ZkpComRef: Current State and Process

Daniel Benarroch[1], Luís Brandão[2], Eran Tromer[3]

[1]QEDIT, [2]NIST/Strativia, [3]Columbia & TAU

editors@zkproof.org

Presented at the 4th ZKProof Workshop
April 26, 2021 @ Online

[2] Contractor at NIST. Opinions expressed here are from the speaker and are not to be construed as official views of NIST.

Outline

Resources

ZkpComRef

ZKProof
Community
Rerefence

Link

GitHub

Code
Issues
Diff

Link

Calls

Comments
and
Contributions

Link

Overleaf

Ongoing
development
(paradigms ...)

Link

Webpage

Forum
and
Resources

Link

Workshop

Writathon
(various
topics)

Link

Contact the editors for any questions/comments: editors@zkproof.org

ZkpComRef: why might you care?

If it's not:

- A paper with the newest technique
- A standard on its own
- A finished document

ZkpComRef: why might you care?

If it's not:

- A paper with the newest technique
- A standard on its own
- A finished document

It has a potential utility:

- **in bringing a wide community together in a joint effort**
  - Settle on terminology, interfaces, motivating applications, ...
- **to non-researchers and non-implementers:**
  - Useful for privacy policy, vendors/consumers, standardization bodies, ...
  - Its collaborative nature evinces the relevance of ZKP tech ...

ZkpComRef: why might you care?

If it's not:

- A paper with the newest technique
- A standard on its own
- A finished document

It has a potential utility:

- **in bringing a wide community together in a joint effort**
  - Settle on terminology, interfaces, motivating applications, ...
- **to non-researchers and non-implementers:**
  - Useful for privacy policy, vendors/consumers, standardization bodies, ...
  - Its collaborative nature evinces the relevance of ZKP tech ...

ZkpComRef: why might you care?

If it's not:

- A paper with the newest technique
- A standard on its own
- A finished document

It has a potential utility:

- **in bringing a wide community together in a joint effort**
  - Settle on terminology, interfaces, motivating applications, ...
- **to non-researchers and non-implementers:**
  - Useful for privacy policy, vendors/consumers, standardization bodies, ...
  - Its collaborative nature evinces the relevance of ZKP tech ...

The above is a vision, to be increasingly achieved. We are all invited!

2020–2021 Editorial Process

2020:

- May: 3rd ZKProof workshop: motivate review
- By July: Received 7 sets of comments
- Aug-14: Call for Contributions issued ... new GitHub issues 29–50
- 2020 was a tough year ... no further contributions received

2021: (next slides)

- **January:** New editorial approach: Editors pick a topic (**"Paradigms"**), select/prepare material, then ask for focused contributions.
- **April:** 4th workshop: new motivation / Writathon idea
- **December:** (tentative) ZkpComRef 0.3

Observation 1: poor intuition

Problem: ZkpComRef 0.2 gives poor intuition on how to achieve actual ZKPs

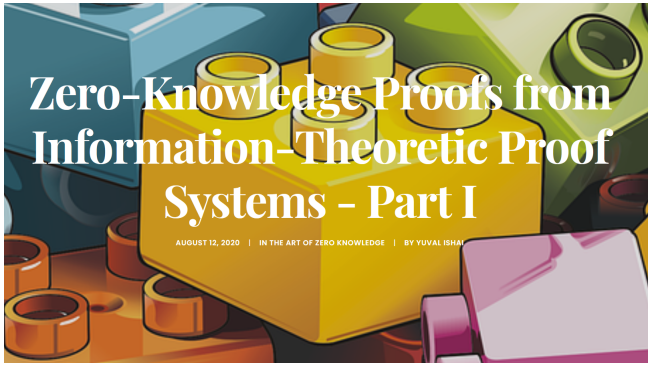
Observation 1: poor intuition

Problem: ZkpComRef 0.2 gives poor intuition on how to achieve actual ZKPs

Editorial solution:

- **1. Choose external text with substantive content covering various paradigms**

  Blogposts from Y.Ishai: ZKPs from IT proof systems:



https://zkproof.org/2020/08/12/information-theoretic-proof-systems

- **2. Distill and organize content for new ZkpComRef sections:**

  Current Sec. 2.1 of ZkpComRef 0.2 will be replaced by four new sections.

  Background; IT proof systems; Crypto compilers; Concrete ZKP schemes.

