

ZKProof Community Reference

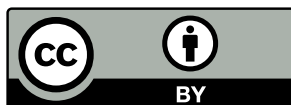
Version 0.1.x (towards 0.2)

(Draft 2019-10-26)

This document is an ongoing work.

Feedback and contributions are encouraged.

editors@zkproof.org



Attribution 4.0 International
(CC BY 4.0)

7 **Abstract**

8 **To appear**

E1: D1.5

9 Editorial note

10 To appear

E2: D1.6

11 Change-log

- 12 • Version 0 — 2018-08-01: Baseline documents available at ZKProof.org, with the proceedings
13 of the 1st ZKProof Workshop, and subsequent major contributions. The original documents
14 corresponded to the three tracks of the Workshop: security, applications, implementation.
15 The contributors to those initial documents were as follows:
 - 16 – ZKProof Standards Applications Implementation Proceedings
 - 17 * **Track chairs:** Sean Bowe, Kobi Gurkan, Eran Tromer
 - 18 * **Track participants:** Benedikt Bünz, Konstantinos Chalkias, Daniel Genkin, Jack
19 Grigg, Daira Hopwood, Jason Law, Andrew Poelstra, abhi shelat, Muthu Venkita-
20 subramaniam, Madars Virza, Riad S. Wahby, Pieter Wuille
 - 21 – ZKProof Standards Applications Track Proceedings
 - 22 * **Track chairs:** Daniel Benarroch, Ran Canetti and Andrew Miller
 - 23 * **Track participants:** Shashank Agrawal, Tony Arcieri, Vipin Bharathan, Josh
24 Cincinnati, Joshua Daniel, Anuj Das Gupta, Angelo De Caro, Michael Dixon, Maria
25 Dubovitskaya, Nathan George, Brett Hemenway Falk, Hugo Krawczyk, Jason Law,
26 Anna Lysyanskaya, Zaki Manian, Eduardo Morais, Neha Narula, Gavin Pacini,
27 Jonathan Rouach, Kartheek Solipuram, Mayank Varia, Douglas Wikstrom and Aviv
28 Zohar
 - 29 – ZKProof Standards Applications Implementation Proceedings
 - 30 * **Track chairs:** Jens Groth, Yael Kalai, Muthu Venkitasubramaniam
 - 31 * **Track participants:** Nir Bitansky, Ran Canetti, Henry Corrigan-Gibbs, Shafi
32 Goldwasser, Charanjit Jutla, Yuval Ishai, Rafail Ostrovsky, Omer Paneth, Tal Ra-
33 bin, Maryana Raykova, Ron Rothblum, Alessandra Scafuro, Eran Tromer, Douglas
34 Wikström
- 35 • Version 0.1 — 2019-04-11: Initial compilation of the baseline documents into a single PDF
36 document. Ported all the write-ups to LaTeX code; merged the six original documents;
37 numerous editorial adjustments for easier indexation of content and consistent style.
- 38 • Version 0.2 — To appear: explain changes at high level

39 External resources

- 40 • ZKProof repository: <https://github.com/zkpstandard/>
- 41 • ZKProof repository for file formats: https://github.com/zkpstandard/file_formats
- 42 • ZKProof documents on Security, Applications and Implementation Tracks on
43 <https://zkproof.org/documents.html>
- 44 • zkp.science - a curated and annotated list of references
- 45 • Zcon0 ZKProof Workshop breakout notes: https://zkproof.org/zcon0_notes.pdf

46 Acknowledgments

47 To appear: name contributors, scribes, ZKProof committees, workshop participants, ..., workshop E3: D1.7
48 sponsors

Expectations on disclosure and licensing of intellectual property

E4: D6.1

ZKProof is an open initiative that seeks to promote the secure and interoperable use of zero-knowledge proofs. To foster open development and wide adoption, it is valuable to promote technologies with open-source implementations, unencumbered by royalty-bearing patents. However, some useful technologies may fall within the scope of patent claims. Since ZKProof seeks to represent the technology, research and community in an inclusive manner, it is valuable to set expectations about the disclosure of intellectual property and the handling of patent claims.

The members of the ZKProof community are hereby strongly encouraged to provide information on known patent claims potentially applicable to the guidance, requirements, recommendations, proposals and examples provided in ZKProof documentation, including by disclosing known pending patent applications or any relevant unexpired patent. Particularly, such disclosure is promptly required from the patent holders, or those acting on their behalf, as a condition for providing content contributions to the “Community Reference” and to “Proposals” submitted to ZKProof for consideration by the community. Furthermore, any technology that is promoted in said ZKProof documentation and that falls within patent claims should be made available under licensing terms that are reasonable, and demonstrably free of unfair discrimination, preferably allowing free open-source implementations.

The ZKProof documentation will be updated based on received disclosures about pertinent patent claims. Please email information to editors@zkproof.org.

Contents

Table of Contents

Abstract	i
Editorial note	ii
Acknowledgments	iii
Intellectual Property	iv
Contents	v
Executive summary	vii
Charter and code of conduct	ix
1 Security	1
1.1 Introduction	1
1.2 Terminology	2
1.3 Specifying Statements for ZK	3
1.4 ZKPs of knowledge vs. ZKPs of membership	5
1.5 Syntax	7
1.6 Definition and Properties	9
1.7 Assumptions	14
1.8 Efficiency	15
2 Construction paradigms	19
2.1 Taxonomy of Constructions	19
2.2 Interactivity	22
2.3 Several construction paradigms	27
3 Implementation	29
3.1 Overview	29
3.2 Backends: Cryptographic System Implementations	29
3.3 Frontends: Constraint-System Construction	30
3.4 APIs and File Formats	31
3.5 Benchmarks	35
3.6 Correctness and Trust	38
3.7 Extended Constraint-System Interoperability	43
3.8 Future goals	45
4 Applications	47
4.1 Introduction and Motivation	47
4.2 Notation and Definitions	48
4.3 Previous works	48
4.4 Gadgets within predicates	48
4.5 Identity framework	49
4.6 Asset Transfer	64
4.7 Regulation Compliance	70

106	4.8 Conclusions	73
107	References	75
108	A Acronyms and glossary	79
109	A.1 Acronyms	79
110	A.2 Glossary	79
111	B Summaries of proposals	81
112	Table of comments and contributions v0.1 \rightarrow 0.2	83
113	List of Contributions	84
114	Structural changes	85
115	New or adapted content	86
116	List of Tables	
117	Table 1.1: Example scenarios for zero-knowledge proofs	3
118	Table 2.1: Different types of PCPs	20
119	Table 3.1: APIs and interfaces by types of universality and preprocessing	32
120	Table 4.1: List of gadgets	49
121	Table 4.2: Commitment gadget	50
122	Table 4.3: Signature gadget	51
123	Table 4.4: Encryption gadget	51
124	Table 4.5: Distributed-decryption gadget	52
125	Table 4.6: Random-function gadget	52
126	Table 4.7: Set-membership gadget	53
127	Table 4.8: Mix-net gadget	53
128	Table 4.9: Generic-computation gadget	54
129	Table 4.10: Functionalities vs. privacy and robustness requirements	58
130	List of Figures	
131	Figure 3.1: Abstract parties and objects in a NIZK	32

Executive summary

E5: D2.1

Zero-knowledge proofs (ZKPs) are an important privacy-enhancing tool from cryptography. They preserve confidentiality of data, while proving the veracity of statements about the data. They can also be used to prove knowledge of such data without having to disclose it. ZKPs can have a positive impact in industries, agencies, and for personal use, by allowing privacy-preserving applications where designated private data can be made useful to third parties, despite not being disclosed to them. The development of this “ZKProof Community Reference” is a step towards enabling wider adoption of interoperable ZKP technology, possibly preceding the establishment of future standards.

ZKPs were developed by the academic community in the 1980s, and have seen tremendous improvements since then. They are now of practical feasibility in multiple domains of interest to the industry, and to a large community of developers and researchers. This document aims to be a community-built reference for understanding and aiding the development of ZKP systems in a secure, practical and interoperable manner. It is not a substitution for research papers, technical books, or standards. It is intended to serve as a reference handbook of introductory concepts, basic techniques, implementation suggestions and application use-cases. This aims to serve the broader community, particularly those interested in understanding ZKP systems, making an impact in their advancement, and using related products.

ZKP systems involve at least two parties: a prover and a verifier. The goal of the prover is to convince the verifier that a statement is true, without revealing any additional information. For example, suppose the prover holds a birth certificate digitally signed by an authority. In order to access some service, the prover may have to prove being at least 18 years old, that is, that there exists a birth certificate, tied to the identify of the prover and digitally signed by a trusted certification authority, stating a birthdate consistent with the age claim. A ZKP allows this, without the prover having to reveal the birthdate.

This document describes important aspects of the current state of the art in ZKP security, implementation, and applications. There are several use-cases and applications where ZKPs can add value. However, this requires benchmarking implementations under several metrics, evaluating tradeoffs between security and efficiency, and developing a basis for interoperability. The security of a proof system is paramount for the system users, but system efficiency is also essential for user experience.

The “Security” chapter introduces the theory and terminology of ZKP systems. A ZKP system can be described with three components: **setup**, **prove**, **verify**. The **setup**, which can be implemented with various techniques, determines the initial state of the prover and the verifier, including private and common elements. The **prove** and **verify** components are the algorithms followed by the prover and verifier, respectively, possibly in an interactive manner. These algorithms are defined so as to ensure three main security requirements: completeness, soundness, and zero-knowledge.

Completeness requires that if both **prove** and **verify** are correct, and if the statement is true, then at the end of the interaction the prover is convinced of this fact. Soundness requires that not even a malicious prover can convince the verifier of a false statement. Zero knowledge requires that even a malicious verifier cannot extract any information beyond the truthfulness of the given statement.

The “Implementation” chapter focuses on devising a framework for the implementation of ZKPs, which is important for interoperability. One important aspect to consider upfront is the represen-

tation of statements. In a ZKP protocol, the statement needs to be converted into a mathematical object. For example, in the case of proving that an age is at least 18, the statement is equivalent to proving that the private birthdate Y_1 - M_1 - D_1 (year-month-day) satisfies a relation with the present date Y_2 - M_2 - D_2 , namely that their distance is greater than or equal to 18 years. This simple example can be represented as a disjunction of conditions: $Y_2 > Y_1 + 18$, or $Y_2 = Y_1 + 18 \wedge M_2 > M_1$, or $Y_2 = Y_1 + 18 \wedge M_2 = M_1 \wedge D_2 \geq D_1$. An actual conversion suitable for ZKPs, namely for more complex statements, can pose an implementation challenge. There are nonetheless various techniques that enable converting a statement into a mathematical object, such as a circuit. This document gives special attention to representations based on a Rank-1 constraint system (R1CS) and quadratic arithmetic programs (QAP), which are adopted by several ZKP solutions in use today. Also, the document gives special emphasis to implementations of non-interactive proof systems.

The privacy enhancement offered by ZKPs can be applied to a wide range of scenarios. The “Applications” chapter presents two use-cases that can benefit from ZKP systems: identity framework and asset transfer. In a privacy-preserving identity framework, one can for example prove useful personal attributes, such as age and state of residency, without revealing more detailed personal data such as birthdate and address. In an asset-transfer setting, financial institutions that facilitate transactions usually require knowing the identities of the sender and receiver, and the asset type and amount. ZKP systems enable a privacy-preserving variant where the transaction is performed between anonymous parties, while at the same time ensuring they and their assets satisfy regulatory requirements. These use cases, as well as a wide range of many other conceivable privacy-preserving applications, can be enabled by a common set of tools, or gadgets, for example including commitments, signatures, encryption and circuits.

The interplay between security concepts and implementation guidelines must be balanced to enable the development of secure, practical, and interoperable ZKP applications. Solutions provided by ZKP technology must be ensured by careful security practices and realistic assumptions. This document aims to summarize security properties and implementation techniques that help achieve these goals.

Charter and code of conduct



ZKProof charter

Boston, May 10th and 11th 2018

The goal of the ZKProof Standardization effort is to advance the use of Zero Knowledge Proof technology by bringing together experts from industry and academia. To further the goals of the effort, we set the following guiding principles:

- The initiative is aimed at producing documents that are open for all and free to use.
 - As an open initiative, all content issued from the ZKProof Standards Workshop is under Creative Commons Attribution 4.0 International license.
- We seek to represent all aspects of the technology, research and community in an inclusive manner.
- Our goal is to reach consensus where possible, and to properly represent conflicting views where consensus was not reached.
- As an open initiative, we wish to communicate our results to the industry, the media and to the general public, with a goal of making all voices in the event heard.
 - Participants in the event might be photographed or filmed.
 - We encourage you to tweet, blog and share with the hashtag #ZKProof. Our official twitter handle is @ZKProof.

For further information, please refer to contact@zkproof.org

219 ZKProof code of conduct

220

Boston, May 10th and 11th 2018

221 All participants, speakers and sponsors of the ZKProof Standard Workshop shall adhere to the
222 following code of conduct to ensure a safe and productive environment for everybody¹:


223 At the workshop, you agree to:

- 224 • Respect the boundaries of other attendees.
- 225 • Respect the opinions of other attendees even if you are not in agreement with them.
- 226 • Avoid aggressively pushing your own services, products or causes.
- 227 • Respect confidentiality requests by participants.
- 228 • Look out for one another.

229 These behaviors don't belong at the workshop:

- 230 • Invasion of privacy
- 231 • Being disruptive, drinking excessively, stalking, following or threatening anyone.
- 232 • Abuse of power (including abuses related to position, wealth, race or gender).
- 233 • Homophobia, racism or behavior that discriminates against a group or class of people.
- 234 • Sexual harassment of any kind, including unwelcome sexual attention and inappropriate
- 235 physical contact.

236 For further information, please refer to contact@zkproof.org

¹This code of conduct is adapted from that of TEDx. 

Chapter 1. Security

1.1 Introduction

1.1.1 What is a zero-knowledge proof?

A zero-knowledge proof (ZKP) makes it possible to prove a statement is true while preserving confidentiality of secret information. This makes sense when the veracity of the statement is not obvious on its own, but the prover knows relevant secret information (or has a skill, like super-computation ability) that enables producing a proof. The notion of secrecy is used here in the sense of prohibited leakage, but a ZKP makes sense even if the ‘secret’ (or any portion of it) is known apriori by the verifier(s).

E6: D3.1

E7: D3.3

There are numerous uses of ZKPs, useful for proving claims about confidential data, such as:

E8: D3.4

1. adulthood, without revealing the birth date;
2. solvency (not being bankrupt), without showing the portfolio composition;
3. ownership of an asset, without revealing or linking to past transactions;
4. validity of a chessboard configuration, without revealing the legal sequence of chess moves;
5. correctness (demonstrability) of a theorem, without revealing its mathematical proof.

Some of these claims (commonly known by the prover and verifier, and here described as informal *statements*) require a substrate (called *instance*, also commonly known by the prover and verifier) to support an association with the confidential information (called *witness*, known by the prover and to not be leaked during the proof process). For example, the proof of solvency (the statement) may rely on encrypted and certified bank records (the instance), and with the verifier knowing the corresponding decryption key and plaintext (the witness) as secrets that cannot be leaked. Table 1.1 in Section 1.2 differentiates these elements across several examples. In concrete instantiations, the exemplified ZKPs are specified by means of a more formal *statement of knowledge* of a witness.

E9: D3.5

A zero-knowledge proof system is a specification of how a prover and verifier can interact for the prover to convince the verifier that the statement is true. The proof system must be complete, sound and zero-knowledge.

- **Complete:** If the statement is true and both prover and verifier follow the protocol; the verifier will accept.
- **Sound:** If the statement is false, and the verifier follows the protocol; the verifier will not be convinced.
- **Zero-knowledge:** If the statement is true and the prover follows the protocol; the verifier will not learn any confidential information from the interaction with the prover but the fact the statement is true.

E10: D3.6

Proofs vs. arguments. The theory of ZKPs distinguishes between *proofs* and *arguments*, as related to the computational power of the prover and verifier. *Proofs* need to be sound even against computationally unbounded provers, whereas *arguments* only need to preserve soundness against computationally bounded provers (often defined as probabilistic polynomial time algorithms). For simplicity, “proof” is used hereafter to designate both *proofs* and *arguments*, although there are theoretical circumstances where the distinction can be relevant.

1.1.2 Requirements for a zero-knowledge proof system specification

A full proof system specification MUST include:

1. Precise specification of the type of statements the proof system is designed to handle
2. Construction including algorithms used by the prover and verifier
3. If applicable, description of setup the prover and verifier use
4. Precise definitions of security the proof system is intended to provide
5. A security analysis that proves the zero-knowledge proof system satisfies the security definitions and a full list of any unproven assumptions that underpin security


Efficiency claims about a zero-knowledge proof system should include all relevant performance parameters for the intended usage. Efficiency claims must be reported fairly and accurately, and if a comparison is made to other zero-knowledge proof systems a best effort must be made to compare apples to apples.

The remainder of the document will outline common approaches to specifying a zero-knowledge proof system, outline some construction paradigms, and give guidelines for how to present efficiency claims.

1.2 Terminology

Instance: Input commonly known to both prover (P) and verifier (V), and used to support the statement of what needs to be proven. This common input may either be local to the prover-verifier interaction, or public in the sense of being known by external parties. Notation: x . (Some scientific articles use “instance” and “statement” interchangeably, but we distinguish between the two.)

Witness: Private input to the prover. Others may or may not know something about the witness. Notation: w .

Relation:  Specification of relationship between instances and witness. A relation can be viewed as a set of permissible pairs (instance, witness). Notation: R .

Language: Set of instances that appear as a permissible pair in R . Notation: L .

Statement: Defined by instance and relation. Claims the instance has a witness in the relation

(which is either true or false). Notation: $x \in L$.

Security parameter: Positive integer indicating the desired security level (e.g. 128 or 256) where higher security parameter means greater security. In most constructions, distinction is made between computational security parameter and statistical security parameter. Notation: k (computational) or s (statistical).

Setup: The inputs given to the prover and to the verifier, apart from the instance x and the witness w . The setup of each party can be decomposed into a private component (“PrivateSetup_P” or “PrivateSetup_V”, respectively not known to the other party) and a common component “Common-Setup = CRS” (known by both parties), where CRS denotes a “common reference string” (required by some zero-knowledge proof systems). Notation: $\text{setup}_P = (\text{PrivateSetup}_P, \text{CRS})$ and $\text{setup}_V = (\text{PrivateSetup}_V, \text{CRS})$.

For simplicity, some parameters of the setup are left implicit (possibly inside the CRS), such as the security parameters, and auxiliary elements defining the language and relation. See more details in Section 1.5.3. While the witness (w) and the instance (x) could be assumed as elements of the setup of a concrete ZKP protocol execution, they are often distinguished in their own category. In practice, the term “Setup” is often used with respect to the setup of a proof system that can then be instantiated for multiple executions with varying instances (x) and witnesses (w).

Table 1.1 exemplifies at a high level a differentiation between the *statement*, the *instance* and the *witness* elements for the initial examples mentioned in Section 1.1.1.

Table 1.1: Example scenarios for zero-knowledge proofs

#	Elements Scenarios	Statement being proven	Instance used as substrate	Witness treated as confidential
1	Legal age for purchase	I am an adult	Tamper-resistant identification chip	Birthdate and personal data (signed by a CA)
2	Hedge fund solvency	We are not bankrupt	Encrypted & certified bank records	Portfolio data and decryption key
3	Asset transfer	I own this <asset>	A blockchain or other commitments	Sequence of transactions (and secret keys that establish ownership)
4	Chessboard configuration	This <configuration> can be reached	(The rules of Chess)	A sequence of valid chess moves
5	Theorem validity	This <expression> is a theorem	(A set of axioms, and the logical rules of inference)	A sequence of logical implications

Legend: CA = certification authority

1.3 Specifying Statements for ZK

This document considers types of statements defined by a relation R between instances x and witnesses w . The relation R specifies which pairs (x, w) are considered related to each other, and which are not related to each other. The relation defines a matching language L consisting of instances x that have a witness w in R .

A *statement* is either a *membership* claim of the form “ $x \in L$ ”, or a *knowledge* claim of the form “In the scope of relation R , I know a witness for instance x .” For some cases, the *knowledge* and *membership* types of statement can be informally considered interchangeable, but formally there are technical reasons to distinguish between the two notions. In particular, there are scenarios where a statement of knowledge cannot be converted into a statement of membership, and vice-versa (as exemplified in Section 1.4). The examples in this document are often based on statements of knowledge.

The relation R can for instance be specified as a program (e.g. in C or Java), which given inputs x and w decides to accept, meaning $(x, w) \in R$, or reject, meaning w is not a witness to $x \in L$. Examples of such specifications of the relation are detailed in the [Applications track](#). In the academic literature, relations are often specified either as random access memory (RAM) programs or through Boolean and arithmetic circuits, which we describe below.

Circuits: A circuit is a directed acyclic graph (DAG) comprised of nodes and labels for nodes, which satisfy the following constraints:

- Nodes with in-degree 0 are referred to as the **input nodes** and are labeled with some constant (e.g., 0, 1, ...) or with input variable names (e.g., v_1, v_2, \dots)
- There is a single node with out-degree 0 that is referred to as the **output node**.
- Internal nodes are referred to as **gate nodes** and describe a computation performed at the node.

Parameters. Depending on the application, various parameters may be important, for instance the number of gates in the circuit, the number of instance variables n_x , the number of witness variables n_w , the circuit depth, or the circuit width.

Boolean Circuit satisfiability. The relation R has instances of the form $x = (C, v_1, \dots, v_{n_x})$ and witnesses $w = (w_1, \dots, w_{n_w})$. For (x, w) to be in the relation, C must be a circuit with fan-in 2 gate nodes that are labeled with Boolean operations, e.g., XOR or AND, v_1, \dots, v_{n_x} must specify truth values for some of the input nodes, and w_1, \dots, w_{n_w} must specify truth values for the remaining input variables, such that when evaluating the circuit the output node becomes 1 (true).

Arithmetic Circuit satisfiability. The relation has instances of the form $x = (F, C, v_1, \dots, v_{n_x})$ and witnesses $w = (w_1, \dots, w_{n_w})$. For (x, w) to be in the relation, F must be a finite field (e.g., integers modulo a prime p), C must be a circuit with gate nodes that are labeled with field operations, i.e., addition or multiplication, v_1, \dots, v_{n_x} must specify field elements for some of the input nodes, and w_1, \dots, w_{n_w} must specify field elements for the remaining input variables, such that when evaluating the circuit the output node becomes 1.

Special purpose relations: Circuit satisfiability is a complete problem within the non-deterministic polynomial (NP) class, i.e., it is NP-complete, but a relation does not have to be that. Examples of statements that appear in cryptographic usage include that a committed value falls in a certain range $[A; B]$ or belongs to a set S , that a ciphertext has plaintext 0 or that two ciphertexts encrypt the same value, that the prover has a secret key associated with a set of public verification keys for a signature scheme, etc.

Setup-dependent relations: Sometimes it is convenient to let the relation R take an additional input setup_R , i.e., let the relation contain triples (setup_R, x, w) . The input setup_R can be used to

specify persistent information, e.g., for arithmetic circuit satisfiability maybe the same finite field and circuit is used many times, so we let $\text{setup}_R = (F, C)$ and $x = (v_1, \dots, v_{n_x})$. The input setup_R can also be used to capture trusted input the relation does not check, e.g., a trusted Rivest–Shamir–Adleman (RSA) modulus.

1.4 ZKPs of knowledge vs. ZKPs of membership

The theory of ZKPs distinguishes between two types of proofs, based on the type of statement (and also on the type of security properties — see Sections 1.6.2 and 1.6.3):

- A ZKP of knowledge (ZKPoK) proves the veracity of a *statement of knowledge*, i.e., it proves knowledge of private data that supports the statement, without revealing the former.
- A ZKP of membership proves the veracity of a *statement of membership*, i.e., that the *instance* belongs to the *language*, as related to the *statement*, but without revealing information that could not have been produced by a computationally bounded verifier.

The *statements* exemplified in Table 1.1 were expressed as facts, but each of them corresponds to a knowledge of a secret witness that supports the statement in the context of the instance. For example, the statement “I am an adult” in scenario 1 can be interpreted as an abbreviation of “I know a birthdate that is consistent with adulthood today, and I also know a certificate (signed by some trusted certification authority) associating the birthdate with my identity.”

The first three use-cases (adulthood, solvency and asset ownership) in Table 1.1 have instances with some kind of protection, such as physical access control, encryption, signature and/or commitments. The “chessboard configuration” and the “theorem validity” use-cases are different in that their instances do not contain any cryptographic support or physical protection. Each of those two statements can be seen as a claim of membership, in the sense of claiming that the expression/configuration belongs respectively to the language of valid chessboard configurations (i.e., reachable by a sequence of moves), or the language of theorems (i.e., of provable expressions). At the same time, a further specification of the statement can be expressed as a claim of knowledge of a sequence of legal moves or a sequence of logical implications.

1.4.1 Example: ZKP of knowledge of a discrete logarithm (discrete-log)

Let p be a large prime (e.g., with 4096 bits) of the form $p = 2q + 1$, where q is also a prime. Let g be a generator of the group $\mathbb{Z}_p^* = \{1, \dots, p - 1\} = \{g^i : i = 1, \dots, p - 1\}$ under multiplication modulo p . Assume that it is computationally infeasible to compute discrete-logs in this group, and that the primality of p and q has been verified by both prover and verifier. Let w be a secret element (the witness) known by the prover, and let $x = g^w \pmod{p}$ be the instance known by both the prover and verifier, corresponding to the following statement by the prover: “I know the discrete-log (base g) of the instance (x) , modulo p ” (in other words: “I know a secret exponent that raises the generator (g) into the instance (x) , modulo p ”). Consider now the relation $R = \{(x, w) : g^w = x \pmod{p}\}$. In this case, the corresponding language $L = \{x : \exists w : (x, w) \in R\}$ is simply the set $\mathbb{Z}_p^* = \{1, 2, \dots, p - 1\}$, for which membership is self-evident (without any knowledge of w). In that sense, a proof of membership

E15: D3.9

E16: D3.10

does not make sense (or can be trivially considered accomplished with even an empty bit string). Conversely, whether or not the prover knows a witness is a non-trivial matter, since the current publicly-known state of the art does not provide a way to compute discrete-logs in time polynomial in the size of the prime modulus (except if with a quantum computer). In summary, this is a case where a ZKPoK makes sense but a ZKP of membership does not.

