Petit panorama des mathématiques de la cryptologie

Damien Robert

Avec une partie des transparents gentiment prêtés par Jean-Marc Couveignes

INRIA Bordeaux Sud-Ouest

Labri, 04 Avril 2013

Fonctionnalités cryptographiques

À quoi sert la cryptographie ?

- Chiffrement (pli confidentiel)
- Identification (badge cantine, carte à puce, empreinte digitale)
- Intégrité (clé RIB, scellés)
- Signature (ordre de virement) : identification, intégrité, non-répudiation
- Vie privée, anonymat, argent électronique
- ...

Chiffrement

Alice (Sophie Germain)

veut écrire

à Bob (Carl Friedrich Gauss)

Chiffrement à clé secrète

Alice

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = f_K{}^{(-1)}(c) = f_{K'}(c)$

Chiffrement à clé secrète

Alice

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = f_K{}^{(-1)}(c) = f_{K'}(c)$

Chiffrement à clé secrète

Alice

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = f_K{}^{(-1)}(c) = f_{K'}(c)$

Chiffrement à clé secrète

- Trois étapes : création et distribution de clés, chiffrement, déchiffrement
- Boîte mail, consultation de compte en banque, ...
- Avantages : simple, rapide, bien connu
- Fragilités : attaques statistiques, gestion de clés

Chiffrement à clé publique

Alice
veut envoyer m à Bob.
Elle trouve la clé publique de chiffrement K_{Bob}^{pub} dans l'annuaire.
Elle calcule $c = f_{K_{Bob}^{pub}}(m)$

c est envoyé

à Bob

c

qui utilise sa clé secrète de déchiffrement K_{Bob}^{sec}

$$m = f_{K_{Bob}^{pub}}{}^{(-1)}(c) = g_{K_{Bob}^{sec}}(c)$$

Chiffrement à clé publique

Alice
veut envoyer m à Bob.
Elle trouve la clé publique de chiffrement K_{Bob}^{pub} dans l'annuaire.
Elle calcule $c = f_{K_{Bob}^{pub}}(m)$

c est envoyé

à Bob

c

qui utilise sa clé secrète de déchiffrement K_{Bob}^{sec}

$$m = f_{K_{Bob}^{pub}}{}^{(-1)}(c) = g_{K_{Bob}^{sec}}(c)$$

Chiffrement à clé publique

Alice
veut envoyer m à Bob.
Elle trouve la clé publique de chiffrement K_{Bob}^{pub} dans l'annuaire.
Elle calcule $c = f_{K_{Bob}^{pub}}(m)$

c est envoyé

à Bob

c

qui utilise sa clé secrète de déchiffrement K_{Bob}^{sec}

$$m = f_{K_{Bob}^{pub}}{}^{(-1)}(c) = g_{K_{Bob}^{sec}}(c)$$

Chiffrement à clé publique

- Trois étapes : création et publication de clés, chiffrement, déchiffrement
- Avantages : gestion de clé simplifiée, solidité mathématique
- Fragilités : plus lent, plus compliqué à implémenter

En pratique on combine les deux chiffrements : clé publique pour échanger une clé de session (secrète) qui servira à chiffrer à la volée.

Comment faire ?

- Situations asymétriques : l'un saît l'autre pas.
- Celui qui connaît le secret a un avantage (il peut déchiffrer, il peut se prouver).
- Mesurer cet avantage : théorie de la complexité algorithmique.
- S'appuyer sur des problèmes difficiles.

La thèse de Turing-Church

Alan Turing

Alonzo Church

Tests de primalité

Savoir si un entier P est premier.

Pierre de Fermat

Agrawal, Kayal et Saxena

$$T = n^{6+\epsilon(n)}$$

où n est le nombre de chiffres décimaux de P.

Factorisation

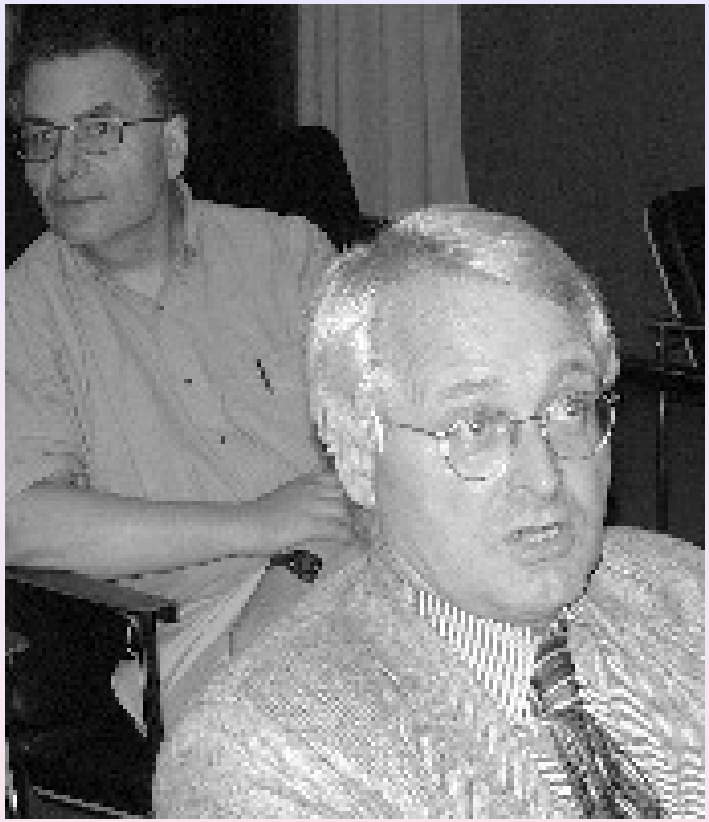
Théorème fondamental de l'arithmétique.

Euclide

Carl Friedrich Gauss

$N = \prod_{1 \leq i \leq I} p_i^{e_i}$.

Factorisation



Hendrik Lenstra

Brigitte Vallée

Factoriser un entier N prend un temps $T = \exp(\sqrt{n})$ où n est le nombre de chiffres décimaux de n.

Asymétrie

$$(p, q) \rightarrow N = pq$$

$$(p, q) \leftarrow N = pq$$

Asymétrie

- En décembre 2009, Thorsten Kleinjung et une dizaine de collègues ont factorisé un nombre de 232 décimales.
- *The sieving, which was done on many hundreds of machines, took almost two years.*
- Calculer le produit de deux nombres de 116 décimales prend 8 millionièmes de secondes sur mon ordinateur portable.

Protocole RSA

Rivest, Shamir et Adleman

Protocole RSA

- Soit $N = pq$ un produit de deux grands nombres premiers ;
- Soit e premier à $\phi(N) = (p-1)(q-1)$ et d l'inverse de e modulo $\phi(N)$;
- Chiffrement : $x \mapsto x^e \mod N$;
- Déchiffrement : $x \mapsto x^d \mod N$;

Théorème (Petit théorème de Fermat)

$x^{\#(\mathbb{Z}/N\mathbb{Z})^\times} = 1 \mod N.$

Identification par mot de passe

Alice

mot de passe d'Alice BELOTE

BELOTE est envoyé

à Bob

mot de passe de Bob REBELOTE

REBELOTE est envoyé à Alice

Identification par mot de passe

- Alice et Bob doivent convenir d'un mot de passe secret partagé (question secrète)
- Avantage : simple
- Fragilités : risque de réutilisation e.g. par un tiers, gestion de mots de passe

