

Quand l'ajout de structure casse un cryptosystème : quelques exemples de cryptanalyse

2024/08/29 — Journées Scientifiques Inria, Grenoble

Damien Robert

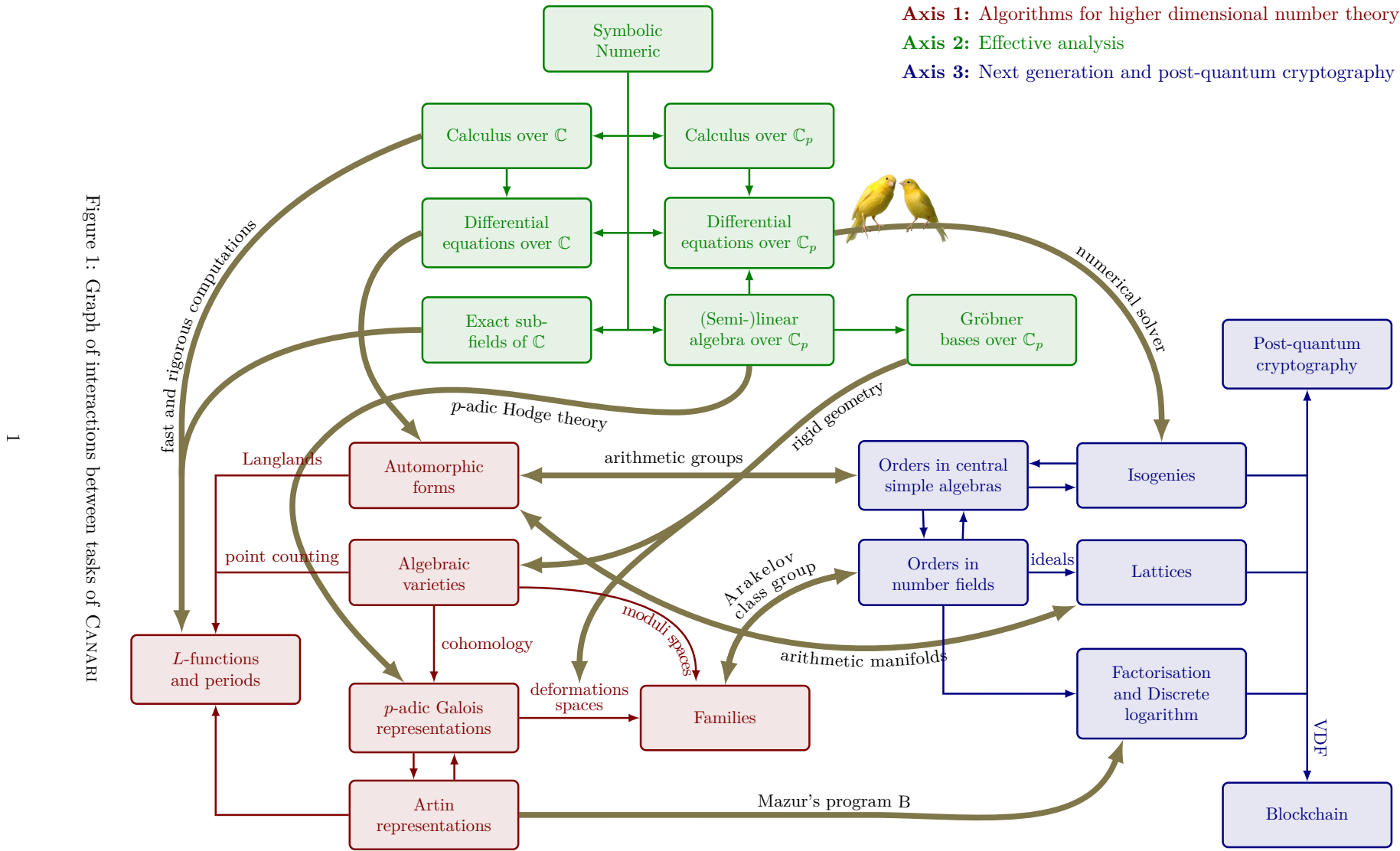
Équipe Canari, Inria Bordeaux Sud-Ouest



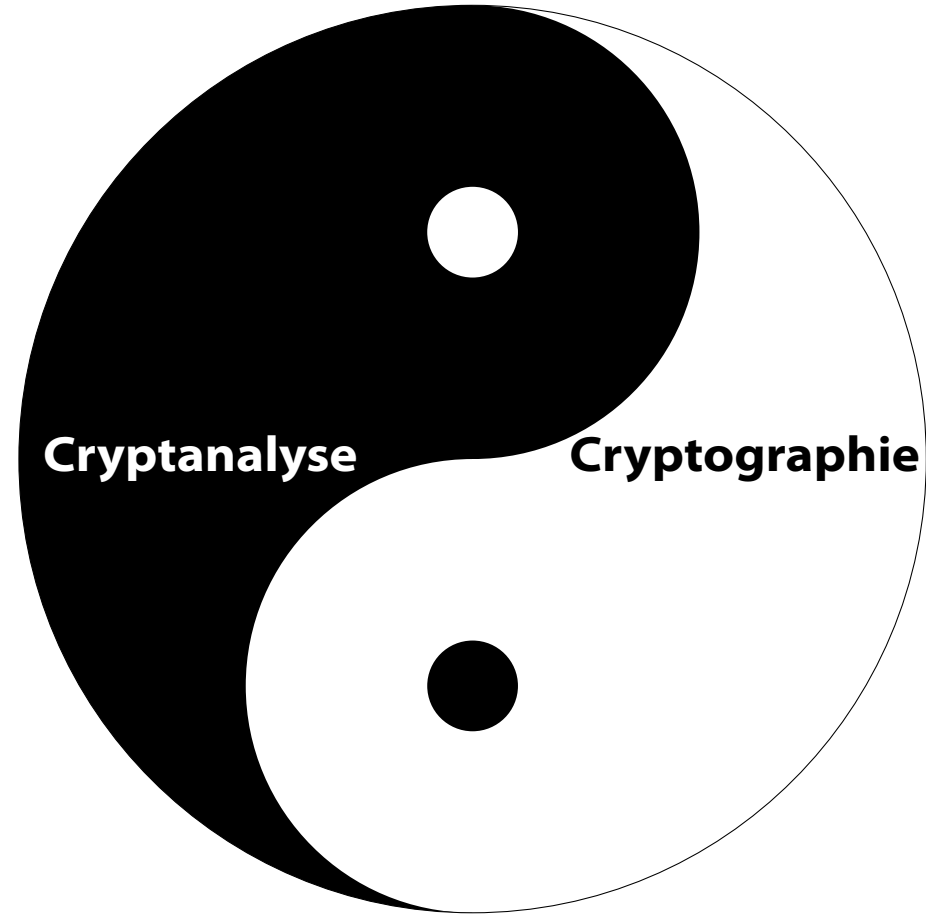
université
de BORDEAUX

Inria

Canari = Cryptography ANalysis and ARithmetic



Cryptologie = Cryptographie + Cryptanalyse



- **Cryptographie** : conception de systèmes cryptographiques
Chiffrement, signatures, chiffrement homomorphe, fonctionnel, preuves sans divulgation de connaissances, vote électronique, blockchains...
- **Cryptanalyse** : attaques contre ces cryptosystèmes
- Permet de choisir les paramètres optimaux préservant la sécurité

