Cryptography engineering at

Adjoint

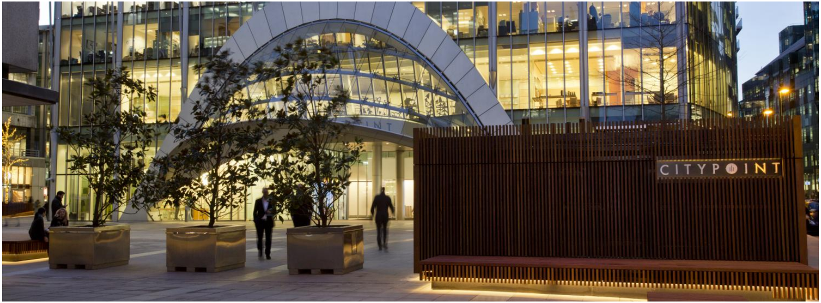
Industrial placement presentation

David Kurniadi Angdinata

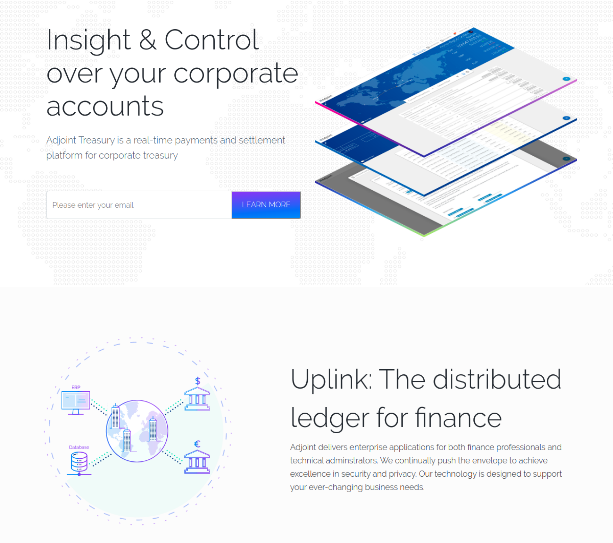
Imperial College London

Friday, 4 October 2019

Company profile



Company profile



Insight & Control over your corporate accounts

Adjoint Treasury is a real-time payments and settlement platform for corporate treasury

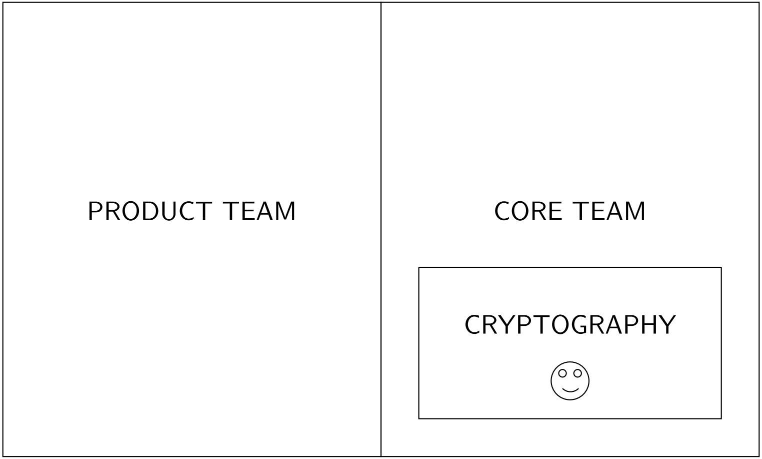
Please enter your email

LEARN MORE

Uplink: The distributed ledger for finance

Adjoint delivers enterprise applications for both finance professionals and technical adminstrators. We continually push the envelope to achieve excellence in security and privacy. Our technology is designed to support your ever-changing business needs.

