Les preuves sans divulgation de connaissances

Fabrice Mouhartem

Journée Alkindi, 30 mai 2018

École Normale Supérieure de Lyon

ENS DE LYON

Le problème de l'identification

Le problème de l'identification

Affirmation
Je suis le seul à connaître ce secret.

Le problème de l'identification

Affirmation
Je suis le seul à connaître ce secret.

Problème : Comment le prouver ?

1. Envoyer le secret ?
    - Non : Le vérifieur va alors connaître mon secret.

Le problème de l'identification

Affirmation
Je suis le seul à connaître ce secret.

Problème : Comment le prouver ?

1. Envoyer le secret ?
   - Non : Le vérifieur va alors connaître mon secret.
2. Prendre comme secret une signature, et signer un message demandé par le vérifieur ?
   - Encore trop, le vérifieur peut faire signer des messages de son choix.

Le problème de l'identification

Affirmation
Je suis le seul à connaître ce secret.

Problème : Comment le prouver ?

1. Envoyer le secret ?
   - Non : Le vérifieur va alors connaître mon secret.
2. Prendre comme secret une signature, et signer un message demandé par le vérifieur ?
   - Encore trop, le vérifieur peut faire signer des messages de son choix.
3. Prendre une clef privée comme secret et déchiffrer un message ?
   - Toujours trop, le vérifieur peut déchiffrer un message [Ble98].

Ce qu'on voudrait

Intuition
Prouver la connaissance d'un secret sans révéler plus d'information.

Ce qu'on voudrait

Intuition
Prouver la connaissance d'un secret sans révéler plus d'information.

Deux questions :

1. Que signifie prouver ?
2. Que signifie « révéler de l'information » ?

Mais que veut-dire prouver ?

Preuve Mathématique

- Non-interactive
- Doit convaincre le lecteur

Mais que veut-dire prouver ?

Preuve Mathématique

- Non-interactive
- Doit convaincre le lecteur

Ici, la preuve est :

- Interactive
- Destinée à convaincre son interlocuteur

Mais que veut-dire prouver ?

Preuve Mathématique

- Non-interactive
- Doit convaincre le lecteur

Ici, la preuve est :

- Interactive
- Destinée à convaincre son interlocuteur
    - Utile pour préserver l'anonymat

Mais que veut-dire prouver ?

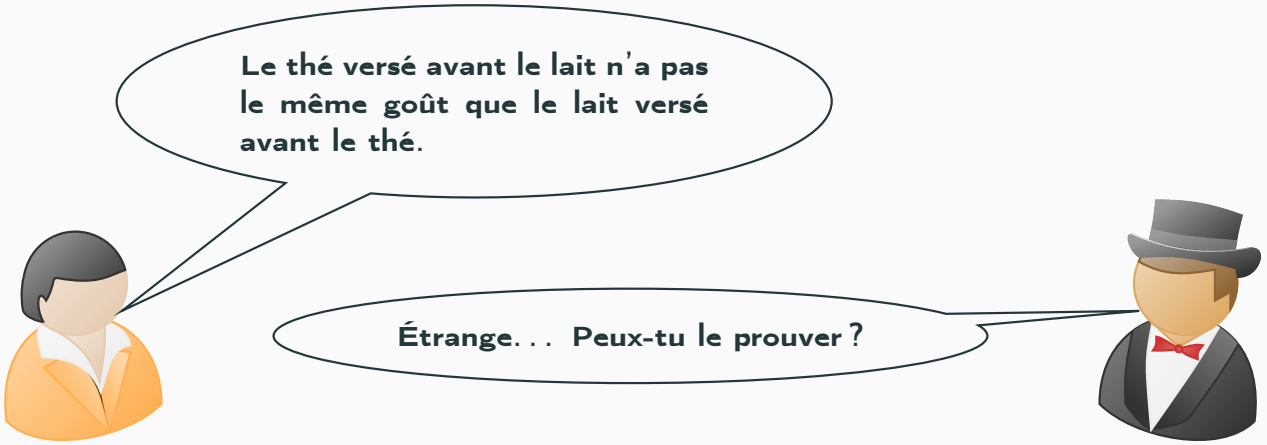
Preuve Mathématique

- Non-interactive
- Doit convaincre le lecteur

Ici, la preuve est :

- Interactive
- Destinée à convaincre son interlocuteur
  - Utile pour préserver l'anonymat
- Probabiliste

Preuve interactive



Inspiré de « *Mathematics of a Lady Testing Tea* », Ronald Fisher, 1956.