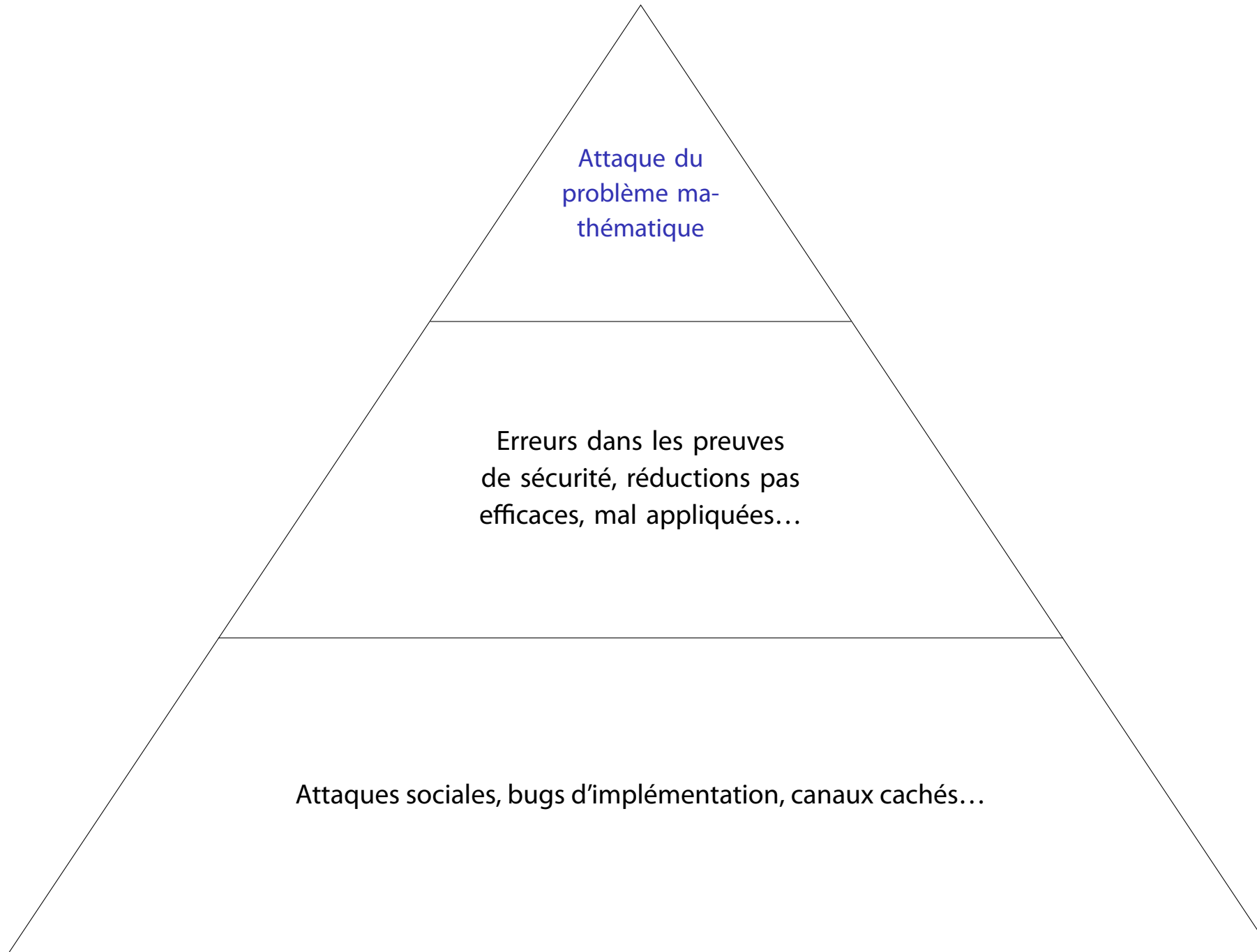
Cryptanalyse ?

- Dans un monde idéal : cryptosystème **compact**, **efficace**, et **prouvé sûr**
- Nécessite des **bornes mins** sur les attaques possibles...
- $P \neq NP$? **Pire cas vs cas moyens**...
Les **5 mondes** d'Impagliazzo : Algorithmica, Heuristica, Pessiland, Minicrypt, Cryptomania
- Identification de **problèmes mathématiques** bien définis (factorisation, logarithme discret, ...) **supposés** difficiles
- Construction de **cryptosystèmes** reposant sur ces problèmes avec **preuve de sécurité**
- **Casser** le cryptosystème $\Rightarrow$ **résoudre** le problème mathématique
- Changement du modèle d'attaque : **pré-quantique** $\rightarrow$ **post-quantique**

Cryptanalyse ?

- Dans un monde idéal : cryptosystème **compact**, **efficace**, et **prouvé sûr**
- Nécessite des **bornes mins** sur les attaques possibles...
- $P \neq NP$? **Pire cas vs cas moyens**...
Les **5 mondes** d'Impagliazzo : Algorithmica, Heuristica, Pessiland, Minicrypt, Cryptomania
- Identification de **problèmes mathématiques** bien définis (factorisation, logarithme discret, ...) **supposés** difficiles
- Construction de **cryptosystèmes** reposant sur ces problèmes avec **preuve de sécurité**
- **Casser** le cryptosystème $\Rightarrow$ **résoudre** le problème mathématique
- Changement du modèle d'attaque : **pré-quantique** $\rightarrow$ **post-quantique**

La pyramide de la cryptanalyse



Rajout de structure dans un cryptosystème

- Situation typique : cryptosystème **sûr** (conjecturalement!), mais **peu efficace**
- Ajout de **structure** pour le rendre efficace
- On **espère** que ça ne nuit pas à sa **sécurité**...

Exemple (Équations quadratiques multivariées)

- Résoudre des **équations quadratiques multivariées** est **difficile** (NP-complet)
- Ajout d'équations linéaires cachées (**trapdoor**) $\Rightarrow$ cryptosystème **uOV** (unbalanced Oil and Vinegar) [Patarin 1997]
- **Rainbow** [Ding-Schmidt 2005] : imbrication d'équations linéaires
« A scheme with more **efficient computations** and **smaller key sizes** at the same level of security » (Rainbow specification document)
- [Beullens 2022] : « **Breaking Rainbow** Takes a Weekend on a Laptop »
- [MAYO 2023] : « MAYO is a variant of the Oil and Vinegar scheme whose public keys are **smaller** »

Rajout de structure dans un cryptosystème

- Situation typique : cryptosystème **sûr** (conjecturalement!), mais **peu efficace**
- Ajout de **structure** pour le rendre efficace
- On **espère** que ça ne nuit pas à sa **sécurité**...

Exemple (Équations quadratiques multivariées)

- Résoudre des **équations quadratiques multivariées** est **difficile** (NP-complet)
- Ajout d'équations linéaires cachées (**trapdoor**) $\Rightarrow$ cryptosystème **uOV** (unbalanced Oil and Vinegar) [Patarin 1997]
- **Rainbow** [Ding-Schmidt 2005] : imbrication d'équations linéaires
« A scheme with more **efficient computations** and **smaller key sizes** at the same level of security » (Rainbow specification document)
- [Beullens 2022] : « **Breaking Rainbow** Takes a Weekend on a Laptop »
- [MAYO 2023] : « MAYO is a variant of the Oil and Vinegar scheme whose public keys are **smaller** »

Exemple 2 : cryptographie à base de code

- Un **code correcteur d'erreur** permet de corriger des erreurs de transmission
- Modélisé par une **matrice** M de taille $n \times k$ sur $\mathbb{F}_2$
- ☺ Le problème du décodage d'un code aléatoire est **NP-dur**

- [McEliece 1978] : **cache** un **code structuré** G par des opérations linéaires $G' = PGS$
- **Paramètres** : $n=6960, k=5413 \Rightarrow 4.7$ MO
- Beaucoup (la plupart ?) des versions suggérées pour **réduire la taille** des paramètres ont été **cassées** :
GRS, Reed-Muller, LDPC, MDPC, ...

- [Randriambololona, Juillet 2024] : « The syzygy distinguisher »

Exemple 3 : cryptographie à base de réseaux (lattices)

- Réseau = matrice à coefficients entier (en pratique modulo un nombre premier)
- ☺ Trouver un petit vecteur dans un réseau aléatoire = NP-dur
- Comment réduire la taille des matrices ?

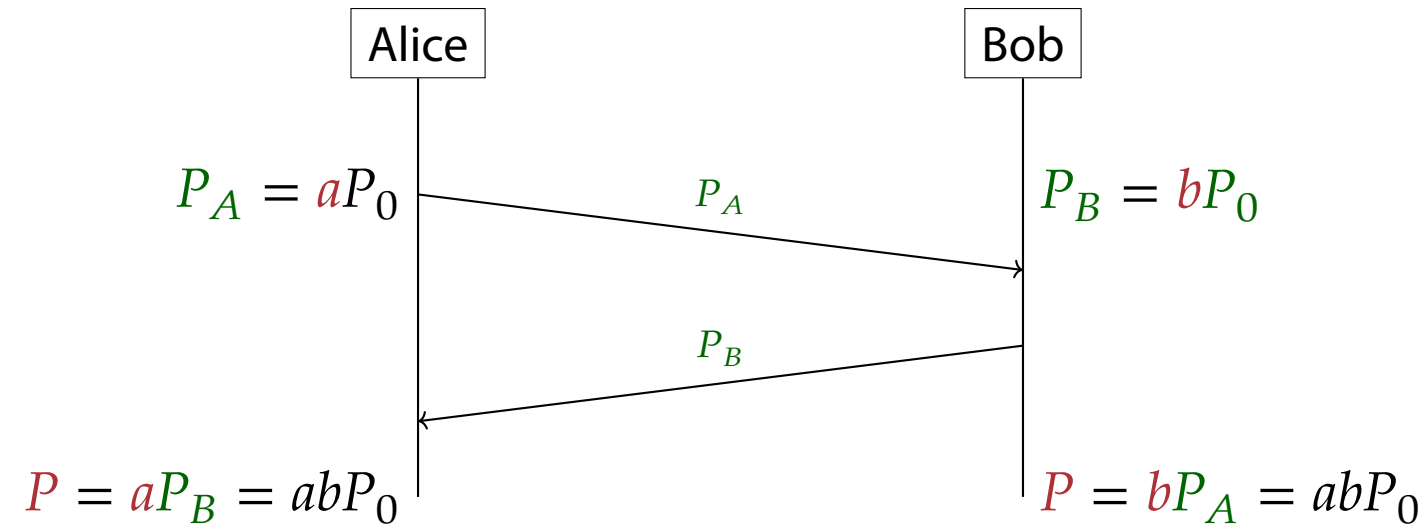
Exemple (Matrice « cyclique »)

