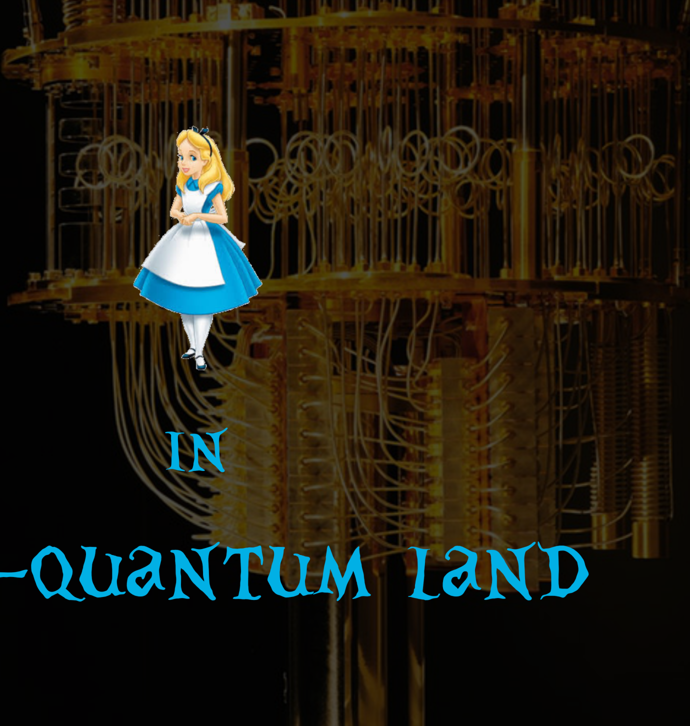
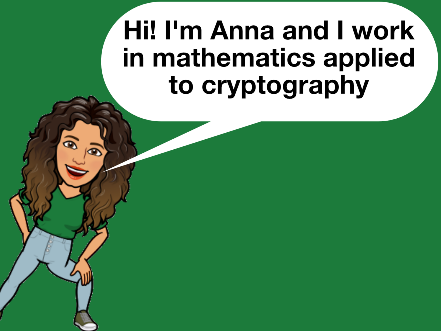


IN

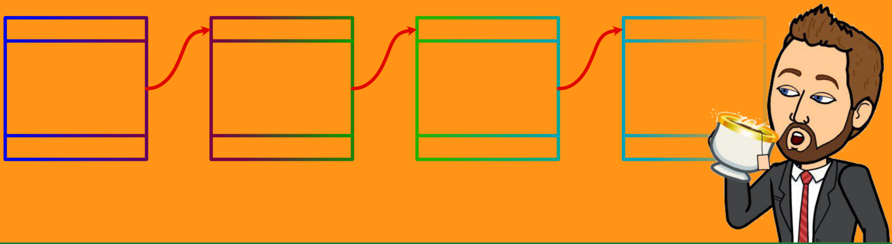
POST-QUANTUM LAND

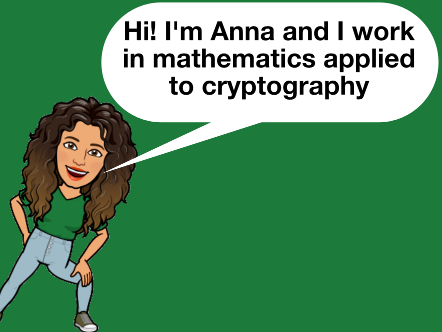
Hi! I'm Anna and I work in mathematics applied to cryptography

What do you think about ₿itcoins?

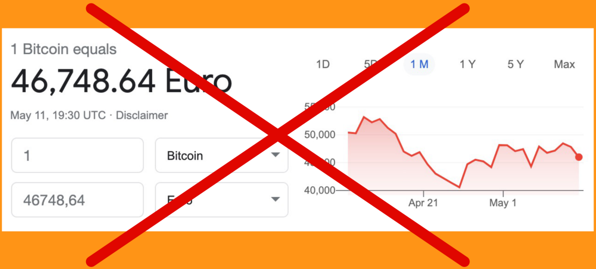

Hi! I'm Anna and I work in mathematics applied to cryptography

What do you think about ₿itcoins?




