Les Preuves à Apport Nul d'Information

Paul Simon

ENS
Langages Formels, Calculabilité, Complexité

13 Janvier 2011

Sommaire

Protocole de preuve interactive

Interaction

Dans les situations que l'on présentera, un Prouveur (Prospéro) tentera de convaincre un vérifieur (Viola) d'une propriété sur un objet.

Protocole de preuve interactive

Interaction

Dans les situations que l'on présentera, un Prouveur (Prospéro) tentera de convaincre un vérifieur (Viola) d'une propriété sur un objet.
Viola et Prospéro sont chacun des machines de Turing, qui disposent d'une bande commune pour échanger des informations.
Ils communiquent par des séries de *passes*, où chacun effectue simultanément :

1. Lecture de la bande commune
2. Calcul en privé
3. Ecriture sur la bande commune

Protocole de preuve interactive

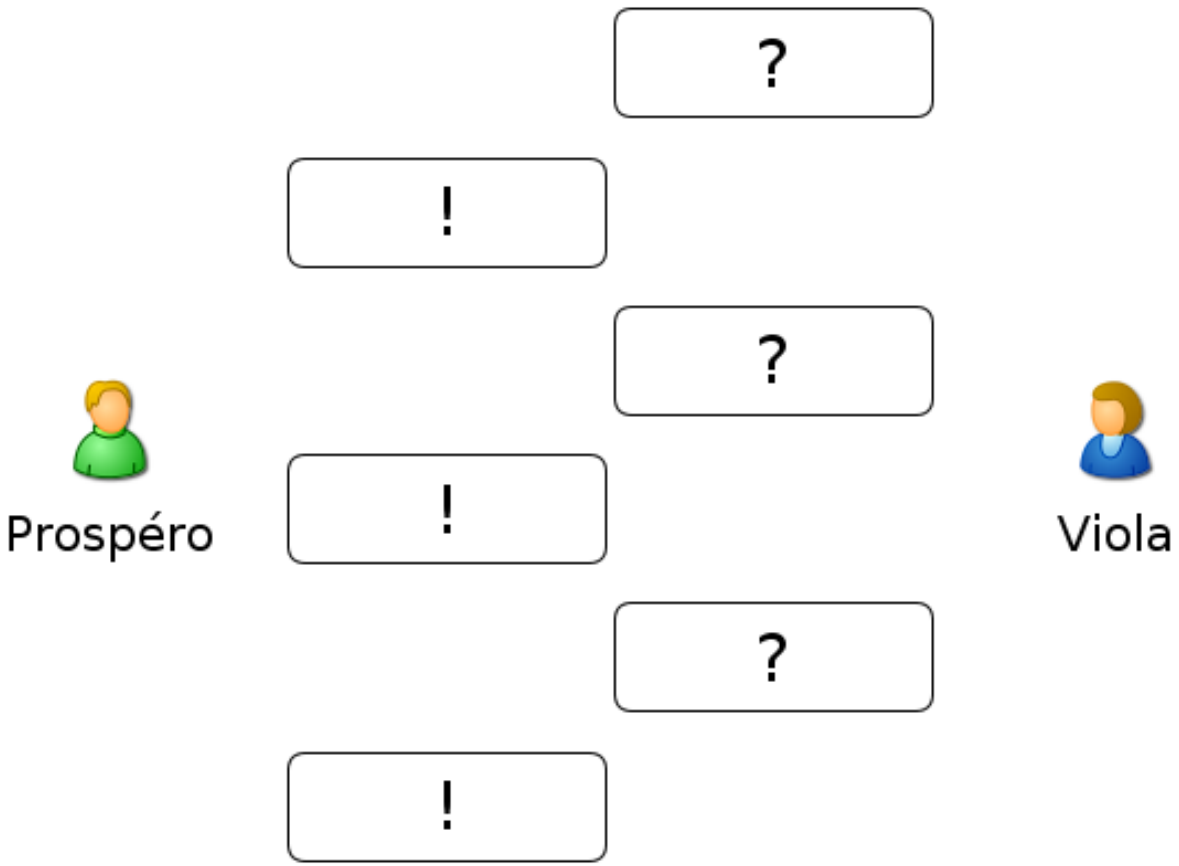
Interaction

Dans les situations que l'on présentera, un Prouveur (Prospéro) tentera de convaincre un vérifieur (Viola) d'une propriété sur un objet.
Viola et Prospéro sont chacun des machines de Turing, qui disposent d'une bande commune pour échanger des informations.
Ils communiquent par des séries de *passes*, où chacun effectue simultanément :

1. Lecture de la bande commune
2. Calcul en privé
3. Ecriture sur la bande commune

A la fin de l'interaction, Viola doit décider si elle accepte ou rejette la preuve.