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ -a_3 & a_0 & a_1 & a_2 \\ -a_2 & -a_3 & a_0 & a_1 \\ -a_1 & -a_2 & -a_3 & a_0 \end{pmatrix}$$

- Anneau $\mathbb{Z}[X]/(X^{2^n} + 1)$ (ordre cyclotomique)
- Pas d'attaque connue exploitant cette structure (pour l'instant)!
- Des anneaux de forme $R = \mathbb{Z}[X]/(X^n + aX + b)$ vulnérables pour certains a, b spécifiques
Dépend si le conditionnement du bruit est fait sur R ou $R^\vee$.

Échange de clé de Diffie-Hellman

$G = \langle P_0 \rangle$ groupe commutatif



☺ Réductions (partielles) entre casser le protocole d'échange de Diffie-Hellman et casser le problème du **logarithme discret** :

$$(P_0, aP_0) \mapsto a$$

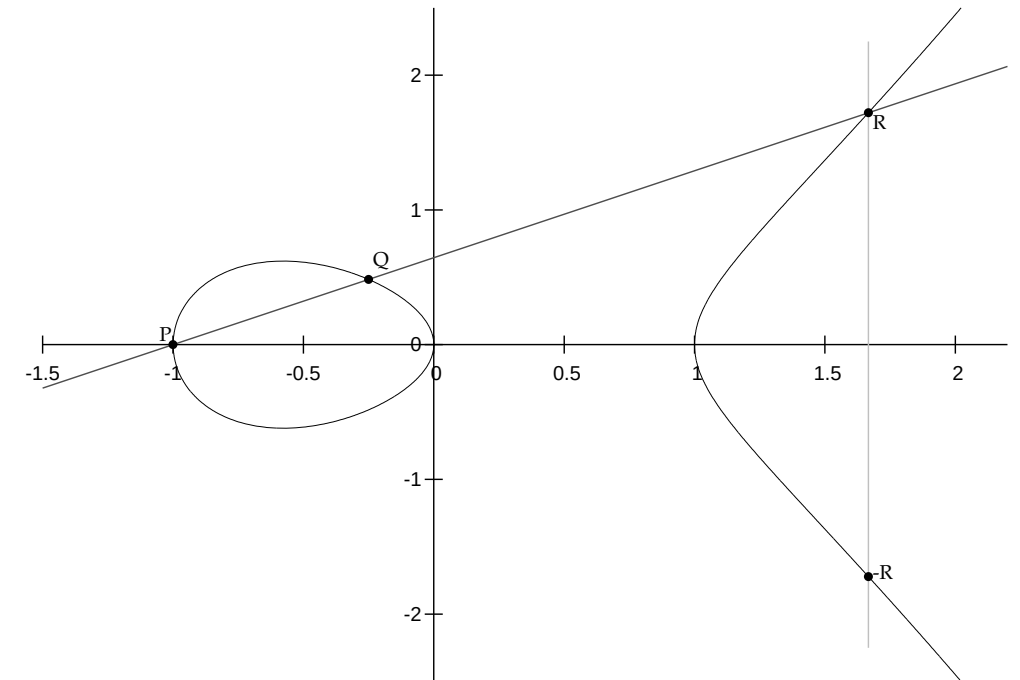
☺ Le logarithme discret dans un **groupe générique** G de cardinal ℓ premier coûte au moins $\sqrt{\ell}$ [Shoup 1997]

☹ Il est **impossible** de calculer efficacement dans un « **groupe générique** »

Échange de clé de Diffie-Hellman

- [Diffie-Hellman 1976] : $G = (\mathbb{F}_p^*, \times)$ groupe multiplicatif d'un corps fini.
- ☹️ Attaques sous-exponentielles en $\approx 2^{\log^{1/3} p}$ reposant sur la factorisation des nombres entiers (nombres friables)

- [Koblitz, Miller 1985] $G = E/\mathbb{F}_q$ courbe elliptique
- 😊 La meilleure attaque connue est l'attaque « générique »
En enlevant un petit nombre de courbes elliptiques « rares » : E ne doit pas être anormale, avoir un petit « degré de plongement », ...
- [Koblitz 2000] : « Miracles of the Height Function - A Golden Shield Protecting ECC »



- ☹️ [Shor 1994] : algorithme quantique cassant la factorisation et le logarithme discret

Échange de clé de Diffie-Hellman

- [Diffie-Hellman 1976] : $G = (\mathbb{F}_p^*, \times)$ groupe multiplicatif d'un corps fini.

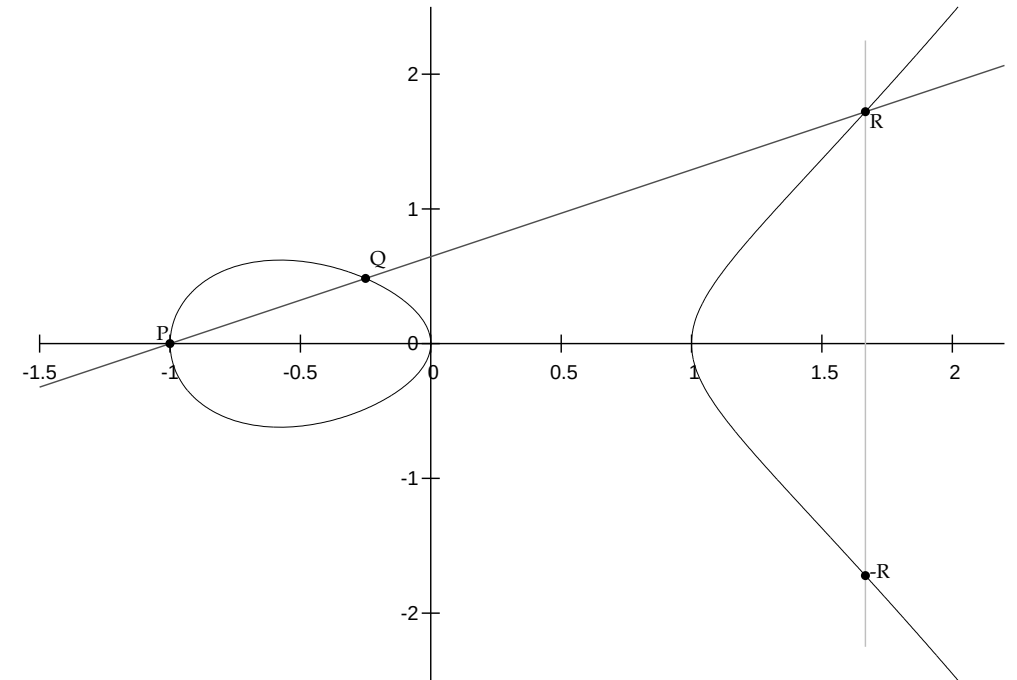
☹️ Attaques sous-exponentielles en $\approx 2^{\log^{1/3} p}$ reposant sur la factorisation des nombres entiers (nombres friables)

- [Koblitz, Miller 1985] $G = E/\mathbb{F}_q$ courbe elliptique

😊 La meilleure attaque connue est l'attaque « générique »