Identification sans divulgation de connaissance

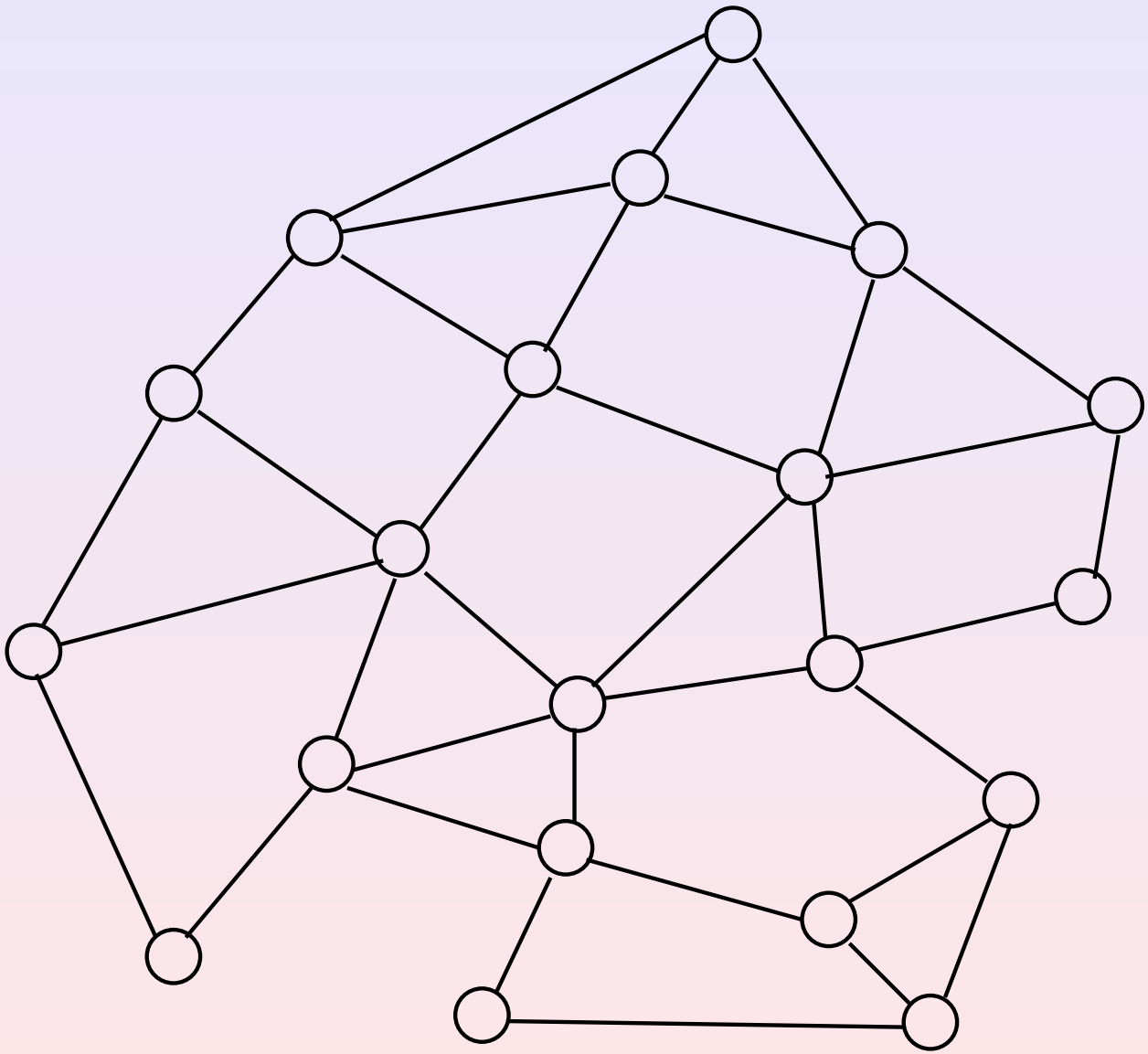
Alice
connaît un secret S_{Alice}

Bob

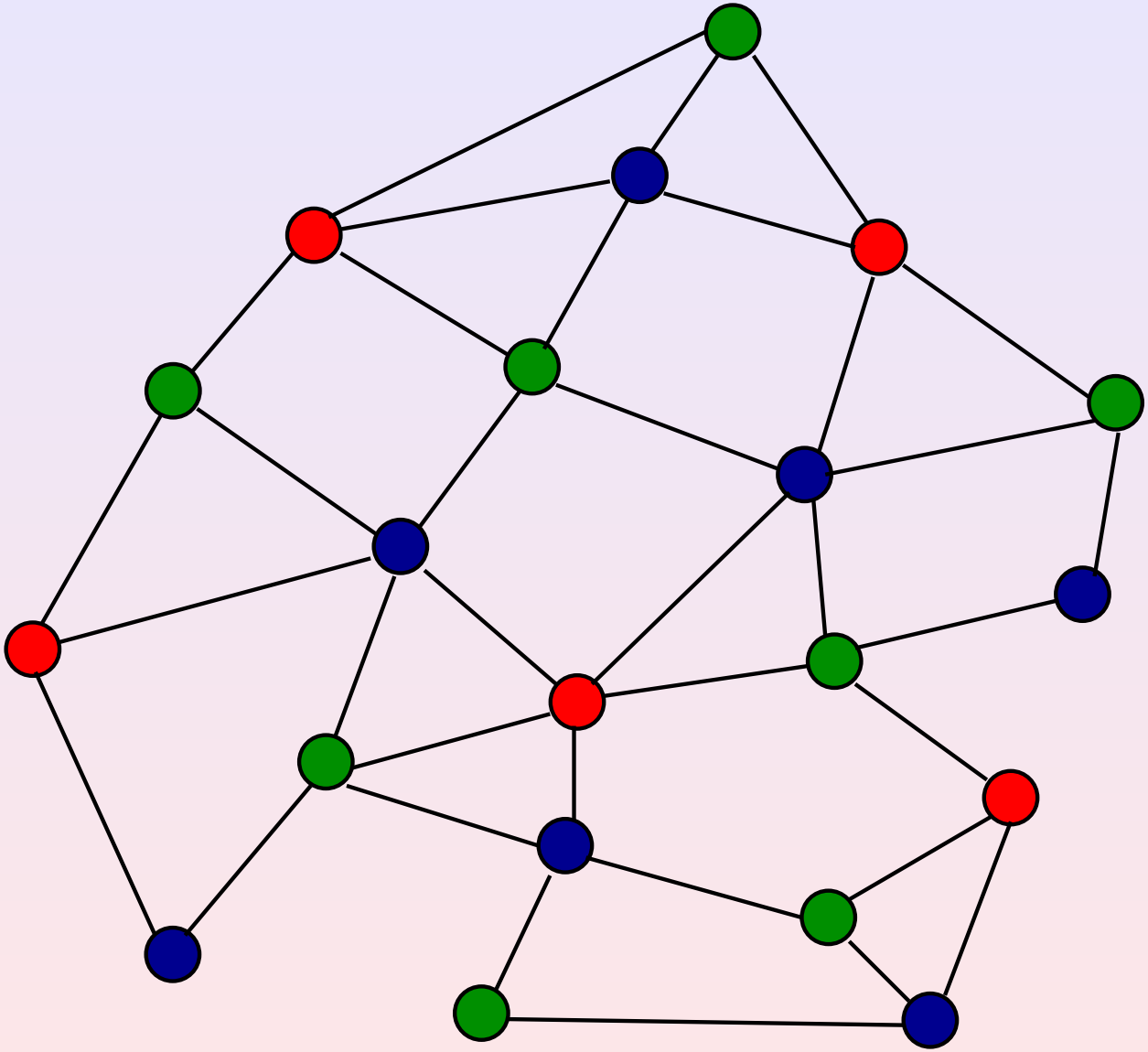
interroge Alice et se convainc qu'elle connaît bien le secret.

À la fin de l'échange, Bob n'a rien appris sur ce secret !

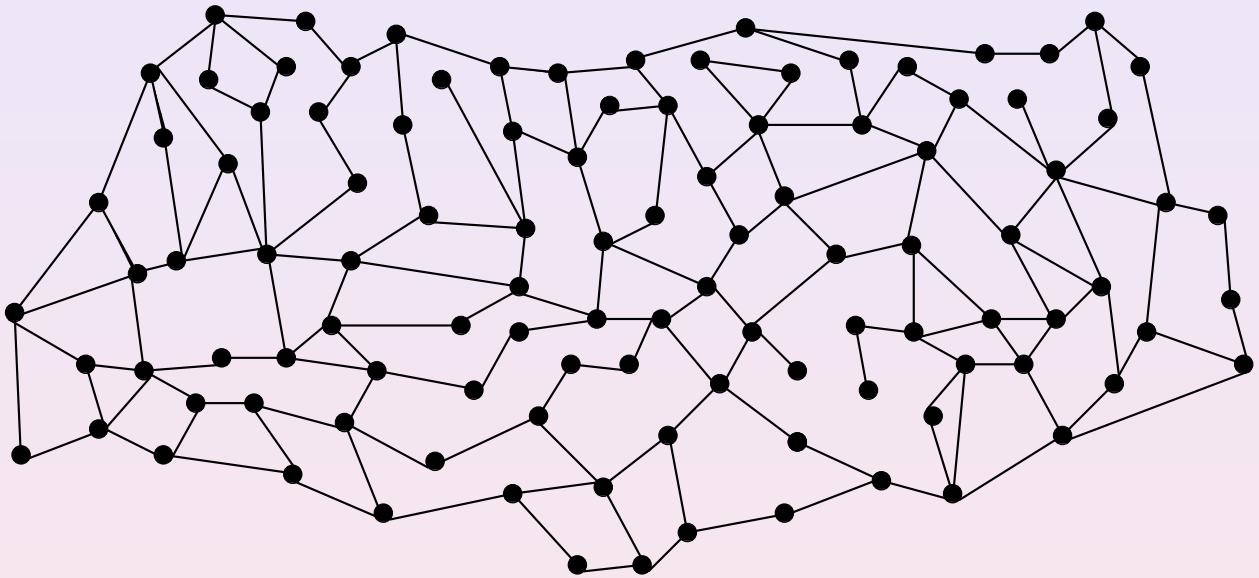
Coloriage de graphe



Coloriage de graphe



Coloriage de graphe

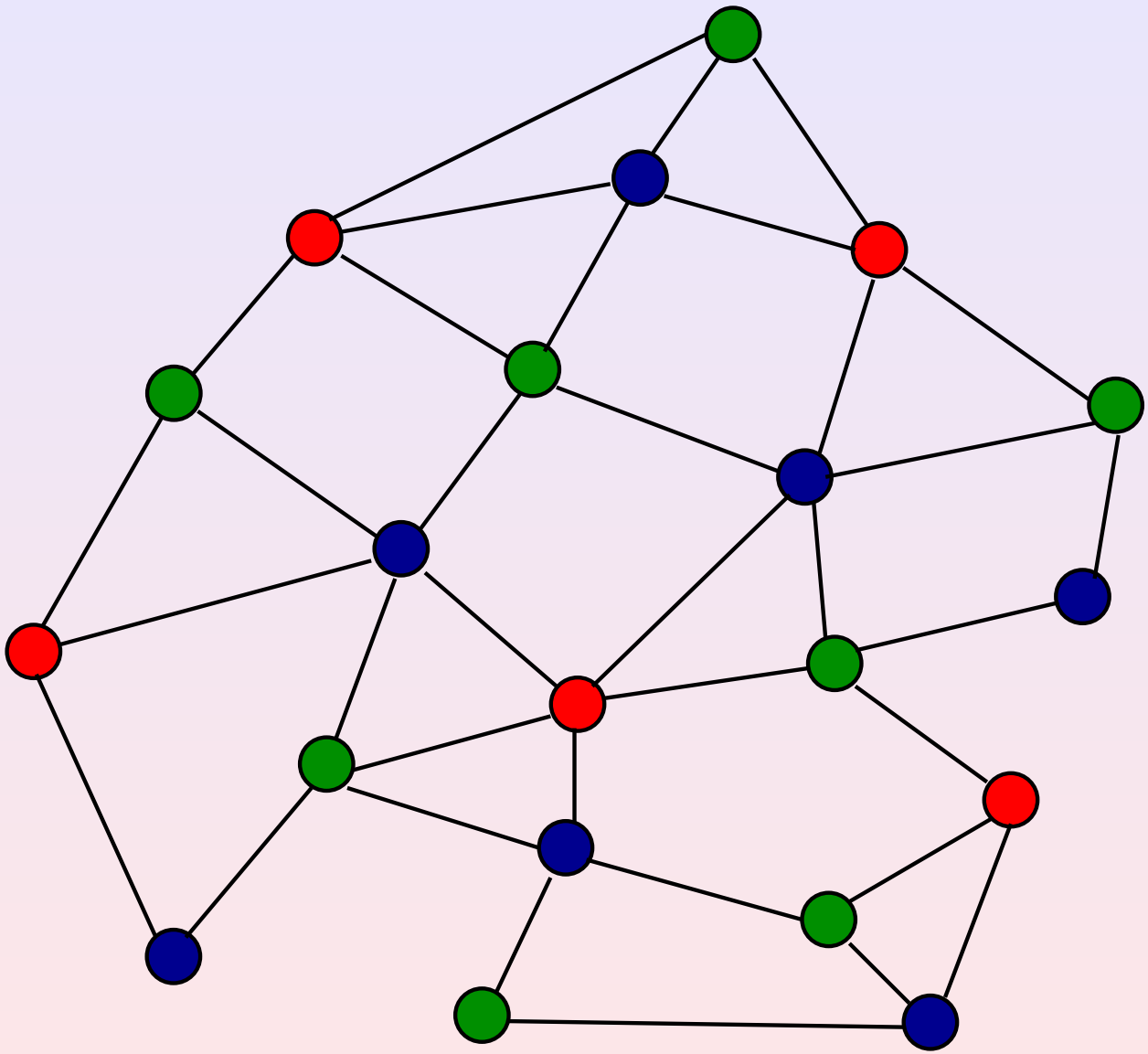


Zero Knowledge Proofs

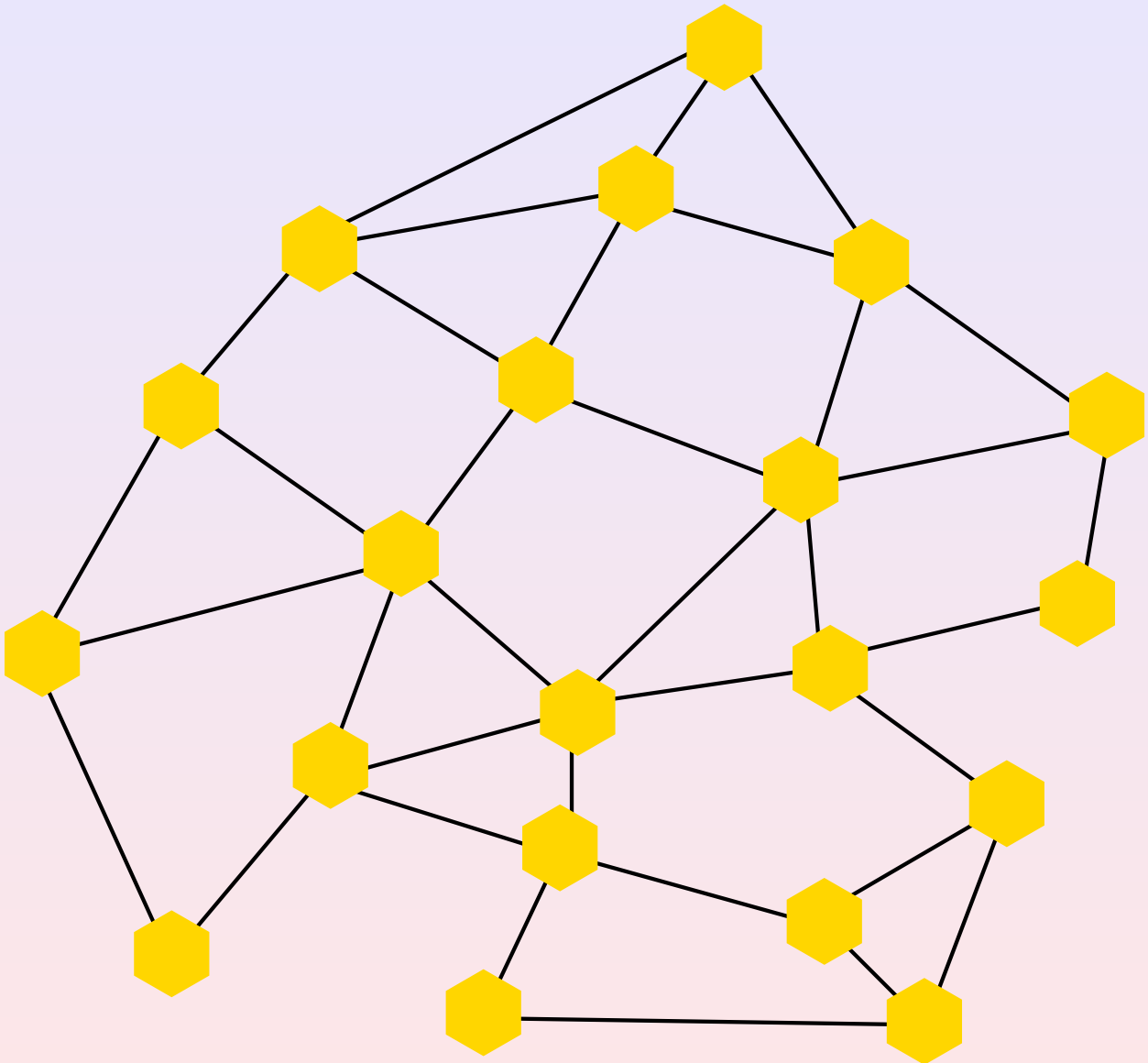
Shafi Goldwasser (1981)