Hi! I'm Anna and I work in mathematics applied to cryptography

What do you think about Ƀitcoins?



1 Bitcoin equals

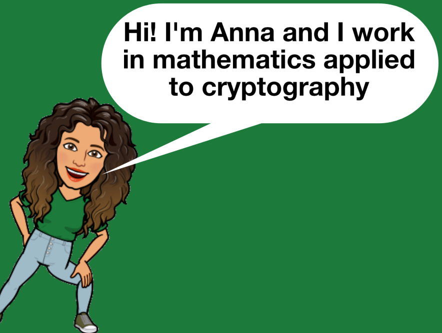
46,748.64 Euro

May 11, 19:30 UTC · Disclaimer

1 | Bitcoin

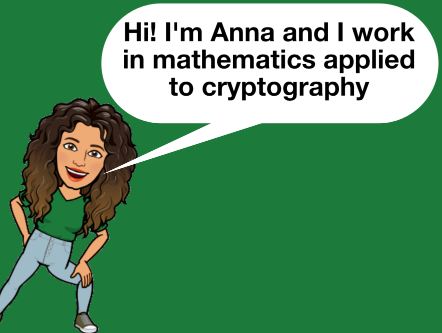
46748,64 | Euro

1D 5D 1 M 1 Y 5 Y Max



Hi! I'm Anna and I work in mathematics applied to cryptography

So, you can tell me how to hack credit cards!


Hi! I'm Anna and I work in mathematics applied to cryptography

So, you can tell me how to hack credit cards!

Cryptography is the science of keeping information secure. As a result, it's designed to make it "extremely hard" for an unauthorized party (like a hacker) to get access to the protected data.

