

ch 2 : Diffie-Hellman et courbes elliptiques

I] Diffie-Hellman

II] Cryptographie à base de courbes elliptiques

① Diffie-Hellman sur un groupe

② Courbes elliptiques

$$E = \{(x,y) \in K^2, y^2 = x^3 + ax + b\} \cup \{O\}$$

$$K \text{ corps} \quad \text{avec } 4a^3 + 27b^2 \neq 0$$

$+$: opération d'addition de 2 points de E
définie par les familles d'addition

$$\begin{aligned} (\text{er : } P + O = O + P = P) \\ O + O = O \end{aligned}$$

Th: $(E, +)$ est un groupe commutatif

• Cardinal de E (nb de points de la courbe elliptique)
avec $K = \mathbb{Z}/p\mathbb{Z}$ (avec p premier)

Remarque: $y^2 = \underbrace{x^3 + ax + b}_{\text{est-ce un carré dans } \mathbb{Z}/p\mathbb{Z}} ?$

Propriété 1 : Soit p un nombre premier, $p \geq 3$

Parmi les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$, $\frac{p-1}{2}$ éléments
sont des carrés (et $\frac{p-1}{2}$ éléments n'en sont pas)

Preuve: Soit $\Phi : (\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$
 $\begin{cases} u & \mapsto u^2 \end{cases}$



Φ est un morphisme de groupes

• $\Phi(1) = 1$ homomorphisme

$$\bullet \forall u, v \in (\mathbb{Z}/p\mathbb{Z})^*, \quad \Phi(u \times v) = \underbrace{\Phi(u)}_{(uv)^2} \times \underbrace{\Phi(v)}_{u^2 \times v^2}$$

$$\bullet \forall u \in (\mathbb{Z}/p\mathbb{Z})^*, \quad \Phi(u^{-1}) = \underbrace{\Phi(u)}_{(u^{-1})^2}^{-1} = \underbrace{\Phi(u)}_{(u^2)^{-1}}$$

$$\ker \Phi = \{u \in (\mathbb{Z}/p\mathbb{Z})^* / \Phi(u) = 1\}$$

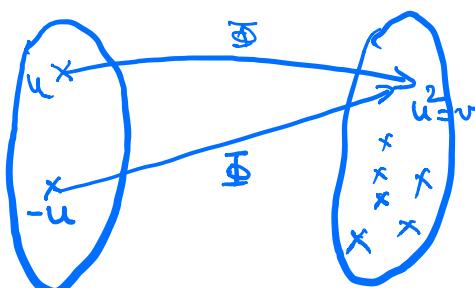
$$= \{u \in (\mathbb{Z}/p\mathbb{Z})^* / \underbrace{u^2 = 1}\}$$

$$= \{-1, +1\}$$

nb de solutions ≤ 2
car on est sur le cercle $K = \mathbb{Z}/p\mathbb{Z}$

$$\boxed{\text{Im } \Phi \simeq (\mathbb{Z}/p\mathbb{Z})^*/\ker \Phi}$$

$$\Rightarrow \underbrace{\text{Card Im } \Phi}_{\substack{\text{nombre de} \\ \text{cercles dans} \\ (\mathbb{Z}/p\mathbb{Z})^*}} = \frac{\text{Card } (\mathbb{Z}/p\mathbb{Z})^*}{\text{Card Ker } \Phi} = \frac{p-1}{2}$$



Remarque En particulier, si on prend un élément de $(\mathbb{Z}/p\mathbb{Z})^*$ tiré aléatoirement, il a 50% de chances d'être un carré

Propriété 2 : Soit p premier ≥ 3

Soit $u \in (\mathbb{Z}/p\mathbb{Z})^*$

u est un carré dans $(\mathbb{Z}/p\mathbb{Z})^* \Leftrightarrow u^{\frac{p-1}{2}} = 1 \pmod{p}$

Remarque : Ce critère est vérifiable en temps polynomial

On calcule $u^{\frac{p-1}{2}} \pmod{p}$ avec l'algorithme square and multiply

Preuve de la propriété 2 :

