Prouver sans rien dire : les Preuves à Apport Nul d'Information

Paul Simon
paul.simon@ens.fr
Langages formels, calculabilité, complexité
École Normale Supérieure

Décembre 2010

Résumé

On présente ici des protocoles interactifs de preuve, qui nous serviront de cadre pour définir ce que sont des preuves sans apport d'information. Ces preuves établissent la véracité d'une propriété sur un objet sans rien révéler d'autre sur cet objet que cette propriété. Le problème d'isomorphisme de graphes nous servira d'exemple récurrent. Ensuite, avec le problème de 3-coloriabilité d'un graphe, nous montrerons que tous les problèmes NP admettent de telles preuves, avec quelques restrictions néanmoins. Enfin, nous étudierons une application de ces preuves au protocole d'identification de Fiat-Shamir, qui est la base des protocoles actuels d'identification à divulgation nulle d'information.

1 Preuves interactives

On va s'intéresser ici à des protocoles de preuves qui, au contraire des preuves usuelles, sont interactifs. Un tel protocole sera en effet constitué d'une série de *passes* entre un prouveur (Prospéro) et un vérifieur (Viola). Viola pose une série de questions auxquelles Prospéro répond, dans le but de convaincre Viola d'une propriété particulière sur un objet donné. Ce type de preuve se rapproche donc plus d'une interaction entre un professeur et ses élèves en classe que d'une suite d'assertions formelles trouvée dans un livre de mathématiques.

1.1 Protocole de preuve interactive

On suppose que Prospéro et Viola fonctionnent comme deux algorithmes probabilistes, donc qu'ils disposent chacun d'un générateur aléatoire qu'ils utilisent pour faire des calculs en privé. Ils possèdent aussi un canal de communication, dont ils se servent pour échanger des messages.

On imposera à Viola de n'effectuer que des calculs en temps polynomial. En effet, sans cette restriction la preuve de problèmes NP perd son intérêt, puisque Viola peut tout aussi bien les résoudre elle-même. En revanche, les capacités de calcul de Prospéro, puissant magicien, sont, elles, illimitées.

Remarque 1.1

On peut voir Prospéro et Viola comme des machines de Turing interactives*, c'est-à-dire qu'en plus d'avoir chacune leur ruban propre, elles disposent d'un ruban commun pour échanger des informations.*

On imposera une borne sur la taille du ruban de Viola pour que celle-ci n'effectue de des calculs en temps polynomial, mais pas sur celle de Prospéro.

Rigoureusement, ce protocole consiste en une entrée x, et une série de *passes*, typiquement une question de Viola suivie d'une réponse de Prospéro. A chaque passe, chacun d'eux effectue alternativement :

1. Réception d'un message
2. Calcul en privé
3. Émission d'un message

Après la série de passes, Viola choisit entre accepter et rejeter ce que Prospéro vient de lui prouver.

Définition 1.2 (*Preuve interactive*)

On dit que le protocole précédent est une preuve interactive pour le problème de décision Π *si les deux critères suivants sont vérifiés.*

1. Consistance *: Quand l'entrée x est une instance positive de* Π*, Viola accepte la preuve avec une probabilité* 1.
2. Significativité *: Si x est une instance négative de* Π*, alors la probabilité que Viola accepte la preuve de Prospéro est* très faible *(tend vers 0 avec le nombre de passes).*

On notera IP l'ensemble des problèmes qui admettent une preuve interactive.

Remarque 1.3

On peut montrer que IP=PSPACE, c'est-à-dire que les problèmes admettant une preuve interactive sont exactement les problèmes pouvant être résolus par une machine de Turing avec une quantité polynomiale de mémoire. En particulier, on peut noter que NP$\subset$IP.

1.2 Un exemple : l'absence d'isomorphisme entre deux graphes

On s'intéresse au problème d'isomorphisme de graphes, pour lequel on présente à titre d'exemple une preuve interactive du complémentaire. Il est important de noter que, même si l'on ne sait pas si ce problème est NP-complet, on ne connait pas d'algorithme polynomial pour le résoudre.

