Compressed Σ-Protocol Theory and Practical Application to Plug & Play Secure Algorithmics

Mathias Hall-Andersen

April 14, 2021

1 Background

Zero-knowledge proofs intutively enables a 'prover' to convince a 'verifier' about the truth of a statement without revealing anything about why the statement is true. Besides being theoretically interesting, e.g. rigorously defining what it means to reveal nothing, zero-knowledge proofs have seen massive adoption perhaps most famously in the form of digital signatures – in which a signer convinces the verifier that she knows the private key of the corresponding public key. Σ-protocols are a particularly simple, well-studied, well-behaved and beautiful subset of 3 message zero-knowledge proofs. They form the basis of modern signature schemes like Schnorr.

Recently Boneh et. al. proposed Bulletproofs, presented as an alternative to Σ-protocols. Unlike traditional Σ-protocols, Bulletproofs yields proofs with sizes only logarithmic in size of the statement and good concrete efficiency. At a high level Bulletproofs enables proving that an inner product between a public vector and a hidden vector inside a commitment takes a particular value, the reduction in communication is attained by recursively 'splitting' the inner product in two and 'folding' them together with a random linear combination. They then use a separate protocol on-top which enables providing satisfiability of a rank-1 constraint system: essentially opening a random inner product sampled by the verifier which encodes the circuit. Bulletproofs have seen wide adoption, particularly in the crypto currency space.

Unfortunately Bulletproofs are awkward in many ways: namely they do not easily encompass existing Σ-protocol theory, the techniques seem somewhat bespoke and the need for a (complex) separate protocol to show circuit sat is cumbersome.

2 Contributions

Last year, Attema and Cramer introduced Compressed Σ-protocols to overcome this awkwardness: providing simple abstractions, unifying the new techniques with existing techniques and also providing a simple arithmetization technique for showing circuit satisfiability (drawing on standard tricks from multi-party computation). At a high level the trick is to observe that in a Σ-protocol, the last message from the prover to the verifier is essentially a proof that he knows a message which will make the verifier accept: the proof is done by simply sending the message. This observation allows us to consider if this trivial proof can be replaced by a proof with smaller communication? Attema and Cramer replaces the trivial proof for the last-round message with a more efficient 2 message interactive proof of knowledge: having communication $n/2$. However, the last message of this new proof is again a trivial proof that the prover knows a message which will make the verifier accept and can again be replaced with a more efficient one having $n/4$ communication, which can be replaced with a more efficient one having $n/8$...

This yields a protocol with a logarithmic number of rounds and logarithmic communication – just like Bulletproofs (down to the constants). But unlike Bulletproofs it is simply composing variations of existing protocols and uses simple techniques for circuit arithmetization, similar to those in Ligero.

3 Importance

Σ-protocls have been used in numerous applications since the 90ties: constructions of signatures, ring signatures, identification protocols, anonymous eCash and post-quantum signatures, among others. Unifying the techniques of Bulletproofs with the existing Σ-protocol techniques (e.g. 'proofs of partial knowledge') accumulated over 30 years is a great addition to the cryp-

tographers tool belt. Lately these very succinct proofs ($\approx$ 1KB in practice) for complex statements have found renewed interest in the context of blockchains, both for applications in privacy (e.g. anonymous cryptocurrencies) and scalability – since proving that a computation was executed correctly and posting the proof (rather than the entire input) can lead to substantially smaller communication.

4 Strong points

The formulations and abstractions described in the paper are quite elegant. The paper is also significantly easier to understand than the original Bulletproof work.

5 Areas of improvement

The paper does not yield an increase in efficiency over Bulletproofs and essentially 'merely' reformulates what Boneh et. al. has previously proposed. It also assumes quite a bit of familiarity with prior concepts.