- **3. Then ask focused contributions/reviews per component**
  Asked recently (April) ... contributions will continue.

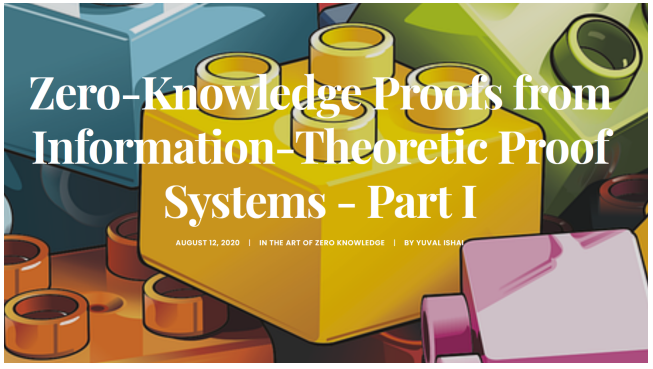
Observation 1: poor intuition

Problem: ZkpComRef 0.2 gives poor intuition on how to achieve actual ZKPs

Editorial solution:

- **1. Choose external text with substantive content covering various paradigms**

  Blogposts from Y.Ishai: ZKPs from IT proof systems:



https://zkproof.org/2020/08/12/information-theoretic-proof-systems

- **2. Distill and organize content for new ZkpComRef sections:**

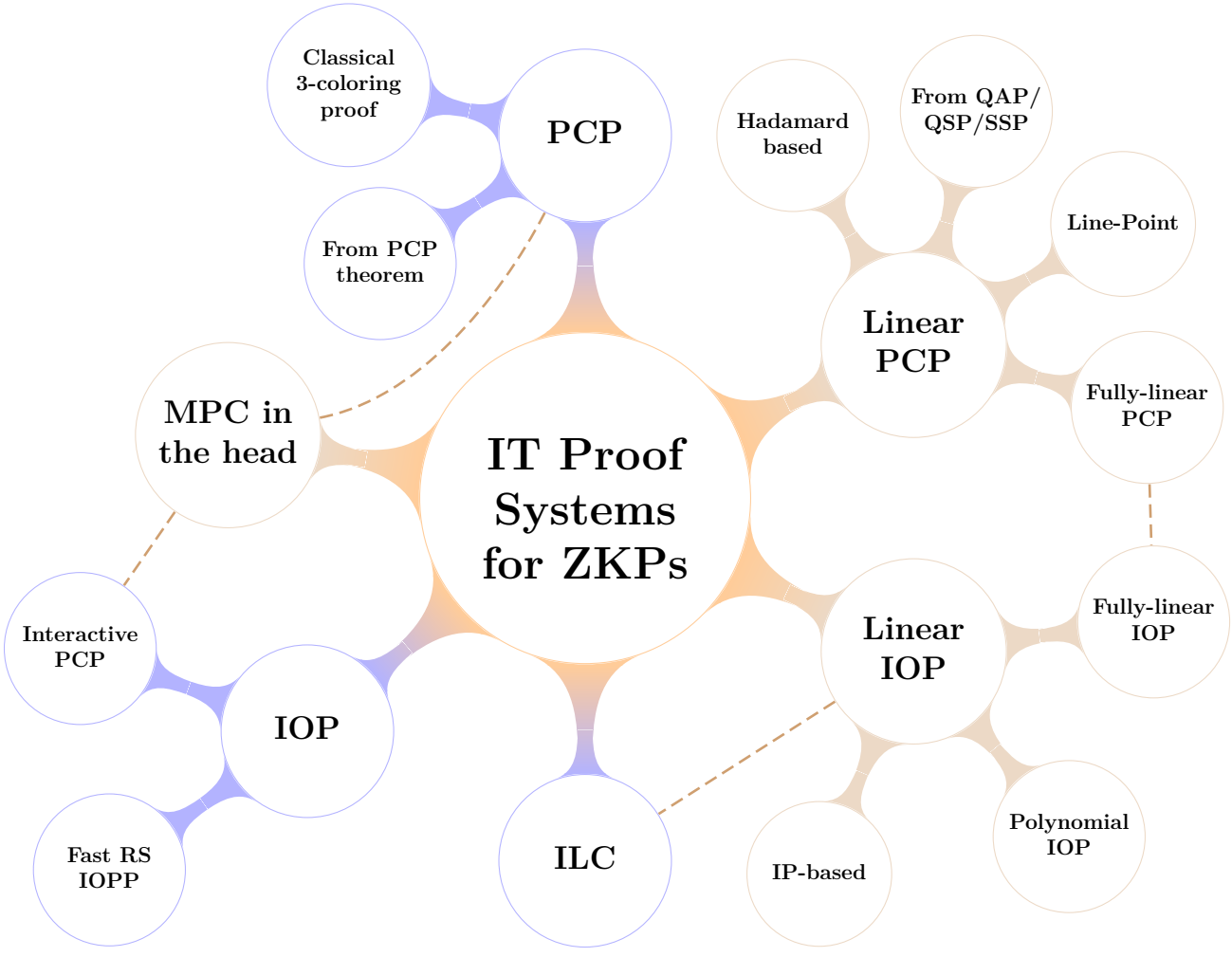
  Current Sec. 2.1 of ZkpComRef 0.2 will be replaced by four new sections.