Preuve interactive

1. Le vérifieur commence par lancer une pièce pour choisir s'il met le lait ou le thé en premier.

Preuve interactive

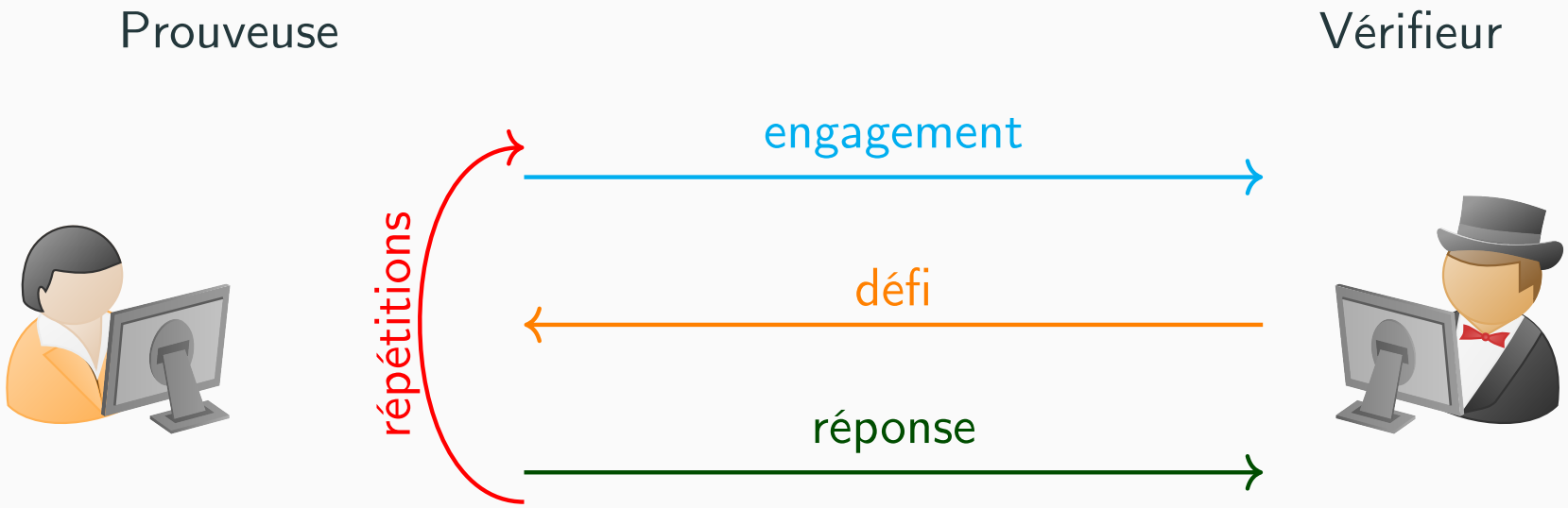
1. Le vérifieur commence par lancer une pièce pour choisir s'il met le lait ou le thé en premier.
2. La prouveuse devine.
   - Si elle sait distinguer, c'est toujours vrai.
   - Si les deux recettes sont identiques, elle a une chance sur deux de deviner correctement.

Preuve interactive

1. Le vérifieur commence par lancer une pièce pour choisir s'il met le lait ou le thé en premier.
2. La prouveuse devine.
   - Si elle sait distinguer, c'est toujours vrai.
   - Si les deux recettes sont identiques, elle a une chance sur deux de deviner correctement.
3. Si on répète 20 fois, la prouveuse a une chance sur un million de tout deviner correctement.

Définition plus formelle

Une preuve interactive met en jeu deux acteurs : la prouveuse et le vérifieur.