Protocole de preuve interactive



Définition

On impose aux calculs effectués par Viola d'être polynomiaux.
Prospéro, lui, n'a aucune limite.

Définition

On impose aux calculs effectués par Viola d'être polynomiaux. Prospéro, lui, n'a aucune limite.

Preuve Interactive

Une preuve interactive d'un problème Π doit vérifier les deux propriétés suivantes :

Définition

On impose aux calculs effectués par Viola d'être polynomiaux. Prospéro, lui, n'a aucune limite.

Preuve Interactive

Une preuve interactive d'un problème Π doit vérifier les deux propriétés suivantes :

1. Consistance : Viola accepte la preuve quand l'entrée est une instance positive de Π

Définition

On impose aux calculs effectués par Viola d'être polynomiaux. Prospéro, lui, n'a aucune limite.

Preuve Interactive

Une preuve interactive d'un problème Π doit vérifier les deux propriétés suivantes :

1. Consistance : Viola accepte la preuve quand l'entrée est une instance positive de Π
2. Significativité : Pour les instances négatives, elle n'accepte la preuve qu'avec une faible probabilité.

Un exemple

On va montrer un exemple de preuve interactive pour le problème de non-isomorphisme de graphes.

Graphes isomorphes

Deux graphes (S_1, A_1) et (S_2, A_2) sont dits *isomorphes* s'il existe une bijection f entre S_1 et S_2 qui préserve les sommets, c'est-à-dire :

$$\forall (u, v) \in S_1^2, (u, v) \in A_1 \Leftrightarrow (f(u), f(v)) \in A_2$$

Un exemple

On va montrer un exemple de preuve interactive pour le problème de non-isomorphisme de graphes.

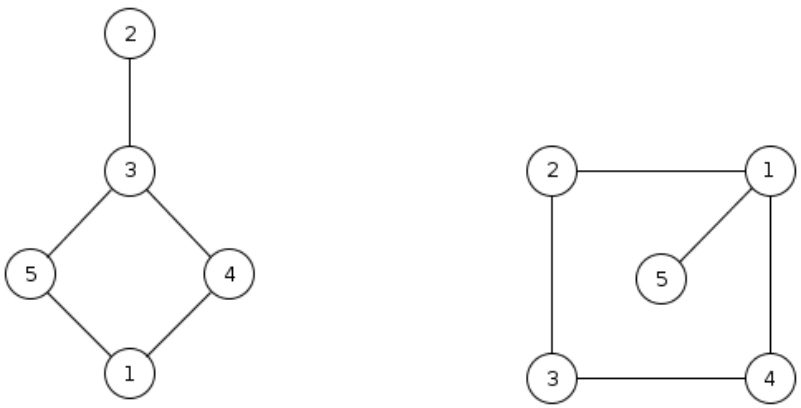
Graphes isomorphes

Deux graphes (S_1, A_1) et (S_2, A_2) sont dits *isomorphes* s'il existe une bijection f entre S_1 et S_2 qui préserve les sommets, c'est-à-dire :

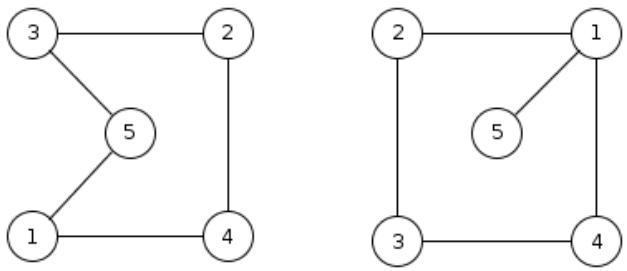
$$\forall (u, v) \in S_1^2, (u, v) \in A_1 \Leftrightarrow (f(u), f(v)) \in A_2$$

On note GI le problème de l'isomorphisme entre deux graphes. On ne connait pas d'algorithme polynomial pour le résoudre, mais on ne sait pas non plus si GI est NP-complet.