Oded Goldreich (1991)

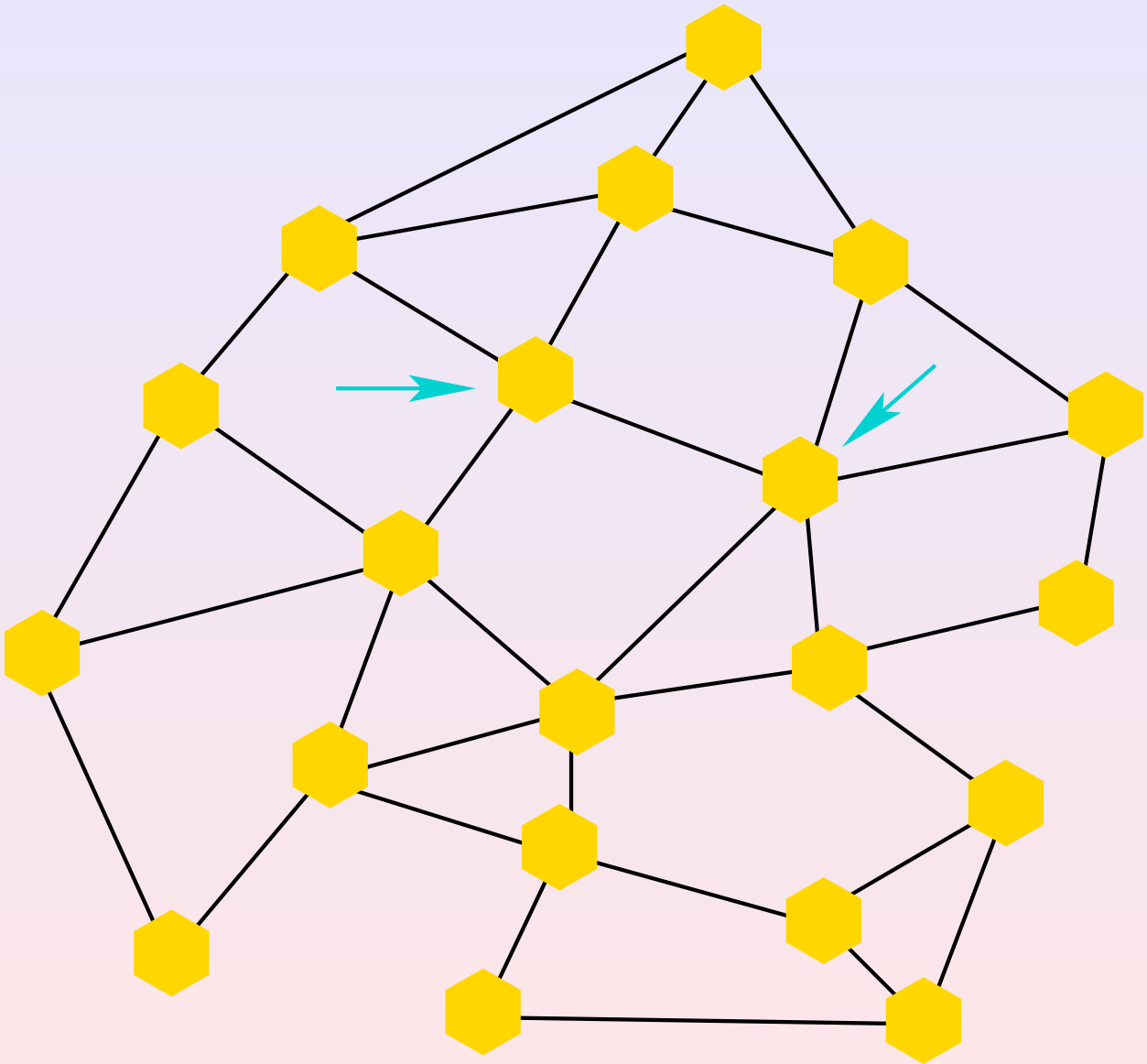
Le coloriage d'Alice (secret)