  Background; IT proof systems; Crypto compilers; Concrete ZKP schemes.

- **3. Then ask focused contributions/reviews per component**
  Asked recently (April) ... contributions will continue.

Conclusion: current motion assures we'll have an improved version 0.3

Paradigms Chapter — mindmap of IT proof systems

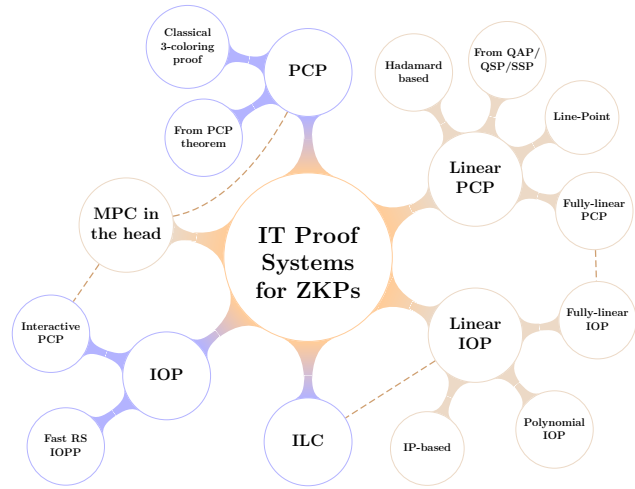


Fast RS IOPP (aka FRI): Fast Reed-Solomon IOP of Proximity. **ILC**: Ideal Linear Commitment. **IOP**: Interactive Oracle Proof. **IP**: Interactive Proof. **IT**: Information Theoretic. **MPC**: [Secure] Multi-Party Computation. **PCP**: Probabilistic Checkable Proof. **QAP**: Quadratic Arithmetic Program. **QSP**: Quadratic Span Program. **SSP**: Square Span Program. **ZKP**: Zero-Knowledge Proof.

Ack: thanks to Yuval Ishai for continued feedback during the design of this mindmap

Paradigms Chapter – Ongoing work

- One section on IT: each node will have its own subsection
- One section on crypto compilers (CC)
- One section on concrete ZKP schemes. Each may refer refer to an IT/CC pair.
- What if you don't find your favorite IT/CC/Scheme?
  Contact editors@zkproof.org



Work in progress (collaborative overleaf) ... various contributors contacted.

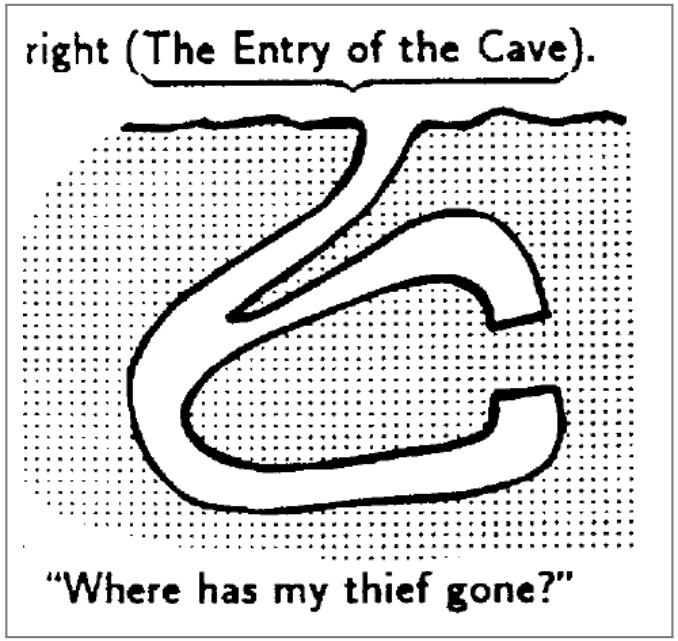
Observation 2: low visual appeal

Problem: Low ratio image/text. Bad for large portion of intended audience that will not read this as a typical paper.

