Séminaire Épiphymaths

Jeudi 18 octobre 2012

« Cryptographie et problème du logarithme discret »

Cryptographie et problème du logarithme discret

Crypto provient du Grec "*kruptos*" = caché.

Graphie de *graphein* = écrire.

Cryptologie $\rightsquigarrow$ science du secret.

Cryptanalyse $\rightsquigarrow$ étude des messages secrets pour les décoder.

Cryptogramme $\rightsquigarrow$ message secret.

"Crypter", "décrypter" ne sont pas acceptés par l'Académie Française (préfère coder et décoder). Mais, on les utilise souvent...

Cryptographie et problème du logarithme discret

Crypto provient du Grec "*kruptos*" = caché.

Graphie de *graphein* = écrire.

Cryptologie $\rightsquigarrow$ science du secret.

Cryptanalyse $\rightsquigarrow$ étude des messages secrets pour les décoder.

Cryptogramme $\rightsquigarrow$ message secret.

"Crypter", "décrypter" ne sont pas acceptés par l'Académie Française (préfère coder et décoder). Mais, on les utilise souvent...

Cryptographie et problème du logarithme discret

Crypto provient du Grec "*kruptos*" = caché.

Graphie de *graphein* = écrire.

Cryptologie $\rightsquigarrow$ science du secret.

Cryptanalyse $\rightsquigarrow$ étude des messages secrets pour les décoder.

Cryptogramme $\rightsquigarrow$ message secret.

"Crypter", "décrypter" ne sont pas acceptés par l'Académie Française (préfère coder et décoder). Mais, on les utilise souvent...

Les buts de la cryptologie

1. Confidentialité : le texte codé ne peut pas être lu par un intrus.
2. Authentification : Le destinataire doit être sûr de l'auteur du message.
3. Intégrité : le message n'a pas été modifié pendant la transmission.
4. La non-répudiation : l'expéditeur ne peut pas nier être l'auteur du message.
5. Et quelques autres... ex. : jouer à pile ou face par téléphone.

La cryptologie moderne répond à ces demandes.

Les buts de la cryptologie

1. Confidentialité : le texte codé ne peut pas être lu par un intrus.
2. Authentification : Le destinataire doit être sûr de l'auteur du message.
3. Intégrité : le message n'a pas été modifié pendant la transmission.
4. La non-répudiation : l'expéditeur ne peut pas nier être l'auteur du message.
5. Et quelques autres... ex. : jouer à pile ou face par téléphone.

La cryptologie moderne répond à ces demandes.

Les buts de la cryptologie

1. Confidentialité : le texte codé ne peut pas être lu par un intrus.
2. Authentification : Le destinataire doit être sûr de l'auteur du message.
3. Intégrité : le message n'a pas été modifié pendant la transmission.
4. La non-répudiation : l'expéditeur ne peut pas nier être l'auteur du message.
5. Et quelques autres... ex. : jouer à pile ou face par téléphone.

La cryptologie moderne répond à ces demandes.

Les buts de la cryptologie

1. Confidentialité : le texte codé ne peut pas être lu par un intrus.
2. Authentification : Le destinataire doit être sûr de l'auteur du message.
3. Intégrité : le message n'a pas été modifié pendant la transmission.
4. La non-répudiation : l'expéditeur ne peut pas nier être l'auteur du message.
5. Et quelques autres... ex. : jouer à pile ou face par téléphone.

La cryptologie moderne répond à ces demandes.

Les buts de la cryptologie

1. Confidentialité : le texte codé ne peut pas être lu par un intrus.
2. Authentification : Le destinataire doit être sûr de l'auteur du message.
3. Intégrité : le message n'a pas été modifié pendant la transmission.
4. La non-répudiation : l'expéditeur ne peut pas nier être l'auteur du message.
5. Et quelques autres... ex. : jouer à pile ou face par téléphone.

La cryptologie moderne répond à ces demandes.

Les buts de la cryptologie

1. Confidentialité : le texte codé ne peut pas être lu par un intrus.
2. Authentification : Le destinataire doit être sûr de l'auteur du message.
3. Intégrité : le message n'a pas été modifié pendant la transmission.
4. La non-répudiation : l'expéditeur ne peut pas nier être l'auteur du message.
5. Et quelques autres... ex. : jouer à pile ou face par téléphone.

La cryptologie moderne répond à ces demandes.

Les buts de la cryptologie

1. Confidentialité : le texte codé ne peut pas être lu par un intrus.
2. Authentification : Le destinataire doit être sûr de l'auteur du message.
3. Intégrité : le message n'a pas été modifié pendant la transmission.
4. La non-répudiation : l'expéditeur ne peut pas nier être l'auteur du message.
5. Et quelques autres... ex. : jouer à pile ou face par téléphone.

La cryptologie moderne répond à ces demandes.

Les buts de la cryptologie

1. Confidentialité : le texte codé ne peut pas être lu par un intrus.
2. Authentification : Le destinataire doit être sûr de l'auteur du message.
3. Intégrité : le message n'a pas été modifié pendant la transmission.
4. La non-répudiation : l'expéditeur ne peut pas nier être l'auteur du message.
5. Et quelques autres... ex. : jouer à pile ou face par téléphone.

La cryptologie moderne répond à ces demandes.

Les 2 familles de cryptographie

1. La cryptographie à clef secrète (ou symétrique).

   PRINCIPE : L'émetteur et le récepteur partagent le même secret pour crypter et décrypter.

2. La cryptographie à clef publique (ou asymétrique).

   PRINCIPE : Une clé publique (tout le monde la connaît) pour crypter. Une clé secrète (seulement) détenu par le récepteur permet de décrypter.

Les 2 familles de cryptographie

1. La cryptographie à clef secrète (ou symétrique).

   PRINCIPE : L'émetteur et le récepteur partagent le même secret pour crypter et décrypter.

2. La cryptographie à clef publique (ou asymétrique).

   PRINCIPE : Une clé publique (tout le monde la connaît) pour crypter. Une clé secrète (seulement) détenu par le récepteur permet de décrypter.

Les 2 familles de cryptographie

1. La cryptographie à clef secrète (ou symétrique).

   PRINCIPE : L'émetteur et le récepteur partagent le même secret pour crypter et décrypter.

2. La cryptographie à clef publique (ou asymétrique).

   PRINCIPE : Une clé publique (tout le monde la connaît) pour crypter. Une clé secrète (seulement) détenu par le récepteur permet de décrypter.

Les 2 familles de cryptographie

1. La cryptographie à clef secrète (ou symétrique).

   PRINCIPE : L'émetteur et le récepteur partagent le même secret pour crypter et décrypter.

2. La cryptographie à clef publique (ou asymétrique).

   PRINCIPE : Une clé publique (tout le monde la connaît) pour crypter. Une clé secrète (seulement) détenu par le récepteur permet de décrypter.

Les 2 familles de cryptographie

1. La cryptographie à clef secrète (ou symétrique).

   PRINCIPE : L'émetteur et le récepteur partagent le même secret pour crypter et décrypter.

2. La cryptographie à clef publique (ou asymétrique).

   PRINCIPE : Une clé publique (tout le monde la connaît) pour crypter. Une clé secrète (seulement) détenu par le récepteur permet de décrypter.

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Exemples :

Chiffrement à la César ou du même type $\left\{ \begin{array}{ccc} A & \to & C \\ B & \to & D \\ C & \to & E \\ & etc. & \end{array} \right.$ ($\rightsquigarrow$ Très faible).

Machine historique : ENIGMA
Utilisée par les Allemands
Cassée par des mathématiciens.

Systèmes modernes :

- DES : Data Encryption Standard.
- AES : Advanced Encryption Standard.
- etc.

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Exemples :

Chiffrement à la César
ou du même type

$$\begin{cases} A & \to & C \\ B & \to & D \\ C & \to & E \\ & etc. & \end{cases}$$

($\rightsquigarrow$ Très faible).

Machine historique : ENIGMA
Utilisée par les Allemands
Cassée par des mathématiciens.

Systèmes modernes :

- DES : Data Encryption Standard.
- AES : Advanced Encryption Standard.
- etc.

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Exemples :

Chiffrement à la César
ou du même type : $\begin{cases} A & \to & C \\ B & \to & D \\ C & \to & E \\ & etc. & \end{cases}$ ($\rightsquigarrow$ Très faible).

Machine historique : ENIGMA
Utilisée par les Allemands
Cassée par des mathématiciens.

Systèmes modernes :

- DES : Data Encryption Standard.
- AES : Advanced Encryption Standard.
- etc.

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Exemples :

Chiffrement à la César
ou du même type

$$: \begin{cases} A & \to & C \\ B & \to & D \\ C & \to & E \\ & etc. & \end{cases}$$

($\rightsquigarrow$ Très faible).

Machine historique : ENIGMA
Utilisée par les Allemands
Cassée par des mathématiciens.

Systèmes modernes :

- DES : Data Encryption Standard.
- AES : Advanced Encryption Standard.
- etc.

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Exemples :

Chiffrement à la César
ou du même type

$$: \begin{cases} A & \to & C \\ B & \to & D \\ C & \to & E \\ & etc. & \end{cases}$$

($\rightsquigarrow$ Très faible).

Machine historique : ENIGMA
Utilisée par les Allemands
Cassée par des mathématiciens.

Systèmes modernes :

- DES : Data Encryption Standard.
- AES : Advanced Encryption Standard.
- etc.

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Exemples :

Chiffrement à la César
ou du même type

$$: \begin{cases} A & \to & C \\ B & \to & D \\ C & \to & E \\ & etc. & \end{cases}$$

($\rightsquigarrow$ Très faible).

Machine historique : ENIGMA
Utilisée par les Allemands
Cassée par des mathématiciens.

Systèmes modernes :

- DES : Data Encryption Standard.
- AES : Advanced Encryption Standard.
- etc.

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Exemples :

Chiffrement à la César
ou du même type

$$: \begin{cases} A & \to & C \\ B & \to & D \\ C & \to & E \\ & etc. & \end{cases}$$

($\rightsquigarrow$ Très faible).

Machine historique : ENIGMA
Utilisée par les Allemands
Cassée par des mathématiciens.

Systèmes modernes :

- DES : Data Encryption Standard.
- AES : Advanced Encryption Standard.
- etc.

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Exemples :

Chiffrement à la César
ou du même type

$$: \begin{cases} A & \to & C \\ B & \to & D \\ C & \to & E \\ & etc. & \end{cases}$$

($\rightsquigarrow$ Très faible).

Machine historique : ENIGMA
Utilisée par les Allemands
Cassée par des mathématiciens.

Systèmes modernes :

- DES : Data Encryption Standard.
- AES : Advanced Encryption Standard.
- etc.

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Avantages :

- Les systèmes (AES, etc.) sont "sûrs".
- Le cryptage et le décryptage sont rapides à effectuer.

Inconvénients :

- Il faut beaucoup de clefs.
  Il faut $\frac{n(n-1)}{2}$ clés pour un réseau de n personnes.
- Il faut échanger les clefs !
  Question : Comment échanger les clefs ?

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Avantages :

- Les systèmes (AES, etc.) sont "sûrs".
- Le cryptage et le décryptage sont rapides à effectuer.

Inconvénients :

- Il faut beaucoup de clefs.
  Il faut $\frac{n(n-1)}{2}$ clés pour un réseau de n personnes.
- Il faut échanger les clefs !
  Question : Comment échanger les clefs ?

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Avantages :

- Les systèmes (AES, etc.) sont "sûrs".
- Le cryptage et le décryptage sont rapides à effectuer.

Inconvénients :

- Il faut beaucoup de clefs.
  Il faut $\frac{n(n-1)}{2}$ clés pour un réseau de n personnes.
- Il faut échanger les clefs !
  Question : Comment échanger les clefs ?

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Avantages :

- Les systèmes (AES, etc.) sont "sûrs".
- Le cryptage et le décryptage sont rapides à effectuer.

Inconvénients :

- Il faut beaucoup de clefs.
  Il faut $\frac{n(n-1)}{2}$ clés pour un réseau de n personnes.
- Il faut échanger les clefs !
  Question : Comment échanger les clefs ?

La cryptographie à clef secrète

PRINCIPE : Même clef pour coder et pour décoder.

Avantages :

- Les systèmes (AES, etc.) sont "sûrs".
- Le cryptage et le décryptage sont rapides à effectuer.

Inconvénients :

- Il faut beaucoup de clefs.

  Il faut $\frac{n(n-1)}{2}$ clés pour un réseau de n personnes.

- Il faut échanger les clefs !

  Question : Comment échanger les clefs ?

La cryptographie à clef publique

PRINCIPE : Une clef pour coder et un secret pour décoder.

$\rightsquigarrow$ Pour créer un tel système, il faut une fonction à sens unique :

C'est une fonction f telle que :

- Il est facile de calculer $f(x)$.
- Connaissant $f(x)$, il est difficile de trouver x.

Premier système apparu $\approx$ 1977 :

Il s'agit du système R.S.A.

Inventé par Rivest, Shamir, Adleman.

Autres systèmes

- Cryptosystème de ElGamal.
- DSA : Digital Signature Algorithm.
- ECDSA : Elliptic Curve Digital Signature Algorithm.
- etc.

La cryptographie à clef publique

PRINCIPE : Une clef pour coder et un secret pour décoder.

$\rightsquigarrow$ Pour créer un tel système, il faut une fonction à sens unique :

C'est une fonction f telle que :

- Il est facile de calculer $f(x)$.
- Connaissant $f(x)$, il est difficile de trouver x.

Premier système apparu $\approx$ 1977 :

Il s'agit du système R.S.A.

Inventé par Rivest, Shamir, Adleman.

Autres systèmes

- Cryptosystème de ElGamal.
- DSA : Digital Signature Algorithm.
- ECDSA : Elliptic Curve Digital Signature Algorithm.
- etc.

La cryptographie à clef publique

PRINCIPE : Une clef pour coder et un secret pour décoder.

$\rightsquigarrow$ Pour créer un tel système, il faut une fonction à sens unique :

C'est une fonction f telle que :

- Il est facile de calculer $f(\mathbf{x})$.
- Connaissant $f(\mathbf{x})$, il est difficile de trouver $\mathbf{x}$.

Premier système apparu $\approx$ 1977 :

Il s'agit du système R.S.A.

Inventé par Rivest, Shamir, Adleman.

Autres systèmes

- Cryptosystème de ElGamal.
- DSA : Digital Signature Algorithm.
- ECDSA : Elliptic Curve Digital Signature Algorithm.
- etc.

La cryptographie à clef publique

PRINCIPE : Une clef pour coder et un secret pour décoder.

$\rightsquigarrow$ Pour créer un tel système, il faut une fonction à sens unique :

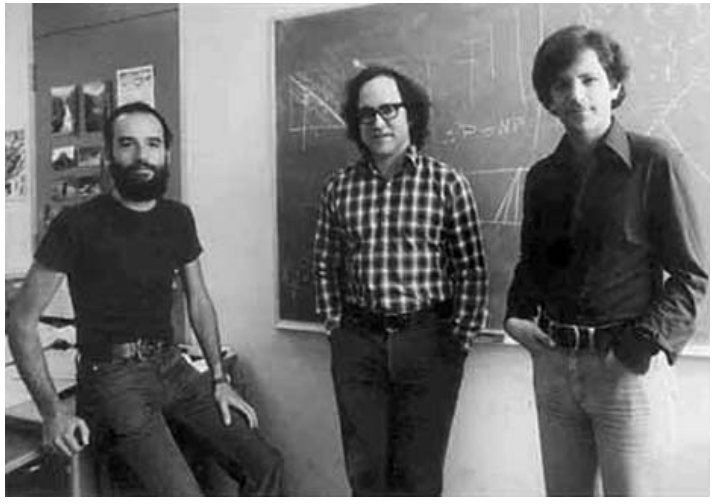
C'est une fonction f telle que :

- Il est facile de calculer $f(\mathbf{x})$.
- Connaissant $f(\mathbf{x})$, il est difficile de trouver $\mathbf{x}$.

Premier système apparu $\approx$ 1977 :

Il s'agit du système R.S.A.

Inventé par Rivest, Shamir, Adleman.



Autres systèmes

- Cryptosystème de ElGamal.
- DSA : Digital Signature Algorithm.
- ECDSA : Elliptic Curve Digital Signature Algorithm.
- etc.

La cryptographie à clef publique

PRINCIPE : Une clef pour coder et un secret pour décoder.

$\rightsquigarrow$ Pour créer un tel système, il faut une fonction à sens unique :

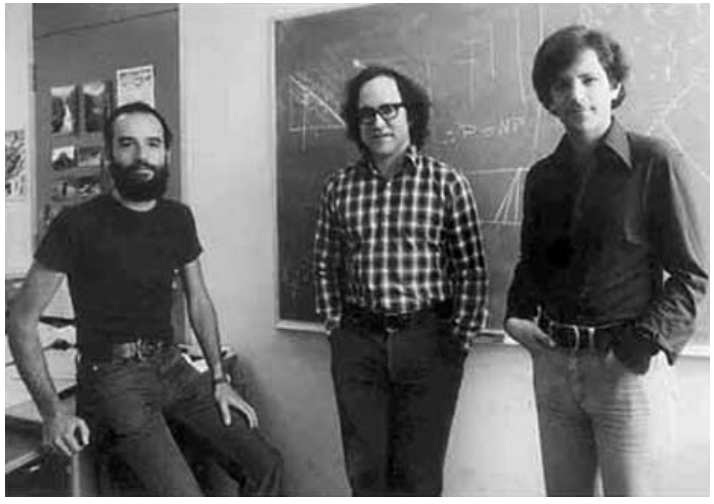
C'est une fonction f telle que :

- Il est facile de calculer $f(\mathbf{x})$.
- Connaissant $f(\mathbf{x})$, il est difficile de trouver $\mathbf{x}$.

Premier système apparu $\approx$ 1977 :

Il s'agit du système R.S.A.

Inventé par Rivest, Shamir, Adleman.



Autres systèmes

- Cryptosystème de ElGamal.
- DSA : Digital Signature Algorithm.
- ECDSA : Elliptic Curve Digital Signature Algorithm.
- etc.

Le problème du logarithme discret

Soit G un groupe cyclique engendré par g d'ordre n :

$$G = \{1, g, g^2, \cdots, g^{n-1}\}$$

On suppose que les opérations se font rapidement dans G.

$\rightsquigarrow$ Connaissant g et $\ell \in \mathbb{Z}$, il est facile de calculer $y = g^\ell \in G$.