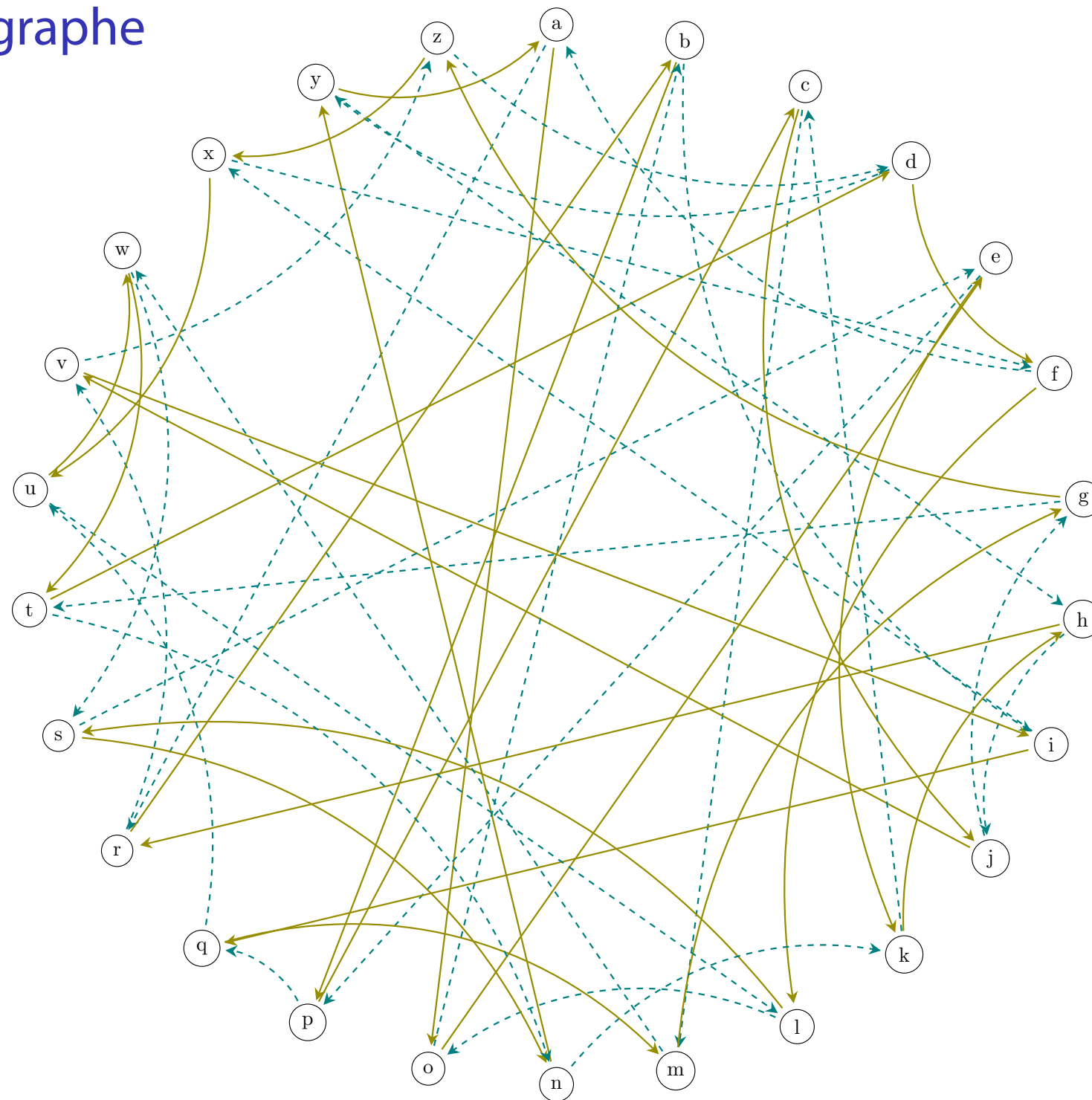
En enlevant un petit nombre de courbes elliptiques « rares » : E ne doit pas être anormale, avoir un petit « degré de plongement », ...

- [Koblitz 2000] : « Miracles of the Height Function - A Golden Shield Protecting ECC »



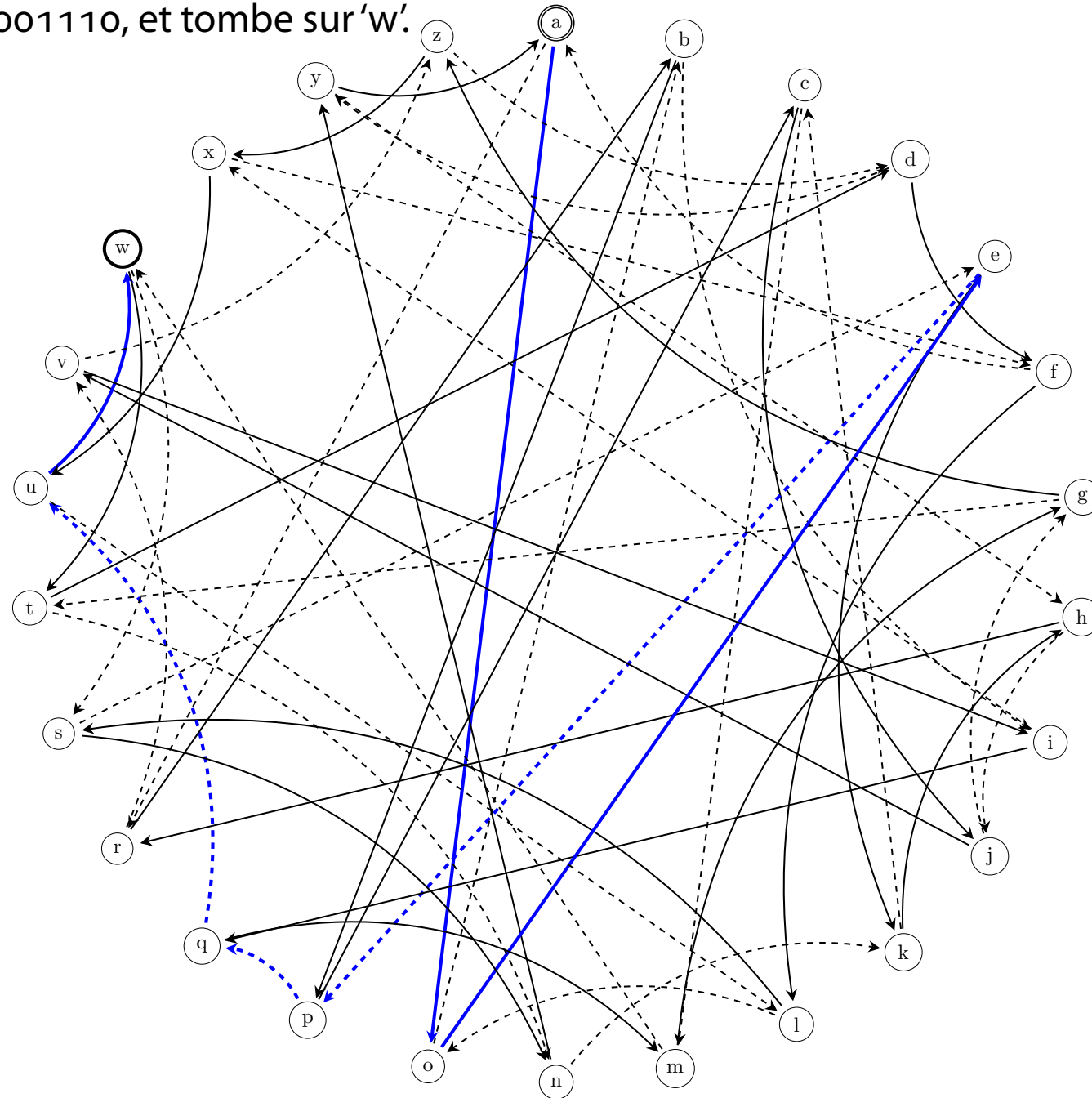
☹️ [Shor 1994] : algorithme quantique cassant la factorisation et le logarithme discret

