NIST-PEC contributions to advance the draft ZKProof Community Reference from version 0.1 to 0.2

Luís T. A. N. Brandão, René Peralta, Angela Robinson

National Institute of Standards and Technology

October 10, 2019,* Gaithersburg USA

The Privacy-Enhancing Cryptography (PEC) team at the National Institute of Standards and Technology (NIST) is interested in the development of reference material to aid in the advancement of cryptographic technology that can be used to enhance privacy in a secure, practical, and interoperable way. In this scope, we are collaborating with the development of the ZKProof Community Reference, which intends to promote zero-knowledge proofs technology in an open and inclusive manner. Our collaboration follows the editorial process initiated in the 2nd ZKProof Workshop (April 10–12, 2019).

In the present document, we propose contributions to the process of advancing the draft version 0.1 of the ZKProof Community Reference to a new draft version 0.2. Our contributions are organized into seven topics, as indexed in the table below. Each topic relates to a comment included in the "NIST comments on the initial ZKProof documentation" (April 06, 2019) and further detailed as an "issue" in the Github repository of ZKProof.

Topic	NIST early comment #	Github issue #	In this document	
			Section	Comments
Intellectual property	C22	Issue #5	1	D1.1
Executive summary	C5	Issue #1	2	D2.1
Proofs of Knowledge	C7	Issue #2	3	D3.1–D3.12
CRS public or not	C11	Issue #4	4	D4.1–D4.2
Computational security	C18	Issue #3	5	D5.1–D5.6
Statistical security	C19	Issue #10	6	D6.1
Transferability	C9	Issue #6	7	D7.1–D7.3

We offer these contributions as part of an ongoing editorial process. The proposed items cover a limited number of components in a draft that is expected to be subjected to more revision stages. Our participation should not be construed as endorsement of standardization of any content.

1. Proposal about Intellectual Property

1.1. Context

In community efforts that promote the development of new technologies, the subject of intellectual property involves a diverse set of perspectives from different stakeholders. This topic deserves

*This is a revision with improvements over the version (with the same title) dated September 10, 2019.

explicit consideration and setting of community expectations. For that reason we have proposed that some related guidance be included in the ZKProof Reference document.

In the "NIST comments on the initial ZKProof documentation" (April 6, 2019) we commented the following: *"C22. [...] Consider discussing possible guidance regarding intellectual property."*

After the 2nd ZKProof workshop, we detailed further the proposed contribution in the GitHub ZKProof Reference repository, as Issue #5 ("Mention intellectual property"): *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.*

Section 1.2 shows the actual text proposed for inclusion in the Community Reference. The text tries, without an overly legalese format, to convey clear expectations related to licensing terms and disclosure of patent claims. We shared in advance with the ZKProof Editors and Steering Committee an earlier version of the proposal, for feedback. We propose that the current text, to be integrated in the new draft Community Reference, also be presented to the community during the 3rd ZKProof Workshop.

1.2. Proposed changes

D1.1. Add IP guidance

In the preamble, before the executive summary, add the following unnumbered section:

> **Expectations on disclosure and licensing of intellectual property**
>
> 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.

2. Proposal about Executive Summary

2.1. Context

In the "NIST comments on the initial ZKProof documentation" (April 6, 2019) we commented the following: *"C5. [...] Consider adding an executive summary, describing at a high level the structure and content of the overall reference documentation. [...] "*

After the 2nd ZKProof workshop, we further detailed the proposed contribution in the GitHub ZKProof Reference repository, as Issue #1 ("Add an executive summary"): *"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."*

Some of the mentioned elements — purpose, aim, scope and format — can be left to an editorial note different from the executive summary. Section 2.2 shows the actual text proposed as an initial executive summary for inclusion in the Community Reference.

2.2. Proposed changes

D2.1. Add an executive summary

In the preamble of the document, add the following as a new unnumbered section:

> **Executive Summary**
>
> 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 representation 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 $\mathtt{Y}_1$-M_1-D_1 (year-month-day) satisfies a relation with the present date $\mathtt{Y}_2$-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: $\mathtt{Y}_2 > \mathtt{Y}_1\mathtt{+18}$, or $\mathtt{Y}_2\mathtt{=}\mathtt{Y}_1\mathtt{+18} \wedge \mathtt{M}_2 > \mathtt{M}_1$, or $\mathtt{Y}_2\mathtt{=}\mathtt{Y}_1\mathtt{+18} \wedge \mathtt{M}_2\mathtt{=}\mathtt{M}_1 \wedge \mathtt{D}_2 \geq \mathtt{D}_1$. 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.