Organisation roles



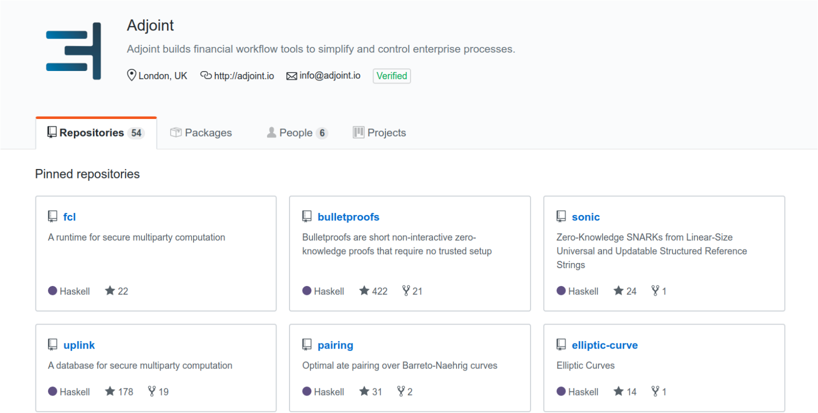
PRODUCT TEAM

CORE TEAM

CRYPTOGRAPHY

☺

Organisation roles



Adjoint

Adjoint builds financial workflow tools to simplify and control enterprise processes.

London, UK http://adjoint.io info@adjoint.io Verified

Pinned repositories

fcl
A runtime for secure multiparty computation
● Haskell ★ 22

bulletproofs
Bulletproofs are short non-interactive zero-knowledge proofs that require no trusted setup
● Haskell ★ 422 21

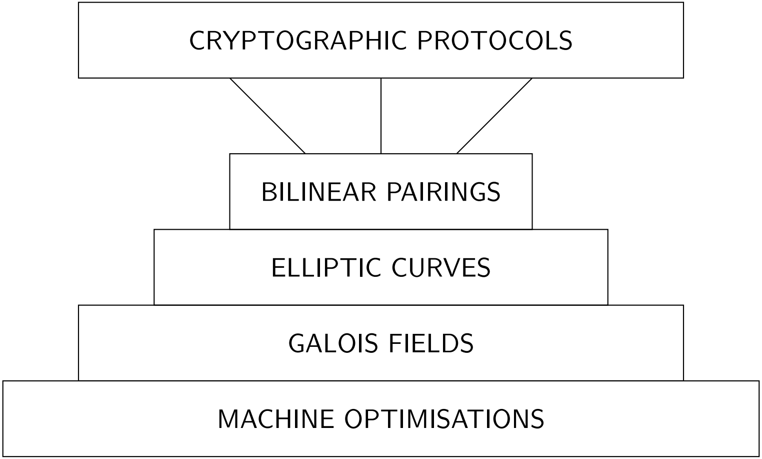
sonic
Zero-Knowledge SNARKs from Linear-Size Universal and Updatable Structured Reference Strings
● Haskell ★ 24 1

uplink
A database for secure multiparty computation
● Haskell ★ 178 19

pairing
Optimal ate pairing over Barreto-Naehrig curves
● Haskell ★ 31 2

elliptic-curve
Elliptic Curves
● Haskell ★ 14 1

Cryptography roadmap



CRYPTOGRAPHIC PROTOCOLS

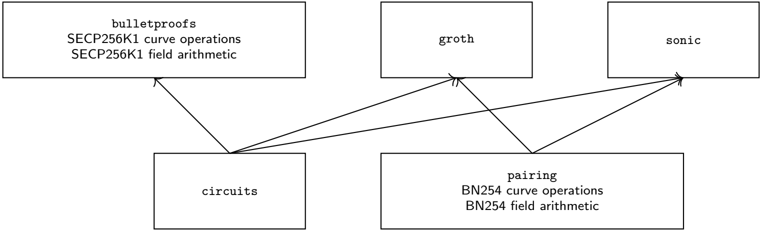
BILINEAR PAIRINGS

ELLIPTIC CURVES

GALOIS FIELDS

MACHINE OPTIMISATIONS

Cryptography roadmap


bulletproofs
SECP256K1 curve operations
SECP256K1 field arithmetic

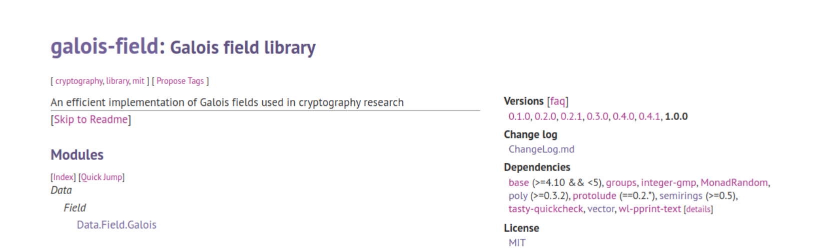
groth

sonic

circuits

pairing
BN254 curve operations
BN254 field arithmetic

An efficient library of Galois fields



galois-field: Galois field library

[cryptography, library, mit] [Propose Tags]