Sens \Rightarrow Supposons que u est un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$
Montrons que $u^{\frac{p-1}{2}} = 1 \pmod{p}$

u est un carré $\Rightarrow \exists v \in (\mathbb{Z}/p\mathbb{Z})^*/u = v^2$

Donc : $u^{\frac{p-1}{2}} = (v^2)^{\frac{p-1}{2}} = v^{p-1} = 1 \pmod{p}$

↑ petit th. de Fermat

Sens \Leftarrow $A = \{u \in (\mathbb{Z}/p\mathbb{Z})^* / u \text{ est un carré}\}$

$B = \{u \in (\mathbb{Z}/p\mathbb{Z})^* / u^{\frac{p-1}{2}} = 1 \pmod{p}\}$

équation polynomiale de degré $\frac{p-1}{2}$

On vient de montrer que $A \subseteq B$

D'après la propriété 1, $\boxed{\text{Card } A = \frac{p-1}{2}}$

De plus $\boxed{\text{Card } B \leq \frac{p-1}{2}}$ (car $\mathbb{Z}/p\mathbb{Z}$ est un corps)

(A et B sont des ensembles finis)

$\left. \begin{array}{l} A \subseteq B \\ \text{Card } B \leq \text{Card } A \end{array} \right\} \Rightarrow \boxed{A = B}$ (en particulier $B \subseteq A$)

ce qui termine la démonstration

Propriété 3 : Soit p un nombre premier tel que $p \equiv 3 \pmod{4}$

Soit $u \in (\mathbb{Z}/p\mathbb{Z})^*$ qui est un caré entier

$$\text{Alors } u = v^2 \Leftrightarrow v = \pm u^{\frac{p+1}{4}} \pmod{p}$$

analogie de \sqrt{u} dans les réels

$$\text{Preuve : } \left(u^{\frac{p+1}{4}}\right)^2 = u^{\frac{p+1}{2}} \pmod{p}$$

$$= u \times u^{\frac{p-1}{2}} \pmod{p}$$

= 1 car u est un caré
(propriété 2)

$$\Rightarrow \left(u^{\frac{p+1}{4}}\right)^2 = u \pmod{p}$$

Cardinal de E : $E = \{(x,y) \in \mathbb{Z}/p\mathbb{Z} \mid y^2 = x^3 + ax + b \} \cup \{0\}$

$$\text{Card } E = 0 \times \text{Card } \{x \in \mathbb{Z}/p\mathbb{Z} \mid x^3 + ax + b \text{ n'est pas un caré}\}$$

$$+ 2 \times \text{Card } \{x \in \mathbb{Z}/p\mathbb{Z} \mid x^3 + ax + b \text{ est un caré } \neq 0\}$$

$$+ 1 \times \text{Card } \{x \in \mathbb{Z}/p\mathbb{Z} \mid x^3 + ax + b = 0\}$$

+ 1 (point à l'infini)

Remarque : Si on remplace $x^3 + ax + b$ par x , cela donnerait

$$\text{Card } E = 0 \times \frac{p-1}{2}$$

$$+ 2 \times \frac{p-1}{2}$$

$$+ 1 \times 1$$

$$+ 1$$

$$\Rightarrow \text{Card } E = p+1$$

Heuristiquement

Donc on peut conjecturer

$$\text{que Card } E \cong p+1$$

(cela revient à faire l'hypothèse que les valeurs $x^3 + ax + b$ se répartissent en carés/non carés de la même façon que x)

Théorème [Hasse, 1940] : Si E est une courbe elliptique sur $K = \mathbb{Z}/p\mathbb{Z}$, alors

