Sigma Protocols

Updates from the call for adoption
draft-orru-zkproof-sigma-protocols

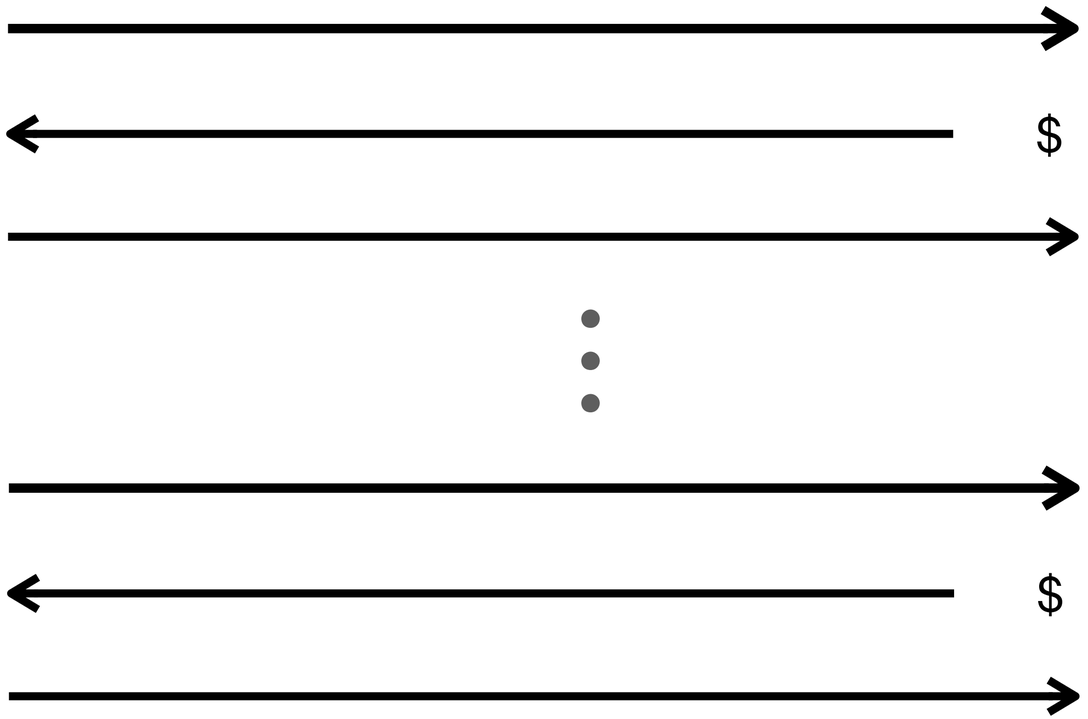
IETF 123 - CFRG
Cathie Yun
sigma.zkproof.org

Recap of Sigma Protocols

Sigma Protocols are…

A zero-knowledge proof

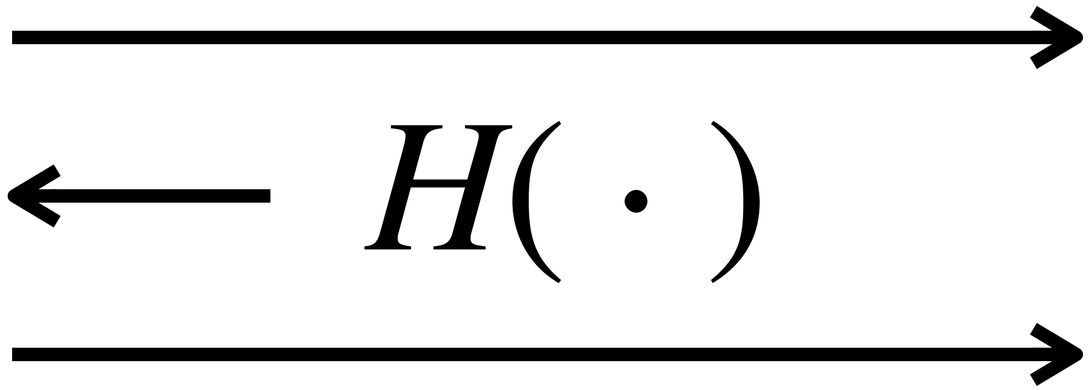
prove (statement, secrets)

