

Dismiss

Join GitHub today















GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together.

Sign up

🔗 master ▾


Go to file

Code ▾

	<b>armfazh</b> Disable cache o... 	✓ 23 days ago	🕒 221
	.etc	Bumping golangci-lint ver...	23 days ago
	.github/w...	Disable cache of test runs.	23 days ago
	dh	Replacing math.rand by c...	23 days ago
	ecc	Fix spelling	2 months ago
	internal	Fix spelling (#134)	2 months ago
	math	Fix spelling (#134)	2 months ago
	pki	Generic signature API (#1...	last month
	sign	Generic signature API (#1...	last month
	simd	Fix spelling (#134)	2 months ago
	.gitignore	Makefile: redo after introd...	16 months ago
	LICENSE	Set year to the original date.	2 months ago
	Makefile	Bumping golangci-lint ver...	23 days ago

About

Cloudflare  
Interoperable  
Reusable  
Cryptographic  
Library

 [blog.cloudflare...](#)

#go

#golang

#post-quantum

#cryptography

#dilithium

#sike


#ed25519






#ed448

#csidh


#sidh

📖 Readme

 View license

	READM...	Lint markdown readme file.	2 months ago
	codecov....	add codecov.io to ci and r...	7 months ago
	doc.go	Fix small typo (from armf...	12 months ago
	go.mod	Re-enabling support for g...	2 months ago
	go.sum	Re-enabling support for g...	2 months ago

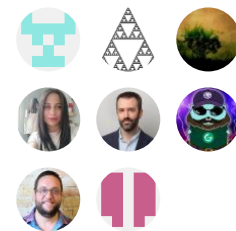
## Releases 1

 Initial ... **Latest**  
on Jul 10, 2019





## Packages

No packages published

## Contributors 8



## Languages

-  Go 67.7%
-  Assembly 29.2%
-  C 2.5%
-  Other 0.6%

### README.md




# CIRCL

 CIRCL **passing**  godoc **reference**  go report **A+**

 codecov **73%**

**CIRCL** (Cloudflare Interoperable, Reusable Cryptographic Library) is a collection of cryptographic primitives written in Go. The goal of this library is to be used as a tool for experimental deployment of cryptographic algorithms targeting Post-Quantum (PQ) and Elliptic Curve Cryptography (ECC).

## Security Disclaimer

 This library is offered as-is, and without a guarantee. Therefore, it is expected that changes in the code, repository, and API occur in the future. We recommend to take caution before using this library in a production application since part of its content is experimental.

## Installation

You can get it by typing:

```
go get -u github.com/cloudflare/circl
```

## Versioning

Version numbers are [Semvers](#). We release a minor version for new functionality, a major version for breaking API changes, and increment the patchlevel for bugfixes.

## Implemented Primitives

Category	Algorithms	Description	Ap
PQ Key Exchange	SIDH	SIDH provide key exchange mechanisms using ephemeral keys.	Pos key in T
PQ Key Exchange	cSIDH	Isogeny based drop-in replacement for Diffie–Hellman	Pos Key exc

Category	Algorithms	Description	Ap
PQ KEM	SIKE	SIKE is a key encapsulation mechanism (KEM).	Pos key in T
Key Exchange	X25519, X448	RFC-7748 provides new key exchange mechanisms based on Montgomery elliptic curves.	TLS Sec
Key Exchange	FourQ	One of the fastest elliptic curves at 128-bit security level.	Exp for l agre and sigr
Key Exchange / Digital signatures	P-384	Our optimizations reduce the burden when moving from P-256 to P-384.	ECI ECI Suit sec
Digital Signatures	Ed25519, Ed448	RFC-8032 provides new signature schemes based on Edwards curves.	Digi cert and auth
PQ Digital Signatures	Dilithium, Hybrid modes	Lattice (Module LWE) based	Pos PKI

Category	Algorithms	Description	Ap
		signature scheme	
<b>Work in Progress</b>			
Category	Algorithms	Description	Ap
Hashing to Elliptic Curve Groups	Several algorithms: Elligator2, Ristretto, SWU, Icart.	Protocols based on elliptic curves require hash functions that map bit strings to points on an elliptic curve.	VC OF PA Ve rai ful
Bilinear Pairings	Plans for moving BN256 to stronger pairing curves.	A bilinear pairing is a mathematical operation that enables the implementation of advanced cryptographic protocols, such as identity- based encryption (IBE), short digital signatures (BLS), and attribute-based encryption (ABE).	Ge Ma Ra Be Et an blo ap
PQ KEM	HRSS-SXY	Lattice (NTRU) based key encapsulation	Ke ex lov

Category	Algorithms	Description	A
		mechanism.	en
PQ KEM	Kyber	Lattice (M-LWE) based key encapsulation mechanism.	Pc Qt Ke ex
PQ Digital Signatures	SPHINCS+	Stateless hash-based signature scheme	Pc Qt

## Testing and Benchmarking

Library comes with number of make targets which can be used for testing and benchmarking:

- `test` performs testing of the binary.
- `bench` runs benchmarks.
- `cover` produces coverage.
- `lint` runs set of linters on the code base.

## Contributing

To contribute, fork this repository and make your changes, and then make a Pull Request. A Pull Request requires approval of the admin team and a successful CI build.

## License

The project is licensed under the [BSD-3-Clause License](#).