$$p+1 - 2\sqrt{p} \leq \text{Card } E \leq p+1 + 2\sqrt{p}$$

Autrement dit $\text{Card } E \in [p+1 - 2\sqrt{p}, p+1 + 2\sqrt{p}]$

$$|\text{Card } E - (p+1)| \leq 2\sqrt{p}$$

ex: si p fait 1024 bits $\rightarrow \sqrt{p}$ fait 512 bits

③ Diffie-Hellman sur une courbe elliptique

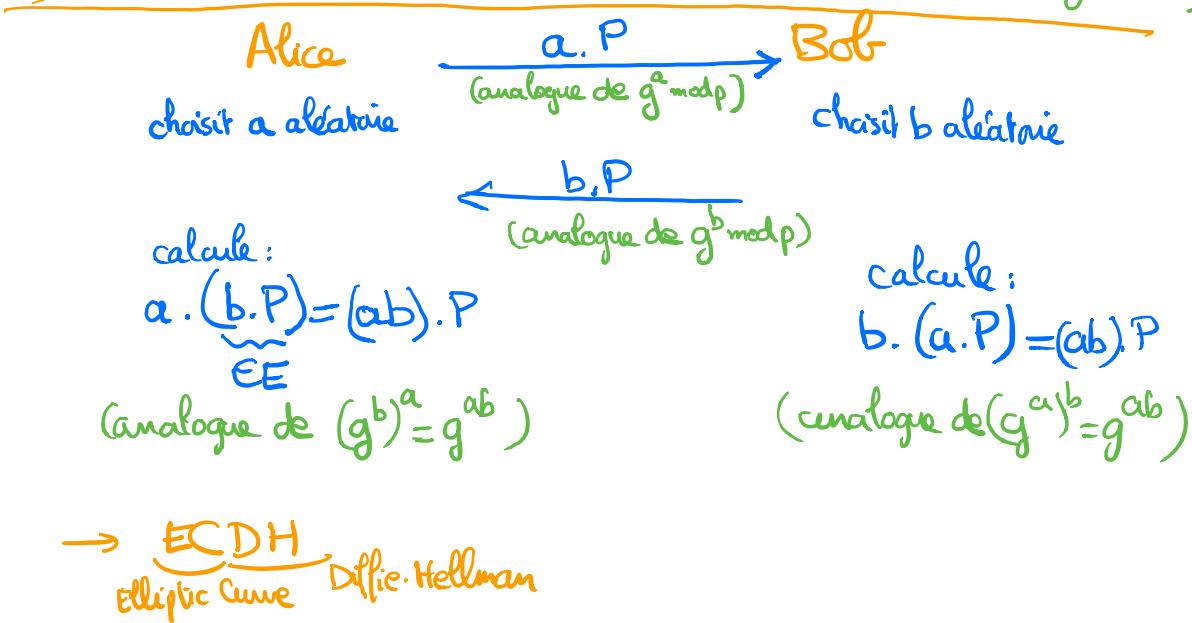
p : nombre premier (grand)

E : courbe elliptique (d'équation $y^2 = x^3 + ax + b$ avec $4a^3 + 27b^2 \neq 0$)

P : point de la courbe, qui est un générateur de E

$$\{0, P, 2P, 3P, 4P, \dots\} = E$$

(analogie de $\{g^0, g^1, g^2, \dots\} = (\mathbb{Z}/p\mathbb{Z})^*$ quand g est un générateur)



Sécurité (contre un attaquant passif)

Elle repose sur la difficulté du pb du logarithme discret

ECDLP
Elliptic Curve
Discrete Log Problem

Etant donné E et P un générateur de E

et $a \cdot P$, trouver a
 $= \underbrace{P + P + \dots + P}_{a \text{ fois}}$

(analogie de : trouver a
quand on connaît $g^a \bmod p$)

Remarque : De façon générale, on peut considérer le pb du log discret sur \rightarrow n'importe quel groupe G ayant un générateur g

→ Etant donné g et g^a , trouver a

Pour résoudre le logarithme discret :

- méthode naïve : on essaie toutes les valeurs possibles pour a
(recherche exhaustive)

$$\rightarrow \text{complexité} = O(|G|)$$

- méthode "Baby step - Giant step"

On connaît $y \in G$, on cherche a / $g^a = y$ (inconnue)

- on considère $w = \lfloor \sqrt{|G|} \rfloor$ (partie entière de $\sqrt{|G|}$)