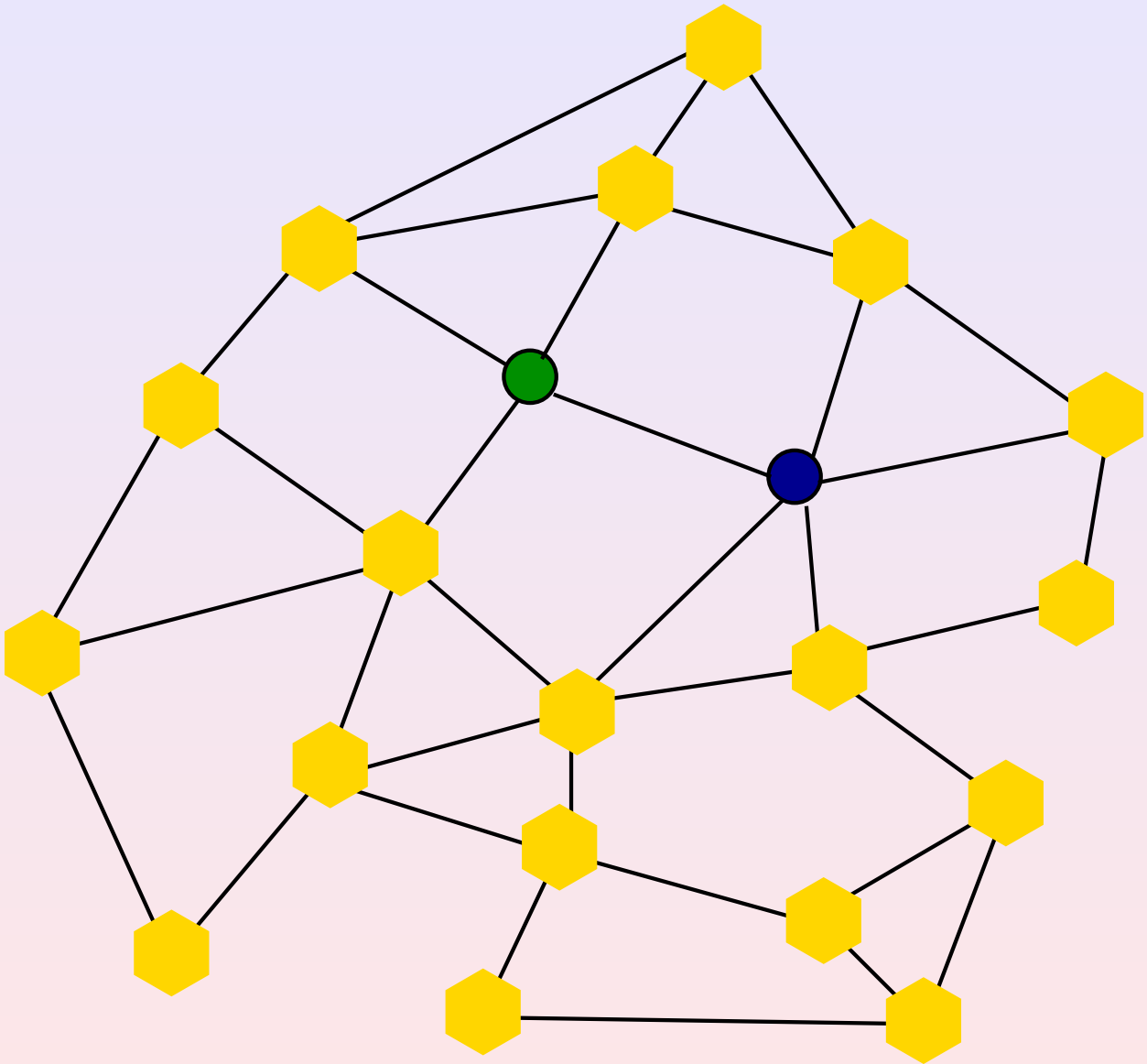
Le coloriage d'Alice caché



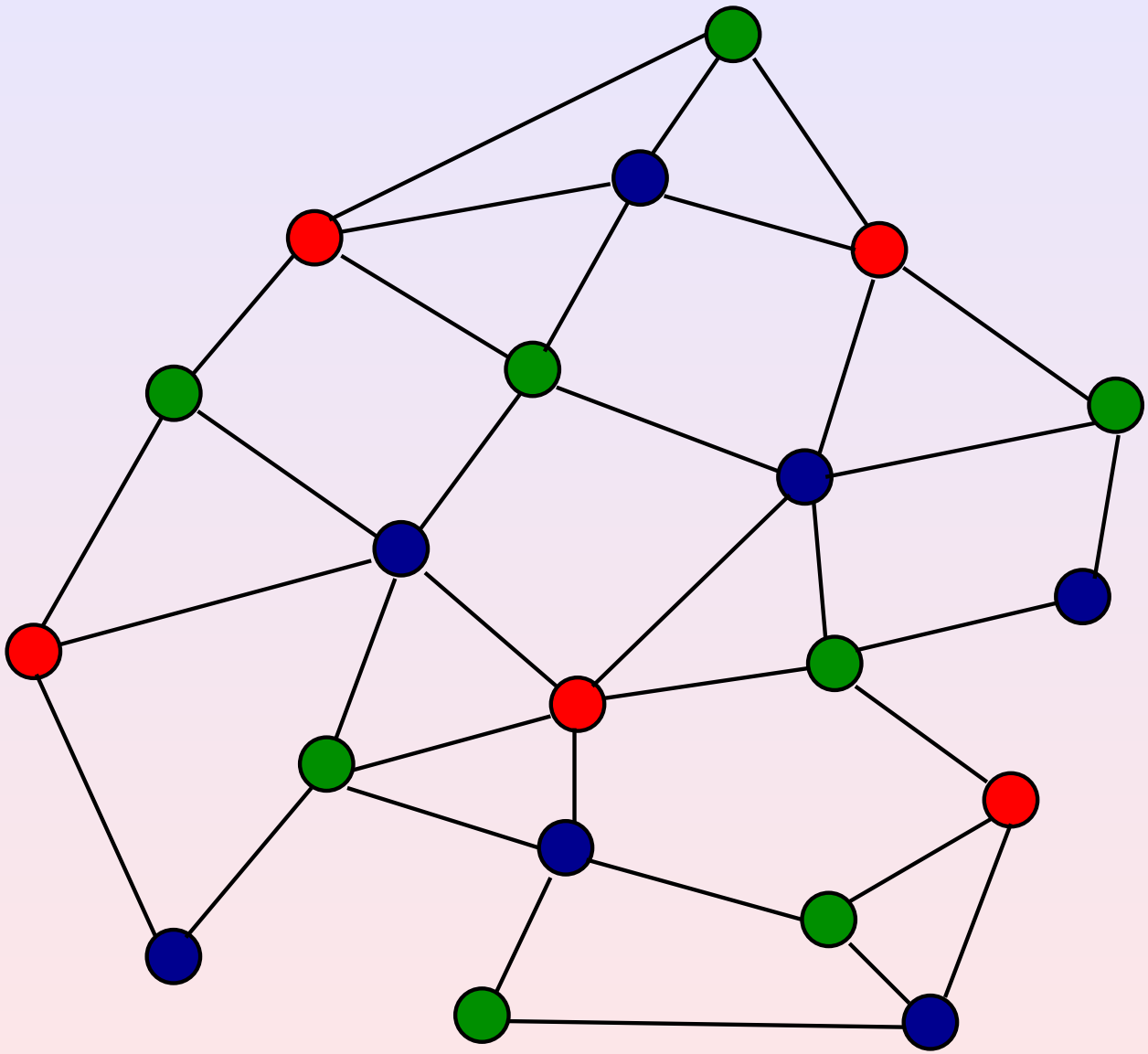
La question de Bob



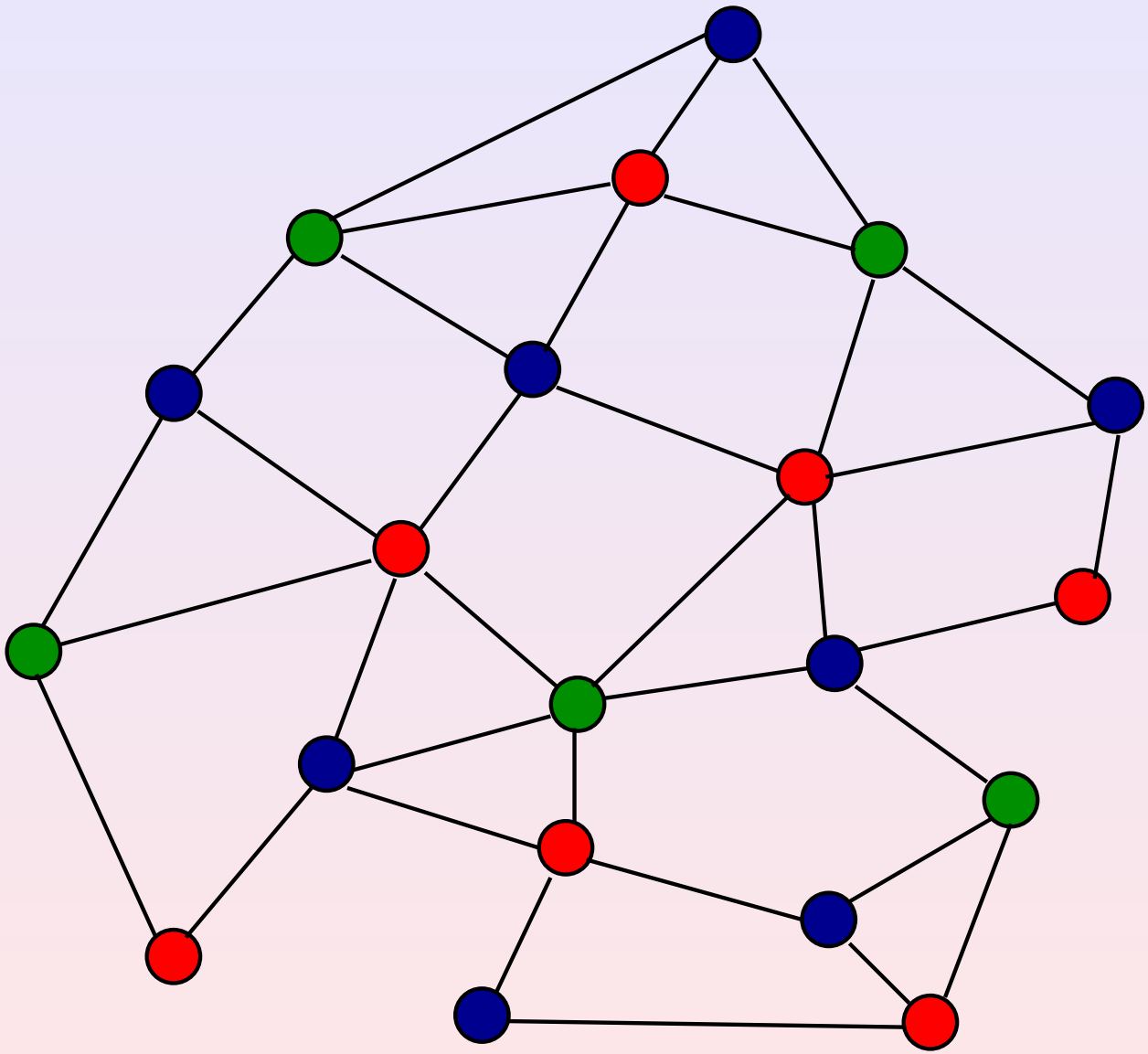
Dévoilement



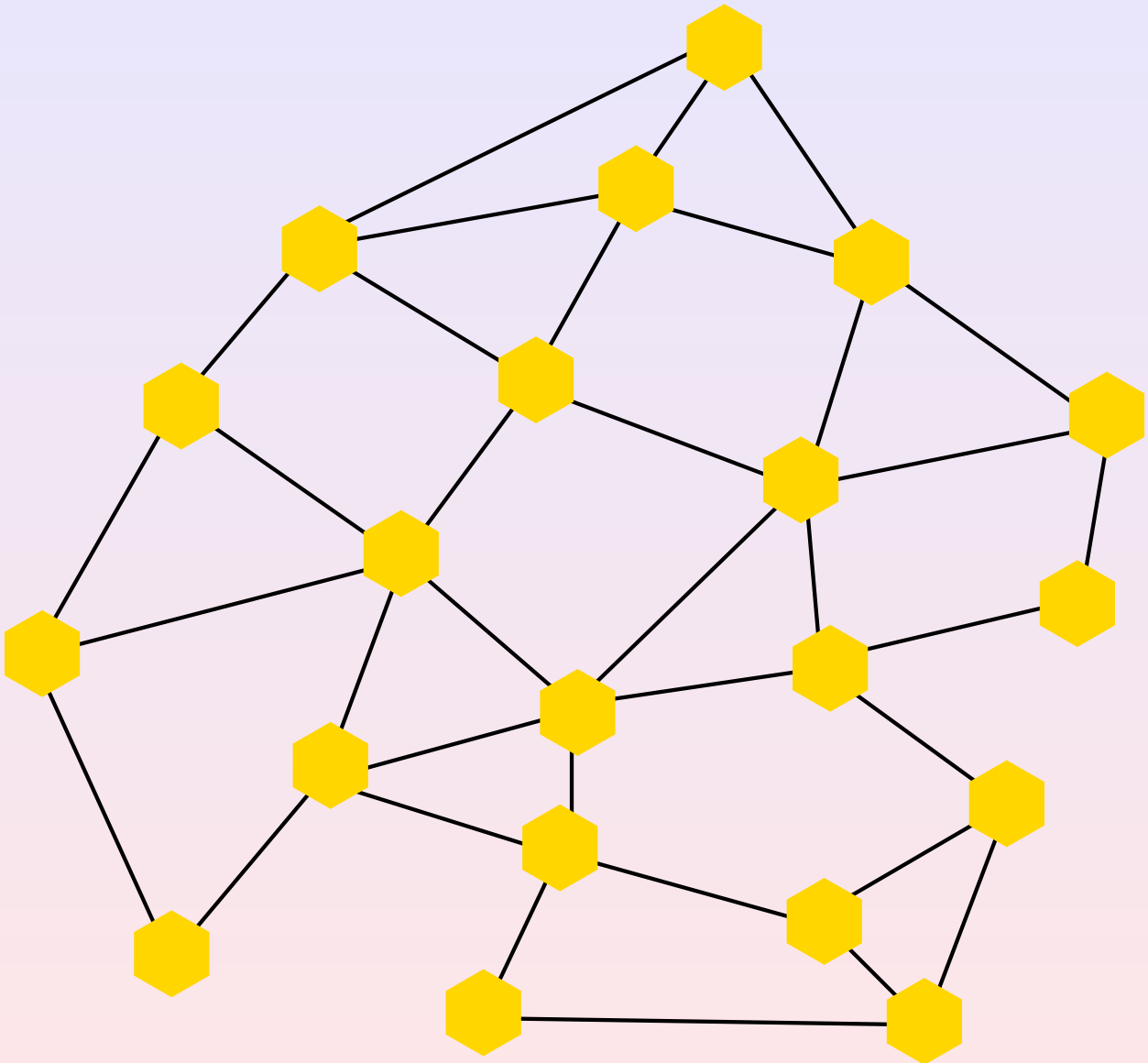
Le coloriage d'Alice (secret)