Après un certain nombre de répétitions, on peut être sûr que la prouveuse n'a pas triché.

Preuves sans divulgation de connaissances

Pour être correcte et sûre, une preuve sans divulgation doit vérifier les propriété suivantes :

Preuves sans divulgation de connaissances

Pour être correcte et sûre, une preuve sans divulgation doit vérifier les propriété suivantes :

Cohérence Si tout le monde suit le protocole correctement, alors le vérifieur accepte.

Robustesse Si le prouveur ne connaît pas son secret, alors il ne peut pas convaincre le vérifieur sauf avec de la chance.

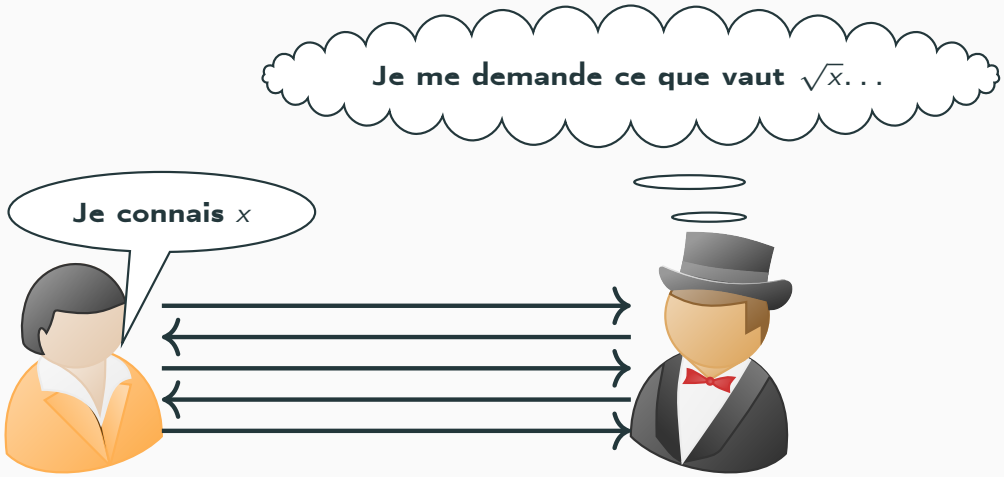
Zero-Knowledge Le vérifieur ne peut pas obtenir plus d'information sur le secret que sa connaissance par le prouveur.

Qu'est-ce que la connaissance ?

Exemple

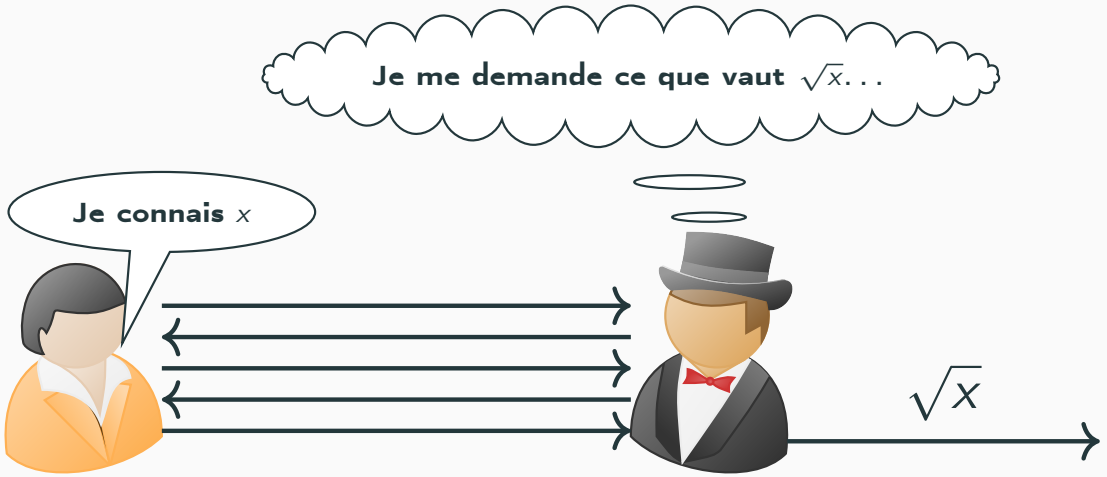
Qu'est-ce que la connaissance ?