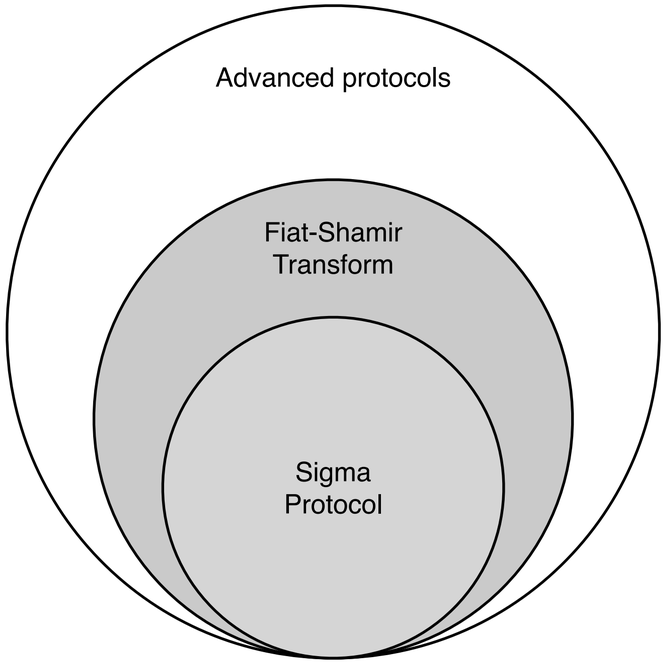


verify (statement, messages)

A zero-knowledge proof

With a Fiat-Shamir transform for non-interactivity





A widely used building block

- In signature schemes:
  - Schnorr signatures (rfc8235)
  - BBS signatures (IETF drafts: CFRG, Privacy Pass)
- In anonymous authentication schemes:
  - VOPRF (rfc9497)
  - BBS blind signatures (IETF draft), BBS pseudonyms (IETF draft)
  - Anonymous Rate-limited Credentials (ARC) (IETF drafts: CFRG, Privacy Pass)
- In multi-party threshold cryptography (NIST MPTC Call)

A prime candidate for standardization

A reusable building block

- Better modularity
  - **Less work for the IETF (and everyone)!** Easier to write and audit proofs
  - **Composability:** Fiat-Shamir, Sigma linear equations can be re-used
- Better security
  - **One place** to fix any vulnerabilities
  - **More robust security guarantees**, with analysis from the academic community. For example, new security proofs of Fiat-Shamir properties

Call for adoption

Support for standardization

General support

For a reusable building block

- ““This work is **relevant to several IETF drafts** currently in progress, […] and likely for future drafts as well.” - Thibault Meunier
- “This draft addresses a **pressing need across multiple areas** (especially Privacy Pass and digital identity).” - Dennis Jackson
- “I support adoption, and agree that this will **help streamline work** on other proposals that rely on Sigma protocols.” - Jonathan Katz
- “This is a **necessary building block** for many applications across the IETF.” - Watson Ladd
- This can be very **useful as a building block** for many protocols.” - Frank Denis

Support from deployed privacy systems

Tor, Ethereum

- “**Tor is relying on Σ-protocols** for our Lox implementation and a specification for this building block would be helpful for us.” - Lindsey Tulloch

- “At the **Ethereum Foundation**, Sigma protocols present a first well established step towards for our long term needs to scale to more transactions securely.” - Mary Maller

Support from in-design privacy systems
EUDI, BBS

- “Having a modular standard for sigma protocols will help in the specification of more complex ZKP-based protocols, such as a **privacy-preserving identity system as envisioned by the EUDI**.” - Anja Lehman

- “This specification synthesizes years of research and engineering experience into an easy-to-use building block for **higher-level constructions like ARC** (and protocols like **Privacy Pass**).” - Chris Wood

- “I’m interested in […] a minimalist formulation that could be **easily adopted by current CFRG work** in progress” - Greg Bernstein

Call for adoption

Feedback and follow-up

Feedback

Scoping, and relationship to Fiat-Shamir spec

- “The draft seems to be **conflating "Sigma Protocols"** (which can be [are?] interactive) **with a Sigma-inspired non-interactive (NI) ZKPoK** obtained using the Fiat-Shamir (FS) transformation.” - Luís Brandão

- “The Fiat-Shamir transformation is not the only possibility for converting a Sigma protocol into a non-interactive ZKP. Thus, consider […] leaving the **current spec to be about sigma protocols**, and do **another [related] spec about the FS transformation**.” - Luís Brandão

Feedback

Scoping, and relationship to Fiat-Shamir spec

- “The draft seems to be **conflating "Sigma Protocols"** (which can be [are?] interactive) **with a Sigma-inspired non-interactive (NI) ZKPoK** obtained using the Fiat-Shamir (FS) transformation.” - Luís Brandão

→ Clarified scope and renamed Sigma spec to “Interactive Sigma Protocols”

- “The Fiat-Shamir transformation is not the only possibility for converting a Sigma protocol into a non-interactive ZKP. Thus, consider […] leaving the **current spec to be about sigma protocols**, and do **another [related] spec about the FS transformation**.” - Luís Brandão

→ Created a separate spec: “Fiat-Shamir Transformation”

What curves to support?