Échange de clé par graphe



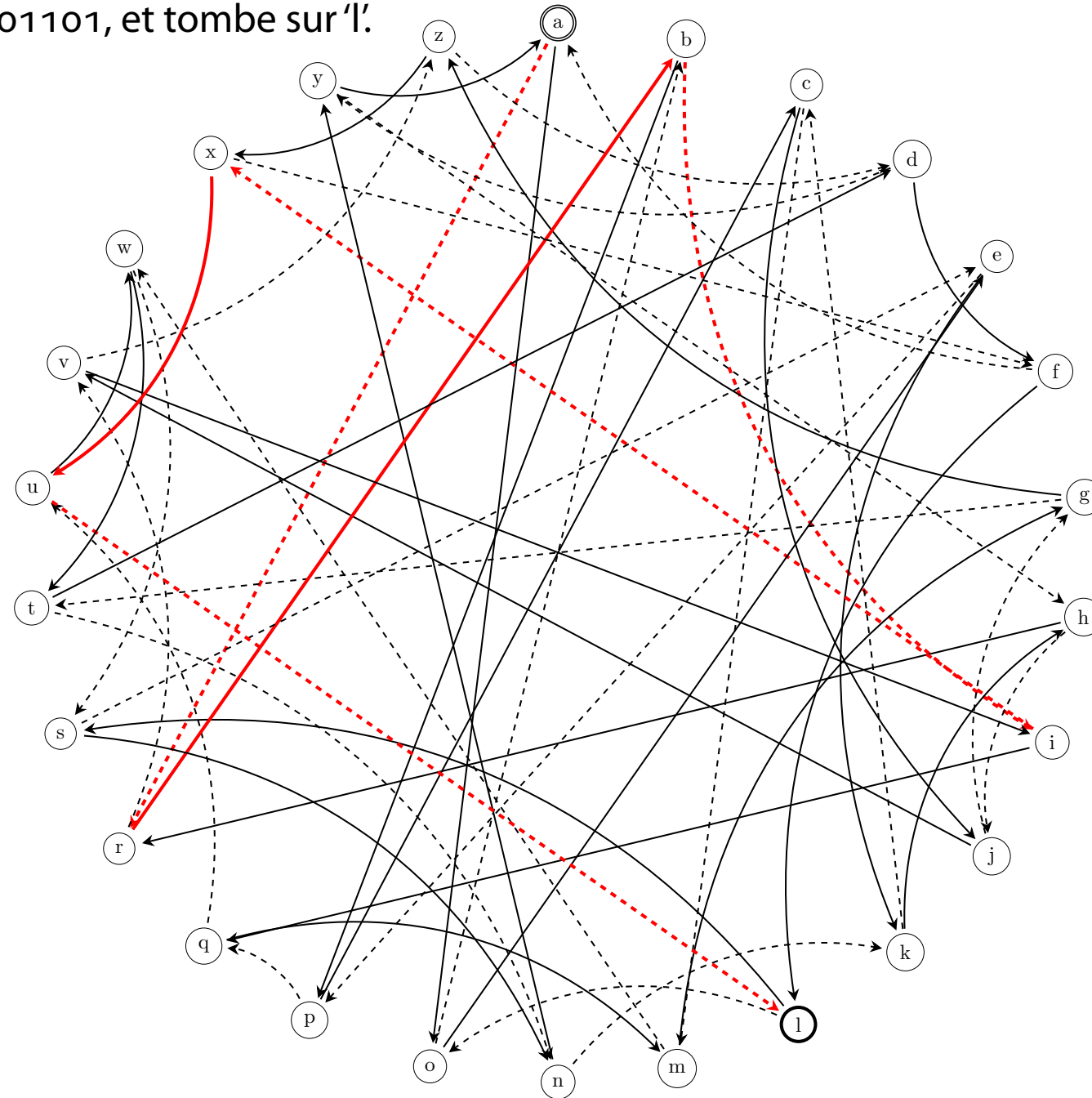
Échange de clé par graphe

Alice part de 'a', suit le chemin 001110, et tombe sur 'w'.



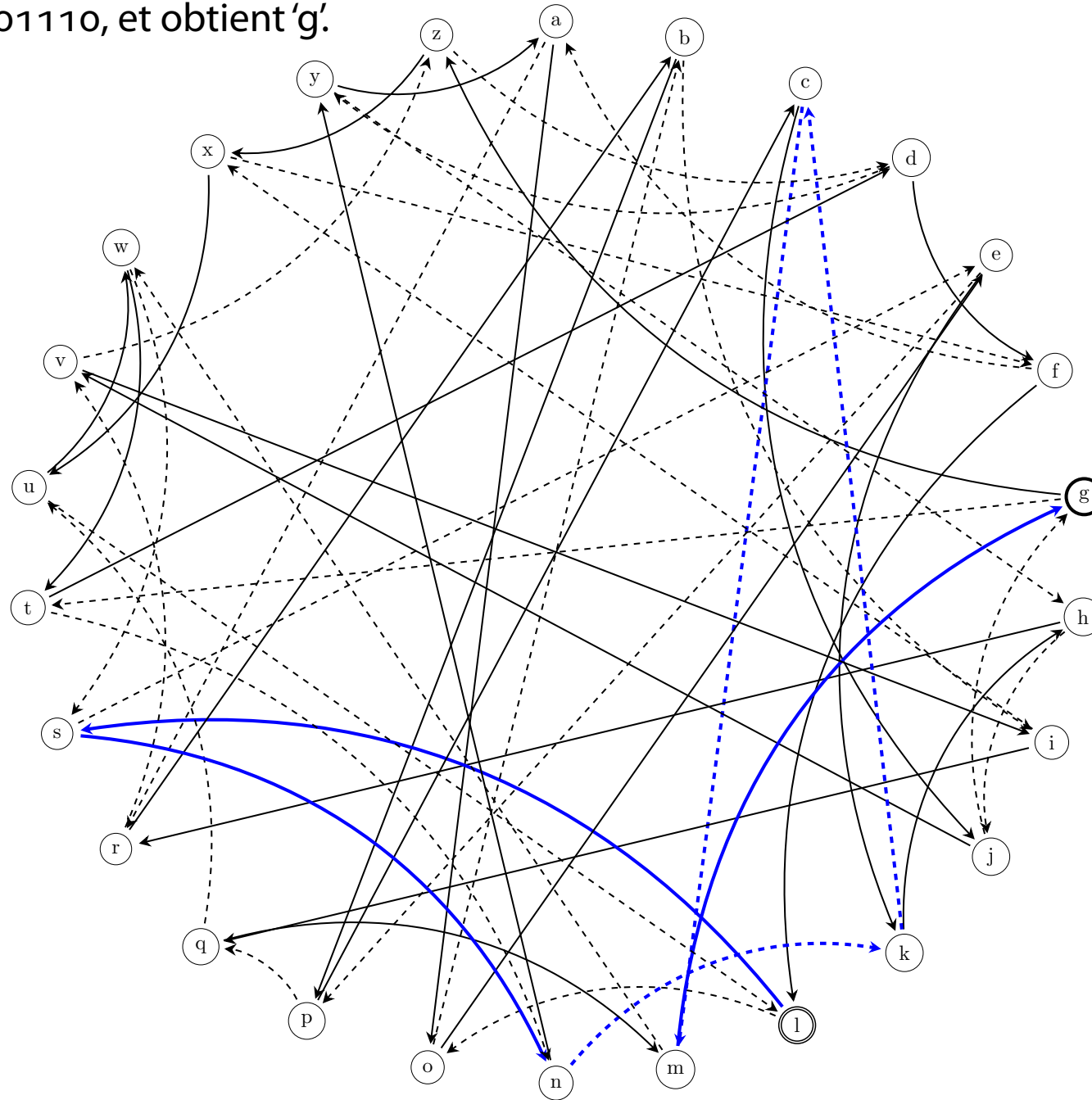
Échange de clé par graphe

Bob part de 'a', suit le chemin 101101, et tombe sur 'l'.