3. Proposal about Proofs of Knowledge

3.1. Context

In the "NIST comments on the initial ZKProof documentation" (April 6, 2019) we commented: *"C7. [...] Consider making a clearer distinction of ZK proofs of membership vs. ZK proofs of knowledge, including by means of examples and definitions. Consider clarifying how the formalism can adequately model proofs of knowledge. A definition of an "extractability" property/game may be useful."*

After the 2nd ZKProof workshop, we detailed further the proposed contribution in the GitHub ZKProof Reference repository, Issue #2 ("Explain the computational security parameter"): *"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."*

Section 3.2 shows the proposed changes to the Community Reference.

3.2. Proposed changes

The following proposed changes relate to old sections 1.1, 1.3, and 1.5.3, and propose a new section 1.4.

D3.1. Introduce acronym ZKP

In Section 1.1.1, line 131, introduce the ZKP acronym, when first writing the extended form. Where it says "A zero-knowledge proof makes it possible [...]", write:

> A zero-knowledge proof (ZKP) makes it possible [...]

D3.2. Clarify secrecy of witness

In Section 1.1.1, line 132, introduce sentences clarifying the meaning of secret information. Within the text "[...] secret information. There are numerous uses of [...]", write:

> [...] 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).
>
> There are numerous uses of [...]

D3.3. List examples at a high level

In section 1.1.1, lines 132–133 (before Table 1.1), the draft 0.1 contained Table 1.1 with examples of ZKP scenarios. Further below, comment D3.6 proposes enhancing the table, to convey intuition about additional elements in a ZKP. However, to retain a simple beginning of Section 1, before the table gets more complex, we can mention first in running text (in an enumerated environment) a simple description of the scenarios (including two new proposed ones).

Proposed change — where it says “There are numerous uses of zero-knowledge proofs. Table 1.1 gives three examples where proving claims about confidential data can be useful.”, change the text to:

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

D3.4. Allude to the need of an instance

In section 1.1.1, after the enumeration of scenarios proposed in the previous item, add a paragraph alluding to the need of a supporting *instance* (a substrate) and to the qualification of *statement of knowledge*. Proposed text:

> 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.

D3.5. Mention proof vs. argument

In the end of section 1.1.1, after old line 147, add a paragraph conveying at a high level the distinction between “proof” and “argument” and stating that in [the current version of] this document the terminology is simplified to simply use “proof”:

> **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.

D3.6. Enhance table of examples

From section 1.1.1, move and change Table 1.1 (old lines 134–137) to the end of section 1.2. Transpose the table to enable space for more examples, and add a column to describe the “instance” (commonly known by prover and verifier) for each example scenario, in order to enable intuition about the substrate (the instance) that supports the statement with respect to the confidential info. In the table, add an example with the chessboard configuration problem (mentioned in old section 3.4 “Gadgets within predicates”), as well as a similar but more formal example on theorem validity. These examples are also useful to compare the perspectives of ZKP of knowledge vs. ZKP of membership. As a way to let section 1.1 remain simple, we propose that the table, which became more complex, be moved to the end of old section 1.2 (“Terminology”), along with an introductory sentence mentioning it. Here is the proposed result for the end of section 1.2:

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

D3.7. Distinguish types of statements: knowledge vs. membership

In section 1.3, old line 183, change "A statement is a claim $x \in L$, which can be true or false" to:

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.

See related contribution items D3.8–D3.11.

D3.8. Distinguish types of ZKP: knowledge vs. membership

After Section 1.3, old line 221, add a new Section (1.4) conveying the distinction between ZKP of knowledge and ZKP of membership, as follows:

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.