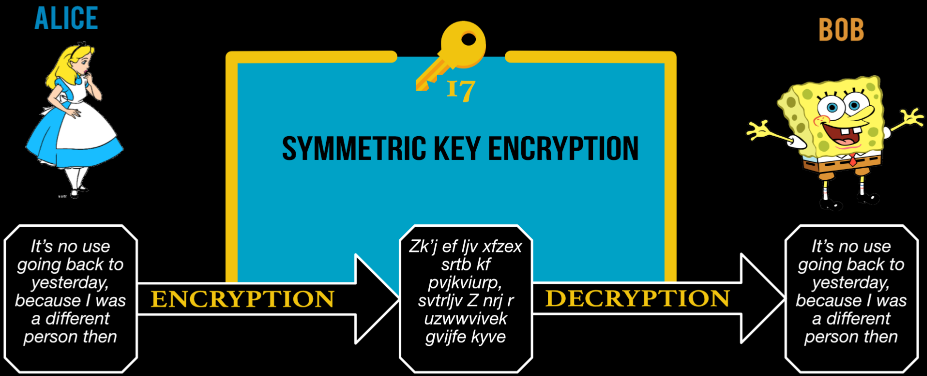
ALICE

BOB

BOB THE BUILDER

BOB THE MINION

BOB MARLEY



ALICE

BOB

17

SYMMETRIC KEY ENCRYPTION

It's no use going back to yesterday, because I was a different person then

ENCRYPTION

Zk'j ef ljv xfzex srtb kf pvjkviurp, svtrljv Z nrj r uzwwvivek gvijfe kyve

DECRYPTION

It's no use going back to yesterday, because I was a different person then

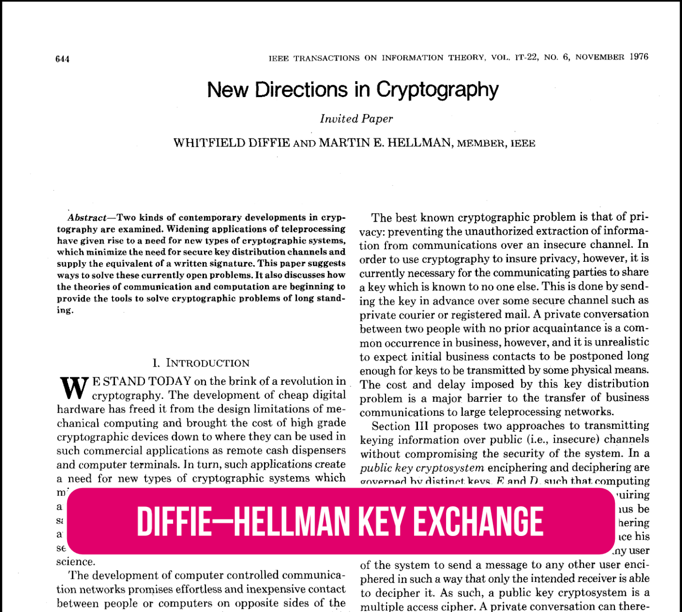
SHARED KEY

0	1	1	···	0	0	1	0

KEY EXCHANGE PROBLEM

*How can Alice and Bob establish a **shared key** over a public insecure channel?*

1976



New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

I. Introduction

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which m

a

s

a

se

science.

The development of computer controlled communication networks promises effortless and inexpensive contact between people or computers on opposite sides of the

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a *public key cryptosystem* enciphering and deciphering are governed by distinct keys, E and D, such that computing

uiring

ius be

hering

ice his

ny user

of the system to send a message to any other user enciphered in such a way that only the intended receiver is able to decipher it. As such, a public key cryptosystem is a multiple access cipher. A private conversation can there-

DIFFIE–HELLMAN KEY EXCHANGE

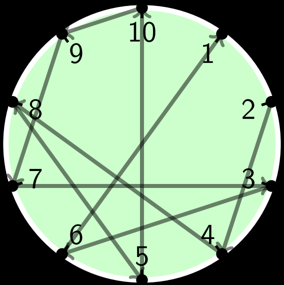
The multiplicative group $\mathbb{F}_p^\times$

p a prime number, $\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$

$\mathbb{F}_p^\times$ is cyclic. Let g be a generator of the group, i.e.

$$\mathbb{F}_p^\times = \{g, g^2, g^3, \ldots, g^{p-1}\} =< g > .$$

Example: 2 is a generator of $\mathbb{F}_{11}^\times = \{1, 2, \ldots, 10\}$.



A large prime number p
A generator g of $\mathbb{F}_p^\times$

$1 \leq a \leq p-1$

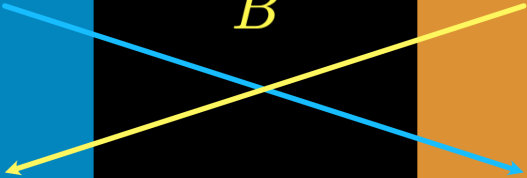
$A = g^a$

A

B

$1 \leq b \leq p-1$

$B = g^b$



$B^a = (g^b)^a$

$\boxed{k = g^{ab}}$

$A^b = (g^a)^b$

$\boxed{k = g^{ab}}$

A large prime number p

A generator g of $\mathbb{F}_p^\times$

$A = g^a$

$B = g^b$

A

B

Goal

g^{ab}

DISCRETE LOGARITHM PROBLEM

Given g^a, compute a

$\mathbb{F}_p^\times$ is an example of finite abelian group.

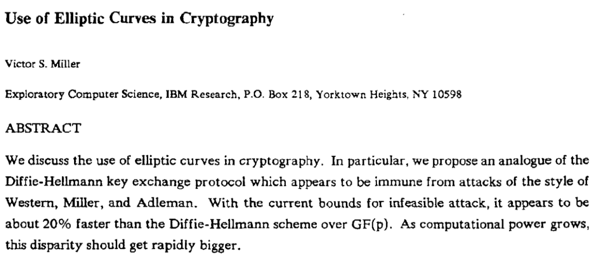
The Diffie–Hellman key exchange works with any finite abelian group. In particular we are interested in finite abelian groups G such that:

- Given g in G and $1 \leq a \leq \operatorname{ord}(g)$, it is easy to compute g^a.
- Given g in G and $x = g^a$, it is difficult to compute a (Discrete Logarithm problem)

Which other group can be “even more interesting” for a Diffie–Hellman key exchange?