Observation 2: low visual appeal

Problem: Low ratio image/text. Bad for large portion of intended audience that will not read this as a typical paper.

Envisioned solution: Add 20–40 diagrams, illustrations, figures. This will facilitate visual intuition, and will ease the reading.



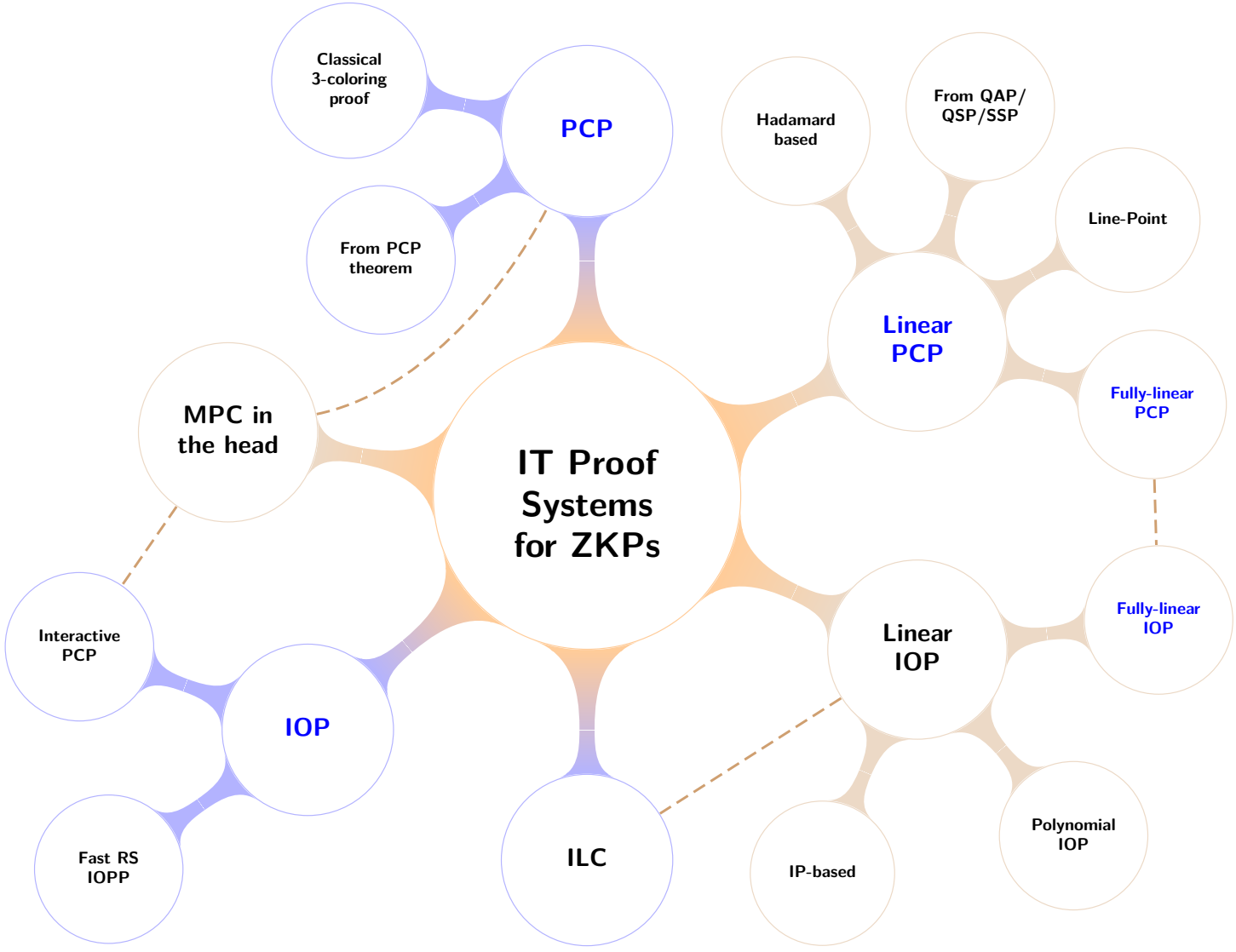
How to Explain Zero-Knowledge Protocols to Your Children
Quisquater et al. (1989) DOI:10.1007/0-387-34805-0_60

Visual intuition: 1 image = 1000 words

Natural source: presentation slides

Many topics: IT proof systems, crypto compilers, gadgets, security games, applications, deployment case-studies, examples, ...

