“Le monde change, les métiers aussi”

# JOURNÉE DE LA FORMATION PROFESSIONNELLE DE L'UGA

CONFÉRENCES / ATELIERS / RENCONTRES

**11 AVRIL 2024**

DOMAINE UNIVERSITAIRE
DE SAINT-MARTIN-D'HÈRES

GRENOBLE INP UGA

UGA Université Grenoble Alpes

ANNÉE EUROPÉENNE DES COMPÉTENCES

# Quel avenir pour les courbes elliptiques en cryptographie ?

Vanessa Vitse

Université Grenoble Alpes

AMUSEC – 22 mars 2024

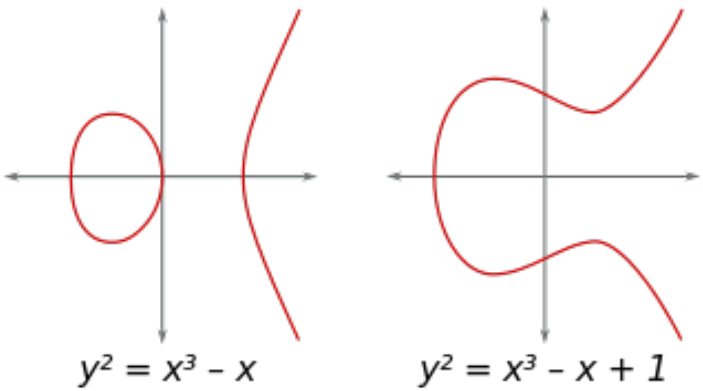
# 40 ans (ou presque) de courbes elliptiques en cryptographie

XVIIIe – XIXe siècle : étude des fonctions et intégrales elliptiques, en lien avec le calcul du périmètre d'une ellipse

À partir de 1950 : développement de la géométrie algébrique moderne

1976-1977 : Diffie-Hellman et RSA, apparition de la cryptographie à clef publique

1985-1986 : Miller et Koblitz proposent l'utilisation de courbes elliptiques en cryptographie




## ECDLP :

Étant donnés $P \in E(\mathbb{F}_q)$, $Q \in \langle P \rangle$
trouver $s \in \mathbb{Z}$ tel que $Q = sP$

# Des avantages certains

- Taille de clefs publiques / privées et de signature plus petite qu'avec RSA / DLP sur corps finis
- Temps de calcul plus court
- Versatilité : courbes elliptiques utilisables en échange de clefs (ECDH), chiffrement (ElGamal), signature (ECDSA)
- Pas de brevet ! (RSA : brevet jusqu'en 2000)

## Des avantages certains

- Taille de clefs publiques / privées et de signature plus petite qu'avec RSA / DLP sur corps finis
- Temps de calcul plus court
- Versatilité : courbes elliptiques utilisables en échange de clefs (ECDH), chiffrement (ElGamal), signature (ECDSA)
- Pas de brevet ! (RSA : brevet jusqu'en 2000)

## Une seule contrainte

**Résistance aux attaques génériques**

$\#E(\mathbb{F}_q)$ divisible par un grand nombre premier

# Débuts difficiles et doutes persistants

Problème comment calculer efficacement la cardinalité d'une courbe ?

- facile sur courbes supersingulières
  $\longrightarrow$ attaque par transfert (MOV et Frey-Rück)
- facile sur $E(\mathbb{F}_{q^d})$ si $\#E(\mathbb{F}_q)$ connu
  $\longrightarrow$ attaque par descente de Weil
- contournable avec la méthode de multiplication complexe
- comptage de points efficace à partir de 1995 (Schoof, SEA)

# Débuts difficiles et doutes persistants

Problème comment calculer efficacement la cardinalité d'une courbe ?