2006

1985



Use of Elliptic Curves in Cryptography

Victor S. Miller

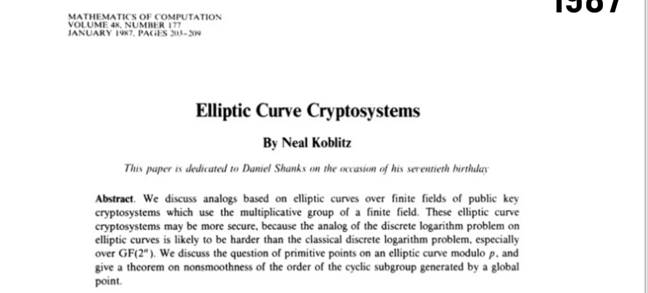
Exploratory Computer Science, IBM Research, P.O. Box 218, Yorktown Heights, NY 10598

ABSTRACT

We discuss the use of elliptic curves in cryptography. In particular, we propose an analogue of the Diffie-Hellmann key exchange protocol which appears to be immune from attacks of the style of Western, Miller, and Adleman. With the current bounds for infeasible attack, it appears to be about 20% faster than the Diffie-Hellmann scheme over GF(p). As computational power grows, this disparity should get rapidly bigger.

ELLIPTIC CURVE DIFFIE–HELLMAN

1987



MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 203-209

Elliptic Curve Cryptosystems

By Neal Koblitz

This paper is dedicated to Daniel Shanks on the occasion of his seventieth birthday

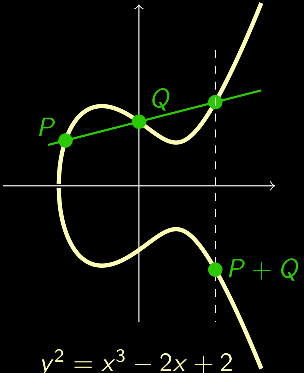
Abstract. We discuss analogs based on elliptic curves over finite fields of public key cryptosystems which use the multiplicative group of a finite field. These elliptic curve cryptosystems may be more secure, because the analog of the discrete logarithm problem on elliptic curves is likely to be harder than the classical discrete logarithm problem, especially over GF(2^n). We discuss the question of primitive points on an elliptic curve modulo p, and give a theorem on nonsmoothness of the order of the cyclic subgroup generated by a global point.

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0.$$

If $a, b \in \mathbb{R}$:

$$E(\mathbb{R}) = \{(x, y) \in \mathbb{R}^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$$

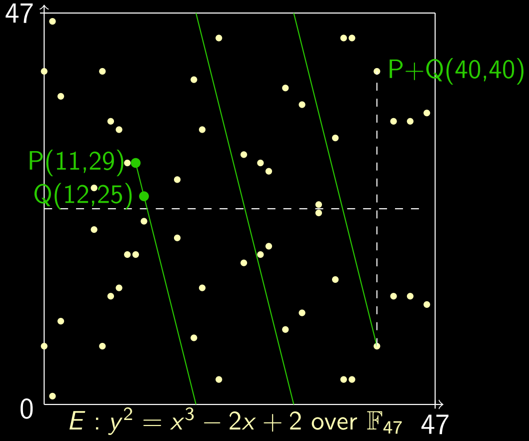


$y^2 = x^3 - 2x + 2$

Elliptic curves over finite fields

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_p, \quad 4a^3 + 27b^2 \neq 0.$$

$$E(\mathbb{F}_p) = \{(x, y) \in (\mathbb{F}_p)^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$$