- puis on considère la division euclidienne

de a par w

$$a \mid w \\ r \nmid q$$

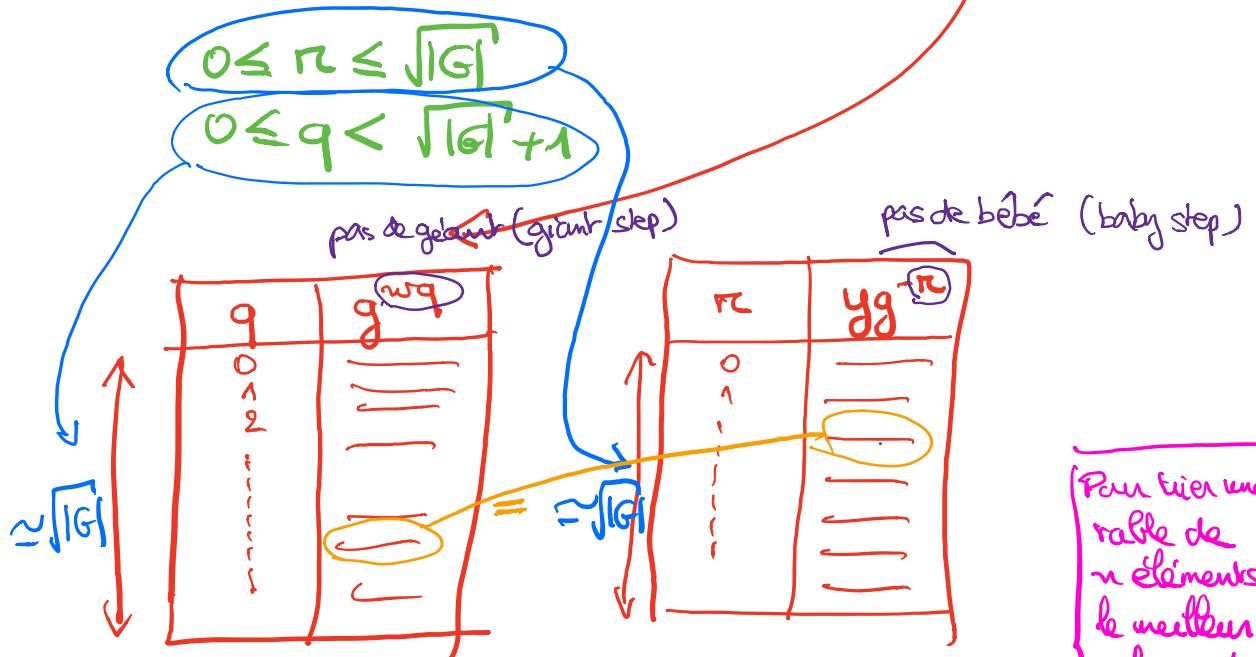
$$a = wq + r \quad \begin{matrix} \text{connue} \\ \text{inconnue} \end{matrix} \quad \begin{matrix} \text{inconnue} \\ \text{inconnue} \end{matrix}$$

$$g^a = y \iff g^{wq+r} = yg^{-r}$$

Il suffit donc de trouver q et r tels que $g^{wq} = yg^{-r}$
 sachant que $0 \leq r < w \leq \sqrt{|G|}$

et $q = \frac{a-r}{w} < \frac{|G|-1}{\sqrt{|G|}-1} = \sqrt{|G|} + 1$

(car $a-r \leq a \leq |G|-1$
 et $w = \lfloor \sqrt{|G|} \rfloor > \sqrt{|G|} - 1$)



Pour trouver un élément commun aux 2 tables

- trier les 2 tables \rightarrow complexité

$$O(\sqrt{|G|} \ln \sqrt{|G|})$$

- trouver la valeur commune \rightarrow complexité

$$O(\sqrt{|G|})$$

Complexité totale: $O(\sqrt{|G|} \ln \sqrt{|G|})$

(meilleure que la recherche exhaustive sur a qui était en $O(|G|)$)

Pour trier une table de n éléments le meilleur algo est en $O(n \ln n)$

Remarque: Il existe une amélioration en $\mathcal{O}(\sqrt{|G|})$ (algorithme de Pollard)

Diffie-Hellman sur courbes elliptiques → sécurité contre un attaquant passif
 \downarrow
 ECDLP

Difficulté du pb du logarithme discret Meilleure attaque connue est en

- Pour $G = (\mathbb{Z}_{p^2})^*, \times$: $\mathcal{O}(e^{c(\ln p)^{1/3} (\ln \ln p)^{2/3}})$ avec $c \approx 1.92$

(mieux que $\mathcal{O}(\sqrt{|G|})$): par exemple

si p faut 1024 bits
 $\mathcal{O}(e^{c(\ln p)^{1/3} (\ln \ln p)^{2/3}}) \approx 2^{80}$