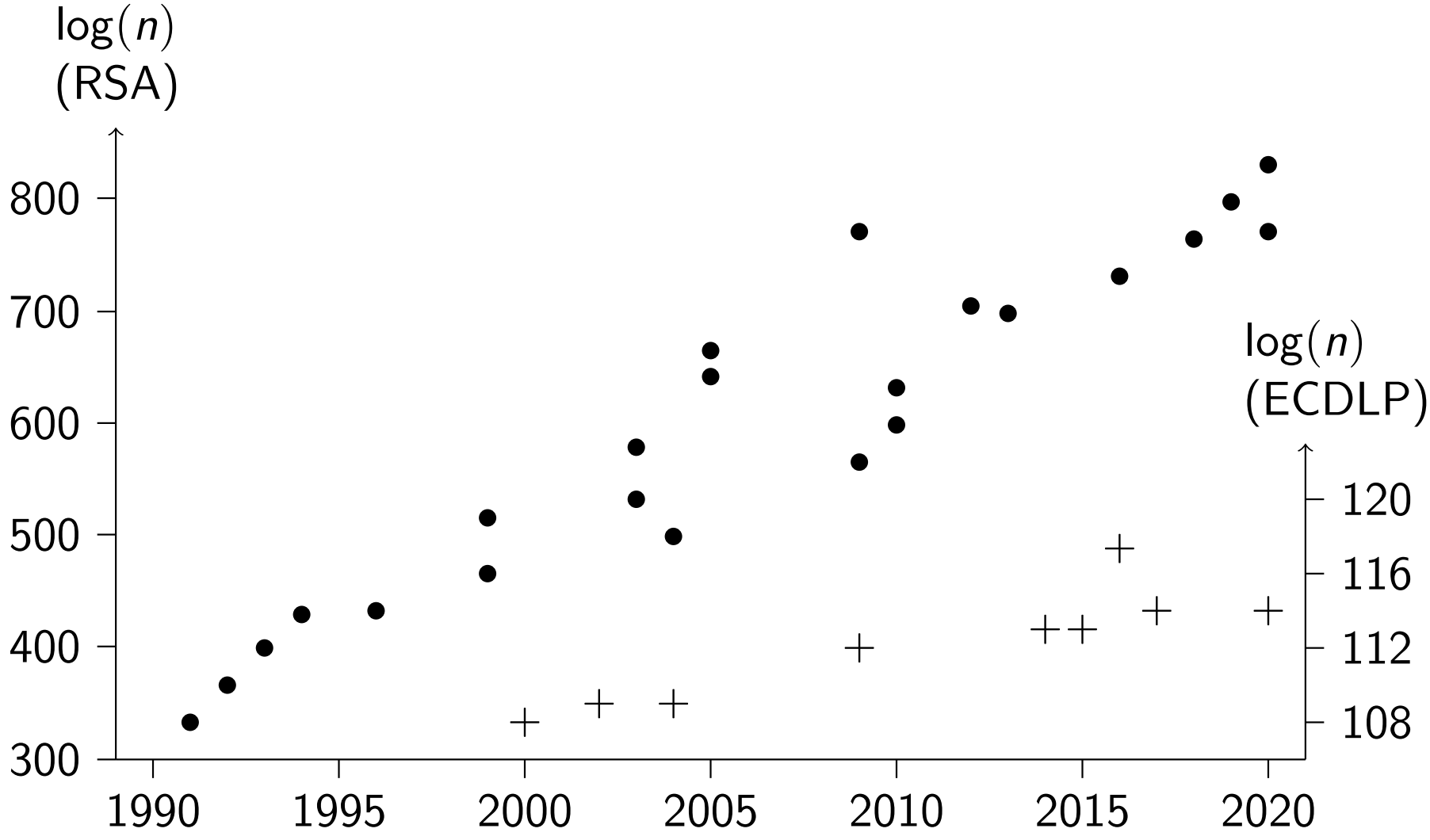
- facile sur courbes supersingulières
  → attaque par transfert (MOV et Frey-Rück)
- facile sur $E(\mathbb{F}_{q^d})$ si $\#E(\mathbb{F}_q)$ connu
  → attaque par descente de Weil
- contournable avec la méthode de multiplication complexe
- comptage de points efficace à partir de 1995 (Schoof, SEA)

## 1990-2000

- Lobbying intense de RSA Security contre les courbes elliptiques
  « *Trop abstrait, trop compliqué...* »
- **Fort doutes** sur les courbes proposées par le NIST
- Existence d'autres vulnérabilités ??

# Un concurrent qui s'effondre

Depuis 1985 très peu de progrès spécifiques ECDLP mais **gros progrès** sur la factorisation (NFS)



# Un concurrent qui s'effondre

**Cryptographie hybride**
Crypto asymétrique utilisée actuellement seulement pour échange de clefs et signature ; courbes mieux adaptées pour ça que RSA

**Actuellement**

RSA en chiffrement/échange de clefs supprimé dans TLS 1.3

**SafeCurve project** catalogue de courbes sûres et sans backdoor

# Une vraie menace

| | |
|---|---|
| Shor 1994 : | algorithme quantique pour factoriser et calculer des log discrets en temps polynomial |
| 2015 : | la NSA conseille de passer à la crypto post-quantique |
| 2016-2023 : | compétition de standardisation de la crypto post-quantique par le NIST |

Faut-il abandonner les courbes elliptiques ?