$E : y^2 = x^3 - 2x + 2$ over $\mathbb{F}_{47}$

$E(\mathbb{F}_{47})$ is an abelian group with 55 elements

$$a = 7$$

$$7P = (9, 14)$$

$$7 * (19, 33) = (36, 3)$$

$$\boxed{k = (36, 3)}$$

$$y^2 = x^3 - 2x + 2/\mathbb{F}_{47}$$

$$P(16, 27)$$

$$(9, 14)$$

$$(19, 33)$$

$$b = 9$$

$$9P = (19, 33)$$

$$9 * (9, 14) = (36, 3)$$

$$\boxed{k = (36, 3)}$$

$$y^2 = x^3 - 2x + 2/\mathbb{F}_{47}$$

$$P(16, 27)$$

$$(9, 14)$$

$$(19, 33)$$

DISCRETE LOGARITHM PROBLEM

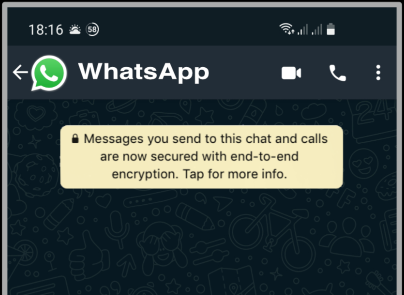
Compute a such that $aP = (9, 14)$

Curve25519

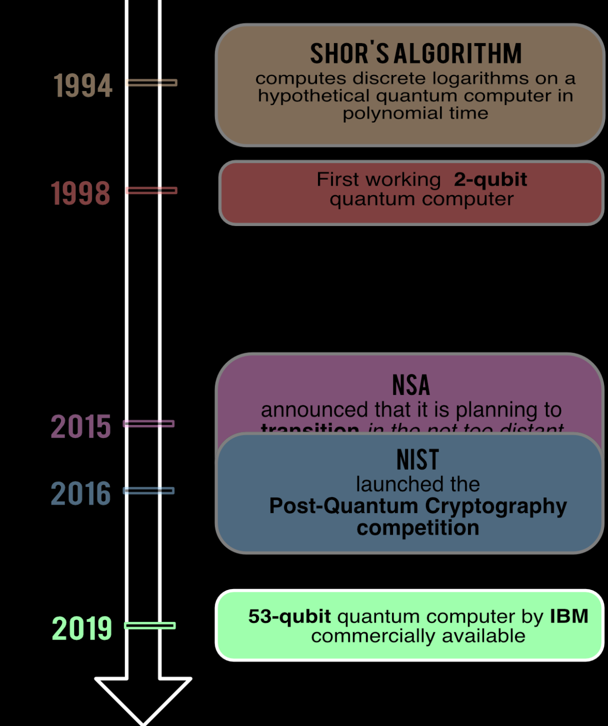
Public parameters:

- $y^2 = x^3 + 48662x^2 + x$
- $p = 2^{255} - 19 =$

  $= 57896044618658097711785492504343953926634992332820282019728792003956564819949$
- $P = (9, 14781619447589544791020593568409986887264606134616475288964881837755586237401)$



Messages you send to this chat and calls are now secured with end-to-end encryption. Tap for more info.



1994

SHOR'S ALGORITHM

computes discrete logarithms on a hypothetical quantum computer in polynomial time