Définition 1.4 (*Isomorphisme de graphes*)

Étant donnés deux graphes à n sommets $G_1 = (S_1, A_1)$ et $G_2 = (S_2, A_2)$, le problème de l'isomorphisme de graphes consiste à savoir s'il existe une fonction bijective $\pi : S_1 \to S_2$ préservant les arêtes, c'est-à-dire vérifiant $\{u, v\} \in A_1$ si et seulement si $\{\pi(u), \pi(v)\} \in A_2$.

On note GI le langage des instances positives de ce problème. GI∈NP.

Avec le protocole suivant, Prospéro convainc Viola de l'absence d'isomorphisme entre les deux graphes donnés en entrée. On suppose sans nuire à la généralité que ces deux graphes partagent le même ensemble de sommets : $\{1, \ldots, n\}$. Un isomorphisme est alors à rechercher parmi les éléments de $\mathfrak{S}_n$.

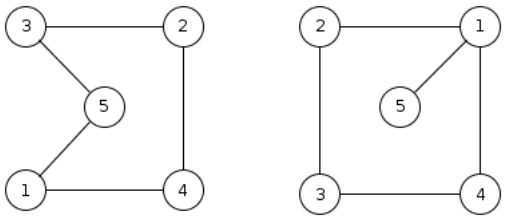
Protocole 1

Entrée : Deux graphes : G_1 et G_2, ayant tous les deux pour ensemble de sommets $\{1, \ldots, n\}$.

Répéter n fois les opérations suivantes :

1. *Viola choisit au hasard une permutation π sur $\{1, \ldots, n\}$*
2. *Viola choisit aléatoirement un entier i entre 1 et 2, et calcule H, l'image de G_i par π.*
3. *Viola transmet H à Prospéro, et lui demande pour quel entier j on a G_j isomorphe à H*
4. *Prospéro détermine cet entier j, et le transmet à Viola.*
5. *Viola vérifie que $i = j$.*

Si à la fin de chaque passe Viola constate que $i = j$, alors elle accèpte la preuve, et la rejette dans le cas contraire.



Deux graphes non isomorphes

Ce protocole est-il bien une preuve interactive au sens définie précédemment ? Il est aisé de s'en rendre compte.

Consistance Si les deux graphes donnés en entrée ne sont pas isomorphe, Prospéro ne peut pas (pourvu qu'il calcule correctement) se tromper de graphe, et est certain de donner la bonne réponse à Viola, et ce, à chaque passe. Viola accepte donc la preuve avec une probabilité 1.

Significativité Si les deux graphes sont isomorphes, par contre, comme la permutation choisie par Viola au début de la passe est aléatoire, Prospéro n'a aucun moyen de deviner quel a été le graphe choisi par Viola. Il se voit en effet présenter un graphe H isomorphe à G_1 et G_2, et se retrouve contraint de tirer à pile ou face pour répondre à Viola. Il n'a alors qu'une chance sur deux de valider

la passe, et ne parvient à duper Viola qu'avec une probabilité de 2^{-n}.

On constate de plus que Viola ne fait que tirer des permutations au hasard, et calculer des images de graphes par ces permutations ; et tous ces calculs se font bien sûr en temps polynomial. Ce protocole est donc bien une preuve interactive pour le problème voulu.

Rien n'est dit sur le temps de calcul de Prospéro, qui à chaque passe doit déterminer un isomorphisme entre deux graphes (ce qui, *a priori*, ne peut s'effectuer en temps polynomial).

2 Preuves sans apport d'information

Un des intérêts de ces preuves interactives est qu'elles fournissent un cadre rigoureux à une définition de preuves sans apport d'information. Intuitivement, ces preuves parviennent à convaincre le vérifieur d'une propriété sur un objet sans rien lui apprendre d'autre sur l'objet en question.