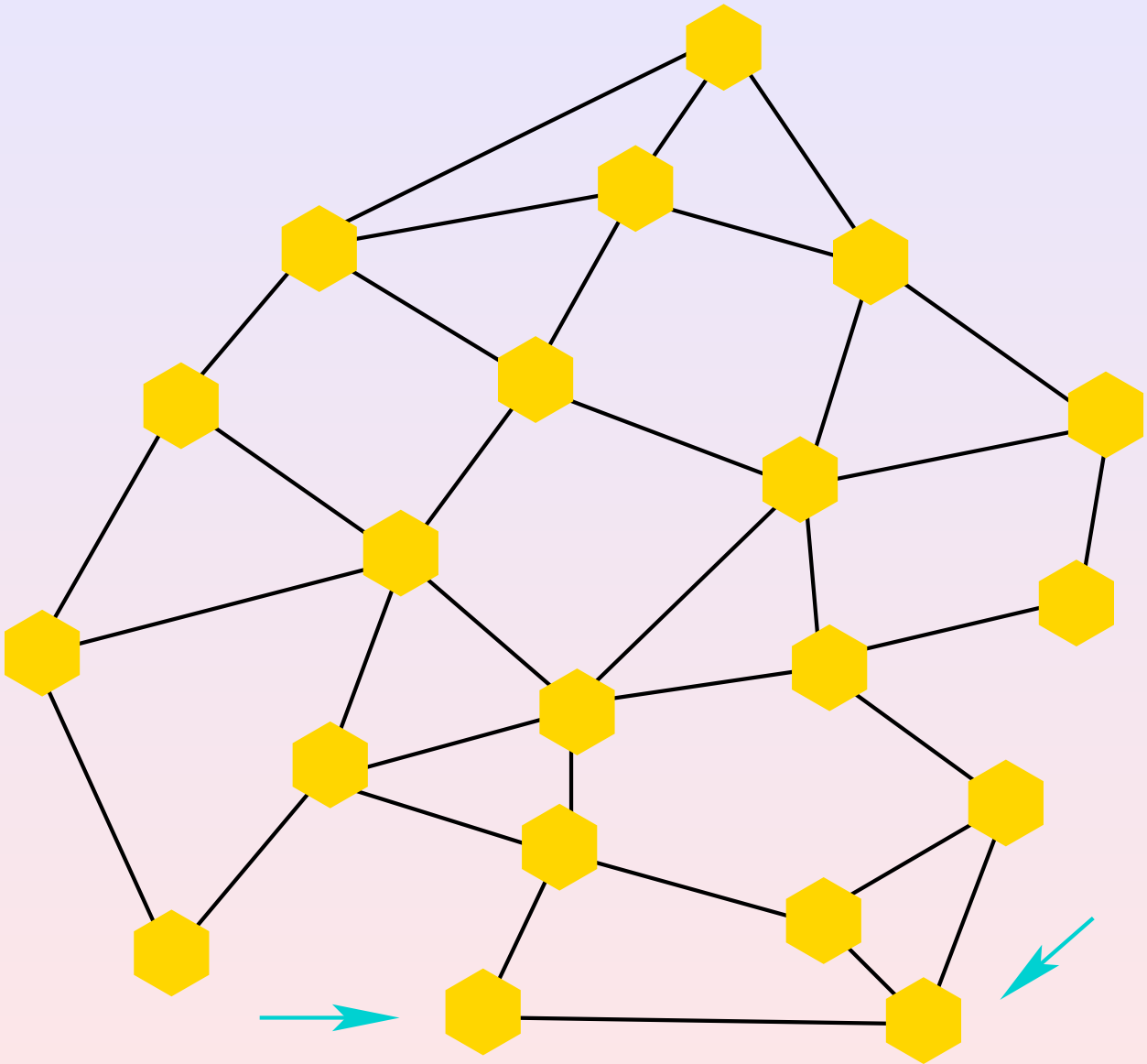
Le coloriage d'Alice permuté



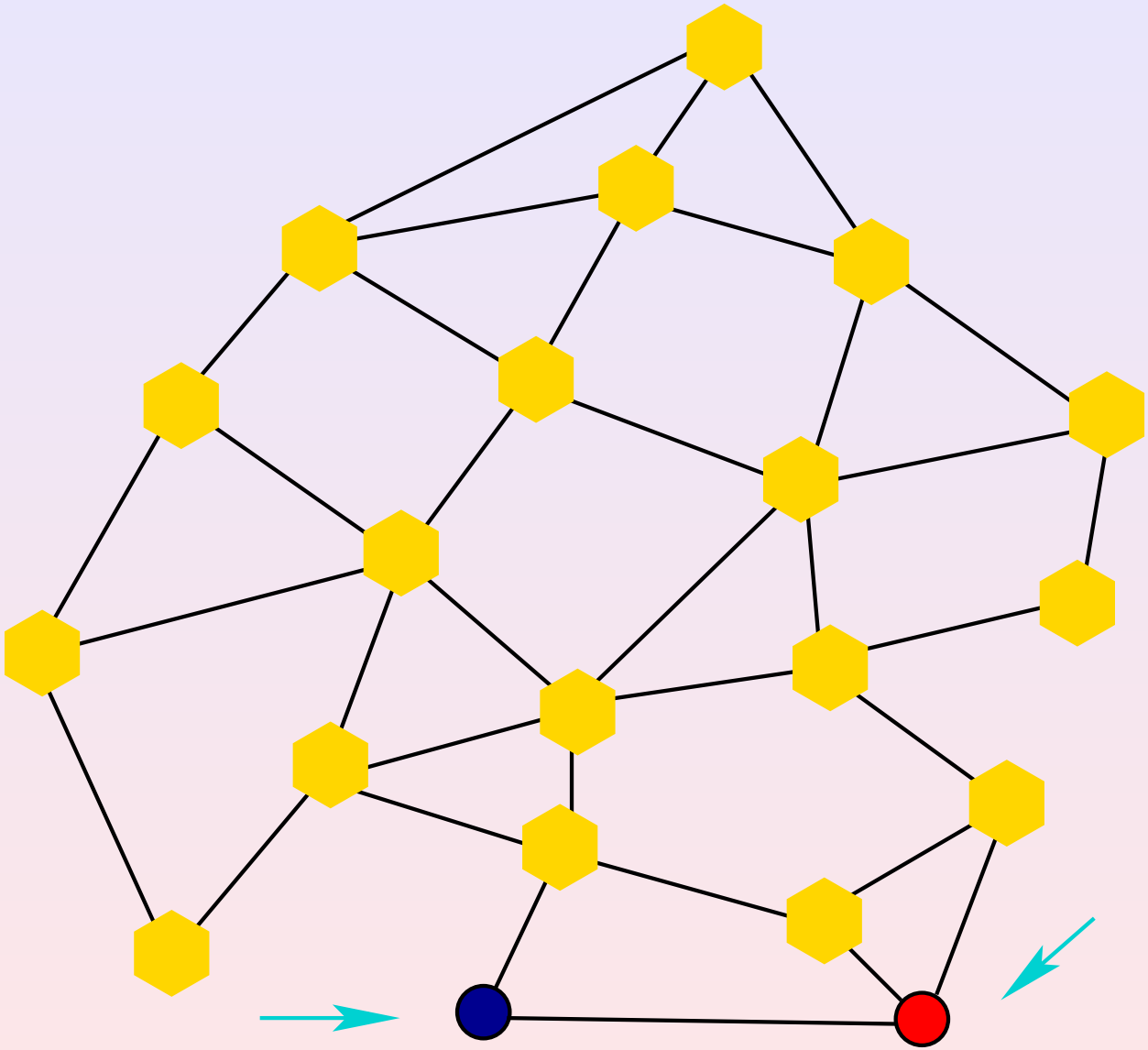
Le coloriage d'Alice caché



La deuxième question de Bob



Dévoilement



Fonctions de Hachage cryptographique

Définition

Compresse des données arbitraires en un “hash” de longueur fixée (typiquement 128 bits).

Une fonction de hachage est dite cryptographiquement sûre si

- Très difficile de trouver des collisions.
- Très difficile de retrouver m à partir de $H(m)$ (si l'on ne connaît pas m).

Mettre en gage des données

Jouer à pile ou face par téléphone.

- Alice lance une pièce
- Bob dit « tu as lancé pile »
- Alice répond « perdu c'était face ! »

Mettre en gage des données

Jouer à pile ou face par téléphone.

- Alice lance une pièce
- Alice envoie le haché de “Pile” ou “Face” à Bob.
- ...

Mettre en gage des données

Jouer à pile ou face par téléphone.

- Alice lance une pièce
- Alice envoie le haché $H(m||\text{Pile})$ ou $H(m||\text{Face})$ à Bob, où m est un message aléatoire.
- Bob dit « tu as lancé pile »
- Alice dévoile m à Bob pour qu'il puisse vérifier le résultat.

Remarque

Attention : en cas de plusieurs tirages, Alice doit changer le message aléatoire m à chaque fois !

Équipe LFANT

Étude de la complexité des grands problèmes algorithmiques de la cryptographie, robustesse des algorithmes (stabilité), implémentations fiables et efficaces, logiciel PARI/GP.

Une équipe de poids lourds.

Équipe LFANT

Mon parcours

- 2007–2010 : Thèse d'informatique au Loria à Nancy dans l'équipe Caramel ;
- 2010–2012 : Postdoctorats à Inria Bordeaux et à Microsoft ;
- 2012 : Chargé de recherche dans l'équipe LFANT.

Échange de clé de Diffie Hellmann

Alice et Bob veulent échanger une clé commune via un canal non sécurisé.

- On part de $7 \mod 61$;
- Alice choisit $17 \mod 61$ et envoie $17 \times 7 = 58 \mod 61$;
- Bob choisit $31 \mod 61$ et envoie $31 \times 7 = 34 \mod 61$;
- Le clé commune est $29 = 34 \times 17 = 58 \times 31$.

Remarque

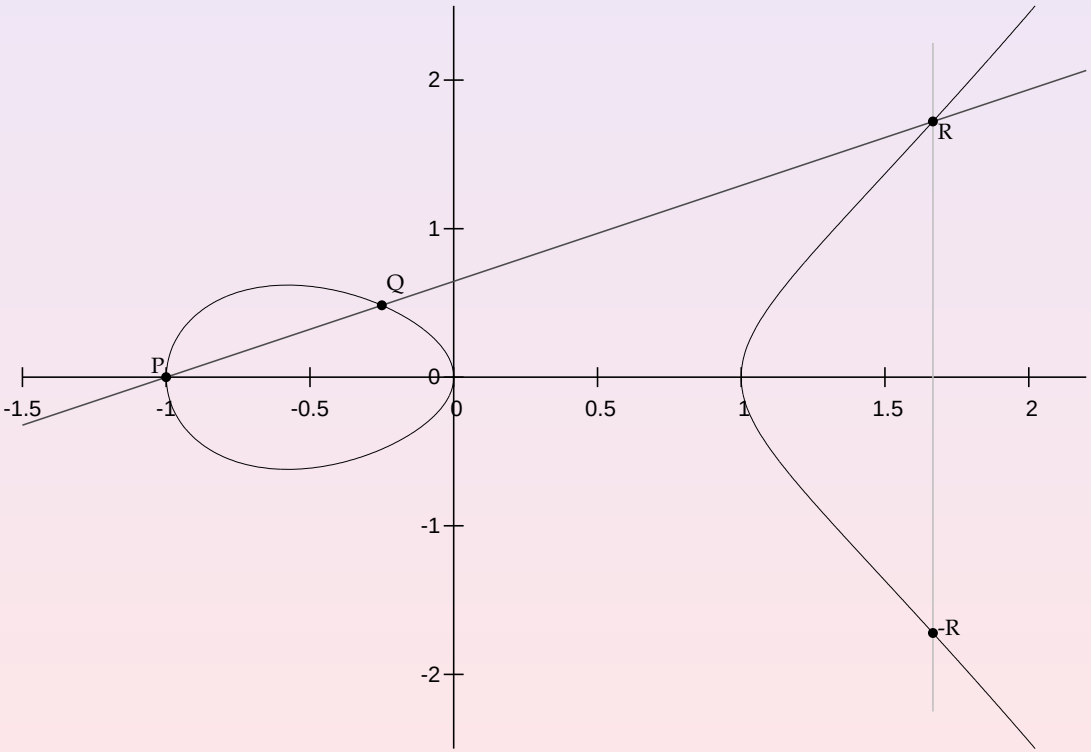
Pour retrouver la clé, Eve calcule $1/7 = 35 \mod 61$ *et retrouve* $17 = 58 \times 35 \mod 61$ ☹.

Les courbes elliptiques

Définition (char $k \neq 2, 3$)

Une courbe elliptique est une courbe plane d'équation

$$y^2 = x^3 + ax + b \qquad 4a^3 + 27b^2 \neq 0.$$



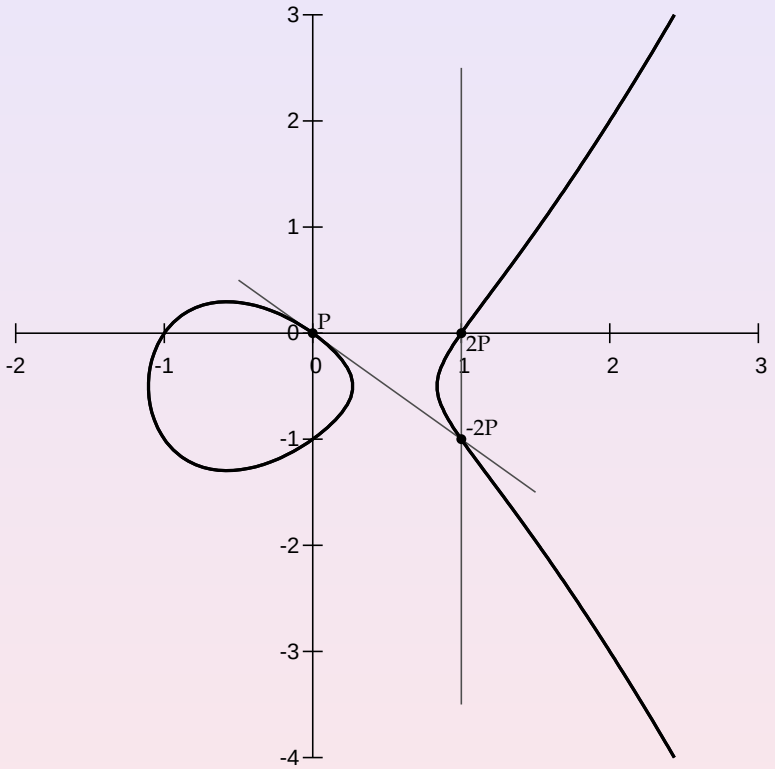
Exponentiation :

$$(\ell, P) \mapsto \ell P$$

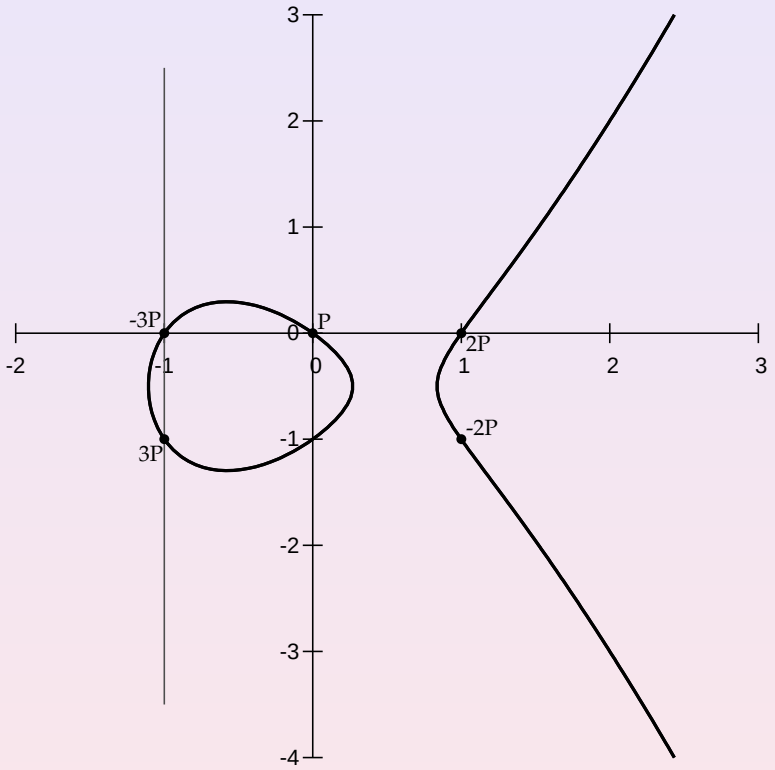
Logarithme discret :