Performance and security considerations

- “As an implementer, in general **I think fewer choices for curves is always better**. It just strikes me as odd to choose P384 over something smaller and more widely used, like P256.” - Christopher Patton
- “*256 (SHA, P, whatever) are the de facto universal standards that everything supports […] So there's **no reason to use a weirdo suite** like *384 when *256 is available.” - Peter Gutmann
- “I have yet to see an application where P384 is too “expensive” (in whatever metrics), but P256 is OK.” - Uri Blumenthal
- “FWIW, I believe the (interactive versions of the) Sigma protocols under consideration are **unconditionally secure**, i.e., special soundness and honest-verifier zero knowledge hold without any computational assumptions.” - Jonathan Katz

What curves to support?

Performance and security considerations

- “As an implementer, in general **I think fewer choices for curves is always better**. It just strikes me as odd to choose P384 over something smaller and more widely used, like P256.” - Christopher Patton → We heard you! Moved from P384 to P256
- “*256 (SHA, P, whatever) are the de facto universal standards that everything supports […] So there's **no reason to use a weirdo suite** like *384 when *256 is available.” - Peter Gutmann
- “I have yet to see an application where P384 is too “expensive” (in whatever metrics), but P256 is OK.” - Uri Blumenthal → Because performance does matter!
- “FWIW, I believe the (interactive versions of the) Sigma protocols under consideration are **unconditionally secure**, i.e., special soundness and honest-verifier zero knowledge hold without any computational assumptions.” - Jonathan Katz → And it’s safe to do so

Requests

Can we make all users happy?

- “I’m interested in […] extended work that could incorporate what are referred to as “**compressed sigma protocols**” (a generalization of “bulletproofs”). In enhancing the privacy of our BBS pseudonym work we have come across the potential need for such optimizations.” - Greg Bernstein

- “For us it would be desirable if the method of generating challenges is **compatible with multi-round protocols**, as it will be helpful for our longer term scaling as well as transitioning our core protocol to post-quantum cryptographic solutions.” - Mary Maller

Requests

Can we make all users happy?

- “I’m interested in […] extended work that could incorporate what are referred to as “**compressed sigma protocols**” (a generalization of “bulletproofs”). In enhancing the privacy of our BBS pseudonym work we have come across the potential need for such optimizations.” - Greg Bernstein

→ We have made parts of the spec compatible with compressed proofs. Feedback is welcome!

- “For us it would be desirable if the method of generating challenges is **compatible with multi-round protocols**, as it will be helpful for our longer term scaling as well as transitioning our core protocol to post-quantum cryptographic solutions.” - Mary Maller

→ Perfect, we support this in the Fiat-Shamir Transform spec!

Call for adoption

Open questions

Open Questions

Can we converge on one design?

- “Can the existing drafts **converge on a single abstraction and protocol**, or will variant proliferation hinder that?” - Thibault Meunier
- “My impression is that a lot of protocols end up using some variant of Sigma that is **optimized for the given use case** but wire-incompatible with something generic you'd see in a paper.” - Christopher Patton

Open Questions

Can we converge on one design?

- “Can the existing drafts **converge on a single abstraction and protocol**, or will variant proliferation hinder that?” - Thibault Meunier

→ This spec is our proposal for convergence!

- “My impression is that a lot of protocols end up using some variant of Sigma that is **optimized for the given use case** but wire-incompatible with something generic you'd see in a paper.” - Christopher Patton

→ Potential adopters: does the Sigma spec capture your optimizations? Let us know!

Scope for specification

We prefer to bias toward simplicity

- Should we support **compressed sigma protocols**?
- Should we support **composability**?
  - **AND** composition of multiple proofs
  - **OR** composition of multiple statements
- Anything else?

Adoption

“It’s clear sigma protocols are used all over the place. What is not clear to me is **which documents actually want to standardise their use of them** using this effort.” - Bas Westerbaan

We have interest from:
- Anonymous Rate-limited Credentials (ARC)
- BBS Blind Signatures
- Anonymous Counting Tokens (ACT)

How do we move the needle from interest to adoption?
What are the blockers?

Next Steps

Ready for adoption

- Successful call for adoption
  - Lots of support for the specification
  - Good feedback, which we addressed
- Questions around scope: we are biasing towards simplicity
- We would like to push for adoption