2.1 Isomorphisme de graphes sans apport d'information

On poursuit l'exemple précédent en montrant cette fois un protocole de preuve pour l'isomorphisme de graphes. Intuitivement, on verra que quand cette preuve aboutit, Viola est convaincue de l'existence d'un isomorphisme entre G_1 et G_2, mais ne sait absolument rien de cet isomorphisme.

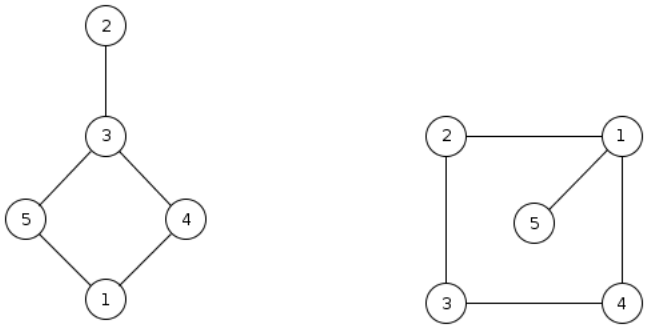
Protocole 2

Entrée : Deux graphes : G_1 et G_2, ayant tous les deux pour ensemble de sommets $\{1, \ldots, n\}$.

Répéter n fois les opérations suivantes :

1. *Prospéro tire au hasard une permutation π sur $\{1, \ldots, n\}$*
2. *Prospéro calcule et transmet à Viola l'image H de G_1 par π*
3. *Viola choisit un entier i au hasard entre 1 et 2, et demande à Prospéro de lui montrer un isomorphisme entre G_i et H*
4. *Prospéro envoie ρ, la permutation demandée (il renvoie π si $i = 1$, et $\sigma\pi$ sinon, avec σ un isomorphisme entre G_1 et G_2.*
5. *Viola vérifie que H est bien l'image de G_i par ρ*

Viola accepte la preuve si et seulement si la vérification est positive à la fin de chaque passe



Deux graphes isomorphes

Consistance et significativité Si les deux graphes sont isomorphes, Prospéro, avec sa capacité de calcul infinie, peut sans difficulté déterminer un isomorphisme σ entre les deux graphes. Sans aucun problème, il peut alors parvenir à répondre correctement à toutes les demandes de Viola.

En revanche, si les deux graphes ne sont pas isomorphes, la seule façon pour Prospéro d'espérer satisfaire aux demandes de Viola est de prévoir avant la phase 3 quel sera le graphe demandé par Viola, et de lui fournir à la phase 2 un graphe isomorphe à ce dernier. Il ne peut encore une fois que deviner au hasard, et n'a qu'une chance sur deux de passer la phase avec succès. Il ne pourra donc tromper Viola, après les n passes, qu'avec une probabilité de 2^{-n}.

Encore une fois, les calculs de Viola ne sont jamais supra-polynomiaux, et donc le protocole présenté est bien une preuve interactive.

Ce que cette preuve a de plus que la première, c'est que Viola, après les n passes, n'a appris aucune information qui pourrait lui permettre de construire un isomorphisme entre les deux graphes, alors même qu'elle est persuadée de l'existence de cet isomorphisme.

A chaque passe, on lui donne un graphe H, isomorphe à G_1 et G_2, mais elle n'a le droit de demander à voir qu'un seul des deux isomorphismes correspondant, ce qui ne lui suffit pas pour construire un isomorphisme entre G_1 et G_2 (cette opération est trop difficile pour elle).

2.2 Une définition formelle des preuves sans apport d'information

On peut se servir de l'exemple précédent pour formaliser la notion d'apport nul d'information dans les preuves. Pour ce faire, supposons que l'on ait pris en note une *transcription* des échanges entre Viola et Prospéro, c'est-à-dire : les graphes donnés en entrée et les messages échangés entre les deux parties. Rien n'empêche une personne extérieure de créer artificiellement et aléatoirement, sans prendre part au protocole, une transcription semblable à celle de la preuve. Comme Viola ne reçoit des informations que par la transcription de la preuve, et que cette transcription peut être remplacée par une autre créée par quelqu'un qui ne'est pas Prospéro, Viola n'apprend finalement rien du tout de la preuve.