En revanche, la réciproque...

Pb du log discret en base g

Soit $y \in G$, trouver $\ell \in \mathbb{Z}$ tel que $g^\ell = y$ est le problème du logarithme discret en base g. On note :

$$\ell = \log_g y$$

$\rightsquigarrow$ En principe, ce problème est difficile.

$\rightsquigarrow$ En principe, on a donc une fonction à sens unique : la fonction puissance dans G.

Le problème du logarithme discret

Soit G un groupe cyclique engendré par g d'ordre n :

$$G = \{1, g, g^2, \cdots, g^{n-1}\}$$

On suppose que les opérations se font rapidement dans G.

$\rightsquigarrow$ Connaissant g et $\ell \in \mathbb{Z}$, il est facile de calculer $y = g^\ell \in G$.

En revanche, la réciproque...

Pb du log discret en base g

Soit $y \in G$, trouver $\ell \in \mathbb{Z}$ tel que $g^\ell = y$ est le problème du logarithme discret en base g. On note :

$$\ell = \log_g y$$

$\rightsquigarrow$ En principe, ce problème est difficile.

$\rightsquigarrow$ En principe, on a donc une fonction à sens unique : la fonction puissance dans G.

Le problème du logarithme discret

Soit G un groupe cyclique engendré par g d'ordre n :

$$G = \{1, g, g^2, \cdots, g^{n-1}\}$$

On suppose que les opérations se font rapidement dans G.

$\rightsquigarrow$ Connaissant g et $\ell \in \mathbb{Z}$, il est facile de calculer $y = g^\ell \in G$.

En revanche, la réciproque...

Pb du log discret en base g

Soit $y \in G$, trouver $\ell \in \mathbb{Z}$ tel que $g^\ell = y$ est le problème du logarithme discret en base g. On note :

$$\ell = \log_g y$$

$\rightsquigarrow$ En principe, ce problème est difficile.

$\rightsquigarrow$ En principe, on a donc une fonction à sens unique : la fonction puissance dans G.

Le problème du logarithme discret

Soit G un groupe cyclique engendré par g d'ordre n :

$$G = \{1, g, g^2, \cdots, g^{n-1}\}$$

On suppose que les opérations se font rapidement dans G.

$\rightsquigarrow$ Connaissant g et $\ell \in \mathbb{Z}$, il est facile de calculer $y = g^\ell \in G$.

En revanche, la réciproque...

Pb du log discret en base g

Soit $y \in G$, trouver $\ell \in \mathbb{Z}$ tel que $g^\ell = y$ est le problème du logarithme discret en base g. On note :

$$\ell = \log_g y$$

$\rightsquigarrow$ En principe, ce problème est difficile.

$\rightsquigarrow$ En principe, on a donc une fonction à sens unique : la fonction puissance dans G.

Le problème du logarithme discret

Soit G un groupe cyclique engendré par g d'ordre n :

$$G = \{1, g, g^2, \cdots, g^{n-1}\}$$

On suppose que les opérations se font rapidement dans G.

$\rightsquigarrow$ Connaissant g et $\ell \in \mathbb{Z}$, il est facile de calculer $y = g^\ell \in G$.

En revanche, la réciproque...

Pb du log discret en base g

Soit $y \in G$, trouver $\ell \in \mathbb{Z}$ tel que $g^\ell = y$ est le problème du logarithme discret en base g. On note :

$$\ell = \log_g y$$

$\rightsquigarrow$ En principe, ce problème est difficile.

$\rightsquigarrow$ En principe, on a donc une fonction à sens unique :
la fonction puissance dans G.

Protocole Diffie-Hellman

Alice et Bob se mettent d'accord sur un groupe G et $g \in G$ d'ordre n.

$\rightsquigarrow$ Alice choisit k_A secrètement, calcule $y_A = g^{k_A}$ et l'envoie à Bob.

$\rightsquigarrow$ Bob choisit k_B secrètement, calcule $y_B = g^{k_B}$ et l'envoie à Alice.

$\rightsquigarrow$ Alice reçoit y_B et calcule $(y_B)^{k_A} = g^{k_B k_A}$.

$\rightsquigarrow$ Bob reçoit y_A et calcule $(y_A)^{k_B} = g^{k_A k_B}$.

$\rightsquigarrow$ Alice et Bob partagent le secret commun $g^{k_A k_B}$.

$\triangleright$ Un espion, Eve ou Charlie, connaît : G, g, g^{k_A} et g^{k_B}.
Il doit calculer $g^{k_A k_B}$.

Heuristique

Résoudre le problème de Diffie-Hellman i.e. trouver $g^{k_A k_B}$ en connaissant g, g^{k_A} et g^{k_B} est aussi difficile que de résoudre le problème du logarithme discret.

$\rightsquigarrow$ Il y a des pièges à éviter (ex. l'attaque de l'homme du milieu).

$\rightsquigarrow$ Le protocole Diffie-Hellman est à la base de nombreux autres.

Protocole Diffie-Hellman

Alice et Bob se mettent d'accord sur un groupe G et $g \in G$ d'ordre n.

$\rightsquigarrow$ Alice choisit k_A secrètement, calcule $y_A = g^{k_A}$ et l'envoie à Bob.

$\rightsquigarrow$ Bob choisit k_B secrètement, calcule $y_B = g^{k_B}$ et l'envoie à Alice.

$\rightsquigarrow$ Alice reçoit y_B et calcule $(y_B)^{k_A} = g^{k_B k_A}$.

$\rightsquigarrow$ Bob reçoit y_A et calcule $(y_A)^{k_B} = g^{k_A k_B}$.

$\rightsquigarrow$ Alice et Bob partagent le secret commun $g^{k_A k_B}$.

$\triangleright$ Un espion, Eve ou Charlie, connaît : G, g, g^{k_A} et g^{k_B}.
Il doit calculer $g^{k_A k_B}$.

Heuristique

Résoudre le problème de Diffie-Hellman i.e. trouver $g^{k_A k_B}$ en connaissant g, g^{k_A} et g^{k_B} est aussi difficile que de résoudre le problème du logarithme discret.

$\rightsquigarrow$ Il y a des pièges à éviter (ex. l'attaque de l'homme du milieu).

$\rightsquigarrow$ Le protocole Diffie-Hellman est à la base de nombreux autres.

Protocole Diffie-Hellman

Alice et Bob se mettent d'accord sur un groupe G et $g \in G$ d'ordre n.

$\rightsquigarrow$ Alice choisit k_A secrètement, calcule $y_A = g^{k_A}$ et l'envoie à Bob.

$\rightsquigarrow$ Bob choisit k_B secrètement, calcule $y_B = g^{k_B}$ et l'envoie à Alice.

$\rightsquigarrow$ Alice reçoit y_B et calcule $(y_B)^{k_A} = g^{k_B k_A}$.

$\rightsquigarrow$ Bob reçoit y_A et calcule $(y_A)^{k_B} = g^{k_A k_B}$.

$\rightsquigarrow$ Alice et Bob partagent le secret commun $g^{k_A k_B}$.

$\triangleright$ Un espion, Eve ou Charlie, connaît : G, g, g^{k_A} et g^{k_B}.
Il doit calculer $g^{k_A k_B}$.

Heuristique

Résoudre le problème de Diffie-Hellman i.e. trouver $g^{k_A k_B}$ en connaissant g, g^{k_A} et g^{k_B} est aussi difficile que de résoudre le problème du logarithme discret.

$\rightsquigarrow$ Il y a des pièges à éviter (ex. l'attaque de l'homme du milieu).

$\rightsquigarrow$ Le protocole Diffie-Hellman est à la base de nombreux autres.

Protocole Diffie-Hellman

Alice et Bob se mettent d'accord sur un groupe G et $g \in G$ d'ordre n.

$\rightsquigarrow$ Alice choisit k_A secrètement, calcule $y_A = g^{k_A}$ et l'envoie à Bob.

$\rightsquigarrow$ Bob choisit k_B secrètement, calcule $y_B = g^{k_B}$ et l'envoie à Alice.

$\rightsquigarrow$ Alice reçoit y_B et calcule $(y_B)^{k_A} = g^{k_B k_A}$.

$\rightsquigarrow$ Bob reçoit y_A et calcule $(y_A)^{k_B} = g^{k_A k_B}$.

$\rightsquigarrow$ Alice et Bob partagent le secret commun $g^{k_A k_B}$.

$\triangleright$ Un espion, Eve ou Charlie, connaît : G, g, g^{k_A} et g^{k_B}.
Il doit calculer $g^{k_A k_B}$.

Heuristique

Résoudre le problème de Diffie-Hellman i.e. trouver $g^{k_A k_B}$ en connaissant g, g^{k_A} et g^{k_B} est aussi difficile que de résoudre le problème du logarithme discret.

$\rightsquigarrow$ Il y a des pièges à éviter (ex. l'attaque de l'homme du milieu).

$\rightsquigarrow$ Le protocole Diffie-Hellman est à la base de nombreux autres.

Protocole Diffie-Hellman

Alice et Bob se mettent d'accord sur un groupe G et $g \in G$ d'ordre n.

$\rightsquigarrow$ Alice choisit k_A secrètement, calcule $y_A = g^{k_A}$ et l'envoie à Bob.

$\rightsquigarrow$ Bob choisit k_B secrètement, calcule $y_B = g^{k_B}$ et l'envoie à Alice.

$\rightsquigarrow$ Alice reçoit y_B et calcule $(y_B)^{k_A} = g^{k_B k_A}$.

$\rightsquigarrow$ Bob reçoit y_A et calcule $(y_A)^{k_B} = g^{k_A k_B}$.

$\rightsquigarrow$ Alice et Bob partagent le secret commun $g^{k_A k_B}$.

$\triangleright$ Un espion, Eve ou Charlie, connaît : G, g, g^{k_A} et g^{k_B}.
Il doit calculer $g^{k_A k_B}$.

Heuristique

Résoudre le problème de Diffie-Hellman i.e. trouver $g^{k_A k_B}$ en connaissant g, g^{k_A} et g^{k_B} est aussi difficile que de résoudre le problème du logarithme discret.

$\rightsquigarrow$ Il y a des pièges à éviter (ex. l'attaque de l'homme du milieu).

$\rightsquigarrow$ Le protocole Diffie-Hellman est à la base de nombreux autres.

Protocole Diffie-Hellman

Alice et Bob se mettent d'accord sur un groupe G et $g \in G$ d'ordre n.

$\rightsquigarrow$ Alice choisit k_A secrètement, calcule $y_A = g^{k_A}$ et l'envoie à Bob.

$\rightsquigarrow$ Bob choisit k_B secrètement, calcule $y_B = g^{k_B}$ et l'envoie à Alice.

$\rightsquigarrow$ Alice reçoit y_B et calcule $(y_B)^{k_A} = g^{k_B k_A}$.

$\rightsquigarrow$ Bob reçoit y_A et calcule $(y_A)^{k_B} = g^{k_A k_B}$.

$\rightsquigarrow$ Alice et Bob partagent le secret commun $g^{k_A k_B}$.

$\triangleright$ Un espion, Eve ou Charlie, connaît : G, g, g^{k_A} et g^{k_B}.
Il doit calculer $g^{k_A k_B}$.

Heuristique

Résoudre le problème de Diffie-Hellman i.e. trouver $g^{k_A k_B}$ en connaissant g, g^{k_A} et g^{k_B} est aussi difficile que de résoudre le problème du logarithme discret.

$\rightsquigarrow$ Il y a des pièges à éviter (ex. l'attaque de l'homme du milieu).

$\rightsquigarrow$ Le protocole Diffie-Hellman est à la base de nombreux autres.

Protocole Diffie-Hellman

Alice et Bob se mettent d'accord sur un groupe G et $g \in G$ d'ordre n.

$\rightsquigarrow$ Alice choisit k_A secrètement, calcule $y_A = g^{k_A}$ et l'envoie à Bob.

$\rightsquigarrow$ Bob choisit k_B secrètement, calcule $y_B = g^{k_B}$ et l'envoie à Alice.

$\rightsquigarrow$ Alice reçoit y_B et calcule $(y_B)^{k_A} = g^{k_B k_A}$.

$\rightsquigarrow$ Bob reçoit y_A et calcule $(y_A)^{k_B} = g^{k_A k_B}$.

$\rightsquigarrow$ Alice et Bob partagent le secret commun $g^{k_A k_B}$.

$\triangleright$ Un espion, Eve ou Charlie, connaît : G, g, g^{k_A} et g^{k_B}.
Il doit calculer $g^{k_A k_B}$.

Heuristique

Résoudre le problème de Diffie-Hellman i.e. trouver $g^{k_A k_B}$ en connaissant g, g^{k_A} et g^{k_B} est aussi difficile que de résoudre le problème du logarithme discret.

$\rightsquigarrow$ Il y a des pièges à éviter (ex. l'attaque de l'homme du milieu).

$\rightsquigarrow$ Le protocole Diffie-Hellman est à la base de nombreux autres.

Protocole Diffie-Hellman

Alice et Bob se mettent d'accord sur un groupe G et $g \in G$ d'ordre n.

$\rightsquigarrow$ Alice choisit k_A secrètement, calcule $y_A = g^{k_A}$ et l'envoie à Bob.

$\rightsquigarrow$ Bob choisit k_B secrètement, calcule $y_B = g^{k_B}$ et l'envoie à Alice.

$\rightsquigarrow$ Alice reçoit y_B et calcule $(y_B)^{k_A} = g^{k_B k_A}$.

$\rightsquigarrow$ Bob reçoit y_A et calcule $(y_A)^{k_B} = g^{k_A k_B}$.

$\rightsquigarrow$ Alice et Bob partagent le secret commun $g^{k_A k_B}$.

$\triangleright$ Un espion, Eve ou Charlie, connaît : G, g, g^{k_A} et g^{k_B}.
Il doit calculer $g^{k_A k_B}$.

Heuristique

Résoudre le problème de Diffie-Hellman i.e. trouver $g^{k_A k_B}$ en connaissant g, g^{k_A} et g^{k_B} est aussi difficile que de résoudre le problème du logarithme discret.

$\rightsquigarrow$ Il y a des pièges à éviter (ex. l'attaque de l'homme du milieu).

$\rightsquigarrow$ Le protocole Diffie-Hellman est à la base de nombreux autres.

Protocole Diffie-Hellman

Alice et Bob se mettent d'accord sur un groupe G et $g \in G$ d'ordre n.

$\rightsquigarrow$ Alice choisit k_A secrètement, calcule $y_A = g^{k_A}$ et l'envoie à Bob.

$\rightsquigarrow$ Bob choisit k_B secrètement, calcule $y_B = g^{k_B}$ et l'envoie à Alice.

$\rightsquigarrow$ Alice reçoit y_B et calcule $(y_B)^{k_A} = g^{k_B k_A}$.

$\rightsquigarrow$ Bob reçoit y_A et calcule $(y_A)^{k_B} = g^{k_A k_B}$.

$\rightsquigarrow$ Alice et Bob partagent le secret commun $g^{k_A k_B}$.

$\triangleright$ Un espion, Eve ou Charlie, connaît : G, g, g^{k_A} et g^{k_B}.
Il doit calculer $g^{k_A k_B}$.

Heuristique

Résoudre le problème de Diffie-Hellman i.e. trouver $g^{k_A k_B}$ en connaissant g, g^{k_A} et g^{k_B} est aussi difficile que de résoudre le problème du logarithme discret.

$\rightsquigarrow$ Il y a des pièges à éviter (ex. l'attaque de l'homme du milieu).

$\rightsquigarrow$ Le protocole Diffie-Hellman est à la base de nombreux autres.

Protocole Diffie-Hellman

Alice et Bob se mettent d'accord sur un groupe G et $g \in G$ d'ordre n.

$\rightsquigarrow$ Alice choisit k_A secrètement, calcule $y_A = g^{k_A}$ et l'envoie à Bob.

$\rightsquigarrow$ Bob choisit k_B secrètement, calcule $y_B = g^{k_B}$ et l'envoie à Alice.

$\rightsquigarrow$ Alice reçoit y_B et calcule $(y_B)^{k_A} = g^{k_B k_A}$.

$\rightsquigarrow$ Bob reçoit y_A et calcule $(y_A)^{k_B} = g^{k_A k_B}$.

$\rightsquigarrow$ Alice et Bob partagent le secret commun $g^{k_A k_B}$.

$\triangleright$ Un espion, Eve ou Charlie, connaît : G, g, g^{k_A} et g^{k_B}.
Il doit calculer $g^{k_A k_B}$.

Heuristique

Résoudre le problème de Diffie-Hellman i.e. trouver $g^{k_A k_B}$ en connaissant g, g^{k_A} et g^{k_B} est aussi difficile que de résoudre le problème du logarithme discret.

$\rightsquigarrow$ Il y a des pièges à éviter (ex. l'attaque de l'homme du milieu).

$\rightsquigarrow$ Le protocole Diffie-Hellman est à la base de nombreux autres.

Pourquoi est-il facile de calculer g^ℓ ?

Pour calculer g^ℓ, on utilise le principe suivant :

$$g^\ell = \begin{cases} \left(g^{\frac{\ell}{2}}\right)^2 & \text{si } \ell \text{ est pair} \\ g \cdot \left(g^{\frac{\ell-1}{2}}\right)^2 & \text{si } \ell \text{ est impair} \end{cases}.$$

En réitérant le procédé :

Théorème

Le calcul de g^ℓ nécessite moins de $3\log(\ell)$ multiplications dans G.

$\rightsquigarrow$ La complexité d'un calcul se mesure en fonction de la taille des données. La taille de ℓ est $\log_2 \ell$.

$\rightsquigarrow$ Le calcul de g^ℓ est donc polynomial, même linéaire.

Pourquoi est-il facile de calculer g^ℓ ?

Pour calculer g^ℓ, on utilise le principe suivant :

$$g^\ell = \begin{cases} \left(g^{\frac{\ell}{2}}\right)^2 & \text{si } \ell \text{ est pair} \\ g \cdot \left(g^{\frac{\ell-1}{2}}\right)^2 & \text{si } \ell \text{ est impair} \end{cases}.$$

En réitérant le procédé :

Théorème

Le calcul de g^ℓ nécessite moins de $3\log(\ell)$ multiplications dans G.

$\rightsquigarrow$ La complexité d'un calcul se mesure en fonction de la taille des données. La taille de ℓ est $\log_2 \ell$.

$\rightsquigarrow$ Le calcul de g^ℓ est donc polynomial, même linéaire.

Pourquoi est-il facile de calculer g^ℓ ?