# Faire fonctionner l'algorithme de Shor

But : trouver $s$ tel que $Q = sP$

## Partie quantique

**Recherche de périodes** de la fonction $\begin{array}{ccc} \mathbb{Z}^2 & \to & E \\ (x,y) & \mapsto & xP + yQ \end{array}$

(retrouver $s$ à partir de $t_1 P + t_2 Q = \mathcal{O}$ est facile en général)

Requiert d'effectuer la transformation

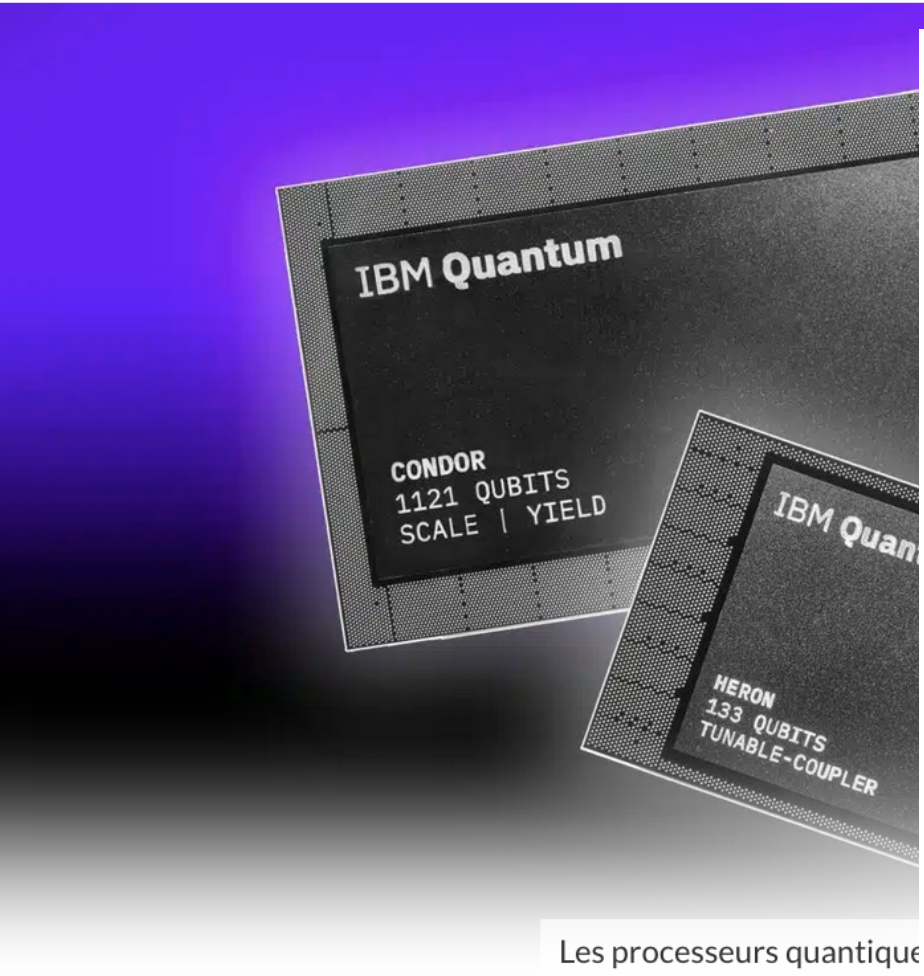
$$|x\rangle \otimes |y\rangle \otimes |\mathcal{O}\rangle \mapsto |x\rangle \otimes |y\rangle \otimes |xP + yQ\rangle$$

sur un registre de qubits **en superposition d'états**
$\longrightarrow$ besoin de $O(\log(p))$ qubits

Roetteler-Naehrig-Svore-Lauter : $\approx$ **1500** qubits pour l'algorithme de Shor avec $p$ de 160 bits

# IBM dévoile deux processeurs quantiques innovants, dont un comptant plus de 1121 qubits

Miotisoa Randrianarisoa & J. Paiano · 5 décembre 2023




Les processeurs quantique

# Record : cet ordinateur quantique intègre plus de 1 000 qubits

*Soit plus de deux fois plus qu'Osprey, précédent détenteur du record développé par IBM*

*Image d'illustration — metamorworks / Shutterstock.com*



# Atom Computing a dévoilé le premier ordinateur quantique dépassant la barre des 1

# Don't panic !

Nombres de qubits **peu pertinent** sans savoir si on peut :