An efficient implementation of Galois fields used in cryptography research

[Skip to Readme]

Modules

[Index] [Quick Jump]

Data

Field

Data.Field.Galois

Versions [faq]

0.1.0, 0.2.0, 0.2.1, 0.3.0, 0.4.0, 0.4.1, **1.0.0**

Change log

ChangeLog.md

Dependencies

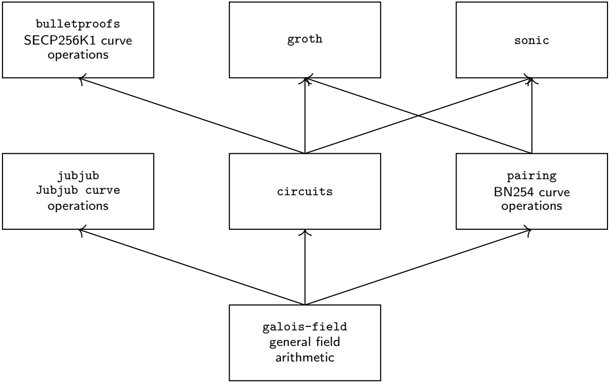
base (>=4.10 && <5), groups, integer-gmp, MonadRandom, poly (>=0.3.2), protolude (==0.2.*), semirings (>=0.5), tasty-quickcheck, vector, wl-pprint-text [details]

License

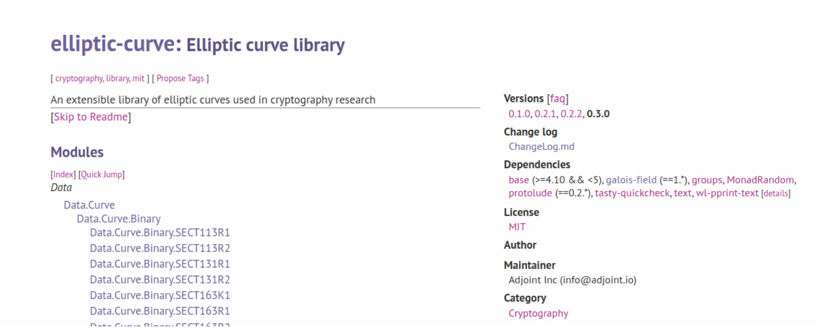
MIT

- Prime fields and extension fields
- Extensive usage of type system
- Slow performance of binary fields
- Square roots and scalar multiplication
- Heavy compile-time and run-time optimisations

An efficient library of Galois fields



A universal library of elliptic curves



elliptic-curve: Elliptic curve library

[cryptography, library, mit] [Propose Tags]

An extensible library of elliptic curves used in cryptography research

[Skip to Readme]

Modules

[Index] [Quick Jump]

Data

- Data.Curve
  - Data.Curve.Binary
    - Data.Curve.Binary.SECT113R1
    - Data.Curve.Binary.SECT113R2
    - Data.Curve.Binary.SECT131R1
    - Data.Curve.Binary.SECT131R2
    - Data.Curve.Binary.SECT163K1
    - Data.Curve.Binary.SECT163R1
    - Data.Curve.Binary.SECT163R2

Versions [faq]
0.1.0, 0.2.1, 0.2.2, **0.3.0**

Change log
ChangeLog.md

Dependencies
base (>=4.10 && <5), galois-field (==1.*), groups, MonadRandom, protolude (==0.2.*), tasty-quickcheck, text, wl-pprint-text [details]