D3.9. Example: ZKPoK of DL

After the text from contribution D3.8 (creating a new Section 1.4), add as a new subsection (1.4.1) a concrete example of a ZKP of knowledge (of discrete log) that does not have a dual ZKP of membership:

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 $\mathbb{Z}_p^* = \{1, ..., p-1\} = \left\{g^i : i = 1, ..., p-1\right\}$ 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 $x = g^w (\text{mod } p)$ 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 $\mathbb{Z}_p^* = \{1, 2, ..., p-1\}$, for which membership is self-evident (without any knowledge of w). In that sense, a proof of membership 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.

D3.10. Example: ZKPoK of hash pre-image

After the example of ZKPoK from contribution D3.9, add as a new subsection (1.4.2) an example of a ZKP of knowledge (of a hash pre-image) with a different subtlety about the duality between knowledge vs. of membership:

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 $\{0,1\}^{256}$. Let w be a witness (hash pre-image) know 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.

D3.11. Example: ZKP of graph non-isomorphism

After the previous proposed item, provide as a new subsection (1.4.3) an example of ZKP of membership without a ZKPoK counterpart:

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.

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.

D3.12. Suggestion to define ZKPoK game

In the end of old subsection 1.5.3 (new subsection 1.6.3), after old line 356, add the following editorial suggestion, to be carefully addressed in a future revision:

[[**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.]]

4. Proposal about CRS as public or not

4.1. Context

In the "NIST comments on the initial ZKProof documentation" (April 6, 2019) we commented the following: *"C11. [...] Consider clarifying the distinction between common knowledge (between* *prover and verifier) and public knowledge. The lack of distinction is noticed in several parts when trying to think of a comparison between transferable vs. non-transferable cases. CRS is being defined as public, although in practice it could be obtained as common to the intervening parties, private to a particular interaction.".*

After the 2nd ZKProof workshop, we detailed further the proposed contribution in the GitHub ZKProof Reference repository, as Issue #4 ("Explain the computational security parameter"): *"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."*

Section 4.2 shows the proposed changes to the Community Reference.

4.2. Proposed changes

The following proposed changes relate to section 1.2.

D4.1. Clarify public vs. common input

In section 1.2 "Terminology", old lines 187–188, change "Instance: Public input that is known to both prover and verifier. Sometimes scientific articles use 'instance' and 'statement' interchangeably, but we distinguish between the two." to:

> Instance: Input commonly known to both prover and verifier, 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.

D4.2. Syntax of setup — common and private components

In section 1.2 "Terminology", old line 200–202, where it says "**Setup:** Input to e.g. prover and verifier. **Common reference string:** Some zero-knowledge systems require common public input, e.g., CRS = setup$_P$ = setup$_V$." adjust as follows:

> **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 "CommonSetup = CRS" (known by both parties), where CRS denotes a "common reference string" (required by some zero-knowledge proof systems). Notation: setup$_P$ = (PrivateSetup$_P$, CRS) and setup$_V$ = (PrivateSetup$_V$, 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.
>
> Note: 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).

5. Proposal about Computational Security parameter

5.1. Context

In the “NIST comments on the initial ZKProof documentation” (April 6, 2019) we commented the following: *“C18. [...] Consider providing rationale for the recommendation of 120 bits of computational security. [...] ”*

After the 2nd ZKProof workshop, we detailed further the proposed contribution in the GitHub ZKProof Reference repository, as Issue #3 (“Explain the computational security parameter”): *“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’.”*

Section 5.2 shows the proposed changes to the Community Reference.

5.2. Proposed changes

The following proposed changes relate to the old section 2.5 (new number 3.5) and to a new subsection 1.5.6

D5.1. Benchmark security levels

In old section 2.5.2 “How to run the benchmarks” (new section 3.5.2), old line 916, replace “The benchmarks should be run at approximately 120-bit security or larger.” by:

> The benchmarks should be obtained preferably for more than one security level, following the recommendations stated in Section 1.7.1

Note: See D5.4 for the proposal of creating the new subsection 1.7.1 (within section the old section “1.7 Efficiency”), moving and adapting there the content of old section 2.5.4. This will also contain requirements and recommendation about statistical security levels (as proposed in Section 6.2)

D5.2. SHA-256 at 128-bit level

In old section 2.5.3 “What benchmarks to run” (new section 3.5.3), old line 935: where it says “(e.g. SHA-256) [...] at 120-bit classical security.” change to

> (e.g., SHA-256) [...] at 128-bit classical security.

