Sur les preuves sans divulgation de connaissances

Fabrice Mouhartem

Fête de la Science

15/10/2016

ENS DE LYON

fête de la Science

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].

Preuve sans divulgation de connaissances

Intuition

Prouver la connaissance d'un secret sans donner d'autres information.

Preuve sans divulgation de connaissances

Intuition

Prouver la connaissance d'un secret sans donner d'autres information.

Applications :

Preuve sans divulgation de connaissances

Intuition

Prouver la connaissance d'un secret sans donner d'autres information.

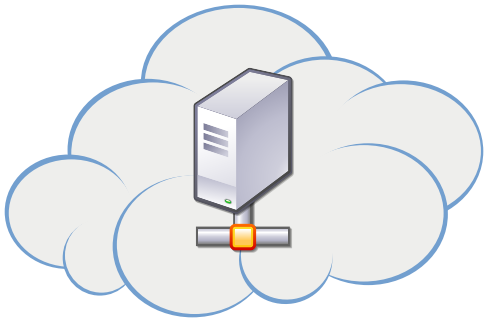
Applications :

Preuve sans divulgation de connaissances

Intuition

Prouver la connaissance d'un secret sans donner d'autres information.

Applications :

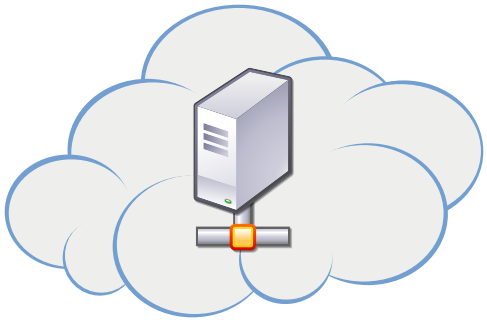


Preuve sans divulgation de connaissances

Intuition

Prouver la connaissance d'un secret sans donner d'autres information.

Applications :



C'est une construction importante en cryptographie moderne !

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 :

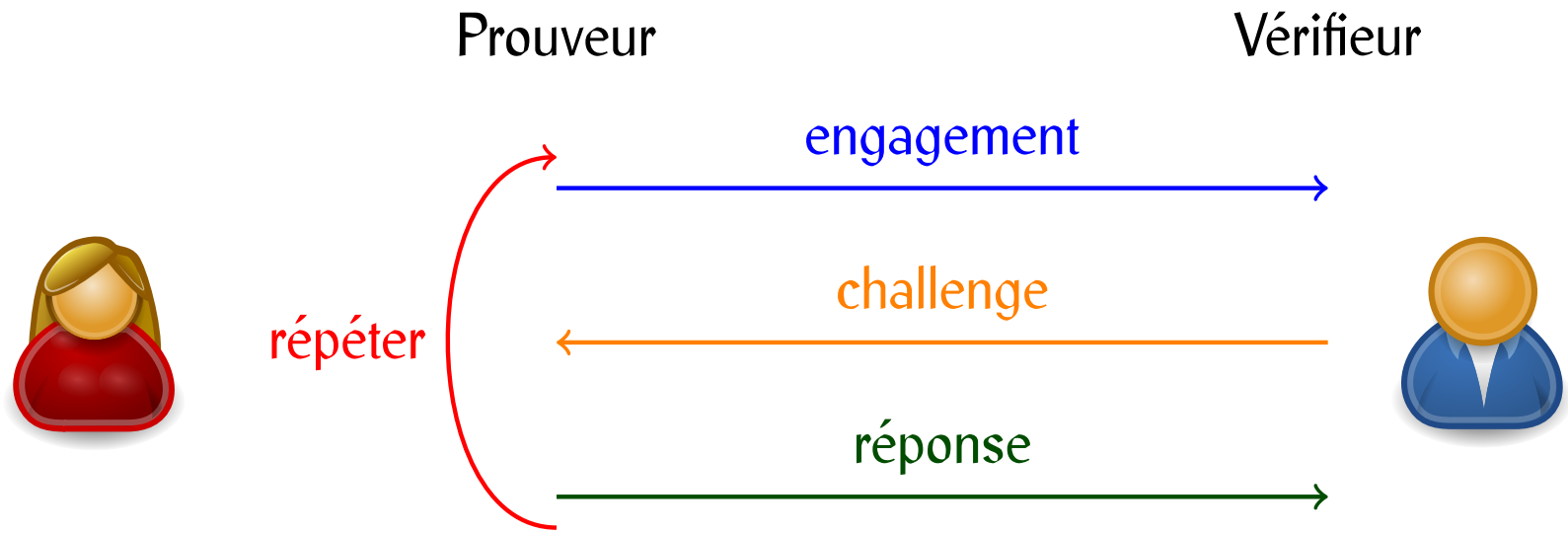
- Interactive
- Destinée à convaincre son interlocuteur
  - Utile pour préserver l'anonymat
- Probabiliste

Preuves sans divulgation de connaissances

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

Preuves sans divulgation de connaissances

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



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

Preuves sans divulgation de connaissances

Pour être correcte, une preuve ZK doit vérifier les propriété suivantes :

Preuves sans divulgation de connaissances

Pour être correcte, une preuve ZK 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.