License
MIT

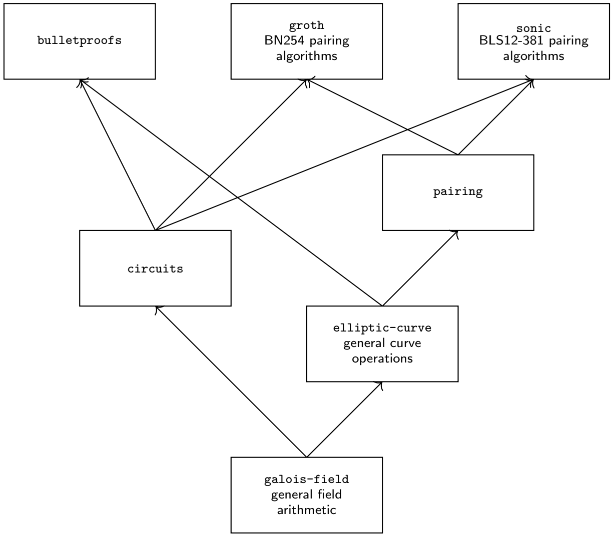
Author

Maintainer
Adjoint Inc (info@adjoint.io)

Category
Cryptography

- Eighty elliptic curve domain parameters
- Elliptic curve multi-parameter type class
- Elliptic curve point associated type
- Elliptic curve point addition formulas
- Elliptic curve source code generator

A universal library of elliptic curves



bulletproofs

groth
BN254 pairing
algorithms

sonic
BLS12-381 pairing
algorithms

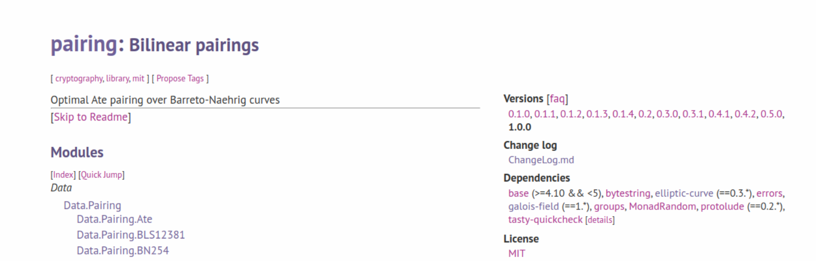
pairing

circuits

elliptic-curve
general curve
operations

galois-field
general field
arithmetic

A polymorphic library of bilinear pairings



pairing: Bilinear pairings

[cryptography, library, mit] [Propose Tags]

Optimal Ate pairing over Barreto-Naehrig curves

[Skip to Readme]

Modules

[Index] [Quick Jump]

Data

- Data.Pairing
  - Data.Pairing.Ate
  - Data.Pairing.BLS12381
  - Data.Pairing.BN254

Versions [faq]

0.1.0, 0.1.1, 0.1.2, 0.1.3, 0.1.4, 0.2, 0.3.0, 0.3.1, 0.4.1, 0.4.2, 0.5.0, **1.0.0**

Change log

ChangeLog.md

Dependencies

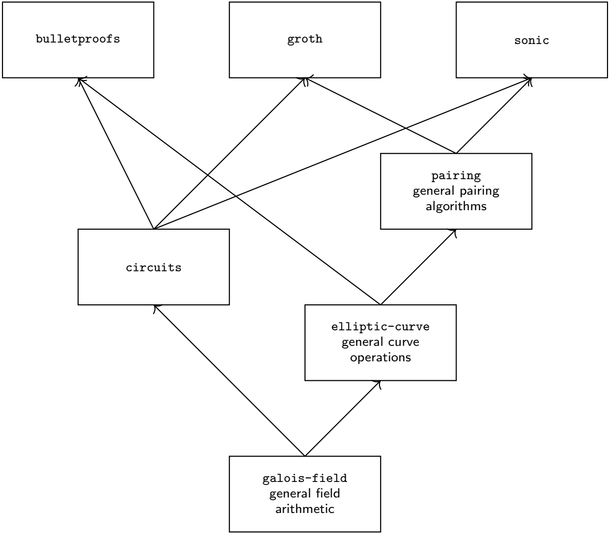
base (>=4.10 && <5), bytestring, elliptic-curve (==0.3.*), errors, galois-field (==1.*), groups, MonadRandom, protolude (==0.2.*), tasty-quickcheck [details]

License

MIT

- Pairing for BN and BLS
- General bilinear pairing type class
- General optimal ate pairing algorithm
- Seven elliptic curve bilinear pairings
- BN elliptic curve hashing function

A polymorphic library of bilinear pairings



Conclusion

Powerful type system in Haskell

Crucial performance optimisations in Haskell

Mathematical background behind zero-knowledge proofs

Cryptographic applications of number theory

Collaborative communication and productivity management