State of Σ-protocols

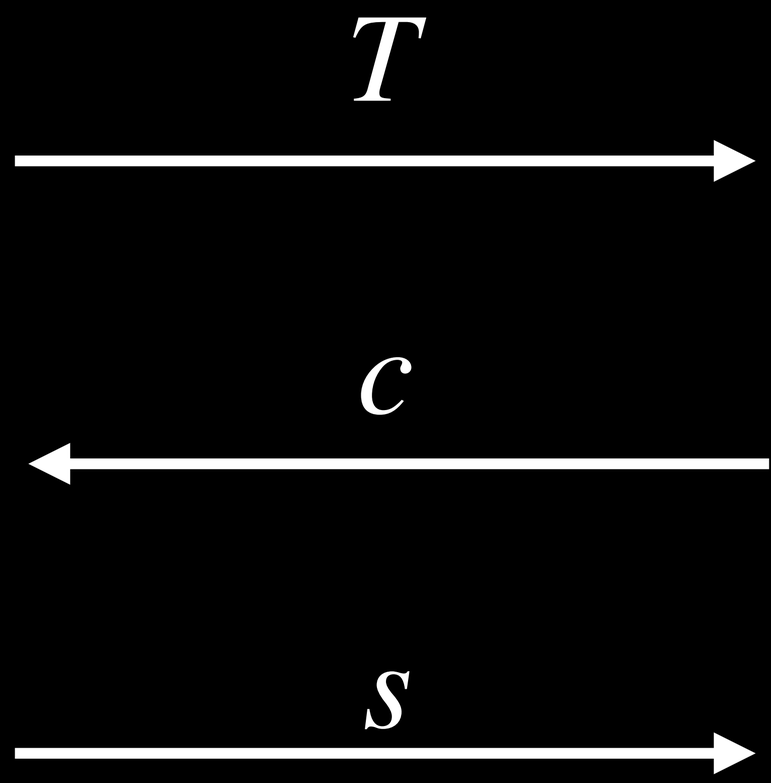
Stephan Krenn, Michele Orrù

https://github.com/zkpstandard/wg-sigma-protocols/blob/build/sigma.pdf

https://docs.zkproof.org/pages/standards/accepted-workshop4/proposal-sigma.pdf

What are Σ-protocols

Simple, versatile, mature zero-knowledge proofs [Sch91].



schnorr signatures , anonymous credentials , small range proofs, discrete log equality , proof of possession, ring signatures

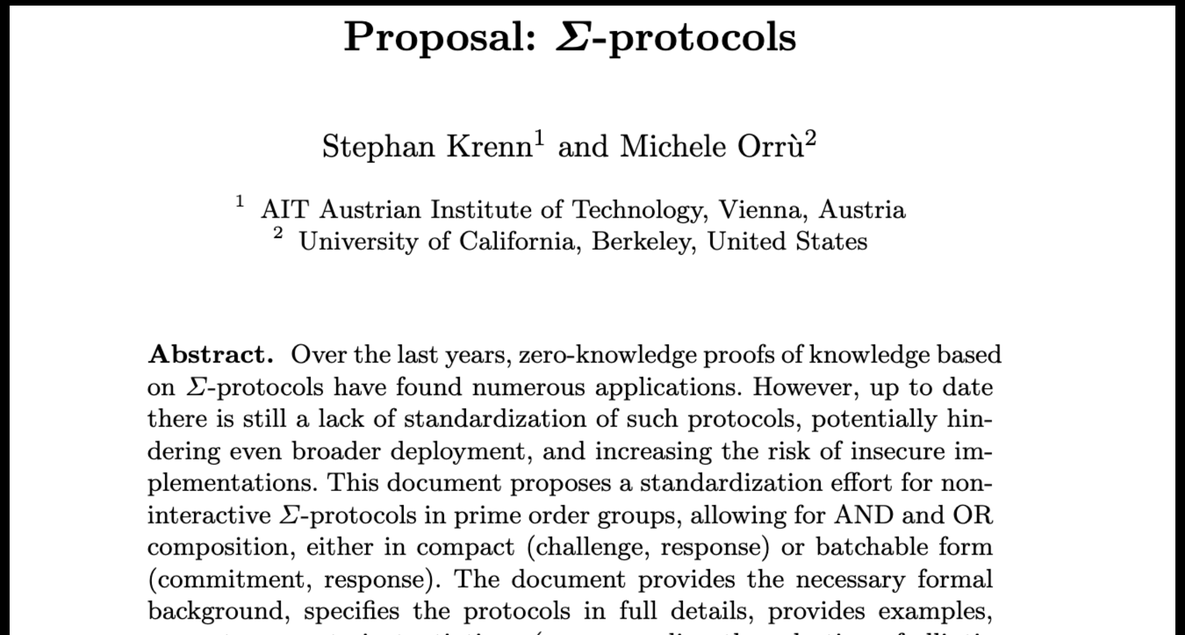
The Σ-protocols working group

Mission: Provide a specification around sigma protocols

Last year: A proposal for Σ-protocols

This year: A specification for Σ-protocols

https://github.com/zkpstandard/wg-sigma-protocols



Proposal: Σ-protocols

Stephan Krenn[1] and Michele Orrù[2]

[1] AIT Austrian Institute of Technology, Vienna, Austria
[2] University of California, Berkeley, United States

Abstract. Over the last years, zero-knowledge proofs of knowledge based on Σ-protocols have found numerous applications. However, up to date there is still a lack of standardization of such protocols, potentially hindering even broader deployment, and increasing the risk of insecure implementations. This document proposes a standardization effort for non-interactive Σ-protocols in prime order groups, allowing for AND and OR composition, either in compact (challenge, response) or batchable form (commitment, response). The document provides the necessary formal background, specifies the protocols in full details, provides examples,

A Spec for Σ-Protocols

Authors: Michele Orrù, Stephan Krenn

Contributors:

Jan Bobolz Mary Maller Ivan Visconti
Yuwen Zhang

Why this is important

Adopters

Infrastructure

A website, a discussion platform.

sigmaprotocols+subscribe@zkproof.org

Reviewers

Coders

https://github.com/yuwen01/wg-sigma-protocols/tree/sage-impls/poc/python

New Sections

Post-quantum protocols, Algebraic hashing

Research Questions.

Q. Concrete security for Σ-protocols based on MLWE?

Q. Is there an algebraic hash map $\mathsf{H} : \mathbb{Z}_q \to \mathbb{Z}_p$?

Q. Can you prove DLOG equality across groups?