Il reste à définir rigoureusement en quoi une transcription artificielle est semblable à une transcription de preuve réelle, et l'on pourra alors proposer un modèle formel de preuve sans apport d'information.

Définition 2.1 (*Preuve parfaitement sans apport d'information*)

Soit P une preuve interactive d'un problème de décision Π et soit S un simulateur probabiliste de transcription. On suppose qu'aussi bien P que S s'éxécutent en temps polynomial.

Si x est une instance positive de Π, on note $\mathcal{T}(x)$ l'ensemble des transcriptions possibles de l'application du protocole P à l'entrée x, et $\mathcal{F}(x)$ l'ensemble des transcriptions produites par le simulateur S pour l'entrée x.

Si $\mathcal{T}(x) = \mathcal{S}(x)$ pour toute entrée x, alors pour une transcription t, on note $p_T(t)$ (resp. $p_F(t)$) la probabilité que t soit produite par le protocole de preuve (resp. par le simulateur).

On dit que la preuve interactive P est parfaitement sans apport d'information pour Viola *s'il existe un simulateur S tel que pour toute transcription t, on a $p_T(t) = p_F(t)$ (*ie *le simulateur produit des transcriptions avec la même distribution de probabilité que l'interaction effective).*

Bien qu'on ne définit pas clairement ce qu'est *l'information* dans cette preuve, il est clair que si Viola au lieu de lire les messages que lui envoie Prospéro peut tout aussi bien lire ceux générés par une machine randomisée, c'est que Prospéro ne peut pas réellement lui apprendre quelque chose de nouveau.

On s'attend maintenant à ce que cette définition soit cohérente avec l'exemple précédent. Montrons-le.

Proposition 2.2

La preuve interactive du problème de l'isomorphisme de graphe est parfaitement sans apport d'information pour Viola.

Démonstration : Comme précédemment σ désigne un isomorphisme entre G_1 et G_2.

Prospéro tire à chaque passe une permutation π au hasard, et renvoie de façon équiprobable (tant que Viola suit le protocole) ou bien π, ou bien $\sigma\pi$. Comme σ est fixe, la permutation $\sigma\pi$ apparait, comme π, de façon équiprobable dans l'ensemble des permutations.

Un simulateur qui, de façon équiprobable, tire n fois un entier entre 1 et 2 et une permutation à n éléments reproduit donc des transcriptions identiques à celles produites par la preuve interactive. ■

Dans la preuve, on a supposé que Viola suivait à la lettre le protocole, c'est-à-dire qu'elle laissait au hasard le soin de choisir sur lequel des deux graphes elle allait poser une question. Viola pourrait par exemple, à chaque passe, choisir $i = 1$.

Intuitivement, on ne voit pas pourquoi ce choix apporterait plus d'information à Viola, cependant il n'est plus immédiat de voir que le protocole est encore sans apport d'information, et on ne le montrera pas ici. Dans [2], on étend la définition des preuves parfaitement sans apport d'information pour montrer la robustesse de la preuve précédente à la fuite d'information, même quand Viola n'en fait qu'à sa tête.

3 Des preuves sans apport d'information pour les problèmes NP

Il est naturel de se demander quelles sont les classes de problème qui admettent des preuves sans apport d'information. Dans cette partie, on montrera que de telles preuves existent pour tous les problèmes NP.

On commencera par exhiber une preuve sans apport d'information pour la 3-coloriabilité d'un graphe, puis on utilisera la NP-complétude de ce problème pour aboutir au résultat voulu.

3.1 Engagement de bit

On commence par présenter ce qui sera un outil essentiel au moment de prouver la 3-coloriabilité : *l'engagement de bit*.

On souhaite disposer d'une façon pour Prospéro de s'engager sur un message auprès de Viola, sans le lui montrer sur le moment, mais en gardant la possibilité de le faire plus tard. Par s'engager, on entend que Prospéro ne pourra plus modifier son message une fois celui engagé.