$$(P, \ell P) \mapsto \ell$$

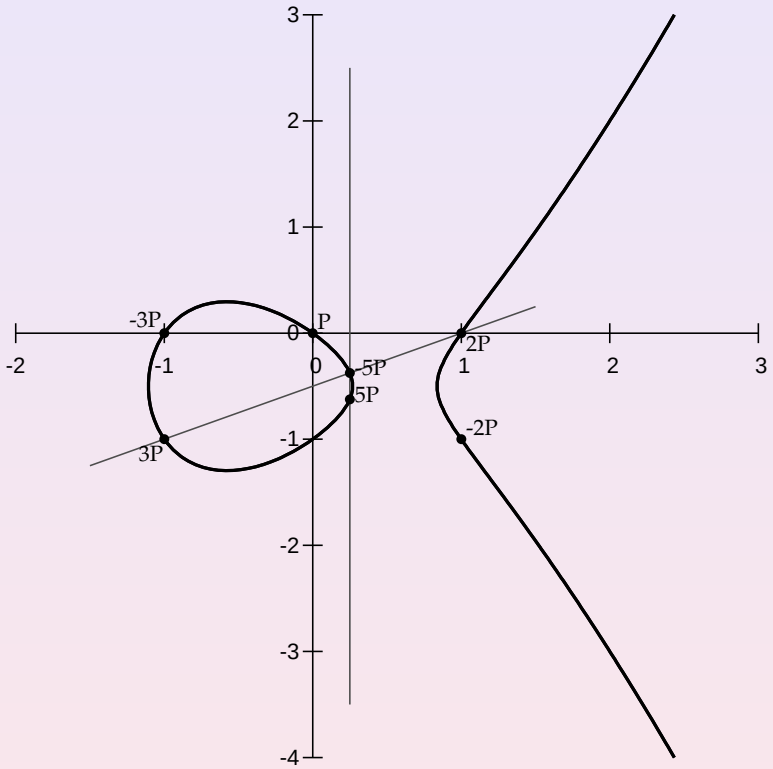
Exponentiation sur une courbe elliptique



Exponentiation sur une courbe elliptique



Exponentiation sur une courbe elliptique



Utilisation des courbes elliptiques

Exemple (ECC 160 bits)

- E courbe elliptique $y^2 = x^3 + x + 333$ sur $\mathbb{F}_{1461501637330902918203684832716283019655932542983}$
- Clé publique :

$$P = (1369962487580788774992199588498961558341362086296,$$
$$407160203592982096299905031630798490942043935021);$$
$$Q = (695697562436343265984113032286189105569389589 80,$$
$$1126203611660190221708449639677667925024412968395);$$

- Clé secrète : ℓ tel que $Q = \ell P$.

- Utilisées par la NSA ;
- Utilisées dans les passeports biométriques Européens.

Avantage des courbes elliptiques

À niveau de sécurité égale, les cryptosystèmes basés sur les courbes elliptiques, par rapport à RSA sont

- plus rapides ;
- plus compacts ;
- plus puissants.

Exemple (Couplages)

Sur une courbe elliptique, à partir d'une clé publique on peut générer d'autres clé publiques. De même pour la clé secrète.
$\Rightarrow$ Certificats anonymes.

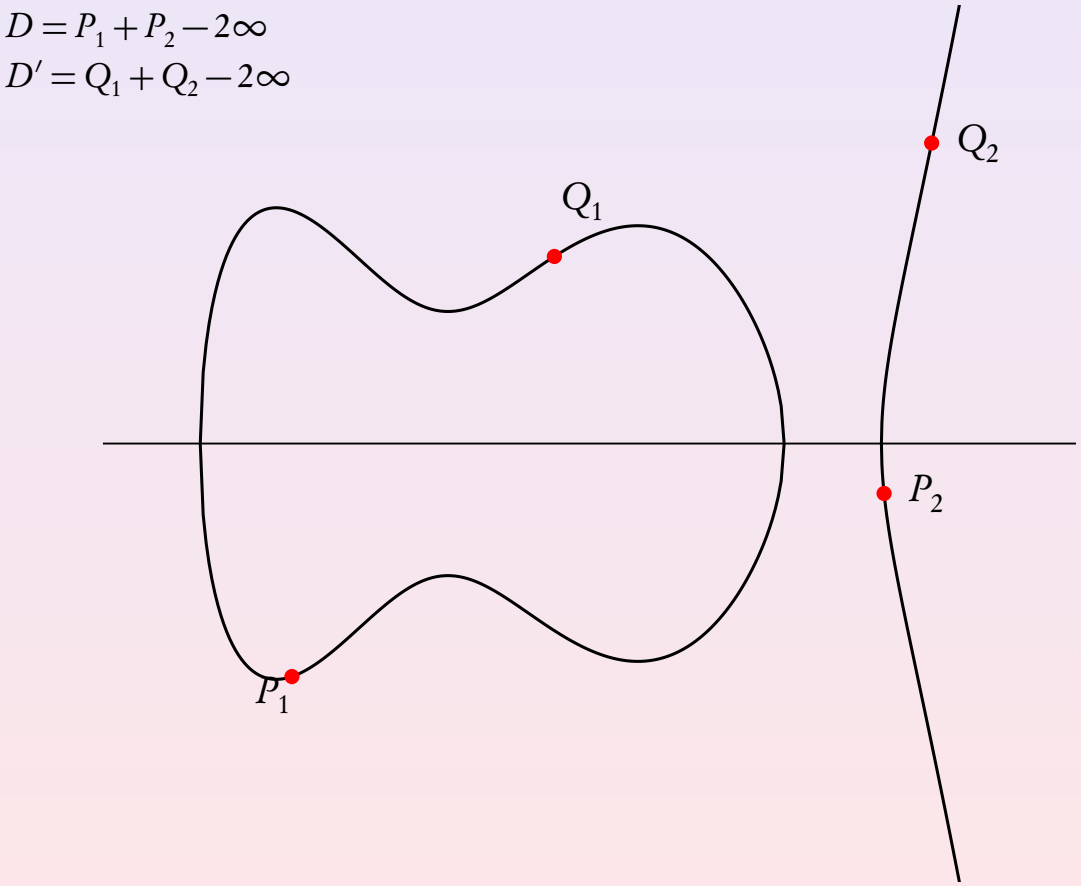
Exemple (Fonctions de hachage)

Les graphes d'isogénies de courbes elliptiques supersingulières fournissent des fonctions de hachage cryptographiquement sûres.

Dimension supérieure

Dimension 2 : Loi d'addition sur la Jacobienne d'une courbe hyperelliptique de genre 2 :

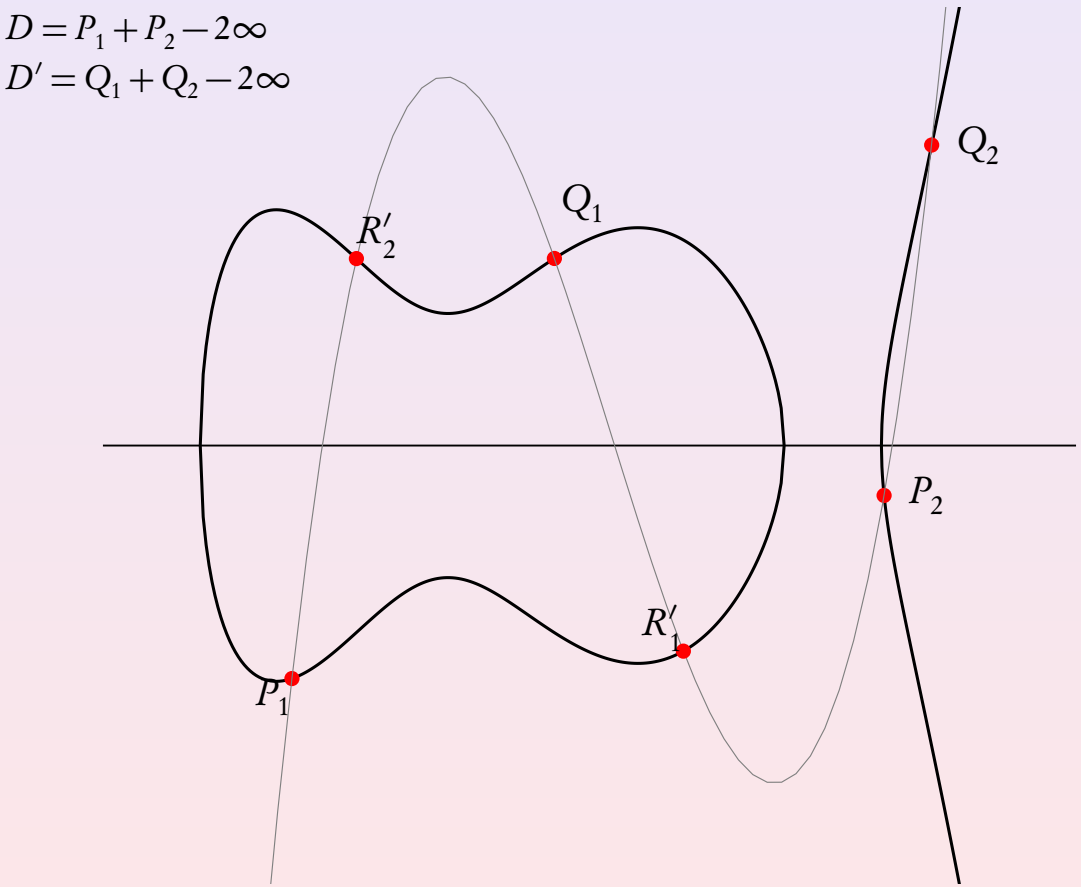
$$y^2 = f(x), \deg f = 5.$$



Dimension supérieure

Dimension 2 : Loi d'addition sur la Jacobienne d'une courbe hyperelliptique de genre 2 :