1.4.2 Example: ZKP of knowledge of a hash pre-image

Consider a cryptographic hash function $H : \{0, 1\}^{512} \rightarrow \{0, 1\}^{256}$, restricted to binary inputs of length 512. For many (possibly all) 256-bit instances in the co-domain $\{0, 1\}^{256}$ of H there are many pre-images in $\{0, 1\}^{512}$. Let w be a witness (hash pre-image) known by the prover (and unpredictable to the verifier), for some instance $x = H(w)$ known by the verifier. Since a cryptographic hash function is one-way, it makes sense to give a ZKPoK of a pre-image, corresponding to proving knowledge of a witness in the relation $R = \{(x, w) : H(w) = x\}$. Such proof also constitutes directly a proof of membership, i.e., that the instance x does in fact belong to the co-domain of H . However, interestingly, membership in the co-domain of H is a problem that might or might not make sense depending on the known properties of the hash function H . If H is known to have as a co-domain the set of all bit-strings of length 256, then membership is self-evident. Otherwise it may be that an element x uniformly selected from the range $\{0, 1\}^{256}$ is in fact not in the co-domain of H , case in which a proof of membership makes sense.

E17: D3.11

1.4.3 Example: ZKP of membership for graph non-isomorphism

In the theoretical context of provers with super-polynomial computation ability (e.g., unbounded), one can conceive a proof of membership without the notion of witness. Therefore, in this case the dual notion of a ZKP of knowledge does not apply. A classical example uses the language of pairs of non-isomorphic graphs, for which the proof is about convincing a verifier that two graphs are not isomorphic. The classical example uses an interactive proof that does not follow from a witness, but rather from a super-ability, by the prover, in deciding isomorphism between graphs. The verifier challenges the prover to detect which of the two graphs is isomorphic to a random permutation of one of the two original graphs. If the prover decides correctly enough times, without ever failing, then the verifier becomes convinced of the non-isomorphism.

E18: D3.12

This document is not focused on settings that require provers with super-polynomial ability (in an asymptotic setting). However, this notion of ZKP of membership without witness still makes sense in other conceivable applications, namely within a concrete setting (as opposed to asymptotic). This may apply in contexts of proofs of work, or when provers are “supercomputers” or quantum computers, possibly interacting with verifiers with significantly less computational resources. Another conceivable setting is when a verifier wants to confirm whether the prover is able to solve a mathematical problem, for which the prover claims to have found a first efficient technique, e.g., the ability to decide fast about graph isomorphism.

1.5 Syntax

A proof system (for a relation R defining a language L) is a protocol between a prover and a verifier sending messages to each other. The prover and verifier are defined by two algorithms, which we call Prove and Verify. The algorithms Prove and Verify may be probabilistic and may keep internal state between invocations.

1.5.1 $\text{Prove}(state, m) \rightarrow (state, p)$

The Prove algorithm in a given state receiving message m , updates its state and returns a message p .

- The initial state of Prove must include an instance x and a witness w . The initial state may also include additional setup information setup_P , e.g., $state = (\text{setup}_P, x, w)$.
- If receiving a special initialization message $m = \mathbf{start}$ when first invoked it means the prover is to initiate the protocol.
- If Prove outputs a special error symbol $p = \mathbf{error}$, it must output **error** on all subsequent calls as well.

1.5.2 $\text{Verify}(state, p) \rightarrow (state, m)$

The Verify algorithm in a given state receiving message p , updates its state and returns a message m .

- The initial state of Verify must include an instance x .
- The initial state of Verify may also include additional setup information setup_V , e.g., $state = (\text{setup}_V, x)$.
- If receiving a special initialization message $p = \mathbf{start}$, it means the verifier is to initiate the protocol.
- If Verify outputs a special symbol $m = \mathbf{accept}$, it means the verifier accepts the proof of the statement $x \in L$. In this case, Verify must return $m = \mathbf{accept}$ on all future calls.
- If Verify outputs a special symbol $m = \mathbf{reject}$, it means the verifier rejects the proof of the statement $x \in L$. In this case, Verify must return $m = \mathbf{reject}$ on all future calls.

The setup information setup_P and setup_V can take many forms. A common example found in the cryptographic literature is that $\text{setup}_P = \text{setup}_V = k$, where k is a security parameter indicating the desired security level of the proof system. It is also conceivable that setup_P and setup_V contain descriptions of particular choices of primitives to instantiate the proof system with, e.g., to use the SHA-256 hash function or to use a particular elliptic curve. The setup information may also be generated by a probabilistic process, e.g., it may be that setup_P and setup_V include a common reference string, or in the case of designated verifier proofs that setup_P and setup_V are correlated in a particular way. When we want to specifically refer to this process, we use a probabilistic setup algorithm **Setup**.

1.5.3 Setup(parameters) (setup_R, setup_P, setup_V, auxiliary output)

The setup algorithm may take input parameters, which could for instance be computational or statistical security parameters indicating the desired security level of the proof system, or size parameters specifying the size of the statements the proof system should work for, or choices of cryptographic primitives e.g. the SHA-256 hash function or an elliptic curve.

- The setup algorithm returns an input setup_R for the relation the proof system is for. An important special case is where the setup_R is just the empty string, i.e., the relation is independent of any setup.
- The setup algorithm returns setup_P for the prover and setup_V for the verifier.
- There may potentially be additional auxiliary outputs.
- If the inputs are malformed or any error occurs, the Setup algorithm may output an error symbol.

Some examples of possible setups.

- NIZK proof system for 3SAT in the uniform reference string model based on trapdoor permutations
 - setup_R = n , where n specifies the maximal number of clauses
 - setup_P = setup_V = uniform random string of length $N = \text{size}(n, k)$ for some function $\text{size}(n, k)$ of n and security parameter k
- Groth-Sahai proofs for pairing-product equations
 - setup_R = description of bilinear group defining the language
 - setup_P = setup_V = common reference string including description of the bilinear group in setup_R plus additional group elements
- SNARK for QAP such as e.g. Pinocchio
 - setup_R = QAP specification including finite field F and polynomials
 - setup_P = setup_V = common reference string including a bilinear group defined over the same finite field and some group elements

The prover and verifier do not use the same group elements in the common reference string. For efficiency reasons, one may let setup_P be the subset of the group elements the prover uses, and setup_V another (much smaller) subset of group elements the verifier uses.
- Cramer-Shoup hash proof systems
 - setup_R = specifies finite cyclic group of prime order
 - setup_P = the cyclic group and some group elements
 - setup_V = the cyclic group and some discrete logarithms

It depends on the concrete setting how Setup runs. In some cases, a trusted third party runs an algorithm to generate the setup. In other cases, Setup may be a multi-party computation offering resilience against a subset of corrupt and dishonest parties (and the auxiliary output may represent side-information the adversarial parties learn from the MPC protocol). Yet, another possibility is to work in the plain model, where the setup does nothing but copy a security parameter, e.g., setup_P = setup_V = k .

There are variations of proof systems, e.g., multi-prover proof systems and commit-and-prove systems; this document only covers standard systems.

Common reference string: If the setup information is public and known to everybody, we say the proof system is in the common reference string model. The setup may for instance specify $\text{setup}_R = \text{setup}_P = \text{setup}_V$, which we then refer to as a common reference string CRS.

Non-interactive proof systems: A proof system is non-interactive if the interaction consists of a single message from the prover to the verifier. After receiving the prover's message p (called a proof), the verifier then returns accept or reject.

Public verifiability vs designated verifier: If setup_V is public information (e.g. in the CRS model) known to multiple parties in a non-interactive proof system, then they can all verify a proof p . In this case, the proof is transferable, the prover only needs to create it once after which it can be copied and transferred to many verifiers. If on the other hand, setup_V is private we refer to it as a designated verifier proof system.

Public coin: In an interactive proof system, we say it is public coin if the verifier's messages are uniformly random and independent of the prover's messages.

1.6 Definition and Properties

A proof system (Setup, Prove, Verify) for a relation R must be complete and sound. It may have additional desirable security properties such as being a proof of knowledge or being zero knowledge.

1.6.1 Completeness

Intuitively, a proof system is complete if an honest prover with a valid witness w for a statement $x \in L$ can convince an honest verifier that the statement is true. A full specification of a proof system **must** include a precise definition of completeness that captures this intuition. We give an example of a definition below for a proof system where the prover initiates.

Consider a completeness attacker **Adversary** in the following experiment.

1. Run **Setup**(parameters) \rightarrow ($\text{setup}_R, \text{setup}_P, \text{setup}_V, \text{aux}$)
 2. Let the adversary choose a worst case instance and witness:
 $\text{Adversary}(\text{parameters}, \text{setup}_R, \text{setup}_P, \text{setup}_V, \text{aux}) \rightarrow (x, w)$
 3. Run the interaction between Prove and Verify until the prover returns **error** or the verifier accepts or rejects. Let result be the outcome, with the convention that $\text{result} = \text{error}$ if the protocol does not terminate. $\langle \text{Prove}(\text{setup}_P, x, w, \text{start}) ; \text{Verify}(\text{setup}_V, x) \rangle \rightarrow \text{result}$
- **Adversary** wins if $(\text{setup}_R, x, w) \in R$ and result is not **accept**.

We define the adversary's advantage as a function of parameters to be $\text{Advantage}(\text{parameters}) = \Pr[\text{Adversary wins}]$

A proof system for R running on parameters is complete if nobody ever constructs an efficient adversary with significant advantage.

It depends on the application what is an efficient adversary (computing equipment, running time, memory consumption, usage lifetime, incentives, etc.) and how large an advantage can be tolerated. Special strong cases include statistical completeness (aka unconditional completeness) where the winning probability is small for any adversary, and perfect completeness, where for any adversary the advantage is exactly 0.

1.6.2 Soundness

Intuitively, a proof system is sound if a cheating prover has little or no chance of convincing an honest verifier that a false statement is true. A full specification of a proof system must include a precise definition of soundness that captures this intuition. We give an example of a definition below.

Consider a soundness attacker **Adversary** in the following experiment.

1. Run **Setup**($parameters$) \rightarrow ($setup_R, setup_P, setup_V, aux$)
 2. Let the (stateful) adversary choose an instance
 $\mathbf{Adversary}(parameters, setup_R, setup_P, setup_V, aux) \rightarrow x$
 3. Let the adversary interact with the verifier and $result$ be the verifier's output (letting $result = \mathbf{reject}$ if the protocol does not terminate). $\langle \mathbf{Adversary} ; \mathbf{Verify}(setup_V, x) \rangle \rightarrow result$
- **Adversary** wins if $(setup_R, x) \notin L$ and result is **accept**.

We define the adversary's advantage as a function of parameters to be

$$\text{Advantage}(parameters) = \Pr[\mathbf{Adversary} \text{ wins}]$$

A proof system for R running on parameters is sound if nobody ever constructs an efficient adversary with significant advantage.

It depends on the application what is considered an efficient adversary (computing equipment, running time, memory consumption, usage lifetime, etc.) and how large an advantage can be tolerated. Special strong notions of soundness includes statistical soundness (aka unconditional soundness) where any adversary has small chance of winning, and perfect soundness, where for any adversary the advantage is exactly 0.

1.6.3 Proof of knowledge

Intuitively, a proof system is a proof of knowledge if it is not just sound, but that the ability to convince an honest verifier implies that the prover must "know" a witness. To "know" a witness can be defined as it being possible to extract a witness from a successful prover. If a proof system is claimed to be a proof of knowledge, then the full specification **must** include a precise definition of knowledge soundness that captures this intuition, but we do not define proofs of knowledge here.

[[**To improve.** Consider adding, in a future version of this document draft, a game definition for the extractor required by the formal notion of proof of knowledge. This security property also arises naturally in the ideal/real simulation paradigm, in the context of an *ideal ZKP functionality* that, in the ideal world, receives the witness directly from the prover.]]

1.6.4 Zero knowledge

Intuitively, a proof system is zero knowledge if it does not leak any information about the prover's witness beyond what the attacker may already know about the witness from other sources. Zero knowledge is defined through the specification of an efficient simulator that can generate kosher looking proofs without access to the witness. If a proof system is claimed to be zero knowledge, then the full specification **MUST** include a precise definition of zero knowledge that captures this intuition. We give an example of a definition below.

A proof system is zero knowledge if the designers provide additional efficient algorithms **SimSetup**, **SimProve** such that realistic attackers have small advantage in the game below. Let **Adversary** be an attacker in the following experiment:

1. Choose a bit uniformly at random $0,1 \rightarrow b$
 2. If $b = 0$ run **Setup**(parameters) $\rightarrow (\text{setup}_R, \text{setup}_P, \text{setup}_V, \text{aux})$
 3. Else if $b = 1$ run **SimSetup**(parameters) $\rightarrow (\text{setup}_R, \text{setup}_P, \text{setup}_V, \text{aux}, \text{trapdoor})$
 4. Let the (stateful) adversary choose an instance and witness
Adversary(parameters, $\text{setup}_R, \text{setup}_P, \text{setup}_V, \text{aux}$) $\rightarrow (x, w)$
 5. If $(\text{setup}_R, x, w) \notin R$ return $\text{guess} = 0$
 6. If $b = 0$ let the adversary interact with the prover and output a guess (letting $\text{guess} = 0$ if the protocol does not terminate). $\langle \text{Prove}(\text{setup}_P, x, w) ; \text{Adversary} \rangle \rightarrow \text{guess}$
 7. Else if $b = 1$ let the adversary interact with a simulated prover and output a guess (letting $\text{guess} = 0$ if the protocol does not terminate)
 $\langle \text{SimProve}(\text{setup}_P, x, \text{trapdoor}) ; \text{Adversary} \rangle \rightarrow \text{guess}$
- **Adversary** wins if $\text{guess} = b$

We define the adversary's advantage as a function of parameters to be

$$\text{Advantage}(\text{parameters}) = | \Pr[\text{Adversary wins}] - 1/2 |$$

A proof system for R running on parameters is zero knowledge if nobody ever constructs an efficient adversary with significant advantage.

It depends on the application what is considered an efficient adversary (computing equipment, running time, memory consumption, usage lifetime, etc.) and how large an advantage can be tolerated. Special strong notions include statistical zero knowledge (aka unconditional zero knowledge) where any adversary has small advantage, and perfect zero knowledge, where for any adversary the advantage is exactly 0.



multi-theorem zero knowledge. In the zero-knowledge definition, the adversary interacts with the prover or simulator on a single instance. It is possible to strengthen the zero-knowledge definition to guard also against an adversary that sees proofs for multiple instances.

Honest verifier zero knowledge. A weaker privacy notion is honest verifier zero-knowledge, where we assume the adversary follows the protocol honestly (i.e., in steps 6 and 7 in the definition it runs the verification algorithm). It is a common design technique to first construct an HVZK proof system, and then use efficient standard transformations to get a proof system with full zero knowledge.

Witness indistinguishability and witness hiding. Sometimes a weaker notion of privacy than zero knowledge suffices. Witness-indistinguishable proof systems make it infeasible for an adversary to distinguish which out of several possible witnesses the prover has. Witness-hiding proof systems ensure the interaction with an honest prover does not help the adversary to compute a witness.

1.6.5 Advanced security properties

The literature describes many advanced security notions a proof system may have. These include security under concurrent composition and nonmalleability to guard against man-in-the-middle attacks, security against reset attacks in settings where the adversary has physical access, simulation soundness and simulation extractability to assist sophisticated security proofs, and universal composability.

Universal composability. The UC framework defines a protocol to be secure if it realizes an ideal functionality in an arbitrary environment. We can think of an ideal zero-knowledge functionality as taking an input (x, w) from the prover and if and only if $(x, w) \in R$ it sends the message (x, accept) to the verifier. The ideal functionality is perfectly sound, since no statement without valid witness will be accepted, and perfectly zero knowledge, since the proof is just the message accept. A proof system is then UC secure, if the real life execution of the system is ‘security-equivalent’ to the execution of the ideal proof system functionality. Usually it takes more work to demonstrate a proof system is UC secure, but on the other hand the framework offers strong security guarantees when the proof system is composed with other cryptographic protocols.

1.6.6 Transferability vs. deniability

In the traditional notion of zero-knowledge, a ZKP system prevents the verifier from even being able to convincingly advertise having interacted in a legitimate proof execution. In other words, the verifier cannot transfer onto others the confidence gained about the proven statement. This property is sometimes called *deniability* or *non-transferability*, since a prover that has interacted as a legitimate prover in a proof is later able to *plausibly deny* having done so, even if the original verifier releases the transcript publicly.

Despite *deniability* being often a desired property, the dual property of *transferability* can also be considered a feature, and such a setting is also of interest in this document. *Transferability* means that the verifier in a legitimate proof execution becomes able to convince an external party that

E20: D7.1

the corresponding statement is true. In the case of a statement of knowledge, this means being convinced that some prover did indeed have the claimed knowledge. In some cases this can be done by simply sending the transcript (the verifier's view) of the interaction (messages exchanged and the internal state of the verifier).

For a proper security analysis of an application, it is important to characterize whether deniability of transferability (or a nuanced version of them) is intended. This may be an important aspect of composability with other applications.

1.6.7 Examples of setup and trust

The security definitions assume a trusted setup. There are several variations of what the setup looks like and the level of trust placed in it.

- No setup or trustless setup. This is when no trust is required, for instance because the setup is just a copy of a security parameter k , or because everybody can verify the setup is correct directly.
- Uniform random string. All parties have access to a uniform random string $URS = \text{setup}_R = \text{setup}_P = \text{setup}_V$. We can distinguish between the lighter trust case where the parties just need to get a uniformly sampled string, which they may for instance get from a trusted common source of randomness e.g. sunspot activity, and the stronger trust case where zero-knowledge relies on the ability to simulate the URS generation together with a simulation trapdoor.
- Common reference string. The URS model is a special case of the CRS model. But in the CRS model it is also possible that the common setup is sampled with a non-uniform distribution, which may exclude easy access to a trusted common source. A distinction can be made whether the CRS has a verifiable structure, i.e., it is easy to verify it is well-formed, or whether full trust is required.
- Designated verifier setup. If we have a setup that generates correlated setup_P and setup_V , where setup_V is intended only for a designated verifier, we also need to place trust in the setup algorithm. This is for instance the case in Cramer-Shoup public-key encryption where a designated verifier NIZK proof is used to provide security under chosen-ciphertext attack. Here the setup is generated as part of the key generation process, and the recipient can be trusted to do this honestly because it is the recipient's own interest to make the encryption scheme secure.
- Random oracle model. The common setup describes a cryptographic hash function, e.g. SHA256. In the random oracle model, the hash function is heuristically assumed to act like a random oracle that returns a random value whenever it is queried on an input not seen before. There are theoretical examples where the random oracle model fails, exploiting the fact that in real life the hash function is a deterministic function, but in practice the heuristic gives good efficiency and currently no weaknesses are known for 'natural' proof systems.
- There are several proposals to reduce the trust in the setup such as using secure multi-party computation to generate a CRS, using a multi-string model where there are many CRSs and security only relies on a majority being honestly generated, and subversion resistant CRS where zero-knowledge holds even against a maliciously generated CRS.

1.7 Assumptions

A full specification of a proof system **must** state the assumptions under which it satisfies the security definitions and demonstrate the assumptions imply the proof system has the claimed security properties.

A security analysis may take the form of a mathematical proof by reduction, which demonstrates that a realistic adversary gaining significant advantage against a security property, would make it possible to construct a realistic adversary gaining significant advantage against one of the underpinning assumptions.

To give an example, suppose soundness relies on a collision-resistant hash function. The demonstration of this fact may take the form of describing a simple and efficient algorithm **Reduction**, which may call a soundness attacker **Adversary** as a subroutine a few times. Furthermore, the demonstration may establish that the advantage **Reduction** has in finding a collision is closely related to the advantage an arbitrary **Adversary** has against soundness, for instance

$$\text{Advantage_soundness}(\text{parameters}) \leq 8 \times \text{Advantage_collision}(\text{parameters})$$

Suppose the proof system is designed such that we can instantiate it with the SHA-256 hash function as part of the parameters. If we assume the risk of an attacker with a budget of \$1,000,000 finding a SHA-256 collision within 5 years is less than 2^{-128} , then the reduction shows the risk of an adversary with similar power breaking soundness is less than 2^{-125} .

Cryptographic assumptions: Cryptographic assumptions, i.e. intractability assumptions, specify what the proof system designers believe a realistic attacker is incapable of computing. Sometimes a security property may rely on no cryptographic assumptions at all, in which case we say security of unconditional, i.e., we may for instance say a proof system has unconditional soundness or unconditional zero knowledge. Usually, either soundness or zero knowledge is based on an intractability assumption though. The choice of assumption depends on the risk appetite of the designers and the type of adversary they want to defend against.

Plausibility. At all costs, an intractability assumption that has been broken should not be used. We recommend designing flexible and modular proof systems such that they can be easily updated if an underpinning cryptographic assumption is shown to be false.

Sometimes, but not always, it is possible to establish an order of plausibility of assumptions. It is for instance known that if you can break the discrete logarithm problem in a particular group, then you can also break the computational Diffie-Hellman problem in the same group, but not necessarily the other way around. This means the discrete logarithm assumption is more plausible than the computational Diffie-Hellman assumption and therefore preferable from a security perspective.

Post-quantum resistance. There is a chance that quantum computers will be developed within a few decades. Quantum computers are able to efficiently break some cryptographic assumptions, e.g., the discrete logarithm problem. If the expected lifetime of the proof system extends beyond the emergence of quantum computers, then it is necessary to rely on intractability assumptions that are believed to resist quantum computers. Different security properties may require different lifetimes. For instance, it may be that proofs are verified immediately and hence post-quantum soundness is

not required, while at the same time an attacker may collect and store proof transcripts and later try to learn something from them, so post-quantum zero knowledge is required.

Concrete parameters. It is common in the cryptographic literature to use vague phrasing such as “the advantage of a polynomial time adversary is negligible” when describing the theory behind a proof system. However, concrete and precise security is needed for real-world deployment. A proof system should therefore come with concrete parameter recommendation and a statement about the level of security they are believed to provide.

System assumptions: Besides cryptographic assumptions, a proof system may rely on assumptions about the equipment or environment it works in. As an example, if the proof system relies on a trusted setup it should be clearly stated what kind of trust is placed in.

Setup. If the prover or verifier are probabilistic, they require an entropy source to generate randomness. Faulty pseudorandomness generation has caused vulnerabilities in other types of cryptographic systems, so a full specification of a proof system should make explicit any assumptions it makes about the nature or quality of its source of entropy.

1.8 Efficiency

A specification of a proof system may include claims about efficiency and if it does the units of measurement MUST be clearly stated. Relevant metrics may include:

- **Round complexity:** Number of transmissions between prover and verifier. Usually measured in the number of moves, where a move is a message from one party to the other. An important special case is that of 1-move proof systems, aka non-interactive proof systems, where the verifier receives a proof from the prover and directly decides whether to accept or not. Non-interactive proofs may be transferable, i.e., they can be copied, forwarded and used to convince several verifiers.
- **Communication:** Total size of communication between prover and verifier. Usually measured in bits.
- **Prover computation:** Computational effort the prover expends over the duration of the protocol. Sometimes measured as a count of the dominant cryptographic operations (to avoid system dependence) and sometimes measured in seconds on a particular system (when making concrete measurements).
- Depending on the intended usage, many other metrics may be important: memory consumption, energy consumption, entropy consumption, potential for parallelisation to reduce time, and offline/online computation trade-offs.
- **Verifier computation:** Computational effort the verifier expends over the duration of the protocol.
- **Setup cost:** Size of setup parameters, e.g. a common reference string, and computational cost of creating the setup.

Readers of a proof system specification may differ in the granularity they need in the efficiency measurements. Take as an example a proof system consisting of an information theoretic core that is then compiled with cryptographic primitives to yield the full system. An implementer will likely want

to have a detailed performance analysis of the information theoretic core as well as the cryptographic compilation, since this will guide her choice of trade-offs and optimizations. A consumer on the other hand will likely want to have a high-level performance analysis and an apples-to-apples comparison to competing proof systems. We therefore recommend to provide both a detailed analysis that quantifies all the dominant efficiency costs, and a bottom-line analysis that summarizes performance for reasonable choices of parameters and identifies the optimal performance region.

1.8.1 Characterization of security properties

E21: D4.3

The benchmarking of a technique should clarify the distinct security levels achieved/conjectured for different security properties, e.g., soundness vs. zero-knowledge. In each case, the security type should also be clarified with respect to being unconditional, statistical or computational. When considering computational security, it should be clarified to what extent pre-computations may affect the security level, and whether/how known attacks may be parallelizable. All security claims/assertions should be qualified clearly with respect to whether they are based on proven security reductions or on heuristic conjectures. In either case the security analysis should make clear which computational assumptions and implementation requirements are needed. It should be made explicit whether (and how) the security levels relate to classical or quantum adversaries. When applicable, the benchmarking should characterize the security (including possible unsuitability) of the technique against quantum adversaries.

1.8.2 Computational security levels for benchmarking

E22: D4.4

The benchmarks for each technique **shall** include at least one parameterization for achieving a conjectured computational security level κ approximately equal to, or greater than, 128 bits. Each technique **should** also be benchmarked for at least one additional higher computational security level, such as 192 or 256 bits. (If only one, the latter is preferred.) The benchmarking at more than one level aids with the understanding of how the efficiency varies with the security level. The interest in a security level as high as 256 bits can be considered a precautionous (and heuristic) safety margin, compared for example with intended 128 bits. This is intended to handle the possibility that the conjectured level of security is later found to have been over-estimated. The evaluation at computational security below 128 bits may be justified for the purpose of clarifying how the execution complexity or time varies with the security parameter, but should not be construed as a recommendation for practical security.

An exception allowing lower computational security parameter. With utmost care, a computational security level may be justified below 128 bits, including for benchmarking. The following text describes as exception. In some interactive ZKPs (see Section 2.2), there may be cryptographic properties that only need to be held during a portion of a protocol execution, which in turn may be required to take less than a fixed amount of time, say, one minute. For example, a commitment scheme used to enable temporary hiding during a coin-flipping protocol may only need to hold until the other party reveals a secret value. In such case the property may be implemented with less than 128 bits of security, under special care (namely with respect to composition in a concurrent setting) and if the difference in efficiency is substantial. Such decreased security level

E23: D4.4

of a component of a protocol may also be useful for example to enable properties of deniability (non-transferability).

Depending on the application, other exceptions may be acceptable, upon careful analysis, when the witness whose knowledge is being proven is itself discoverable from the ZK instance with less computational resources than those corresponding to 128 bits of security.

1.8.3 Statistical security levels for benchmarking

E24: D11.1

The soundness security of certain interactive ZKP systems may be based on the ability of the verifier(s) to validate-or-trust the freshness and entropy of a challenge (e.g., a nonce produced by a verifier, or randomness obtained by a trusted randomness Beacon). In some of those cases, a statistical security parameter σ (e.g., 40 or 64 bits) may be used to refer to the error probability (e.g., 2^{-40} or 2^{-64} , respectively) of a protocol with “one-shot” security, i.e., when the ability of a malicious prover to succeed without knowledge of a valid witness requires guessing in advance what the challenge would be. In those cases, a low statistical security parameter may be suitable if there is a mechanism capable of detecting and preventing a repetition of failed proof attempts.