Pour calculer g^ℓ, on utilise le principe suivant :

$$g^\ell = \begin{cases} \left(g^{\frac{\ell}{2}}\right)^2 & \text{si } \ell \text{ est pair} \\ g \cdot \left(g^{\frac{\ell-1}{2}}\right)^2 & \text{si } \ell \text{ est impair} \end{cases}.$$

En réitérant le procédé :

Théorème

Le calcul de g^ℓ nécessite moins de $3\log(\ell)$ multiplications dans G.

$\rightsquigarrow$ La complexité d'un calcul se mesure en fonction de la taille des données. La taille de ℓ est $\log_2 \ell$.

$\rightsquigarrow$ Le calcul de g^ℓ est donc polynomial, même linéaire.

Pourquoi est-il facile de calculer g^ℓ ?

Pour calculer g^ℓ, on utilise le principe suivant :

$$g^\ell = \begin{cases} \left(g^{\frac{\ell}{2}}\right)^2 & \text{si } \ell \text{ est pair} \\ g \cdot \left(g^{\frac{\ell-1}{2}}\right)^2 & \text{si } \ell \text{ est impair} \end{cases}.$$

En réitérant le procédé :

Théorème

Le calcul de g^ℓ nécessite moins de $3\log(\ell)$ multiplications dans G.

$\rightsquigarrow$ La complexité d'un calcul se mesure en fonction de la taille des données. La taille de ℓ est $\log_2 \ell$.

$\rightsquigarrow$ Le calcul de g^ℓ est donc polynomial, même linéaire.

Facile ? Pas facile ?

Supposons que l'entrée d'un programme soit ℓ.

- ▷ Calcul en $O(\log(\ell)) = O(e^{\log\log \ell})$ → linéaire (très facile).
- ▷ Calcul en $O(\log(\ell)^k) = O(e^{k \log\log \ell})$ → polynomial (facile).
- ▷ Calcul en $O(e^{k \log(\ell)^a (\log\log \ell)^{1-a}})$ → sous-exponentiel (compliqué).
- ▷ Calcul en $O(\ell) = O(e^{\log \ell})$ → exponentiel (très compliqué).

Exemples :

- ⇝ Calculer g^ℓ par l'exponentiation rapide → linéaire.
- ⇝ Décider si un entier ℓ est premier → polynomial.
- ⇝ Factoriser un entier ℓ → sous-exponentiel ($a = 1/3$).
- ⇝ Calculer g^ℓ en faisant $g \times g \cdots \times g$ → exponentiel.

- ▷ Et résoudre le pb. du log discret, i.e. trouver ℓ tel que $y = g^\ell$?
- ⇝ Dépend du groupe.

Facile ? Pas facile ?

Supposons que l'entrée d'un programme soit ℓ.

▷ Calcul en $O(\log(\ell)) = O(e^{\log\log\ell})$ → linéaire (très facile).

▷ Calcul en $O(\log(\ell)^k) = O(e^{k\log\log\ell})$ → polynomial (facile).

▷ Calcul en $O(e^{k\log(\ell)^a(\log\log\ell)^{1-a}})$ → sous-exponentiel (compliqué).

▷ Calcul en $O(\ell) = O(e^{\log\ell})$ → exponentiel (très compliqué).

Exemples :

⇝ Calculer g^ℓ par l'exponentiation rapide → linéaire.

⇝ Décider si un entier ℓ est premier → polynomial.

⇝ Factoriser un entier ℓ → sous-exponentiel ($a = 1/3$).

⇝ Calculer g^ℓ en faisant $g \times g \cdots \times g$ → exponentiel.

▷ Et résoudre le pb. du log discret, i.e. trouver ℓ tel que $y = g^\ell$?

⇝ Dépend du groupe.

Facile ? Pas facile ?

Supposons que l'entrée d'un programme soit ℓ.

- ▷ Calcul en $O(\log(\ell)) = O(e^{\log\log\ell})$ → linéaire (très facile).
- ▷ Calcul en $O(\log(\ell)^k) = O(e^{k\log\log\ell})$ → polynomial (facile).
- ▷ Calcul en $O(e^{k\log(\ell)^a(\log\log\ell)^{1-a}})$ → sous-exponentiel (compliqué).
- ▷ Calcul en $O(\ell) = O(e^{\log\ell})$ → exponentiel (très compliqué).

Exemples :

- ⇝ Calculer g^ℓ par l'exponentiation rapide → linéaire.
- ⇝ Décider si un entier ℓ est premier → polynomial.
- ⇝ Factoriser un entier ℓ → sous-exponentiel ($a = 1/3$).
- ⇝ Calculer g^ℓ en faisant $g \times g \cdots \times g$ → exponentiel.

- ▷ Et résoudre le pb. du log discret, i.e. trouver ℓ tel que $y = g^\ell$?
- ⇝ Dépend du groupe.

Facile ? Pas facile ?

Supposons que l'entrée d'un programme soit ℓ.

- ▷ Calcul en $O(\log(\ell)) = O(e^{\log\log\ell})$ → linéaire (très facile).
- ▷ Calcul en $O(\log(\ell)^k) = O(e^{k\log\log\ell})$ → polynomial (facile).
- ▷ Calcul en $O(e^{k\log(\ell)^a(\log\log\ell)^{1-a}})$ → sous-exponentiel (compliqué).
- ▷ Calcul en $O(\ell) = O(e^{\log\ell})$ → exponentiel (très compliqué).

Exemples :

- ⇝ Calculer g^ℓ par l'exponentiation rapide → linéaire.
- ⇝ Décider si un entier ℓ est premier → polynomial.
- ⇝ Factoriser un entier ℓ → sous-exponentiel ($a = 1/3$).
- ⇝ Calculer g^ℓ en faisant $g \times g \cdots \times g$ → exponentiel.

- ▷ Et résoudre le pb. du log discret, i.e. trouver ℓ tel que $y = g^\ell$?
- ⇝ Dépend du groupe.

Facile ? Pas facile ?

Supposons que l'entrée d'un programme soit ℓ.

- ▷ Calcul en $O(\log(\ell)) = O(e^{\log\log\ell})$ → linéaire (très facile).
- ▷ Calcul en $O(\log(\ell)^k) = O(e^{k\log\log\ell})$ → polynomial (facile).
- ▷ Calcul en $O(e^{k\log(\ell)^a(\log\log\ell)^{1-a}})$ → sous-exponentiel (compliqué).
- ▷ Calcul en $O(\ell) = O(e^{\log\ell})$ → exponentiel (très compliqué).

Exemples :

- ⇝ Calculer g^ℓ par l'exponentiation rapide → linéaire.
- ⇝ Décider si un entier ℓ est premier → polynomial.
- ⇝ Factoriser un entier ℓ → sous-exponentiel ($a = 1/3$).
- ⇝ Calculer g^ℓ en faisant $g \times g \cdots \times g$ → exponentiel.

- ▷ Et résoudre le pb. du log discret, i.e. trouver ℓ tel que $y = g^\ell$?
- ⇝ Dépend du groupe.

Facile ? Pas facile ?

Supposons que l'entrée d'un programme soit ℓ.

- ▷ Calcul en $O(\log(\ell)) = O(e^{\log\log\ell})$ → linéaire (très facile).
- ▷ Calcul en $O(\log(\ell)^k) = O(e^{k\log\log\ell})$ → polynomial (facile).
- ▷ Calcul en $O(e^{k\log(\ell)^a(\log\log\ell)^{1-a}})$ → sous-exponentiel (compliqué).
- ▷ Calcul en $O(\ell) = O(e^{\log\ell})$ → exponentiel (très compliqué).

Exemples :

- ⇝ Calculer g^ℓ par l'exponentiation rapide → linéaire.
- ⇝ Décider si un entier ℓ est premier → polynomial.
- ⇝ Factoriser un entier ℓ → sous-exponentiel ($a = 1/3$).
- ⇝ Calculer g^ℓ en faisant $g \times g \cdots \times g$ → exponentiel.

- ▷ Et résoudre le pb. du log discret, i.e. trouver ℓ tel que $y = g^\ell$?
- ⇝ Dépend du groupe.

Facile ? Pas facile ?

Supposons que l'entrée d'un programme soit ℓ.

- ▷ Calcul en $O(\log(\ell)) = O(e^{\log\log\ell})$ → linéaire (très facile).
- ▷ Calcul en $O(\log(\ell)^k) = O(e^{k\log\log\ell})$ → polynomial (facile).
- ▷ Calcul en $O(e^{k\log(\ell)^a(\log\log\ell)^{1-a}})$ → sous-exponentiel (compliqué).
- ▷ Calcul en $O(\ell) = O(e^{\log\ell})$ → exponentiel (très compliqué).

Exemples :

- ⇝ Calculer g^ℓ par l'exponentiation rapide → linéaire.
- ⇝ Décider si un entier ℓ est premier → polynomial.
- ⇝ Factoriser un entier ℓ → sous-exponentiel ($a = 1/3$).
- ⇝ Calculer g^ℓ en faisant $g \times g \cdots \times g$ → exponentiel.

▷ Et résoudre le pb. du log discret, i.e. trouver ℓ tel que $y = g^\ell$?

⇝ Dépend du groupe.

Facile ? Pas facile ?

Supposons que l'entrée d'un programme soit ℓ.

▷ Calcul en $O(\log(\ell)) = O(e^{\log\log\ell})$ → linéaire (très facile).

▷ Calcul en $O(\log(\ell)^k) = O(e^{k\log\log\ell})$ → polynomial (facile).

▷ Calcul en $O(e^{k\log(\ell)^a(\log\log\ell)^{1-a}})$ → sous-exponentiel (compliqué).

▷ Calcul en $O(\ell) = O(e^{\log\ell})$ → exponentiel (très compliqué).

Exemples :

⇝ Calculer g^ℓ par l'exponentiation rapide → linéaire.

⇝ Décider si un entier ℓ est premier → polynomial.

⇝ Factoriser un entier ℓ → sous-exponentiel ($a = 1/3$).

⇝ Calculer g^ℓ en faisant $g \times g \cdots \times g$ → exponentiel.

▷ Et résoudre le pb. du log discret, i.e. trouver ℓ tel que $y = g^\ell$?

⇝ Dépend du groupe.

Facile ? Pas facile ?

Supposons que l'entrée d'un programme soit ℓ.

- ▷ Calcul en $O(\log(\ell)) = O(e^{\log\log\ell})$ → linéaire (très facile).
- ▷ Calcul en $O(\log(\ell)^k) = O(e^{k\log\log\ell})$ → polynomial (facile).
- ▷ Calcul en $O(e^{k\log(\ell)^a(\log\log\ell)^{1-a}})$ → sous-exponentiel (compliqué).
- ▷ Calcul en $O(\ell) = O(e^{\log\ell})$ → exponentiel (très compliqué).

Exemples :

- ⇝ Calculer g^ℓ par l'exponentiation rapide → linéaire.
- ⇝ Décider si un entier ℓ est premier → polynomial.
- ⇝ Factoriser un entier ℓ → sous-exponentiel ($a = 1/3$).
- ⇝ Calculer g^ℓ en faisant $g \times g \cdots \times g$ → exponentiel.

- ▷ Et résoudre le pb. du log discret, i.e. trouver ℓ tel que $y = g^\ell$?
- ⇝ Dépend du groupe.

Facile ? Pas facile ?

Supposons que l'entrée d'un programme soit ℓ.

▷ Calcul en $O(\log(\ell)) = O(e^{\log\log\ell})$ → linéaire (très facile).

▷ Calcul en $O(\log(\ell)^k) = O(e^{k\log\log\ell})$ → polynomial (facile).

▷ Calcul en $O(e^{k\log(\ell)^a(\log\log\ell)^{1-a}})$ → sous-exponentiel (compliqué).

▷ Calcul en $O(\ell) = O(e^{\log\ell})$ → exponentiel (très compliqué).

Exemples :

⇝ Calculer g^ℓ par l'exponentiation rapide → linéaire.

⇝ Décider si un entier ℓ est premier → polynomial.

⇝ Factoriser un entier ℓ → sous-exponentiel ($a = 1/3$).

⇝ Calculer g^ℓ en faisant $g \times g \cdots \times g$ → exponentiel.

▷ Et résoudre le pb. du log discret, i.e. trouver ℓ tel que $y = g^\ell$?

⇝ Dépend du groupe.

Résoudre le problème du log discret : $y = g^\ell$

▷ Réduction de Pohlig-Hellman :

$\rightsquigarrow$ Si G est d'ordre $n = pq$ avec p et q premiers entre eux.

On écrit $pu + qv = 1$. On résout

$$y^{pu} = \left(g^p\right)^{\ell_1} \quad \leftarrow \text{Pb dans un groupe d'ordre } q.$$
$$y^{qv} = \left(g^q\right)^{\ell_2} \quad \leftarrow \text{Pb dans un groupe d'ordre } p.$$

On a $y = y^{pu+qv} = g^{p\ell_1 + q\ell_2}$!

$\rightsquigarrow$ Si G est d'ordre p^m avec p premier.

Il existe une astuce similaire qui permet de résoudre le pb du log discret dans G en résolvant m pbs du log discret dans un groupe d'ordre p.

Fait

Il faut absolument prendre des groupes d'ordre premier.

Résoudre le problème du log discret : $y = g^\ell$

▷ Réduction de Pohlig-Hellman :

$\rightsquigarrow$ Si G est d'ordre $n = pq$ avec p et q premiers entre eux.

On écrit $pu + qv = 1$. On résout

$$y^{pu} \qquad \left(g^p\right)^{\ell_1} \qquad \leftarrow \text{Pb dans un groupe d'ordre } q.$$

$$y^{qv} \qquad \left(g^q\right)^{\ell_2} \qquad \leftarrow \text{Pb dans un groupe d'ordre } p.$$

On a $y = y^{pu+qv} = g^{p\ell_1 + q\ell_2}$!

$\rightsquigarrow$ Si G est d'ordre p^m avec p premier.

Il existe une astuce similaire qui permet de résoudre le pb du log discret dans G en résolvant m pbs du log discret dans un groupe d'ordre p.

Fail

Il faut absolument prendre des groupes d'ordre premier.

Résoudre le problème du log discret : $y = g^\ell$

▷ Réduction de Pohlig-Hellman :

⇝ Si G est d'ordre $n = pq$ avec p et q premiers entre eux.

On écrit $pu + qv = 1$. On résout

$$y^{pu} = (g^p)^{\ell_1} \quad \leftarrow \text{Pb dans un groupe d'ordre } q.$$

$$y^{qv} = (g^q)^{\ell_2} \quad \leftarrow \text{Pb dans un groupe d'ordre } p.$$

On a $y = y^{pu+qv} = g^{p\ell_1 + q\ell_2}$!

⇝ Si G est d'ordre p^m avec p premier.

Il existe une astuce similaire qui permet de résoudre le pb du log discret dans G en résolvant m pbs du log discret dans un groupe d'ordre p.

Fail

Il faut absolument prendre des groupes d'ordre premier.

Résoudre le problème du log discret : $y = g^\ell$

▷ Réduction de Pohlig-Hellman :

$\rightsquigarrow$ Si G est d'ordre $n = pq$ avec p et q premiers entre eux.

On écrit $pu + qv = 1$. On résout

$$y^{pu} = (g^p)^{\ell_1} \quad \leftarrow \text{Pb dans un groupe d'ordre } q.$$

$$y^{qv} = (g^q)^{\ell_2} \quad \leftarrow \text{Pb dans un groupe d'ordre } p.$$

On a $y = y^{pu+qv} = g^{p\ell_1+q\ell_2}$!

$\rightsquigarrow$ Si G est d'ordre p^m avec p premier.

Il existe une astuce similaire qui permet de résoudre le pb du log discret dans G en résolvant m pbs du log discret dans un groupe d'ordre p.

Fail

Il faut absolument prendre des groupes d'ordre premier.

Résoudre le problème du log discret : $y = g^\ell$

▷ Réduction de Pohlig-Hellman :

$\rightsquigarrow$ Si G est d'ordre $n = pq$ avec p et q premiers entre eux.

On écrit $pu + qv = 1$. On résout

$$\begin{aligned} y^{pu} &= (g^p)^{\ell_1} && \leftarrow \text{Pb dans un groupe d'ordre } q. \\ y^{qv} &= (g^q)^{\ell_2} && \leftarrow \text{Pb dans un groupe d'ordre } p. \end{aligned}$$

On a $y = y^{pu+qv} = g^{p\ell_1+q\ell_2}$!

$\rightsquigarrow$ Si G est d'ordre p^m avec p premier.

Il existe une astuce similaire qui permet de résoudre le pb du log discret dans G en résolvant m pbs du log discret dans un groupe d'ordre p.

Fail

Il faut absolument prendre des groupes d'ordre premier.

Résoudre le problème du log discret : $y = g^\ell$

▷ Réduction de Pohlig-Hellman :

$\rightsquigarrow$ Si G est d'ordre $n = pq$ avec p et q premiers entre eux.

On écrit $pu + qv = 1$. On résout

$$\begin{aligned} y^{pu} &= (g^p)^{\ell_1} && \leftarrow \text{Pb dans un groupe d'ordre } q. \\ y^{qv} &= (g^q)^{\ell_2} && \leftarrow \text{Pb dans un groupe d'ordre } p. \end{aligned}$$

On a $y = y^{pu+qv} = g^{p\ell_1+q\ell_2}$!

$\rightsquigarrow$ Si G est d'ordre p^m avec p premier.

Il existe une astuce similaire qui permet de résoudre le pb du log discret dans G en résolvant m pbs du log discret dans un groupe d'ordre p.

Fail

Il faut absolument prendre des groupes d'ordre premier.

Résoudre le problème du log discret : $y = g^\ell$

▷ Réduction de Pohlig-Hellman :

$\rightsquigarrow$ Si G est d'ordre $n = pq$ avec p et q premiers entre eux.

On écrit $pu + qv = 1$. On résout

$$\begin{aligned} y^{pu} &= (g^p)^{\ell_1} && \leftarrow \text{Pb dans un groupe d'ordre } q. \\ y^{qv} &= (g^q)^{\ell_2} && \leftarrow \text{Pb dans un groupe d'ordre } p. \end{aligned}$$

On a $y = y^{pu+qv} = g^{p\ell_1+q\ell_2}$!

$\rightsquigarrow$ Si G est d'ordre p^m avec p premier.

Il existe une astuce similaire qui permet de résoudre le pb du log discret dans G en résolvant m pbs du log discret dans un groupe d'ordre p.