1998

First working **2-qubit** quantum computer

2015

NSA

announced that it is planning to **transition** *in the not too distant*

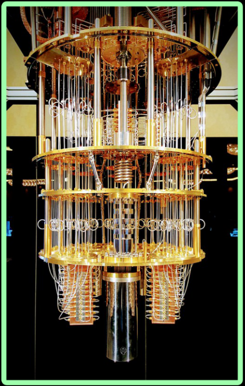
2016

NIST

launched the **Post-Quantum Cryptography competition**

2019

53-qubit quantum computer by **IBM** commercially available

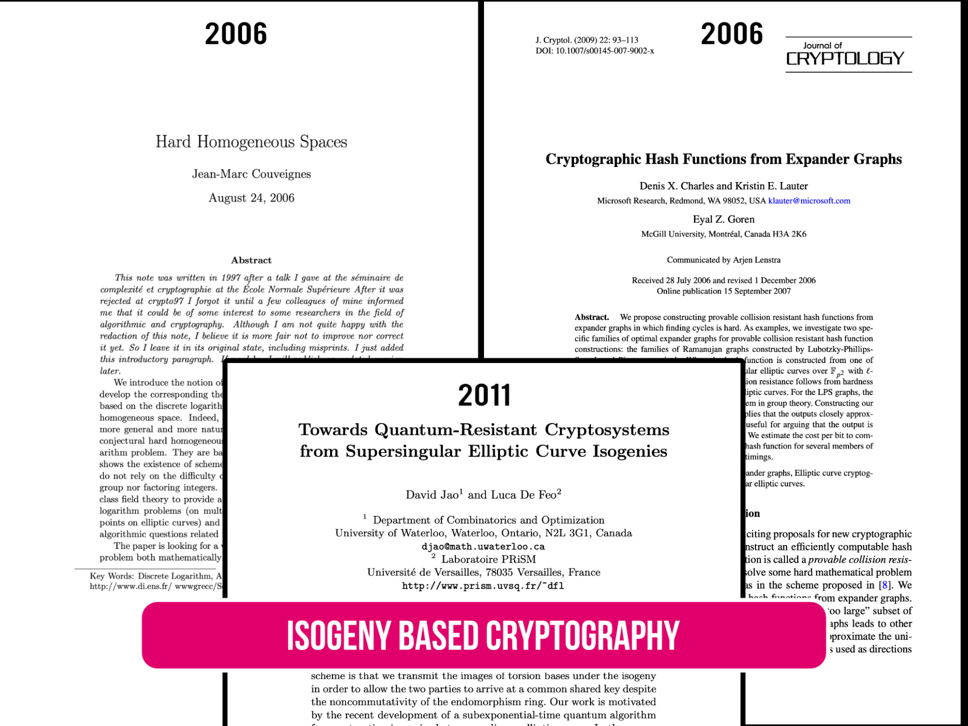


IBM Q quantum computer
Stephen Shankland
(Flickr)

Can Bob and I still use

ELLIPTIC CUVES

in Post-Quantum Land?



ISOGENY BASED CRYPTOGRAPHY

2006

Hard Homogeneous Spaces

Jean-Marc Couveignes

August 24, 2006

Abstract

This note was written in 1997 after a talk I gave at the séminaire de complexité et cryptographie at the École Normale Supérieure After it was rejected at crypto97 I forgot it until a few colleagues of mine informed me that it could be of some interest to some researchers in the field of algorithmic and cryptography. Although I am not quite happy with the redaction of this note, I believe it is more fair not to improve nor correct it yet. So I leave it in its original state, including misprints. I just added this introductory paragraph.
later.

We introduce the notion of
develop the corresponding the
based on the discrete logarith
homogeneous space. Indeed,
more general and more natu
conjectural hard homogeneous
arithm problem. They are ba
shows the existence of scheme
do not rely on the difficulty o
group nor factoring integers.
class field theory to provide a
logarithm problems (on mult
points on elliptic curves) and
algorithmic questions related

The paper is looking for a
problem both mathematically

Key Words: Discrete Logarithm, A
http://www.di.ens.fr/ wwwgrecc/S

2006

J. Cryptol. (2009) 22: 93–113
DOI: 10.1007/s00145-007-9002-x

Journal of
CRYPTOLOGY

Cryptographic Hash Functions from Expander Graphs

Denis X. Charles and Kristin E. Lauter
Microsoft Research, Redmond, WA 98052, USA klauter@microsoft.com

Eyal Z. Goren
McGill University, Montréal, Canada H3A 2K6

Communicated by Arjen Lenstra

Received 28 July 2006 and revised 1 December 2006
Online publication 15 September 2007

Abstract. We propose constructing provable collision resistant hash functions from expander graphs in which finding cycles is hard. As examples, we investigate two specific families of optimal expander graphs for provable collision resistant hash function constructions: the families of Ramanujan graphs constructed by Lubotzky-Phillips-
function is constructed from one of
ular elliptic curves over $\mathbb{F}_{p^2}$ with ℓ-
ion resistance follows from hardness
iptic curves. For the LPS graphs, the
em in group theory. Constructing our
plies that the outputs closely approx-
useful for arguing that the output is
We estimate the cost per bit to com-
hash function for several members of
timings.

ander graphs, Elliptic curve cryptog-
ar elliptic curves.

ion

citing proposals for new cryptographic
nstruct an efficiently computable hash
tion is called a *provable collision resis-*
solve some hard mathematical problem
as in the scheme proposed in [8]. We
hash functions from expander graphs.
'oo large" subset of
aphs leads to other
proximate the uni-
s used as directions