While an appropriate minimal parameter may depend on the application scenario, benchmarking **shall** be done with statistical security of at least 64 bits. Whenever the efficiency variation is substantial across variations of statistical security parameter, it is recommended that more than one security level be benchmarked. The cases of 40, 64, 80 and 128 bits are suggested.

For interactive techniques where the efficiency upon using 64 bits of statistical security is similar to that of using a higher parameter similar to the computation security parameter (at least 128 bits), then the benchmark **should** use at least one higher statistical parameter that enables retaining high computational security (at least 128 bits) even if the protocol is transformed into a non-interactive version via a Fiat-Shamir transformation or similar. In the resulting non-interactive protocols, the prover is the sole generator of the proof, and so a malicious prover can rewind and restart an attempt to generate a forged proof whenever a non-interactively produced challenge is unsuitable to complete the forgery. Computational security remains if the expected number of needed attempts is of the order of 2^κ .

List of references: [BCIOP13], [BCS16], [BISW17], [BCCGP16], [BCGGHJ17], [BCGJM18], [CD98], [GGPR13a], [GKR15], [Gro10], [WTSTW18], [IKOS07], [IMS12], [Ki95], [KR08], [AHIV17], [Mic00], [RRR16], [ZGKPP18], [ZGKPP17], [GMO16].

Chapter 2. Construction paradigms

E25: D1.2

2.1 Taxonomy of Constructions

E26: D1.3


There are many different types of zero-knowledge proof systems in the literature that offer different tradeoffs between communication cost, computational cost, and underlying cryptographic assumptions. Most of these proofs can be decomposed into an “information-theoretic” zero-knowledge proof system, sometimes referred to as a zero-knowledge *probabilistically checkable proof* (PCP), and a *cryptographic compiler*, or crypto compiler for short, that compiles such a PCP into a zero-knowledge proof. (Here and in the following, we will sometimes omit the term “zero-knowledge” for brevity even though we focus on zero-knowledge proof systems by default.)

Different kinds of PCPs require different crypto compilers. The crypto compilers are needed because PCPs make unrealistic independence assumptions between values contributed by the prover and queries made by the verifier, and also do not take into account the cost of communicating a long proof. The main advantage of this separation is modularity: PCPs can be designed, analyzed and optimized independently of the crypto compilers, and their security properties (soundness and zero-knowledge) do not depend on any cryptographic assumptions. It may be beneficial to apply different crypto compilers to the same PCP, as different crypto compilers may have incomparable efficiency and security features (e.g., trade succinctness for better computational complexity or post-quantum security).

PCPs can be divided into two broad categories: ones in which the verifier makes point queries, namely reads individual symbols from a proof string, and ones where the verifier makes linear queries that request linear combinations of field elements included in the proof string. Crypto compilers for the former types of PCPs typically only use symmetric cryptography (a collision-resistant hash function in their interactive variants and a random oracle in their non-interactive variants) whereas crypto compilers for the latter type of PCPs typically use homomorphic public-key cryptographic primitives (such as SNARK-friendly pairings).

Table 2.1 summarizes different types of PCPs and corresponding crypto compilers. The efficiency and security features of the resulting zero-knowledge proofs depend on both the parameters of the PCP and the features of the crypto compiler.

Table 2.1: Different types of PCPs

Proof System	Inter-action	Queries to Proof	Crypto Compilers 	Features
Classical proof (no zk)	No	All	GMW, ...,	1,2,3e
			Cramer-Damgård 98, ...	1,3e
Classical PCP	No	Point Queries	Kilian, Micali, IMS	1,2,3b
Linear PCP	No	Inner-product Queries	IKO,Groth10,GGPR,BCIOP	3a
IOP	Yes	Point Queries	BCS16+ZKStarks	1,2,3b
			BCS16+Ligero	1,2,3d
Linear IOP	Yes	Inner-product Queries	Hyrax	1,3b/3c
			vSQL	3c
			vRAM	3b
ILC	Yes	Matrix-vector Queries	Bootle 16,18	1,3b
			Bootle 17	1,2,3d

Notation: We say that a verifier makes “point queries” to the proof Π if the verifier has access to a proof oracle O^Π that takes as input an index i and outputs the i -th symbol $\Pi(i)$ of the proof. We say that a verifier makes “inner-product queries” to the proof $\Pi \in \mathbb{F}^m$ (for some finite field \mathbb{F}) if the proof oracle takes as input a vector $q \in \mathbb{F}^m$ and returns the value $\langle \Pi, q \rangle \in \mathbb{F}$. We say that a verifier makes “matrix-vector queries” to the proof $\Pi \in \mathbb{F}^{m \times k}$ if the proof oracle takes as input a vector $q \in \mathbb{F}^k$ and returns the matrix-vector product $(\Pi.q) \in \mathbb{F}^m$.

1. No trusted setup
2. Relies only on symmetric-key cryptography (e.g., collision-resistant hash functions and/or random oracles)
3. Succinct proofs
 - (a) Fully succinct: Proof length independent of statement size. $O(1)$ crypto elements (fully)
 - (b) Polylog succinct: Polylogarithmic number of crypto elements
 - (c) Depth-succinct: Depends on depth of a verification circuit representing the statement.
 - (d) Sqrt succinct: Proportional to square root of circuit size
 - (e) Non succinct: Proof length is larger than circuit size.

2.1.1 Proof Systems

Note: For all of the applications we consider, the prover must run in polynomial time, given a statement-witness pair, and the verifier must run in (possibly randomized) polynomial time.

- a. Classical Proofs: In a classical NP/MA proof, the prover sends the verifier a proof string π , the verifier reads the entire proof π and the entire statement x , and accepts or rejects.

- b. PCP (Probabilistically Checkable Proofs): In a PCP proof, the prover sends the verifier a (possibly very long) proof string π , the verifier makes “point queries” to the proof, reads the entire statement x , and accepts or rejects. Relevant complexity measures for a PCP include the verifier’s query complexity, the proof length, and the alphabet size.
- c. Linear PCPs: In a linear PCP proof, the prover sends the verifier a (possibly very long) proof string π , which lies in some vector space \mathbb{F}^m . The verifier makes some number of linear queries to the proof, reads the entire statement x , and accepts or rejects. Relevant complexity measures for linear PCPs include the proof length, query complexity, field size, and the complexity of the verifier’s decision predicate (when expressed as an arithmetic circuit).
- d. IOP (Interactive Oracle Proofs): An IOP is a generalization of a PCP to the interactive setting. In each round of communication, the verifier sends a challenge string c_i to the prover and the prover responds with a PCP proof π_i that the verifier may query via point queries. After several rounds of interactions, the verifier accepts or rejects. Relevant complexity measures for IOPs are the round complexity, query complexity, and alphabet size. IOP generalizes the notion of Interactive PCP [KR08], and coincides with the notion of Probabilistically Checkable Interactive Proof [RRR16].
- e. Linear IOP: A linear IOP is a generalization of a linear PCP to the interactive setting. (See IOP above.) Here the prover sends in each round a proof vector π_i that the verifier may query via linear (inner-product) queries.
- f. ILC (Ideal Linear Commitment): The ILC model is similar to linear IOP, except that the prover sends in each round a proof matrix rather than proof vector, and the verifier learns the product of the proof matrix and the query vector. This model relaxes the Linear Interactive Proofs (LIP) model from [BCIOP13]. (That is, each ILC proof matrix may be the output of an arbitrary function of the input and the verifier’s messages. In contrast, each LIP proof matrix must be a linear function of the verifier’s messages.) Important complexity measures for ILCs are the round complexity, query complexity, and dimensions of matrices.

2.1.2 Compilers: Cryptographic

- a. Cramer-Damgård [CD98]: Compiles an NP proof into a zero-knowledge proof. The prover evaluates the circuit C recognizing the relation on its statement-witness pair (x, w) . The prover commits to every wire value in the circuit and sends these commitments to the verifiers. The prover then convinces the verifier using sigma protocols that the wire values are all consistent with each other. The prover opens the input wires to x and thus convinces the verifier that the circuit $C(x, \cdot)$ is satisfied on some witness w . The compiler uses additively homomorphic commitments (instantiated using the discrete-log assumption, for example) and generating or verifying the proof requires a number of public-key operations that is linear in the size of the circuit C .
- b. Kilian [Kil95] / Micali [Mic00] / IMS [IMS12]: Compiles a PCP with a small number of queries into a succinct proof. The prover produces a PCP proof that x is in L . The prover commits to the entire PCP proof using a Merkle tree. The verifier asks the prover to open a few positions in the proof. The prover opens these positions and uses Merkle proofs to convince the verifier that the openings are consistent with the Merkle commitment. The verifier accepts iff the

PCP verifier accepts. The compiler can be made non-interactive in the random oracle model via the Fiat-Shamir heuristic.

- c. GGPR [GGPR13a] / BCIOP [BCIOP13]: Compiles a linear PCP into a SNARG via a transformation to LIPs. The public parameters of the SNARG are as long as the linear PCP proof and the SNARG proof consists of a constant number of ciphertexts/commitments (if the linear PCP has constant query complexity). In the public verification setting, this compiler relies on “SNARG-friendly” bilinear maps and is thus not post-quantum secure. In the designated verifier setting, it can be made post-quantum secure via linear-only encryption [BISW17]. Generating the proof requires a number of public-key operations that grows linearly (or quasi-linearly) in the size of the circuit recognizing the relation.
- d. BCS16 [BCS16]: A generalization of the Fiat-Shamir compiler that is useful for collapsing many-round public-coin proofs (such as IOPs) into NIZKs in the random-oracle model.
- e. Hyrax [WTSTW18] and vSQL [ZGKPP17]: Give mechanisms for compiling the GKR protocol [GKR15] into NIZKs in the random oracle model. The techniques in these works generalize to compile any public-coin linear IOP (without zero knowledge) into a non-interactive zero-knowledge proof in the random-oracle model, that additionally relies on algebraic commitment schemes. The latter are typically implemented using homomorphic public-key cryptography.
- f. Bootle16 [BCCGP16]: Compiler for converting an ILC proof into a many-round succinct proof under the discrete-log assumption. Generating and verifying the proof requires a number of public-key operations that grows linearly with the size of the circuit recognizing the NP relation in question.

Note: In addition to the crypto compilers described above, there are information-theoretic compilers that convert between different types of information-theoretic objects.

2.1.3 Compilers: Information-theoretic

- a. MPC-in-the-Head (IKOS [IKOS07], ZKboo [GMO16], Ligero [AHIV17]): Compiles secure multi-party computation protocols into either (zero-knowledge) PCPs or IOPs.
- b. BCIOP [BCIOP13]: Compiles quadratic arithmetic programs (QAPs) or quadratic span programs (QSPs) into linear PCPs such that resulting linear PCP has a degree-two decision predicate. The BCIOP paper also gives a compiler for converting linear PCP into 1-round LIP/ILC and adding zero-knowledge to linear PCP.
- c. Bootle17 [BCGGHJ17]: Compiles a proof in the ILC model into an IOP. They also give an example instantiation of the ILC proof that yields an IOP proof system with square-root complexity.

2.2 Interactivity

Several of the proof systems described in the Taxonomy of Constructions given in Section 2.1 are interactive, including classical interactive proofs (IPs), IOPs, and linear IOPs. This means that the verifier sends multiple challenge messages to the prover, with the prover replying to challenge i before receiving challenge $i + 1$; soundness relies on the prover being unable to predict challenge $i + 1$ when it responds to challenge i . The other proof systems from the Taxonomy of Constructions are non-interactive, namely classical PCPs and linear PCPs. All of these proof systems can be combined with cryptographic compilers to yield argument systems that may or may not be interactive, depending on the compiler.

2.2.1 Advantages of Interactive Proof and Argument Systems

- a. Efficiency and Simplicity. Interactive proof systems can be simpler or more efficient than non-interactive ones. As an example, researchers introduced the IOP model [BCS16; RRR16], which is interactive, in part because interactivity allowed for circumventing efficiency bottlenecks arising in state of the art PCP constructions [BCGT13]. As another example, some argument systems derived from IPs [WTSTW18; XZZPS19] have substantially better space complexity for the prover (a key scalability bottleneck) than state of the art PCPs [BCGT13] or linear PCPs [GGPR13a; Gro16].

Yet, if an interactive protocol is public coin, it can be rendered non-interactive and publicly verifiable in most settings via the Fiat-Shamir transformation (see Section 2.1.2), often with little loss in efficiency. This means that protocol designers have the freedom to leverage interactivity as a “resource” to simplify protocol design, improve efficiency, weaken or remove trusted setup, etc., and still have the option of obtaining a non-interactive argument using the Fiat-Shamir transformation.

(Applying the Fiat-Shamir heuristic to an interactive protocol to obtain a non-interactive argument may increase soundness error, and may transform statistical security to computational security — see Section 1.8.3. However, recent works [BCS16; CCHL+19] show that when the transformation is applied to specific IP, IOP, and linear IOP protocols of both practical and theoretical interest, the blowup in soundness error is only polynomial in the number of rounds of interaction.)

- b. Setup. Cryptographic compilers for linear PCPs currently require a structured reference string (SRS) (see Section 3.6.2). Here, an SRS is a structured string that must be generated by a trusted third party during a setup phase, and soundness requires that any trapdoor used during this trusted setup must not be revealed. In contrast, some compilers that apply to IPs, IOPs (as well as PCPs), and linear IPs yields arguments in which the prover and the verifier need only access a uniform random string (URS), which can be obtained from a common source of randomness. Such a setup is referred as *transparent* setup in the literature.

- c. Cryptographic Primitives. Argument systems derived from IPs, IOPs, or linear IOPs also sometimes rely on more desirable cryptographic primitives. For example, IPs themselves are information-theoretically secure, relying on no cryptographic assumptions at all. And in contrast to arguments derived from linear PCPs, those derived from IOPs rely only on symmetric-key cryptographic primitives (see, e.g., [BCS16]). Finally, it has long been known how to obtain succinct *interactive* arguments in the plain model based on falsifiable assumptions like collision-resistant hash families [Kil95], but this is not the case for succinct *non-interactive* arguments.

- d. Non-transferability. In some applications, it is essential that proofs be deniable or *non-transferable* (i.e., it must be impossible for a verifier to convince a third party of the validity of the statement — see Sections 1.6.6). While these properties are not unique to interactive protocols, interaction offers a natural way to make proofs non-transferable (for details, see Section 2.2.3).
- e. Interactivity May Limit Adversaries' Abilities. Interactive protocols can potentially be run with fewer bits of security and hence be more efficient. For example, interactive settings may allow for the enforcement of a time limit for the protocol to terminate, limiting the runtime of attackers. Alternatively, in an interactive setting it may be possible to ensure that adversaries only have one attempt to attack a protocol, while this will not be possible in many non-interactive settings. See Section 1.8.2 for details.
- f. Interactivity May Be Inherent to Applications. Many applications are inherently interactive. For example, real-world networking protocols involve multiple messages just to initiate a connection. In addition, zero-knowledge protocols are often combined with other cryptographic primitives in applications (e.g., oblivious transfer). If the other primitives are interactive, then the final cryptographic protocol will be interactive regardless of whether the zero-knowledge protocol is non-interactive. If an application is inherently interactive, it may be reasonable to leverage the interaction as a resource if it can render a protocol simpler, more efficient, etc.

2.2.2 Disadvantages of Interactive Proof and Argument Systems

- 1. Interactive protocols must occur online. In an interactive protocol, the proof cannot simply be published or posted and checked later at the verifier's convenience, as can be done with non-interactive protocols.
- 2. Public Verifiability. Many applications require that proofs be verifiable by any party at any time. Public verifiability may be difficult to achieve for interactive protocols. This is because soundness of interactive protocols relies on the prover being unable to predict the next challenge it will receive in the protocol. Unless there is a publicly trusted source of unpredictable randomness (e.g., a randomness beacon) and a way for provers to timestamp messages, it is not clear how any party other than the one sending the challenges can be convinced that the challenges were properly generated, and the prover replied to challenge i before learning challenge $i + 1$. See Section 2.2.3 below for further details.
- 3. Network latency can make interactive protocols slow. If an interactive protocol consists of many messages sent over a network, network latency may contribute significantly to the total execution time of the protocol.
- 4. Timing or Side Channel Attacks. Because interactive protocols require the prover to send multiple messages, there may be more vulnerability to side channel or timing attacks compared to non-interactive protocols. Timing attacks will only affect zero-knowledge, not soundness, for public-coin protocols, because the verifier's messages are simply random coins, and timing attacks should not leak information to the prover in this case. In private coin protocols, both zero-knowledge and soundness may be affected by these attacks.
- 5. Concurrent Security. If an interactive protocol is not used in isolation, but is instead used in an environment where multiple interactive protocols may be executed concurrently, then

considerable care should be taken to ensure that the protocol remains secure. See for example [Gol13, Section 2.1] and the references therein. Issues of concurrent execution security are greatly mitigated for non-interactive protocols [GOS06].

6. **Proof Length.** Currently, the zero-knowledge protocols with the shortest known proofs are based on linear PCPs, which are non-interactive. These proofs are just a few group elements (see Table 2.1). While (public-coin) zero-knowledge protocols based on IPs or IOPs can be rendered non-interactive with the Fiat-Shamir heuristic, they currently produce longer proofs. The longer proofs may render these protocols unsuitable for some applications (e.g., public blockchain), but they may still be suitable for other applications (even related ones, like enterprise blockchain applications).

2.2.3 Nuances on transferability vs. interactivity

The relation between interactivity and transferability/deniability is not without nuances. The following paragraphs show several possible combinations.

Non-interactive and deniable. A non-interactive ZKP may be non-transferable. This may be based for example on a setup assumption such as a local CRS that is itself deniable. In that case, a malicious verifier cannot prove to an external party that the CRS was the one used in a real protocol execution, leading the external party to have reasonable suspicion that the verifier may have simulated the CRS so as to become able to simulate a protocol execution transcript, without actual participation of a legitimate prover. Another example of non-transferability is when a ZKP intended to prove (i) an assertion (of membership or knowledge) actually proves its disjunction with (ii) the knowledge of the secret key of a designated verifier, for example assuming a public key infrastructure (PKI). This suffices to convince the original verifier the initial statement (i) is true, since the verifier knows that the prover does not actually know the secret key (ii). In other words, a success in the interactive proof stems from the initial assertion (i) being truthful. However, for any external party, the transcript of the proof may conceivably have been produced by the original designated verifier, who can simply do it with the knowledge of the secret key (ii). In that sense, the designated verifier would be unable to convince others that the transcript of a legitimate proof was not simulated by the verifier.

Non-interactive and transferable. If transferability is intended as a feature, then a non-interactive protocol can be achieved for example with a public (undeniable) CRS. For example, if a CRS is generated by a trusted randomness beacon, and if soundness follows from the inability of the prover to control the CRS, then any external party (even one not involved with the prover at the time of proof generation) can at a later time verify that a proof transcript could have only been generated by a legitimate prover.

Interactive and deniable. A classical example (in a standalone setting, without concurrent executions) for obtaining the deniability property comes from interactive ZKP protocols proven secure based on the use of rewinding. Here, deniability follows from the simulatability of transcripts for any malicious verifier. For each interactive step, the simulator learns the challenge issued by the possibly malicious verifier, and then rewinds to reselect the preceding message of the prover, so as to be able to answer the subsequent challenge. Some techniques require the use of commitments and/or trapdoors, and may enable this property even for straight-line simulation (i.e., without rewinding),

E28: D7.1

1096 provided there is an appropriate trusted setup.

1097 **Interactive and transferable.** In certain settings it is possible, even from an interactive ZKP
 1098 protocol execution, to produce a transcript that constitutes a transferable proof. Usually, trans-
 1099 ferability can be achieved when the (possibly malicious) verifier can convincingly show to external
 1100 parties that the challenges selected during a protocol execution were unpredictable at the time of
 1101 the determination of the preceding messages of the prover. The transferable proof transcript is then
 1102 composed of the messages sent by the prover and additional information from the internal state of
 1103 a malicious verifier, including details about the generation of challenges. For example, a challenge
 1104 produced (by the verifier) as a cryptographic hash output (or as a keyed pseudo-random function) of
 1105 the previous messages may later be used to provide assurance that only a legitimate prover would have
 1106 been able to generate a valid subsequent message (response). As another example, if the interactive
 1107 ZKP protocol is composed with a communication protocol where the prover authenticates all sent
 1108 messages (e.g., signed within a PKI, and timestamped by a trusted service), then the overall sequence
 1109 of those certified messages becomes, in the hands of the verifier, a transferable proof. Furthermore,
 1110 from a transferable transcript, the actual transfer can also be performed in an interactive way: the
 1111 verifier (in possession of the transcript) acts as prover in a transferable ZKP of knowledge of a
 1112 transferable transcript, thereby transferring to the external verifier a new transferable transcript.

1113 (Non)-Transferability/Deniability of Zero-Knowledge Proofs

1114 **Off-line non-transferability (deniability) of ZK proofs.** Zero-knowledge proofs are in general
 1115 interactive. Interaction is inherent without a setup. Indeed, Goldreich and Oren showed that for
 1116 non-trivial languages zero-knowledge proofs require at least 3 rounds.

E29: D7.3

1117 The zero-knowledge property in absence of setup guarantees¹ a property called off-line non-
 1118 transferability, also known as deniability. This property means that the verifier gets no evidence
 1119 of having received an accepting proof from a prover and thus has no advantage in transferring the
 1120 received proof to others.

1121 **On-line non-transferability of ZK proofs.** The situation is more complicated in case of on-line
 1122 non-transferability. Indeed, in this case a malicious verifier plays with a honest prover in a zero-
 1123 knowledge proof system and at the same time the malicious verifier plays with others in the attempt
 1124 of transferring the proof that he his receiving from the prover. Non-transferability is therefore a form
 1125 of security against man-in-the-middle attacks. Security against such attacks is typically referred to
 1126 as non-malleability when the same zero-knowledge proof system is used by the adversary to try to
 1127 transfer the proof to a honest verifier. When instead different protocols are involved as part of the
 1128 activities of the adversary, some stronger notions are required to model security under such attacks
 1129 (e.g., universal composability).

1130 **Transferability of a NIZK proof: publicly verifiable ZK.** The transferability of a zero-
 1131 knowledge proof could become unavoidable when some forms of setups are considered and the
 1132 zero-knowledge proof makes some crucial use of it. Indeed, notice that both in the common reference
 1133 string model and in the programmable random oracle model one can construct non-interactive

¹A verifier could always compute an equivalent transcript by running the simulator.

1134 zero-knowledge proofs. Such proofs cannot be simulated by the verifier with the same setup or the
 1135 same instantiation of the random oracle. More specifically, non-interactive zero-knowledge proofs
 1136 are constructed without the contribution of any verifier, therefore they are publicly verifiable proofs
 1137 that can naturally be transferred among verifiers.

1138 **Designated-verifier NIZK proofs.** With more sophisticated setups other options become possi-
 1139 ble. Consider for instance a verifier possessing a public identity implemented through a public key.
 1140 In this case the prover can compute a non-interactive zero-knowledge proof that makes crucially
 1141 use of the public key of the verifier at the point that the verifier using the corresponding secret key
 1142 could compute an indistinguishable proof. In this case we have that the proof is a non-interactive
 1143 designated-verifier zero-knowledge proof and is non-transferable since the verifier that receives the
 1144 proof could have computed an equivalent proof by herself, therefore there is no evidence to share
 1145 with others about the fact that the proof comes from a honest prover.

1146 **Transferability of interactive ZK proofs.** The use of identities implemented through public
 1147 keys can also have impact in the interactive case. Consider the case where there is no trusted setup.
 1148 In this case one can design an interactive zero-knowledge proof system that can have a transferability
 1149 flavor by exploiting the public keys of prover and verifier. Indeed, if the prover signs the transcript,
 1150 then the proof is transferable by the verifier to whoever believes that the prover is honest.

1151 2.3 Several construction paradigms

1152 Zero-knowledge proof protocols can be devised within several paradigms, such as:

E30: D1.4

- 1153 • Specialized protocols for specialized proofs of membership or proofs of knowledge
- 1154 • Proofs based on discrete-log and/or pairings
- 1155 • Probabilistic checkable proofs
- 1156 • Quadratic arithmetic programs
- 1157 • GKR
- 1158 • Interactive oracle proofs
- 1159 • MPC in the head
- 1160 • Using garbled circuits

Chapter 3. Implementation

3.1 Overview

By having a standard or framework around the implementation of ZKPs, we aim to help platforms adapt more easily to new constructions and new schemes, that may be more suitable because of efficiency, security or application-specific changes. Application developers and the designers of new proof systems all want to understand the performance and security tradeoffs of different ZKP constructions when invoked in various applications. This track focuses on building a standard interface that application developers can use to interact with ZKP proof systems, in an effort to improve facilitate interoperability, flexibility and performance comparison. In this first effort to achieve such an interface, our focus is on non-interactive proof systems (NIZKs) for general statements (NP) that use an R1CS/QAP-style constraint system representation. This includes many, though not all, of the practical general-purpose ZKP schemes currently deployed. While this focus allows us to define concrete formats for interoperability, we recognize that additional constraint system representation styles (e.g., arithmetic and Boolean circuits) are in use, and are within scope of the ongoing effort. We also aim to establish best practices for the deployment of these proof systems in production software.

3.1.1 What this document is NOT about:

- A unique explanation of how to build ZKP applications
- An exhaustive list of the security requirements needed to build a ZKP system
- A comparison of front-end tools
- A show of preference for some use-cases or others

3.2 Backends: Cryptographic System Implementations

The backend of a ZK proof implementation is the portion of the software that contains an implementation of the low-level cryptographic protocol. It proves statements where the instance and witness are expressed as variable assignments, and relations are expressed via low-level languages (such as arithmetic circuits, Boolean circuits, R1CS/QAP constraint systems or arithmetic constraint satisfaction problems).

The backend typically consists of a concrete implementation of the ZK proof system(s) given as pseudocode in a corresponding publication (see the [Security Track](#) document for extensive discussion of these), along with supporting code for the requisite arithmetic operations, serialization formats, tests, benchmarking etc.

There are numerous such backends, including implementations of many of the schemes discussed in the [Security Track](#). Most have originated as academic research prototypes, and are available as

open-source projects. Since the offerings and features of backends evolve rapidly, we refer the reader to the curated taxonomy at <https://zkp.science> for the latest information.

Considerations for the choice of backends include:

- ZK proof system(s) implemented by the backend, and their associated security, assumptions and asymptotic performance (as discussed in the Security Track document)
- Concrete performance (see Benchmarks section)
- Programming language and API style (this consideration may be satisfied by adherence to prospective ZK proof standards; see the the API and File Formats section)
- Platform support
- Availability as open source
- Active community of maintainers and users
- Correctness and robustness of the implementation (as determined, e.g., by auditing and formal verification)
- Applications (as evidence of usability and scrutiny).