$\mathcal{O}(\sqrt{|G|}) \approx \mathcal{O}(\sqrt{p}) \approx 2^{512}$

• Pour $G = (E, +)$: Meilleure attaque connue est en $\mathcal{O}(\sqrt{|G|})$

(le pb est étudié depuis l'idée d'utiliser les courbes elliptiques en cryptographie ≈ 1985 (V. Miller, N. Koblitz))

Consequence: Pour avoir une sécurité en 2^{80} il suffit d'avoir $|G| \approx 2^{160}$

Et comme $|G| \approx p+1$

il suffit de prendre p de 160 bits

	D-H "classique"	ECDH
Alice	<p>p premier, g générateur de $(\mathbb{Z}/p\mathbb{Z})^*$ Sécurité $2^{80} \Leftrightarrow p$ fait 1024 bits</p> <p>$g^a \text{ mod } p$ complexité (square and multiply) $O(k^3)$ où k est la taille de p $\hookrightarrow \approx 1024^3$</p> <p>Idem pour $(g^b)^a \text{ mod } p$</p>	<p>p premier, E : courbe elliptique sur $\mathbb{Z}/p\mathbb{Z}$ P : générateur de E Sécurité $2^{80} \Leftrightarrow p$ fait 160 bits</p> <p>$a.P$ complexité (double and add) $O(k^3)$ où k est la taille de p $\hookrightarrow \approx 160^3$</p> <p>Idem pour $a.(b.P)$</p>
Bob	<p>$g^b \text{ mod } p \hookrightarrow \approx 1024^3$</p> <p>Idem pour $(g^a)^b \text{ mod } p$</p>	<p>$b.P$ $\hookrightarrow \approx 160^3$</p> <p>Idem pour $b.(a.P)$</p>
Gain de performance $\approx \frac{(1024)^3}{160} \approx 10 \rightarrow \approx 20$		
	Algorithm Square and multiply	Algorithm Double and Add
	<p>Pour calculer $y = g^a \text{ mod } p$</p> $a = a_{k-1}2^{k-1} + \dots + a_12^1 + a_0$ <p>$y := 1 \rightarrow$ élément neutre du groupe</p> <p>Pour i de $k-1$ à 0</p> $\begin{cases} y := y^2 \text{ mod } p & O(k^2) \\ \text{si } (a_i=1) \text{ alors } y := y \times g \text{ mod } p & O(k^2) \end{cases}$	<p>Pour calculer $Q = a.P$</p> $a = a_{k-1}2^{k-1} + \dots + a_12^1 + a_0$ <p>$Q := 0 \rightarrow$ élément neutre du groupe</p> <p>& Pour i de $k-1$ à 0</p> $\begin{cases} Q := 2Q & O(k^2) \\ \text{Si } (a_i=1) \text{ alors } Q := Q + P & O(k^2) \end{cases}$
	$O(k^3)$ (avec $k \approx 1024$)	$O(k^3) \times$ (avec $k \approx 160$)

Application : Passeport électronique (biométrique)

→ Diffie-Hellman sur canaux elliptiques



ch 3 : Authentification et Zero-knowledge

I] Authentification

① Concept général

Authentification d'une personne

- carte d'identité
- signature
- voix
- Image
- lien zoom
- ⋮
- ⋮

On peut classer ces informations en 3 catégories

- a) Ce qu'on est :
- visage (photo) (informations biométriques)
 - voix
 - empreintes digitales
 - ADN
 - Iris

- b) Ce qu'on connaît :
- lien zoom
 - la crypto
 - magicien
 - mot de passe

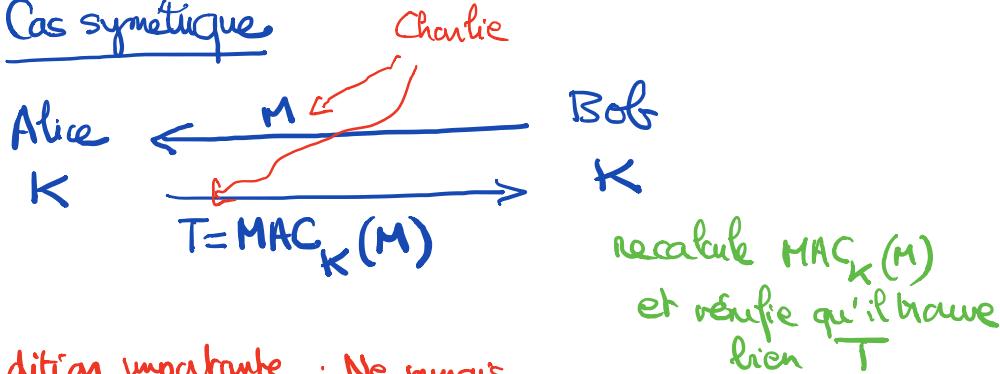
c) Ce qu'on possède :