Deux graphes isomorphes



Deux graphes non-isomorphes



Preuve interactive de non-isomorphisme

- Entrée : Deux graphes G_1 et G_2, ayant chacun $\{1, \ldots, n\}$ comme ensemble de sommets
- Répéter x fois la passe suivante :

Preuve interactive de non-isomorphisme

- Entrée : Deux graphes G_1 et G_2, ayant chacun $\{1, \ldots, n\}$ comme ensemble de sommets
- Répéter x fois la passe suivante :
  1. Viola choisit une permutation π de $\{1, \ldots, n\}$ au hasard.

Preuve interactive de non-isomorphisme

- Entrée : Deux graphes G_1 et G_2, ayant chacun $\{1, \ldots, n\}$ comme ensemble de sommets
- Répéter x fois la passe suivante :
  1. Viola choisit une permutation π de $\{1, \ldots, n\}$ au hasard.
  2. Elle calcule l'image de G_1 ou G_2 par π (en tirant au sort).
  3. Elle envoie cette image H à Prospéro.

Preuve interactive de non-isomorphisme

- Entrée : Deux graphes G_1 et G_2, ayant chacun $\{1, \ldots, n\}$ comme ensemble de sommets
- Répéter x fois la passe suivante :
  1. Viola choisit une permutation π de $\{1, \ldots, n\}$ au hasard.
  2. Elle calcule l'image de G_1 ou G_2 par π (en tirant au sort).
  3. Elle envoie cette image H à Prospéro.
  4. Prospéro calcule auquel des deux graphes H est isomorphe, et le dit à Viola.

Preuve interactive de non-isomorphisme

- Entrée : Deux graphes G_1 et G_2, ayant chacun $\{1, \ldots, n\}$ comme ensemble de sommets
- Répéter x fois la passe suivante :
  1. Viola choisit une permutation π de $\{1, \ldots, n\}$ au hasard.
  2. Elle calcule l'image de G_1 ou G_2 par π (en tirant au sort).
  3. Elle envoie cette image H à Prospéro.
  4. Prospéro calcule auquel des deux graphes H est isomorphe, et le dit à Viola.
  5. Viola vérifie qu'il s'agissait bien de son graphe choisi à l'étape 2.
- Viola accepte la preuve si à toutes les passes Prospéro a répondu correctement.

La classe IP

On note IP la classe des problèmes admettant une preuve interactive. On montre (mais vous le savez déjà) que :

$$\text{IP}=\text{PSPACE}$$

Une preuve interactive d'isomorphisme

Une preuve interactive d'isomorphisme

- Entrée : Deux graphes G_1 et G_2, ayant chacun $\{1, \ldots, n\}$ comme ensemble de sommets
- Répéter x fois la passe suivante :

Une preuve interactive d'isomorphisme

- Entrée : Deux graphes G_1 et G_2, ayant chacun $\{1, \ldots, n\}$ comme ensemble de sommets
- Répéter x fois la passe suivante :
  1. Prospéro tire une permutation π de $\{1, \ldots, n\}$ au hasard.
  2. Il calcule H, l'image de G_1 par π, et l'envoie à Viola.

Une preuve interactive d'isomorphisme

- Entrée : Deux graphes G_1 et G_2, ayant chacun $\{1, \ldots, n\}$ comme ensemble de sommets
- Répéter x fois la passe suivante :
  1. Prospéro tire une permutation π de $\{1, \ldots, n\}$ au hasard.
  2. Il calcule H, l'image de G_1 par π, et l'envoie à Viola.
  3. Viola tire au sort un graphe G_i entre G_1 et G_2.
  4. Elle demande à Prospéro de lui montrer un isomorphisme entre H et G_i.

