

INTRODUCTION À LA SÉCURITÉ INFORMATIQUE SÉANCE 6

Marc-Olivier Killijian

UQAM, CNRS

INF4471 A21

APPLICATIONS DE LA CRYPTO

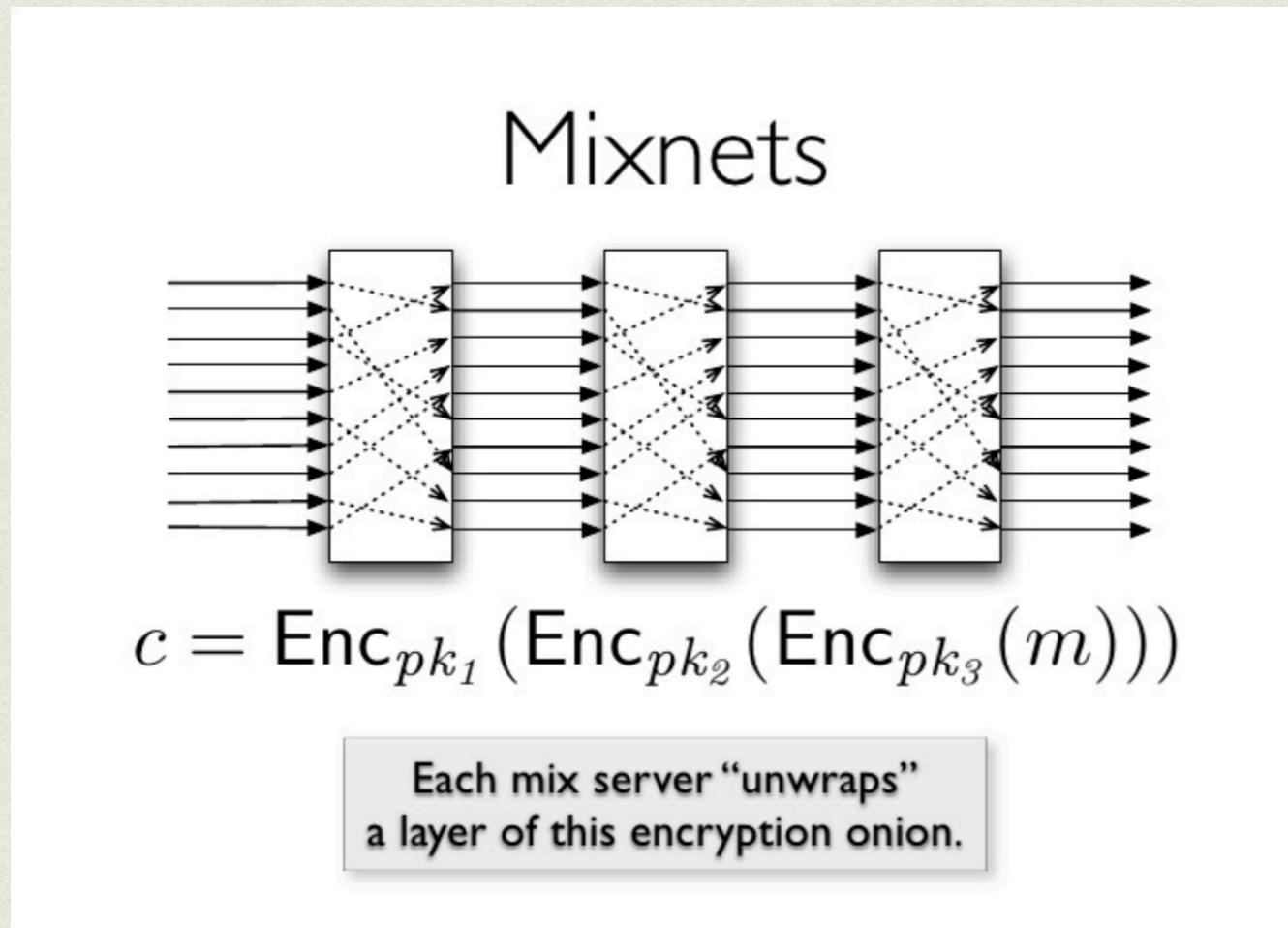
- Communications anonymes
- Chaîne de blocs et crypto-monnaies
- Accréditations anonymes
- Retrait d'information privé
- Messageries sécurisées