Exemple



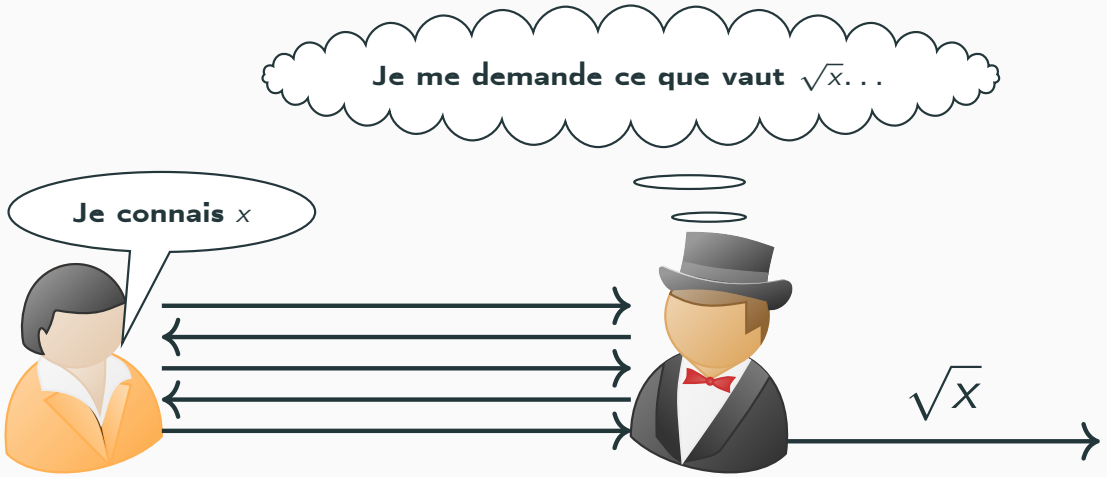
Qu'est-ce que la connaissance ?

Exemple



Qu'est-ce que la connaissance ?

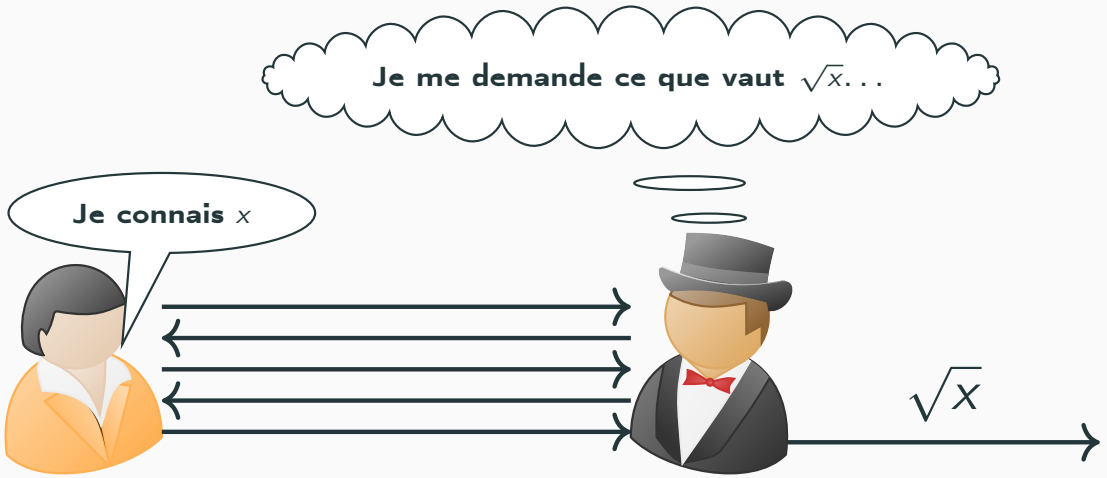
Exemple



Cette situation est mauvaise si le vérifieur ne peut calculer $\sqrt{x}$ sans l'interaction !

