Introduction aux preuves interactives et au *zero-knowledge*

François Arnault • Université de Limoges • arnault@unilim.fr

1. Identification

Toujours basée sur la connaissance d'une donnée secrète. Pierre (le prouveur) s'identifie auprès de Vincent (le vérificateur) en prouvant qu'il connaît cette donnée secrète.

Identification par mot de passe

Protocole le plus faible : Pierre prouve qu'il connaît le secret en le donnant à Vincent.

Identification par signature

On utilise un schéma de signature. Le secret de Pierre est la clé secrète. Vincent utilise la clé publique pour vérifier la validité de la signature.

Pierre		**Vincent**
	$\xleftarrow{m}$	m message aléatoire
$s = \mathrm{Sign}(m)$	$\xrightarrow{s}$	s est signature valide de m ?

Schéma 1. Identification par signature

Le secret s'use (très lentement) quand on s'en sert. Vincent peut collecter la signature de 2, 3, 5, 7, 11, etc. Ensuite, il peut signer lui-même à peu près ce qu'il veut. (Coût en $L^{1/2}(N)$ pour RSA, soit 2^{50} en 1024 bits.)

Identification *zero-knowledge*

Convaincre Vincent que l'on connaît le secret, sans qu'aucun attaquant (espion des communications ou Vincent lui-même) ne puisse obtenir d'informations sur ce secret (autres que celles qu'il peut éventuellement obtenir à partir des données publiques).

2. Preuves interactives

Soit $\mathcal{D}$ un problème de décision. Comment prouver prouver qu'une instance donnée de $\mathcal{D}$ est vraie ? Si $\mathcal{D}$ est de classe NP, on peut tout simplement donner la preuve au vérificateur. Les systèmes de preuves interactives sont une méthode plus sophistiquée et plus puissante.

Graphes isomorphes

Le problème de l'isomorphie de deux graphes est un problème de décision. On considère une instance vraie de ce problème, soit deux graphes G_0 et G_1 et un isomorphisme $\pi : G_0 \to G_1$ qu'utilisera Pierre.

Pierre		**Vincent**
Permutation ϕ de G_1		
$H = \phi(G_1)$	$\xrightarrow{H}$	
	$\xleftarrow{r}$	$r \in \{0,1\}$
$\psi = \pi^{1-r} \circ \phi$	$\xrightarrow{\psi}$	$\psi(G_r) = H$?

Schéma 2. Preuve interactive d'isomorphie de deux graphes

Si les graphes sont effectivement isomorphes, alors Pierre parviendra à chaque fois à fournir une réponse satisfaisante pour Vincent. On dit que le protocole est *consistant*.

Si au contraire les graphes ne sont pas isomorphes, Pierre ou n'importe qui d'autre, ne pourra apporter la réponse qu'attend Vincent avec probabilité meilleure que 1/2. On dit que le protocole est *significatif*.

2.1. — Définition. Un *système de preuves interactives* pour un problème de décision $\mathcal{D}$ est un protocole entre un vérificateur V, algorithme probabiliste polynomial, et un prouveur P, algorithme de puissance non-bornée, satisfaisant les deux propriétés suivantes.

• *Consistance.* Pour tout instance vraie de $\mathcal{D}$, le vérificateur V atteint un état d'acceptation après interaction avec P.

• *Significativité.* Pour toute instance fausse de $\mathcal{D}$ et tout substitut P' à P, le vérificateur atteint un état de rejet après interaction avec P' avec probabilité $\geqslant 1/2$.

Le problème de l'isomorphie de graphes est de classe NP et on montre facilement que tout problème de classe NP admet un système de preuves interactives (le rôle de Vincent se limitant à fournir à Pierre un témoin de la validité de l'assertion). La *classe IP* des problèmes de décision admettant un système de preuves interactives contient donc la classe NP :

2.2. — Proposition. *On a l'inclusion NP $\subseteq$ IP.* □

Graphes non-isomorphes

Le problème complémentaire (la non-isomorphie) est de ce point de vue beaucoup plus intéressant parce que son appartenance à la classe NP est restée non-démontrée jusqu'à présent. Il admet pourtant lui aussi un système de preuves interactives.