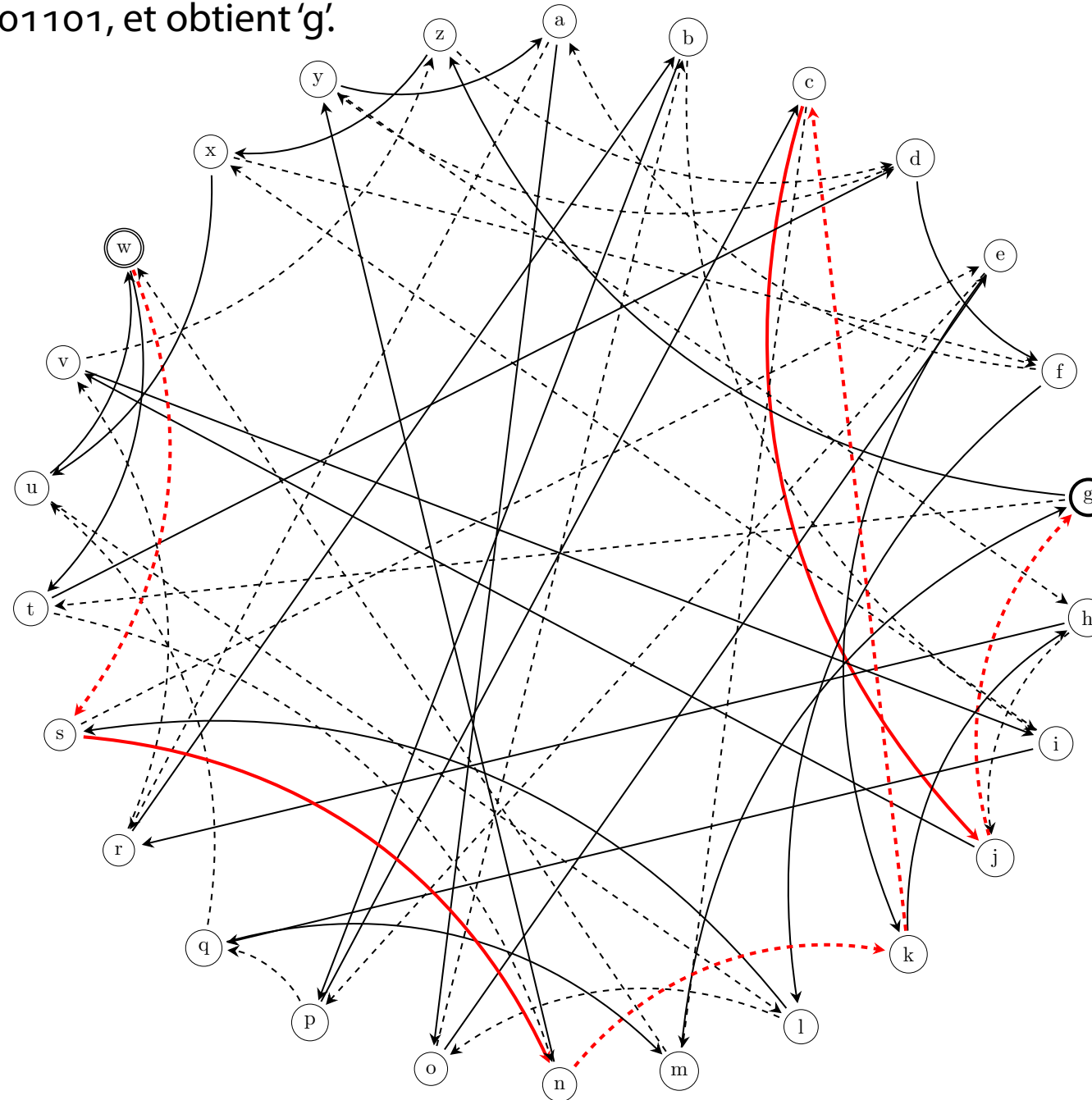
Échange de clé par graphe

Alice part de 'l', suit le chemin 001110, et obtient 'g'.



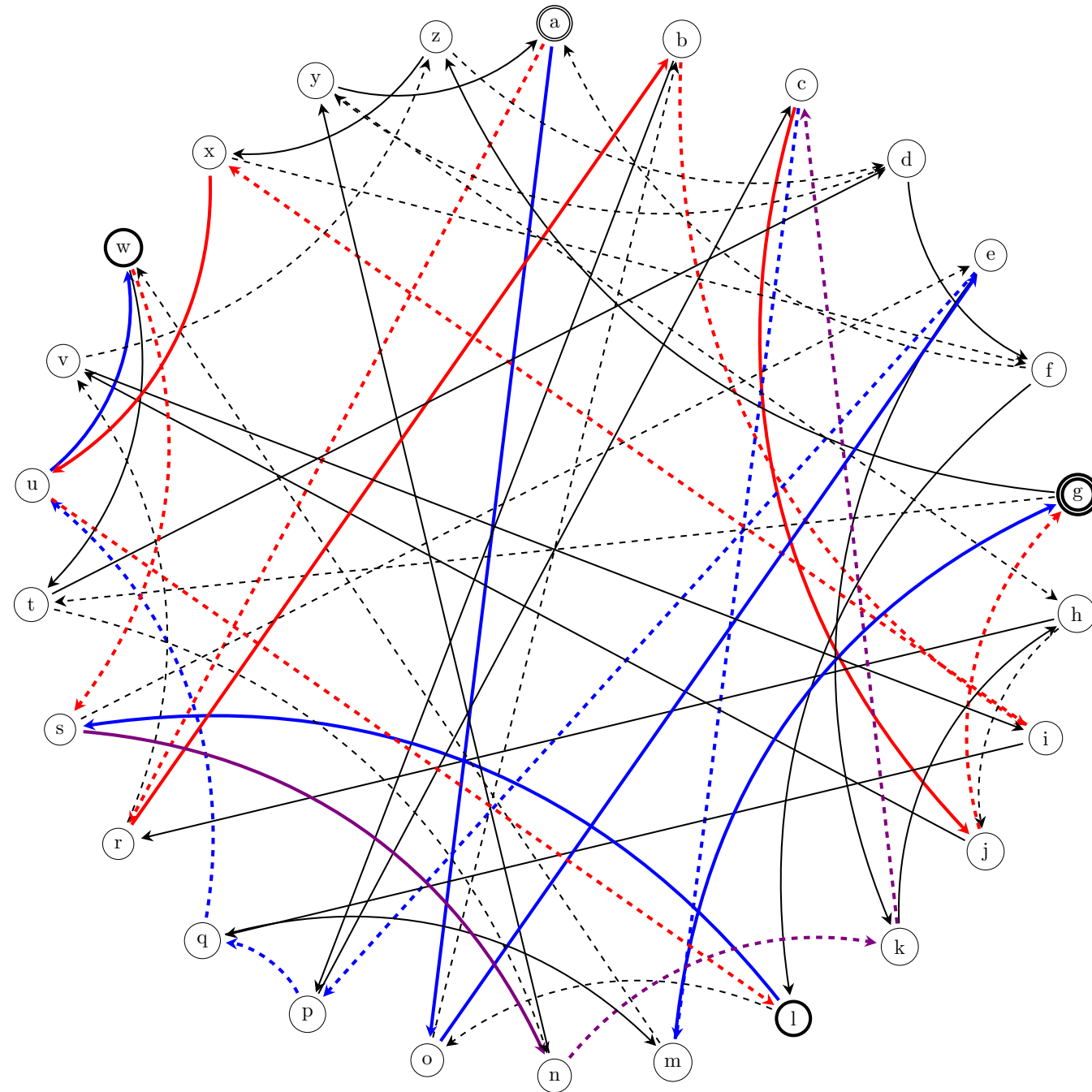
Échange de clé par graphe

Bob part de 'w', suit le chemin 101101, et obtient 'g'.