Fail

Il faut absolument prendre des groupes d'ordre premier.

Résoudre le problème du log discret : $y = g^\ell$

▷ Réduction de Pohlig-Hellman :

$\rightsquigarrow$ Si G est d'ordre $n = pq$ avec p et q premiers entre eux.

On écrit $pu + qv = 1$. On résout

$$\begin{aligned} y^{pu} &= (g^p)^{\ell_1} && \leftarrow \text{Pb dans un groupe d'ordre } q. \\ y^{qv} &= (g^q)^{\ell_2} && \leftarrow \text{Pb dans un groupe d'ordre } p. \end{aligned}$$

On a $y = y^{pu+qv} = g^{p\ell_1+q\ell_2}$!

$\rightsquigarrow$ Si G est d'ordre p^m avec p premier.

Il existe une astuce similaire qui permet de résoudre le pb du log discret dans G en résolvant m pbs du log discret dans un groupe d'ordre p.

Fait

Il faut absolument prendre des groupes d'ordre premier.

Résoudre le problème du log discret : $y = g^\ell$

▷ Réduction de Pohlig-Hellman :

$\rightsquigarrow$ Si G est d'ordre $n = pq$ avec p et q premiers entre eux.

On écrit $pu + qv = 1$. On résout

$$\begin{aligned} y^{pu} &= (g^p)^{\ell_1} && \leftarrow \text{Pb dans un groupe d'ordre } q. \\ y^{qv} &= (g^q)^{\ell_2} && \leftarrow \text{Pb dans un groupe d'ordre } p. \end{aligned}$$

On a $y = y^{pu+qv} = g^{p\ell_1+q\ell_2}$!

$\rightsquigarrow$ Si G est d'ordre p^m avec p premier.

Il existe une astuce similaire qui permet de résoudre le pb du log discret dans G en résolvant m pbs du log discret dans un groupe d'ordre p.

Fait

Il faut absolument prendre des groupes d'ordre premier.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

$\rightsquigarrow$ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

⇝ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

⇝ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

$\rightsquigarrow$ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

⇝ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé
$(g^m)^0$	yg^{-0}
$(g^m)^1$	yg^{-1}
⋮	⋮
$(g^m)^k$	⋮
⋮	yg^{-r}
$(g^m)^{m-1}$	

▷ On calcule les pas de géant. ← m étapes.

▷ On calcule les pas de bébé jusqu'à une collision. ← $\leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

$\rightsquigarrow$ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé

▷ On calcule les pas de géant.

▷ On calcule les pas de bébé jusqu'à une collision.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

$\rightsquigarrow$ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé
$(g^m)^0$	yg^{-0}
$(g^m)^1$	yg^{-1}
$\vdots$	$\vdots$
$(g^m)^k$	$\vdots$
$\vdots$	yg^{-r}
$(g^m)^{m-1}$	

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

$\rightsquigarrow$ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé
$(g^m)^0$	yg^{-0}
$(g^m)^1$	yg^{-1}
$\vdots$	$\vdots$
$(g^m)^k$	$\vdots$
$\vdots$	yg^{-r}
$(g^m)^{m-1}$	

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

$\rightsquigarrow$ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé
$(g^m)^0$	yg^{-0}
$(g^m)^1$	yg^{-1}
$\vdots$	$\vdots$
$(g^m)^k$	$\vdots$
$\vdots$	yg^{-r}
$(g^m)^{m-1}$	

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

$\rightsquigarrow$ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé
$(g^m)^0$	yg^{-0}
$(g^m)^1$	yg^{-1}
$\vdots$	$\vdots$
$(g^m)^k$	yg^{-r}
$\vdots$	
$(g^m)^{m-1}$	

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

$\rightsquigarrow$ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé
$(g^m)^0$	yg^{-0}
$(g^m)^1$	yg^{-1}
$\vdots$	$\vdots$
$(g^m)^k$	yg^{-r}
$\vdots$	
$(g^m)^{m-1}$	

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

$\rightsquigarrow$ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé
$(g^m)^0$	yg^{-0}
$(g^m)^1$	yg^{-1}
$\vdots$	$\vdots$
$(g^m)^k$	yg^{-r}
$\vdots$	
$(g^m)^{m-1}$	

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

$\rightsquigarrow$ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé
$(g^m)^0$	yg^{-0}
$(g^m)^1$	yg^{-1}
$\vdots$	$\vdots$
$(g^m)^k$	yg^{-r}
$\vdots$	
$(g^m)^{m-1}$	

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

⇝ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé
$(g^m)^0$	yg^{-0}
$(g^m)^1$	yg^{-1}
$\vdots$	$\vdots$
$(g^m)^k$	$\vdots$
$\vdots$	yg^{-r}
$(g^m)^{m-1}$	

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

$\rightsquigarrow$ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé
$(g^m)^0$	yg^{-0}
$(g^m)^1$	yg^{-1}
$\vdots$	$\vdots$
$(g^m)^k$	$\vdots$
$\vdots$	yg^{-r}
$(g^m)^{m-1}$	

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

⇝ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé
$(g^m)^0$	yg^{-0}
$(g^m)^1$	yg^{-1}
$\vdots$	$\vdots$
$(g^m)^k$	$\vdots$
$\vdots$	yg^{-r}
$(g^m)^{m-1}$	

▷ On calcule les pas de géant. ← m étapes.

▷ On calcule les pas de bébé jusqu'à une collision. ← $\leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

▷ Algorithme Baby-Steps / Giant Steps :

$\rightsquigarrow$ Si G est d'ordre n. On pose $m = \lceil \sqrt{n} \rceil$. Dans $y = g^\ell$, on écrit $\ell = km + r$ avec $0 \leq k, r < m$. On a $yg^{-r} = (g^m)^k$.

Pas de géant	Pas de bébé
$(g^m)^0$	yg^{-0}
$(g^m)^1$	yg^{-1}
$\vdots$	$\vdots$
$(g^m)^k$	$\vdots$
$\vdots$	yg^{-r}
$(g^m)^{m-1}$	

▷ On calcule les pas de géant. $\leftarrow m$ étapes.

▷ On calcule les pas de bébé jusqu'à une collision. $\leftarrow \leq m$ étapes.

On a alors $yg^{-r} = (g^m)^k$ donc $y = g^{km+r}$.

Résoudre le problème du log discret

$\rightsquigarrow$ La méthode Baby-Steps / Giant Steps permet de résoudre le log discret en $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Il existe d'autres méthodes simples (utilisant moins d'espace mémoire).

$\rightsquigarrow$ Cela reste exponentiel : $\sqrt{n} = e^{\frac{1}{2}\log n}$.

Théorème de Shoup (1997)

Dans un groupe générique, la résolution du problème du log discret nécessite $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Dans un groupe générique, le pb du log discret est difficile.

$\rightsquigarrow$ Dans les applications, il n'existe pas de groupe générique.

Résoudre le problème du log discret

$\rightsquigarrow$ La méthode Baby-Steps / Giant Steps permet de résoudre le log discret en $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Il existe d'autres méthodes simples (utilisant moins d'espace mémoire).

$\rightsquigarrow$ Cela reste exponentiel : $\sqrt{n} = e^{\frac{1}{2}\log n}$.

Théorème de Shoup (1997)

Dans un groupe générique, la résolution du problème du log discret nécessite $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Dans un groupe générique, le pb du log discret est difficile.

$\rightsquigarrow$ Dans les applications, il n'existe pas de groupe générique.

Résoudre le problème du log discret

$\rightsquigarrow$ La méthode Baby-Steps / Giant Steps permet de résoudre le log discret en $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Il existe d'autres méthodes simples (utilisant moins d'espace mémoire).

$\rightsquigarrow$ Cela reste exponentiel : $\sqrt{n} = e^{\frac{1}{2}\log n}$.

Théorème de Shoup (1997)

Dans un groupe générique, la résolution du problème du log discret nécessite $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Dans un groupe générique, le pb du log discret est difficile.

$\rightsquigarrow$ Dans les applications, il n'existe pas de groupe générique.

Résoudre le problème du log discret

$\rightsquigarrow$ La méthode Baby-Steps / Giant Steps permet de résoudre le log discret en $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Il existe d'autres méthodes simples (utilisant moins d'espace mémoire).

$\rightsquigarrow$ Cela reste exponentiel : $\sqrt{n} = e^{\frac{1}{2}\log n}$.

Théorème de Shoup (1997)

Dans un groupe générique, la résolution du problème du log discret nécessite $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Dans un groupe générique, le pb du log discret est difficile.

$\rightsquigarrow$ Dans les applications, il n'existe pas de groupe générique.

Résoudre le problème du log discret

$\rightsquigarrow$ La méthode Baby-Steps / Giant Steps permet de résoudre le log discret en $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Il existe d'autres méthodes simples (utilisant moins d'espace mémoire).

$\rightsquigarrow$ Cela reste exponentiel : $\sqrt{n} = e^{\frac{1}{2}\log n}$.

Théorème de Shoup (1997)

Dans un groupe générique, la résolution du problème du log discret nécessite $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Dans un groupe générique, le pb du log discret est difficile.

$\rightsquigarrow$ Dans les applications, il n'existe pas de groupe générique.

Résoudre le problème du log discret

$\rightsquigarrow$ La méthode Baby-Steps / Giant Steps permet de résoudre le log discret en $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Il existe d'autres méthodes simples (utilisant moins d'espace mémoire).

$\rightsquigarrow$ Cela reste exponentiel : $\sqrt{n} = e^{\frac{1}{2}\log n}$.

Théorème de Shoup (1997)

Dans un groupe générique, la résolution du problème du log discret nécessite $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Dans un groupe générique, le pb du log discret est difficile.

$\rightsquigarrow$ Dans les applications, il n'existe pas de groupe générique.

Résoudre le problème du log discret

$\rightsquigarrow$ La méthode Baby-Steps / Giant Steps permet de résoudre le log discret en $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Il existe d'autres méthodes simples (utilisant moins d'espace mémoire).

$\rightsquigarrow$ Cela reste exponentiel : $\sqrt{n} = e^{\frac{1}{2}\log n}$.

Théorème de Shoup (1997)

Dans un groupe générique, la résolution du problème du log discret nécessite $O(n^{1/2+\varepsilon})$ multiplications.

$\rightsquigarrow$ Dans un groupe générique, le pb du log discret est difficile.

$\rightsquigarrow$ Dans les applications, il n'existe pas de groupe générique.

Quels groupes ?

▷ $G = (\mathbb{Z}/n\mathbb{Z}, +)$ et $g = 1$. → Résoudre $y = \ell \cdot 1$: trivial !

▷ $G = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ et g un générateur (qui existe).

⇝ Il faut que l'ordre du groupe $p - 1$ soit presque premier.

⇝ Il faut trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

⇝ C'est le groupe le plus utilisé. Il faut des grands nombres p car il existe une attaque sous-exponentielle.

Index calculus

On peut résoudre le pb du log discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$ en effectuant $O(e^{k \log(p)^{1/3} (\log \log p)^{2/3}})$ multiplications

⇝ Basé sur la factorisation dans $\mathbb{Z}$.

⇝ Assez technique à mettre bien en oeuvre.

▷ $G = E(\mathbb{Z}/p\mathbb{Z})$ où E est une courbe elliptique.

→ Résoudre $y = ng$. À part pour certaines courbes faibles, on ne connaît pas de méthode sous-exponentielle.

Quels groupes ?

▷ $G = (\mathbb{Z}/n\mathbb{Z}, +)$ et $g = 1$.

$\rightarrow$ Résoudre $y = \ell \cdot 1$: trivial !

▷ $G = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ et g un générateur (qui existe).

$\rightsquigarrow$ Il faut que l'ordre du groupe $p - 1$ soit presque premier.

$\rightsquigarrow$ Il faut trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

$\rightsquigarrow$ C'est le groupe le plus utilisé. Il faut des grands nombres p car il existe une attaque sous-exponentielle.

Index calculus

On peut résoudre le pb du log discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$ en effectuant $O(e^{k \log(p)^{1/3} (\log \log p)^{2/3}})$ multiplications

$\rightsquigarrow$ Basé sur la factorisation dans $\mathbb{Z}$.

$\rightsquigarrow$ Assez technique à mettre bien en oeuvre.

▷ $G = E(\mathbb{Z}/p\mathbb{Z})$ où E est une courbe elliptique.

$\rightarrow$ Résoudre $y = ng$. À part pour certaines courbes faibles, on ne connaît pas de méthode sous-exponentielle.

Quels groupes ?

▷ $G = (\mathbb{Z}/n\mathbb{Z}, +)$ et $g = 1$. → Résoudre $y = \ell \cdot 1$: trivial !

▷ $G = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ et g un générateur (qui existe).

⇝ Il faut que l'ordre du groupe $p - 1$ soit presque premier.

⇝ Il faut trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

⇝ C'est le groupe le plus utilisé. Il faut des grands nombres p car il existe une attaque sous-exponentielle.

Index calculus

On peut résoudre le pb du log discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$ en effectuant $O(e^{k \log(p)^{1/3} (\log \log p)^{2/3}})$ multiplications

⇝ Basé sur la factorisation dans $\mathbb{Z}$.

⇝ Assez technique à mettre bien en oeuvre.

▷ $G = E(\mathbb{Z}/p\mathbb{Z})$ où E est une courbe elliptique.

→ Résoudre $y = ng$. À part pour certaines courbes faibles, on ne connaît pas de méthode sous-exponentielle.

Quels groupes ?

▷ $G = (\mathbb{Z}/n\mathbb{Z}, +)$ et $g = 1$. → Résoudre $y = \ell \cdot 1$: trivial !

▷ $G = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ et g un générateur (qui existe).

⇝ Il faut que l'ordre du groupe $p - 1$ soit presque premier.

⇝ Il faut trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

⇝ C'est le groupe le plus utilisé. Il faut des grands nombres p car il existe une attaque sous-exponentielle.

Index calculus

On peut résoudre le pb du log discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$ en effectuant $O(e^{k \log(p)^{1/3} (\log \log p)^{2/3}})$ multiplications

⇝ Basé sur la factorisation dans $\mathbb{Z}$.

⇝ Assez technique à mettre bien en oeuvre.

▷ $G = E(\mathbb{Z}/p\mathbb{Z})$ où E est une courbe elliptique.

→ Résoudre $y = ng$. À part pour certaines courbes faibles, on ne connaît pas de méthode sous-exponentielle.

Quels groupes ?

▷ $G = (\mathbb{Z}/n\mathbb{Z}, +)$ et $g = 1$. → Résoudre $y = \ell \cdot 1$: trivial !

▷ $G = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ et g un générateur (qui existe).

⇝ Il faut que l'ordre du groupe $p - 1$ soit presque premier.

⇝ Il faut trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

⇝ C'est le groupe le plus utilisé. Il faut des grands nombres p car il existe une attaque sous-exponentielle.

Index calculus

On peut résoudre le pb du log discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$ en effectuant $O(e^{k \log(p)^{1/3} (\log \log p)^{2/3}})$ multiplications

⇝ Basé sur la factorisation dans $\mathbb{Z}$.

⇝ Assez technique à mettre bien en oeuvre.

▷ $G = E(\mathbb{Z}/p\mathbb{Z})$ où E est une courbe elliptique.

→ Résoudre $y = ng$. À part pour certaines courbes faibles, on ne connaît pas de méthode sous-exponentielle.

Quels groupes ?

▷ $G = (\mathbb{Z}/n\mathbb{Z}, +)$ et $g = 1$. → Résoudre $y = \ell \cdot 1$: trivial !

▷ $G = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ et g un générateur (qui existe).

⇝ Il faut que l'ordre du groupe $p - 1$ soit presque premier.

⇝ Il faut trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

⇝ C'est le groupe le plus utilisé. Il faut des grands nombres p car il existe une attaque sous-exponentielle.

Index calculus

On peut résoudre le pb du log discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$ en effectuant $O(e^{k \log(p)^{1/3} (\log \log p)^{2/3}})$ multiplications

⇝ Basé sur la factorisation dans $\mathbb{Z}$.

⇝ Assez technique à mettre bien en oeuvre.

▷ $G = E(\mathbb{Z}/p\mathbb{Z})$ où E est une courbe elliptique.

→ Résoudre $y = ng$. À part pour certaines courbes faibles, on ne connaît pas de méthode sous-exponentielle.

Quels groupes ?

▷ $G = (\mathbb{Z}/n\mathbb{Z}, +)$ et $g = 1$. → Résoudre $y = \ell \cdot 1$: trivial !

▷ $G = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ et g un générateur (qui existe).

⇝ Il faut que l'ordre du groupe $p - 1$ soit presque premier.

⇝ Il faut trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

⇝ C'est le groupe le plus utilisé. Il faut des grands nombres p car il existe une attaque sous-exponentielle.

Index calculus

On peut résoudre le pb du log discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$ en effectuant $O(e^{k \log(p)^{1/3} (\log \log p)^{2/3}})$ multiplications

⇝ Basé sur la factorisation dans $\mathbb{Z}$.

⇝ Assez technique à mettre bien en oeuvre.

▷ $G = E(\mathbb{Z}/p\mathbb{Z})$ où E est une courbe elliptique.

→ Résoudre $y = ng$. À part pour certaines courbes faibles, on ne connaît pas de méthode sous-exponentielle.

Quels groupes ?

▷ $G = (\mathbb{Z}/n\mathbb{Z}, +)$ et $g = 1$. → Résoudre $y = \ell \cdot 1$: trivial !

▷ $G = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ et g un générateur (qui existe).

⇝ Il faut que l'ordre du groupe $p - 1$ soit presque premier.

⇝ Il faut trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

⇝ C'est le groupe le plus utilisé. Il faut des grands nombres p car il existe une attaque sous-exponentielle.

Index calculus

On peut résoudre le pb du log discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$ en effectuant $O(e^{k \log(p)^{1/3} (\log\log p)^{2/3}})$ multiplications

⇝ Basé sur la factorisation dans $\mathbb{Z}$.

⇝ Assez technique à mettre bien en oeuvre.

▷ $G = E(\mathbb{Z}/p\mathbb{Z})$ où E est une courbe elliptique.

→ Résoudre $y = ng$. À part pour certaines courbes faibles, on ne connaît pas de méthode sous-exponentielle.

Quels groupes ?

▷ $G = (\mathbb{Z}/n\mathbb{Z}, +)$ et $g = 1$. → Résoudre $y = \ell \cdot 1$: trivial !

▷ $G = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ et g un générateur (qui existe).