Une preuve interactive d'isomorphisme

- Entrée : Deux graphes G_1 et G_2, ayant chacun $\{1, \ldots, n\}$ comme ensemble de sommets
- Répéter x fois la passe suivante :
  1. Prospéro tire une permutation π de $\{1, \ldots, n\}$ au hasard.
  2. Il calcule H, l'image de G_1 par π, et l'envoie à Viola.
  3. Viola tire au sort un graphe G_i entre G_1 et G_2.
  4. Elle demande à Prospéro de lui montrer un isomorphisme entre H et G_i.
  5. Viola vérifie que la fonction envoyée par Prospéro est bien un isomorphisme.
- Si Prospéro répond correctement à chaque passe, Viola accepte la preuve.

Aucun apport d'information

A la fin du protocole précédent, Viola est convaincue de l'existence d'un isomorphisme entre G_1 et G_2, cependant elle n'a rien appris d'utile pour construire cette isomorphisme.

Aucun apport d'information

A la fin du protocole précédent, Viola est convaincue de l'existence d'un isomorphisme entre G_1 et G_2, cependant elle n'a rien appris d'utile pour construire cette isomorphisme.
Viola a vu passer, à chaque passe, un graphe H isomorphe à G_1 et G_2, mais elle n'a pu demander à voir qu'un seul des deux isomorphismes ; ce qui ne lui sert à rien.

Aucun apport d'information

A la fin du protocole précédent, Viola est convaincue de l'existence d'un isomorphisme entre G_1 et G_2, cependant elle n'a rien appris d'utile pour construire cette isomorphisme.
Viola a vu passer, à chaque passe, un graphe H isomorphe à G_1 et G_2, mais elle n'a pu demander à voir qu'un seul des deux isomorphismes ; ce qui ne lui sert à rien.
Une personne autre que Prospéro aurait pu générer aléatoirement des fausses transcriptions des échanges entre Viola et Prospéro, et ceci avec une capacité de calcul polynomiale.

Définition un peu plus formelle

Absence d'apport d'information

On dit qu'un protocole de preuve est sans apport d'information si une machine polynomiale extérieure à Viola et Prospéro peut générer des répliques des transcriptions des échanges entre les deux parties avec la même distribution de probabilité que celles réalisées par la preuve.

Définition un peu plus formelle

Absence d'apport d'information

On dit qu'un protocole de preuve est sans apport d'information si une machine polynomiale extérieure à Viola et Prospéro peut générer des répliques des transcriptions des échanges entre les deux parties avec la même distribution de probabilité que celles réalisées par la preuve.

Informellement, si Viola peut tout aussi bien lire une transcription aléatoire que les réponses de Prospéro, c'est qu'elle n'apprend effectivement rien.

Définition un peu plus formelle

Absence d'apport d'information

On dit qu'un protocole de preuve est sans apport d'information si une machine polynomiale extérieure à Viola et Prospéro peut générer des répliques des transcriptions des échanges entre les deux parties avec la même distribution de probabilité que celles réalisées par la preuve.

Informellement, si Viola peut tout aussi bien lire une transcription aléatoire que les réponses de Prospéro, c'est qu'elle n'apprend effectivement rien.
Pour une définition plus rigoureuse et indigeste, voir le premier article de la bibliographie.

Que peut-on prouver sans rien dire ?

- Objectif : déterminer un peu plus précisément l'allure de la sous-classe de IP des problèmes admettant une preuve Zero-Knowledge.

Que peut-on prouver sans rien dire ?

- Objectif : déterminer un peu plus précisément l'allure de la sous-classe de IP des problèmes admettant une preuve Zero-Knowledge.
- On va montrer que tous les problèmes NP admettent une ZKP

Que peut-on prouver sans rien dire ?

- Objectif : déterminer un peu plus précisément l'allure de la sous-classe de IP des problèmes admettant une preuve Zero-Knowledge.
- On va montrer que tous les problèmes NP admettent une ZKP
  1. On introduira un outil technique : les *procédés d'engagement de bits*

Que peut-on prouver sans rien dire ?