2011

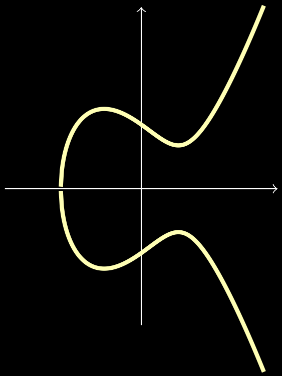
Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies

David Jao[1] and Luca De Feo[2]

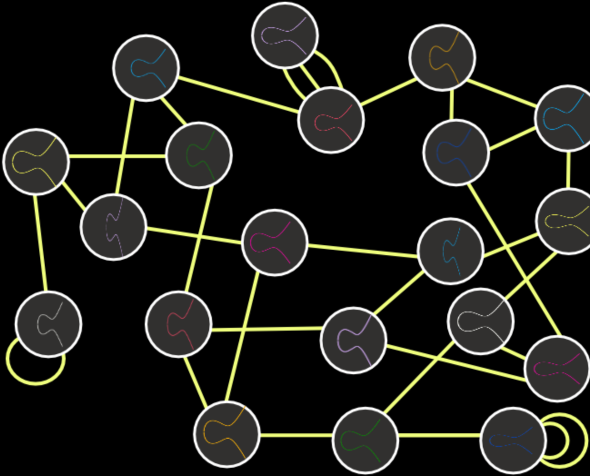
[1] Department of Combinatorics and Optimization
University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada
djao@math.uwaterloo.ca
[2] Laboratoire PRiSM
Université de Versailles, 78035 Versailles, France
http://www.prism.uvsq.fr/~dfl

scheme is that we transmit the images of torsion bases under the isogeny in order to allow the two parties to arrive at a common shared key despite the noncommutativity of the endomorphism ring. Our work is motivated by the recent development of a subexponential-time quantum algorithm

We are not going to work with inside a fixed elliptic curve



We are going to work with a set of elliptic curves



Supersingular ℓ-isogeny graph over $\mathbb{F}_{p^2}$

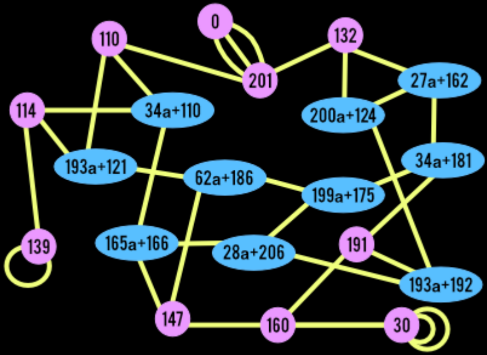
Vertices

$$\left\{ \begin{array}{c} \text{Supersingular elliptic curves} \\ E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_{p^2}, \\ \\ \left(j_E := 1728 \cdot \frac{4a^3}{4a^3+27b^2} \in \mathbb{F}_{p^2}\right) \end{array} \right\}$$

Edges

$$\left\{ \begin{array}{c} \text{Isogenies of degree } \ell \\ \begin{array}{rccc} \varphi : & E_1 & \longrightarrow & E_2 \\ & (x, y) & \mapsto & \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)} y\right) \end{array} \end{array} \right\}$$

$$p = 227$$
$$\ell = 2$$



Supersingular ℓ-isogeny graph over $\mathbb{F}_{p^2}$

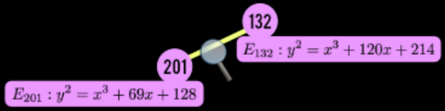
Vertices

$$\left\{ \begin{array}{c} \text{Supersingular elliptic curves} \\ E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_{p^2}, \\ \\ \left(j_E := 1728 \cdot \frac{4a^3}{4a^3+27b^2} \in \mathbb{F}_{p^2}\right) \end{array} \right\}$$

