BLS Signature Scheme

Dan Boneh
Sergey Gorbunov
Hoeteck Wee
Zhenfei Zhang

BLS signatures **[Boneh Lynn Shacham 2001]**

- efficient **pairing**-based signatures
- **aggregatable.** compress n signatures into one

BLS signatures **[Boneh Lynn Shacham 2001]**

- efficient **pairing**-based signatures
- **aggregatable.** compress n signatures into one

applications.

- compressing signature chains in PKI, SBGP
- reducing bandwidth and storage in blockchains

BLS signatures **[Boneh Lynn Shacham 2001]**

- efficient **pairing**-based signatures
- **aggregatable.** compress n signatures into one

related.

- draft-yonezawa-pairing-friendly-curves-01
- draft-irtf-cfrg-hash-to-curve-03

soliciting **feedback**

- security against rogue public-key attacks
  1. sign (pk || msg) **[BLGS03,BNN07]**
  2. include proofs of posessions **[B03,RY07]**
  3. modify verification **[BDN18]**

soliciting **feedback**

- security against rogue public-key attacks
  1. sign (pk || msg) **[BLGS03,BNN07]**
  2. include proofs of posessions **[B03,RY07]**
  3. modify verification **[BDN18]**
- ciphersuites
  - hashing onto curves – try-and-increment?
  - which curves?
  - serialization

soliciting **feedback**

- security against rogue public-key attacks
  1. sign (pk || msg) **[BLGS03,BNN07]**
  2. include proofs of posessions **[B03,RY07]**
  3. modify verification **[BDN18]**
- ciphersuites
  - hashing onto curves – try-and-increment?
  - which curves?
  - serialization

github.com/pairingwg/**bls_standard**