Maximize your points with the Microsoft Rewards extension Quick access to your daily points and offers

No thanks Add it now

SIDH Library

Established: April 16, 2016

SIDH Library is a fast and portable software library that implements a new suite of algorithms for supersingular isogeny Diffie-Hellman key exchange [1]. The chosen parameters aim to provide 128 bits of security against attackers running a large-scale quantum computer, and 192 bits of security against classical algorithms. SIDH has the option of a hybrid key exchange that combines supersingular isogeny Diffie-Hellman with a high-security classical elliptic curve Diffie-Hellman key exchange at a small overhead.

SIDH is the first supersingular isogeny Diffie-Hellman software that is fully protected against timing and cache attacks: all operations on secret data run in constant time. The library is also significantly faster than previous implementations, e.g., it is about 2.5 times faster than the previously best (non-constant-time) supersingular isogeny Diffie-Hellman software.

The need for post-quantum

cryptography

A large-scale quantum computer breaks most public-key cryptography that is currently used on the internet such as RSA encryption and digital signatures, ECDH key exchange and ECDSA signatures. Even if no such quantum computer exists today, the prospect of one being built in the not-too-distant future makes it necessary to prepare our cryptography infrastructure and protect our data into the future now. This release is part of a larger effort to identify and deploy asymmetric cryptographic schemes that resist quantum attacks and can replace vulnerable algorithms.

Supersingular isogeny Diffie Hellman key exchange

The supersingular isogeny Diffie-Hellman key exchange protocol was proposed by Jao and DeFeo in [2]. The mathematical structures that provide the key exchange operations are supersingular elliptic curves and isogeny maps between them. Despite the use of elliptic curves, its security is not based on the hardness of the elliptic curve discrete logarithm problem, but instead on the hardness of computing large-degree isogenies between two given elliptic curves. Computing such isogenies is currently believed to be infeasible even for a quantum computer, which makes SIDH a candidate for post-quantum key exchange.

SIDH Library:

- Supports ephemeral Diffie-Hellman key exchange
- Supports a “peace-of-mind” hybrid key exchange mode that adds a classical elliptic curve Diffie-Hellman key exchange on a high security Montgomery curve, providing 384 bits of classical ECDH security
- Protected against timing and cache-timing attacks through regular, constant-time implementation of all operations on secret key material
- Support for Windows using Microsoft Visual Studio and Linux OS using GNU GCC and clang
- Provides basic implementation of the underlying arithmetic functions using portable C to enable support on a wide range of platforms, including x64, x86, and ARM

- Provides an optimized implementation of the underlying arithmetic functions for x64 platforms with optional, high-performance x64 assembly for Linux
- Provides an optimized implementation of the underlying arithmetic functions for 64-bit ARM platforms using assembly for Linux
- Includes testing and benchmarking code for key exchange
- New in version 2.0:
  - A new variant of the isogeny-based key exchange that includes a new suite of algorithms for efficient public key compression [3]. In this variant, public keys are only 330 bytes (compared to 564 bytes required by the original SIDH key exchange variant without compression)
  - An optimized implementation of the underlying arithmetic functions for 64-bit ARM (ARMv8) platforms

Accessing SIDH Library

SIDH Library v2.0 is on GitHub: https://github.com/Microsoft/PQCrypto-SIDH

The SIDH Library v1.1 is available for download at: https://www.microsoft.com/en-us/download/details.aspx?id=52438

A patch for OpenSSL 1.0.2g to support Supersingular Isogeny-based Diffie-Hellman (SIDH) key exchange using the SIDH Library is available for download at: https://www.microsoft.com/en-us/download/details.aspx?id=54053

References

[1] Craig Costello, Patrick Longa, and Michael Naehrig, "Efficient algorithms for supersingular isogeny Diffie-Hellman", available at http://eprint.iacr.org/2016/413

[2] David Jao and Luca DeFeo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies", in PQCrypto 2011, LNCS 7071, pp. 19-34, 2011.

[3] Craig Costello, David Jao, Patrick Longa, Michael Naehrig, Joost Renes, and David Urbanik, "Efficient compression of SIDH public keys". Advances in Cryptology – EUROCRYPT 2017, LNCS 10210, pp. 679-706, 2017. The preprint version is available at http://eprint.iacr.org/2016/963

Brian LaMacchia
Distinguished Engineer

Craig Costello
Researcher

Karen Easterbrook
Sr Principal PM Manager

Michael Naehrig
Principal Researcher

Patrick Longa
Senior Researcher

Follow us:

Share this page:

What's new
Surface Duo
Surface Go 2
Surface Book 3
Microsoft 365
Surface Pro X
Windows 10 apps

Microsoft Store
Account profile
Download Center
Microsoft Store support
Returns
Order tracking
Virtual workshops and training
Microsoft Store Promise

Education
Microsoft in education
Office for students
Office 365 for schools
Deals for students & parents
Microsoft Azure in education

Enterprise
Azure
AppSource
Automotive
Government
Healthcare
Manufacturing
Financial services
Retail

Developer
Microsoft Visual Studio
Windows Dev Center
Developer Center
Microsoft developer program
Channel 9
Office Dev Center
Microsoft Garage

Company
Careers
About Microsoft
Company news
Privacy at Microsoft
Investors
Diversity and inclusion
Accessibility
Security

Sitemap Contact Microsoft Privacy & cookies Terms of use Trademarks Safety & eco
About our ads © Microsoft 2020