- carte d'identité
- badge
- carte d'étudiant

② Authentification en cryptographie

S'authentifier = prouver que l'on connaît un secret

Cas symétrique



Condition importante : Ne jamais réutiliser le même message M

(pour éviter les attaques de "re-jeu")

→ soit Bob doit garder une trace de tous les messages déjà utilisés

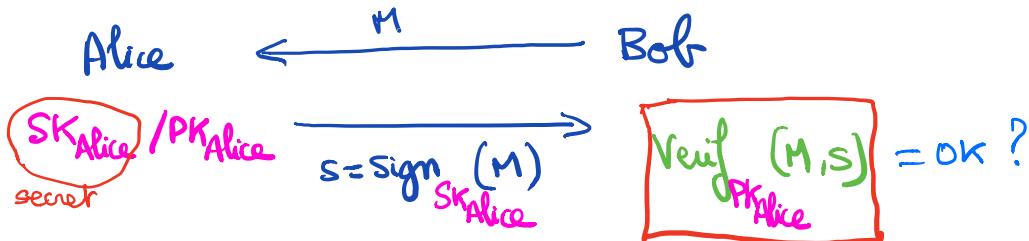
→ soit Bob génère M aléatoirement

(\Rightarrow si M est assez grand, la probabilité de réutiliser un même message est négligeable)

"Défaut" de cette solution symétrique

Alice peut s'authentifier auprès de Bob
mais Bob ne peut pas prouver à un tiers
qu'Alice s'est réellement authentifiée
auprès de lui.

• Cas asymétrique



L'authentification nécessite qu'on ne réutilise jamais 2 fois le même M

- soit on garde en mémoire les M déjà utilisés
(ou on a un compteur)
 - soit on prend M aléatoire

Remarque : Cette fois, Bob peut convaincre un tiers qu'Alice s'est vraiment authentifiée

Défi: Peut-on concevoir un protocole d'authentification asymétrique qui garantisse la non-tragabilité des authentications.

→ Zero-knowledge

II] Protocols d'authentification zero-knowledge

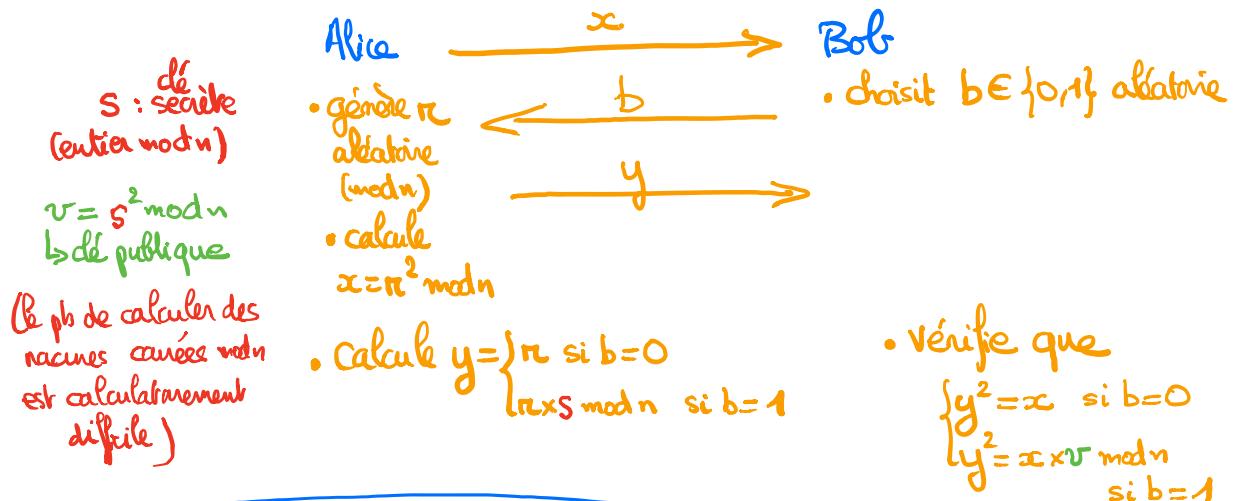
The diagram illustrates a digital signature exchange between Alice and Bob. Alice, on the left, has a secret key (SK_{Alice}) and a public key (PK_{Alice}). She signs a message (M) using her secret key to produce a signature ($s = \text{Sign}(M)$). This signature is sent to Bob, who uses Alice's public key (PK_{Alice}) to verify the signature. Bob checks if the verification equation $\text{Verif}_{PK_{Alice}}(M, s) = \text{OK}$ holds true.