3.3 Frontends: Constraint-System Construction

The frontend of a ZK proof system implementation provides means to express statements in a convenient language and to prove such statements in zero knowledge by compiling them into a low-level representation and invoking a suitable ZK backend.

A frontend consists of:

- The specification of a high-level language for expressing statements.
- A compiler that converts relations expressed in the high-level language into the low-level relations suitable for some backend(s). For example, this may produce an R1CS constraint system.
- Instance reduction: conversion of the instance in a high-level statement to a low-level instance (e.g., assignment to R1CS instance variables).
- Witness reduction: conversion of the witness to a high-level statement to a low-level witness (e.g., assignment to witness variables).
- Typically, a library of "gadgets" consisting of useful and hand-optimized building blocks for statements.

Languages for expressing statements, which have been implemented in frontends to date include: code library for general-purpose languages, domain-specific language, suitably-adapted general-purpose high-level language, and assembly language for a virtual CPU.

Frontends' compilers, as well as gadget libraries, often implement various optimizations aiming to reduce the cost of the constraint systems (e.g., the number of constraints and variables). This includes techniques such as making use of "free linear combinations" in R1CS, using nondeterministic advice given in witness variables (e.g., for integer arithmetic or random-access memory), removing redundancies, using cryptographic schemes tailored for the given algebraic settings (e.g., Pedersen hashing on the Jubjub curve or MiMC for hash functions, RSA verification for digital signatures), and many other techniques. See the [Zcon0 Circuit Optimisation handout](#) for further discussion.

1233 There are many implemented frontends, including some that provide alternative ways to invoke the
1234 same underlying backends. Most have originated as academic research prototypes, and are available
1235 as open-source projects. Since the offerings and features of frontends evolve rapidly, we refer the
1236 reader to the curated taxonomy at <https://zkp.science> for the latest information.

1237 3.4 APIs and File Formats

1238 Our primary goal is to improve interoperability between proving systems and frontend consumers of
1239 proving system implementations. We focused on two approaches for building standard interfaces for
1240 implementations:

- 1241 1. We aim to develop a common API for proving systems to expose their capabilities to frontends
1242 in a way that is maximally agnostic to the underlying implementation details.
- 1243 2. We aim to develop a file format for encoding a popular form of constraint systems (namely
1244 R1CS), and its assignments, so that proving system implementations and frontends can interact
1245 across language and API barriers.

1246 We did not aim to develop standards for interoperability between backends implementing the same
1247 (abstract) scheme, such as serialization formats for proofs (see the Extended Constraint-System
1248 Interoperability section for further discussion).

1249 3.4.1 Generic API

1250 In order to help compare the performance and usability tradeoffs of proving system implementations,
1251 frontend application developers may wish to interact with the underlying proof systems via a generic
1252 interface, so that proving systems can be swapped out and the tradeoffs observed in practice. This
1253 also helps in an academic pursuit of analysis and comparison.

1254 The abstract parties and objects in a NIZK are depicted in Figure 3.1.

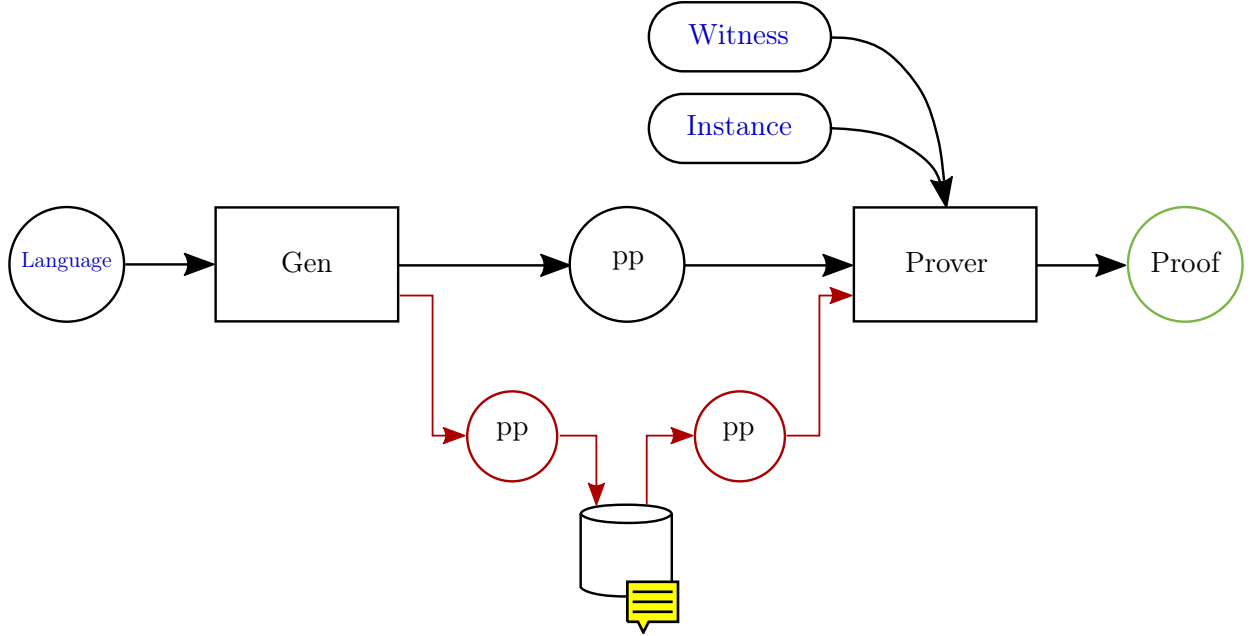


Figure 3.1. Abstract parties and objects in a NIZK

1255 We did not complete a generic API design for proving systems, but we did survey numerous tradeoffs
 1256 and design approaches for such an API that may be of future value.

1257 We separate the APIs and interfaces between the universal and non-universal NIZK setting. In
 1258 the universal setting, the NIZK's CRS generation is independent of the relation (i.e., one CRS
 1259 enables proving any NP statement). In the non-universal settings, the CRS generation depends on
 1260 the relation (represented as a constraint system), and a given CRS enables proving the statements
 1261 corresponding to any instance with respect to the specific relation.

Table 3.1: APIs and interfaces by types of universality and preprocessing

	Preprocessing (Generate has superpolylogarithmic runtime / output size as function of constraint system size)	Non-preprocessing (Generate runtime and output size is fast and CRS is at most polylogarithmic in constraint system size)
Non-universal (Generate needs constraint system as input)	QAP-based [PHGR13], [GGPR13b], [BCGTV13]	?
Universal (Generate needs just a size bound)	vnTinyRAM vRAM Bulletproofs (with explicit CRH)	Bulletproofs (with PRG-based CRH generation)

1266	Universal and scalable (Generate needs nothing but security parameter)	(impossible)	“Fully scalable” SNARKs based on PCD (recursive composition)
------	--	--------------	---

1267 In any case, we identified several capabilities that proving systems may need to express via a generic
1268 interface:

- 1269 1. The creation of CRS objects in the form of proving and verifying parameters, given the input
1270 language or size bound.
- 1271 2. The serialization of CRS objects into concrete encodings.
- 1272 3. Metadata about the proving system such as the size and characteristic of the field (for arithmetic
1273 constraints).
- 1274 4. Witness objects containing private inputs known only to the prover, and Instance objects
1275 containing public inputs known to the prover and verifier.
- 1276 5. The creation of Proof objects when supplied proving parameters, an Instance, and a Witness.
- 1277 6. The verification of Proof objects given verifying parameters and an Instance.

1278 **Future work:** We would like to see a concrete API design which leverages our tentative model,
1279 with additional work to encode concepts such as recursive composition and the batching of proving
1280 and verification operations.

1281 3.4.2 R1CS File Format

1282 There are many frontends for constructing constraint systems, and many backends which consume
1283 constraint systems (and variable assignments) to create or verify proofs. We focused on creating a
1284 file format that frontends and backends can use to communicate constraint systems and variable
1285 assignments. Goals include simplicity, ease of implementation, compactness and avoiding hard-coded
1286 limits.

1287 Our initial work focuses on R1CS due to its popularity and familiarity. Refer to the [Security](#)
1288 [Track](#) document for more information about constraint systems. The design we arrived at is
1289 tentative and requires further iteration. Implementation and specification work will appear at
1290 https://github.com/zkpstandard/file_formats.

1291 *R1CS (Rank 1 Constraint Systems)* is an NP-complete language for specifying relations as a system of
1292 bilinear constraints (i.e., a rank 1 quadratic constraint system), as defined in [BCGTV13, Appendix
1293 E in extended version]; this is a more intuitive reformulation of QAP *QAP (Quadratic Arithmetic*
1294 *Program)*, defined in [PHGR13]. R1CS is the native constraint system language of many ZK proof
1295 constructions (see the [Security Track](#) document), including many ZK proof applications in operational
1296 deployment.

Our proposed format makes heavy use of variable-length integers which are prevalent in the (space-efficient) encoding of an R1CS. We refer to `VarInt` as a variable-length unsigned integer, and `SignedVarInt` as a variable-length signed integer. We typically use `VarInt` for lengths or version numbers, and `SignedVarInt` for field element constants. The actual description of a `VarInt` is not yet specified.

We'll be working with primitive variable indices of the following form:

```
ConstantVar ← SignedVarInt(0)
InstanceVar(i) ← SignedVarInt(-(i + 1))
WitnessVar(i) ← SignedVarInt(i + 1)
VariableIndex ← ConstantVar / InstanceVar(i) / WitnessVar(i)
```

ConstantVar represents an indexed constant in the field, usually assigned to one. *InstanceVar* represents an indexed variable of the instance, or the public input, serialized with negative indices. *WitnessVar* represents an indexed variable of the witness, or the private/auxiliary input, serialized with positive indices. *VariableIndex* represents one of any of these possible variable indices.

We'll also be working with primitive expressions of the following form:

```
Coefficient ← SignedVarInt
Sequence(Entry) ← | length: VarInt | length * Entry |
LinearCombination ← Sequence(| VariableIndex | Coefficient |)
```

- Coefficients must be non-zero.
- Entries should be sorted by type, then by index:
 - | ConstantVar | sorted(InstanceVar) | sorted(WitnessVar) |

```
Constraint ←
| A: LinearCombination | B: LinearCombination | C: LinearCombination |
```

We represent a *Coefficient* (a constant in a linear combination) with a *SignedVarInt*. (TODO: there is no constraint on its canonical form.) These should never be zero. We express a *LinearCombination* as sequences of *VariableIndex* and *Coefficient* pairs. Linear combinations should be sorted by type and then by index of the *VariableIndex*; i.e., *ConstantVar* should appear first, *InstanceVar* should appear second (ascending) and *WitnessVar* should appear last (ascending).

We express constraints as three *LinearCombination* objects A, B, C, where the encoded constraint represents $A * B = C$.

The file format will contain a header with details about the constraint system that are important for the backend implementation or for parsing.

```
Header(version, vals) ←
| version: VarInt | vals: Sequence(SignedVarInt) |
```

The *vals* component of the *Header* will contain information such as:

- $P \leftarrow$ Field characteristic
- $D \leftarrow$ Degree of extension

- 1334 • $N_X \leftarrow$ Number of instance variables
- 1335 • $N_W \leftarrow$ Number of witness variables

1336 The representation of elements of extension fields is not currently specified, so D should be 1.

1337 The file format contains a magic byte sequence “R1CSstmt”, a header, and a sequence of constraints,
1338 as follows:

```
1339 R1CSFile  $\leftarrow$ 
1340 | "R1CSstmt" | Header(0, [ P, D,  $N_X$ ,  $N_W$ , ... ]) | Sequence(Constraint) |
```

1341 Further values in the header are undefined in this specification for version 0, and should be ignored.
1342 The file extension “.rlcs” is used for R1CS circuits.

1343 **Further work:** We wish to have a format for expressing the assignments for use by the backend in
1344 generating the proof. We reserve the magic “R1CSsig” and the file extension “.assignments” for this
1345 purpose. We also wish to have a format for expressing symbol tables for debugging. We reserve the
1346 magic “R1CSsymb” and the file extension “.rlcssym” for this purpose.

1347 In the future we also wish to specify other kinds of constraint systems and languages that some
1348 proving systems can more naturally consume.

1349 3.5 Benchmarks

1350 As the variety of zero-knowledge proof systems and the complexity of applications has grown, it
1351 has become more and more difficult for users to understand which proof system is the best for their
1352 application. Part of the reason is that the tradeoff space is high-dimensional. Another reason is the
1353 lack of good, unified benchmarking guidelines. We aim to define benchmarking procedures that both
1354 allow fair and unbiased comparisons to prior work and also aim to give enough freedom such that
1355 scientists are incentivized to explore the whole tradeoff space and set nuanced benchmarks in new
1356 scenarios and thus enable more applications.

1357 The benchmark standardisation is meant to document best practices, not hard requirements. They
1358 are especially recommended for new general-purpose proof systems as well as implementations
1359 of existing schemes. Additionally the long-term goal is to enable independent benchmarking on
1360 standardized hardware.

1361 3.5.1 What metrics and components to measure

1362 We recommend that as the primary metrics the **running time (single-threaded)** and the **com-**
1363 **munication complexity** (proof size, in the case of non-interactive proof systems) of all components
1364 should be measured and reported for any benchmark. The measured components should at least
1365 include the **prover** and the **verifier**. If the setup is significant then this should also be measured,
1366 further system components like parameter loading and number of rounds (for interactive proof
1367 systems) are suggested.

1368 The following metrics are additionally suggested:

- 1369 - Parallelizability
- 1370 - Batching
- 1371 - Memory consumption (either as a precise measurement or as an upper bound)
- 1372 - Operation counts (e.g. number of field operations, multi-exponentiations, FFTs and their sizes)
- 1373 - Disk usage/Storage requirement
- 1374 - Crossover point: point where verifying is faster than running the computation
- 1375 - Largest instance that can be handled on a given system
- 1376 - Witness generation (this depends on the higher-level compiler and application)
- 1377 - Tradeoffs between any of the metrics.

1378 3.5.2 How to run the benchmarks

1379 Benchmarks can be both of analytical and computational nature. Depending on the system either
 1380 may be more appropriate or they can supplement each other. An analytical benchmark consists of
 1381 asymptotic analysis as well as concrete formulas for certain metrics (e.g. the proof size). Ideally
 1382 analytical benchmarks are parameterized by a security level or otherwise they should report the
 1383 security level for which the benchmark is done, along with the assumptions that are being used.

1384 Computational benchmarks should be run on a consistent and commercially available machine.
 1385 The use of cloud providers is encouraged, as this allows for cheap reproducibility. The machine
 1386 specification should be reported along with additional restrictions that are put on it (e.g. throttling,
 1387 number of threads, memory supplied). Benchmarking machines should generally fall into one of
 1388 the following categories and the machine description should indicate the category. If the software
 1389 implementation makes certain architectural assumptions (such as use of special hardware instructions)
 1390 then this should be clearly indicated.

- 1391 - Battery powered mobile devices
- 1392 - Personal computers such as laptops
- 1393 - Server style machines with many cores and large memories
- 1394 - Server clusters using multiple machines
- 1395 - Custom hardware (should not be used to compare to software implementations)

1396 We recommend that most runs are executed on a single-threaded machine, with parallelizability
 1397 being an optional metric to measure. The benchmarks should be obtained preferably for more than
 1398 one security level, following the recommendations stated in Sections [D4.3](#) and [1.8.2](#).

E31: D4.1

1399 In order to enable better comparisons we recommend that the metrics of other proof systems/
 1400 implementations are also run on the same machine and reported. The onus is on the library
 1401 developer to provide a simple way to run any instance on which a benchmark is reported. This
 1402 will additionally aid the reproducibility of results. Links to implementations will be gathered at
 1403 zkp.science and library developers are encouraged to ensure that their library is properly referenced.
 1404 Further we encourage scientific publishing venues to require the submission of source code if an
 1405 implementation is reported. Ideally these venues even test the reproducibility and indicate whether
 1406 results could be reproduced.

3.5.3 What benchmarks to run

We propose a set of benchmarks that is informed by current applications of zero-knowledge proofs, as well as by differences in proving systems. This list in no way complete and should be amended and updated as new applications emerge and new systems with novel properties are developed. Zero-knowledge proof systems can be used in a black-box manner on an existing application, but often designing the application with a proof system in mind can yield large efficiency gains. To cover both scenarios we suggest a set of benchmarks that include commonly used primitives (e.g. SHA-256) and one where only the functionality is specified but not the primitives (e.g. a collision-resistant hash function at 128-bit classical security).

E32: D4.2

Commonly used primitives. Here we list a set of primitives that both serve as microbenchmarks and are of separate interest. Library developers are free to choose how their library runs a given primitive, but we will aid the process by providing circuit descriptions in commonly used file formats (e.g. R1CS).

Recommended

- SHA-256
- AES
- A simple vector or matrix product at different sizes

Further suggestions

- Zcash Sapling “spend” relation
- RC4 (for RAM memory access)
- Scrypt
- TinyRAM running for n steps with memory size s
- Number theoretic transform (coefficients to points)
 - Small fields
 - Big fields
 - Pattern matching

Repetition

The above relations, parallelized by putting n copies in parallel.

Functionalities. The following are examples of cryptographic functionalities that are especially interesting to application developers. The realization of the primitive may be secondary, as long as it achieves the security properties. It is helpful to provide benchmarks for a constraint-system implementation of a realization of these primitives that is tailored for the NIZK backend.

In all of the following, the primitive underlying the ZKP statement should be given at a level of 128 bits or higher and match the security of the NIZK proof system.

E33: D4.2

- Asymmetric cryptography
 - Signature verification

- 1443 - Public key encryption
- 1444 - Diffie Hellman key exchange over any group with 128 bit security
- 1445 • Symmetric & Hash
 - 1446 - Collision-resistant hash function on a 1024-byte message
 - 1447 - Set membership in a set of size 2^{20} (e.g., using Merkle authentication tree)
 - 1448 - MAC
 - 1449 - AEAD
- 1450 • The scheme's own verification circuit, with matching parameters, for recursive composition
(Proof-Carrying Data)
- 1451 • Range proofs [Freely chosen commitment scheme]
 - 1452 - Proof that number is in $[0, 2^{64})$
 - 1453 - Proof that number is positive
 - 1454 - Proof that number is positive
- 1455 • Proof of permutation (proving that two committed lists contain the same elements)

1456 3.6 Correctness and Trust

1457 In this section we explore the requirements for making the implementation of the proof system
 1458 trustworthy. Even if the mathematical scheme fulfills the claimed properties (e.g., it is proven
 1459 secure in the requisite sense, its assumptions hold and security parameters are chosen judiciously),
 1460 many things can go wrong in the subsequent implementation: code bugs, structured reference string
 1461 subversion, compromise during deployment, side channels, tampering attacks, etc. This section aims
 1462 to highlight such risks and offer considerations for practitioners.

1463 3.6.1 Considerations

1464 **Design of high-level protocol and statement.** The specification of the high-level protocol that
 1465 invokes the ZK proof system (and in particular, the NP statement to be proven in zero knowledge)
 1466 may fail to achieve the intended domain-specific security properties.

1467 Methodology for specifying and verifying these protocols is at its infancy, and in practice often relies
 1468 on manual review and proof sketches. Possible methods for attaining assurance include reliance on
 1469 peer-reviewed academic publications (e.g., Zerocash [BCGG+14] and Cinderella [DFKP16]) reuse of
 1470 high-level gadgets as discussed in the [Applications Track](#), careful manual specification and proving
 1471 of protocol properties by trained cryptographers, and emerging tools for formal verification.

1472 Whenever nontrivial optimizations are applied to a statement, such as algebraic simplification, or
 1473 replacement of an algorithm used in the original intended statement with a more efficient alternative,
 1474 those optimizations should be supported by proofs at an appropriate level of formality.

1475 See the [Applications Track](#) document for further discussion.

1476 **Choice of cryptographic primitives.** Traditional cryptographic primitives (hash functions,
 1477 PRFs, etc.) in common use are generally not designed for efficiency when implemented in circuits
 1478 for ZK proof systems. Within the past few years, alternative "circuit-friendly" primitives have

been proposed that may have efficiency advantages in this setting (e.g., LowMC and MiMC). We recommend a conservative approach to assessing the security of such primitives, and advise that the criteria for accepting them need to be as stringent as for the more traditional primitives.

Implementation of statement. The concrete implementation of the statement to be proven by the ZK proof system (e.g., as a Boolean circuit or an R1CS) may fail to capture the high-level specification. This risk increases if the statement is implemented in a low abstraction level, which is more prone to errors and harder to reason about.

The use of higher-level specifications and domain-specific languages (see the Front Ends section) can decrease the risk of this error, though errors may still occur in the higher-level specifications or in the compilation process.

Additionally, risk of errors often arises in the context of optimizations that aim to reduce the size of the statement (e.g., circuit size or number of R1CS constraints).

Note that correct statement semantics is crucial for security. Two implementations that use the same high-level protocol, same constraint system and compatible backends may still fail to correctly interoperate if their instance reductions (from high-level statement to the low-level input required by the backend) are incompatible – both in completeness (proofs don’t verify) or soundness (causing false but convincing proofs, implying a security vulnerability).

Side channels. Developers should be aware of the different processes in which side channel attacks can be detrimental and take measure to minimize the side channels. These include:

- SRS generation — in some schemes, randomly sampled elements which are discarded can be used, if exposed, to subvert the soundness of the system.
- Assignment generation / proving — the private auxiliary data can be exposed, which allows the attacker to understand the secret data used for the proof.

Auditing. First of all, circuit designers should provide a high-level description of their circuit and statement alongside the low-level circuit, and explain the connections between them.

The high-level description should facilitate auditing of the security properties of the protocol being implemented, and whether these match the properties intended by the designers or that are likely to be expected by users.

If the low-level description is not expressed directly in code, then the correspondence between the code and the description should be clear enough to be checked in the auditing process, either manually or with tool support.

A major focus of auditing the correctness and security of a circuit implementation will be in verifying that the low-level description matches the high-level one. This has several aspects, corresponding to the security properties of a ZK proof system:

- An instance for the low-level circuit must reveal no more information than an instance for the

1514 high-level statement. This is most easily achieved by ensuring that it is a canonical encoding
 1515 of the high-level instance.
 1516 • It must not be possible to find an instance and witness for the low-level circuit that does not
 1517 correspond to an instance and witness for the high-level statement.

1518 At all levels of abstraction, it is beneficial to use types to clarify the domains and representations
 1519 of the values being manipulated. Typically, a given proving system will not be able to *directly*
 1520 represent all of the types of value needed for a given high-level statement; instead, the values will
 1521 be encoded, for example as field elements in the case of R1CS-based proof systems. The available
 1522 operations on these elements may differ from those on the values they are representing; for instance,
 1523 field addition does not correspond to integer addition in the case of overflow.

1524 An adversary who is attempting to prove an instance of the statement that was not intended to be
 1525 provable, is not necessarily constrained to using instance and witness variables that correspond to
 1526 these intended representations. Therefore, close attention is needed to ensuring that the constraint
 1527 system explicitly excludes unintended representations.

1528 There is a wide space of design tradeoffs in how the frontend to a proof system can help to address
 1529 this issue. The frontend may provide a rich set of types suitable for directly expressing high-level
 1530 statements; it may provide only field elements, leaving representation issues to the frontend user;
 1531 it may provide abstraction mechanisms by which users can define new types; etc. Auditability of
 1532 statements expressed using the frontend should be a major consideration in this design choice.

1533 If the frontend takes a "gadget" approach to composition of statement elements, then it must be
 1534 clear whether each gadget is responsible for constraining the input and/or output variables to their
 1535 required types.

1536 **Testing.** Methods to test constraint systems include:

- 1537 - Testing for failure - does the implementation accept an assignment that should not be accepted?
- 1538 - Fuzzing the circuit inputs.
- 1539 - Finding missing constraints - e.g., missing boolean constraints on variables that represent bits,
 1540 or other missing type constraints.
- 1541 - Finding dead constraints, and reporting them (instead of optimising out).
- 1542 - Detection of unintended nondeterminism. For instance, given a partial fixed assignment, solve
 1543 for the remainder and check that there is only one solution.

1544 A proof system implementation can support testing by providing access, for test and debugging
 1545 purposes, to the reason why a given assignment failed to satisfy the constraints. It should also
 1546 support injection of values for instance and witness variables that would not occur in normal use
 1547 (e.g. because they do not represent a value of the correct type). These features facilitate “white
 1548 box testing”, i.e. testing that the circuit implementation rejects an instance and witness *for the*
 1549 *intended reason*, rather than incidentally. Without this support, it is difficult to write correct tests
 1550 with adequate coverage of failure modes.

3.6.2 SRS Generation

A prominent trust issue arises in proving systems which require a parameter setup process (structured reference string) that involves secret randomness. These may have to deal with scenarios where the process is vulnerable or expensive to perform security. We explore the real world social and technical problems that these setups must confront, such as air gaps, public verifiability, scalability, handing aborts, and the reputation of participants, and randomness beacons.

ZKP schemes require a URS (*uniform* reference string) or SRS (*structured* reference string) for their soundness and/or ZK properties. This necessitates suitable randomness sources and, in the case of a common reference string, a securely-executed setup algorithm. Moreover, some of the protocols create reference strings that can be reused across applications. We thus seek considerations for executing the setup phase of the leading ZKP scheme families, and for sharing of common resources. This section summarizes an open discussion made by the participants of the Implementation Track, aiming to provide considerations for practitioners to securely generate a CRS.

SRS subversion and failure modes. Constructing the SRS in a single machine might fit some scenarios. For example, this includes a scenario where the verifier is a single entity — the one who generates the SRS. In that scenario, an aspect that should be considered is subversion zero-knowledge — a property of proving schemes allowing to maintain zero-knowledge, even if the SRS is chosen maliciously by the verifier.

Strategies for subversion zero knowledge include:

- Using a multi-party computation to generate the SRS
- Adaptation of either [Gro16] [PHGR13]
- Updatable SRS - the SRS is generated once in a secure manner, and can then be specialized to many different circuits, without the need to re-generate the SRS

There are other subversion considerations which are discussed in the ZKProof [Security Track](#).