Pierre		**Vincent**
		$r \in \{0,1\}$, permutation ϕ de G_r
	$\xleftarrow{H}$	$H = \phi(G_r)$
r' tel que $H \simeq G_{r'}$	$\xrightarrow{r'}$	$r' = r$?

Schéma 3. Preuve interactive de non-isomorphie de deux graphes

Comme le prouveur n'est pas limité en puissance de calcul, il peut trouver lequel des deux graphes G_0 ou G_1 est isomorphe à H. Le protocole est donc consistant. Il est aussi significatif puisque si G_0 et G_1 sont isomorphes la réponse r' de Pierre ne peut être égale à r qu'avec probabilité 1/2.

Le problème SAT est dans une situation semblable à l'isomorphie de graphes, à savoir qu'il est de classe NP et que son complémentaire admet aussi un système de preuves interactives (bien plus compliqué que celui qui vient d'être décrit). Toutefois, le problème SAT est NP-complet. On obtient donc :

2.3. — Théorème. *On a l'inclusion co-NP $\subseteq$ IP.* □

3. *Zero-knowledge*

Reprenons l'exemple de l'isomorphie de graphes. On peut simuler les échanges produits par Pierre et Vincent de la façon suivante.

On choisit l'un des deux graphes G_{r_0} (avec $r_0 \in \{0,1\}$) au hasard uniforme et une permutation ψ de ce graphe, produisant un graphe H isomorphe à G_{r_0}. On choisit ensuite une valeur r en suivant la stratégie de Vincent (qui peut dépendre de H). Si $r = r_0$ alors le résultat de la simulation est le triplet (H, r, ψ). Si $r \neq r_0$ alors on recommence la simulation au début, en espérant que le cas favorable $r = r_0$ finira par se produire. Puisque r_0 est choisit sans stratégie, il faut **en moyenne** deux tentatives pour que le cas favorable se produise.

$r_0 \in \{0,1\}$, $H = \psi(G_{r_0})$ permutation de G_{r_0}
$r \in \{0,1\}$, choisit selon la stratégie de Vincent
Si $r = r_0$ alors retourner (H, r, ψ), sinon recommencer.

Schéma 4. Simulation de l'interaction Pierre/Vincent

Les échanges produits par ce simulateur sont indiscernables (au sens de la théorie de l'information) de ceux que produit un échange entre Pierre et Vincent (même si ce dernier essaie de tricher en utilisant une stratégie dans le choix de r). Pourtant, le simulateur n'utilise pas d'isomorphisme entre G_0 et G_1 (il n'en "connaît" peut-être même pas). Ces échanges ne peuvent donc être d'aucune aide pour trouver l'isomorphisme utilisé dans le cas "réel".

3.1. — Définitions. • Un *simulateur* d'un couple (P, V) est algorithme probabiliste polynomial produisant des données indiscernables des échanges qui ont normalement lieu entre P et V lorsque une instance vraie de $\mathcal{D}$ est examinée

• Un système de preuves interactives (ou plus exactement le prouveur P) pour un problème de décision $\mathcal{D}$ est dit *zero-knowledge* si, pour n'importe quel vérificateur V', il existe un simulateur de (P, V').

3.2. — Propriété. *Le système de preuves interactives du schéma 2 est (parfaitement) zero-knowledge.* □

4. Engagement

L'engagement cryptographique d'un bit est un protocole permettant dans un premier temps de *dissimuler* un bit d'information (sceller une boîte contenant le bit d'information), et dans un deuxième temps de révéler l'information (ouvrir la boîte) *sans avoir pu modifier* l'information entre-temps.

Voici deux protocoles d'engagement d'un bit b utilisant la résidualité quadratique. Soit N un entier RSA. Le problème de la résidualité quadratique est celui de distinguer les (vrais) carrés modulo N des entiers non carrés modulo N mais de symbole de Jacobi 1 (les "faux carrés").

Méthode 1

	Pierre		**Vincent**
Paramètres :		N entier RSA, m **faux** carré modulo N	
Engagement :	$r \in \mathbb{Z}_N^*$, $e = m^b r^2$	$\xrightarrow{e}$	
Révélation :		$\xrightarrow{b,r}$	$e = m^b r^2$?

Schéma 5. Engagement, méthode 1

• Le bit est dissimulé sous l'hypothèse que Vincent n'a pas les moyens de reconnaître les résidus quadratiques (donc ne sait pas factoriser).