D5.3. Primitives at 128-bit level

In old section 2.5.3 “What benchmarks to run” (new section 3.5.3), old line 959: where it says “the primitive should be given at a level of 120 bits or higher” change to the primitive underlying the ZKP statement should be given at a level of 128 bits or higher.

D5.4. Characterize the security properties

Move the old section "2.5.4 Security", old lines 978–981, to the end of old Section "1.7 Efficiency" in Chapter "1 Security". Then, replace "**2.5.4 Security** To aid this benchmarks should make it clear which security level (Definition see theory track document) is being used. In particular the benchmark should clearly state under which assumptions the claimed security is achieved. If the security is conjectured then benchmarks should display both the conjectured as well as the proven performance." as follows (beginning a new subsection 1.7.1):

1.7.1 Characterization of security properties.

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.

D5.5. Computational security levels

In the paragraph of old section "2.5.4 Security", lines 981-982 (proposed in D5.4 to be moved to the new subsection 1.7.1), change "Benchmarks should be run with at least 120-bit security." to (begin a new subsection 1.7.2) as follows:

1.7.2 Computational security levels for benchmarking.

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 precautious (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.

D5.6. Exception for lower levels

In the newly proposed subsection 1.7.2 (see D5.5), add the following paragraph:

An exception allowing lower computational security parameter. With utmost care, a computational security level may be justified below 128 bits, including for benchmarking.

Here is an 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 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.

6. Proposal about Statistical security

6.1. Context

In the "NIST comments on the initial ZKProof documentation" (April 6, 2019) we commented: *"C19. [...] Consider discussing various examples of acceptable values of statistical security parameter. It can be useful to 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."*

After the 2nd ZKProof workshop, we transcribed the proposed contribution in the GitHub ZKProof Reference repository, Issue #10 ("Explain the statistical security parameter"), with a slight variation that added the example of a possibility of 40 bits of statistical security.

Section 6.2 shows the proposed changes to the Community Reference.

6.2. Proposed changes

D6.1. Statistical security levels

In the end of section "1.7 Efficiency" (after the proposed new subsection 1.7.2 — see D5.5), add a new subsection 1.7.3 with considerations about the statistical security parameter, including guidance for benchmarking:

1.7.3 Statistical Security levels for benchmarking. 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.

7. Proposal about transferability and deniability

7.1. Context

In the "NIST comments on the initial ZKProof documentation" (April 6, 2019) we commented: *"C9. [...] The concept of transferability could benefit from more attention. 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?"*

After the 2nd ZKProof workshop, we detailed further the proposed contribution in the GitHub ZKProof Reference repository, as Issue #10 ("Discuss transferability and deniability"): *Elaborate more on the concept of transferability. [...content mentioned above...]*

Also, 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.

This topic was also discussed in the breakout session on "Interactive Zero Knowledge" during the 2nd ZKProof Workshop (April 10–12, 2019), and is expected to receive complementary contributions.

Section 7.2 shows the proposed changes to the Community Reference.

7.2. Proposed changes

[Note: some of the contributions described herein may be adapted to related contributions that may appear concurrently in connection with the discussion of interactivity in ZKP systems.]

D7.1. Mention deniability vs. transferability

After old section 1.5.5 (new section 1.6.5), after old line 417, add a new subsection (1.6.6) introducing the dual features of transferability and deniability:

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 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.

D7.2. Remove incorrect statement

In old section 3.2 (new section 4.2), lines 1325–1326, item 1 ("Publicly verifiable as a requirement), remove the statement "Only non-interactive ZK (NIZK) can actually hold this property."

D7.3. Nuances on transferability vs. interactivity

Within the new section 2.2 to be developed about "Interactivity" in the scope of another contribution — see GitHub Issue #18 "Introduction to interactive zero-knowledge proofs") – add a new subsection 2.2.3 with a discussion of nuanced possibilities of transferability/deniability vs. interactivity:

2.2.x Transferability/deniability vs. interactivity.

The relation between interactivity and transferability/deniability is also 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), provided there is an appropriate trusted setup.

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