CSCI 2590

Final Report: Reversible Proofs of Sequential Work

Valerie May Tomic
B01096101

Summary

Main Results

This report concerns the Eurocrypt 2019 paper *Reversible Proofs of Sequential Work* by Abusala, Kamath, Klein, Pietrzak, and Walter. [1] In general, a proof of sequential work (PoSW) is a proof system which shows that T sequential time steps have passed since a statement χ was received. Unlike other constructions in timed-release cryptography, a PoSW requires that sampling the statement χ be public-coin (so that the Fiat-Shamir heuristic can be applied), and it must produce a proof $\phi(\chi, T)$ that is efficiently and publicly verifiable (i.e. not just by the party who generated χ). For many applications, it is also desirable that a PoSW be *unique*; that is, it should be impossible (or at least computationally intractable) to compute more than one accepting proof for the same χ.

The construction given in the paper maintains these properties, achieving simplicity and efficiency comparable to recent PoSW constructions like that of Cohen and Pietrzak [2], and uses a novel "skip list" structure instantiated with permutations in order to realize the added property that the sequence of states underlying each proof is reversible. The authors conclude by showing how a type of hash function called a "sloth" can be used to improve the efficiency of verifying uniqueness in their PoSW construction.

TECHNIQUES

The core building block of this paper's reversible PoSW construction is the skip list structure, which I introduce via an example in Figures 1 and 2 below.

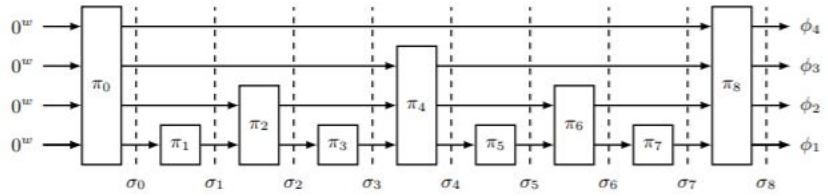

Fig 1: An illustrated example of the paper's skip list structure for $N = 8$. [1]

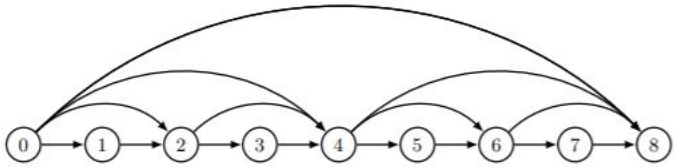

Fig 2: The corresponding directed acyclic graph. [1]

In Figure 1, it is shown how a set of permutations $\Pi = \{\pi_i\}$ are used to produce a sequence of states $\sigma_\Pi = \sigma_0, \ldots, \sigma_N$, for $0 \leq i \leq N$. The dashed lines indicate the states, and the blocks represent permutations. Each state is a string consisting of chunks (four in the example above) to which permutations have been selectively applied in a manner that mimics a skip list data structure. [3] Note that this construction is reversible, as required, since the permutations can be inverted in order to compute state σ_{i-1} from state σ_i.

In Figure 2, we see a DAG that corresponds to the skip list structure. Each node represents a permutation, and the arrows indicate where output from one permutation is piped directly into another permutation. We define a $\mathsf{path}(j)$ as the shortest path that goes from node 0 to node N via node j. In terms of the skip list structure itself, this can be thought of as a partial stack trace for the computation of the entire σ_N, running through a particular permutation j.

In the paper's PoSW construction, the randomness for generating the permutation set Π serves as the challenge statement χ, and σ_N, the final state of the skip list structure, serves as the proof ϕ. The public time parameter is $T = N$.

In order to efficiently verify the sequential computation, the Verifier asks the Prover to reveal the $\mathsf{path}(\gamma)$ for each challenge γ in $(\gamma_1, \ldots, \gamma_t)$. Intuitively, by sending the Verifier ϕ, the Prover has committed itself to the subset of paths that it can actually reveal. The proof of security for the protocol shows that if the Prover can respond to all the Verifier's challenges correctly, then (with overwhelming likelihood) the Prover's responses form a long sequence that must have been computed with the required number of sequential steps.

In the final sections of paper, the authors use a sloth function [4] to make verifying the uniqueness of the output proofs more efficient. The sloth function is essentially a chain of

hash functions whose results can be verified several hundred times faster than they can be computed. By "embedding" the sloth function in between each permutation of their skip graph construction, the authors create a reversible PoSW whose output uniqueness can be efficiently verified relative to the proof computation time.

Points of Interest

I think that the most interesting thing about this paper is the simplicity and versatility of the construction that it presents. The construction realizes an interesting and potentially useful new property (namely, it is reversible) with a unique approach that doesn't simply add to existing constructions. It can be combined in interesting ways with other cryptographic constructions, such as the sloth function, to produce desirable results like efficient uniqueness verification. Even though more recent "verifiable delay function" (VDF) constructions largely subsume PoSW constructions, there are still applications for PoSW in the post-quantum setting, since VDFs are not currently known to be post-quantum secure.

Related Class Topics

In general, this paper revolves around interactive proof systems with special properties, and thus at a high level relates closely to the concepts we've been covering throughout the semester. Although this paper does not deal specifically with zero-knowledge proofs, but rather discusses proof systems imposing special time constraints, its ideas are founded upon the same theoretical framework we encountered repeatedly in class.

More specifically, many of the definitions and constructions we covered in class were key to understanding this paper. For example, the use of public-coin verifiers and the Fiat-Shamir heuristic for non-interactivity (see the class papers from 2/21) played an important role in the definition of the PoSW proof systems, distinguishing them from other timed-release cryptographic constructions. The concept of a malleable proof (see class papers from 3/12) also came up in the discussion of VDFs and how they differ from a PoSW.

Finally, it's notable that the real-world applications for PoSW are similar to those we've seen for many of the constructions presented in class: as the authors discuss in their introduction, renewed interested in time-delayed cryptography has arisen due to the potential applications in decentralized systems such as blockchains.

Future Research Directions

As noted above, the authors state that most of the applications envisioned for PoSW are in fact better suited to more recent VDF constructions, except perhaps in the post-quantum setting. Thus it would seem that one of the most promising directions for further research on the topic of PoSW is in fact VDFs, and potentially post-quantum VDFs.

Although VDFs are promising, there is still important research to be done on PoSW as well, since both types of timed-release cryptographic constructions are very recent: a practical

PoSW construction was first proposed in 2018, and practical constructions of VDFs have only started being published this year.

In terms of research that would build directly on the PoSW from this paper, a likely next step would be to further explore the applications and implications of the reversible property. In particular, the authors mention that the reversibility of their PoSW could be helpful for proofs of replication – a topic that they point out has been the subject of several recent papers, and remains a fruitful area for research. [1]

REFERENCES

[1] H. Abusalah, C. Kamath, K. Klein, K. Pietrzak, and M. Walter. *Reversible Proofs of Sequential Work*. Eurocrypt 2019.

`https://eprint.iacr.org/2019/252.pdf`

[2] B. Cohen and K. Pietrzak. *Simple Proofs of Sequential Work*. Eurocrypt 2018.

`https://eprint.iacr.org/2018/183.pdf`

[3] CMSC 420. *Skip Lists*. Carnegie Mellon University.

`https://www.cs.cmu.edu/~ckingsf/bioinfo-lectures/skiplists.pdf`

[4] A. Lenstra and B. Wesolowski. *Trustworthy Public Randomness with Sloth, Unicorn, and Trx* IACR 2017.

`https://eprint.iacr.org/2015/366.pdf`