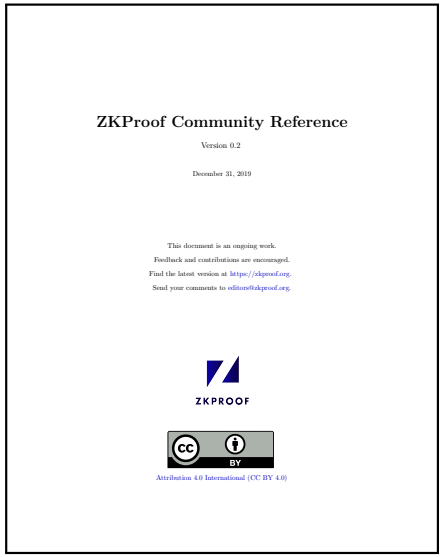
Interactive images



Upcoming version 0.3

Aimed to the end 2021, with material based on:

- Developing writeup about **paradigms** (IT/CC).
- Contributions initiated in the **Writathon**:
  - **Diagrams/illustrations**, e.g., from nice slides
  - Examples of **implementations**
  - Examples of **applications**
  - Succinct comparison of concrete ZKP **protocols**
  - ...



https://docs.zkproof.org/pages/reference/reference.pdf

Many identified needs will be deferred to a later version (0.4^{+})

- But we welcome review comments/contributions at any time

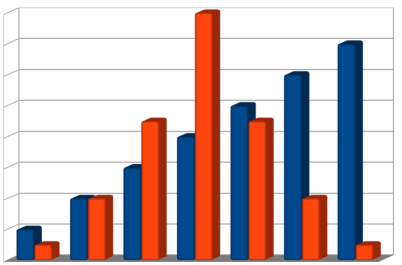
Other topics (for subsequent phases)

Many other topics for contributions:

- Table of gadgets
- Security definitions (e.g., game for extractability)
- Varied notions (e.g., witness indistinguishability)
- Recommendations (and/or requirements?)
- Benchmarking
- Thorough editorial revision of the text

#	Gadget name
G1	Commitment
G2	Signatures
G3	Encryption
G4	Distributed decryption
G5	Random function

...



More details: Call for contributions (2020-Aug-24) and GitHub Issues.

Advancing the ZkpComRef

- There is **value** in aiming for a community/collaborative output:
  - Reference material for a wide audience
  - A basis for seeking initial consensus (future standards?)
- There are inherent **challenges**:
  - Prevent overgrowth, ensure uniform style, filter pertinent content.
  - Contributors' hesitation on stepping on someone else's text or area.
- **Updated editorial approach:**
  - Focused requests after structure prepared by editors;
  - Writathon to produce support material/suggestions;
  - Still open to spontaneous contributions.
- **ZkpComRef:** it's a vision ... being iteratively built.
- Your collaboration is welcome and needed.

3. The Writathon!

Writathon breakout rooms

- Concrete schemes
  Add short descriptions of numerous concrete ZKP schemes
- Applications
  Describe additional high-level applications of ZKPs
- Deployment case studies
  Brief case studies describing real-world deployments + lessons learned
- SNARK-friendly primitives
  Briefly survey ZK-optimized cryptographic primitives
- Interfaces, formats and interoperability
  Expanding on APIs, File Formats and Constraint-System Interoperability
- Diagrams and illustrations
  Create/suggest visual illustrations

Zcash Community Reference writathon

6 parallel breakout rooms:

- 15:50–16:35 UTC Session 1
- 17:10–18:00 UTC Session 2
- 18:00 Summary presentations at end. Choose your rep.

Documents at hackmd.io/@workshop4/links under “breakout”.

Choose your room, open the docs and edit away!
Be considerate and coordinate verbally. Feel free to switch.

7th+8th breakout room:

- Interactive Arkworks ZK tutorial by Pratyush Mishra
  (also on GitHub)