- Objectif : déterminer un peu plus précisément l'allure de la sous-classe de IP des problèmes admettant une preuve Zero-Knowledge.
- On va montrer que tous les problèmes NP admettent une ZKP
  1. On introduira un outil technique : les *procédés d'engagement de bits*
  2. On exhibera une ZKP du problème G3C, qui est NP-complet.

Que peut-on prouver sans rien dire ?

- Objectif : déterminer un peu plus précisément l'allure de la sous-classe de IP des problèmes admettant une preuve Zero-Knowledge.
- On va montrer que tous les problèmes NP admettent une ZKP
  1. On introduira un outil technique : les *procédés d'engagement de bits*
  2. On exhibera une ZKP du problème G3C, qui est NP-complet.

En fait, Goldreich et Goldwasser ont montré en 1988 que tous les problèmes dans IP admettaient une ZKP ; au procédé d'engagement près.

Procédé d'engagement de bits

Définition

Un procédé d'engagement (*commitment scheme*) est une façon particulière pour Prospéro de crypter un message M. Ce procédé doit garantir :

Procédé d'engagement de bits

Définition

Un procédé d'engagement (*commitment scheme*) est une façon particulière pour Prospéro de crypter un message M. Ce procédé doit garantir :

1. Dissimulation : Viola ne peut pas décrypter le message chiffré.

Procédé d'engagement de bits

Définition

Un procédé d'engagement (*commitment scheme*) est une façon particulière pour Prospéro de crypter un message M. Ce procédé doit garantir :

1. Dissimulation : Viola ne peut pas décrypter le message chiffré.
2. Engagement : Prospéro ne sait pas produire le même message chiffré à partir de deux sources différents.

Procédé d'engagement de bits

Définition

Un procédé d'engagement (*commitment scheme*) est une façon particulière pour Prospéro de crypter un message M. Ce procédé doit garantir :

1. Dissimulation : Viola ne peut pas décrypter le message chiffré.
2. Engagement : Prospéro ne sait pas produire le même message chiffré à partir de deux sources différents.

Prospéro peut plus tard montrer M à Viola de sorte qu'elle puisse vérifier qu'il s'agissait bien de la source.

Procédé d'engagement de bits

Définition

Un procédé d'engagement (*commitment scheme*) est une façon particulière pour Prospéro de crypter un message M. Ce procédé doit garantir :

1. Dissimulation : Viola ne peut pas décrypter le message chiffré.
2. Engagement : Prospéro ne sait pas produire le même message chiffré à partir de deux sources différents.

Prospéro peut plus tard montrer M à Viola de sorte qu'elle puisse vérifier qu'il s'agissait bien de la source.

Tout se passe en fait comme si Prospéro écrivait un message sur une feuille de papier, l'enfermait dans un coffre fort qu'il donne ensuite à Viola.

Procédé d'engagement de bits

De tels procédés existent-ils ?

Procédé d'engagement de bits

De tels procédés existent-ils ?

Oui.

Procédé d'engagement de bits

De tels procédés existent-ils ?

Oui.

Ils se fondent principalement sur la difficulté du problème de résiduosité quadratique.

Procédé d'engagement de bits

De tels procédés existent-ils ?

Oui.

Ils se fondent principalement sur la difficulté du problème de résiduosité quadratique.
Pour simplifier la suite de l'exposé, on supposera posséder un tel procédé, dont on ne se servira que comme d'une boîte noire au fonctionnement peu clair.

Le problème G3C

3-coloriabilité

On dit qu'un graphe (S, A) est *3-coloriable* lorsque qu'il existe une fonction $f : S \to \{0, 1, 2\}$ vérifiant :

$$\forall (u, v) \in A, f(u) \neq f(v)$$

En clair, on colorie chaque sommet de sorte que deux sommets distincts ne soient pas de la même couleur.