SRS generation using MPC In order to reduce the need of trust in a single entity generating the SRS, it is possible to use a multi-party computation to generate the SRS. This method should ideally be secure as long as one participant is honest (per independent computation phase). Some considerations to strengthen the security of the MPC include:

- Have as many participants as possible
 - Diversity of participants; reduce the chance they will collude
 - Diversity of implementations (curve, MPC code, compiler, operating system, language)
 - Diversity of hardware (CPU architecture, peripherals, RAM)
 - One-time-use computers
 - GCP / EC2 (leveraging enterprise security)
 - If you are concerned about your hardware being compromised, then avoid side channels (power, audio/radio, surveillance)
 - Hardware removal:
 - Remove WiFi/Bluetooth chip

- 1589 - Disconnect webcam / microphone / speakers
- 1590 - Remove hard disks if not needed, or disable swap
- 1591 - Air gaps
- 1592 [label=-]
- 1593 - Deterministic compilation
- 1594 - Append-only logs
- 1595 - Public verifiability of transcripts
- 1596 - Scalability
- 1597 - Handling aborts
- 1598 - Reputation
- 1599 - Information extraction from the hardware is difficult
- 1600 - Flash drives with hardware read-only toggle

1601 Some protocols (e.g., Powers of Tau) also require sampling unpredictable public randomness. Such
 1602 randomness can be harnessed from proof of work blockchains or other sources of entropy such as stock
 1603 markets. Verifiable Delay Functions can further reduce the ability to bias these sources [BBBF18]

1604 **SRS reusability** For schemes that require an SRS, it may be possible to design an SRS generation
 1605 process that allows the re-usability of a part of the SRS, thus reducing the attack surface. A good
 1606 example of it is the [Powers of Tau](#) method for the [Groth16](#) construction, where most of the SRS can
 1607 be reused before specializing to a specific constraint system.

1608 **Designated-verifier setting** There are cases where the verifier is a known-in-advance single
 1609 entity. There are schemes that excel in this setting. Moreover, schemes with public verifiability can
 1610 be specialized to this setting as well.

1611 3.6.3 Contingency plans

1612 We would like to explore in future workshops the notion of contingency plans. For example, how do
 1613 we cope:

- 1614 - With our proof system being compromised?
- 1615 - With our specific circuit having a bug?
- 1616 - When our ZKP protocol has been breached (identifying proofs with invalid witness, etc)

1617 Some ideas that were discussed and can be expanded on are:

- 1618 - Scheme-agility and protocol-agility in protocols - when designing the system, allow flexibility
 1619 for the primitives used
- 1620 - Combiners (using multiple proof systems in parallel) - to reduce the reliance on a single proof
 1621 system, use multiple
- 1622 - Discuss ways to identify when ZKP protocol has been breached (identifying proofs with invalid
 1623 witness, etc)

3.7 Extended Constraint-System Interoperability

The following are stronger forms of interoperability which have been identified as desirable by practitioners, and are to be addressed by the ongoing standardization effort.

3.7.1 Statement and witness formats

In the R1CS File Format section and associated resources, we define a file format for R1CS constraint systems. There remains to finalize this specification, including instances and witnesses. This will enable users to have their choice of frameworks (frontends and backends) and streaming for storage and communication, and facilitate creation of benchmark test cases that could be executed by any backend accepting these formats.

Crucially, analogous formats are desired for constraint system languages other than R1CS.

3.7.2 Statement semantics, variable representation & mapping

Beyond the above, there's a need for different implementations to coordinate the semantics of the statement (instance) representation of constraint systems. For example, a high-level protocol may have an RSA signature as part of the statement, leaving ambiguity on how big integers modulo a constant are represented as a sequence of variables over a smaller field, and at what indices these variables are placed in the actual R1CS instance.

Precise specification of statement semantics, in terms of higher-level abstraction, is needed for interoperability of constraint systems that are invoked by several different implementations of the instance reduction (from high-level statement to the actual input required by the ZKP prover and verifier). One may go further and try to reuse the actual implementation of the instance reduction, taking a high-level and possibly domain-specific representation of values (e.g., big integers) and converting it into low-level variables. This raises questions of language and platform incompatibility, as well as proper modularization and packaging.

Note that correct statement semantics is crucial for security. Two implementations that use the same high-level protocol, same constraint system and compatible backends may still fail to correctly interoperate if their instance reductions are incompatible – both in completeness (proofs don't verify) or soundness (causing false but convincing proofs, implying a security vulnerability). Moreover, semantics are a requisite for verification and helpful for debugging.

Some backends can exploit uniformity or regularity in the constraint system (e.g., repeating patterns or algebraic structure), and could thus take advantage of formats and semantics that convey the requisite information.

At the typical complexity level of today's constraint systems, it is often acceptable to handle all of the above manually, by fresh re-implementation based on informal specifications and inspection of prior implementation. We expect this to become less tenable and more error prone as application complexity grows.

3.7.3 Witness reduction

Similar considerations arise for the witness reduction, converting a high-level witness representation (for a given statement) into the assignment to witness variables. For example, a high-level protocol may use Merkle trees of particular depth with a particular hash function, and a high-level instance may include a Merkle authentication path. The witness reduction would need to convert these into witness variables, that contain all of the Merkle authentication path data (encoded by some particular convention into field elements and assigned in some particular order) and moreover the numerous additional witness variables that occur in the constraints that evaluate the hash function, ensure consistency and Booleanity, etc.

The witness reduction is highly dependent on the particular implementation of the constraint system. Possible approaches to interoperability are, as above: formal specifications, code reuse and manual ad hoc compatibility.

3.7.4 Gadgets interoperability

At a finer grain than monolithic constraint systems and their assignments, there is need for sharing subcircuits and gadgets. For example, libsnark offers a rich library of highly optimized R1CS gadgets, which developers of several front-end compilers would like to reuse in the context of their own constraint-system construction framework.

While porting chunks of constraints across frameworks is relatively straightforward, there are challenges in coordinating the semantics of the externally-visible variables of the gadget, analogous to but more difficult than those mentioned above for full constraint systems: there is a need to coordinate or reuse the semantics of a gadget's externally-visible variables, as well as to coordinate or reuse the witness reduction function of imported gadgets in order to convert a witness into an assignment to the internal variables.

As for instance semantics, well-defined gadget semantics is crucial for soundness, completeness and verification, and is helpful for debugging.

3.7.5 Procedural interoperability

An attractive approach to the aforementioned needs for instance and witness reductions (both at the level of whole constraint systems and at the gadget level) is to enable one implementation to invoke the instance/witness reductions of another, even across frameworks and programming languages.

This requires communication not of mere data, but invocation of procedural code. Suggested approaches to this include linking against executable code (e.g., .so files or .dll), using some elegant and portable high-level language with its associated portable, or using a low-level portable executable format such as WebAssembly. All of these require suitable calling conventions (e.g., how are field elements represented?), usage guidelines and examples.

Beyond interoperability, some low-level building blocks (e.g., finite field and elliptic curve arithmetic) are needed by many or all implementations, and suitable libraries can be reused. To a large extent

1695 this is already happening, using the standard practices for code reuse using native libraries. Such
1696 reused libraries may offer a convenient common ground for consistent calling conventions as well.

1697 3.7.6 Proof interoperability

1698 Another desired goal is interoperability between provers and verifiers that come from different
1699 implementations, i.e., being able to independently write verifiers that make consistent decisions and
1700 being able to re-implement provers while still producing proofs that convince the old verifier.

1701 This is especially pertinent in applications where proofs are posted publicly, such as in the context
1702 of blockchains (see the Applications Track document), and multiple independent implementations
1703 are desired for both provers and verifiers.

1704 To achieve such interoperability between provers and verifiers, they must agree on all of the following:

- 1705 • ZK proof system (including fixing all degrees of freedom, such as choice of finite fields and
1706 elliptic curves)
- 1707 • Instance and witness formats (see above subsection)
- 1708 • Prover parameters formats
- 1709 • Verifier parameters formats
- 1710 • Proof formats
- 1711 • A precise specification of the constraint system (e.g., R1CS) and corresponding instance and
1712 witness reductions (see above subsection).

1713 Alternatively: a precise high-level specification along with a precisely-specified, deterministic frontend
1714 compilation.

1715 3.7.7 Common reference strings

1716 There is also a need for standardization regarding Common Reference String (CRS), i.e., prover
1717 parameters and verifier parameters. First, interoperability is needed for streaming formats (com-
1718 munication and storage), and would allow application developers to easily switch between different
1719 implementations, with different security and performance properties, to suit their need. Moreover,
1720 for Structured Reference Strings (SRS), there are nontrivial semantics that depend on the ZK proof
1721 system and its concrete realization by backends, as well as potential for partial reuse of SRS across
1722 different circuits in some schemes (e.g., the Powers of Tau protocol).

1723 3.8 Future goals

1724 3.8.1 Interoperability

1725 Many additional aspects of interoperability remain to be analyzed and supported by standards,
1726 to support additional ZK proof system backends as well as additional communication and reuse
1727 scenarios. Work has begun on multiple fronts both, and a dedicated public [mailing list](#) is established.

Additional forms of interoperability. As discussed in the Extended Constraint-System Interoperability section above, even within the R1CS realm, there are numerous additional needs beyond plain constraint systems and assignment representations. These affect security, functionality and ease of development and reuse.

Additional relation styles. The R1CS-style constraint system has been given the most focus in the Implementation Track discussions in the first workshop, leading to a file format and an API specification suitable for it. It is an important goal to discuss other styles of constraint systems, which are used by other ZK proof systems and their corresponding backends. This includes arithmetic and Boolean circuits, variants thereof which can exploit regular/repeating elements, as well as arithmetic constraint satisfaction problems.

Recursive composition. The technique of recursive composition of proofs, and its abstraction as Proof-Carrying Data (PCD) [CT10][BCTV14], can improve the performance and functionality of ZK proof systems in applications that deal with multi-stage computation or large amounts of data. This introduces additional objects and corresponding interoperability considerations. For example, PCD compliance predicates are constraint systems with additional conventions that determine their semantics, and for interoperability these conventions require precise specification.

Benchmarks. We strive to create concrete reference benchmarks and reference platforms, to enable cross-paper milliseconds comparisons and competitions.

We seek to create an open competition with well-specified evaluation criteria, to evaluate different proof schemes in various well-defined scenarios.

3.8.2 Frontends and DSLs

We would like to expand the discussion on the areas of domain-specific languages, specifically in aspects of interoperability, correctness and efficiency (even enabling source-to-source optimisation).

The goal of Gadget Interoperability, in the Extended Constraint-System Interoperability section, is also pertinent to frontends.

3.8.3 Verification of implementations

We would to discuss the following subjects in future workshops, to assist in guiding towards best practices: formal verification, auditing, consistency tests, etc.

List of references: [BBBF18], [BCGG+14], [BCGTV13], [BCTV14], [CT10], [DFKP16], [Gro16], [GGPR13b], [PHGR13].

Chapter 4. Applications

4.1 Introduction and Motivation

In this track we aim to overview existing techniques for building ZKP based systems, including designing the protocols to meet the best-practice security requirements. One can distinguish between high-level and low-level applications, where the former are the protocols designed for specific use-cases and the latter are the underlying operations needed to define a ZK predicate. We call gadgets the sub-circuits used to build the actual constraint system needed for a use-case. In some cases, a gadget can be interpreted as a security requirement (e.g.: using the commitment verification gadget is equivalent to ensuring the privacy of underlying data).

As we will see, the protocols can be abstracted and generalized to admit several use-cases; similarly, there exist compilers that will generate the necessary gadgets from commonly used programming languages. Creating the constraint systems is a fundamental part of the applications of ZKP, which is the reason why there is a large variety of front-ends available.

In this document, we present three use-cases and a set of useful gadgets to be used within the predicate of each of the three use-cases: identity framework, asset transfer and regulation compliance.

The design of ZKPs is subject to the tradeoff between functionality and performance. Users would like to have powerful ZKPs, in the sense that the system permits constructing proofs for any predicate, which leads to the necessity of universal ZKPs. On the other hand, users would like to have efficient constructions. According to Table 3.1, it is possible to classify ZKPs as: (i) universal or non-universal; (ii) scalable or non-scalable; and (iii) preprocessing or non-preprocessing. Item (i) is related to the functionality of the underlying ZKP, while items (ii) and (iii) are related to performance. The utilization of zk-SNARKs allows universal ZKPs with very efficient verifiers. However, most proposals depend upon an expensive preprocessing, which makes such systems hard to scale for some use-cases. A technique called *Proof-Carrying Data* (PCD), originally proposed in Ref. [CT10], allows obtaining *recursive composition* for existing ZKPs in a modular way. This means that zk-SNARKs can be used as a building block to construct scalable and non-preprocessing solutions. The result is not only an efficient verifier, as in zk-SNARKs, but also a prover whose consumption of computational resources is efficient, in particular with respect to memory requirements, as described in Refs. [BCTV17] and [BCCT13].

What this document is NOT about:

- A unique explanation of how to build ZKP applications
- An exhaustive list of the security requirements needed to build a ZKP system
- A comparison of front-end tools
- A show of preference for some use-cases or others

4.2 Notation and Definitions

See [Security](#) and [Implementation](#) tracks for definitions of predicate / prover / verifier / proof / proving key, etc.

When designing ZK based applications, one needs to keep in mind which of the following three models (that define the functionality of the ZKP) is needed:

1. Publicly verifiable as a requirement: a scheme / use-case where the proofs are transferable, where such property is actually a requirement of the system. E36: D7.2
2. Designated verifier as a security feature: only the intended receiver of the proof can verify it, making the proof non-transferable. This property can apply to both interactive and non-interactive ZK.
3. The final model is one where neither of the above is needed: a ZK where there is no need to be able to transfer but also no non-transferability requirement. Again, this model can apply both in the interactive and non-interactive model.

For example, digital money based applications belong to the first model, compliance for regulation lives in the second model (albeit depending on the use-case). In general, the credential system can be in both of the last two models, given the extra constraints that would make it belong to the second model.

4.3 Previous works

This section will include an overview of some of the works and applications existing in the zero-knowledge world. We asked the Applications track participants to send us a description of their work. We are now in the process of collecting the content.

4.4 Gadgets within predicates

Formalizing the security of these protocols is a very difficult task, especially since there is no predetermined set of requirements, making it an ad-hoc process. Here we outline a set of initial gadgets to be taken into account. See Table 4.1 for a simple list of gadgets — this list should be expanded continuously and on a case by case basis. For each of the gadgets we write the following representations, specifying what is the secret / witness, what is public / statement:

NP statements for non-technical people:


**For the [public] chess board configurations A and B ;
I know some [secret] sequence S of chess moves;
such that when starting from configuration A , and applying S , all moves are
legal and the final configuration is B .**

1821 General form (Camenisch-Stadler): $\mathbf{Zk} \{ (wit): P(wit, statement) \}$

1822 Example of ring signature: $\mathbf{Zk} \{ (sig): \text{VerifySignature}(P1, sig) \text{ or } \text{VerifySignature}(P2, sig) \}$

1824 **Table 4.1:** List of gadgets

E37: D19.1


#	Gadget name	English description of the initial gadget (before adding ZKP)	Table with examples
G1	Commitment	Envelope 	Table 4.2
G2	Signatures	Signature authorization letter	Table 4.3
G3	Encryption	Envelope with a receiver stamp	Table 4.4
G4	Distributed decryption	Envelope with a receiver stamp that requires multiple people to open	Table 4.5
G5	Random function	Lottery machine	Table 4.6
G6	Set membership	Whitelist/blacklist	Table 4.7
G7	Mix-net	Ballot box	Table 4.8
G8	Generic circuits, TMs, or RAM programs	General calculations	Table 4.9

1834 4.5 Identity framework

1835 4.5.1 Overview

1836 In this section we describe identity management solutions using zero knowledge proofs. The idea is
 1837 that some user has a set of attributes that will be attested to by an issuer or multiple issuers, such
 1838 that these attestations correspond to a validation of those attributes or a subset of them.

1839 After attestation it is possible to use this information, hereby called a credential, to generate a claim
 1840 about those attributes. Namely, consider the case where Alice wants to show that she is over 18
 1841 and lives in a country that belongs to the European Union. If two issuers were responsible for the
 1842 attestation of Alice's age and residence country, then we have that Alice could use zero knowledge
 1843 proofs in order to show that she possesses those attributes, for instance she can use zero knowledge
 1844 range proofs to show that her age is over 18, and zero knowledge set membership to prove that she
 1845 lives in a country that belongs to the European Union. This proof can be presented to a Verifier
 1846 that must validate such proof to authorize Alice to use some service. Hence there are three parties
 1847 involved: (i) the credential holder; (ii) the credential issuer; (iii) and the verifier.

Table 4.2: Commitment gadget (G1; envelope) 

Enhanced gadget (after adding ZKP)	ZKP statement (in a PoK notation)	Prover knows a witnessfor the public instances.t. the following predicate holds	Technical notation (API)
I know the value hidden inside this envelope, even though I cannot change it	Knowledge of committed value(s) (openings)	Opening(s) $O = (v, r)$ containing a value and randomness	Committed value(s) C	$C = Comm(O)$, component-wise if there are multiple C, O	
I know that the value hidden inside these two envelopes are equal	Equality of committed values	Opening O	Committed values C_1 and C_2	$C_1 = Comm(O)$ and $C_2 = Comm(O)$	
I know that the values hidden inside these two envelopes are related in a specific way	Relationships between committed values – logical, arithmetic, etc.	Witnesses O_1 and O_2	Committed values C_1 and C_2 , relation R	$C_1 = Comm(O_1)$, $C_2 = Comm(O_2)$, and $R(O_1, O'_2) = \mathbf{True}$	
The value inside this envelope is within a particular range	Range proofs	Opening O	Committed value C , interval I	$C = Comm(O)$ and O is in the range I	

E38: D19.1

Table 4.3: Signature gadget (G2; signature authorization letter)

Enhanced gadget (after adding ZKP)	ZKP statement (in a PoK notation)	Prover knows a witnessfor the public instances.t. the following predicate holds	Technical notation (API)
Secret valid signature over commonly known message	Knowledge of a secret signature σ on a commonly known message M	Signature σ	Verification key VK , message M	$\text{Verify}(VK, M, \sigma) = \text{True}$	
Secret valid signature over committed message	Knowledge of a secret signature σ on a commonly known commitment C of a secret message M	Opening O , signature σ	Verification key VK , committed value C	$C = \text{Comm}(M)$ and $\text{Verify}(VK, M, \sigma) = \text{True}$	

E39: D19.1

Table 4.4: Encryption gadget (G3; envelope with a receiver stamp)

Enhanced gadget (after adding ZKP)	ZKP statement (in a PoK notation)	Prover knows a witnessfor the public instances.t. the following predicate holds	Technical notation (API)
The output plaintext(s) correspond to the public ciphertext(s).	Knowledge of a secret plaintext M	Secret decryption key SK	Ciphertext(s) C and Encryption key PK	$\text{Dec}(SK, C) = M$, component-wise if \exists multiple C and M	

Table 4.5: Distributed-decryption gadget (G4; envelope with a receiver stamp that requires multiple people to open)

Enhanced gadget (after adding ZKP)	ZKP statement (in a PoK notation)	Prover knows a witnessfor the public instances.t. the following predicate holds	Technical notation (API)
The output plaintext(s) correspond to the public ciphertext(s).	Knowledge of a secret plaintext M	Secret shares $[SK_i]$ of the decryption key SK	Ciphertext(s) C and Encryption key PK	$SK = \text{Derive}([SK_i])$ and $\text{Dec}(SK, C) = M$, component-wise if \exists multiple C	

Table 4.6: Random-function gadget (G5; lottery machine)

Enhanced gadget (after adding ZKP)	ZKP statement (in a PoK notation)	Prover knows a witnessfor the public instances.t. the following predicate holds	Technical notation (API)
Verifiable random function (VRF)	VRF was computed correctly from a secret seed and a public (or secret) input	Secret seed W	Input X , Output Y	$Y = \text{VRF}(W, X)$	


E41: D19.1

Table 4.7: Set-membership gadget (G6; whitelist/blacklist)

Enhanced gadget (after adding ZKP)	ZKP statement (in a PoK notation)	Prover knows a witnessfor the public instances.t. the following predicate holds	Technical notation (API)
Accumulator	Set inclusion	Secret element X	Public set S	$X \in S$	
Universal accumulator	Set non-inclusion	Secret element X	Public set S	$X \notin S$	
Merkle Tree	Element occupies a certain position within the vector	Secret element X	Public vector V	$X = V[i]$ for some i	

Table 4.8: Mix-net gadget (G7; ballot box)

Enhanced gadget (after adding ZKP)	ZKP statement (in a PoK notation)	Prover knows a witnessfor the public instances.t. the following predicate holds	Technical notation (API)
Shuffle	The set of plaintexts in the input and the output ciphertexts respectively are identical.	Permutation π , Decryption key SK	Input ciphertext list C and Output ciphertext list C'	$\forall j, Dec(SK, \pi(C_j)) = Dec(SK, C'_j)$	
Shuffle and reveal	The set of plaintexts in the input ciphertexts is identical to the set of plaintexts in the output.	Permutation π , Decryption key SK	Input ciphertext list C and Output plaintext list P	$\forall j, Dec(SK, \pi(C_j)) = P_j$	

Table 4.9: Generic circuits, TMs, or RAM programs  gadgets (G8; general calculations)

Enhanced gadget (after adding ZKP)	ZKP statement (in a PoK notation)	Prover knows a witnessfor the public instances.t. the following predicate holds	Technical notation (API)
There exists some secret input that makes this calculation correct	ZK proof of correctness of circuit/Turing machine/RAM program computation	Secret input w	Program C (either a circuit, TM, or RAM program), public input x , output y	$C(x, w) = y$	
This calculation is correct, given that I already know that some sub-calculation is correct	ZK proof of verification + post-processing of another output (Composition)	Secret input w	Program C with subroutine C' , public input x , output y , intermediate value $z = C'(x, w)$, zk proof π that $z = C'(x, w)$	$C(x, w) = y$	

We are going to focus our description on a specific use case: accredited investors. In this scenario the credential holder will be able to show that she is accredited without revealing more information than necessary to prove such a claim.

4.5.2 Motivation for Identity and Zero Knowledge

Digital identity has been a problem of interest to both academics and industry practitioners since the creation of the internet. Specifically, it is the problem of allowing an individual, a company, or an asset to be identified online without having to generate a physical identification for it, such as an ID card, a signed document, a license, etc. Digitizing Identity comes with some unique risks, loss of privacy and consequent exposure to Identity theft, surveillance, social engineering and other damaging efforts. Indeed, this is something that has been solved partially, with the help of cryptographic tools to achieve moderate privacy (password encryption, public key certificates, internet protocols like TLS and several others). Yet, these solutions are sometimes not enough to meet the privacy needs to the users / identities online. Cryptographic zero knowledge proofs can further enhance the ability to interact digitally and gain both privacy and the assurance of legitimacy required for the correctness of a process.

The following is an overview of the generalized version of the identity scheme. We define the terminology used for the data structures and the actors, elaborate on what features we include and what are the privacy assurances that we look for.

4.5.3 Terminology / Definitions

In this protocol we use several different data structures to represent the information being transferred or exchanged between the parties. We have tried to generalize the definitions as much as possible, while adapting to the existing Identity standards and previous ZKP works.

Attribute. The most fundamental information about a holder in the system (e.g.: age, nationality, univ. Degree, pending debt, etc.). These are the properties that are factual and from which specific authorizations can be derived.

(Confidential and Anonymous) Credential. The data structure that contains attribute(s) about a holder in the system (e.g.: credit card statement, marital status, age, address, etc). Since it contains private data, a credential is not shareable.

(Verifiable) Claim. A zero-knowledge predicate about the attributes in a credential (or many of them). A claim must be done about an identity and should contain some form of logical statement that is included in the constraint system defined by the zk-predicate.

Proof of Credential. The zero knowledge proof that is used to verify the claim attested by the credential. Given that the credential is kept confidential, the proof derived from it is presented as a way to prove the claim in question.

1916 The following are the different parties present in the protocol:

1917 **Holder.** The party whose attributes will be attested to. The holder holds the credentials that
 1918 contain his / her attributes and generates Zero Knowledge Proofs to prove some claim about these.
 1919 We say that the holder presents a proof of credential for some claim.

1920 **Issuer.** The party that attests attributes of holders. We say that the issuer issues a credential to
 1921 the holder.

1922 **Verifier.** The party that verifies some claim about a holder by verifying the zero knowledge proof
 1923 of credential to the claim.

1924

1925 Remark: The main difference between this protocol and a non-ZK based Identity protocol is the
 1926 fact that in the latter, the holder presents the credentials themselves as the proof for the claim
 1927 / authorization, whereas in this protocol, the holder presents a zero knowledge proof that was
 1928 computed from the credentials.

1929 4.5.4 The Protocol Description

1930 **Functionality.** There are many interesting features that we considered as part of the identity
 1931 protocol. There are four basic functionalities that we decided to include from the get go:

- 1932 (1) third party anonymous and confidential attribute attestations through **credential issuance**
 1933 by the issuer;
- 1934 (2) confidentially proving claims using zero knowledge proofs through the **presentation of proof**
 1935 **of credential** by the holder;
- 1936 (3) **verification of claims** through zero knowledge proof verification by the verifier; and
- 1937 (4) unlinkable **credential revocation** by the issuer.

1938 There are further functionalities that we find interesting and worth exploring but that we did not
 1939 include in this version of the protocol. Some of these are credential transfer, authority delegation
 1940 and trace auditability. We explain more in detail what these are and explore ways they could be
 1941 instantiated.

1942 **Privacy requirements.** One should aim for a high level of privacy for each of the actors in
 1943 the system, but without compromising the correctness of the protocol. We look at anonymity
 1944 properties for each of the actors, confidentiality of their interactions and data exchanges, and
 1945 at the unlinkability of public data (in committed form). These usually can be instantiated as
 1946 cryptographic requirements such as commitment non-malleability, indistinguishability from random
 1947 data, unforgeability, accumulator soundness or as statements in zero-knowledge such as proving
 1948 knowledge of preimages, proving signature verification, etc.

- 1949 • Holder anonymity: the underlying physical identity of the holder must be hidden from the
 1950 general public, and if needed from the issuer and verifier too. For this we use pseudo-random
 1951 strings called identifiers, which are tied to a secret only known to the holder.
- 1952 • Issuer anonymity: only the holder should know what issuer issued a specific credential.

- Anonymous credential: when a holder presents a credential, the verifier may not know who issued the certificate. He / She may only know that the credential was issued by some approved issuer.
- Holder untraceability: the holder identifiers and credentials can't be used to track holders through time.
- Confidentiality: no one but the holder and the issuer should know what the credential attributes are.
- Identifier linkability: no one should be able to link two identifier unless there is a proof presented by the holder.
- Credential linkability: No one should be able to link two credentials from the publicly available data. Mainly, no two issuers should be able to collude and link two credentials to one same holder by using the holder's digital identity.

In depth view. For the specific instantiation of the scheme, we examine in Table 4.10 the different ways that these requirements can be achieved and what are the trade-offs to be done (e.g.: using pairwise identifiers vs. one fixed public key; different revocation mechanisms; etc.) and elaborate on the privacy and efficiency properties of each.

Gadgets. Each of the methods for instantiating the different functionalities use some of the following gadgets that have been described in the Gadgets section. There are three main parts to the predicate of any proof.

