Supersingular Isogeny Key Encapsulation

Presented by David Jao

University of Waterloo and evolutionQ, Inc.

Full list of submitters:

Reza Azarderakhsh, FAU
Matt Campagna, Amazon
Craig Costello, MSR
Luca De Feo, UVSQ
Basil Hess, ISG
Amir Jalali, FAU
David Jao, UW
Brian Koziel, TI
Brian LaMacchia, MSR
Patrick Longa, MSR
Michael Naehrig, MSR
Joost Renes, Radboud
Vladimir Soukharev, ISG
David Urbanik, UW

April 11, 2018

Brian Koziel

FOLLOW

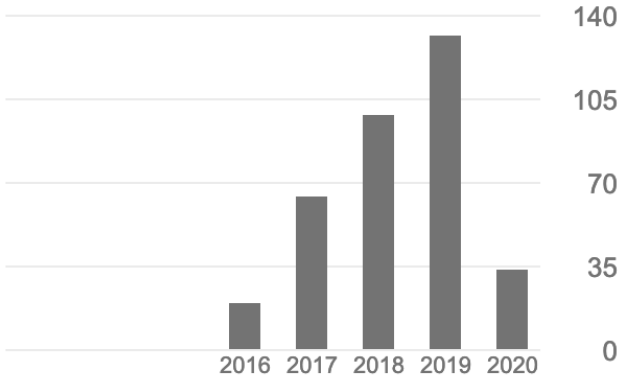
Texas Instruments
Verified email at ti.com - Homepage

Post-Quantum Cryptography Cryptographic Engineering
Applied Cryptography

TITLE	CITED BY	YEAR
Further Optimizations of CSIDH: A Systematic Approach to Efficient Strategies, Permutations, and Bound Vectors A Hutchinson, J LeGrow, B Koziel, R Azarderakhsh Cryptology ePrint Archive, Report 2019/1121, 2019. https://eprint. iacr. org …	5	2019
Edsidh: Supersingular isogeny diffie-hellman key exchange on edwards curves R Azarderakhsh, EB Lang, D Jao, B Koziel International Conference on Security, Privacy, and Applied Cryptography …	2	2018
An exposure model for supersingular isogeny Diffie-Hellman key exchange B Koziel, R Azarderakhsh, D Jao Cryptographers' Track at the RSA Conference, 452-469	2	2018
A high-performance and scalable hardware architecture for isogeny-based cryptography B Koziel, R Azarderakhsh, MM Kermani IEEE Transactions on Computers 67 (11), 1594-1609	16	2018
EdSIDH: Supersingular Isogeny Di# 14; e-Hellman Key Exchange on Edwards Curves R Azarderakhsh, BE Lang, D Jao, B Koziel International Conference on Security, Privacy, and Applied Cryptography …		2018
Supersingular isogeny key encapsulation november 30, 2017 D Jao, R Azarderakhsh, M Campagna, C Costello, A Jalali, B Koziel, ...	1	2017

Cited by

	All	Since 2015
Citations	351	351
h-index	8	8
i10-index	7	7



Co-authors


Reza Azarderakhsh
Florida Atlantic University


David Jao
University of Waterloo


Amir Jalali
LinkedIn Corporation


Mehran Mozaffari Kermani
Assistant Professor of Computer …

Isogeny

From Wikipedia, the free encyclopedia

In mathematics, in particular, in algebraic geometry, an **isogeny** is a morphism of algebraic groups (a.k.a group varieties) that is surjective and has a finite kernel.

If the groups are abelian varieties, then any morphism $f : A \to B$ of the underlying algebraic varieties which is surjective with finite fibres is automatically an isogeny, provided that $f(1_A) = 1_B$. Such an isogeny f then provides a group homomorphism between the groups of k-valued points of A and B, for any field k over which f is defined.

The terms "isogeny" and "isogenous" come from the Greek word ισογενη-ς, meaning "equal in kind or nature". The term "isogeny" was introduced by Weil; before this, the term "isomorphism" was somewhat confusingly used for what is now called an isogeny.

Overview of SIDH

1. Public parameters: Supersingular elliptic curve E over F.
2. Alice chooses a kernel $A \subset E$ and sends E/A to Bob.
3. Bob chooses a kernel $B \subset E$ and sends E/B to Alice.
4. The shared secret is

$$E/\langle A, B\rangle = (E/A)/\phi_A(B) = (E/B)/\phi_B(A).$$

$$\begin{array}{ccc} E & \xrightarrow{\phi_A} & E/A \\ {\scriptstyle \phi_B}\downarrow & & \downarrow \\ E/B & \longrightarrow & E/\langle A, B\rangle \end{array}$$

Supersingular isogeny key exchange

From Wikipedia, the free encyclopedia

Supersingular isogeny Diffie–Hellman key exchange (**SIDH**) is a post-quantum cryptographic algorithm used to establish a secret key between two parties over an otherwise insecure communications channel. It is analogous to the Diffie–Hellman key exchange, but is based on walks in a supersingular isogeny graph and is designed to resist cryptanalytic attack by an adversary in possession of a quantum computer. SIDH boasts one of the smallest key sizes of all post-quantum key exchanges; with compression, SIDH uses 2688-bit[1] public keys at a 128-bit quantum security level. SIDH also distinguishes itself from similar systems such as NTRU and Ring-LWE by supporting perfect forward secrecy, a property that prevents compromised long-term keys from compromising the confidentiality of old communication sessions. These properties make SIDH a natural candidate to replace Diffie–Hellman (DHE) and elliptic curve Diffie–Hellman (ECDHE), which are widely used in Internet communication.