- pb 1 : Alice révèle "une partie" de son secret.
 pb 2 : Cette authentification est "fragile" : Bob peut ensuite prouver à un tiers qu'Alice s'est réellement authentifiée
 (ce qui pose pb dans certains casernes où on veut protéger la vie privée des utilisateurs)

Authentification zero-knowledge (à divulgation nulle de connaissance)

Protocole de Fischer-Micali-Rackoff (1983)

Paramètre : $n (= p \times q)$, où p et q sont premiers



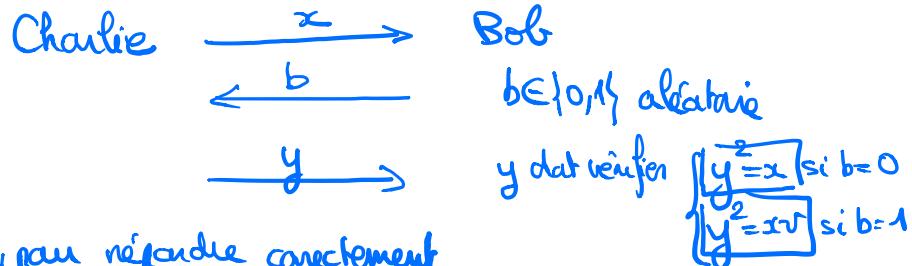
- Si Alice et Bob jouent ce protocole honnêtement, la vérification est satisfaites :

$$\underline{1^{\text{er}} \text{ cas}} : b=0 \quad : \quad y^2 = r^2 = x \text{ mod } n \quad : \text{OK}$$

$$\underline{2^{\text{e}} \text{ cas}} : b=1 \quad : \quad y^2 = (r \times s)^2 = r^2 s^2 = x v \text{ mod } n : \text{OK}$$

→ authentification réussie

- Supposons que Charlie essaie de se faire passer pour Alice



\Rightarrow Charlie, pour répondre correctement dans plus de 50% des cas (avec une proba $> \frac{1}{2}$), doit être capable de fabriquer deux valeurs y et y' telles que

$$\begin{cases} \bullet y^2 = x \pmod{n} \\ \bullet (y')^2 = x \times v \pmod{n} \end{cases}$$

\Rightarrow Charlie connaît $\frac{y'}{y}$ qui vérifie $\left(\frac{y'}{y}\right)^2 = \frac{v}{x} = v \pmod{n}$
 → il connaît une "racine carrée" de $v \pmod{n}$

On it est calculatoirement difficile de trouver de telles racines carrées mod n (c'est équivalent au pb de la factorisation)

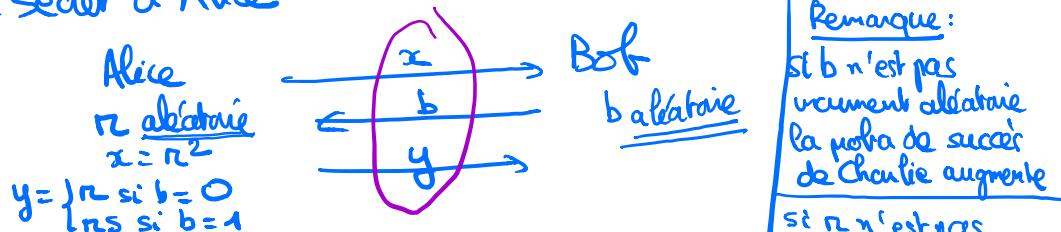
(la seule méthode connue pour résoudre $\exists z^2 = \alpha \pmod{n}$ consiste à : • factoriser n)