Preuves sans divulgation de connaissances

Pour être correcte, une preuve ZK doit vérifier les propriété suivantes :

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

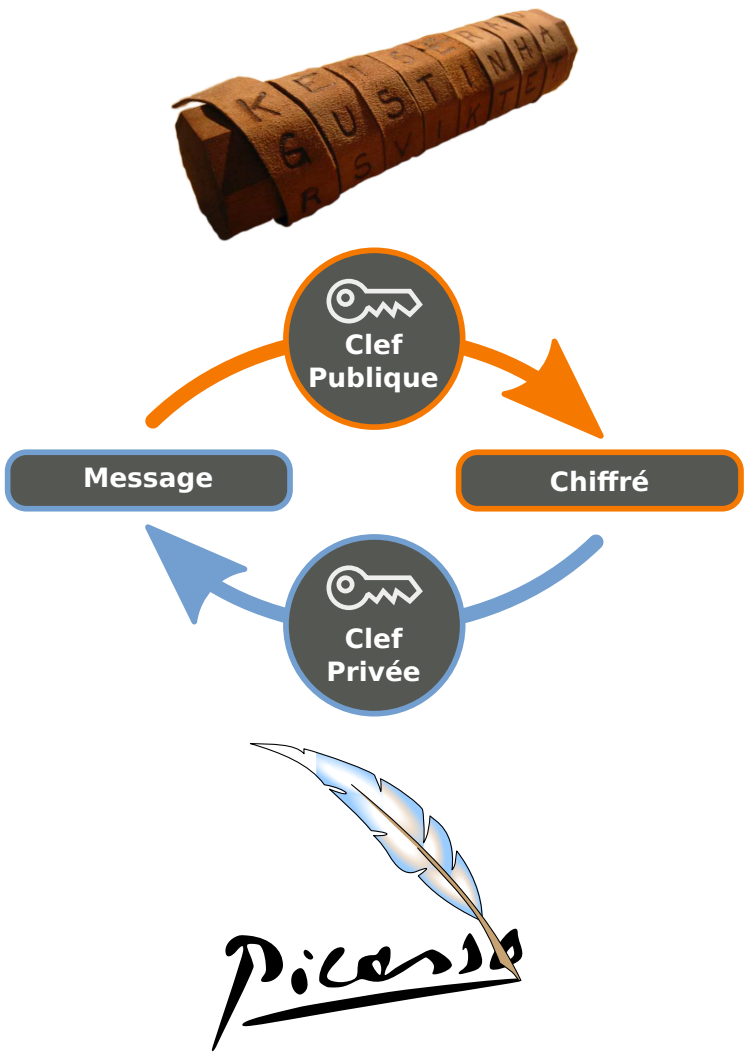
Robustesse Si le prouveur ne connaît pas son secret, alors il ne peut pas convaincre le vérifieur sauf avec de la chance.

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

Cela se formalise proprement, mais on va laisser ça sous le tapis :

