FAster, STronger Cryptography (FAST)

Tony Ezome and Damien Robert

Data Security in a Quantum World

Abdoul Aziz Ciss
École Polytechnique de Thiès, Sénégal

2017 LIRIMA Scientific Days, Tunis

Context

High need for security

- Millions of cyber-attacks per day
- Powerful adversaries with high computing resources
- The Prism program collects stored Internet communications based on demands made to Internet companies (Microsoft, Yahoo!, Google, Facebook, Paltalk, YouTube, AOL, Skype, Apple...);
- Bullrun and Edgehill to weaken cryptographic standards and implementations;
- Heartbleed software bug in openssl...

Context

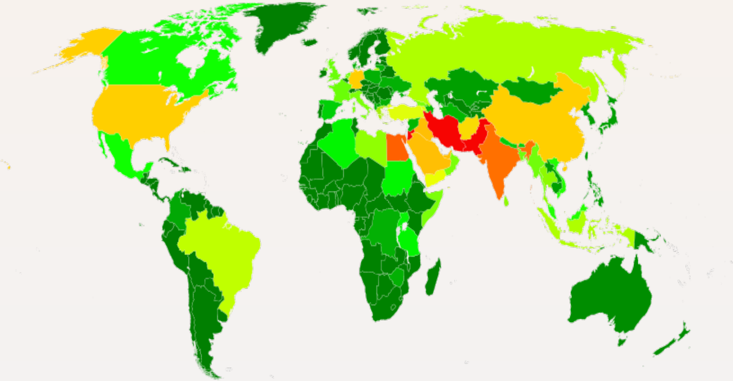


Figure: Map of global NSA data collection

Context

Public key Cryptography

- Authentication
- Encryption
- Integrity
- Digital signature

Some primitives : key exchange, zero-knowledge proofs, homomorphic encryption, commitment schemes, pseudo-random number generators, ...

Applications

- Military and governments
- Privacy and anonymity
- Communications
- E-commerce

Bad News

Powerful quantum computers will be released in less than **15 years**

Impact : Such a computer will break the most popular public key cryptosystems :

- RSA,
- DSA,
- ECDSA,
- ECC,
- HECC,
- ...

can be attacked in polynomial time using Shor's algorithm

Good News : PQ-Cryptography

Post-quantum cryptography deals with cryptosystems that

- run on conventional computers and
- are secure against attacks by quantum computers.

Examples

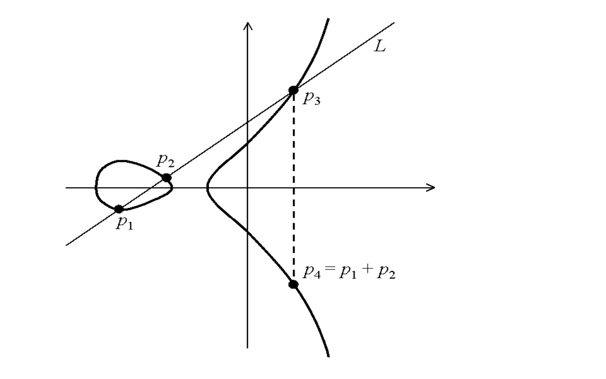
- Hash-based cryptography
- Code-based cryptography
- Lattice-based cryptography
- Multivariate-equations cryptography
- **Isogeny-based cryprography**

Elliptic curves

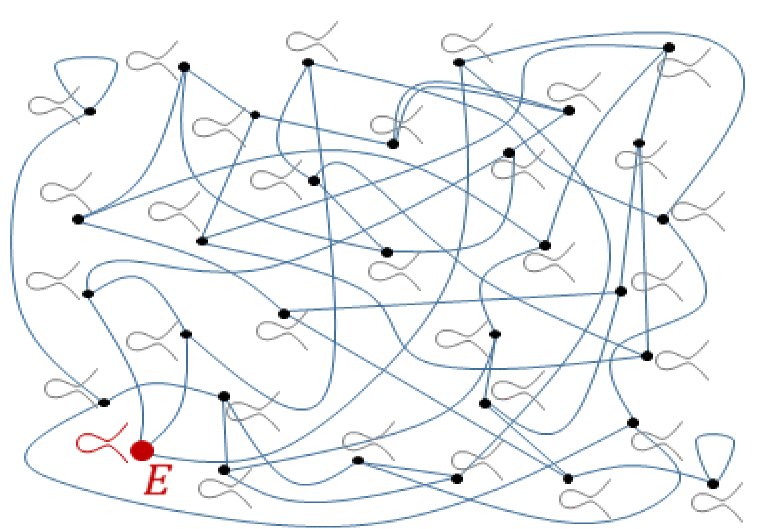
Elliptic curve

An elliptic curve E over a field K can be written in Weierstrass form

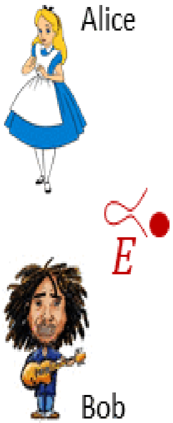
$$y^2 = f(x), \quad with \ \deg(f) = 3.$$



Isogeny-based Cryptography



Isogeny Diffie-Hellman Key Exchange



The FAST challenges (1/2)

FAster Cryptography

- The rise of connected devices (the Internet of Things) in Africa; but they can only be used if they are secure.
- The first challenge is Their lack of memory and computing power makes any cryptographic computation very hard.
- The FAST team will improve algorithms on elliptic curve to better take into account the specific constraints of these devices.
- We will also use abelian varieties of greater dimension to be able to gain a factor two in the size of the base field.

The FAST challenges (2/2)

STronger Cryptography

- The team will study new protocols based on the isogeny graphs of supersingular elliptic curves which are quantum resistant.
- The drawback of this new protocol (like the others quantum-resistant protocols) is that it takes considerably more time and memory than the classical one.
- We will improve these isogenies computations by studying the corresponding moduli spaces.

Organization

- Cameroun : École Normale Supérieure de Bambili, Université de Ngaoundéré, Université de Yaoundé 1;
- France : Inria Bordeaux, Université de Bordeaux, Université de Rennes;
- Gabon : Université des Sciences et Techniques de Masuku, Franceville;
- Mali : Université de Bamako;
- Senegal : Université Cheikh Anta Diop de Dakar, École Polytechnique de Thiès.

Thank you for your attention !