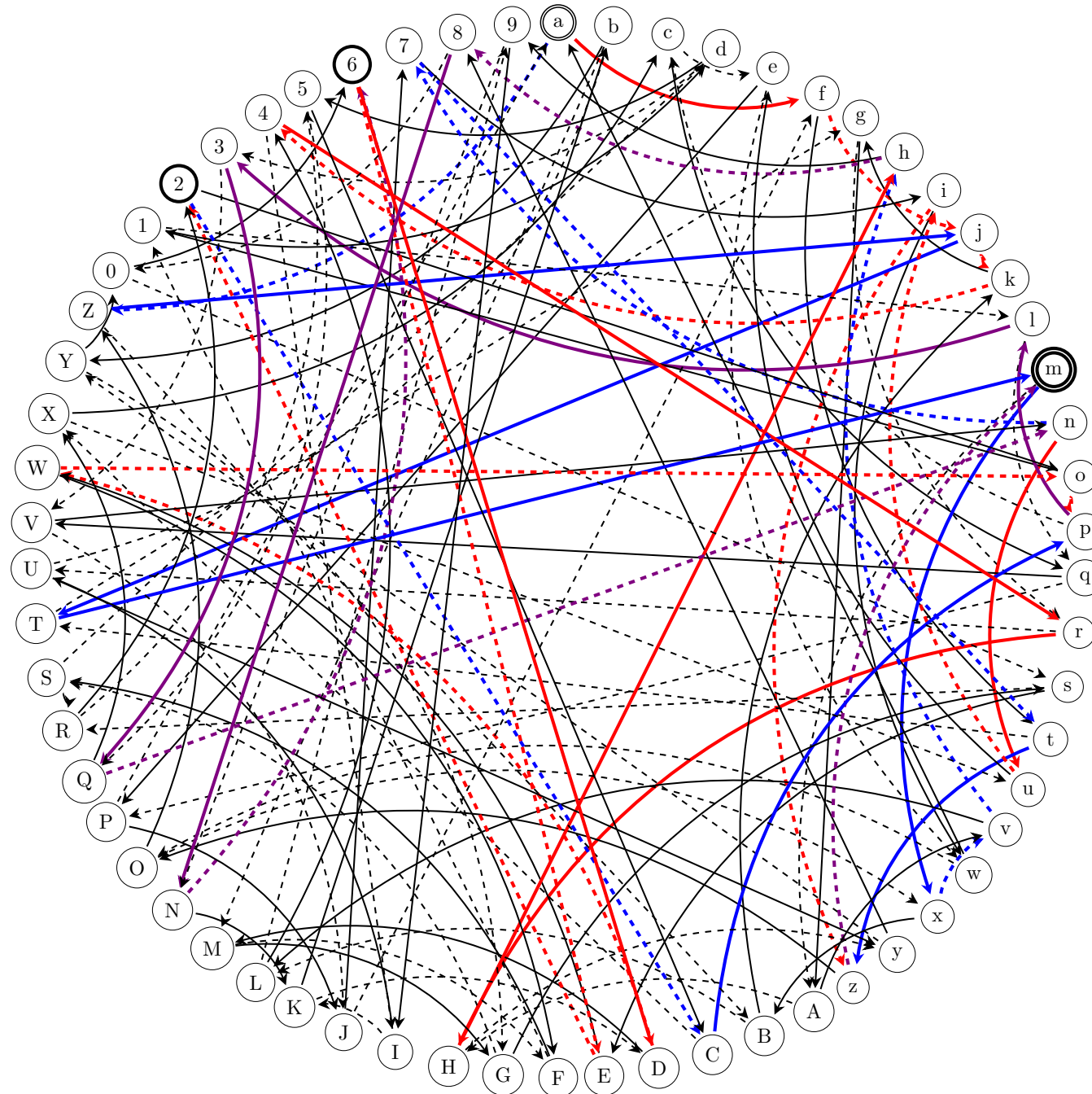
Échange de clé par graphe

L'échange de clé complet



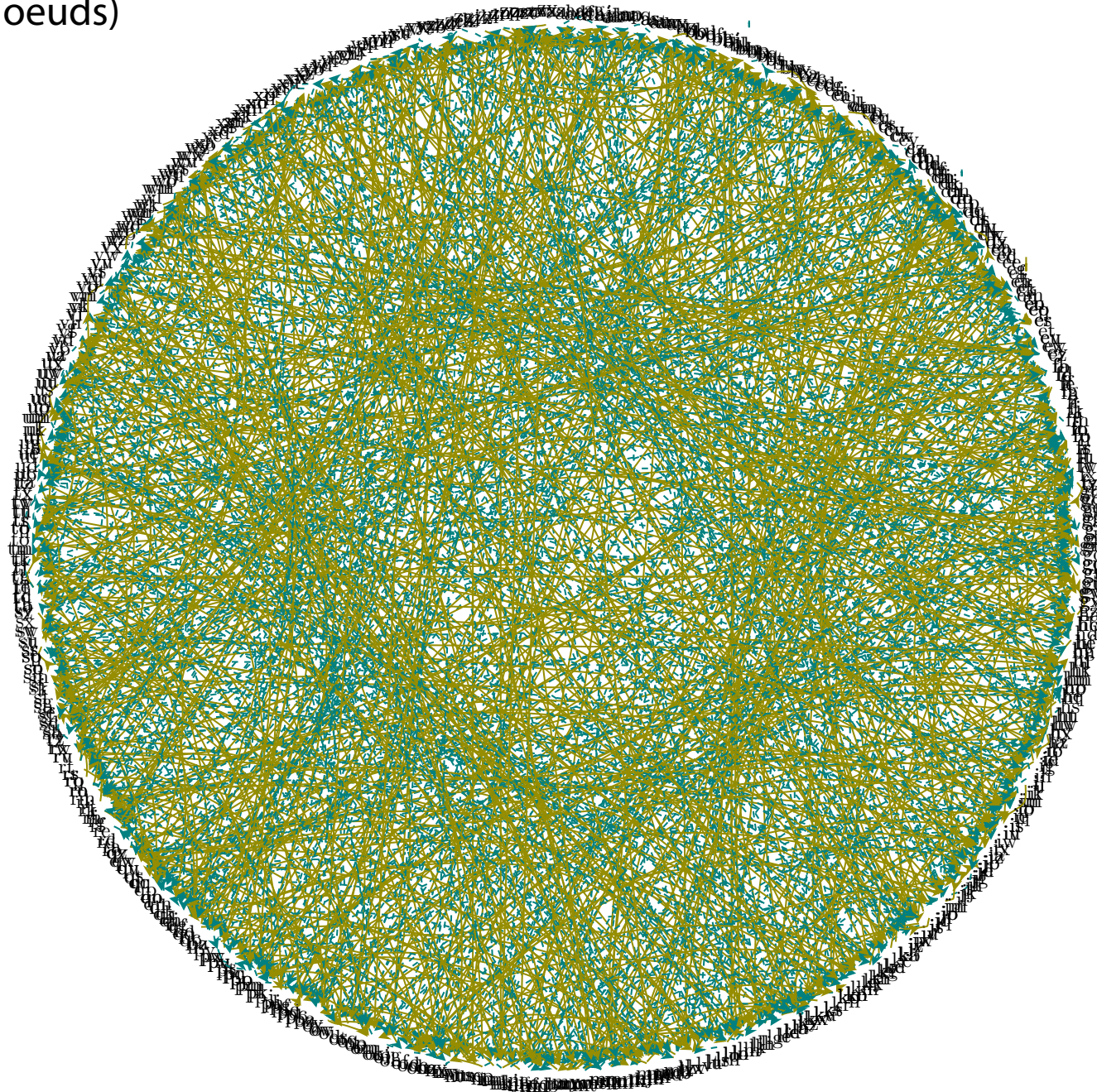
Échange de clé par graphe

Graphe plug grand (62 noeuds)