Définition 3.1 (*Procédé d'engagement de bit*)

Soit une fonction $f : \{0,1\} \times X \to Y$, avec X un ensemble de clé et Y un ensemble d'arrivée. La forme chiffrée $f(b,x)$ du bit b par la clé x est appelée blob *de b.*

On dit que f est un procédé d'engagement de bit si les deux propriétés informelles suivantes sont vérifiées :

1. Dissimulation *: Viola ne peut pas déterminer le bit b à partir d'un blob $f(b,x)$.*
2. Engagement *: Prospéro peut, plus tard, ouvrir le blob en donnant la clé x à Viola, mais ne sait pas comment ouvrir un blob à la fois sur 0 et sur 1.*

Informellement, la fonction f doit donc être suffisament obscure pour que Viola ne sache pas l'inverser, et construite de telle sorte que Prospéro ne puisse trouver un blob ouvrable sur deux bits différents.

On trouve une description d'une telle fonction dans [1], utilisant le *chiffrement probabiliste de Goldwasser-Micali*. La dissimulation de ce procédé d'engagement se fonde essentiellement sur la difficulté de la résiduosité quadratique.

Pile ou face par téléphone On peut trouver une application amusante à l'existence de procédé d'engagement de bit : jouer à pile ou face par téléphone. Si deux personnes (Ariel et Caliban) souhaitent obtenir le résultat non biaisé d'un lancer de pièce en ne communiquant que par téléphone, alors bien sûr, aucun d'eux ne peut de son côté lancer une pièce, puisque l'autre ne pourrait vérifier la manipulation. Cependant, imaginons que par exemple Ariel tire un bit au hasard et l'engage ensuite en un blob y qu'il transmet à Caliban. Caliban tente ensuite de deviner de quel bit il s'agit, et Ariel lui permet de vérifier sa conjecture en ouvrant le blob.

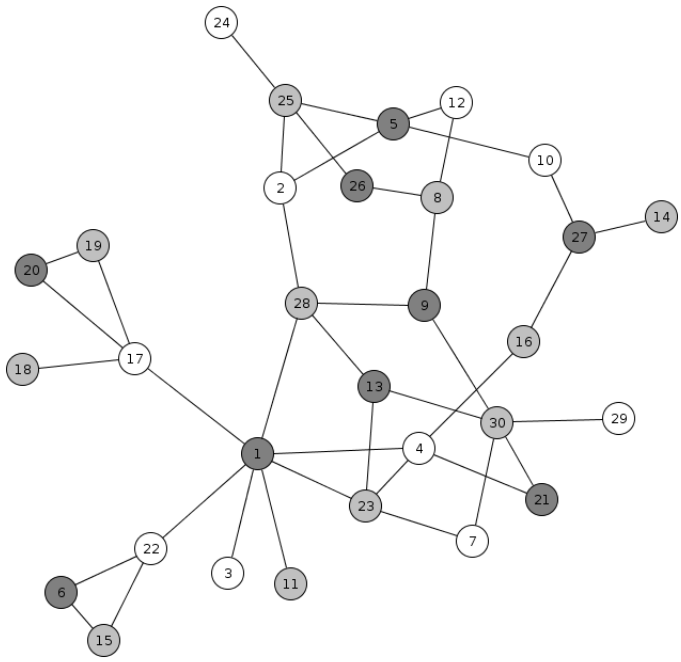
Sil'on déclare que le résultat est "Face" si Caliban avait vu juste et "Pile" sinon, alors Ariel et Caliban sont parvenu à jouer de façon totalement équitable à pile ou face par téléphone.

3.2 Preuve de la 3-coloriabilité

Définition 3.2 (*3-Coloriabilité*)

On dit qu'un graphe $G = (S, A)$ est 3-coloriable s'il existe une fonction $\phi : S \to \{1, 2, 3\}$ (de coloration) vérifiant $\forall \{u, v\} \in A, f(u) \neq f(v)$.De façon informelle, : la fonction de coloration doit associer des couleurs distinctes à des sommets reliés entre eux.