- résoudre $\exists z^2 = \alpha \pmod{p}$ (cf propriété 3 du ch 2)
 et $\exists z^2 = \alpha \pmod{q}$
- appliquer le théorème des restes chinois

Conclusion : Charlie n'a qu'une probabilité $\frac{1}{2}$ de se faire

passer avec succès par Alice

- Montre qu'un observateur (Bob, Charlie,...) n'apprend rien du secret d'Alice



x : ne révèle rien sur s
 b : _____

aléatoire, Charlie
peut apprendre qqch sur le
secret s

y : [1^e cas: $b=0$] $y=r$ → ne révèle rien sur s

[2^e cas: $b=1$] $y=\underbrace{r \times s}_{\text{mod } n} \rightarrow$ aléatoire → ne révèle rien sur s



(x, y) : 1^e cas ($b=0$): $(r^2, r) \rightarrow$ ne révèle rien sur s

2^e cas ($b=1$): $(r^2, \underbrace{r \times s}_{\text{mod } n}) = (\underbrace{\frac{r^2}{s^2} \text{ mod } n}_{\text{aléatoire}}, \underbrace{s}_{\text{aléatoire}}) \rightarrow$ ne révèle rien sur s

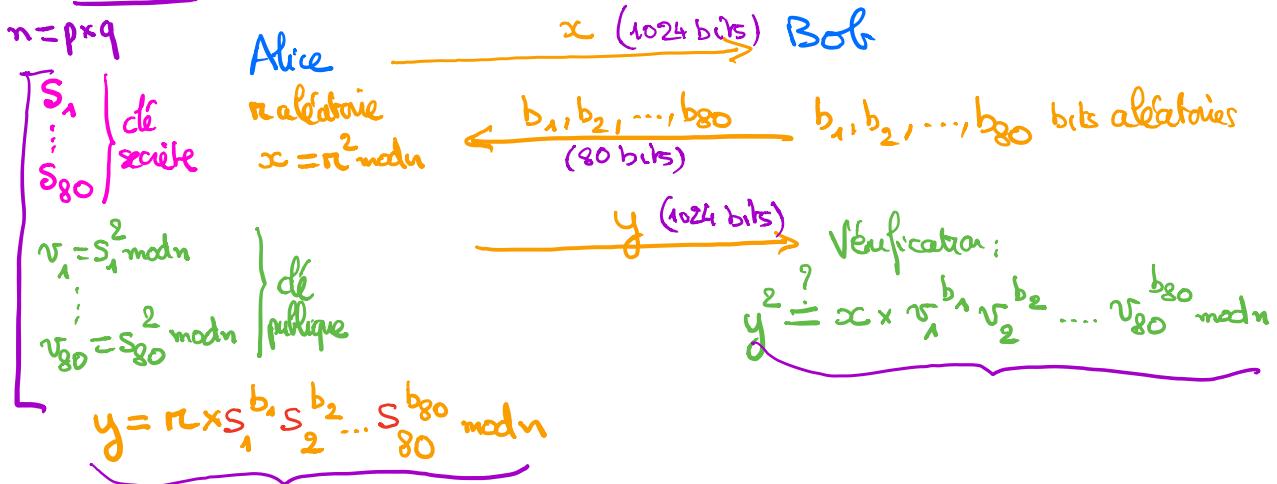
Pour que la probabilité de succès de Charlie soit négligeable
(être pas 50% comme on
a jusqu'à présent)

Idee 1: Répéter l'authentification plusieurs fois

ex: 80 fois Fisher - Micali - Rackoff
→ proba de succès $\frac{1}{2^{80}}$

Inconvénient: 80×3 messages à transmettre
entre Alice et Bob

Idee 2 (affinement): Fiat - Shamir (1984)



Pour les mêmes raisons que dans Fischer-Micali-Rackoff :

- Si Alice joue honnêtement le protocole, l'authentification réussit
- Charlie a une probabilité de se faire passer pour Alice égale à $\frac{1}{2^{80}}$
- Rien du secret d'Alice n'est révélé

Remarque : Fiat-Shamir (1984) ont montré qu'on peut transformer ce protocole d'authentification en algorithme de signature [Heuristique de Fiat-Shamir]