1. The first is proving the veracity of the identity, in this case the holder, for which the following gadgets can / should be used:
 - **Commitment** for checking that the identity has been attested to correctly.
 - **PRF** for proving the preimage of the identifier is known by the holder
 - **Equality of strings** to prove that the new identifier has a connection to the previous identifier used or to an approved identifier.
2. Then there is the part of the constraint system that deals with the legitimacy of the credentials, the fact that it was correctly issued and was not revoked.
 - **Commitment** for checking that the credential was correctly committed to.
 - **PRF** for proving that the holder knows the credential information, which is the preimage of the commitment .
 - **Equality of strings** to prove that the credential was issued to an identifier connected to the current identifier.
 - **Accumulators (Set membership / non-membership)** to prove that the commitment to the credential exists in some set (usually an accumulator), implying that it was issued correctly and that it was not revoked.
3. Finally there is the logic needed to verify the rules / constraints imposed on the attributes themselves. This part can be seen as a general gadget called “credentials”, which allows to verify the specific attributes embedded in a credential. Depending on the credential type, it uses the following low level gadgets:
 - **Data Type** used to check that the data in the credential is of the correct type

Table 4.10: Functionalities vs. privacy and robustness requirements

Functionality / Problem	Instantiation Method	Proof Details	Privacy / Robustness	Reference
Holder identification: how to identify a holder of credentials	Single identifier in the federated realm: PRF based Public Key (idPK) derived from the physical ID of the entity and attested / onboarded by a federal authority	<ul style="list-style-type: none"> The first credential an entity must get is the onboarding credential that attests to its identity on the system Any proof of credential generated by the holder must include a verification that the idPK was issued an onboarding credential 	<ul style="list-style-type: none"> Physical identity is hidden yet connected to the public key. Issuers can collude to link different credentials by the same holder. An entity can have only one identity in the system 	
	Single identifier in the self-sovereign realm: PRF based Public Key (idPK) self derived by the entity.	<ul style="list-style-type: none"> Any proof of credential must show the holder knows the preimage of the idPK and that the credential was issued to the idPK in question 	<ul style="list-style-type: none"> Physical identity is hidden and does not necessarily have to be connected to the public key Issuers can collude to link different credentials by the same holder An entity can have several identities and conveniently forget any of them upon issuance of a “negative credential” 	
	Multiple identifiers: Pairwise identification through identifiers. For each new interaction the holder generates a new identifier.	<ul style="list-style-type: none"> Every time a holder needs to connect to a previous issuer, it must prove a connection of the new and old identifiers in ZK Any proof of credential must show the holder knows the secret of the identifier that the credential was issued to. 	<ul style="list-style-type: none"> Physical identity is hidden and does not necessarily have to be connected to the public key Issuers cannot collude to link the credentials by the same holder An entity can have several identities and conveniently forget any of them upon issuance of a “negative credential” 	

2000	Issuer identification	Federated permissions: there is a list of approved issuers that can be updated by either a central authority or a set of nodes	<ul style="list-style-type: none"> – To accept a credential one must validate the signature against one from the list. To maintain the anonymity of the issuer, ring signatures can be used – For every proof of credential, a holder must prove that the signature in its credential is of an issuer in the approved list 	<ul style="list-style-type: none"> – The verifier / public would not know who the issuer of the credential is but would know it is approved. 	
2001		Free permissions: anyone can become an issuer, which use identifiers: <ul style="list-style-type: none"> – Public identifier: type 1 is the issuer whose signature verification key is publicly available – Pair-wise identifiers: type 2 is the issuer whose signature verification key can be identified only pair-wise with the holder / verifier 	<ul style="list-style-type: none"> – The credentials issued by type 1 issuers can be used in proofs to unrelated parties – The credentials issued by type 2 issuers can only be used in proofs to parties who know the issuer in question. 	<ul style="list-style-type: none"> – If ring signatures are used, the type one issuer identifiers would not imply that the identity of the issuer can be linked to a credential, it would only mean that “Key K_a belongs to company A” – Otherwise, only the type two issuers would be anonymous and unlinkable to credentials 	
2002	Credential issuance	Is- Blind signatures: the issuer signs on a commitment of a self-attested credential after seeing a proof of correct attestation; a second kind of proof would be needed in the system	<ul style="list-style-type: none"> – The proof of correct attestation must contain the structure, data types, ranges and credential type that the issuer allows – In some cases, the proof must contain verification of the attributes themselves (e.g.: address is in Florida, but not know the city) * The proof of credential must not be accepted if the signature of the credential was not verified either in zero-knowledge or as part of some public verification 	<ul style="list-style-type: none"> – Issuer’s signatures on credentials add limited legitimacy: a holder could add specific values / attributes that are not real and the issuer would not know – An Issuer can collude with a holder to produce blind signatures without the issuer being blamed 	

2003		In the clear signatures: the issuer generates the attestation, signing the commitment and sending the credential in the clear to the holder	<ul style="list-style-type: none"> The proof of credential must not be accepted if the signature of the credential was not verified either in zero-knowledge or as part of some public verification 	<ul style="list-style-type: none"> Issuer must be trusted, since she can see the Holder's data and could share it with others The signature of the issuer can be trusted and blame could be allocated to the issuer 	
2004	Credential Revocation	Positive accumulator revocation: the issuer revokes the credential by removing an element from an accumulator	<ul style="list-style-type: none"> The holder must prove set membership of a credential to prove it was issued and was not revoked at the same time The issuer can revoke a credential by removing the element that represents it from the accumulator 	<ul style="list-style-type: none"> If the accumulator is maintained by a central authority, then only the authority can link the revocation to the original issuance, avoiding timing attacks by general parties (join-revoke linkability) If the accumulator is maintained through a public state, then there can be linkability of revocation with issuance since one can track the added values and test its membership 	[CDD17]
2005		Negative accumulator revocation: the issuer revokes by adding an element to an accumulator	<ul style="list-style-type: none"> The holder must prove set membership of a credential to prove it was issued The issuer can revoke a credential by adding to the negative accumulator the revocation secret related to the credential to be revoked The holder must prove set non-membership of a revocation secret associated to the credential in question The verifier must use the most recent version of the accumulator to validate the claim 	<ul style="list-style-type: none"> Even when the accumulator is maintained through a public state, the revocation cannot be linked to the issuance since the two events are independent of each other 	

- 1993 • **Range Proofs** used to check that the data in the credential is within some range
- 1994 • **Arithmetic Operations (field arithmetic, large integers, etc.)** used for verifying
- 2006 arithmetic operations were done correctly in the computation of the instance.
- 2007 • **Logical Operators (bigger than, equality, etc.)** used for comparing some value in
- 2008 the instance to the data in the credentials or some computation derived from it.

2009 Security caveats

- 2010 1. If the Issuer colludes with the Verifier, they could use the revocation mechanism to reveal
- 2011 information about the Holder if there is real-time sharing of revocation information.
- 2012 2. Furthermore, if the commitments to credentials and the revocation information can be tracked
- 2013 publicly and the events are dependent of each other (e.g.: revocation by removing a commit-
- 2014 ment), then there can be linkability between issuance and revocation.
- 2015 3. In the case of self-attestation or collusion between the issuer and the holder, there is a much
- 2016 lower assurance of data integrity. The inputs to the ZKP could be spoofed and then the proof
- 2017 would not be sound.
- 2018 4. The use of Blockchains create a reliance on a trusted oracle for external state. On the other
- 2019 hand, the privacy guaranteed at blockchain-content level is orthogonal to network-level traffic
- 2020 analysis.

2021 4.5.5 A use-case example of credential aggregation

2022 **Use-case description.** As a way to illustrate the above protocol, we present a specific use-case
 2023 and explicitly write the predicate of the proof. Mainly, there is an identity, Alice, who wants to
 2024 prove to some company, Bob Inc. that she is an accredited investor, under the SEC rules, in order
 2025 to acquire some company shares. Alice is the prover; the IRS, the AML entity and The Bank are all
 2026 issuers; and Bob Inc. is the verifier.

2027 The different processes in the adaptation of the use-case are the following:

- 2028 1. Three confidential credentials are issued to Alice which represent the rules that we apply on
- 2029 an entity to be an accredited investor¹:
- 2030 (a) The IRS issues a tax credential, C_0 , that testifies to the claim “from 1/1/2017 until
- 2031 1/1/2018, Alice, with identifier X_0 , owes 0\$ to the IRS, with identifier Y ” and holds two
- 2032 attributes: the net income of Alice, \$income, and a bit b such that $b = 1$ if Alice has paid
- 2033 her taxes.
- 2034 (b) The AML entity issues a KYC credential, C_1 , that testifies to claim $T_1 :=$ “Alice, with
- 2035 identifier X_1 , has NO relation to a (set of) blacklisted organization(s)”
- 2036 (c) The Bank issues a net-worth credential, C_2 , that testifies to claim $T_2 :=$ “Alice has a net
- 2037 worth of V_{Alice} ”

¹We assume that the SEC generates the constraint system for the accreditation rules as the circuit used to generate the proving and verification keys. In the real scenario, here are the [Federal Rules for accreditation](#).

2. Alice then proves to Bob Inc. that:

- (a) “Alice’s identifier, X_{Bob} , is related to the identifiers, X_i for $i = 0, 1, 2$ that are connected to the confidential credentials C_i ”
- (b) “I know the credentials, which are the preimage of some commitment, C_i , were issued by the legitimate issuers”
- (c) “The credentials, which are the preimage of some commitment, C_i , that exist in an accumulator, U , satisfy the three statements T_i ”

Instantiation details. Based on the different options laid out in the table above, the following have been used:

- Holder identification: we instantiate the identifiers as a unique anonymous identifier, `publicKey`
- Issuance identification: the identity of the issuers is known to all the participants, who can publicly verify the signature on the credentials they issue².
- Credential issuance: credentials are issued by publishing a signed commitment to a positive accumulator and sharing the credential in the clear to Alice.
- Credential revocation: is done by removing the commitment of credential from a dynamic and positive accumulator. Alice must prove membership of commitment to show her credential was not revoked.
- Credential verification: Bob Inc. then verifies the cryptographic proof with the instance.

Note that the transfer of company shares as well as the issuance of company shares is outside of the scope of this use-case, but one could use the “Asset Transfer” section of this document to provide that functionality.

On another note, the fact that the proving and verification keys were validated by the SEC is an assurance to Bob Inc. that proof verification implies Alice is an accredited investor.

The Predicate

- Blue = publicly visible in protocol / statement
- Red = secret witness, potentially shared between parties when proving

Definitions / Notation:

Public state: **Accumulator**, for issuance and revocation, which includes all the commitments to the credentials.

ConfCred = Commitment to Cred = { **Revoke**, **certificateType**, **publicKey**, **Attribute(s)** }

Where, again, the IRS, AML and Bank are authorities with well-known public keys. Alice’s **publicKey** is her long term public key and one cannot create a new credential unless her long term ID has

²With public signature verification keys that are hard coded into the circuit

2071 been endorsed. The goal of the scheme is for the holder to create a fresh **proof of confidential**
 2072 **aggregated credentials to the claim of accredited investor.**


2073 IRS issues a $\text{ConfCred}_{\text{IRS}} = \text{Commitment}(\text{openIRS}, \text{revokeIRS}, \text{"IRS"}, \text{myID}, \$\text{Income}, b), \text{sigIRS}$
 2074 AML issues $\text{ConfCred}_{\text{AML}} = \text{Commitment}(\text{openAML}, \text{revokeAML}, \text{"AML"}, \text{myID}, \text{"OK"}, \text{sigAML})$

2075 Holder generates a fresh public key freshCred to serve as an ephemeral blinded aggregate credential,
 2076 and a ZKP of the following:

2077 $\text{ZkPoK}\{ (\text{witness: } \text{myID}, \text{ConfCred}_{\text{IRS}}, \text{ConfCred}_{\text{AML}}, \text{sigIRS}, \text{sigAML}, \$\text{Income}, , \text{mySig}, \text{openIRS},$
 2078 $\text{openAML} \text{ statement: } \text{freshCred}, \text{minIncomeAccredited}) : \text{Predicate:}$

- 2079 - $\text{ConfCred}_{\text{IRS}}$ is a commitment to the IRS credential $(\text{openIRS}, \text{"IRS"}, \text{myID}, \$\text{Income})$
- 2080 - $\text{ConfCred}_{\text{AML}}$ is the AML credential to $(\text{openAML}, \text{"AML"}, \text{myID}, \text{"OK"})$
- 2081 - $\$\text{Income} \geq \text{minIncomeAccredited}$
- 2082 - $b = 1 = \text{"myID paid full taxes"}$
- 2083 - mySig is a signature on freshCred for myID
- 2084 - $\text{ProveNonRevoke}()$

2085 }

2086 Present the credential to relying party:  freshCred and zpk .

2087 $\text{ProveNonRevoke}(\text{rhIRS}, \text{w_hrIRS}, \text{rhAML}, \text{w_hrAML}, \text{a_IRS})$

- 2088 • revokeIRS : revocation handler from IRS. Can be embedded as an attribute in $\text{ConfCred}_{\text{IRS}}$
 2089 and is used to handle revocations.
- 2090 • $\text{wit}_{\text{rhIRS}}$: accumulator witness of revokeIRS .
- 2091 • revokeAML : revocation handler from AML. Can be embedded as an attribute in $\text{ConfCred}_{\text{AML}}$
 2092 and is used to handle revocations.
- 2093 • $\text{wit}_{\text{rhAML}}$: accumulator witness of revokeAML .
- 2094 • acc_{IRS} : accumulator for IRS.
- 2095 • $\text{CommRevoke}_{\text{IRS}}$: commitment to revokeIRS . The holder generates a new commitment for
 2096 each revocation to avoid linkability of proofs.
- 2097 • acc_{AML} : accumulator for AML.
- 2098 • $\text{CommRevoke}_{\text{AML}}$: commitment to revokeAML . The holder generates a new commitment for
 2099 each revocation to avoid linkability of proofs.

2100 $\text{ZkPoK}\{ (\text{witness: } \text{rhIRS}, \text{open}_{\text{rhIRS}}, \text{w}_{\text{rhIRS}}, \text{rhAML}, \text{open}_{\text{rhAML}}, \text{w}_{\text{rhAML}} || \text{statements: } \text{C}_{\text{IRS}}, \text{a}_{\text{IRS}},$
 2101 $\text{C}_{\text{AML}}, \text{a}_{\text{AML}}) : \text{Predicate:}$

- 2102 - C_{IRS} is valid commitment to $(\text{open}_{\text{rhIRS}}, \text{rhIRS})$
- 2103 - rhIRS is part of accumulator a_{IRS} , under witness w_{rhIRS}
- 2104 - rhIRS is an attribute in Cert_{IRS}
- 2105 - C_{AML} is valid commitment to $(\text{open}_{\text{rhAML}}, \text{rhAML})$
- 2106 - rhAML is part of accumulator a_{AML} , under witness w_{rhAML}
- 2107 - rhAML is an attribute in Cert_{AML}

2108 }

- 2109 - myCred is unassociated with myID, with sigIRS, sigAML etc.
- 2110 - Withstands partial compromise: even if IRS leaks myID and sigIRS, it cannot be used to
- 2111 reveal the sigAML or associated myID with myCred

2112 4.6 Asset Transfer

2113 4.6.1 Privacy-preserving asset transfers and balance updates

2114 In this section, we examine two use-cases involving using ZK Proofs (ZKPs) to facilitate private
 2115 asset-transfer for transferring fungible or non-fungible digital assets. These use-cases are motivated
 2116 by privacy-preserving cryptocurrencies, where users must prove that a transaction is valid, without
 2117 revealing the underlying details of the transaction. We explore two different frameworks, and outline
 2118 the technical details and proof systems necessary for each.

2119 There are two dominant paradigms for tracking fungible digital assets, tracking ownership of assets
 2120 individually, and tracking account balances. The Bitcoin system introduced a form of asset-tracking
 2121 known as the UTXO model, where Unspent Transaction Outputs correspond roughly to single-use
 2122 “coins”. Ethereum, on the other hand, uses the balance model, and each account has an associated
 2123 balance, and transferring funds corresponds to decrementing the sender’s balance, and incrementing
 2124 the receiver’s balance accordingly.

2125 These two different models have different privacy implications for users, and have different rules for
 2126 ensuring that a transaction is valid. Thus the requirements and architecture for building ZK proof
 2127 systems to facilitate privacy-preserving transactions are slightly different for each model, and we
 2128 explore each model separately below.

2129 In its simplest form, the asset-tracking model can be used to track non-fungible assets. In this
 2130 scenario, a transaction is simply a transfer of ownership of the asset, and a transaction is valid if:
 2131 the sender is the current owner of the asset. In the balance model (for fungible assets), each account
 2132 has a balance, and a transaction decrements the sender’s account balance while simultaneously
 2133 incrementing the receivers. In a “balance” model, a transaction is valid if 1) The amount the sender’s
 2134 balance is decremented is equal to the amount the receiver’s balance is incremented, 2) The sender’s
 2135 balance remains non-negative 3) The transaction is signed using the sender’s key.

2136 4.6.2 Zero-Knowledge Proofs in the asset-tracking model

2137 In this section, we describe a simple ZK proof system for privacy-preserving transactions in the
 2138 asset-tracking (UTXO) model. The architecture we outline is essentially a simplification of the
 2139 ZCash system. The primary simplification is that we assume that each asset (“coin”) is indivisible.
 2140 In other words, each asset has an owner, but there is no associated value, and a transaction is simply
 2141 a transfer of ownership of the asset.

2142 **Motivation:** Allow stakeholders to transfer non-fungible assets, without revealing the ownership of
 2143 the assets publicly, while ensuring that assets are never created or destroyed.

Parties: There are three types of parties in this system: a Sender, a Receiver and a distributed set of validators. The sender generates a transactions and a proof of validity. The (distributed) validators act as verifiers and check the validity of the transaction. The receiver has no direct role, although the sender must include the receiver’s public-key in the transaction.

What is being proved: At high level, the sender must prove three things to convince the validators that a transaction is valid.

- The asset (or “note”) being transferred is owned by the sender. (Each asset is represented by a unique string)
- The sender proves that they have the private spending keys of the input notes, giving them the authority to send asset.
- The private spending keys of the input assets are cryptographically linked to a signature over the whole transaction, in such a way that the transaction cannot be modified by a party who did not know these private keys.

What information is needed by the verifier:

- The verifiers need access to the CRS used by the proof system
- The validators need access to the entire history of transactions (this includes all UTXOs, commitments and nullifiers as described later). This history can be stored on a distributed ledger (e.g. the Bitcoin blockchain)

Possible attacks:

- CRS compromise: If an attacker learns the private randomness used to generate the CRS, the attacker can forge proofs in the underlying system
- Ledger attacks: validating a transaction requires reading the entire history of transactions, and thus a verifier with an incorrect view of the transaction history may be convinced to accept an incorrect transaction as valid.
- Re-identification attacks: The purpose of incorporating ZKPs into this system is to facilitate transactions without revealing the identities of the sender and receiver. If anonymity is not required, ZKPs can be avoided altogether, as in Bitcoin. Although this system hides the sender and receiver of each transaction, the fact that a transaction occurred (and the time of its occurrence) is publicly recorded, and thus may be used to re-identify individual users.
- IP-level attacks: by monitoring network traffic, an attacker could link transactions to specific senders or receivers (each transaction requires communication between the sender and receiver) or link public-keys (pseudonyms) to real-world identities
- Man-it-the-Middle attacks: An attacker could convince a sender to transfer an asset to an “incorrect” public-key

Setup scenario: This system is essentially a simplified version of Zcash proof system, modified for indivisible assets. Each asset is represented by a unique AssetID, and for simplicity we assume that the entire set of assets has been distributed, and no assets are ever created or destroyed.

At any given time, the public state of the system consists of a collection of “asset notes”. These notes are stored as leaves in a Merkle Tree, and each leaf represents a single indivisible asset represented by unique assetID. In more detail, a “note” is a commitment to Nullifier, publicKey, assetID, indicating that publicKey “owns” assetID.

2185 **Main transaction type:** Sending an asset from Current Owner A to New Owner B

2186 **Security goals:**

- 2187 • Only the current owner can transfer the asset
- 2188 • Assets are never created or destroyed

2189 **Privacy goals:** Ideally, the system should hide all information about the ownership and transaction
 2190 patterns of the users. The system sketched below does not attain that such a high-level of privacy,
 2191 but instead achieves the following privacy-preserving features

- 2192 • Transactions are publicly visible, i.e., anyone can see that a transaction occurred
- 2193 • Transactions do not reveal which asset is being transferred
- 2194 • Transactions do not reveal the identities (public-keys) of the sender or receiver.
 - 2195 – Limitation: Previous owner can tell when the asset is transferred. (Mitigation: after
 - 2196 receiving asset, send it to yourself)

2197 **Details of a transfer:** Each transaction is intended to transfer ownership of an asset from a
 2198 Current Owner to a New Owner. In this section, we outline the proofs used to ensure the validity of
 2199 a transaction. Throughout this description, we use **Blue** to denote information that is globally and
 2200 **publicly** visible in the protocol / statement. We use **Red** to denote **private** information, e.g. a secret
 2201 witness held by the prover or information shared between the Current Owner and New Owner.

2202 The Current Owner, A , has the following information

- 2203 • A **publicKey** and corresponding **secretKey**
- 2204 • An **assetID** corresponding to the asset being transferred
- 2205 • A **note** in the MerkleTree corresponding to the asset
- 2206 • Knows how to open the **commitment** (**Nullifier**, **assetID**, **publicKey**) **publicKeyOut** of the new
- 2207 Owner B

2208 The Current Owner, A , generates

- 2209 • A new **NullifierOut**
- 2210 • A new commitment **commitment** (**NullifierOut**, **assetID**, **publicKey**)

2211 The Current owner, A , sends

- 2212 • Privately to B : **NullifierOut**, **publicKeyOut**, **assetID**
- 2213 • Publicly to the blockchain: **Nullifier**, **comOut**, **ZKProof** (the structure of **ZKProof** is outlined
- 2214 below)

2215 If **Nullifier** does not exist in **MerkleTree** and **ZKProof** validates, then **comOut** is added to the
 2216 merkleTree.

2217 **The structure of the Zero-Knowledge Proof:** We use a modification of Camenisch-Stadler
 2218 notation to describe the structure of the proof.

2219 Public state: MerkleTree of Notes: Note = Commitment to { Nullifier, publicKey, assetID }

2220 ZKProof = ZkPoK_{pp}{
 2221 (witness: publicKey, publicKeyOut, merkleProof, NullifierOut, com, assetID, sig
 2222 statement: MerkleTree, Nullifier, comOut) :
 2223 predicate:
 2224 - com is included in MerkleTree (using merkleProof)
 2225 - com is a commitment to (Nullifier, publicKey, assetID)
 2226 - comOut is a commitment to (NullifierOut, publicKeyOut, assetID)
 2227 - sig is a signature on comOut for publicKey
 2228 }

2229 4.6.3 Zero-Knowledge proofs in the balance model

2230 In this section, we outline a simple system for privately transferring fungible assets, in the “balance
 2231 model.” This system is essentially a simplified version of zkLedger. The state of the system is an
 2232 (encrypted) account balance for each user. Each account balance is encrypted using an additively
 2233 homomorphic cryptosystem, under the account-holder’s key. A transaction decrements the sender’s
 2234 account balance, while incrementing the receiver’s account by a corresponding amount. If the number
 2235 of users is fixed, and known in advance, then a transaction can hide all information about the sender
 2236 and receiver by simultaneously updating all account balances. This provides a high-degree of privacy,
 2237 and is the approach taken by zkLedger. If the set of users is extremely large, dynamically changing,
 2238 or unknown to the sender, the sender must choose an “anonymity set” and the transaction will reveal
 2239 that it involved members of the anonymity set, but not the amount of the transaction or which
 2240 members of the set were involved. For simplicity of presentation, we assume a model like zkLedger’s
 2241 where the set of parties in the system is fixed, and known in advance, but this assumption does not
 2242 affect the details of the zero-knowledge proofs involved.

2243 **Motivation:** Each entity maintains a private account balance, and a transaction decrements the
 2244 sender’s balance and increments the receiver’s balance by a corresponding amount. We assume that
 2245 every transaction updates every account balance, thus all information the origin, destination and
 2246 value of a transaction will be completely hidden. The only information revealed by the protocol is
 2247 the fact that a transaction occurred.

2248 Parties:

- 2249 • A set of n stakeholders who wish to transfer fungible assets anonymously
- 2250 • The stakeholder who initiates the transaction is called the “prover” or the “sender”
- 2251 • The receiver, or receivers do not have a distinguished role in a transaction
- 2252 • A set of validators who maintain the (public) state of the system (e.g. using a blockchain or
 2253 other DLT).

2254 **What is being proved:** The sender must convince the validators that a proposed transaction is

2255 “valid” and the state of the system should be updated to reflect the new transaction. A transaction
 2256 consists of a set of n ciphertexts, (c_1, \dots, c_n) , and where $c_i = \text{Enc}_{pk}(x_i)$, and a transaction is valid if:

- 2257 • The sum of all committed values is 0 (i.e., $x_1 + \dots + x_n = 0$)
- 2258 • The sender owns the private key corresponding to all negative x_i
- 2259 • After the update, all account balances remain positive

2260 What information is needed by the verifier:

- 2261 • The verifiers need access to the CRS used by the proof system
- 2262 • The verifiers need access to the current state of the system (i.e., the current vector of n
 2263 encrypted account balances). This state can be stored on a distributed ledger

2264 Possible attacks:

- 2265 • CRS compromise: If an attacker learns the private randomness used to generate the CRS, the
 2266 attacker can forge proofs in the underlying system
- 2267 • Ledger attacks: validating a transaction requires knowing the current state of the system
 2268 (encrypted account balances), thus a validator with an incorrect view of the current state may
 2269 be convinced to accept an incorrect transaction as valid.
- 2270 • Re-identification attacks: The purpose of incorporating ZKPs into this system is to facilitate
 2271 transactions without revealing the identities of the sender and receiver. If anonymity is not
 2272 required, ZKPs can be avoided altogether, as in Bitcoin. Although this system hides the sender
 2273 and receiver of each transaction, the fact that a transaction occurred (and the time of its
 2274 occurrence) is publicly recorded, and thus may be used to re-identify individual users.
- 2275 • IP-level attacks: by monitoring network traffic, an attacker could link transactions to specific
 2276 senders or receivers (each transaction requires communication between the sender and the
 2277 validators) or link public-keys (pseudonyms) to real-world identities
- 2278 • Man-it-the-Middle attacks: An attacker could convince a sender to transfer an asset to an
 2279 “incorrect” public-key. This is perhaps less of a concern in the situation where the user-base is
 2280 static, and all public-keys are known in advance.

2281 **Setup scenario:** There are fixed number of users, n . User i has a known public-key, pk_i . Each
 2282 user has an account balance, maintained as an additively homomorphic encryption of their current
 2283 balance under their pk . Each transaction is a list of n encryptions, corresponding to the amount
 2284 each balance should be incremented or decremented by the transaction. To ensure money is never
 2285 created or destroyed, the plaintexts in an encrypted transaction must sum to 0. We assume that all
 2286 account balance are initialized to non-negative values.