⇝ Il faut que l'ordre du groupe $p - 1$ soit presque premier.

⇝ Il faut trouver un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

⇝ C'est le groupe le plus utilisé. Il faut des grands nombres p car il existe une attaque sous-exponentielle.

Index calculus

On peut résoudre le pb du log discret dans $(\mathbb{Z}/p\mathbb{Z})^\times$ en effectuant $O(e^{k \log(p)^{1/3} (\log\log p)^{2/3}})$ multiplications

⇝ Basé sur la factorisation dans $\mathbb{Z}$.

⇝ Assez technique à mettre bien en oeuvre.

▷ $G = E(\mathbb{Z}/p\mathbb{Z})$ où E est une courbe elliptique.

→ Résoudre $y = ng$. À part pour certaines courbes faibles, on ne connaît pas de méthode sous-exponentielle.

Courbes elliptiques

Soit k un corps de caractéristique $\neq 2, 3$ (ici $k = \mathbb{Z}/p\mathbb{Z}$ avec p un grand nombre premier ou $k = \mathbb{R}$).

Une courbe elliptique E sur k est une courbe lisse définie par :

$$y^2 = x^3 + ax + b, \quad \text{où} \quad a, b \in k.$$

$\rightsquigarrow$ Lisse : $4a^3 + 27b^2 \neq 0$.

$\rightsquigarrow$ Les points de E :

$$E(k) = \{(x, y) \in k^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

Le point $\mathcal{O}$ s'appelle le point à l'infini.

$\rightsquigarrow$ Fait central : On munit $E(k)$ d'une loi de groupe abélien de nature géométrique :

Si $P, Q \in E(k)$, la droite passant par P et Q recoupe E en un troisième point (x_1, y_1). Par définition : $P + Q = (x_1, -y_1)$.

▷ Le point à l'infini, $\mathcal{O}$, est le neutre de cette addition.

▷ L'opposé de $P = (x_P, y_P)$ est $-P = (x_P, -y_P)$.

Courbes elliptiques

Soit k un corps de caractéristique $\neq 2, 3$ (ici $k = \mathbb{Z}/p\mathbb{Z}$ avec p un grand nombre premier ou $k = \mathbb{R}$).

Une courbe elliptique E sur k est une courbe lisse définie par :

$$y^2 = x^3 + ax + b, \quad \text{où} \quad a, b \in k.$$

$\rightsquigarrow$ Lisse : $4a^3 + 27b^2 \neq 0$.

$\rightsquigarrow$ Les points de E :

$$E(k) = \{(x, y) \in k^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

Le point $\mathcal{O}$ s'appelle le point à l'infini.

$\rightsquigarrow$ Fait central : On munit $E(k)$ d'une loi de groupe abélien de nature géométrique :

Si $P, Q \in E(k)$, la droite passant par P et Q recoupe E en un troisième point (x_1, y_1). Par définition : $P + Q = (x_1, -y_1)$.

▷ Le point à l'infini, $\mathcal{O}$, est le neutre de cette addition.

▷ L'opposé de $P = (x_P, y_P)$ est $-P = (x_P, -y_P)$.

Courbes elliptiques

Soit k un corps de caractéristique $\neq 2, 3$ (ici $k = \mathbb{Z}/p\mathbb{Z}$ avec p un grand nombre premier ou $k = \mathbb{R}$).

Une courbe elliptique E sur k est une courbe lisse définie par :

$$y^2 = x^3 + ax + b, \quad \text{où} \quad a, b \in k.$$

$\rightsquigarrow$ Lisse : $4a^3 + 27b^2 \neq 0$.

$\rightsquigarrow$ Les points de E :

$$E(k) = \{(x, y) \in k^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

Le point $\mathcal{O}$ s'appelle le point à l'infini.

$\rightsquigarrow$ Fait central : On munit $E(k)$ d'une loi de groupe abélien de nature géométrique :

Si $P, Q \in E(k)$, la droite passant par P et Q recoupe E en un troisième point (x_1, y_1). Par définition : $P + Q = (x_1, -y_1)$.

▷ Le point à l'infini, $\mathcal{O}$, est le neutre de cette addition.

▷ L'opposé de $P = (x_P, y_P)$ est $-P = (x_P, -y_P)$.

Courbes elliptiques

Soit k un corps de caractéristique $\neq 2, 3$ (ici $k = \mathbb{Z}/p\mathbb{Z}$ avec p un grand nombre premier ou $k = \mathbb{R}$).

Une courbe elliptique E sur k est une courbe lisse définie par :

$$y^2 = x^3 + ax + b, \quad \text{où} \quad a, b \in k.$$

$\rightsquigarrow$ Lisse : $4a^3 + 27b^2 \neq 0$.

$\rightsquigarrow$ Les points de E :

$$E(k) = \left\{(x, y) \in k^2 : y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\}.$$

Le point $\mathcal{O}$ s'appelle le point à l'infini.

$\rightsquigarrow$ Fait central : On munit $E(k)$ d'une loi de groupe abélien de nature géométrique :

Si $P, Q \in E(k)$, la droite passant par P et Q recoupe E en un troisième point (x_1, y_1). Par définition : $P + Q = (x_1, -y_1)$.

▷ Le point à l'infini, $\mathcal{O}$, est le neutre de cette addition.

▷ L'opposé de $P = (x_P, y_P)$ est $-P = (x_P, -y_P)$.

Courbes elliptiques

Soit k un corps de caractéristique $\neq 2, 3$ (ici $k = \mathbb{Z}/p\mathbb{Z}$ avec p un grand nombre premier ou $k = \mathbb{R}$).

Une courbe elliptique E sur k est une courbe lisse définie par :

$$y^2 = x^3 + ax + b, \quad \text{où} \quad a, b \in k.$$

$\rightsquigarrow$ Lisse : $4a^3 + 27b^2 \neq 0$.

$\rightsquigarrow$ Les points de E :

$$E(k) = \left\{(x, y) \in k^2 : y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\}.$$

Le point $\mathcal{O}$ s'appelle le point à l'infini.

$\rightsquigarrow$ Fait central : On munit $E(k)$ d'une loi de groupe abélien de nature géométrique :

Si $P, Q \in E(k)$, la droite passant par P et Q recoupe E en un troisième point (x_1, y_1). Par définition : $P + Q = (x_1, -y_1)$.

▷ Le point à l'infini, $\mathcal{O}$, est le neutre de cette addition.

▷ L'opposé de $P = (x_P, y_P)$ est $-P = (x_P, -y_P)$.

Courbes elliptiques

Soit k un corps de caractéristique $\neq 2, 3$ (ici $k = \mathbb{Z}/p\mathbb{Z}$ avec p un grand nombre premier ou $k = \mathbb{R}$).

Une courbe elliptique E sur k est une courbe lisse définie par :

$$y^2 = x^3 + ax + b, \quad \text{où} \quad a, b \in k.$$

$\rightsquigarrow$ Lisse : $4a^3 + 27b^2 \neq 0$.

$\rightsquigarrow$ Les points de E :

$$E(k) = \{(x, y) \in k^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

Le point $\mathcal{O}$ s'appelle le point à l'infini.

$\rightsquigarrow$ Fait central : On munit $E(k)$ d'une loi de groupe abélien de nature géométrique :

Si $P, Q \in E(k)$, la droite passant par P et Q recoupe E en un troisième point (x_1, y_1). Par définition : $P + Q = (x_1, -y_1)$.

▷ Le point à l'infini, $\mathcal{O}$, est le neutre de cette addition.

▷ L'opposé de $P = (x_P, y_P)$ est $-P = (x_P, -y_P)$.

Courbes elliptiques

Soit k un corps de caractéristique $\neq 2, 3$ (ici $k = \mathbb{Z}/p\mathbb{Z}$ avec p un grand nombre premier ou $k = \mathbb{R}$).

Une courbe elliptique E sur k est une courbe lisse définie par :

$$y^2 = x^3 + ax + b, \quad \text{où} \quad a, b \in k.$$

$\rightsquigarrow$ Lisse : $4a^3 + 27b^2 \neq 0$.

$\rightsquigarrow$ Les points de E :

$$E(k) = \{(x, y) \in k^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

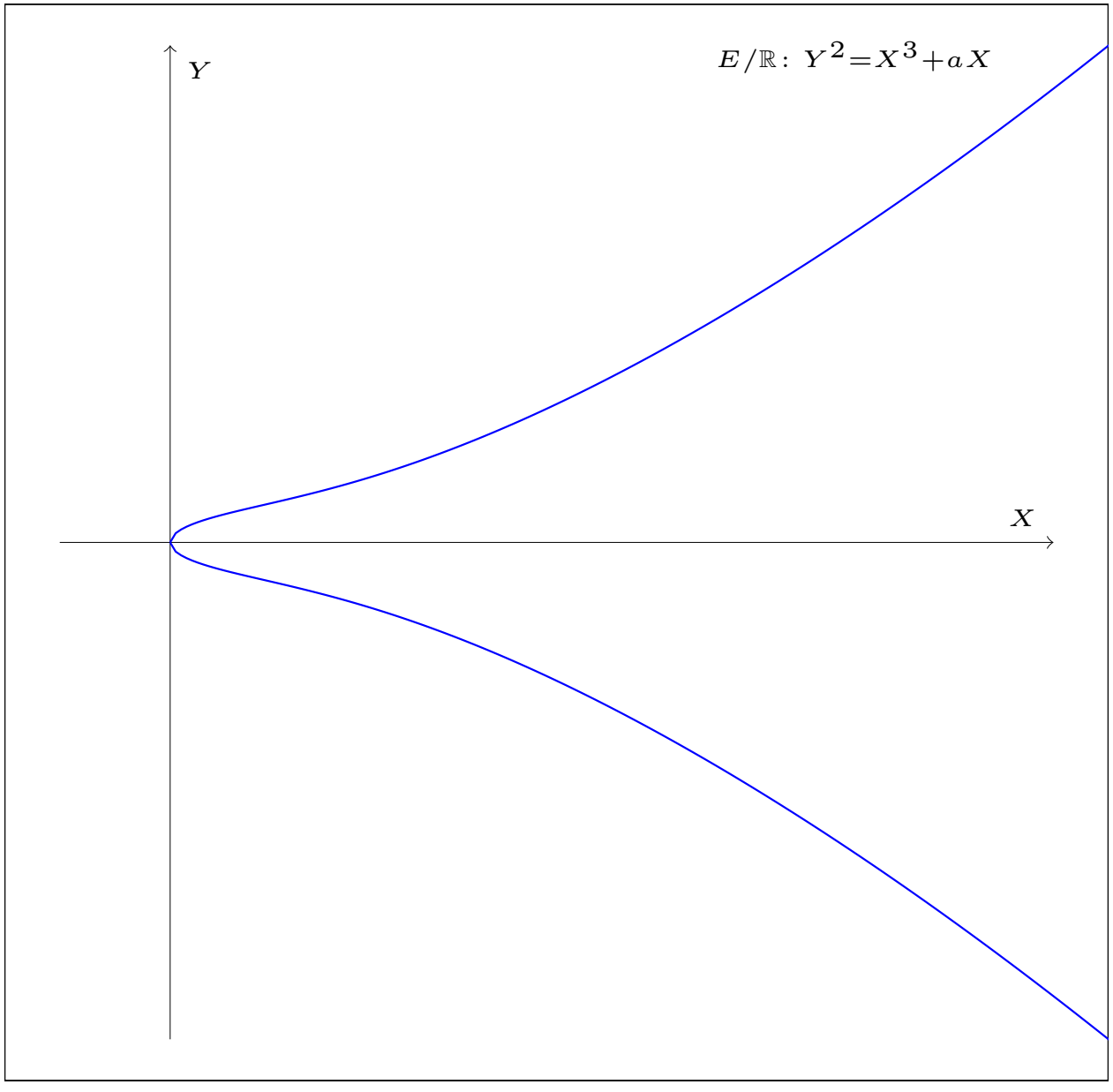
Le point $\mathcal{O}$ s'appelle le point à l'infini.

$\rightsquigarrow$ Fait central : On munit $E(k)$ d'une loi de groupe abélien de nature géométrique :

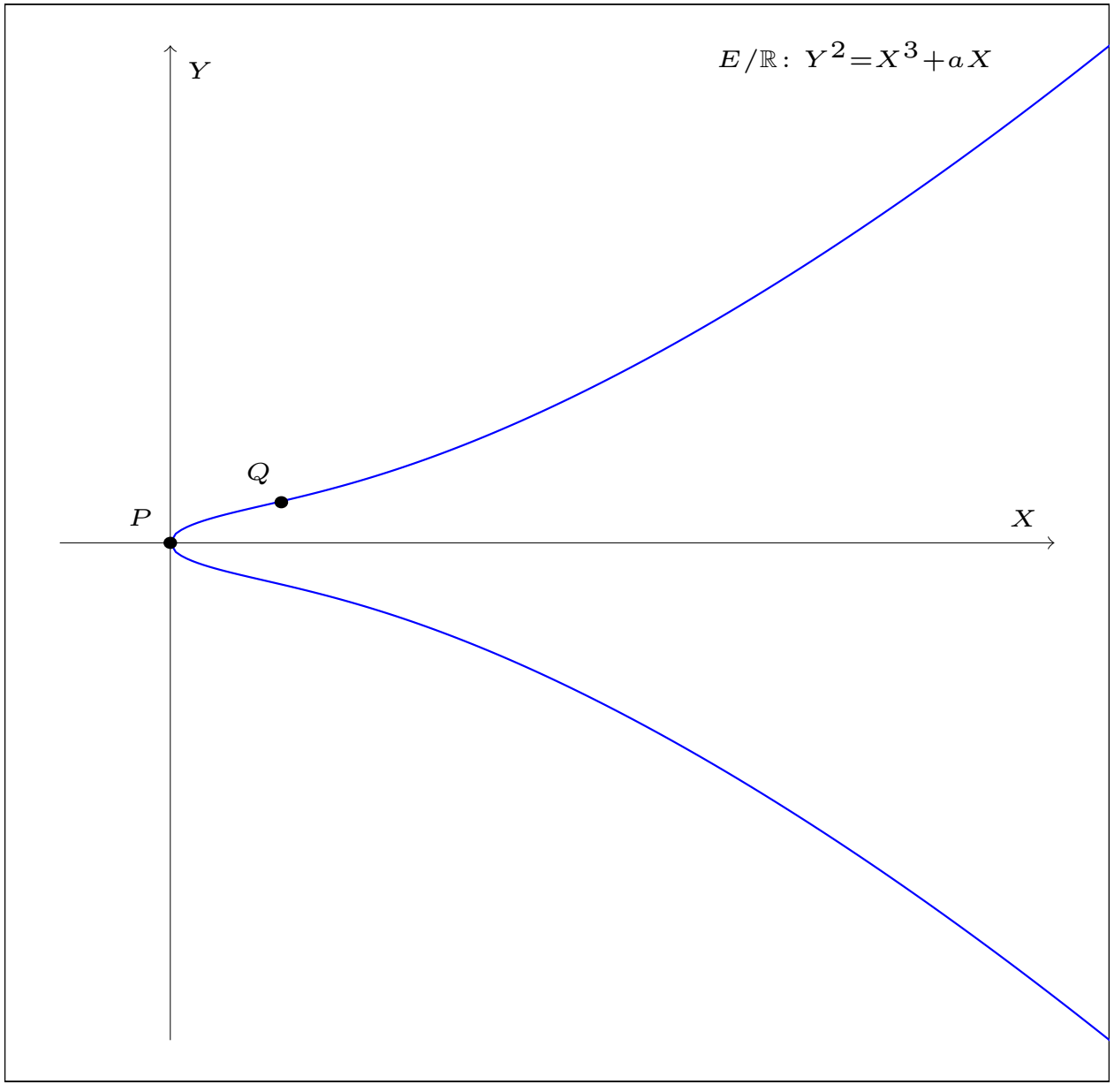
Si $P, Q \in E(k)$, la droite passant par P et Q recoupe E en un troisième point (x_1, y_1). Par définition : $P + Q = (x_1, -y_1)$.

$\triangleright$ Le point à l'infini, $\mathcal{O}$, est le neutre de cette addition.
$\triangleright$ L'opposé de $P = (x_P, y_P)$ est $-P = (x_P, -y_P)$.