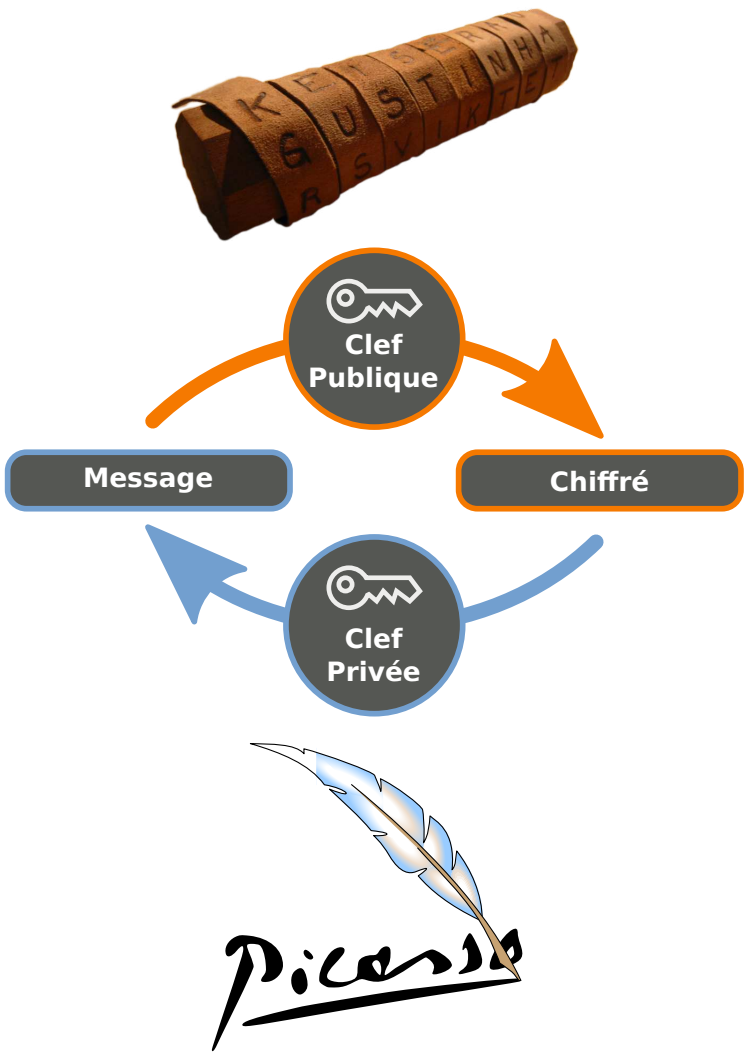
$$\forall (P, V) \in \mathrm{ZK}(R), \forall \hat{V} \in \mathrm{PPT}(\lambda), \exists S \in \mathrm{PPT}(\lambda),$$
$$\forall (x, w) \in R, \forall a \in \{0,1\}^*, \mathrm{Rec}\left\langle P(x,w), \hat{V}(x)\right\rangle = S(x).$$

Primitive Cryptographique



Une primitive cryptographique est la donnée d'un protocole à suivre et de notions de sécurités, comme les preuves sans divulgation de connaissances, mais aussi le chiffrement, la signature...

Primitive Cryptographique



Une primitive cryptographique est la donnée d'un protocole à suivre et de notions de sécurités, comme les preuves sans divulgation de connaissances, mais aussi le chiffrement, la signature...

Ce sont les briques de base de la cryptographie, et sont utilisées pour construire des primitives plus complexes.

Merci de votre attention

Références (en anglais) :

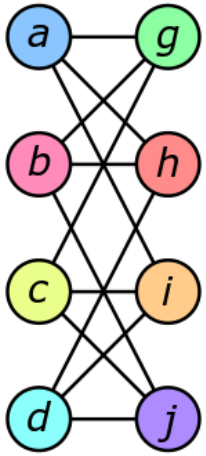
Ivan Damgård et Jesper Buus Nielsen.
Commitment Schemes and Zero Knowledge Protocols.

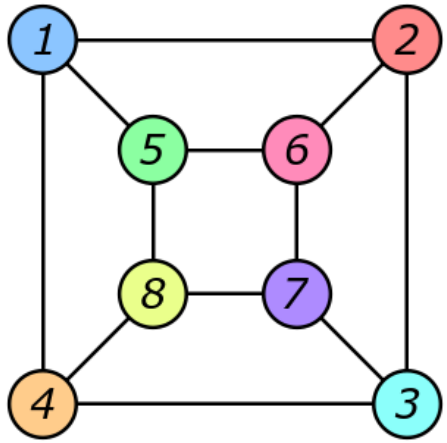
Ivan Damgård.
On Σ-protocols.

Benoît Libert.
Cours de MI sur les preuves sans divulgation de connaissances.
http://perso.ens-lyon.fr/benoit.libert/cours-ZK.pdf

Isomorphisme de graphe

Deux graphes (V_1, E_1), (V_2, E_2) sont isomorphes s'il existe une bijection $f : V_1 \to V_2$ telle que $(x_1, x_2) \in E_1 \implies (f(x_1), f(x_2)) \in E_2$.





- Il n'existe pas d'algorithme *efficace* pour décider si deux graphes sont isomorphes ;
- Babai a montré en 2015 qu'il existait un algorithme « presque efficace » pour le décider

Isomorphisme de graphe

À prouver : connaissance d'un isomorphisme

$$f : G_1 = (V_1, E_1) \to G_2 = (V_2, E_2).$$

engagement Le prouveur envoie un graphe $G_3 = (E_3, V_3)$ construit comme suit :

1. Prendre une bijection aléatoire g de V_1 dans V_3.
2. Construire E_3 de telle manière à ce que G_1 et G_3 soient isomorphes.

challenge Le vérifieur demande 1 ou 2.

réponse
- Si le vérifieur a demandé 1, renvoyer g^{-1} (isomorphisme entre G_3 et G_1)
- Si le vérifieur a demandé 2, renvoyer $f \circ g^{-1}$ (isomorphisme entre G_3 et G_2)