Le problème G3C

3-coloriabilité

On dit qu'un graphe (S, A) est *3-coloriable* lorsque qu'il existe une fonction $f : S \to \{0, 1, 2\}$ vérifiant :

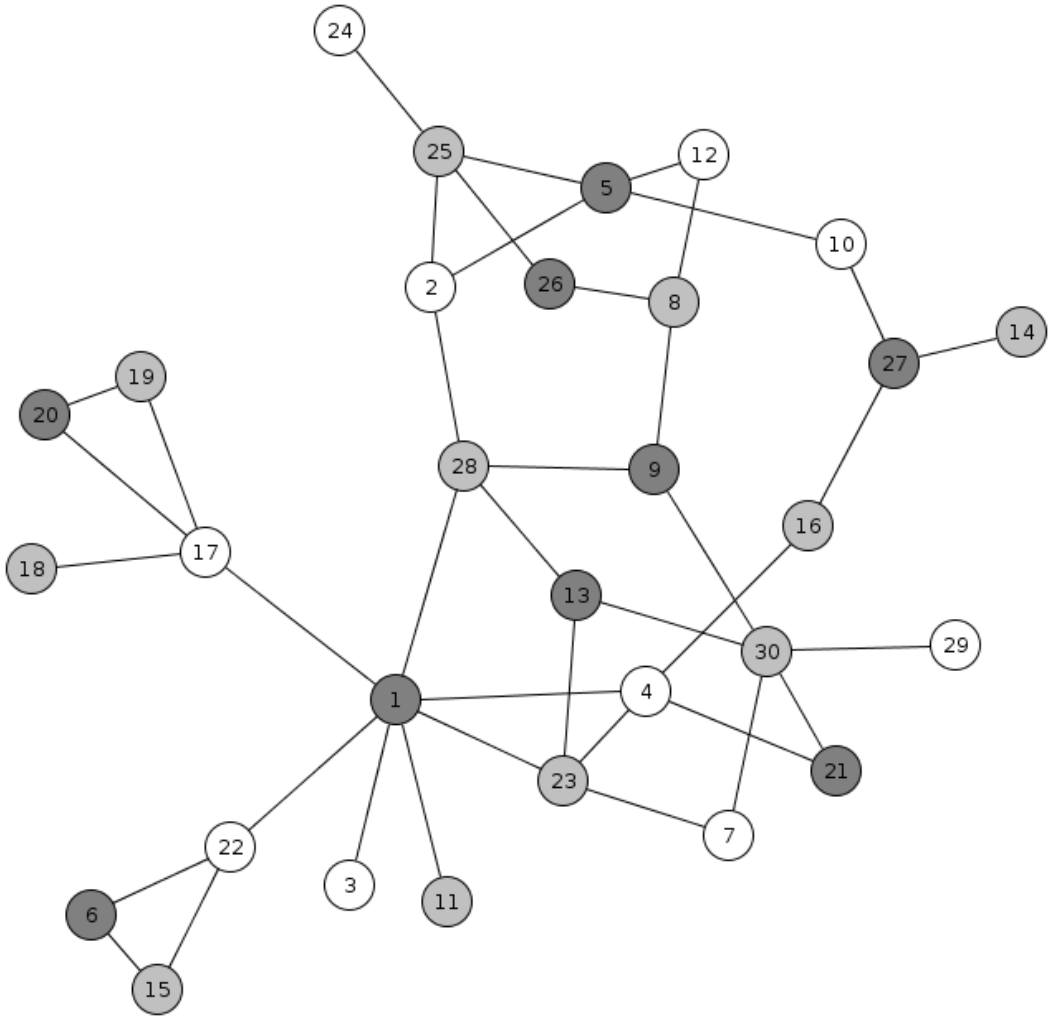
$$\forall (u, v) \in A, f(u) \neq f(v)$$

En clair, on colorie chaque sommet de sorte que deux sommets distincts ne soient pas de la même couleur.

G3C

G3C, le problème de 3-coloriabilité, est NP-complet.

Un graphe 3-coloriable



Une ZKP avec PEB de G3C

- Entrée : un graphe G à n sommets
- Répéter à l'envie la passe suivante :

Une ZKP avec PEB de G3C

- Entrée : un graphe G à n sommets
- Répéter à l'envie la passe suivante :
  1. Prospéro établit une 3-coloration de G

Une ZKP avec PEB de G3C

- Entrée : un graphe G à n sommets
- Répéter à l'envie la passe suivante :
  1. Prospéro établit une 3-coloration de G
  2. Prospéro s'engage. Il envoie à Viola n coffres-fort, chaque coffre contenant la couleur d'un sommet de G.