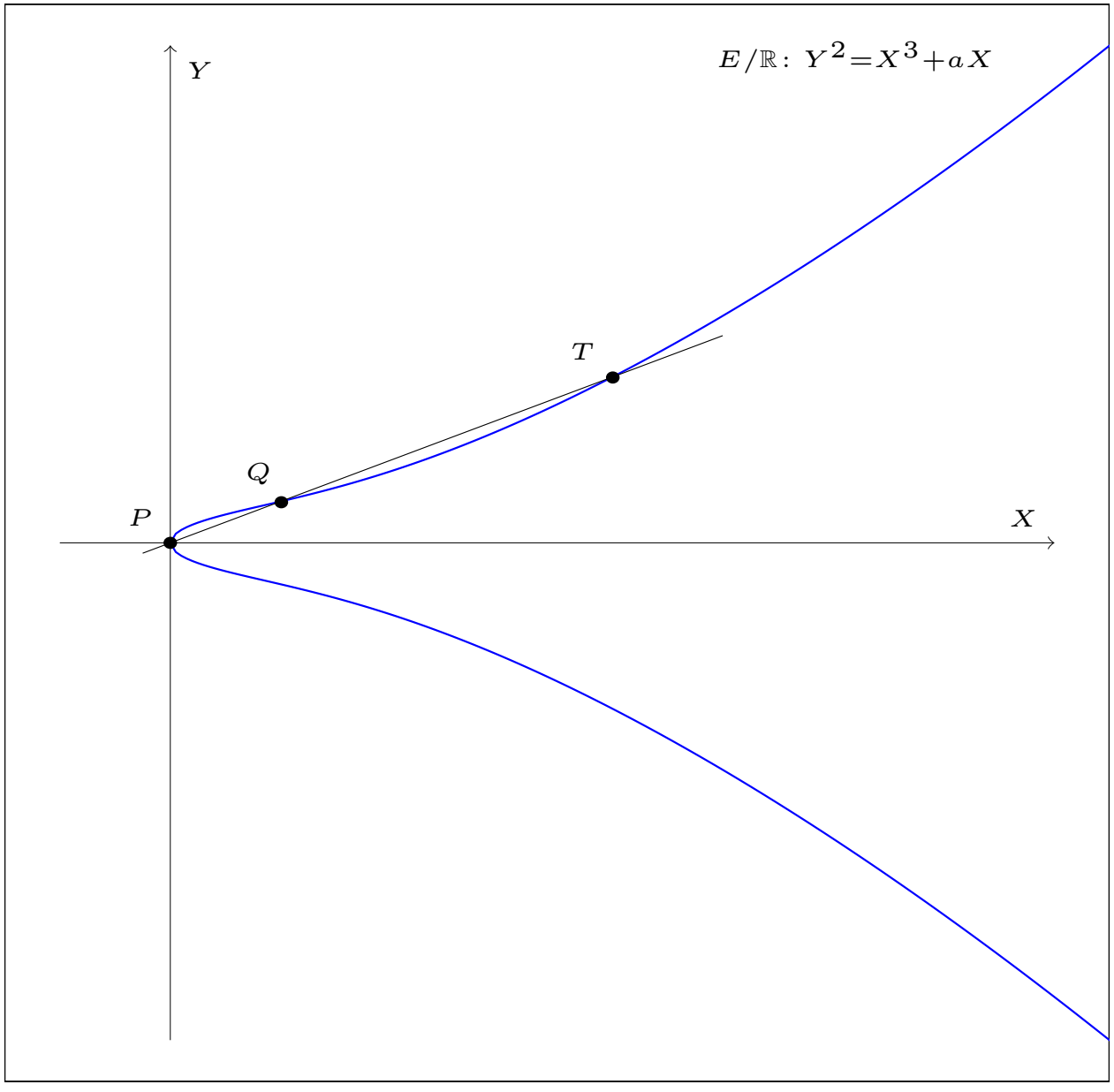
Courbes elliptiques : loi de groupe



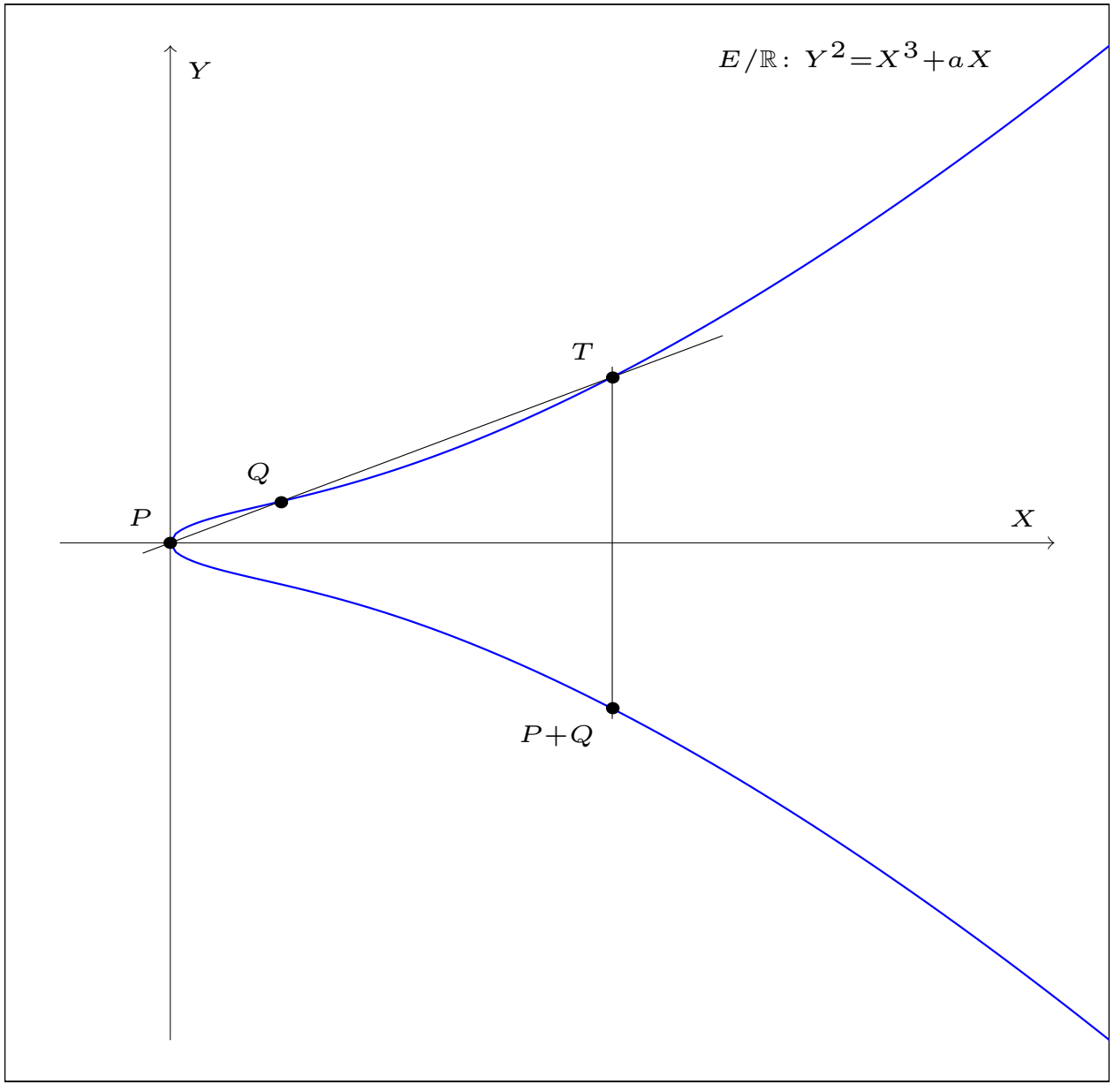
Courbes elliptiques : loi de groupe



Courbes elliptiques : loi de groupe



Courbes elliptiques : loi de groupe



Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_7$. Soit $E : y^2 = x^3 + x + 4$. On a

$$E(\mathbb{F}_7) =< (0,2) >= \{\mathcal{O}, (0,2), 2 \cdot (0,2), \cdots, 9 \cdot (0,2)\}$$

On a donc $(2,0) = \ell \cdot (0,2)$ pour un certain ℓ. Que vaut ℓ ?.

$\rightsquigarrow$ C'est le problème du logarithme discret dans $E(\mathbb{F}_7)$! (ici $\ell = 5$).

$\rightsquigarrow$ $E(\mathbb{F}_7)$ est cyclique (c'est fréquent).

Si E est définie sur $\mathbb{F}_p$ avec p grand, le problème du log discret semble compliqué : utile pour la cryptographie.

Il faut pouvoir le mettre en place :

$\rightsquigarrow$ Trouver E et p tels que $\sharp E(\mathbb{F}_p)$ est (presque) premier ;

$\rightsquigarrow$ Il faut savoir calculer $\sharp E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut savoir trouver un point $G \in E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut que E ne soit pas "faible"...

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_7$. Soit $E : y^2 = x^3 + x + 4$. On a

$$E(\mathbb{F}_7) =< (0,2) >= \{\mathcal{O}, (0,2), 2 \cdot (0,2), \cdots, 9 \cdot (0,2)\}$$

On a donc $(2,0) = \ell \cdot (0,2)$ pour un certain ℓ. Que vaut ℓ ?.

$\rightsquigarrow$ C'est le problème du logarithme discret dans $E(\mathbb{F}_7)$! (ici $\ell = 5$).

$\rightsquigarrow$ $E(\mathbb{F}_7)$ est cyclique (c'est fréquent).

Si E est définie sur $\mathbb{F}_p$ avec p grand, le problème du log discret semble compliqué : utile pour la cryptographie.

Il faut pouvoir le mettre en place :

$\rightsquigarrow$ Trouver E et p tels que $\sharp E(\mathbb{F}_p)$ est (presque) premier ;

$\rightsquigarrow$ Il faut savoir calculer $\sharp E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut savoir trouver un point $G \in E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut que E ne soit pas "faible"...

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_7$. Soit $E : y^2 = x^3 + x + 4$. On a

$$E(\mathbb{F}_7) =< (0,2) >= \{\mathcal{O}, (0,2), 2 \cdot (0,2), \cdots, 9 \cdot (0,2)\}$$

On a donc $(2,0) = \ell \cdot (0,2)$ pour un certain ℓ. Que vaut ℓ ?.

$\rightsquigarrow$ C'est le problème du logarithme discret dans $E(\mathbb{F}_7)$! (ici $\ell = 5$).

$\rightsquigarrow$ $E(\mathbb{F}_7)$ est cyclique (c'est fréquent).

Si E est définie sur $\mathbb{F}_p$ avec p grand, le problème du log discret semble compliqué : utile pour la cryptographie.

Il faut pouvoir le mettre en place :

$\rightsquigarrow$ Trouver E et p tels que $\sharp E(\mathbb{F}_p)$ est (presque) premier ;

$\rightsquigarrow$ Il faut savoir calculer $\sharp E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut savoir trouver un point $G \in E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut que E ne soit pas "faible"...

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_7$. Soit $E : y^2 = x^3 + x + 4$. On a

$$E(\mathbb{F}_7) =< (0,2) >= \{\mathcal{O}, (0,2), 2 \cdot (0,2), \cdots, 9 \cdot (0,2)\}$$

On a donc $(2,0) = \ell \cdot (0,2)$ pour un certain ℓ. Que vaut ℓ ?.

$\rightsquigarrow$ C'est le problème du logarithme discret dans $E(\mathbb{F}_7)$! (ici $\ell = 5$).

$\rightsquigarrow$ $E(\mathbb{F}_7)$ est cyclique (c'est fréquent).

Si E est définie sur $\mathbb{F}_p$ avec p grand, le problème du log discret semble compliqué : utile pour la cryptographie.

Il faut pouvoir le mettre en place :

$\rightsquigarrow$ Trouver E et p tels que $\sharp E(\mathbb{F}_p)$ est (presque) premier ;

$\rightsquigarrow$ Il faut savoir calculer $\sharp E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut savoir trouver un point $G \in E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut que E ne soit pas "faible"...

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_7$. Soit $E : y^2 = x^3 + x + 4$. On a

$$E(\mathbb{F}_7) =< (0,2) >= \{\mathcal{O}, (0,2), 2 \cdot (0,2), \cdots, 9 \cdot (0,2)\}$$

On a donc $(2,0) = \ell \cdot (0,2)$ pour un certain ℓ. Que vaut ℓ ?.

$\rightsquigarrow$ C'est le problème du logarithme discret dans $E(\mathbb{F}_7)$! (ici $\ell = 5$).

$\rightsquigarrow$ $E(\mathbb{F}_7)$ est cyclique (c'est fréquent).

Si E est définie sur $\mathbb{F}_p$ avec p grand, le problème du log discret semble compliqué : utile pour la cryptographie.

Il faut pouvoir le mettre en place :

$\rightsquigarrow$ Trouver E et p tels que $\sharp E(\mathbb{F}_p)$ est (presque) premier ;

$\rightsquigarrow$ Il faut savoir calculer $\sharp E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut savoir trouver un point $G \in E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut que E ne soit pas "faible"...

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_7$. Soit $E : y^2 = x^3 + x + 4$. On a

$$E(\mathbb{F}_7) =< (0,2) >= \{\mathcal{O}, (0,2), 2 \cdot (0,2), \cdots, 9 \cdot (0,2)\}$$

On a donc $(2,0) = \ell \cdot (0,2)$ pour un certain ℓ. Que vaut ℓ ?.

$\rightsquigarrow$ C'est le problème du logarithme discret dans $E(\mathbb{F}_7)$! (ici $\ell = 5$).

$\rightsquigarrow$ $E(\mathbb{F}_7)$ est cyclique (c'est fréquent).

Si E est définie sur $\mathbb{F}_p$ avec p grand, le problème du log discret semble compliqué : utile pour la cryptographie.

Il faut pouvoir le mettre en place :

$\rightsquigarrow$ Trouver E et p tels que $\sharp E(\mathbb{F}_p)$ est (presque) premier ;

$\rightsquigarrow$ Il faut savoir calculer $\sharp E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut savoir trouver un point $G \in E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut que E ne soit pas "faible"...

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_7$. Soit $E : y^2 = x^3 + x + 4$. On a

$$E(\mathbb{F}_7) =< (0,2) >= \{\mathcal{O}, (0,2), 2 \cdot (0,2), \cdots, 9 \cdot (0,2)\}$$

On a donc $(2,0) = \ell \cdot (0,2)$ pour un certain ℓ. Que vaut ℓ ?.

$\rightsquigarrow$ C'est le problème du logarithme discret dans $E(\mathbb{F}_7)$! (ici $\ell = 5$).

$\rightsquigarrow$ $E(\mathbb{F}_7)$ est cyclique (c'est fréquent).

Si E est définie sur $\mathbb{F}_p$ avec p grand, le problème du log discret semble compliqué : utile pour la cryptographie.

Il faut pouvoir le mettre en place :

$\rightsquigarrow$ Trouver E et p tels que $\sharp E(\mathbb{F}_p)$ est (presque) premier ;

$\rightsquigarrow$ Il faut savoir calculer $\sharp E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut savoir trouver un point $G \in E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut que E ne soit pas "faible"...

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_7$. Soit $E : y^2 = x^3 + x + 4$. On a

$$E(\mathbb{F}_7) =< (0,2) >= \{\mathcal{O}, (0,2), 2 \cdot (0,2), \cdots, 9 \cdot (0,2)\}$$

On a donc $(2,0) = \ell \cdot (0,2)$ pour un certain ℓ. Que vaut ℓ ?.

$\rightsquigarrow$ C'est le problème du logarithme discret dans $E(\mathbb{F}_7)$! (ici $\ell = 5$).

$\rightsquigarrow$ $E(\mathbb{F}_7)$ est cyclique (c'est fréquent).

Si E est définie sur $\mathbb{F}_p$ avec p grand, le problème du log discret semble compliqué : utile pour la cryptographie.

Il faut pouvoir le mettre en place :

$\rightsquigarrow$ Trouver E et p tels que $\sharp E(\mathbb{F}_p)$ est (presque) premier ;

$\rightsquigarrow$ Il faut savoir calculer $\sharp E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut savoir trouver un point $G \in E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut que E ne soit pas "faible"...

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_7$. Soit $E : y^2 = x^3 + x + 4$. On a

$$E(\mathbb{F}_7) =< (0,2) >= \{\mathcal{O}, (0,2), 2 \cdot (0,2), \cdots, 9 \cdot (0,2)\}$$

On a donc $(2,0) = \ell \cdot (0,2)$ pour un certain ℓ. Que vaut ℓ ?.

$\rightsquigarrow$ C'est le problème du logarithme discret dans $E(\mathbb{F}_7)$! (ici $\ell = 5$).

$\rightsquigarrow$ $E(\mathbb{F}_7)$ est cyclique (c'est fréquent).

Si E est définie sur $\mathbb{F}_p$ avec p grand, le problème du log discret semble compliqué : utile pour la cryptographie.

Il faut pouvoir le mettre en place :

$\rightsquigarrow$ Trouver E et p tels que $\sharp E(\mathbb{F}_p)$ est (presque) premier ;

$\rightsquigarrow$ Il faut savoir calculer $\sharp E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut savoir trouver un point $G \in E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut que E ne soit pas "faible"...

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_7$. Soit $E : y^2 = x^3 + x + 4$. On a

$$E(\mathbb{F}_7) =< (0,2) >= \{\mathcal{O}, (0,2), 2 \cdot (0,2), \cdots, 9 \cdot (0,2)\}$$

On a donc $(2,0) = \ell \cdot (0,2)$ pour un certain ℓ. Que vaut ℓ ?.

$\rightsquigarrow$ C'est le problème du logarithme discret dans $E(\mathbb{F}_7)$! (ici $\ell = 5$).

$\rightsquigarrow$ $E(\mathbb{F}_7)$ est cyclique (c'est fréquent).

Si E est définie sur $\mathbb{F}_p$ avec p grand, le problème du log discret semble compliqué : utile pour la cryptographie.

Il faut pouvoir le mettre en place :

$\rightsquigarrow$ Trouver E et p tels que $\sharp E(\mathbb{F}_p)$ est (presque) premier ;

$\rightsquigarrow$ Il faut savoir calculer $\sharp E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut savoir trouver un point $G \in E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut que E ne soit pas "faible"...

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_7$. Soit $E : y^2 = x^3 + x + 4$. On a

$$E(\mathbb{F}_7) =< (0,2) >= \{\mathcal{O}, (0,2), 2 \cdot (0,2), \cdots, 9 \cdot (0,2)\}$$

On a donc $(2,0) = \ell \cdot (0,2)$ pour un certain ℓ. Que vaut ℓ ?.

$\rightsquigarrow$ C'est le problème du logarithme discret dans $E(\mathbb{F}_7)$! (ici $\ell = 5$).

$\rightsquigarrow$ $E(\mathbb{F}_7)$ est cyclique (c'est fréquent).

Si E est définie sur $\mathbb{F}_p$ avec p grand, le problème du log discret semble compliqué : utile pour la cryptographie.

Il faut pouvoir le mettre en place :

$\rightsquigarrow$ Trouver E et p tels que $\sharp E(\mathbb{F}_p)$ est (presque) premier ;

$\rightsquigarrow$ Il faut savoir calculer $\sharp E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut savoir trouver un point $G \in E(\mathbb{F}_p)$;

$\rightsquigarrow$ Il faut que E ne soit pas "faible"...

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_p$, p grand et $E : y^2 = x^3 + ax + b$. On écrit

$$\sharp E(\mathbb{F}_p) = p + 1 - t$$

Le nombre t s'appelle la trace du Frobenius.

Théorème

- On a $|t| \leq 2\sqrt{p}$ (th. Hasse-Weil).
- Le nombre t se calcule en temps polynomial.
- $E(\mathbb{F}_p) \simeq \mathbb{Z}/d\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2d\mathbb{Z}$ où $d = \frac{p+1-t}{2}$.

Conséquences :

$\rightsquigarrow \sharp E(\mathbb{F}_p) \approx p$.

$\rightsquigarrow \sharp E(\mathbb{F}_p)$ se calcule facilement.

$\rightsquigarrow E(\mathbb{F}_p)$ est cyclique ou presque.

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_p$, p grand et $E : y^2 = x^3 + ax + b$. On écrit

$$\sharp E(\mathbb{F}_p) = p + 1 - t$$

Le nombre t s'appelle la trace du Frobenius.

Théorème

- On a $|t| \leq 2\sqrt{p}$ (th. Hasse-Weil).
- Le nombre t se calcule en temps polynomial.
- $E(\mathbb{F}_p) \simeq \mathbb{Z}/d_2\mathbb{Z}$ ou $\simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$ avec $d_1 \mid d_2$ et $d_1 \mid p - 1$.