2287 **Main transaction type:** Transferring funds from user i to user j

2288 **Security goals:**

- 2289 • An account balance can only be decremented by the owner of that account
- 2290 • Account balances always remain non-negative
- 2291 • The total amount of money in the system remains constant

2292 **Privacy goals:** Ideally, the system should hide all information about the ownership and transaction
 2293 patterns of the users. The system sketched below does not attain that such a high-level of privacy,
 2294 but instead achieves the following privacy-preserving features:

- 2295 • Transactions are publicly visible, i.e., anyone can see that a transaction occurred
- 2296 • Transactions do not reveal which asset is being transferred
- 2297 • Transactions do not reveal the identities (public-keys) of the sender or receiver.
- 2298 Limitation: transaction times are leaked

2299 **Details of a transfer:** Each transaction is intended to update the current account balances in
 2300 the system. In this section, we outline the proofs used to ensure the validity of a transaction.
 2301 Throughout this description, we use Blue to denote information that is globally and publicly visible
 2302 in the protocol / statement. We use Red to denote private information, e.g. a secret witness held by
 2303 the prover.

2304 The Sender, A , has the following information

- 2305 • Public keys pk_1, \dots, pk_n
- 2306 • secretKey_i corresponding to publicKey_i , and a values x_j , to transfer to user j
- 2307 • The sender's own current account balance, y_i

2308 The Sender, A , generates

- 2309 • a vector of ciphertexts, C_1, \dots, C_n with $C_t = \text{Enc}_{pk_t}(x_t)$

2310 The Sender, A , sends

- 2311 • The vector of ciphertexts C_1, \dots, C_n and ZKProof (described below) to the blockchain

2312 ZK Circuit:

2313 Public state: The current state of the system, i.e., a vector of (encrypted) account balances,
 2314 B_1, \dots, B_n .

2315 $\text{ZKProof} = \text{ZkPoK}_{\text{pp}}\{$ (witness: i, x_1, \dots, x_n, sk statement: C_1, \dots, C_n) :

2316 predicate:

- 2317 - C_t is an encryption to x_t under public key pk_t for $t = 1, \dots, n$
- 2318 - $x_1 + \dots + x_n = 0$
- 2319 - $x_t \geq 0$ OR sk corresponds to pk_t for $t = 1, \dots, n$
- 2320 - $x_t \geq 0$ OR current balance B_t encrypts a value no smaller than $|x_t|$ for $t = 1, \dots, n$

2321 }

4.7 Regulation Compliance

4.7.1 Overview

An important pattern of applications in which zero-knowledge protocols are useful is within settings in which a regulator wishes to monitor, or assess the risk related to some item managed by a regulated party. One such example can be whether or not taxes are being paid correctly by an account holder, or is a bank or some other financial entity solvent, or even stable.

The regulator in such cases is interested in learning “the bottom line”, which is typically derived from some aggregate measure on more detailed underlying data, but does not necessarily need to know all the details. For example, the answer to the question of “did the bank take on too many loans?” Is eventually answered by a single bit (Yes/No) and can be answered without detailing every single loan provided by the bank and revealing recipients, their income, and other related data.

Additional examples of such scenarios include:

- Checking that taxes have been properly paid by some company or person.
- Checking that a given loan is not too risky.
- Checking that data is retained by some record keeper (without revealing or transmitting the data)
- Checking that an airplane has been properly maintained and is fit to fly

The use of Zero knowledge proofs can then allow the generation of a proof that demonstrate the correctness of the aggregate result. The idea is to show something like the following statement: There is a commitment (possibly on a blockchain) to records that show that the result is correct.

Trusting data fed into the computation: In order for a computation on hidden data to prove valuable, the data that is fed in must be grounded as well. Otherwise, proving the correctness of the computation would be meaningless. To make this point concrete: A credit score that was computed from some hidden data can be correctly computed from some financial records, but when these records are not exposed to the recipient of the proof, how can the recipient trust that they are not fabricated?

Data that is used for proofs should then generally be committed to by parties that are separate from the prover, and that are not likely to be colluding with the prover. To continue our example from before: an individual can prove that she has a high credit score based on data commitments that were produced by her previous lenders (one might wonder if we can indeed trust previous lenders to accurately report in this manner, but this is in fact an assumption implicitly made in traditional credit scoring as well).

The need to accumulate commitments regarding the operation and management of the processes that are later audited using zero-knowledge often fits well together with blockchain systems, in which commitments can be placed in an irreversible manner. Since commitments are hiding, such publicly shared data does not breach privacy, but can be used to anchor trust in the veracity of the data.

4.7.2 An example in depth: Proof of compliance for aircraft

An operator is flying an aircraft, and holds a log of maintenance operations on the aircraft. These records are on different parts that might be produced by different companies. Maintenance and flight records are attested to by engineers at various locations around the world (who we assume do not collude with the operator).

The regulator wants to know that the aircraft is allowed to fly according to a certain set of rules. (Think of the Volkswagen emissions cheating story.)

The problem: Today, the regulator looks at the records (or has an auditor do so) only once in a while. We would like to move to a system where compliance is enforced in “real time”, however, this reveals the real-time operation of the aircraft if done naively.

Why is zero-knowledge needed? We would like to prove that regulation is upheld, without revealing the underlying operational data of the aircraft which is sensitive business operations. Regulators themselves prefer not to hold the data (liability and risk from loss of records), prefer to have companies self-regulate to the extent possible.

What is the threat model beyond the engineers/operator not colluding? What about the parts manufacturers? Regulators? Is there an antagonistic relationship between the parts manufacturers?

This scheme will work on regulation that isn’t vague, such as aviation regulation. In some cases, the rules are vague on purpose and leave room for interpretation.

4.7.3 Protocol high level

Parties:

- Operator / Party under regulation: performs operations that need to comply to a regulation. For example an airline operator that operates aircrafts
- Risk bearer / Regulator : verifies that all regulated parties conform to the rules; updates the rules when risks evolve. For example, the FAA regulates and enforces that all aircrafts to be airworthy at all times. For an aircraft owner leasing their assets, they want to know that operation and maintenance does not degrade their asset. Same for a bank that financed an aircraft, where the aircraft is the collateral for the financing.
- Issuer / 3rd party attesting to data: Technicians having examined parts, flight controllers attesting to plane arriving at various locations, embarked equipment providing signed readings of sensors.

What is being proved:

- The operator proves to the regulator that the latest maintenance data indicates the aircraft is airworthy
- The operator proves to the bank that the aircraft maintenance status means it is worth a given value, according to a formula provided by that bank

What are the privacy requirements?

- 2394 • An operator does not want to reveal the details of his operations and assets maintenance status
- 2395 to competition
- 2396 • The aircraft identity must be kept anonymous from all parties except the regulators and the
- 2397 technicians.
- 2398 • The technician's identity must be kept anonymous from the regulator but if needed the operator
- 2399 can be asked to open the commitments for the regulator to validate the reports

2400 **The proof predicate:** “The operator is the owner of the aircraft, and knows some signed data

2401 attesting to the compliance with regulation rules: all the components are safe to fly”.

- 2402 • The plane is made up of the components x_1, \dots, x_n and for each of the components:
- 2403 – There is an legitimate attestation by an engineer who checked the component, and signed
- 2404 it's OK
- 2405 – The latest attestation by a technician is recent: the timestamp of the check was done
- 2406 before date D

2407 **What is the public / private data:**

- 2408 • Private:
- 2409 – Identity of the operator
- 2410 – Airplane record
- 2411 – Examination report of the technicians
- 2412 – Identity of the technician who signed the report
- 2413 • Public:
- 2414 – Commitment to airplane record
- 2415 –

2416 There is a record for the airplane that is committed to a public ledger, which includes miles flown.

2417 There are records that attest to repairs / inspections by mechanics that are also committed to the

2418 ledger. The decommitment is communicated to the operator. These records reference the identifier

2419 of the plane.

2420 Whenever the plane flies, the old plane record needs to be invalidated, and a new one committed

2421 with extra mileage.

2422 When a proof of “airworthiness” is required, the operator proves that for each part, the mileage

2423 is below what requires replacement, or that an engineer replaced the part (pointing to a record

2424 committed by a technician).

2425 **At the gadget level:**

- 2426 • The prover proves knowledge of a de-commitment of an airplane record (decommitment)
- 2427 • The record is in the set of records on the blockchain (set membership)
- 2428 • and knowledge of de-commitments for records for the parts (decommitment) that are also in
- 2429 the set of commitments on the ledger (set membership)
- 2430 • The airplane record is not revoked (i.e., it is the most recent one), (requires set non-membership
- 2431 for the set of published nullifiers)
- 2432 • The id of the plane noted in the parts is the same as the id of the plane in the plane record.
- 2433 (equality)
- 2434 • The mileage of the plane is lower than the mileage needed to replace each part (range proofs)

2435 OTHERWISE

- 2436 • There exists a record (set membership) that says that the part was replaced by a technician
2437 (validate signature of the technician (maybe use ring signature outside of ZK?))

2438 4.8 Conclusions

- 2439 – The asset transfer and regulation can be used in the identity framework in a way that the
2440 additions complete the framework.
2441 – External oracles such as blockchain used for storing reference to data commitments

2442 **List of references:** FHE standards [ACCG+17], ZERO CASH [BCGG+14], Baby-zoe [zca18],
2443 HAWK []; ZKledger [NVV18]. Other identity references: SovrinTM [Sov18], [BCDE+14], [CDD17],
2444 [BCDL+17] (mentioned in Table 4.10), [CKS10].

References

- [AHIV17] S. Ames, C. Hazay, Y. Ishai, and M. Venkitasubramaniam. “Ligero: Lightweight Sublinear Arguments Without a Trusted Setup”. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’17. ACM, 2017, pp. 2087–2104. DOI: [10.1145/3133956.3134104](https://doi.org/10.1145/3133956.3134104).
- [ACCG+17] D. Archer, L. Chen, J. H. Cheon, R. Gilad-Bachrach, R. A. Hallman, Z. Huang, X. Jiang, R. Kumaresan, B. A. Malin, H. Sofia, Y. Song, and S. Wang. *Applications of Homomorphic Encryption*. Tech. rep. 2017. http://homomorphicecryption.org/white_papers/applications_homomorphic_encryption_white_paper.pdf.
- [BCDL+17] F. Baldimtsi, J. Camenisch, M. Dubovitskaya, A. Lysyanskaya, L. Reyzin, K. Samelin, and S. Yakoubov. “Accumulators with Applications to Anonymity-Preserving Revocation”. In: *2017 IEEE European Symposium on Security and Privacy (EuroS P)*. Apr. 2017, pp. 301–315. DOI: [10.1109/EuroSP.2017.13](https://doi.org/10.1109/EuroSP.2017.13). IACR Cryptology Eprint Archive: ia.cr/2017/043.
- [BCGG+14] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. “Zerocash: Decentralized Anonymous Payments from Bitcoin”. In: *2014 IEEE Symposium on Security and Privacy*. May 2014, pp. 459–474. DOI: [10.1109/SP.2014.36](https://doi.org/10.1109/SP.2014.36). <http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf>.
- [BCGT13] E. Ben-Sasson, A. Chiesa, D. Genkin, and E. Tromer. “On the Concrete Efficiency of Probabilistically-checkable Proofs”. In: *Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing*. STOC ’13. ACM, 2013, pp. 585–594. DOI: [10.1145/2488608.2488681](https://doi.org/10.1145/2488608.2488681).
- [BCGTV13] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza. “SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge”. In: *Advances in Cryptology – CRYPTO 2013*. Ed. by R. Canetti and J. A. Garay. Springer Berlin Heidelberg, 2013, pp. 90–108. DOI: [10.1007/978-3-642-40084-1_6](https://doi.org/10.1007/978-3-642-40084-1_6). IACR Cryptology Eprint Archive: ia.cr/2013/507.
- [BCS16] E. Ben-Sasson, A. Chiesa, and N. Spooner. “Interactive Oracle Proofs”. In: *Theory of Cryptography*. Ed. by M. Hirt and A. Smith. Springer Berlin Heidelberg, 2016, pp. 31–60. DOI: [10.1007/978-3-662-53644-5_2](https://doi.org/10.1007/978-3-662-53644-5_2). IACR Cryptology Eprint Archive: ia.cr/2016/116.
- [BCTV14] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza. “Scalable Zero Knowledge via Cycles of Elliptic Curves”. In: *Advances in Cryptology – CRYPTO 2014*. Ed. by J. A. Garay and R. Gennaro. Springer Berlin Heidelberg, 2014, pp. 276–294. DOI: [10.1007/978-3-662-44381-1_16](https://doi.org/10.1007/978-3-662-44381-1_16). IACR Cryptology Eprint Archive: ia.cr/2014/595.
- [BCTV17] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza. “Scalable Zero Knowledge Via Cycles of Elliptic Curves”. In: *Algorithmica* 79.4 (Dec. 2017), pp. 1102–1160. DOI: [10.1007/s00453-016-0221-0](https://doi.org/10.1007/s00453-016-0221-0).
- [BCDE+14] P. Bichsel, J. Camenisch, M. Dubovitskaya, R. R. Enderlein, S. Krenn, I. Krontiris, A. Lehmann, G. Neven, J. D. Nielsen, C. Paquin, F.-S. Preiss, K. Rannenberg, A. Sabouri, and M. Stausholm. *D2.2 - Architecture for Attribute-based Credential Technologies - Final Version*. Ed. by A. Sabour. Aug. 2014. https://abc4trust.eu/download/Deliverable_D2.2.pdf.

- 2488 [BCCT13] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer. “Recursive Composition and
2489 Bootstrapping for SNARKS and Proof-carrying Data”. In: *Proceedings of the Forty-
2490 fifth Annual ACM Symposium on Theory of Computing*. STOC ’13. ACM, 2013,
2491 pp. 111–120. DOI: [10.1145/2488608.2488623](https://doi.org/10.1145/2488608.2488623).
- 2492 [BCIOP13] N. Bitansky, A. Chiesa, Y. Ishai, R. Ostrovsky, and O. Paneth. “Succinct Non-
2493 interactive Arguments via Linear Interactive Proofs”. In: *Theory of Cryptography*.
2494 Ed. by A. Sahai. Springer Berlin Heidelberg, 2013, pp. 315–333. DOI: [10.1007/978-3-
2495 642-36594-2_18](https://doi.org/10.1007/978-3-642-36594-2_18). IACR Cryptology Eprint Archive: ia.cr/2012/718.
- 2496 [BBBF18] D. Boneh, J. Bonneau, B. Bünz, and B. Fisch. “Verifiable Delay Functions”. In:
2497 *Advances in Cryptology – CRYPTO 2018*. Ed. by H. Shacham and A. Boldyreva.
2498 Springer International Publishing, 2018, pp. 757–788. IACR Cryptology Eprint
2499 Archive: ia.cr/2018/601.
- 2500 [BISW17] D. Boneh, Y. Ishai, A. Sahai, and D. J. Wu. “Lattice-Based SNARGs and Their Ap-
2501 plication to More Efficient Obfuscation”. In: *Advances in Cryptology – EUROCRYPT
2502 2017*. Ed. by J.-S. Coron and J. B. Nielsen. Springer International Publishing, 2017,
2503 pp. 247–277. DOI: [10.1007/978-3-319-56617-7_9](https://doi.org/10.1007/978-3-319-56617-7_9). IACR Cryptology Eprint Archive:
2504 ia.cr/2017/240.
- 2505 [BCCGP16] J. Bootle, A. Cerulli, P. Chaidos, J. Groth, and C. Petit. “Efficient Zero-Knowledge
2506 Arguments for Arithmetic Circuits in the Discrete Log Setting”. In: *Advances in
2507 Cryptology – EUROCRYPT 2016*. Ed. by M. Fischlin and J.-S. Coron. Springer
2508 Berlin Heidelberg, 2016, pp. 327–357. DOI: [10.1007/978-3-662-49896-5_12](https://doi.org/10.1007/978-3-662-49896-5_12). IACR
2509 Cryptology Eprint Archive: ia.cr/2016/263.
- 2510 [BCGGHJ17] J. Bootle, A. Cerulli, E. Ghadafi, J. Groth, M. Hajiabadi, and S. K. Jakobsen. “Linear-
2511 Time Zero-Knowledge Proofs for Arithmetic Circuit Satisfiability”. In: *Advances
2512 in Cryptology – ASIACRYPT 2017*. Ed. by T. Takagi and T. Peyrin. Springer
2513 International Publishing, 2017, pp. 336–365. DOI: [10.1007/978-3-319-70700-6_12](https://doi.org/10.1007/978-3-319-70700-6_12).
2514 IACR Cryptology Eprint Archive: ia.cr/2017/872.
- 2515 [BCGJM18] J. Bootle, A. Cerulli, J. Groth, S. Jakobsen, and M. Maller. “Arya: Nearly Linear-Time
2516 Zero-Knowledge Proofs for Correct Program Execution”. In: *Advances in Cryptology
2517 – ASIACRYPT 2018*. Ed. by T. Peyrin and S. Galbraith. Springer International
2518 Publishing, 2018, pp. 595–626. DOI: [10.1007/978-3-030-03326-2_20](https://doi.org/10.1007/978-3-030-03326-2_20).
- 2519 [CDD17] J. Camenisch, M. Drijvers, and M. Dubovitskaya. “Practical UC-Secure Delegatable
2520 Credentials with Attributes and Their Application to Blockchain”. In: *Proceedings
2521 of the 2017 ACM SIGSAC Conference on Computer and Communications Security*.
2522 CCS ’17. ACM, 2017, pp. 683–699. DOI: [10.1145/3133956.3134025](https://doi.org/10.1145/3133956.3134025).
- 2523 [CKS10] J. Camenisch, M. Kohlweiss, and C. Soriente. “Solving Revocation with Efficient
2524 Update of Anonymous Credentials”. In: *Security and Cryptography for Networks*.
2525 Ed. by J. A. Garay and R. De Prisco. Springer Berlin Heidelberg, 2010, pp. 454–471.
2526 DOI: [10.1007/978-3-642-15317-4_28](https://doi.org/10.1007/978-3-642-15317-4_28).
- 2527 [CCHL+19] R. Canetti, Y. Chen, J. Holmgren, A. Lombardi, G. N. Rothblum, R. D. Rothblum,
2528 and D. Wichs. “Fiat-Shamir: From Practice to Theory”. In: *Proceedings of the 51st
2529 Annual ACM SIGACT Symposium on Theory of Computing*. STOC 2019. ACM,
2530 2019, pp. 1082–1090. DOI: [10.1145/3313276.3316380](https://doi.org/10.1145/3313276.3316380).

References

- [CT10] A. Chiesa and E. Tromer. “Proof-Carrying Data and Hearsay Arguments from Signature Cards”. In: *Innovations in Computer Science — ICS 2010*. Vol. 10. 2010, pp. 310–331.
- [CD98] R. Cramer and I. Damgård. “Zero-knowledge proofs for finite field arithmetic, or: Can zero-knowledge be for free?” In: *Advances in Cryptology — CRYPTO ’98*. Ed. by H. Krawczyk. Springer Berlin Heidelberg, 1998, pp. 424–441. DOI: [10.1007/BFb0055745](https://doi.org/10.1007/BFb0055745).
- [DFKP16] A. Delignat-Lavaud, C. Fournet, M. Kohlweiss, and B. Parno. “Cinderella: Turning Shabby X.509 Certificates into Elegant Anonymous Credentials with the Magic of Verifiable Computation”. In: *2016 IEEE Symposium on Security and Privacy (SP)*. May 2016, pp. 235–254. DOI: [10.1109/SP.2016.22](https://doi.org/10.1109/SP.2016.22).
- [GGPR13a] R. Gennaro, C. Gentry, B. Parno, and M. Raykova. “Quadratic Span Programs and Succinct NIZKs without PCPs”. In: *Advances in Cryptology – EUROCRYPT 2013*. Ed. by T. Johansson and P. Q. Nguyen. Springer Berlin Heidelberg, 2013, pp. 626–645. DOI: [10.1007/978-3-642-38348-9_37](https://doi.org/10.1007/978-3-642-38348-9_37). IACR Cryptology Eprint Archive: ia.cr/2012/215.
- [GGPR13b] R. Gennaro, C. Gentry, B. Parno, and M. Raykova. “Quadratic Span Programs and Succinct NIZKs without PCPs”. In: *Advances in Cryptology – EUROCRYPT 2013*. Ed. by T. Johansson and P. Q. Nguyen. Springer Berlin Heidelberg, 2013, pp. 626–645. DOI: [10.1007/978-3-642-38348-9_37](https://doi.org/10.1007/978-3-642-38348-9_37). IACR Cryptology Eprint Archive: ia.cr/2012/215.
- [GMO16] I. Giacomelli, J. Madsen, and C. Orlandi. “ZKBoo: Faster Zero-Knowledge for Boolean Circuits”. In: *25th USENIX Security Symposium (USENIX Security 16)*. USENIX Association, 2016, pp. 1069–1083.
- [Gol13] O. Goldreich. “A Short Tutorial of Zero-Knowledge”. In: *Secure Multi-Party Computation*. Ed. by M. M. Prabhakaran and A. Sahai. Vol. 10. Cryptology and Information Security Series. 2013, pp. 28–60. DOI: [10.3233/978-1-61499-169-4-28](https://doi.org/10.3233/978-1-61499-169-4-28).
- [GKR15] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum. “Delegating Computation: Interactive Proofs for Muggles”. In: *J. ACM* 62.4 (Sept. 2015), 27:1–27:64. DOI: [10.1145/2699436](https://doi.org/10.1145/2699436).
- [Gro10] J. Groth. “Short Non-interactive Zero-Knowledge Proofs”. In: *Advances in Cryptology - ASIACRYPT 2010*. Ed. by M. Abe. Springer Berlin Heidelberg, 2010, pp. 341–358. DOI: [10.1007/978-3-642-17373-8_20](https://doi.org/10.1007/978-3-642-17373-8_20).
- [Gro16] J. Groth. “On the Size of Pairing-Based Non-interactive Arguments”. In: *Advances in Cryptology – EUROCRYPT 2016*. Ed. by M. Fischlin and J.-S. Coron. Springer Berlin Heidelberg, 2016, pp. 305–326. DOI: [10.1007/978-3-662-49896-5_11](https://doi.org/10.1007/978-3-662-49896-5_11). IACR Cryptology Eprint Archive: ia.cr/2016/260.
- [GOS06] J. Groth, R. Ostrovsky, and A. Sahai. “Perfect Non-interactive Zero Knowledge for NP”. In: *Advances in Cryptology - EUROCRYPT 2006*. Ed. by S. Vaudenay. LNC. Springer Berlin Heidelberg, 2006, pp. 339–358. DOI: [10.1007/11761679_21](https://doi.org/10.1007/11761679_21).
- [IKOS07] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai. “Zero-knowledge from Secure Multiparty Computation”. In: *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing*. STOC ’07. ACM, 2007, pp. 21–30. DOI: [10.1145/1250790.1250794](https://doi.org/10.1145/1250790.1250794).

- [IMS12] Y. Ishai, M. Mahmoody, and A. Sahai. “On Efficient Zero-Knowledge PCPs”. In: *Theory of Cryptography*. Ed. by R. Cramer. Springer Berlin Heidelberg, 2012, pp. 151–168. DOI: [10.1007/978-3-642-28914-9_9](https://doi.org/10.1007/978-3-642-28914-9_9).
- [KR08] Y. T. Kalai and R. Raz. “Interactive PCP”. In: *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, Part II*. ICALP ’08. Springer-Verlag, 2008, pp. 536–547. DOI: [10.1007/978-3-540-70583-3_44](https://doi.org/10.1007/978-3-540-70583-3_44).
- [Kil95] J. Kilian. “Improved Efficient Arguments”. In: *Advances in Cryptology — CRYPTO’95*. Ed. by D. Coppersmith. Springer Berlin Heidelberg, 1995, pp. 311–324. DOI: [10.1007/3-540-44750-4_25](https://doi.org/10.1007/3-540-44750-4_25).
- [Mic00] S. Micali. “Computationally Sound Proofs”. In: *SIAM J. Comput.* 30.4 (Oct. 2000), pp. 1253–1298. DOI: [10.1137/S0097539795284959](https://doi.org/10.1137/S0097539795284959).
- [NVV18] N. Narula, W. Vasquez, and M. Virza. “zkLedger: Privacy-Preserving Auditing for Distributed Ledgers”. In: *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*. USENIX Association, 2018, pp. 65–80. IACR Cryptology Eprint Archive: ia.cr/2018/241.
- [PHGR13] B. Parno, J. Howell, C. Gentry, and M. Raykova. “Pinocchio: Nearly Practical Verifiable Computation”. In: *2013 IEEE Symposium on Security and Privacy*. May 2013, pp. 238–252. DOI: [10.1109/SP.2013.47](https://doi.org/10.1109/SP.2013.47). IACR Cryptology Eprint Archive: ia.cr/2013/279.
- [RRR16] O. Reingold, G. N. Rothblum, and R. D. Rothblum. “Constant-round Interactive Proofs for Delegating Computation”. In: *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*. STOC ’16. ACM, 2016, pp. 49–62. DOI: [10.1145/2897518.2897652](https://doi.org/10.1145/2897518.2897652).
- [Sov18] F. Sovrin. *SovrinTM: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust*. Jan. 2018. <https://1514/sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf>.
- [WTSTW18] R. S. Wahby, I. Tzialla, A. Shelat, J. Thaler, and M. Walfish. “Doubly-efficient zk-SNARKs without trusted setup”. In: *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2018, pp. 926–943. IACR Cryptology Eprint Archive: ia.cr/2017/1132.
- [XZZPS19] T. Xie, J. Zhang, Y. Zhang, C. Papamanthou, and D. Song. “Libra: Succinct Zero-Knowledge Proofs with Optimal Prover Computation”. In: *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part III*. 2019, pp. 733–764. DOI: [10.1007/978-3-030-26954-8_24](https://doi.org/10.1007/978-3-030-26954-8_24). IACR Cryptology Eprint Archive: ia.cr/2019/317.
- [zca18] zcash-hackworks/babyzoe. *Baby ZoE - first step towards Zerocash over Ethereum*. 2018. <https://github.com/zcash-hackworks/babyzoe>.
- [ZGKPP17] Y. Zhang, D. Genkin, J. Katz, D. Papadopoulos, and C. Papamanthou. “vSQL: Verifying Arbitrary SQL Queries over Dynamic Outsourced Databases”. In: *2017 IEEE Symposium on Security and Privacy (SP)*. May 2017, pp. 863–880. DOI: [10.1109/SP.2017.43](https://doi.org/10.1109/SP.2017.43).
- [ZGKPP18] Y. Zhang, D. Genkin, J. Katz, D. Papadopoulos, and C. Papamanthou. “vRAM: Faster Verifiable RAM with Program-Independent Preprocessing”. In: *2018 IEEE Symposium on Security and Privacy (SP)*. May 2018, pp. 908–925. DOI: [10.1109/SP.2018.00013](https://doi.org/10.1109/SP.2018.00013).