On note G3C le langage des instances positives de ce problème.



Une 3-coloration de graphe

On suppose que Prospéro dispose d'un procédé d'engagement de bit, qui lui permet (en l'étendant facilement aux chaînes de bits) de s'engager sur un message quelconque auprès de Viola. Le protocole suivant établit la 3-coloriabilité d'un graphe.

Protocole 3

Entrée : Un graphe $G = (S, A)$, à n sommets et et m arêtes.
Répéter m^2 fois les opérations suivantes :

1. *Prospéro établit une 3-coloration aléatoire du graphe G. Comme il connait une 3-coloration de G, il lui suffit simplement de permuter les couleurs.*
2. *Prospéro s'engage sur cette coloration : il engage séparément les n sommets, chaque sommet est engagé avec la couleur choisie à l'étape 1.*
3. *Prospéro envoie les n blobs obtenus à Viola*
4. *Viola choisit une arête a du graphe au hasard, et demande à Prospéro de lui donner les couleurs des extrémités de a dans la coloration calculée en 1.*
5. *Prospéro s'exécute en envoyant les deux clés des blobs concernés.*
6. *Viola constate que les couleurs des extrémités sont bien différentes.*

Viola accepte la preuve si et seulement si à chacune des m^2 étapes, les clés données par Prospéro ouvraient bien les blobs, et que les couleurs données étaient bien différentes.

Proposition 3.3

Ce protocole constitue une preuve sans apport d'information du problème de 3-coloriabilité.

Démonstration : Il y a trois propriétés à vérifier :

Consistance : Claire. On a vu que Prospéro n'avait aucun mal à générer une coloration aléatoire à chaque passe, pour peu que le graphe d'entrée soit 3-coloriable ;

Significativité : Si le graphe n'est pas 3-coloriable, alors une des arêtes au moins n'est pas bien coloriée par Prospéro dans la phase 1. Si Viola suit bien le protocole, elle choisira cette arête à la phase 4 avec une probabilité $1/m$. Prospéro peut donc espérer duper Viola en m^2 phases avec une probabilité inférieure à :

$$\left(1 - \frac{1}{m}\right)^{m^2}$$

On a $(1 - 1/m)^{m^2} = O(e^{-m})$, donc la preuve est significative.

Apport nul d'information : Les seules informations révélées à Viola à chaque passe sont les couleurs distinctes des deux sommets choisis au hasard. Ceux-ci peuvent être simulés par un couple d'entiers distincts pris au hasard dans $\{1, 2, 3\}^2$, tout simplement. ■

La même remarque que pour le problème d'isomorphisme de graphes s'applique. On suppose que Viola "joue le jeu" et qu'elle choisit aléatoirement les questions qu'elle pose à Prospéro. Sans cette hypothèse, la preuve précédente ne tient plus.

3.3 Preuves de problèmes NP

On peut à partir de la preuve précédente montrer l'existence de preuves sans apport d'information pour tous les problèmes NP. On rappelle sans le démontrer le résultat suivant :

Théorème 3.4

G3C est NP-complet.

On en déduit facilement le théorème central de cette présentation :

Théorème 3.5 (*Existence de preuves sans apport d'information pour les problèmes NP*)

Si l'on dispose d'un procédé d'engagement de bit sûr, alors pour tout problème dans NP, il existe un protocole de preuve interactif sans apport d'information prouvant ce problème.

Démonstration : Soit L un problème NP, et soit t la réduction (inversible, et calculable en temps polynomial) de L à G3C. On peut trouver t en composant la réduction de L à 3SAT et celle de 3SAT à G3C. On sait donc que x est une instance positive de L si et seulement si le graphe $t(x)$ est 3-coloriable.