Qu'est-ce que la connaissance ?

Exemple



Cette situation est mauvaise si le vérifieur ne peut calculer $\sqrt{x}$ sans l'interaction !

Une définition de la "connaissance"
Tout ce que le prouveur peut calculer après l'interaction (ou l'enregistrement), il pouvait le connaître avant.

Un paradoxe ?

La situation

- L'interaction doit convaincre le vérifieur d'un fait nouveau
- Le vérifieur doit pouvoir générer l'enregistrement lui même

Un paradoxe ?

La situation

- L'interaction doit convaincre le vérifieur d'un fait nouveau
- Le vérifieur doit pouvoir générer l'enregistrement lui même



Un paradoxe ?

La situation

- L'interaction doit convaincre le vérifieur d'un fait nouveau
- Le vérifieur doit pouvoir générer l'enregistrement lui même



— Pauline sait reconnaître le thé versé avant le lait de l'inverse
— Vraiment ?
— Regarde ces tasses qu'elle a su identifier !
— N'importe qui peut étiqueter des tasses vides...
— Mais j'étais là...

Un paradoxe ?

La situation

- L'interaction doit convaincre le vérifieur d'un fait nouveau
- Le vérifieur doit pouvoir générer l'enregistrement lui même



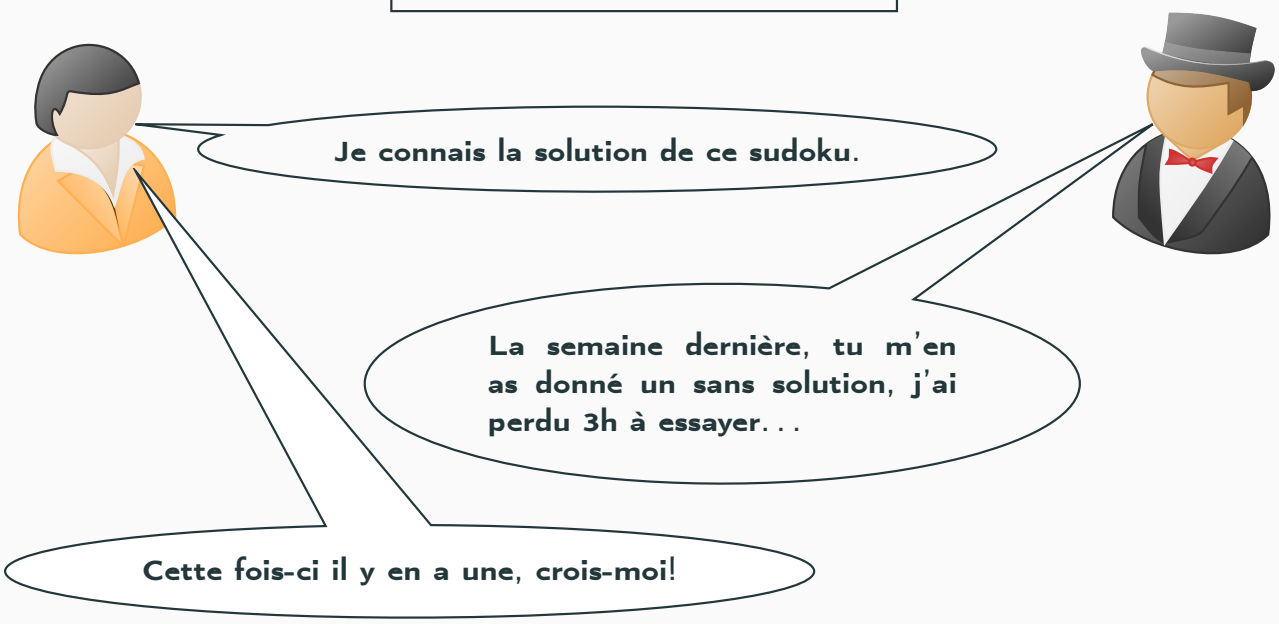
— Pauline sait reconnaître le thé versé avant le lait de l'inverse
— Vraiment ?
— Regarde ces tasses qu'elle a su identifier !
— N'importe qui peut étiqueter des tasses vides. . .
— Mais j'étais là. . .