Conséquences :

$\rightsquigarrow \sharp E(\mathbb{F}_p) \approx p$.

$\rightsquigarrow \sharp E(\mathbb{F}_p)$ se calcule facilement.

$\rightsquigarrow E(\mathbb{F}_p)$ est cyclique ou presque.

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_p$, p grand et $E : y^2 = x^3 + ax + b$. On écrit

$$\sharp E(\mathbb{F}_p) = p + 1 - t$$

Le nombre t s'appelle la trace du Frobenius.

Théorème

- On a $|t| \leq 2\sqrt{p}$ (th. Hasse-Weil).
- Le nombre t se calcule en temps polynomial.
- $E(\mathbb{F}_p) \simeq \mathbb{Z}/d_2\mathbb{Z}$ ou $\simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$ avec $d_1 \mid d_2$ et $d_1 \mid p - 1$.

Conséquences :

$\rightsquigarrow \sharp E(\mathbb{F}_p) \approx p$.

$\rightsquigarrow \sharp E(\mathbb{F}_p)$ se calcule facilement.

$\rightsquigarrow E(\mathbb{F}_p)$ est cyclique ou presque.

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_p$, p grand et $E : y^2 = x^3 + ax + b$. On écrit

$$\sharp E(\mathbb{F}_p) = p + 1 - t$$

Le nombre t s'appelle la trace du Frobenius.

Théorème

- On a $|t| \leq 2\sqrt{p}$ (th. Hasse-Weil).
- Le nombre t se calcule en temps polynomial.
- $E(\mathbb{F}_p) \simeq \mathbb{Z}/d_2\mathbb{Z}$ ou $\simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$ avec $d_1 \mid d_2$ et $d_1 \mid p - 1$.

Conséquences :

$\rightsquigarrow \sharp E(\mathbb{F}_p) \approx p$.

$\rightsquigarrow \sharp E(\mathbb{F}_p)$ se calcule facilement.

$\rightsquigarrow E(\mathbb{F}_p)$ est cyclique ou presque.

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_p$, p grand et $E : y^2 = x^3 + ax + b$. On écrit

$$\sharp E(\mathbb{F}_p) = p + 1 - t$$

Le nombre t s'appelle la trace du Frobenius.

Théorème

- On a $|t| \leq 2\sqrt{p}$ (th. Hasse-Weil).
- Le nombre t se calcule en temps polynomial.
- $E(\mathbb{F}_p) \simeq \mathbb{Z}/d_2\mathbb{Z}$ ou $\simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$ avec $d_1 \mid d_2$ et $d_1 \mid p - 1$.

Conséquences :

$\rightsquigarrow \sharp E(\mathbb{F}_p) \approx p$.

$\rightsquigarrow \sharp E(\mathbb{F}_p)$ se calcule facilement.

$\rightsquigarrow E(\mathbb{F}_p)$ est cyclique ou presque.

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_p$, p grand et $E : y^2 = x^3 + ax + b$. On écrit

$$\sharp E(\mathbb{F}_p) = p + 1 - t$$

Le nombre t s'appelle la trace du Frobenius.

Théorème

- On a $|t| \leq 2\sqrt{p}$ (th. Hasse-Weil).
- Le nombre t se calcule en temps polynomial.
- $E(\mathbb{F}_p) \simeq \mathbb{Z}/d_2\mathbb{Z}$ ou $\simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$ avec $d_1 \mid d_2$ et $d_1 \mid p - 1$.

Conséquences :

$\rightsquigarrow \sharp E(\mathbb{F}_p) \approx p$.

$\rightsquigarrow \sharp E(\mathbb{F}_p)$ se calcule facilement.

$\rightsquigarrow E(\mathbb{F}_p)$ est cyclique ou presque.

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_p$, p grand et $E : y^2 = x^3 + ax + b$. On écrit

$$\sharp E(\mathbb{F}_p) = p + 1 - t$$

Le nombre t s'appelle la trace du Frobenius.

Théorème

- On a $|t| \leq 2\sqrt{p}$ (th. Hasse-Weil).
- Le nombre t se calcule en temps polynomial.
- $E(\mathbb{F}_p) \simeq \mathbb{Z}/d_2\mathbb{Z}$ ou $\simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$ avec $d_1 \mid d_2$ et $d_1 \mid p - 1$.

Conséquences :

$\rightsquigarrow \sharp E(\mathbb{F}_p) \approx p$.

$\rightsquigarrow \sharp E(\mathbb{F}_p)$ se calcule facilement.

$\rightsquigarrow E(\mathbb{F}_p)$ est cyclique ou presque.

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_p$, p grand et $E : y^2 = x^3 + ax + b$. On écrit

$$\sharp E(\mathbb{F}_p) = p + 1 - t$$

Le nombre t s'appelle la trace du Frobenius.

Théorème

- On a $|t| \leq 2\sqrt{p}$ (th. Hasse-Weil).
- Le nombre t se calcule en temps polynomial.
- $E(\mathbb{F}_p) \simeq \mathbb{Z}/d_2\mathbb{Z}$ ou $\simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$ avec $d_1 \mid d_2$ et $d_1 \mid p - 1$.

Conséquences :

$\rightsquigarrow \sharp E(\mathbb{F}_p) \approx p$.

$\rightsquigarrow \sharp E(\mathbb{F}_p)$ se calcule facilement.

$\rightsquigarrow E(\mathbb{F}_p)$ est cyclique ou presque.

Courbes elliptiques sur $\mathbb{Z}/p\mathbb{Z}$

▷ On prend $k = \mathbb{F}_p$, p grand et $E : y^2 = x^3 + ax + b$. On écrit

$$\sharp E(\mathbb{F}_p) = p + 1 - t$$

Le nombre t s'appelle la trace du Frobenius.

Théorème

- On a $|t| \leq 2\sqrt{p}$ (th. Hasse-Weil).
- Le nombre t se calcule en temps polynomial.
- $E(\mathbb{F}_p) \simeq \mathbb{Z}/d_2\mathbb{Z}$ ou $\simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$ avec $d_1 \mid d_2$ et $d_1 \mid p - 1$.

Conséquences :

$\rightsquigarrow \sharp E(\mathbb{F}_p) \approx p$.

$\rightsquigarrow \sharp E(\mathbb{F}_p)$ se calcule facilement.

$\rightsquigarrow E(\mathbb{F}_p)$ est cyclique ou presque.

Applications cryptographiques

Étape 1 : On choisit p un grand nombre premier.

Étape 2 : On choisit une courbe elliptique E définie sur $\mathbb{F}_p$.

Étape 3 : On calcule t et $\sharp E(\mathbb{F}_p)$.
Si $\sharp E(\mathbb{F}_p)$ n'est pas de la forme $c \cdot q$ avec $c = 1, 2$ ou 3 et q premier alors on retourne à l'étape 1 ou 2.

Étape 4 : On cherche un point $G \in E(\mathbb{F}_p)$ d'ordre q.

Exemple :

▷ $p = 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$.

▷ $E : y^2 = x^3 + 3$.

▷ $t = 146402144145231529258894028971$.

▷ $p + 1 - t$ est un nombre premier $\rightsquigarrow E(\mathbb{F}_p)$ est cyclique d'ordre premier.

▷ $G = (1, 2)$ est générateur de $E(\mathbb{F}_p)$.

L'exemple est la courbe $\mathrm{secp192k1}$ de Certicom. La sécurité est annoncée équivalente à RSA/DSA 1536 (i.e. qu'un problème du log discret posé sur un $\mathbb{F}_p^\times$ avec $p \approx 2^{1536}$).

Applications cryptographiques

Étape 1 : On choisit p un grand nombre premier.

Étape 2 : On choisit une courbe elliptique E définie sur $\mathbb{F}_p$.

Étape 3 : On calcule t et $\sharp E(\mathbb{F}_p)$.
Si $\sharp E(\mathbb{F}_p)$ n'est pas de la forme $c \cdot q$ avec $c = 1, 2$ ou 3 et q premier alors on retourne à l'étape 1 ou 2.

Étape 4 : On cherche un point $G \in E(\mathbb{F}_p)$ d'ordre q.

Exemple :

▷ $p = 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$.

▷ $E : y^2 = x^3 + 3$.

▷ $t = 146402144145231529258894028971$.

▷ $p + 1 - t$ est un nombre premier $\rightsquigarrow E(\mathbb{F}_p)$ est cyclique d'ordre premier.

▷ $G = (1, 2)$ est générateur de $E(\mathbb{F}_p)$.

L'exemple est la courbe $\mathrm{secp192k1}$ de Certicom. La sécurité est annoncée équivalente à RSA/DSA 1536 (i.e. qu'un problème du log discret posé sur un $\mathbb{F}_p^\times$ avec $p \approx 2^{1536}$).

Applications cryptographiques

Étape 1 : On choisit p un grand nombre premier.

Étape 2 : On choisit une courbe elliptique E définie sur $\mathbb{F}_p$.

Étape 3 : On calcule t et $\sharp E(\mathbb{F}_p)$.
Si $\sharp E(\mathbb{F}_p)$ n'est pas de la forme $c \cdot q$ avec $c = 1, 2$ ou 3 et q premier alors on retourne à l'étape 1 ou 2.

Étape 4 : On cherche un point $G \in E(\mathbb{F}_p)$ d'ordre q.

Exemple :

- $p = 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$.
- $E : y^2 = x^3 + 3$.
- $t = 146402144145231529258894028971$.
- $p + 1 - t$ est un nombre premier $\rightsquigarrow E(\mathbb{F}_p)$ est cyclique d'ordre premier.
- $G = (1, 2)$ est générateur de $E(\mathbb{F}_p)$.

L'exemple est la courbe $\mathtt{secp192k1}$ de Certicom. La sécurité est annoncée équivalente à RSA/DSA 1536 (i.e. qu'un problème du log discret posé sur un $\mathbb{F}_p^\times$ avec $p \approx 2^{1536}$).

Applications cryptographiques

Étape 1 : On choisit p un grand nombre premier.

Étape 2 : On choisit une courbe elliptique E définie sur $\mathbb{F}_p$.

Étape 3 : On calcule t et $\sharp E(\mathbb{F}_p)$.
Si $\sharp E(\mathbb{F}_p)$ n'est pas de la forme $c \cdot q$ avec $c = 1, 2$ ou 3 et q premier alors on retourne à l'étape 1 ou 2.

Étape 4 : On cherche un point $G \in E(\mathbb{F}_p)$ d'ordre q.

Exemple :

- $p = 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$.
- $E : y^2 = x^3 + 3$.
- $t = 146402144145231529258894028971$.
- $p + 1 - t$ est un nombre premier $\rightsquigarrow E(\mathbb{F}_p)$ est cyclique d'ordre premier.
- $G = (1, 2)$ est générateur de $E(\mathbb{F}_p)$.

L'exemple est la courbe $\mathtt{secp192k1}$ de Certicom. La sécurité est annoncée équivalente à RSA/DSA 1536 (i.e. qu'un problème du log discret posé sur un $\mathbb{F}_p^\times$ avec $p \approx 2^{1536}$).

Applications cryptographiques

Étape 1 : On choisit p un grand nombre premier.

Étape 2 : On choisit une courbe elliptique E définie sur $\mathbb{F}_p$.

Étape 3 : On calcule t et $\sharp E(\mathbb{F}_p)$.
Si $\sharp E(\mathbb{F}_p)$ n'est pas de la forme $c \cdot q$ avec $c = 1, 2$ ou 3 et q premier alors on retourne à l'étape 1 ou 2.

Étape 4 : On cherche un point $G \in E(\mathbb{F}_p)$ d'ordre q.

Exemple :

- $p = 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$.
- $E : y^2 = x^3 + 3$.
- $t = 146402144145231529258894028971$.
- $p + 1 - t$ est un nombre premier $\rightsquigarrow E(\mathbb{F}_p)$ est cyclique d'ordre premier.
- $G = (1, 2)$ est générateur de $E(\mathbb{F}_p)$.

L'exemple est la courbe $\mathtt{secp192k1}$ de Certicom. La sécurité est annoncée équivalente à RSA/DSA 1536 (i.e. qu'un problème du log discret posé sur un $\mathbb{F}_p^\times$ avec $p \approx 2^{1536}$).

Applications cryptographiques

Étape 1 : On choisit p un grand nombre premier.

Étape 2 : On choisit une courbe elliptique E définie sur $\mathbb{F}_p$.

Étape 3 : On calcule t et $\sharp E(\mathbb{F}_p)$.
Si $\sharp E(\mathbb{F}_p)$ n'est pas de la forme $c \cdot q$ avec $c = 1, 2$ ou 3 et q premier alors on retourne à l'étape 1 ou 2.

Étape 4 : On cherche un point $G \in E(\mathbb{F}_p)$ d'ordre q.

Exemple :

▷ $p = 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$.

▷ $E : y^2 = x^3 + 3$.

▷ $t = 146402144145231529258894028971$.

▷ $p + 1 - t$ est un nombre premier $\rightsquigarrow E(\mathbb{F}_p)$ est cyclique d'ordre premier.

▷ $G = (1, 2)$ est générateur de $E(\mathbb{F}_p)$.

L'exemple est la courbe $\mathtt{secp192k1}$ de Certicom. La sécurité est annoncée équivalente à RSA/DSA 1536 (i.e. qu'un problème du log discret posé sur un $\mathbb{F}_p^\times$ avec $p \approx 2^{1536}$).

Applications cryptographiques

Étape 1 : On choisit p un grand nombre premier.

Étape 2 : On choisit une courbe elliptique E définie sur $\mathbb{F}_p$.

Étape 3 : On calcule t et $\sharp E(\mathbb{F}_p)$.
Si $\sharp E(\mathbb{F}_p)$ n'est pas de la forme $c \cdot q$ avec $c = 1, 2$ ou 3 et q premier alors on retourne à l'étape 1 ou 2.

Étape 4 : On cherche un point $G \in E(\mathbb{F}_p)$ d'ordre q.

Exemple :

▷ $p = 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$.

▷ $E\colon y^2 = x^3 + 3$.

▷ $t = 146402144145231529258894028971$.

▷ $p + 1 - t$ est un nombre premier $\rightsquigarrow E(\mathbb{F}_p)$ est cyclique d'ordre premier.

▷ $G = (1, 2)$ est générateur de $E(\mathbb{F}_p)$.

L'exemple est la courbe $\mathtt{secp192k1}$ de Certicom. La sécurité est annoncée équivalente à RSA/DSA 1536 (i.e. qu'un problème du log discret posé sur un $\mathbb{F}_p^\times$ avec $p \approx 2^{1536}$).

Applications cryptographiques

Étape 1 : On choisit p un grand nombre premier.

Étape 2 : On choisit une courbe elliptique E définie sur $\mathbb{F}_p$.

Étape 3 : On calcule t et $\sharp E(\mathbb{F}_p)$.
Si $\sharp E(\mathbb{F}_p)$ n'est pas de la forme $c \cdot q$ avec $c = 1, 2$ ou 3 et q premier alors on retourne à l'étape 1 ou 2.

Étape 4 : On cherche un point $G \in E(\mathbb{F}_p)$ d'ordre q.

Exemple :

$\triangleright$ $p = 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$.

$\triangleright$ $E\colon y^2 = x^3 + 3$.

$\triangleright$ $t = 146402144145231529258894028971$.

$\triangleright$ $p + 1 - t$ est un nombre premier $\rightsquigarrow$ $E(\mathbb{F}_p)$ est cyclique d'ordre premier.

$\triangleright$ $G = (1, 2)$ est générateur de $E(\mathbb{F}_p)$.

L'exemple est la courbe `secp192k1` de Certicom. La sécurité est annoncée équivalente à RSA/DSA 1536 (i.e. qu'un problème du log discret posé sur un $\mathbb{F}_p^\times$ avec $p \approx 2^{1536}$).

Applications cryptographiques

Étape 1 : On choisit p un grand nombre premier.

Étape 2 : On choisit une courbe elliptique E définie sur $\mathbb{F}_p$.

Étape 3 : On calcule t et $\sharp E(\mathbb{F}_p)$.
Si $\sharp E(\mathbb{F}_p)$ n'est pas de la forme $c \cdot q$ avec $c = 1, 2$ ou 3 et q premier alors on retourne à l'étape 1 ou 2.

Étape 4 : On cherche un point $G \in E(\mathbb{F}_p)$ d'ordre q.

Exemple :

▷ $p = 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$.

▷ $E\colon y^2 = x^3 + 3$.

▷ $t = 146402144145231529258894028971$.

▷ $p + 1 - t$ est un nombre premier $\rightsquigarrow E(\mathbb{F}_p)$ est cyclique d'ordre premier.

▷ $G = (1, 2)$ est générateur de $E(\mathbb{F}_p)$.

L'exemple est la courbe `secp192k1` de Certicom. La sécurité est annoncée équivalente à RSA/DSA 1536 (i.e. qu'un problème du log discret posé sur un $\mathbb{F}_p^\times$ avec $p \approx 2^{1536}$).

Applications cryptographiques

Étape 1 : On choisit p un grand nombre premier.

Étape 2 : On choisit une courbe elliptique E définie sur $\mathbb{F}_p$.

Étape 3 : On calcule t et $\sharp E(\mathbb{F}_p)$.
Si $\sharp E(\mathbb{F}_p)$ n'est pas de la forme $c \cdot q$ avec $c = 1, 2$ ou 3 et q premier alors on retourne à l'étape 1 ou 2.

Étape 4 : On cherche un point $G \in E(\mathbb{F}_p)$ d'ordre q.

Exemple :

$\triangleright$ $p = 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$.

$\triangleright$ $E\colon y^2 = x^3 + 3$.

$\triangleright$ $t = 1464021441452315292588940289 71$.

$\triangleright$ $p + 1 - t$ est un nombre premier $\rightsquigarrow$ $E(\mathbb{F}_p)$ est cyclique d'ordre premier.

$\triangleright$ $G = (1, 2)$ est générateur de $E(\mathbb{F}_p)$.

L'exemple est la courbe `secp192k1` de Certicom. La sécurité est annoncée équivalente à RSA/DSA 1536 (i.e. qu'un problème du log discret posé sur un $\mathbb{F}_p^\times$ avec $p \approx 2^{1536}$).