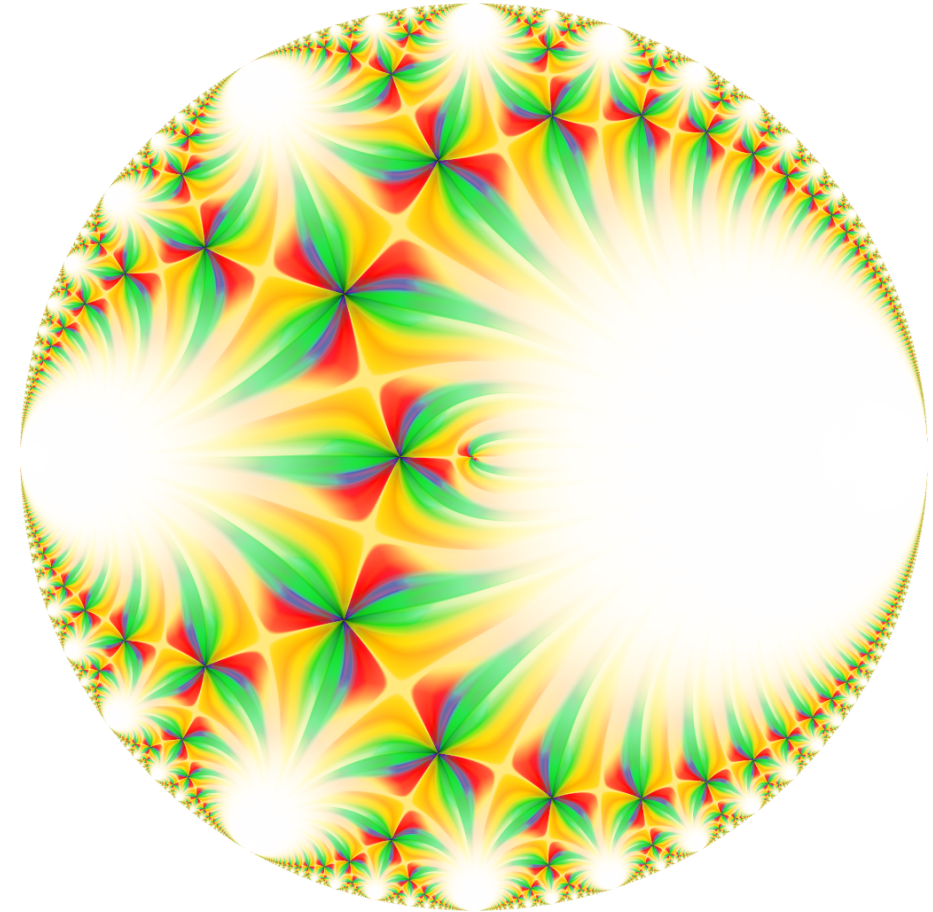
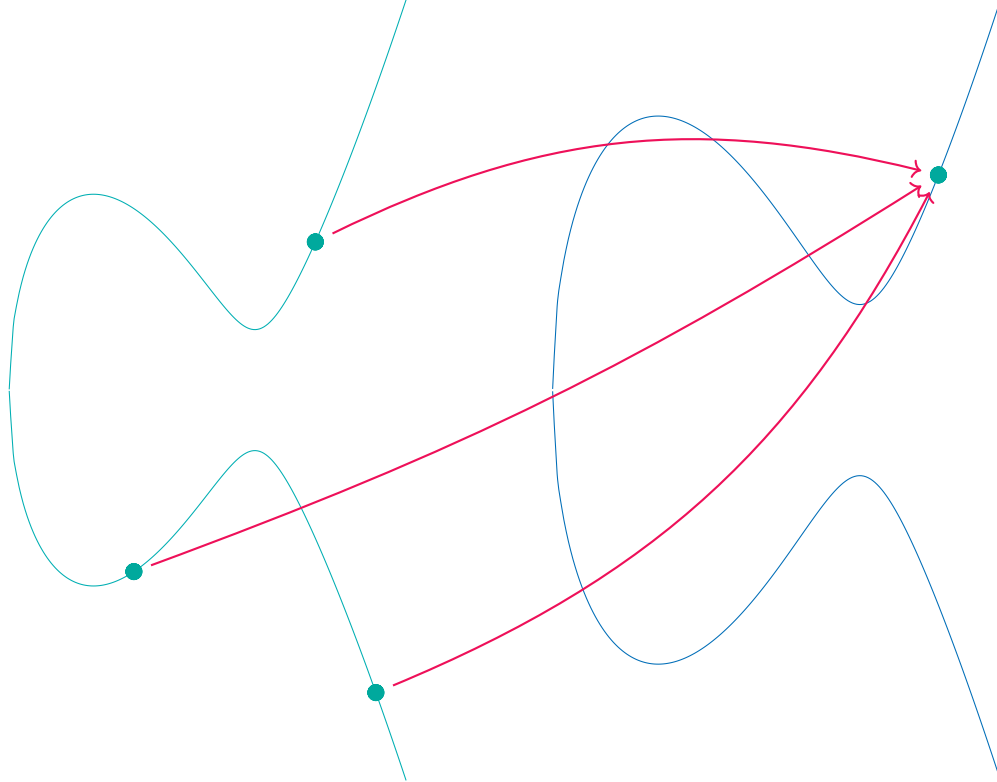
Échange de clé par graphe

Graphe encore plus grand (676 noeuds)



Isogénies de courbes elliptiques

$$E_1 : y^2 = x^3 + a_1x + b_1 \quad E_2 : y^2 = x^3 + a_2x + b_2$$



☺ $E/\mathbb{F}_q$ courbe elliptique **ordinaire** $\Rightarrow$ graphe d'isogénies **commutatif**
[Couveignes 1997, Rostovtsev-Stolbunov 2006] :

☹ **Attaque** quantique sous-exponentielle $\approx 2^{\log^{1/2} N}$

● $E/\mathbb{F}_{p^2}$ **supersingulière** $\Rightarrow$ graphe **expenseur** non commutatif de taille $N \approx p$

Structure mathématique : pushforward dans une catégorie

Isogénies de courbes elliptiques



SIDH/SIKE [De Feo-Jao 2011, De Feo-Jao-Plût 2014]

- Pour faire un échange de clé sur un graphe **non commutatif**, SIDH publie la valeur d'une **isogénie secrète** en certains points
- **Problème mathématique auxiliaire** : étant donné une fraction rationnelle

$$R(x) = \frac{g(x)}{h(x)}$$

de **grand degré** $N \gg 2^{128}$, et la valeur de R en certains points, retrouver R

- **Interpolation rationnelle** : $\tilde{O}(N)$
- Pour SIDH : problème d'interpolation **structuré** : R est compatible avec **l'addition** des courbes elliptiques
- [Castrick-Decru 2022]¹, [Maino-Martindale 2022, Maino-Martindale-Panny-Pope-Wesolowski 2023]² : emploi d'objets mathématiques de **dimension 2** pour attaquer **heuristiquement** SIDH dans **certains cas**
- [R. 2022]² : utilise la **dimension 4 et 8** pour attaquer de manière **prouvée** SIDH dans **tous les cas**
Fun fact : utilise que tout entier N est somme de 4 carrés!

1. Eurocrypt 2023 best paper award

2. Eurocrypt 2023 best paper honorable mention

SIDH/SIKE [De Feo-Jao 2011, De Feo-Jao-Plût 2014]

- Pour faire un échange de clé sur un graphe **non commutatif**, SIDH publie la valeur d'une **isogénie secrète** en certains points
- **Problème mathématique auxiliaire** : étant donné une fraction rationnelle

$$R(x) = \frac{g(x)}{h(x)}$$

de **grand degré** $N \gg 2^{128}$, et la valeur de R en certains points, retrouver R

- **Interpolation rationnelle** : $\tilde{O}(N)$
- Pour SIDH : problème d'interpolation **structuré** : R est compatible avec **l'addition** des courbes elliptiques
- [Castricky-Decru 2022]¹, [Maino-Martindale 2022, Maino-Martindale-Panny-Pope-Wesolowski 2023]² : emploi d'objets mathématiques de **dimension 2** pour attaquer **heuristiquement** SIDH dans **certains cas**
- [R. 2022]² : utilise la **dimension 4 et 8** pour attaquer de manière **prouvée** SIDH dans **tous les cas**
Fun fact : utilise que tout entier N est somme de 4 carrés!

1. Eurocrypt 2023 best paper award

2. Eurocrypt 2023 best paper honorable mention

Conclusion

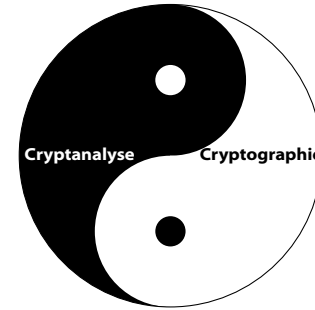
- **Cryptographie** : repose sur des problèmes **difficiles** (théorie de la complexité)
- Une structure **cachée** (trappe) permet de **déchiffrer**
- **Cryptanalyse** : comment exploiter cette structure?

- Nadia Herninger's **invited talk** at PKC 2024 : Cryptanaly · nomics
- Modification de **l'équilibre Cryptographie/Cryptanalyse** dans le **monde académique**
- Plus personne ne fait de la cryptanalyse de la **factorisation** ou du **logarithme discret sur un corps fini**
- Sauf **Caramba**, via le logiciel **Cado-NFS**! « 5 **underpaid** french researchers »
- « **Unique INRIA structure** facilitates this type of research in a way that **US academia** does not »

Conclusion

- **Cryptographie** : repose sur des problèmes **difficiles** (théorie de la complexité)
- Une structure **cachée** (trappe) permet de **déchiffrer**
- **Cryptanalyse** : comment exploiter cette structure ?

- Nadia Herninger's **invited talk** at PKC 2024 : Cryptanaly · nomics
- Modification de **l'équilibre Cryptographie/Cryptanalyse** dans le **monde académique**
- Plus personne ne fait de la cryptanalyse de la **factorisation** ou du **logarithme discret sur un corps fini**
- Sauf **Caramba**, via le logiciel **Cado-NFS** ! « 5 **underpaid** french researchers »
- « **Unique INRIA structure** facilitates this type of research in a way that **US academia** does not »



- Les **attaques** peuvent devenir **constructives**!
- Attaques grâce aux réseaux (sacs à dos, ...) $\Rightarrow$ **cryptographie à base de réseaux**
- Couplages sur courbes elliptiques pour attaquer le logarithme discret $\Rightarrow$ **cryptographie à base de couplages** (prix Gödel 2013)
- Attaques SIDH $\Rightarrow$ **cryptographie à base d'isogénies en dimension supérieure**
- Castryck's **invited talk** at Eurocrypt 2024 : « An attack became a tool : Isogeny based cryptography 2.0 »
- Exemple : SQISignHD [**Dartois, Leroux, R., Wesolowski**]³