→ Le vérifieur est le seul à savoir comment les enregistrements ont été produits

Exemple : le sudoku

Exemple : le sudoku

5	3			7				
			1		5			
		8					6	
8								3
			8					1
7				2				
	6					2		
			4	1				
				8			7	



Exemple : le sudoku

5	3	4	8	5	9	9	6	1
6	7	2	4	2	6	2	8	7
1	9	8	7	1	3	3	4	5
6	7	8	7	6	1	5	3	7
1	9	5	8	5	3	4	1	9
3	4	2	9	2	4	2	8	6
9	1	2	4	2	3	2	8	4
3	4	8	7	9	1	6	3	5
5	6	7	8	5	6	1	7	9

Exemple : le sudoku

1. Renommer les nombres
   $(1 \mapsto 8, 2 \mapsto 4, \ldots)$

9	4	6	7	2	1	5	3	8
7	2	8	3	5	9	4	6	1
3	5	1	4	6	8	9	7	2
1	9	5	2	7	3	6	8	4
6	8	7	1	9	4	2	5	3
2	3	4	5	8	6	1	9	7
5	7	3	9	4	2	8	1	6
8	1	2	6	3	5	7	4	9
4	6	9	8	1	7	3	2	5

Exemple : le sudoku

1. Renommer les nombres ($1 \mapsto 8, 2 \mapsto 4, \ldots$)
2. Cacher les nombres
3. Demander si on dévoile :
4. Vérifier la cohérence

0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Exemple : le sudoku

1. Renommer les nombres ($1 \mapsto 8, 2 \mapsto 4, \ldots$)
2. Cacher les nombres
3. Demander si on dévoile :
   - Une ligne
4. Vérifier la cohérence

0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
6	8	7	1	9	4	2	5	3
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Exemple : le sudoku

1. Renommer les nombres ($1 \mapsto 8, 2 \mapsto 4, \ldots$)
2. Cacher les nombres
3. Demander si on dévoile :
   - Une ligne
   - Une colonne
4. Vérifier la cohérence

0	0	6	0	0	0	0	0	0
0	0	8	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0
0	0	5	0	0	0	0	0	0
0	0	7	0	0	0	0	0	0
0	0	4	0	0	0	0	0	0
0	0	3	0	0	0	0	0	0
0	0	2	0	0	0	0	0	0
0	0	9	0	0	0	0	0	0

Exemple : le sudoku

1. Renommer les nombres ($1 \mapsto 8, 2 \mapsto 4, \ldots$)
2. Cacher les nombres
3. Demander si on dévoile :
   - Une ligne
   - Une colonne
   - Une case 3×3
4. Vérifier la cohérence

0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
1	9	5	0	0	0	0	0	0
6	8	7	0	0	0	0	0	0
2	3	4	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Exemple : le sudoku

1. Renommer les nombres ($1 \mapsto 8, 2 \mapsto 4, \ldots$)
2. Cacher les nombres
3. Demander si on dévoile :
   - Une ligne
   - Une colonne
   - Une case 3×3
   - Les cases initiales
4. Vérifier la cohérence

5	3	0	0	5	0	0	0	0
0	0	0	4	0	6	0	0	0
0	0	8	0	0	0	0	4	0
6	0	0	0	0	0	0	0	7
0	0	0	8	0	0	0	0	9
3	0	0	0	2	0	0	0	0
0	1	0	0	0	0	2	0	0
0	0	0	7	9	0	0	0	0
0	0	0	0	5	0	0	7	0

Exemple : le sudoku

1. Renommer les nombres ($1 \mapsto 8, 2 \mapsto 4, \ldots$)
2. Cacher les nombres
3. Demander si on dévoile :
   - Une ligne
   - Une colonne
   - Une case 3×3
   - Les cases initiales
4. Vérifier la cohérence
5. Répéter n fois

5	3	0	0	5	0	0	0	0
0	0	0	4	0	6	0	0	0
0	0	8	0	0	0	0	4	0
6	0	0	0	0	0	0	0	7
0	0	0	8	0	0	0	0	9
3	0	0	0	2	0	0	0	0
0	1	0	0	0	0	2	0	0
0	0	0	7	9	0	0	0	0
0	0	0	0	5	0	0	7	0

Exemple : le sudoku

Remarque
Si la prouveuse peut répondre à tous les défis correctement, alors le sudoku originel avait une solution.