Edges

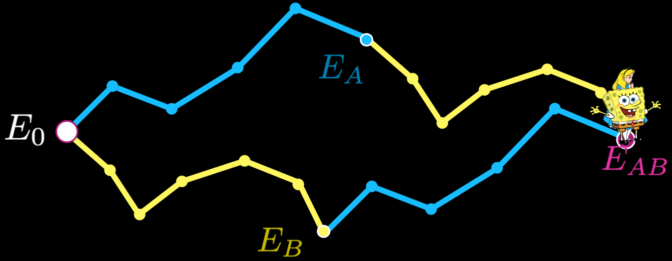
$$\left\{ \begin{array}{cccc} & & \text{Isogenies of degree } \ell & \\ \varphi : & E_1 & \longrightarrow & E_2 \\ & (x, y) & \mapsto & \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)} y\right) \end{array} \right\}$$

$$p = 227$$
$$\ell = 2$$


132
$E_{132} : y^2 = x^3 + 120x + 214$
201
$E_{201} : y^2 = x^3 + 69x + 128$

$$\begin{array}{cccc} \varphi : & E_{201} & \to & E_{132} \\ & (x, y) & \mapsto & \left(\frac{x^2+84x-101}{x+84}, y\frac{x^2-59x-107}{x^2-59x+19}\right) \end{array}$$

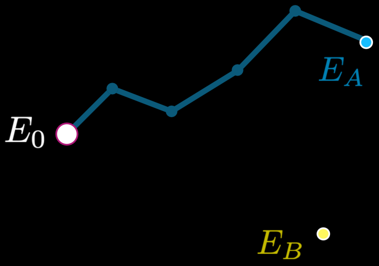
SUPERSINGULAR ISOGENY DIFFIE-HELLMAN



2-ISOGENY GRAPH

3-ISOGENY GRAPH

SUPERSINGULAR ISOGENY DIFFIE-HELLMAN

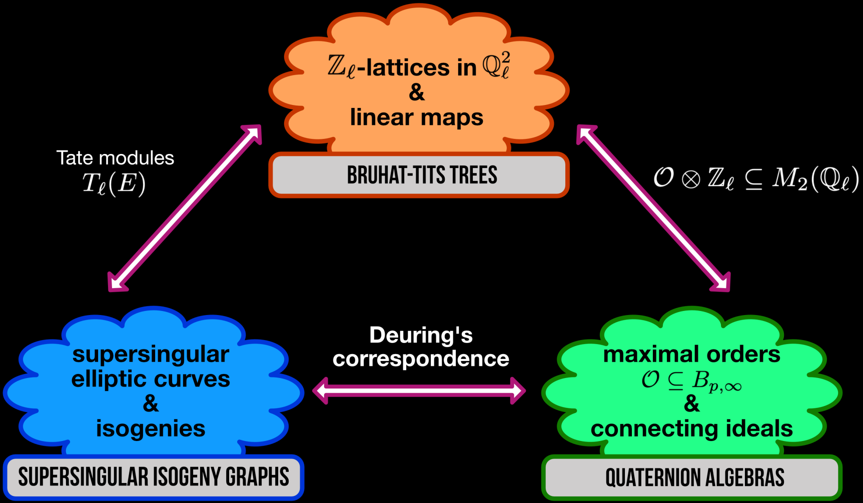


2-ISOGENY GRAPH

3-ISOGENY GRAPH

ISOGENY FINDING PROBLEM

Compute $\varphi : E_0 \to E_A$



$\mathbb{Z}_\ell$-lattices in $\mathbb{Q}_\ell^2$
&
linear maps

BRUHAT-TITS TREES

Tate modules
$T_\ell(E)$

$\mathcal{O} \otimes \mathbb{Z}_\ell \subseteq M_2(\mathbb{Q}_\ell)$

supersingular
elliptic curves
&
isogenies

SUPERSINGULAR ISOGENY GRAPHS

Deuring's
correspondence

maximal orders
$\mathcal{O} \subseteq B_{p,\infty}$
&
connecting ideals

QUATERNION ALGEBRAS

10 mathematicians/cryptographers were mentioned in this talk.

Only 1 is a woman.

Probably in the past we were not given the same opportunities.

But today we can all contribute to a diverse and equal world, each of us in our small ways.

Diversity is richness, and we become rich by investing in different kinds and shades of people.