- les intriquer
- les manipuler fiablement (portes logiques quantiques)

**Gros** problème de stabilité des qubits
$\longrightarrow$ besoin d'importante capacité de correction d'erreurs

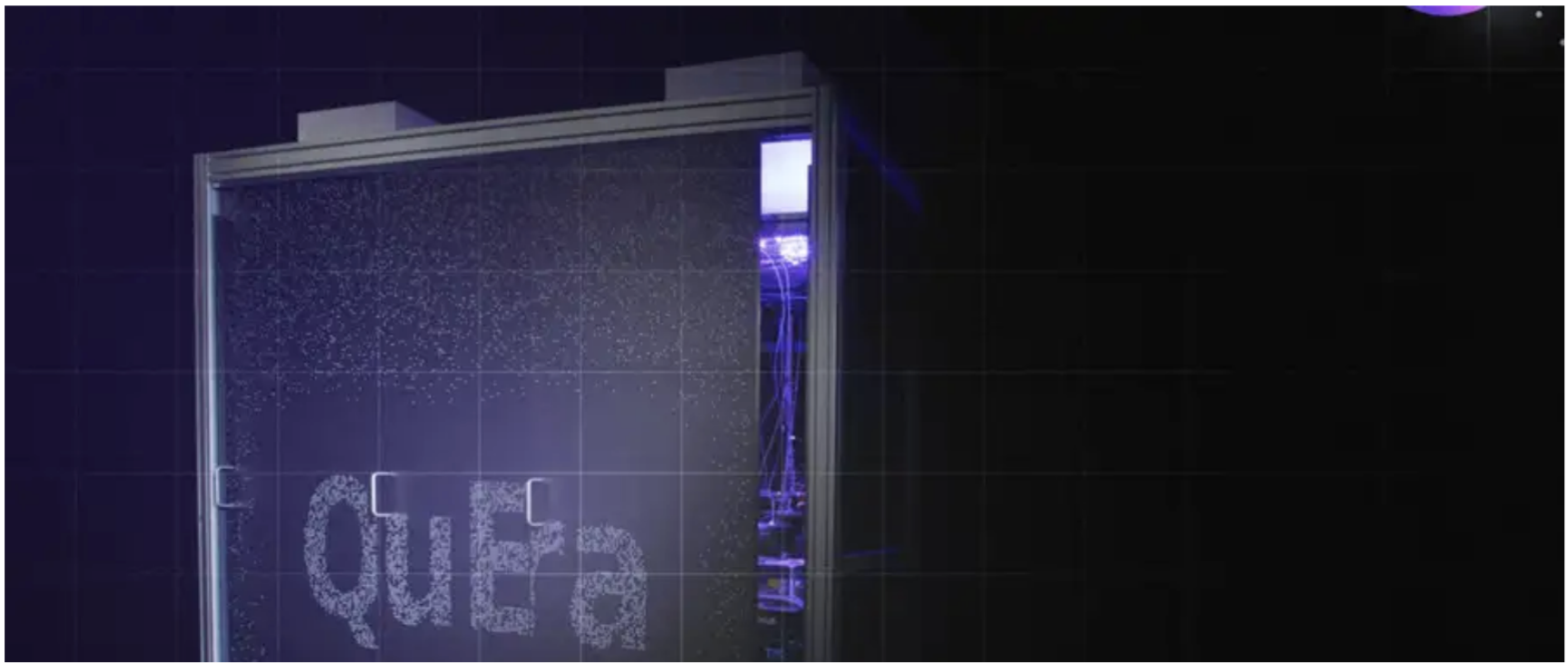
Technology

# Quantum computer sets record on path towards error-free calculations

A quantum computer contains the largest ever number of "logical quantum bits", which can be used for error-free calculations

By Karmela Padavic-Callaghan

6 December 2023



# Actuellement

- $\approx 50$ qubits $+ \approx 200$ qubits pour la redondance
- passent une centaine de portes logiques

On est encore loin du compte !

| ECDLP in $E(\mathbb{F}_p)$ estimation (Roetteler-Naehrig-Svore-Lauter) | | | |
|---|---|---|---|
| $\lceil \log_2(p) \rceil$ bits | # Qubits | # Toffoli gates | Toffoli depth |
| 160 | 1466 | $2.97 \cdot 10^{10}$ | $2.73 \cdot 10^{10}$ |
| 192 | 1754 | $5.30 \cdot 10^{10}$ | $4.86 \cdot 10^{10}$ |
| 256 | 2330 | $1.26 \cdot 10^{11}$ | $1.16 \cdot 10^{11}$ |

# Faut-il abandonner les courbes elliptiques ?

Shor **n'a encore jamais** été complètement implémenté
$\longrightarrow$ quel risque pour la crypto à base de courbe ?