Exemple : le sudoku

Remarque
Si la prouveuse peut répondre à tous les défis correctement, alors le sudoku originel avait une solution.

Si la prouveuse triche, alors au moins un dévoilement pourrait être incohérent.

Exemple : le sudoku

Remarque
Si la prouveuse peut répondre à tous les défis correctement, alors le sudoku originel avait une solution.

Si la prouveuse triche, alors au moins un dévoilement pourrait être incohérent.

- Il y a 9+9+9+1 = 28 défis possibles.

Exemple : le sudoku

Remarque
Si la prouveuse peut répondre à tous les défis correctement, alors le sudoku originel avait une solution.

Si la prouveuse triche, alors au moins un dévoilement pourrait être incohérent.

- Il y a 9+9+9+1 = 28 défis possibles.
- La prouveuse réussit donc à répondre au challenge avec une probabilité au plus $\frac{27}{28}$
- Au bout de 2500 essais, la probabilité qu'elle réussisse à répondre à tous les défis est inférieure à 1%.

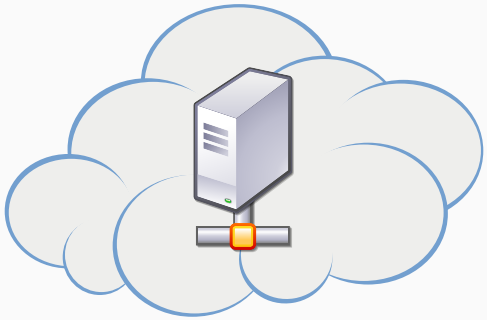
Exemple : le sudoku

Figure 1 – Une réalisation pratique à l'aide de cartes :
`http://www.wisdom.weizmann.ac.il/~naor/PAPERS/SUDOKU_DEMO/`

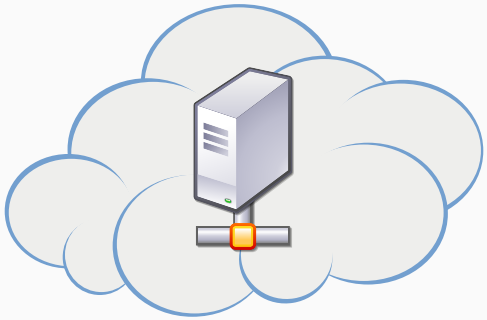
Applications

Applications

Applications



Applications



C'est une construction importante en cryptographie moderne !

Conclusion

- C'est une construction qui permet de prouver quelque chose tout en protégeant les données

- C'est une brique de base importante pour la construction de primitives plus complexes
- Il existe des preuves sans divulgation de connaissances pour une grande classe de problèmes en informatique

Conclusion

- C'est une construction qui permet de prouver quelque chose tout en protégeant les données

- C'est une brique de base importante pour la construction de primitives plus complexes
- Il existe des preuves sans divulgation de connaissances pour une grande classe de problèmes en informatique

Ce n'est pas la bonne solution pour donner un cours

- Les élèves sont convaincu de la connaissance de l'enseignant...
- ...mais n'apprennent rien

Remerciements & Références

Merci de votre attention.

R. Gradwohl, M. Naor, B. Pinkas et G. Rothblum.
Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles.
À *Theory of Computing Systems*. 2009.

M. Rosulek.
Zero-Knoweldge Proofs, with applications to Sudoku & Where's Waldo ?
Cours en ligne. 2008.
`http://web.engr.oregonstate.edu/~rosulekm/pubs/zk-waldo-talk.pdf`