On construit alors trivialement un protocole de preuve pour L, en faisant, pour une entrée x calculer à Viola et Prospéro le graphe $t(x)$. On laisse ensuite Prospéro prouver à Viola que $t(x)$ est 3-coloriable par la méthode décrite précédemment. Ce protocole est bien une preuve interactive sans apport d'information d'après la proposition 3.3, essentiellement parce que t est calculable en temps polynomial. ■

4 Le protocole d'identification de Fiat-Shamir

Pour conclure, on présente une application pratique des preuves sans divulgation d'information : les protocoles d'identification. La problématique est ici différente : Prospéro veut prouver à Viola qu'il est bien Prospéro. Pour ce faire, on suppose que Prospéro (et lui seul) possède un secret, et c'est en prouvant (sans le lui communiquer) à Viola qu'il connait ce secret qu'il parviendra à prouver qu'il est bien lui.

Le protocole de Fiat-Shamir que l'on présente ici, bien que maintenant obsolète, est la pierre angulaire de protocoles utilisés dans des systèmes modernes : Feige-Fiat-Shamir, ou Guillou-Quisquater.

Protocole 4 (*Fiat-Shamir*)

Initialisation

1. *Horatio, une personne de confiance choisit et publie un entier $n = pq$, avec p et q premiers, mais garde ces derniers secrets.*
2. *Prospéro se choisit un secret s : un entier premier avec n. Il calcule le résidu quadratique $v = s^2 \mod n$, et l'enregistre auprès d'Horatio comme sa clé publique.*

Protocole d'identification *Répéter t fois les étapes suivantes :*

1. *Prospéro choisit un entier r au hasard entre 1 et $n-1$ et envoie $x = r^2 \mod n$ à Viola*
2. *Viola choisit au hasard un entier e entre 0 et 1 et l'envoie à Prospéro.*
3. *Si $e = 0$, Prospéro envoie à Viola l'entier $y = r$. Dans le cas contraire, il lui envoie l'entier $y = rs \mod n$.*
4. *Viola vérifie que $xv^e \equiv y^2 \mod n$.*

Si à chacune des t passes la vérification effectuée par Viola est correcte, alors Viola accepte la preuve. Elle la rejette sinon.

Théorème 4.1

Le protocole d'identification de Fiat-Shamir constitue une preuve interactive que Prospéro connait bien son secret s. Cette preuve est de plus sans apport d'information pour Viola.

Démonstration : *Consistance et Significativité* : Ces deux propriétés sont claires, et se montrent sur le même modèle que les preuves précédentes. La probabilité pour un imposteur de réussir à se faire passer pour Prospéro est de 2^{-t}.

Apport nul d'information : Les deux entiers que Prospéro montre à Viola sont $x = r^2$, et y, qui vaut soit r, soit rs. On peut générer la paire (x, y) en commençant par choisir y au hasard, puis en prenant pour x soit y^2, soit y^2/v, au hasard. La distribution de ces couples d'entiers est la même que ceux générés par le protocole. ■

5 Conclusion

Dans cette présentation, on a volontairement fait l'impasse sur des raffinements sur la définition des preuves, en particulier quand le prouveur ne choisit pas ses questions au hasard ; ou quand l'on est obligé d'introduire un procédé d'engagement de bit. On trouvera dans [1] par exemple un définition de preuves *calculatoirement sans apport d'information.*

Les preuves sans apport d'information sont de formidables outils cryptographiques. Elles s'appliquent à une classe très étendue de problèmes (les problèmes NP), et trouvent aussi une utilité pratique dans des systèmes actuels d'information.

Références

[1] Stinson, *Criptography : Theory and Practice*, CRC Press, Boca Raton, 2002

[2] Goldreich, Micali, Wigderson, *Proofs that Yield Nothing but their Validity*, Journal of the ACM, volume 38, issue 3, Juillet 1991

[3] Goldwasser, Micali, Rackoff, *The Knowledge Complexity of Interactive Proof Systems*, SIAM Journal on Computing, 18, 1989

[4] Fiat, Shamir, *How to Prove Yourself : Practical Solutions to Identification and Signature Problems*, CRYPTO 1986