Une ZKP avec PEB de G3C

- Entrée : un graphe G à n sommets
- Répéter à l'envie la passe suivante :
  1. Prospéro établit une 3-coloration de G
  2. Prospéro s'engage. Il envoie à Viola n coffres-fort, chaque coffre contenant la couleur d'un sommet de G.
  3. Viola choisit au hasard une arête de G, et demande à voir les couleurs de ses extrémités.

Une ZKP avec PEB de G3C

- Entrée : un graphe G à n sommets
- Répéter à l'envie la passe suivante :
  1. Prospéro établit une 3-coloration de G
  2. Prospéro s'engage. Il envoie à Viola n coffres-fort, chaque coffre contenant la couleur d'un sommet de G.
  3. Viola choisit au hasard une arête de G, et demande à voir les couleurs de ses extrémités.
  4. Prospéro débloque les coffres concernés pour Viola.
  5. Viola vérifie que les deux sommets sont bien de couleur différente.
- Si Prospéro échoue ne serait-ce qu'une fois, Viola refuse la preuve.

Extension à NP

Comme tous les problèmes NP admettent une réduction polynomiale à G3C, on voit naturellement comment, à partir de la preuve précédente, construire une ZKP pour un problème NP quelconque.

Extension à NP

Comme tous les problèmes NP admettent une réduction polynomiale à G3C, on voit naturellement comment, à partir de la preuve précédente, construire une ZKP pour un problème NP quelconque.

Calculatoirement sans apport d'information

Du fait de la nécéssité du procédé d'engagement de bits, on doit restreindre la définition de preuve sans apport d'information. On parle alors de preuves *calculatoirement* sans apport d'information.

Extension à NP

Comme tous les problèmes NP admettent une réduction polynomiale à G3C, on voit naturellement comment, à partir de la preuve précédente, construire une ZKP pour un problème NP quelconque.

Calculatoirement sans apport d'information

Du fait de la nécéssité du procédé d'engagement de bits, on doit restreindre la définition de preuve sans apport d'information. On parle alors de preuves *calculatoirement* sans apport d'information.

Théorème

Tous les problèmes NP admettent une preuve calculatoirement sans apport d'information.

Extension à NP

Comme tous les problèmes NP admettent une réduction polynomiale à G3C, on voit naturellement comment, à partir de la preuve précédente, construire une ZKP pour un problème NP quelconque.

Calculatoirement sans apport d'information

Du fait de la nécéssité du procédé d'engagement de bits, on doit restreindre la définition de preuve sans apport d'information. On parle alors de preuves *calculatoirement* sans apport d'information.

Théorème

Tous les problèmes NP admettent une preuve calculatoirement sans apport d'information.

On connait également une ZKP du problème des chemins hamiltoniens. Elle requiert également un procédé d'engagement de bits.

Ce dont nous n'avons pas parlé

Ce dont nous n'avons pas parlé

- Que faire si Viola triche ?

Ce dont nous n'avons pas parlé

- Que faire si Viola triche ?
- Utilité pratique des procédés d'engagement de bits

Ce dont nous n'avons pas parlé

- Que faire si Viola triche ?
- Utilité pratique des procédés d'engagement de bits
- Intérêt des ZKP dans le monde réel : protocoles d'identification

Remerciements et Bibliographie

Je remercie Pierre-Alain Fouque pour m'avoir fourni la source principale de cette présentation, à la fois claire et rigoureuse.

Remerciements et Bibliographie

Je remercie Pierre-Alain Fouque pour m'avoir fourni la source principale de cette présentation, à la fois claire et rigoureuse.

Bibliographie

- Stinson, *Cryptography : Theory and Practice*, CRC Press, Boca Raton, 2002
- Goldreich, Micali, Wigderson, *Proofs that Yield Nothing but their Validity*, Journal of the ACM, volume 38, issue 3, Juillet 1991
- Goldwasser, Micali, Rackoff, *The Knowledge Complexity of Interactive Proof Systems*, SIAM Journal on Computing, 18, 1989
- Fiat, Shamir, *How to Prove Yourself : Practical Solutions to Identification and Signature Problems*, CRYPTO 1986