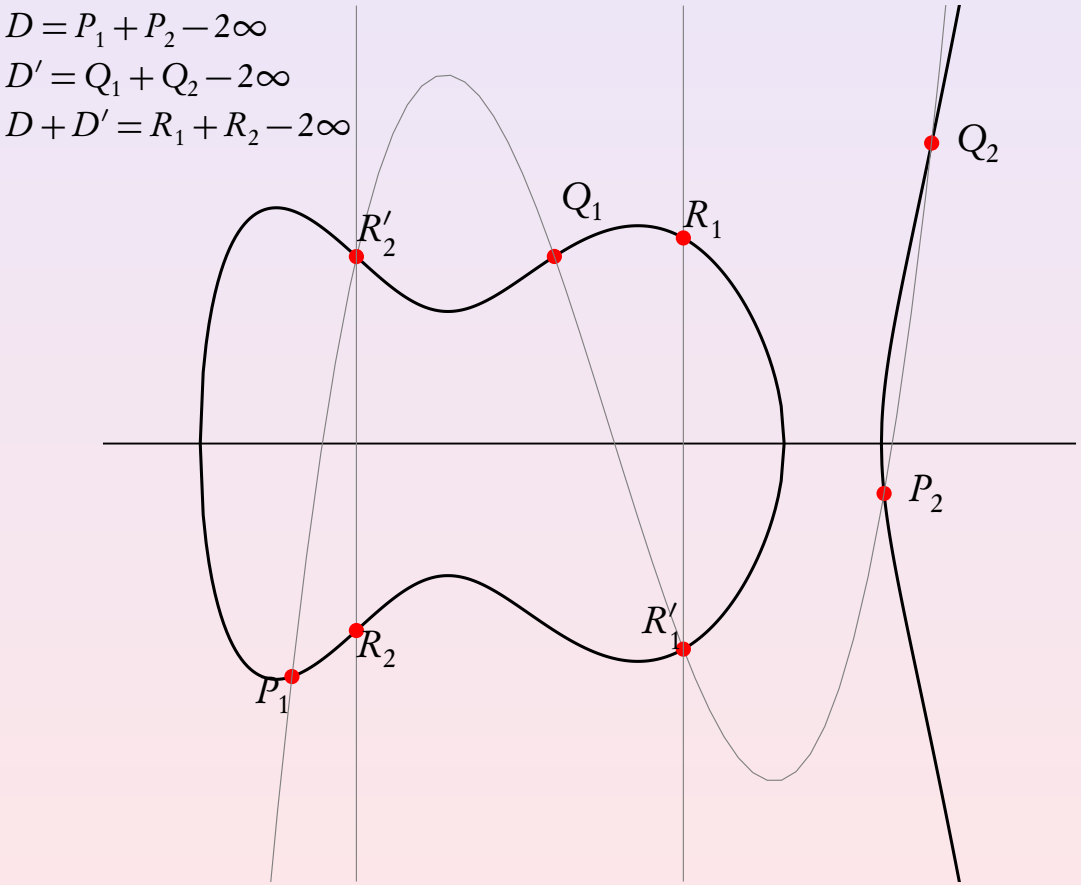
$$y^2 = f(x), \deg f = 5.$$



Dimension supérieure

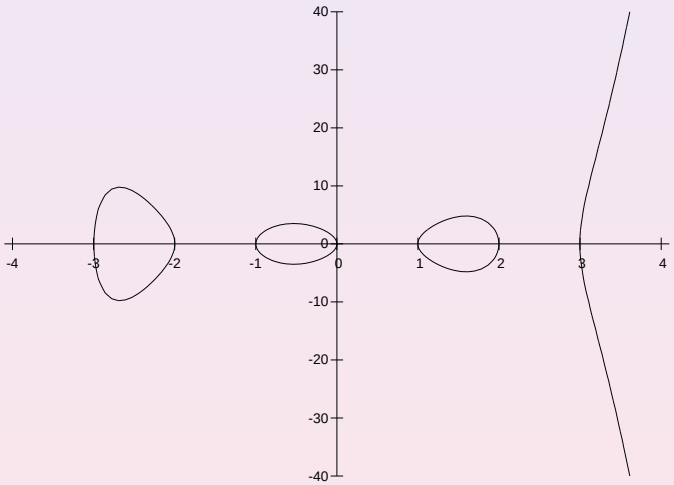
Dimension 2 : Loi d'addition sur la Jacobienne d'une courbe hyperelliptique de genre 2 :

$$y^2 = f(x), \deg f = 5.$$

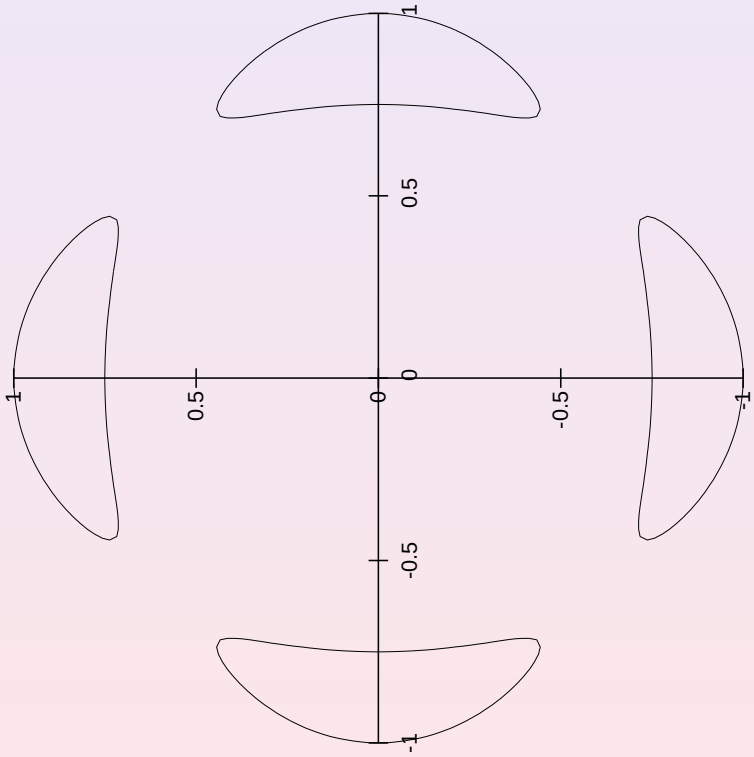


Dimension 3

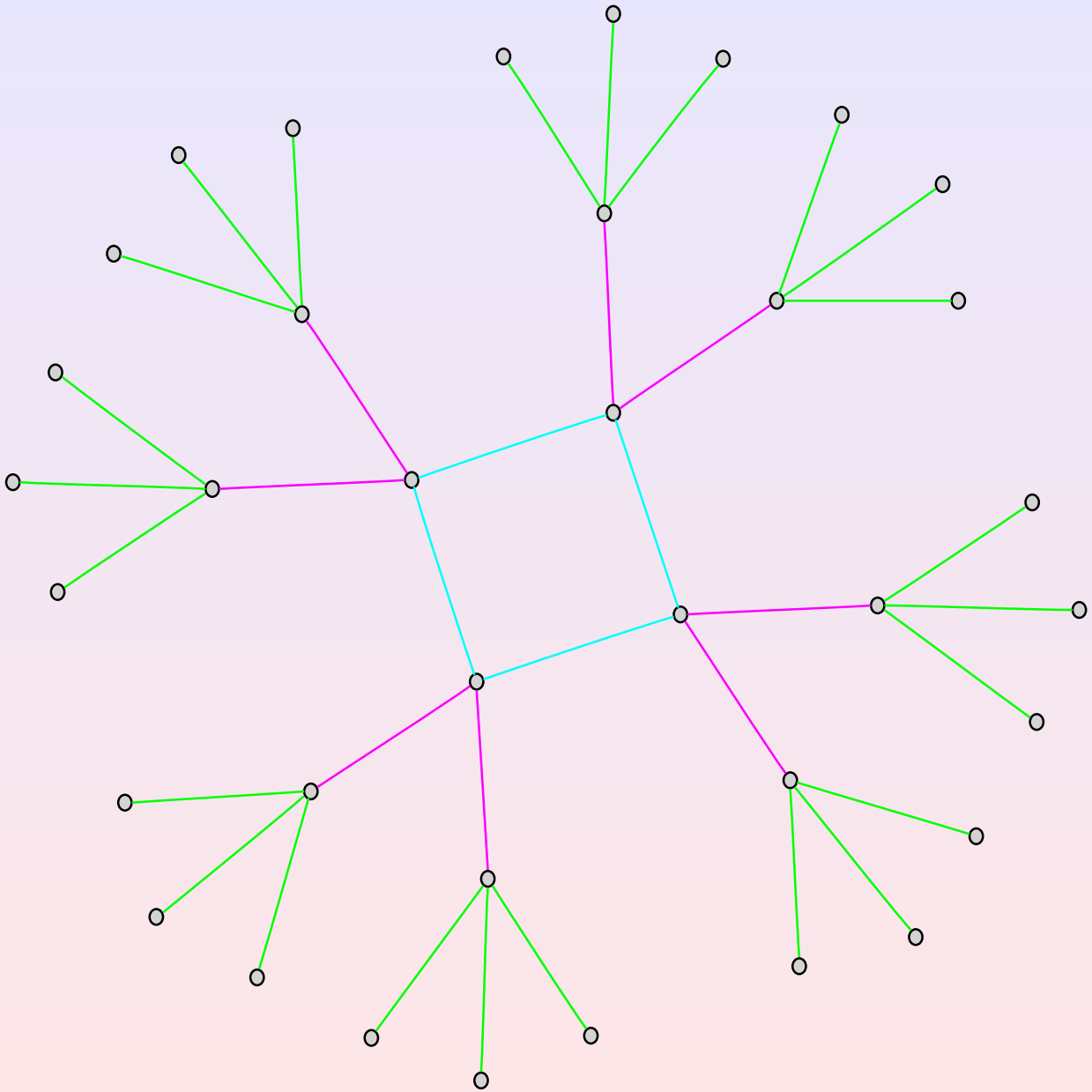
Jacobiennes de courbes hyperelliptiques de genre 3.



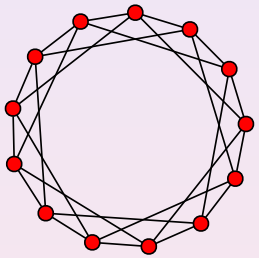
Jacobiennes de quartiques.