Appendix A. Acronyms and glossary

A.1 Acronyms

- | | | |
|--|------|---|
| • 3SAT: 3-satisfiability | 2635 | • QAP: quadratic arithmetic program |
| • AND: AND gate (Boolean gate) | 2636 | • R1CS: rank-1 constraint system |
| • API: application program interface | 2637 | • RAM: random access memory |
| • CRH: collision-resistant hash (function) | 2638 | • RSA: Rivest–Shamir–Adleman |
| • CRS: common-reference string | 2639 | • SHA: secure hash algorithm |
| • DAG: directed acyclic graph | 2640 | • SMPC: secure multiparty computation |
| • DSL: domain specific languages | 2641 | • SNARG: succinct non-interactive argument |
| • ILC: ideal linear commitment | 2642 | • SNARK: SNARG of knowledge |
| • IOP: interactive oracle proofs | 2643 | • SRS: structured reference string |
| • LIP: linear interactive proofs | 2644 | • UC: universal composability or universally composable |
| • MA: Merlin–Arthur | 2645 | • URS: uniform random string |
| • NIZK: non-interactive zero-knowledge | 2646 | • XOR: eXclusive OR (Boolean gate) |
| • NP: non-deterministic polynomial | 2647 | • ZK: zero knowledge |
| • PCD: proof-carrying data | 2648 | • ZKP: zero-knowledge proof |
| • PCP: probabilistic checkable proof | 2649 | • ... |
| • PKI: public-key infrastructure | 2650 | |

A.2 Glossary

- **NIZK:** Non-Interactive Zero-Knowledge. Proof system, where the prover sends a single message to the verifier, who then decides to accept or reject. Usually set in the common reference string model, although it is also possible to have designated verifier NIZK proofs.
- **SNARK:** Succinct Non-interactive ARgument of Knowledge. A special type of non-interactive proof system where the proof size is small and verification is fast.
- **zk-SNARK:** Zero-Knowledge SNARK.
- **Instance:** Public input that is known to both prover and verifier. Sometimes scientific articles use instance and statement interchangeably, but we will distinguish between the two. Notation: x .
- **Witness:** Private input to the prover. Others may or may not know something about the witness. Notation: w .
- **Application Inputs:** Parts of the witness interpreted as inputs to an application, coming from an external data source. The complete witness and the instance can be computed by the prover from application inputs.
- **Relation:** Specification of relationship between instances and witness. A relation can be viewed as a set of permissible pairs (instance, witness). Notation: R .
- **Language:** Set of instances that have a witness in R . Notation: L .
- **Statement:** Defined by instance and relation. Claims the instance has a witness in the

relation, which is either true or false. Notation: $x \in L$.

- **Constraint System:** a language for specifying relations.
- **Proof System:** A zero-knowledge proof system is a specification of how a prover and verifier can interact for the prover to convince the verifier that the statement is true. The proof system must be complete, sound and zero-knowledge.
 - *Complete:* If the statement is true and both prover and verifier follow the protocol; the verifier will accept.
 - *Sound:* If the statement is false, and the verifier follows the protocol; he will not be convinced.
 - *Zero-knowledge:* If the statement is true and the prover follows the protocol; the verifier will not learn any confidential information from the interaction with the prover but the fact the statement is true.
- **Backend:** an implementation of ZK proof system's low-level cryptographic protocol.
- **Frontend:** means to express ZK statements in a convenient language and to prove such statements in zero knowledge by compiling them into a low-level representation and invoking a suitable ZK backend.
- **Instance reduction:** conversion of the instance in a high-level statement to an instance for a low-level statement (suitable for consumption by the backend), by a frontend.
- **Witness reduction:** conversion of the witness to a high-level statement to witness for a low-level statement (suitable for consumption by the backend), by a frontend.
- **R1CS (Rank 1 Constraint Systems):** an NP-complete language for specifying relations, as system of bilinear constraints (i.e., a rank 1 quadratic constraint system), as defined in [BCGTV13, Appendix E in extended version]. This is a more intuitive reformulation of QAP.
- **QAP (Quadratic Arithmetic Program):** An NP-complete language for specifying relations via a quadratic system in polynomials, defined in [PHGR13]. See R1CS for an equivalent formulation.

Reference strings:

- **CRS (Common Reference String):** A string output by the NIZK's Generator algorithm, and available to both the prover and verifier. Consists of proving parameters and verification parameters. May be a URS or an SRS.
- **URS (Uniform Random String):** A common reference string created by uniformly sampling from some space, and in particular involving no secrets in its creation. (Also called Common Random String in prior literature; we avoid this term due to the acronym clash with Common Reference String).
- **SRS (Structured Reference String):** A common reference string created by sampling from some complex distribution, often involving a sampling algorithm with internal randomness that must not be revealed, since it would create a trapdoor that enables creation of convincing proofs for false statements. The SRS may be non-universal (depend on the specific relation) or universal (independent of the relation, i.e., serve for proving all of NP).
- **PP (Prover Parameters) or Proving Key:** The portion of the Common Reference String that is used by the prover.
- **VP (Verifier Parameters) or Verification Key:** The portion of the Common Reference String that is used by the verifier.

2713 Appendix B. Summaries of proposals

2714 This appendix congregates summaries of proposals presented and discussed in ZKProof workshops.

2715 The 2nd ZKProof Workshop counted with the presentation of four proposals:

- 2716 • J-R1CS — a JSON Lines file format for R1CS
- 2717 • Interoperability of zero-knowledge tools
- 2718 • Commit-and-prove functionality
- 2719 • Deterministic Generation of Elliptic Curves for ZK Systems

Table of comments and contributions v0.1 → 0.2

The following pages describe proposed contributions to upgrade the draft reference document from version 0.1 (dated 2019-04-11, available during the 2nd ZKProof Workshop) to version 0.2. [[The current draft 0.1.x only contains description of proposed contributions for which, at the time of writing, there are proposed contributors. The draft version 0.2 (to appear) will only mention the actual committed contributions; other contributions may be deferred to a future version.]]

Explanation of the tables of contributions

Each table describes proposed contributions and corresponding changes/edits made to the baseline version 0.1, in order to achieve version 0.2. Each table, indexed as Dx (where x is an integer), corresponds to a [GitHub issue](#) (GIy , where y is an integer) describing proposed contributions — see <https://github.com/zkpstandard/zkreference/issues>. However, compared with GitHub, the description here can be adjusted and better detailed for the purpose of enabling a better cross-referencing to the edits made in the document. Each table has a header as follows:

#	Item id	Location	Contribution Dx : <i>issue title</i>	Related	Context and changes	Edit id
---	---------	----------	--	---------	---------------------	---------

From left to right, the columns represent:

- #: A consecutive positive integer, used to count all described items of contribution
- **Item id** An index of the contribution item, with a numbering subordinate to the table index. For example, $D1.3$ would be the third item (row) of contribution (table) $D1$.
- **Location**: A hint about the location (typically in the old document) of the edits.
- **Contribution Dx : *issue title***: An identifier Dx (with integer x) of the contribution description, and a title of the issue / contributions.
- **Related**: Related references, such as references (GIx) to GitHub issues, and/or ids of other contribution items.
- **Context and changes**: Column to fill-in with contextual information about the proposed contribution, as well as a high level description of the changes in the document.
- **Edit id**: Index (or possibly several indices) of the edits (Ey , with integer y) made in the document. Across the document, changes will be marked in the right margin with this index, so that the reader can hyperlink it directly to the description of the contribution, i.e., to an explanation of why the change was made.

List of Contributions

Structural changes

#	Item id	Location	Contribution D1: Implement editorial structural changes	Related	Context and changes	Edit id
1	D1.1	All document	<p>– Proposed contribution: Implement editorial structural changes to the document.</p> <p>– Proposed contributors: The editors (Daniel Benarroch, Luís Brandão, Eran Tromer) will consider the necessary structural changes (new chapters, sections, subsections, etc.) based on the overall set of contributions.</p>	GI16	<p>– Context: Inherently related to the editorial development of the reference document.</p> <p>– CHANGED: ...</p>	
2	D1.2	New chapter 2	– Proposed contribution: Create new chapter “2. Construction paradigms” to contain explanations of different protocol paradigms for zero-knowledge proofs.	GI16	<p>– Context: editorial</p> <p>– CHANGED: Done as suggested</p>	E25
3	D1.3	All document	– Proposed contribution: Move the old section 1.8 (“taxonomy of constructions”) to be the first section in the new paradigms chapter.	GI16, D14	<p>– Context: editorial</p> <p>– CHANGED: Done as suggested</p>	E26
4	D1.4	All document	– Proposed contribution: List several possible ZKP protocol paradigms, each of which may later become its own section with a detailed explanation of the paradigm.	GI16, GI17	<p>– Context: editorial</p> <p>– CHANGED: Done as suggested</p>	E30
5	D1.5	Front matter, after the cover	– Proposed contribution: Add an abstract	GI16	<p>– Context: editorial</p> <p>– CHANGED: ...</p>	E1
6	D1.6	Front matter	– Proposed contribution: Add an editorial note explaining the versioning of the document	GI16	<p>– Context: editorial</p> <p>– CHANGED: ...</p>	E2
7	D1.7	Front matter	– Proposed contribution: Add acknowledgments consistent with all the contributions	GI16	<p>– Context: editorial</p> <p>– CHANGED: ...</p>	E3
8	D1.8	Old chapter 4 ZCon0	– Proposed contribution: Remove ZCon0 notes. Based on the editorial process, the workshop notes are separated from the community reference.	GI16	<p>– Context: editorial</p> <p>– CHANGED: Removed the old chapter 4, which contained informal notes from the ZCon0 workshop.</p>	

#	Item id	Location	Contribution D1: Implement editorial structural changes	Related	Context and changes	Edit id
9	D1.9	All document	– Proposed contribution: Address and remove all popup pdf-annotations present in draft version 0.1.	GI16	– Context: editorial – CHANGED:	

New or adapted content

#	Item id	Location	Contribution D2: Add an executive summary	Related	Context and changes	Edit id
10	D2.1	Preamble of the document, before the table of contents	– Proposed contribution: Include an "executive summary" describing at a high level the structure and content of the overall "ZKProof community reference" document; the new text may also allude to the purpose, aim, scope and format of the document. – Proposed contributors: NIST-PEC team (Luís Brandão, René Peralta, Angela Robinson)	GI1	– Context: NIST comments C5, D1-D5 – CHANGED: Adding a new executive summary	E5

#	Item id	Location	Contribution D3: Clarify proofs of knowledge	Related	Context and changes	Edit id
11	D3.1	Sections 1.1 and 1.5.3	– Proposed contribution: Make a clearer distinction of ZK proofs of membership vs. ZK proofs of knowledge, including by means of examples and definitions; clarify how the formalism can adequately model proofs of knowledge; may also include a definition of “extractability” property/game. – Proposed contributors: NIST-PEC team (Luís Brandão, René Peralta, Angela Robinson)	GI2	– Context: NIST comments C7 – CHANGED: Adding paragraph distinguishing Proofs of membership vs. proofs of knowledge; add definition game for extractability.	
12	D3.2	Sections 1.1	Introduce acronym ZKP			E7

#	Item id	Location	Contribution D3: Clarify proofs of knowledge	Related	Context and changes	Edit id
13	D3.3	Sections 1.1	Clarify the meaning of “secrecy” of the “information” held by the prover.			E7
14	D3.4	Sections 1.1	Enumerate the basic examples, including two new ones (chess and theorem)			E8
15	D3.5	Sections 1.1	Allude to the need of an instance			E9
16	D3.6	Sections 1.1	Mention proof vs. argument			E10
17	D3.7	Sections 1.2	Enhance table of examples			E13
18	D3.8	Sections 1.3	Distinguish types of statement: of knowledge vs. of membership			E14
19	D3.9	(New) Sections 1.4	Distinguish types of proof: of knowledge vs. of membership			E15
20	D3.10	(New) Sections 1.4.1	Add example of ZKPoK of DL			E16
21	D3.11	(New) Sections 1.4.2	Add example of ZKPoK of hash pre-image			E17
22	D3.12	(New) Sections 1.4.3	Add example of ZKP of graph non-isomorphism			E18
23	D3.13	Section 1.5	Add suggestion to define ZKPoK game			E19

#	Item id	Location	Contribution D4: Explain the computational security parameter	Related	Context and changes	Edit id
24	D4.1	Chapter 2 ("Implementation"), mostly in Section 2.5.	<p>– Proposed contribution: Add text about possible computational security parameters, and the different security properties they may apply to (e.g., soundness, ZK, short-term vs. long-term, ...). In section 2.5, replace occurrences of "120" by "128".</p> <p>– Proposed contributors: The NIST-PEC team (Luís Brandão, René Peralta, Angela Robinson).</p>	GI3	<p>– Context: Proposed in the "NIST comments on the initial ZKProof documentation" (April 06, 2019) — item C18.</p> <p>– CHANGED: ...</p>	E31

#	Item id	Location	Contribution D4: Explain the computational security parameter	Related	Context and changes	Edit id
25	D4.2	Section 1.5	Wrt to required (approximate) level of security, change 120 to 128			E32 , E33
26	D4.3	Section 1.7.1	In benchmarks, characterize different security properties			E21
27	D4.4	Section 1.7.2	Computational security levels for benchmarks			E22 , E23

#	Item id	Location	Contribution D5: Clarify the public vs. non-public aspect of “common” in CRS enhancement	Related	Context and changes	Edit id
28	D5.1	Mostly in Chapter 1, starting in section 1.2; will also check for other applicable cases across the document.	<p>– Proposed contribution: Clarify the distinction between common (as in shared between prover and verifier) and public knowledge (as in known externally). The lack of distinction was noticed in several parts of the document, when thinking of a comparison between transferable vs. non-transferable ZK proofs. CRS is sometimes being defined as public, although in practice it could be obtained as common to the intervening parties, yet private to a particular interaction. For example, line 177 says “common public input” when first talking of a “common reference string”, but the “public” aspect is arguable – being public vs. common-but-not-public may make the difference between transferability vs. non-transferability.</p> <p>– Proposed contributors: NIST-PEC team (Luís Brandão, René Peralta, Angela Robinson).</p>	GI4	<p>– Context: proposed in the "NIST comments on the initial ZKProof documentation" (April 06, 2019) — item C11.</p> <p>– CHANGED: ...</p>	
29	D5.2	Section 1.2	Syntax of setup — common and private components			E12

#	Item id	Location	Contribution D6: Mention intellectual property	Related	Context and changes	Edit id
30	D6.1	Preamble	<p>– Proposed contribution: Present (in one or two paragraphs), in a non-legalese way, several remarks about intellectual property (IP). A main goal is to raise awareness about the role that IP may take or might not take in the adoption of recommendations and requirements in the community reference document. We are aware this is a delicate topic, so a goal of the contribution is to also motivate future constructive discussion/consideration by the ZKProof community, e.g., about open-source, IP rights, reasonable and non-discriminatory IP terms, etc.</p> <p>– Proposed contributors: NIST-PEC team (Luís Brandão, René Peralta, Angela Robinson).</p>	GI5	<p>– Context: Proposed in the “NIST comments on the initial ZKProof documentation” (April 06, 2019) — item C22.</p> <p>– CHANGED: Added a new section entitled “Expectations on disclosure and licensing of intellectual property”</p>	E4

#	Item id	Location	Contribution D7: Discuss transferability and deniability	Related	Context and changes	Edit id
31	D7.1	Chapter 1 ("Security/Theory")	<p>– Proposed contribution: Elaborate more on the concept of transferability. For example, in an interactive protocol over the Internet, how do regular authenticated channels vs. “ideally” authenticated channels affect transferability? Would a non-transferable protocol become transferable when the prover signs all sent messages and the verifier uses the output of a cryptographic hash function to select random challenges?</p> <p>– Proposed contributors: Luís Brandão</p>	GI6, D7.3	<p>– Context: Proposed in the "NIST comments on the initial ZKProof documentation" (April 06, 2019) — item C9.</p> <p>– CHANGED: ...</p>	E20, E28
32	D7.2	Old Section 3.2.	<p>– Proposed contribution: In Section 3.2, revise the incorrect assertion in item 1: “Only non-interactive ZK (NIZK) can actually hold this property” [being publicly verifiable / transferable?]. For example, if transferability is a design goal then there are settings where it is possible to design interactive protocols for which the view (transcript) of the original verifier (interacting with the original prover) can later serve as a transferable proof for other verifiers.</p> <p>– Proposed contributors: Luís Brandão,</p>	GI6	<p>– Context: Proposed in the "NIST comments on the initial ZKProof documentation" (April 06, 2019) — item C14.</p> <p>– CHANGED: Removed sentence</p>	E36

#	Item id	Location	Contribution D7: Discuss transferability and deniability	Related	Context and changes	Edit id
33	D7.3	...	<ul style="list-style-type: none"> – Proposed contribution: Elaborate more on the concept of deniability. – Proposed contributors: Ivan Visconti 	GI6, D7.1	<ul style="list-style-type: none"> – Context: The “deniability” item was identified in the breakout session on “Interactive Zero Knowledge” in the 2nd ZKProof workshop. – CHANGED: ... 	E29

#	Item id	Location	Contribution D8: Enhance the glossary	Related	Context and changes	Edit id
34	D8.1	Section "A.2 Glossary" in the Appendix.	<ul style="list-style-type: none"> – Proposed contribution: Add to the glossary the suitable technical terms that are used across the document; include hyperlinks to at least its first use in the document. – Proposed contributors: The editors (Daniel Benarroch, Luís Brandão, Eran Tromer). 	GI7	<ul style="list-style-type: none"> – Context: proposed in the "NIST comments on the initial ZKProof documentation" (April 06, 2019) — item C4. – CHANGED: ... 	

#	Item id	Location	Contribution D9: Index and highlight the running examples	Related	Context and changes	Edit id
35	D9.1	Edits across the document; then include "list of recommendations" and "list of requirements" after the toc, lof and lot.	<ul style="list-style-type: none"> – Proposed contribution: Identify in the document which examples can be placed within a boxed environment, with a caption, explanation (possibly an illustration) and a footnote identifying the included concepts (e.g., “setup, trapdoor, CRS, prover and verifier”). Some of these items may be placed as placeholders, as a way to request further contribution by the community. – Proposed contributors: The editors (Daniel Benarroch, Luís Brandão, Eran Tromer) will deal with uniformizing the Latex environment for boxed examples. 	GI8	<ul style="list-style-type: none"> – Context: proposed in the "NIST comments on the initial ZKProof documentation" (April 06, 2019) — item C6. – CHANGED: ... 	

#	Item id	Location	Contribution D10: Highlight the recommendations and requirements	Related	Context and changes	Edit id
36	D10.1	Edit across the document; then include "list of recommendations" and "list of requirements" after the toc, lof and lot.	<ul style="list-style-type: none"> – Proposed contribution: Review the document to identify which statements correspond to requirements and/or recommendations. Create a proper indexed latex environment to highlight these requirements and/or recommendations. It is expected that some of these items will be edited in a tentative manner, as they may need broader discussion by the community. – Proposed contributors: The editors (Daniel Benarroch, Luís Brandão, Eran Tromer). 	GI9	<ul style="list-style-type: none"> – Context: proposed in the "NIST comments on the initial ZKProof documentation" (April 06, 2019) — item C2. – CHANGED: ... 	

#	Item id	Location	Contribution D11: Explain the statistical security parameter	Related	Context and changes	Edit id
37	D11.1	Old sections 1.2, 1.4.3 and 2.5	<ul style="list-style-type: none"> – Proposed contribution: Discuss various examples of acceptable values of statistical security parameter, e.g., 40 bits. Explore how interactive to non-interactive transformations may affect the requirements on the statistical security parameter, e.g., making it become a computational parameter when applying Fiat-Shamir. – Proposed contributors: Luís Brandão. 	GI10	<ul style="list-style-type: none"> – Context: proposed in the "NIST comments on the initial ZKProof documentation" (April 06, 2019) — item C19. Also discussed in the breakout session on "Interactive Zero Knowledge". – CHANGED: ... 	E24

#	Item id	Location	Contribution D12: Clarify the (implicit) scope of some use-cases	Related	Context and changes	Edit id
38	D12.1	Section 3.2	<p>– Proposed contribution: The last paragraph in section 2.2 says “digital money based applications belong to the first model” [public verifiable as a requirement]. This assertion appears implicitly scoped in a too narrow subset of conceivable applications about digital money. Conversely, one could consider a scenario where Alice wants to convince Bob, in a non-transferable way, that Alice bought something from Charlie. Consider clarifying better the scope of examples vs. the scope of areas of application.</p> <p>– Proposed contributors: “DecentrilizedMan”</p>	GI12	<p>– Context: Proposed in the "NIST comments on the initial ZKProof documentation" (April 06, 2019) — item C15.</p> <p>– CHANGED: ...</p>	

#	Item id	Location	Contribution D13: Compare circuits vs. R1CS	Related	Context and changes	Edit id
39	D13.1	Chapters 1 (security/theory) and 2 (implementation)	<p>– Proposed contribution: The “security/theory” track is mentioning Boolean circuits but not R1CS. The “implementation” track is focused on R1CS without explaining why/when it is preferable to a circuit representation. Consider explaining better (in the “security” track) what is R1CS. Consider introducing and exemplifying a circuit-to-R1CS translation and/or vice-versa. Consider clarifying better in the “implementation” track why the focus is on R1CS, for example compared with circuits.</p> <p>– Proposed contributors: Hasini and DecentrilizedMan</p>	GI13	<p>– Context: Proposed in the "NIST comments on the initial ZKProof documentation" (April 06, 2019) — item C10.</p> <p>– CHANGED: ...</p>	

#	Item id	Location	Contribution D14: Introduction to interactive zero-knowledge proofs	Related	Context and changes	Edit id
40	D14.1	Security section	<p>– Proposed contribution: An introduction to advantages and disadvantages of interactive zero-knowledge proofs relative to non-interactive ones, and a discussion of scenarios and applications where interactive protocols may be particularly suitable or relevant.</p> <p>– Proposed contributors: Justin Thaler and Yael Kalai (and further contributors)</p>	GI18, D1.2	<p>– Context: Discussed during the "Interactive Zero Knowledge" breakout session in the 2nd ZKProof Workshop</p> <p>– CHANGED: ...</p>	E27

#	Item id	Location	Contribution D15: Difference between QAPs and linear PCPs	Related	Context and changes	Edit id
41	D15.1	section 1 (security), when defining linear PCPs	<p>– Proposed contribution: to outline similarities and differences between the QAP primitive and linear PCPs, and why QAPs are not just an example of a linear PCPs.</p> <p>– Proposed contributors: Mariana Raykova</p>	GI19, D1.2	<p>– Context: Discussed at the breakout session discussing the ZKProof Community Reference document.</p> <p>– CHANGED: ...</p>	

#	Item id	Location	Contribution D16: Improve description of applications and predicates	Related	Context and changes	Edit id
42	D16.1	Chapter (applications)	<p>– Proposed contribution: Improve the accessibility of the Applications section to meet or exceed that of Security and Implementation. This includes the following: formally expand on the existing applications for correctness and ensure that the notion of “predicates” is well understood.</p> <p>– Proposed contributors: Angela Robinson and Daniel Benarroch</p>	GI20	<p>– Context: discussed during the breakout session about the ZKProof Community Reference document</p> <p>– CHANGED: ...</p>	

#	Item id	Location	Contribution D17: Integrate legacy technology to applications in ZK	Related	Context and changes	Edit id
43	D17.1	Chapter applications	<ul style="list-style-type: none"> – Proposed contribution: Currently, there are already deployed ZKP-based solutions (e.g. anonymous credentials in Hyperledger Fabric) that might need to be bridged to others, freshly deployed, ZKP-based components (e.g. privacy-preserving payments). The goal of the bridge is to have zero or almost zero impact on the ZKP-based components already deployed. In the contribution, I want to highlight the above issues, requirements and propose how to leverage Commit-and-Prove-based techniques, like those in LegoSNARKs, to address them. – Proposed contributors: Angelo de Caro 	GI21	<ul style="list-style-type: none"> – Context: proposed during the breakout session on the ZKProof Community Reference document – CHANGED: ... 	

#	Item id	Location	Contribution D18: Improve motivation in application chapter	Related	Context and changes	Edit id
44	D18.1	Old section 3.1	<ul style="list-style-type: none"> – Proposed contribution: Motivation for ZKPs must be improved in order to allow users to understand how ZKPs can be used to solve practical problems. In particular: Include some missing items as for example recursive composition and proof-carrying data. – Proposed contributors: Eduardo Morais – Submission mode: GitHub pull request 	GI22	<ul style="list-style-type: none"> – Context: Breakout session: ZKProof Community Reference – CHANGED: Included a paragraph to explain motivation for Proof Carrying Data (PCD). 	E34

#	Item id	Location	Contribution D19: Complete Gadgets Table	Related	Context and changes	Edit id
45	D19.1	Old section 3.4	<ul style="list-style-type: none"> – Proposed contribution: Different gadgets were mentioned during the workshops. Some are already described in the document, but it is necessary to review and complete this tables. – Proposed contributors: Eduardo Morais – Submission mode: GitHub pull request 	GI23	<ul style="list-style-type: none"> – Context: Breakout session: ZKProof Community Reference – CHANGED: Updated the gadgets table by filling in missing elements and making a few corrections. Also updated the specific tables for the following gadgets: signature, encryption, Distributed-decryption and set membership 	E37, E38, E39, E40, E41

#	Item id	Location	Contribution D20: Include references in Application chapter	Related	Context and changes	Edit id
46	D20.1	References	<ul style="list-style-type: none"> – Proposed contribution: Some important references are missing. It is necessary to reference papers whenever relevant. See comments in version 0.1. – Proposed contributors: Eduardo Morais – Submission mode: GitHub pull request 	GI24, D17.1	<ul style="list-style-type: none"> – Context: Breakout session: ZKProof Community Reference – CHANGED: Added 3 references to the new paragraph (E34) in the introduction of the “Applications” chapter 	E35

#	Item id	Location	Contribution D21: Add description of each of the 2nd workshop proposals	Related	Context and changes	Edit id
47	D21.1	New appendix, where each section contains the summary of a proposal	<ul style="list-style-type: none"> – Proposed contribution: include a summary of each of the proposals and the discussions that took place, as a way to point to existing efforts of standardization – Proposed contributors: Proposals’ authors: Tromer, Matteo, Naure, Daniel 	GI26	<ul style="list-style-type: none"> – Context: ... – CHANGED: the proposals were submitted and discussed at the zkproof workshop 	