Verifiable Oblivious Pseudorandom Functions (VOPRFs)

draft-sullivan-cfrg-voprf-02

A. Davidson, N. Sullivan, C. Wood

IETF 103 - CFRG

11.05.2018

VOPRF ~= VRF + OPRF

Definitions and Motivation

Verifiable Random Function (VRF)
Public-key version of cryptographic hash function. Can be verified as correct given public key.

“Verifiable Commitment”

Oblivious Pseudorandom Function (OPRF)
Digital signature-like construction where signer is blind to the content being signed. Signature can be verified with the public key.

“Blind Signature”

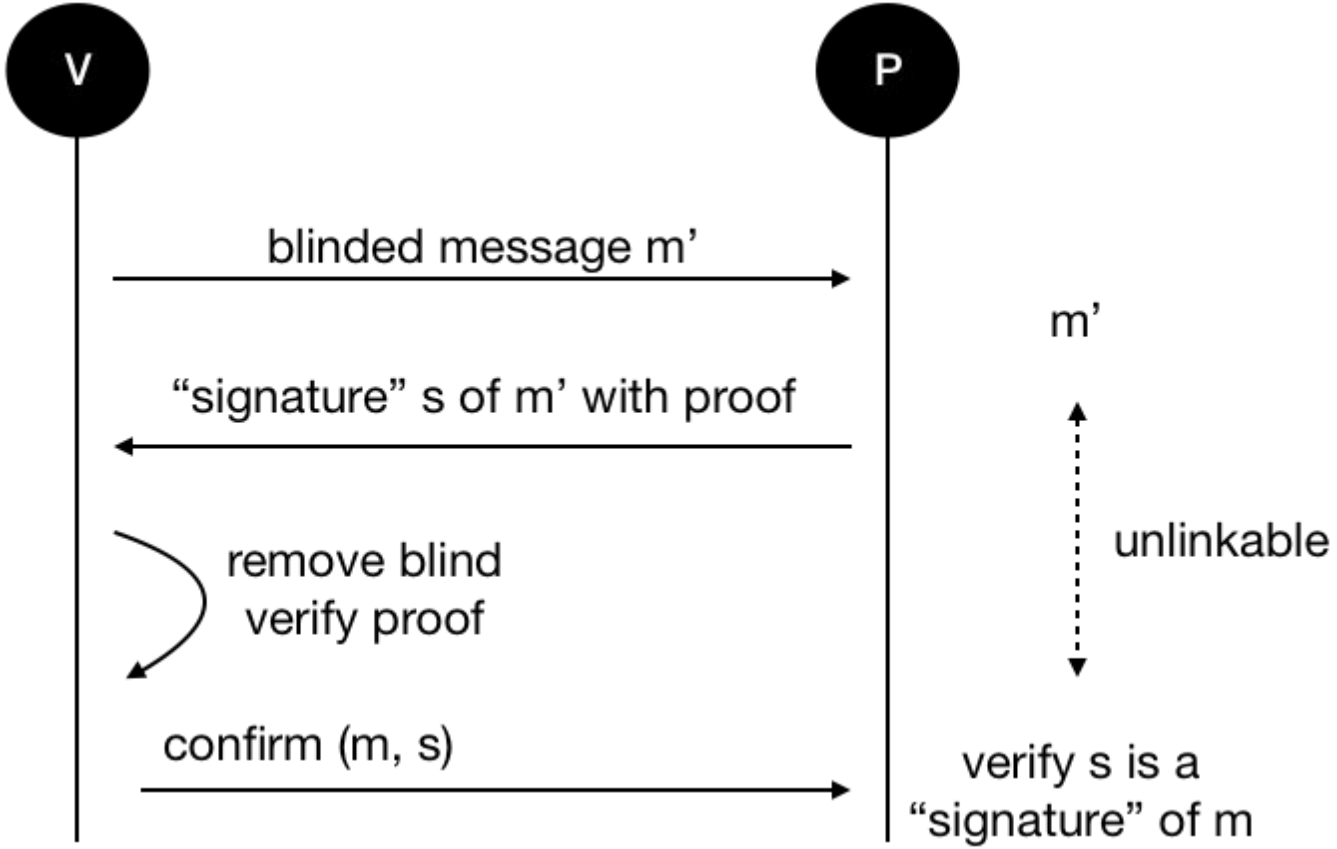
VOPRF ~= VRF + OPRF

Definitions and Motivation

Verifiable Oblivious Pseudorandom Function (VOPRF)

1) Algorithm to deterministically compute (hash, proof) from an input with the private key
2) Algorithm to verify (hash, proof) with public key
3) Ability to compute hash of input from the hash of a blinded version of that input

Hash of input can be checked with private key by computing (hash, proof) from input.


V
P
blinded message m’
m’
“signature” s of m’ with proof
remove blind
verify proof
unlinkable
confirm (m, s)
verify s is a
“signature” of m

VOPRF flow

Generic Construction

Prime-order group with difficult DLP

One way map from a string to a group element

Batch discrete log equivalence proof

Specific Construction

P256 (or x25519 + Ristretto???)

Hash-to-curve ciphersuite
(from draft-irtf-cfrg-hash-to-curve-02)

Batched Chaum-Pedersen proof (Ryan Henry, 2014)

Use Cases

Privacy-preserving applications

- Proof of challenge solution
  - Privacy Pass
- Authorization
- Password compromise checking
- Proof of advertising view

Questions

Does this overlap too much with draft-irtf-cfrg-vrf?

- Blinding mechanism is missing from VRF draft
- Batch verification is missing from VRF draft

Could it be better suited as an extension to the VRF draft?

Are these features fit to be included in the VRF draft?

Verifiable Oblivious Pseudorandom Functions (VOPRFs)

draft-sullivan-cfrg-voprf-02

A. Davidson, N. Sullivan, C. Wood