Applications cryptographiques

▷ Le système est donné par $(\mathbb{F}_p, E, G, n)$ où E est une courbe elliptique définie sur $\mathbb{F}_p$, $G \in E(\mathbb{F}_p)$ est d'ordre n premier.

Attention :

- Si $t = 1$ alors $\sharp E(\mathbb{F}_p) = p + 1 - t = p$ est premier. ← Attaque de Smart (linéaire) pour le log discret.
- Si $t = 0$ alors le problème du log discret sur $E(\mathbb{F}_p)$ se ramène à un problème du log discret sur $\mathbb{F}_q^\times$ ← attaque sous-exponentielle (attaque MOV).

...

Applications cryptographiques

▷ Le système est donné par $(\mathbb{F}_p, E, G, n)$ où E est une courbe elliptique définie sur $\mathbb{F}_p$, $G \in E(\mathbb{F}_p)$ est d'ordre n premier.

Attention :

- Si $t = 1$ alors $\sharp E(\mathbb{F}_p) = p + 1 - t = p$ est premier. ← Attaque de Smart (linéaire) pour le log discret.
- Si $t = 0$ alors le problème du log discret sur $E(\mathbb{F}_p)$ se ramène à un problème du log discret sur $\mathbb{F}_q^\times$ ← attaque sous-exponentielle (attaque MOV).

...

Applications cryptographiques

▷ Le système est donné par $(\mathbb{F}_p, E, G, n)$ où E est une courbe elliptique définie sur $\mathbb{F}_p$, $G \in E(\mathbb{F}_p)$ est d'ordre n premier.

Attention :

• Si $t = 1$ alors $\sharp E(\mathbb{F}_p) = p + 1 - t = p$ est premier. ← Attaque de Smart (linéaire) pour le log discret.

• Si $t = 0$ alors le problème du log discret sur $E(\mathbb{F}_p)$ se ramène à un problème du log discret sur $\mathbb{F}_q^\times$ ← attaque sous-exponentielle (attaque MOV).

...

Applications cryptographiques

$\triangleright$ Le système est donné par $(\mathbb{F}_p, E, G, n)$ où E est une courbe elliptique définie sur $\mathbb{F}_p$, $G \in E(\mathbb{F}_p)$ est d'ordre n premier.

Attention :

• Si $t = 1$ alors $\sharp E(\mathbb{F}_p) = p + 1 - t = p$ est premier. $\leftarrow$ Attaque de Smart (linéaire) pour le log discret.

• Si $t = 0$ alors le problème du log discret sur $E(\mathbb{F}_p)$ se ramène à un problème du log discret sur $\mathbb{F}_q^\times$ $\leftarrow$ attaque sous-exponentielle (attaque MOV).

...

Conclusion

▷ Les courbes elliptiques permettent de réduire la taille des nombres dans les cryptosystèmes :

⇝ Calculs plus rapides ;

⇝ Besoin de moins de mémoire.

▷ Système pensé dans les années 80 et de plus en plus utilisé depuis une dizaine d'années.

▷ Les courbes elliptiques sont aussi utilisée en cryptographie pour :

⇝ Factoriser ;

⇝ Certifier la primalité des nombres premiers.

▷ Il y a des généralisations...

Conclusion

▷ Les courbes elliptiques permettent de réduire la taille des nombres dans les cryptosystèmes :

- ⇝ Calculs plus rapides ;
- ⇝ Besoin de moins de mémoire.

▷ Système pensé dans les années 80 et de plus en plus utilisé depuis une dizaine d'années.

▷ Les courbes elliptiques sont aussi utilisée en cryptographie pour :

- ⇝ Factoriser ;
- ⇝ Certifier la primalité des nombres premiers.

▷ Il y a des généralisations...

Conclusion

▷ Les courbes elliptiques permettent de réduire la taille des nombres dans les cryptosystèmes :

- ⇝ Calculs plus rapides ;
- ⇝ Besoin de moins de mémoire.

▷ Système pensé dans les années 80 et de plus en plus utilisé depuis une dizaine d'années.

▷ Les courbes elliptiques sont aussi utilisée en cryptographie pour :

- ⇝ Factoriser ;
- ⇝ Certifier la primalité des nombres premiers.

▷ Il y a des généralisations...

Conclusion

▷ Les courbes elliptiques permettent de réduire la taille des nombres dans les cryptosystèmes :

- ⇝ Calculs plus rapides ;
- ⇝ Besoin de moins de mémoire.

▷ Système pensé dans les années 80 et de plus en plus utilisé depuis une dizaine d'années.

▷ Les courbes elliptiques sont aussi utilisée en cryptographie pour :

- ⇝ Factoriser ;
- ⇝ Certifier la primalité des nombres premiers.

▷ Il y a des généralisations...

Conclusion

▷ Les courbes elliptiques permettent de réduire la taille des nombres dans les cryptosystèmes :

- ⇝ Calculs plus rapides ;
- ⇝ Besoin de moins de mémoire.

▷ Système pensé dans les années 80 et de plus en plus utilisé depuis une dizaine d'années.

▷ Les courbes elliptiques sont aussi utilisée en cryptographie pour :

- ⇝ Factoriser ;
- ⇝ Certifier la primalité des nombres premiers.

▷ Il y a des généralisations...

Factoriser avec les courbes elliptiques

▷ Soit N un entier premier et $E : y^2 = x^3 + ax + b$ une courbe elliptique sur $\mathbb{F}_N = \mathbb{Z}/N\mathbb{Z}$.

▷ La loi de groupe sur $E(\mathbb{Z}/N\mathbb{Z})$ est donnée par : si $P = (x_1, y_1)$, $Q = (x_2, y_2)$, on pose

$$L = \begin{cases} x_2 - x_1 & \text{si } x_1 \neq x_2 \\ 2y_1 & \text{si } P = Q \end{cases}$$

Si $L \neq 0$ (sinon $P + Q = O$) alors $P + Q = (x_3, y_3)$ avec

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \\ y_3 &= -y_1 + \lambda(x_1 - x_3) \end{aligned} \quad \text{où } \lambda = \begin{cases} (y_2 - y_1)L^{-1} & \text{si } x_1 \neq x_2 \\ (3x_1^2 + a)L^{-1} & \text{si } P = Q \end{cases}$$

▷ Idée (due à Lenstra) : si N n'est pas premier, on fait comme si et on effectue plein de "calculs".

▷ Si un calcul n'est pas possible, c'est que L n'est pas inversible et $\text{pgcd}(N, L)$ fournit un facteur non trivial de N.

▷ On va (essayer de) calculer ℓP, où P est un point de la courbe E définie sur $\mathbb{Z}/N\mathbb{Z}$ et $\ell \in \mathbb{Z}$.

Factoriser avec les courbes elliptiques

▷ Soit N un entier premier et $E : y^2 = x^3 + ax + b$ une courbe elliptique sur $\mathbb{F}_N = \mathbb{Z}/N\mathbb{Z}$.

▷ La loi de groupe sur $E(\mathbb{Z}/N\mathbb{Z})$ est donnée par : si $P = (x_1, y_1)$, $Q = (x_2, y_2)$, on pose

$$L = \begin{cases} x_2 - x_1 & \text{si } x_1 \neq x_2 \\ 2y_1 & \text{si } P = Q \end{cases}$$

Si $L \neq 0$ (sinon $P + Q = \mathcal{O}$) alors $P + Q = (x_3, y_3)$ avec

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \\ y_3 &= -y_1 + \lambda(x_1 - x_3) \end{aligned} \quad \text{où } \lambda = \begin{cases} (y_2 - y_1)L^{-1} & \text{si } x_1 \neq x_2 \\ (3x_1^2 + a)L^{-1} & \text{si } P = Q \end{cases}$$

▷ Idée (due à Lenstra) : si N n'est pas premier, on fait comme si et on effectue plein de "calculs".

▷ Si un calcul n'est pas possible, c'est que L n'est pas inversible et $\text{pgcd}(N, L)$ fournit un facteur non trivial de N.

▷ On va (essayer de) calculer ℓP, où P est un point de la courbe E définie sur $\mathbb{Z}/N\mathbb{Z}$ et $\ell \in \mathbb{Z}$.

Factoriser avec les courbes elliptiques

▷ Soit N un entier premier et $E : y^2 = x^3 + ax + b$ une courbe elliptique sur $\mathbb{F}_N = \mathbb{Z}/N\mathbb{Z}$.

▷ La loi de groupe sur $E(\mathbb{Z}/N\mathbb{Z})$ est donnée par : si $P = (x_1, y_1)$, $Q = (x_2, y_2)$, on pose

$$L = \begin{cases} x_2 - x_1 & \text{si } x_1 \neq x_2 \\ 2y_1 & \text{si } P = Q \end{cases}$$

Si $L \neq 0$ (sinon $P + Q = \mathcal{O}$) alors $P + Q = (x_3, y_3)$ avec

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \\ y_3 &= -y_1 + \lambda(x_1 - x_3) \end{aligned} \quad \text{où } \lambda = \begin{cases} (y_2 - y_1)L^{-1} & \text{si } x_1 \neq x_2 \\ (3x_1^2 + a)L^{-1} & \text{si } P = Q \end{cases}$$

▷ Idée (due à Lenstra) : si N n'est pas premier, on fait comme si et on effectue plein de "calculs".

▷ Si un calcul n'est pas possible, c'est que L n'est pas inversible et $\text{pgcd}(N, L)$ fournit un facteur non trivial de N.

▷ On va (essayer de) calculer ℓP, où P est un point de la courbe E définie sur $\mathbb{Z}/N\mathbb{Z}$ et $\ell \in \mathbb{Z}$.

Factoriser avec les courbes elliptiques

▷ Soit N un entier premier et $E : y^2 = x^3 + ax + b$ une courbe elliptique sur $\mathbb{F}_N = \mathbb{Z}/N\mathbb{Z}$.

▷ La loi de groupe sur $E(\mathbb{Z}/N\mathbb{Z})$ est donnée par : si $P = (x_1, y_1)$, $Q = (x_2, y_2)$, on pose

$$L = \begin{cases} x_2 - x_1 & \text{si } x_1 \neq x_2 \\ 2y_1 & \text{si } P = Q \end{cases}$$

Si $L \neq 0$ (sinon $P + Q = \mathcal{O}$) alors $P + Q = (x_3, y_3)$ avec

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \\ y_3 &= -y_1 + \lambda(x_1 - x_3) \end{aligned} \quad \text{où } \lambda = \begin{cases} (y_2 - y_1)L^{-1} & \text{si } x_1 \neq x_2 \\ (3x_1^2 + a)L^{-1} & \text{si } P = Q \end{cases}$$

▷ Idée (due à Lenstra) : si N n'est pas premier, on fait comme si et on effectue plein de "calculs".

▷ Si un calcul n'est pas possible, c'est que L n'est pas inversible et $\text{pgcd}(N, L)$ fournit un facteur non trivial de N.

▷ On va (essayer de) calculer ℓP, où P est un point de la courbe E définie sur $\mathbb{Z}/N\mathbb{Z}$ et $\ell \in \mathbb{Z}$.

Factoriser avec les courbes elliptiques

▷ Soit N un entier premier et $E : y^2 = x^3 + ax + b$ une courbe elliptique sur $\mathbb{F}_N = \mathbb{Z}/N\mathbb{Z}$.

▷ La loi de groupe sur $E(\mathbb{Z}/N\mathbb{Z})$ est donnée par : si $P = (x_1, y_1)$, $Q = (x_2, y_2)$, on pose

$$L = \begin{cases} x_2 - x_1 & \text{si } x_1 \neq x_2 \\ 2y_1 & \text{si } P = Q \end{cases}$$

Si $L \neq 0$ (sinon $P + Q = \mathcal{O}$) alors $P + Q = (x_3, y_3)$ avec

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \\ y_3 &= -y_1 + \lambda(x_1 - x_3) \end{aligned} \quad \text{où } \lambda = \begin{cases} (y_2 - y_1)L^{-1} & \text{si } x_1 \neq x_2 \\ (3x_1^2 + a)L^{-1} & \text{si } P = Q \end{cases}$$

▷ Idée (due à Lenstra) : si N n'est pas premier, on fait comme si et on effectue plein de "calculs".

▷ Si un calcul n'est pas possible, c'est que L n'est pas inversible et pgcd(N, L) fournit un facteur non trivial de N.

▷ On va (essayer de) calculer ℓP, où P est un point de la courbe E définie sur $\mathbb{Z}/N\mathbb{Z}$ et $\ell \in \mathbb{Z}$.

Factoriser avec les courbes elliptiques

▷ Soit N un entier premier et $E : y^2 = x^3 + ax + b$ une courbe elliptique sur $\mathbb{F}_N = \mathbb{Z}/N\mathbb{Z}$.

▷ La loi de groupe sur $E(\mathbb{Z}/N\mathbb{Z})$ est donnée par : si $P = (x_1, y_1)$, $Q = (x_2, y_2)$, on pose

$$L = \begin{cases} x_2 - x_1 & \text{si } x_1 \neq x_2 \\ 2y_1 & \text{si } P = Q \end{cases}$$

Si $L \neq 0$ (sinon $P + Q = \mathcal{O}$) alors $P + Q = (x_3, y_3)$ avec

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \\ y_3 &= -y_1 + \lambda(x_1 - x_3) \end{aligned} \quad \text{où } \lambda = \begin{cases} (y_2 - y_1)L^{-1} & \text{si } x_1 \neq x_2 \\ (3x_1^2 + a)L^{-1} & \text{si } P = Q \end{cases}$$

▷ Idée (due à Lenstra) : si N n'est pas premier, on fait comme si et on effectue plein de "calculs".

▷ Si un calcul n'est pas possible, c'est que L n'est pas inversible et $\text{pgcd}(N, L)$ fournit un facteur non trivial de N.

▷ On va (essayer de) calculer ℓP, où P est un point de la courbe E définie sur $\mathbb{Z}/N\mathbb{Z}$ et $\ell \in \mathbb{Z}$.

Factoriser avec les courbes elliptiques

▷ Soit $N = pq$, $p < q$. On choisit a, x_1, y_2 au hasard et on pose

$$E : y^2 = x^3 + ax + (y_1^2 - (x_1^3 + ax_1)).$$

Alors E est une c. ellipt. sur $\mathbb{Z}/N\mathbb{Z}$ et $P = (x_1, y_1) \in E(\mathbb{Z}/N\mathbb{Z})$.

▷ Le calcul n'est pas possible : $\ell P = O$ vu modulo p et $\ell P \neq O$ vu modulo q.

▷ On calcule ℓP avec $\ell = \prod_{p \leq B} p^{\lfloor \frac{\log B}{\log p} \rfloor}$, où B est fixé.

▷ « **Théorème** » Si $B \approx e^{0.7\sqrt{\log p}\sqrt{\log\log p}}$ alors la probabilité pour que ça marche est de $\approx 1/B$.

Factoriser avec les courbes elliptiques

▷ Soit $N = pq$, $p < q$. On choisit a, x_1, y_2 au hasard et on pose

$$E : y^2 = x^3 + ax + (y_1^2 - (x_1^3 + ax_1)).$$

Alors E est une c. ellipt. sur $\mathbb{Z}/N\mathbb{Z}$ et $P = (x_1, y_1) \in E(\mathbb{Z}/N\mathbb{Z})$.

▷ Le calcul n'est pas possible : $\ell P = \mathcal{O}$ vu modulo p et $\ell P \neq \mathcal{O}$ vu modulo q.

▷ On calcule ℓP avec $\ell = \prod_{p \leq B} p^{\lfloor \frac{\log B}{\log p} \rfloor}$, où B est fixé.

▷ « **Théorème** » Si $B \approx e^{0.7\sqrt{\log p}\sqrt{\log\log p}}$ alors la probabilité pour que ça marche est de $\approx 1/B$.

Factoriser avec les courbes elliptiques

▷ Soit $N = pq$, $p < q$. On choisit a, x_1, y_2 au hasard et on pose

$$E : y^2 = x^3 + ax + (y_1^2 - (x_1^3 + ax_1)).$$

Alors E est une c. ellipt. sur $\mathbb{Z}/N\mathbb{Z}$ et $P = (x_1, y_1) \in E(\mathbb{Z}/N\mathbb{Z})$.

▷ Le calcul n'est pas possible : $\ell P = \mathcal{O}$ vu modulo p et $\ell P \neq \mathcal{O}$ vu modulo q.

▷ On calcule ℓP avec $\ell = \prod_{p \leq B} p^{\lfloor \frac{\log B}{\log p} \rfloor}$, où B est fixé.

▷ « **Théorème** » Si $B \approx e^{0.7\sqrt{\log p}\sqrt{\log\log p}}$ alors la probabilité pour que ça marche est de $\approx 1/B$.

Factoriser avec les courbes elliptiques

▷ Soit $N = pq$, $p < q$. On choisit a, x_1, y_2 au hasard et on pose

$$E : y^2 = x^3 + ax + (y_1^2 - (x_1^3 + ax_1)).$$

Alors E est une c. ellipt. sur $\mathbb{Z}/N\mathbb{Z}$ et $P = (x_1, y_1) \in E(\mathbb{Z}/N\mathbb{Z})$.

▷ Le calcul n'est pas possible : $\ell P = \mathcal{O}$ vu modulo p et $\ell P \neq \mathcal{O}$ vu modulo q.

▷ On calcule ℓP avec $\ell = \prod_{p \leq B} p^{\lfloor \frac{\log B}{\log p} \rfloor}$, où B est fixé.

▷ « **Théorème** » Si $B \approx e^{0.7\sqrt{\log p}\sqrt{\log \log p}}$ alors la probabilité pour que ça marche est de $\approx 1/B$.

Factoriser avec les courbes elliptiques

▷ Soit $N = pq$, $p < q$. On choisit a, x_1, y_2 au hasard et on pose

$$E : y^2 = x^3 + ax + (y_1^2 - (x_1^3 + ax_1)).$$

Alors E est une c. ellipt. sur $\mathbb{Z}/N\mathbb{Z}$ et $P = (x_1, y_1) \in E(\mathbb{Z}/N\mathbb{Z})$.

▷ Le calcul n'est pas possible : $\ell P = \mathcal{O}$ vu modulo p et $\ell P \neq \mathcal{O}$ vu modulo q.

▷ On calcule ℓP avec $\ell = \prod_{p \leq B} p^{\lfloor \frac{\log B}{\log p} \rfloor}$, où B est fixé.

▷ « **Théorème** » Si $B \approx e^{0.7\sqrt{\log p}\sqrt{\log\log p}}$ alors la probabilité pour que ça marche est de $\approx 1/B$.