Peer Review of "Zero Knowledge Proof: What Can Go Wrong?"

Nico Petzendorfer

June 20, 2023

1 Summary

The paper explains both interactive and non-interactive zero knowledge proofs. It gives a new explanation about the workings of zero knowledge proofs based on the puzzle "Where's Wally". This new explanation can be demonstrated more easily than the previously used examples. Additionally, two identification schemes by Fiat and Shamir are described, which require an additional trust center to create smart cards. The latter one is called "Fiat-Shamir-Heuristic", as it replaces the random challenge bits with the result of a hash-function. This allows interactive zero knowledge proofs to become non-interactive.

After this introduction, the Frozen Heart Vulnerability is explained. This vulnerability affects different implementations of non-interactive zero knowledge proof protocols, where the Fiat-Shamir-Heuristic is incorrectly applied.

The paper does not only explain the protocols on a high level, but also shows the math and notation used for the different protocols.

2 Strength

The paper gives a new and easy to understand example on how to introduce zero knowledge proofs to non-technical readers. It combines the explanation of interactive and non-interactive zero knowledge proofs as well as the explanation of the Frozen Heart vulnerability into a single paper. This has the benefit that the same notation and naming of variables is used throughout the paper, so that readers who do not yet have a good understanding of the topic can look at the definitions without having to think about which variables correspond to which.

3 Weakness

- It is not clear whether the paper is supposed to give an easy overview to nontechnical readers or if it should introduce more technical readers to the vulnerability: For one, the paper gives an easy-to-understand explanation of zero knowledge proofs with the "Where's Wally" example. On the other hand, the later explanations about both zero knowledge proofs and the frozen heart attack are rather technical and include many formulas. While these allow readers to get the technical details, the readers the "Where's Wally" example is aimed at probably do not understand them.
- The stated reason for introducing the new "Where's Wally" example is that while various explanations exist, the most well known one is not easy to demonstrate. It is not clear if the other explanations are all hard to demonstrate as well and therefore the new explanation is indeed needed, or if it would have been better to increase the popularity of an existing explanation.
- When the "Where's Wally" example is first introduced, the author states that the location of the hole should not be able to be guessed by Peggy. It is said that she would have the chance to forge proof otherwise, yet it is not explained in the text how this could be exploited.
- Later, the repetition of the protocol is explained and seems to be the reason for the required randomness. As this is not explicitly stated, this is not clear for the non-technical readers the explanation is aimed at.
- It seems the new explanation has a flaw (or at least this possibility is not explained enough): How can Victor know for sure the puzzle in the stack is indeed the correct puzzle and Peggy does not try to fool him: Peggy could for example simply put a fake puzzle behind the paper, where every person is Wally and therefore easily succeed with any proof no matter the location of the hole. Allowing Victor to simply take apart the stack to check the correctness of the puzzle would not be secure, as he could most probably at least narrow down the position of Wally to a small group, which he could check in less than $\mathcal{O}(2^n)$ complexity. A possible solution might be to have Peggy commit to her proof and then let Victor choose to either unpack the stack and check the puzzle or to open his marked hole and check for Wally.

4 Comments

Comments on the paper can be seen in the provided annotations. A short overview will be listed here:

- The acronym "ZKP" is introduced as "Zero Knowledge Proof". Therefore, when the plural (Zero Knowledge Proof*s*) is meant, "ZKPs" should be used.
- There are some repetitions in the paper (mostly when talking about the ZKP *concept*).
- There is possibly inconsistent or wrong use of the $[0, n]/[n]$ notation: It often seems that an integer in the specified range should be picked, while $[0, n]$ is the set of all real numbers between 0 and n. For this usage, the notation $[n]$ (and $[n]^+$) was introduced and should probably be used (except when indeed a real number is meant).
- The spacing on the ϕ is off.

It shall be noted that these suggestions (especially the ones regarding style) can be personal preference and the presented possibilities should therefore not be taken as the final decision.