**Harvest now, Decrypt later**

Un adversaire peut

- stocker vos échanges chiffrés dès maintenant
- les déchiffrer quand il aura accès à un ordinateur quantique assez puissant

Alternative à ECC / RSA : **crypto post-quantique**, plus lente, avec clés plus grosses

# Faut-il abandonner les courbes elliptiques ?

Harvest now, Decrypt later : **risque** en chiffrement

$\longrightarrow$ passage au post-quantique pour protéger des données potentiellement encore sensibles dans $\geqslant$ 10 ans

**Aucun risque** en signature / authentification

post-quantique inutile avant l'apparition d'un ordinateur quantique

# Les courbes elliptiques au-delà du log discret

Autres fonctions à sens unique sur les courbes elliptiques, en plus de la multiplication $n \mapsto nP$ :

1. **couplages** : $E[n] \times E[n] \to \mathbb{F}_q^*$
2. calculs **d'isogénies** :
   À partir de $E$ et $G \subset E$ avec $\#G$ friable, détermination de $E'$ et $\phi : E \to E'$ telles que $\ker \phi = G$ avec formules de Vélu

# Couplage sur courbes elliptiques

Couplage : application $E[n] \times E'[n] \longrightarrow \mathbb{F}_{q^d}^*$

- **bilinéaire**, non dégénérée
- effectivement calculable pour $E$ *pairing-friendly*
- difficile à inverser ($\leftsquigarrow$ DLP dans $E$ ou dans $\mathbb{F}_{q^d}^*$)

Permet des constructions élégantes (mais pas post-quantiques !).

Première application en crypto : schéma de **chiffrement basé sur l'identité** (IBE) de Boneh-Franklin (2001)

# zk-SNARK

Application actuelle des couplages en cryptographie : zk-SNARK
Déployés dans des technologies à base de blockchain (cryptomonnaie) ou calcul multipartite

- zero-knowledge
- succinct
- non-interactive
- argument of knowledge

Permet de démontrer qu'on a effectué un certain calcul, par ex : un paiement a été réalisé, **sans divulguer** le montant, le vendeur ou l'acheteur

zk-SNARK basés sur couplages **pas post-quantiques** ; pas gênant pour applications blockchain

# Crypto basée sur isogénies

## Le protocole SIDH / SIKE *(Supersingular isogeny Diffie-Hellman)*

- sélectionné pour le 4e round de normalisation post-quantique du NIST
- taille de clés bien plus petite que tous les autres concurrents
- basé sur le problème suivant :

Soient $E$, $E'$ deux courbes supersingulières sur $\mathbb{F}_{p^2}$ et $\phi : E \to E'$ isogénie de degré $2^n \approx \sqrt{p}$.
Connaissant $E$, $E'$, $\deg \phi$ et l'image par $\phi$ de points auxilliaires, retrouver $\ker \phi$.

# Crypto basée sur isogénies

## Le protocole SIDH / SIKE *(Supersingular isogeny Diffie-Hellman)*

- sélectionné pour le 4e round de normalisation post-quantique du NIST
- taille de clés bien plus petite que tous les autres concurrents
- basé sur le problème suivant :

Soient $E$, $E'$ deux courbes supersingulières sur $\mathbb{F}_{p^2}$ et $\phi : E \to E'$ isogénie de degré $2^n \approx \sqrt{p}$.
Connaissant $E$, $E'$, $\deg \phi$ et l'image par $\phi$ de points auxilliaires, retrouver $\ker \phi$.

- définitivement cassé en 2022...

# Crypto basée sur isogénies

Il reste des **problèmes difficiles** et post-quantiques sur les isogénies :

- trouver des isogénies entre deux courbes supersingulières
- calculer l'anneau des endomorphismes d'une courbe supersingulière
- analogues avec des courbes algébriques de genre plus grand

Plusieurs schémas chiffrement / signature existent (C-SIDH, SQIsign)
Pour l'instant : aucun ne s'impose significativement, mais ça pourrait changer !

# Quel avenir pour les courbes elliptiques en cryptographie ?

Vanessa Vitse

Université Grenoble Alpes

AMUSEC – 22 mars 2024