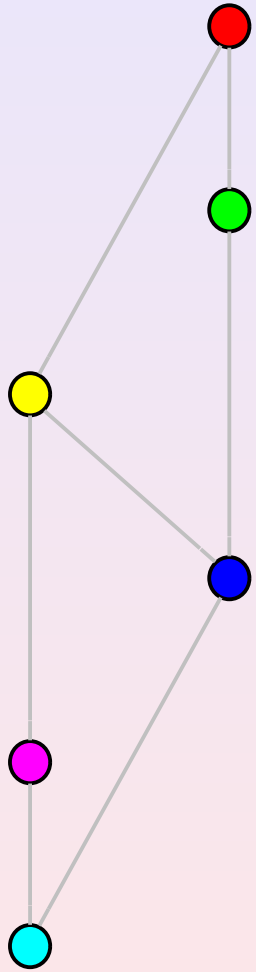


Graphe d'isogénies sur les courbes elliptiques

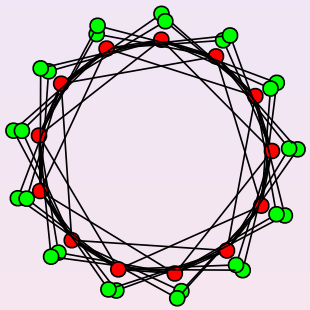


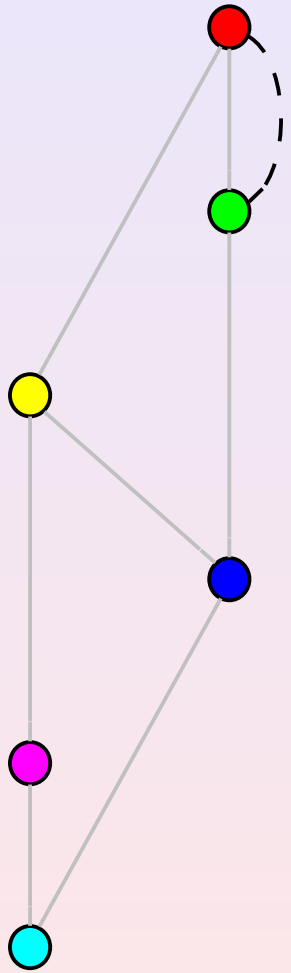
Graphe d'isogénies en dimension 2



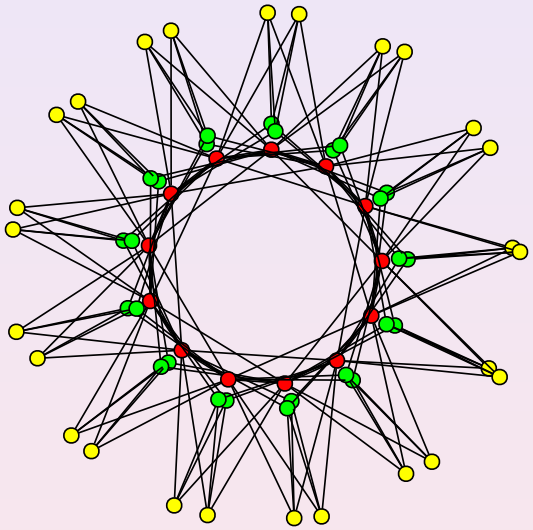


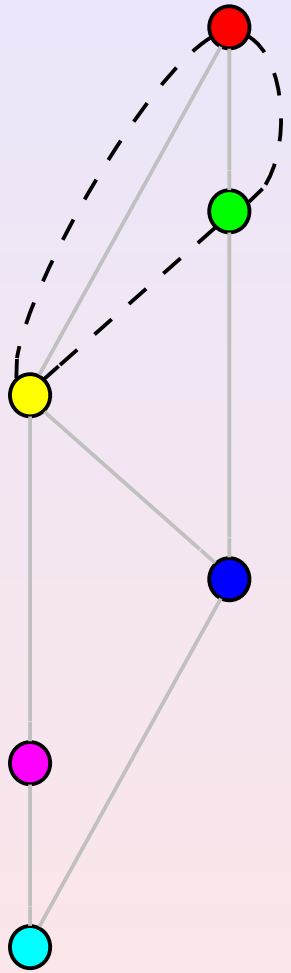
Graphe d'isogénies en dimension 2



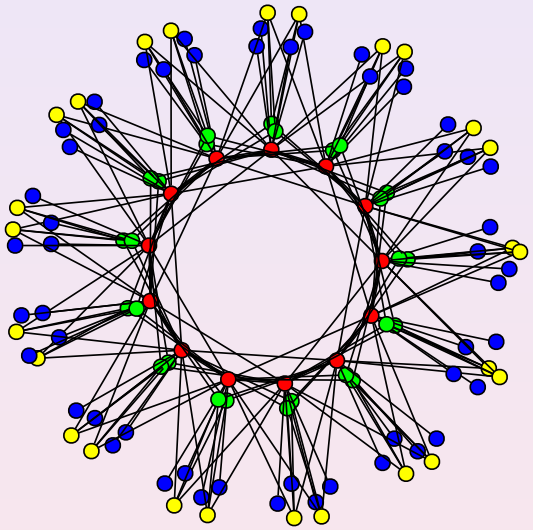


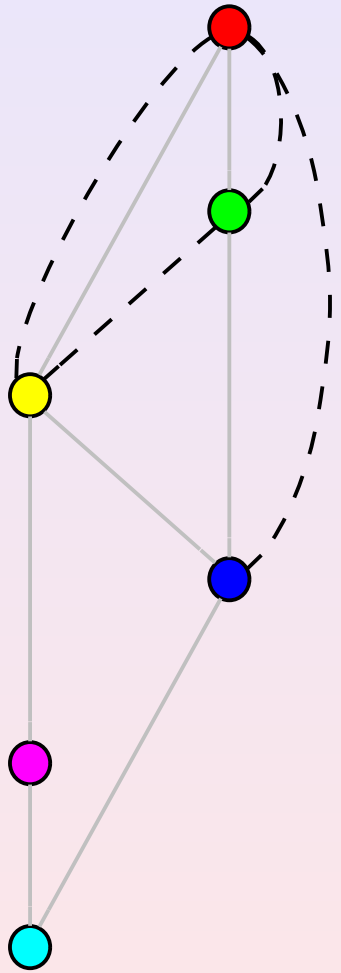
Graphe d'isogénies en dimension 2



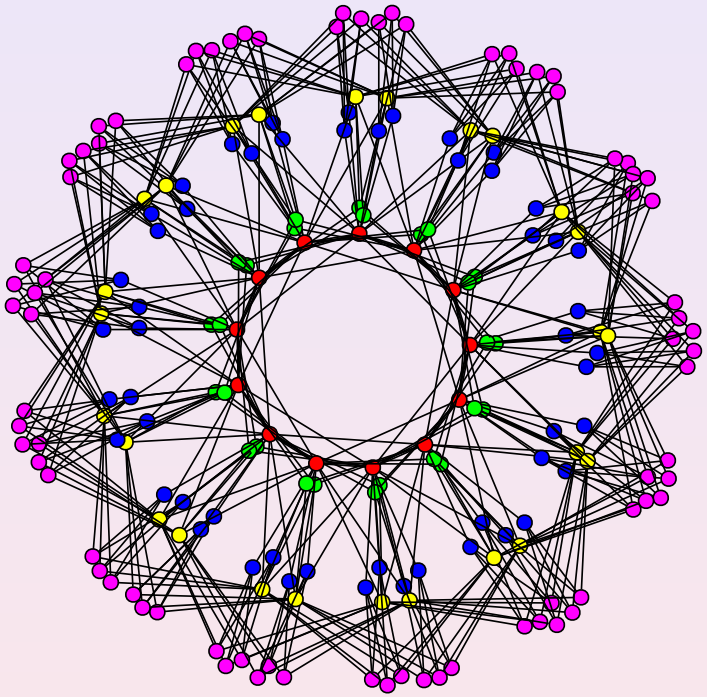


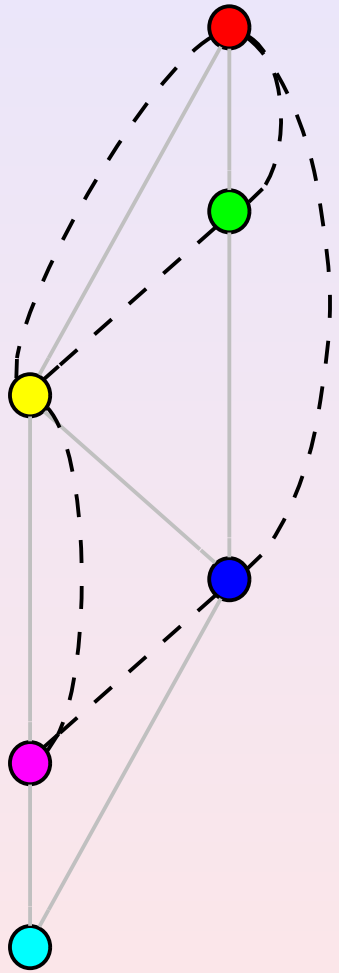
Graphe d'isogénies en dimension 2



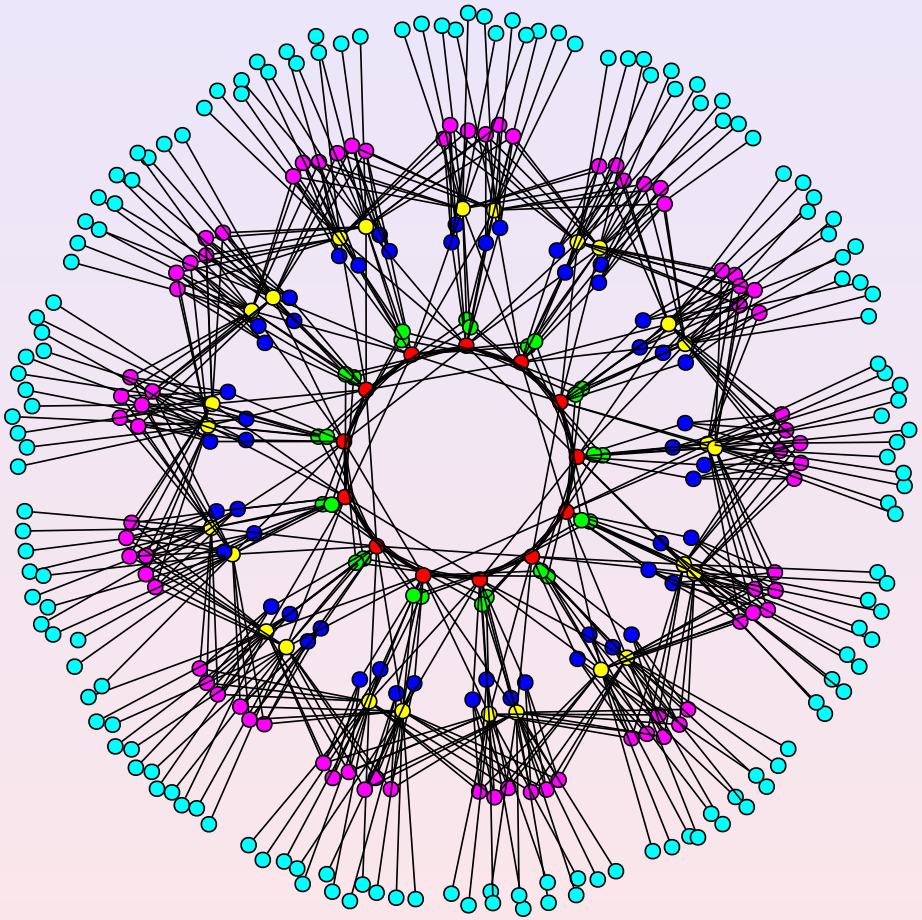


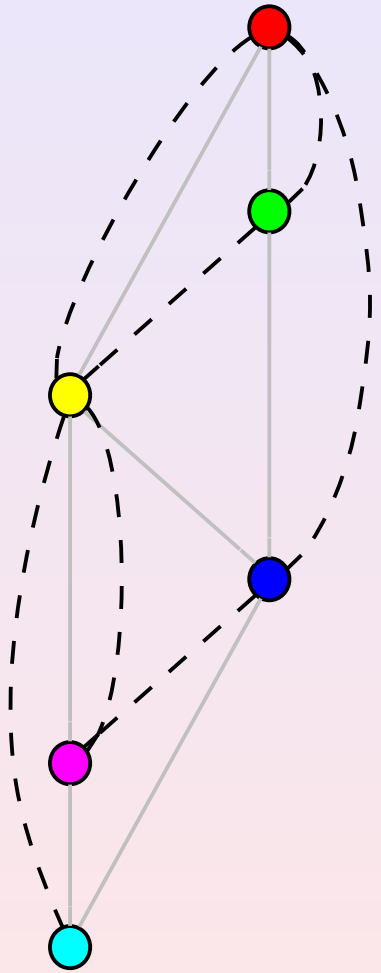
Graphe d'isogénies en dimension 2





Graphe d'isogénies en dimension 2





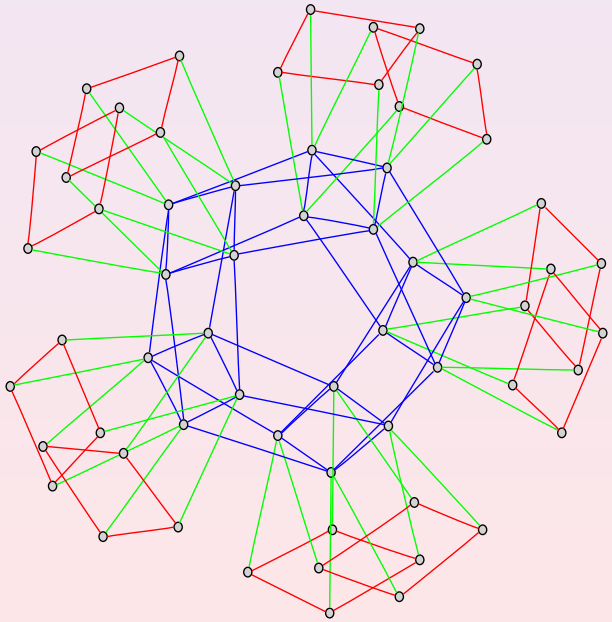
L'essor du cloud computing

- Chiffrement homomorphe : l'utilisateur fournit au nuage un message chiffré $f_K(m)$ et un programme P, et le nuage renvoie $f_K(P(m))$.
  Le nuage n'a rien appris sur la donnée m, ni sur le résultat !
- L'utilisateur fournit au nuage un message chiffré $f_K(m)$ et le chiffrement $f_K(P)$ d'un programme P, et le nuage renvoie $f_K(P(m))$.
  Le nuage ne sait pas ce qu'il a calculé !

$\Rightarrow$ Une version faible utilise les couplages de courbes elliptiques ;

$\Rightarrow$ La version complète utilise des réseaux, en particulier des réseaux d'idéaux dans des corps de nombres ;

☹ Encore très lent.

Quelques secteurs

- développement des cartes à puces
- commerce électronique
- téléphonie mobile
- armement
- intérieur
- sécurité des logiciels
- sécurité des réseaux