• Le bit est inconditionnellement non-modifiable.

Méthode 2

	Pierre		**Vincent**
Paramètres :		N entier RSA, m **vrai** carré modulo N	
Engagement :	$r \in \mathbb{Z}_N^*$, $e = m^b r^2$	$\xrightarrow{e}$	
Révélation :		$\xrightarrow{b,r}$	$e = m^b r^2$?

Schéma 6. Engagement, méthode 2

• La dissimulation du bit est inconditionnelle.

• Le bit est non-modifiable par Pierre sous l'hypothèse qu'il n'a pas le moyens de calculer une racine carrée de m (problème équivalent à factoriser N).

4.1. — Remarque. L'existence de schémas d'engagement est intimement lié à l'existence de fonctions à sens unique. On connaît en particulier les implications suivantes. S'il existe des fonctions à sens unique alors il existe des schémas d'engagement où la donnée est inconditionnellement non-modifiable (type 1). S'il existe des permutations à sens unique alors il existe des schémas d'engagement à dissimulation inconditionnelle (type 2). S'il existe des schémas d'engagement (type 1 ou 2), alors il existe des fonctions à sens unique.

5. Variantes

Graphes 3-colorables

Le problème de l'existence d'un 3-coloriage d'un graphe est NP-complet. Le protocole suivant est un système de preuves interactives de l'existence d'un 3-coloriage.

• Pierre : Numérote arbitrairement les 3 couleurs (de 1 à 3). Pour chaque sommet, engage le numéro de sa couleur. Envoie les engagements à Vincent.

• Vincent : Indique à Pierre une arête au hasard.

• Pierre : Dévoile les numéros des couleurs des extrémités de cette arête.

• Vincent : Vérifie que les engagements sont corrects, que les couleurs sont valides et différentes.

Propriétés nuancées

• Le protocole est consistant.

• Le protocole est "algorithmiquement significatif". En effet, soit m le nombre d'arêtes. En l'absence d'un 3-coloriage, Pierre ne pourra tromper Vincent qu'avec probabilité $\leqslant 1 - 1/m$. Il suffit d'itérer k fois avec $k \geqslant \ln 2 / \ln(m/(m-1))$ pour passer sous la barre des $1/2$.

• On peut simuler les échanges entre Pierre et Vincent en attribuant un numéro de couleur aléatoire à chaque sommet, en les engageant, et en choisissant ensuite une arête aléatoire en espérant que ses deux extrémités soient de couleurs distinctes.

• Avec l'engagement méthode 1, même un Pierre disposant d'une puissance de calcul infinie ne pourra pas tromper Vincent sur l'existence d'un isomorphisme. Le protocole est donc significatif et il s'agit d'une preuve interactive. Mais les données (vrais ou faux carrés) échangées, comparées à celles générées par un simulateur ne sont indistinguables qu'au sens algorithmique seulement. On a donc une **preuve** interactive **algorithmiquement *zero-knowledge***.

• Avec l'engagement méthode 2, on a un **argument** interactif (et non une preuve, parce qu'un Pierre disposant d'une puissance de calcul infinie peut faire croire à tort à l'existence d'un 3-coloriage), de ***zero-knowledge* parfait** (car les échanges sont parfaitement simulables).

6. Notes et références

Sachant que le problème de l'existence d'un 3-coloriage est NP-complet, la remarque 4.1 montre que, sous l'hypothèse de l'existence de fonctions à sens-unique, tout problème de la classe NP admet un système de preuves interactives algorithmiquement *zero-knowledge* (NP $\subseteq$ CZK). D'autre part, on peut montrer que tout système de preuves interactives peut-être rendu algorithmiquement *zero-knowledge* (IP = CZK). Enfin, Shamir a montré qu'un problème de décision admet un système de preuves interactives si et seulement si il peut être vérifié en utilisant une mémoire polynomialement bornée (IP = PSPACE).

Le contenu de ce document est extrait de :

[1] D. Stinson : *Cryptography : Theory and Practice.* CRC 1995.

[2] O. Goldreich : *Modern Cryptography, Probabilistic Proofs and Pseudo-randomness.* Springer 1999.

[3] I. Damgård : *Commitment schemes and Zero-knowledge protocols.* in: Lectures on Data Security, LNCS 1561, Springer 1999.