COMMUNICATIONS ANONYMES

COMMUNICATIONS ANONYMES

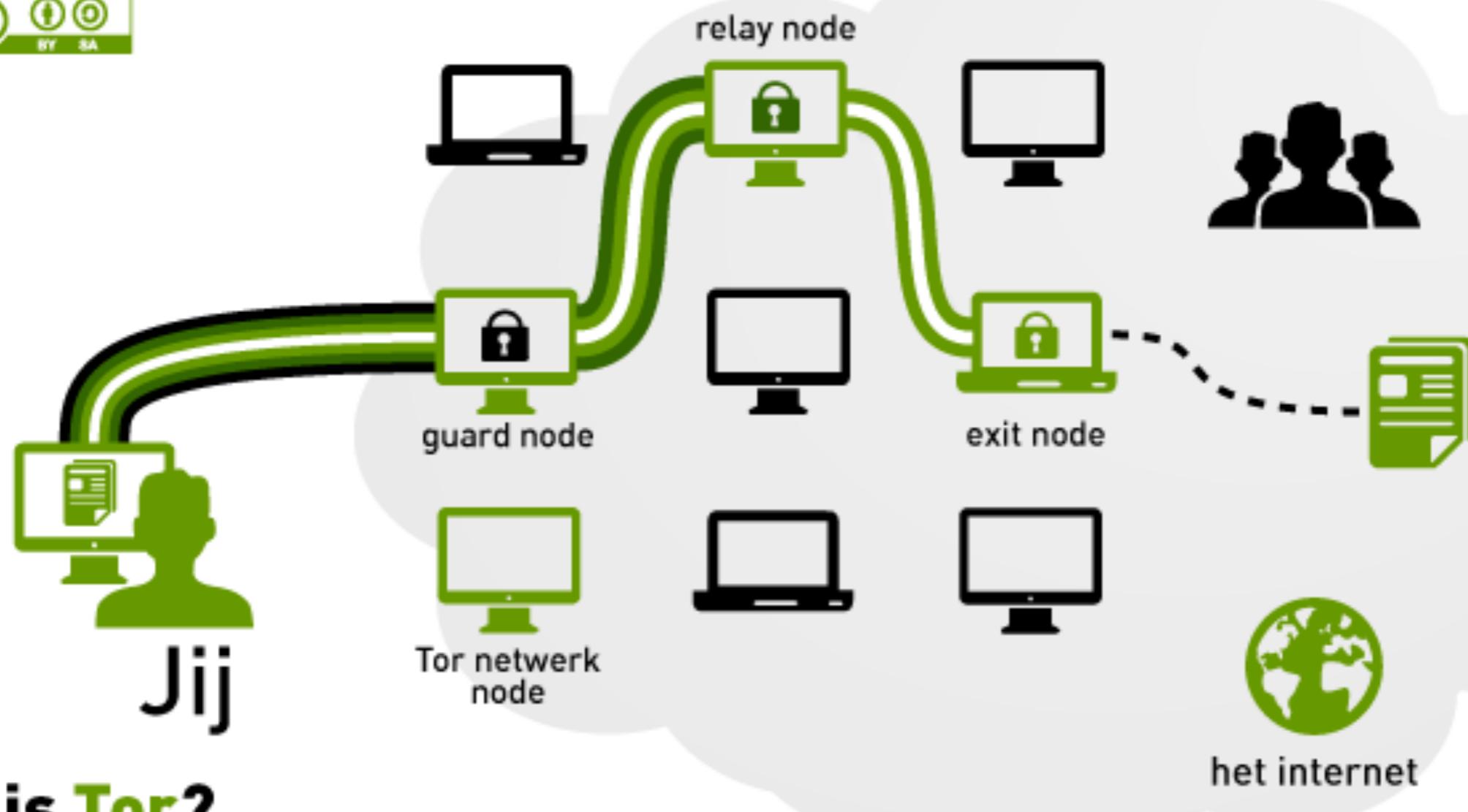
- Communiquer de façon anonyme dans un réseau
 - Protéger ID émetteur et/ou récepteur
 - ex: MixNets, routage en oignon (TOR), Crowds.
- Brique de base pour d'autres TACs pour cacher l'identité d'une entité derrière une action
 - ex. d'application: surf anonyme sur internet, mail anonyme, téléphonie non-observable

ROUTAGE ANONYME



- Questions clés :
- Format du mix
- Stratégie du mix
- Propriétés d'anonymat
 - émetteur
 - récepteur
- Anonymat (cryptographiquement) fort
- Non-observabilité

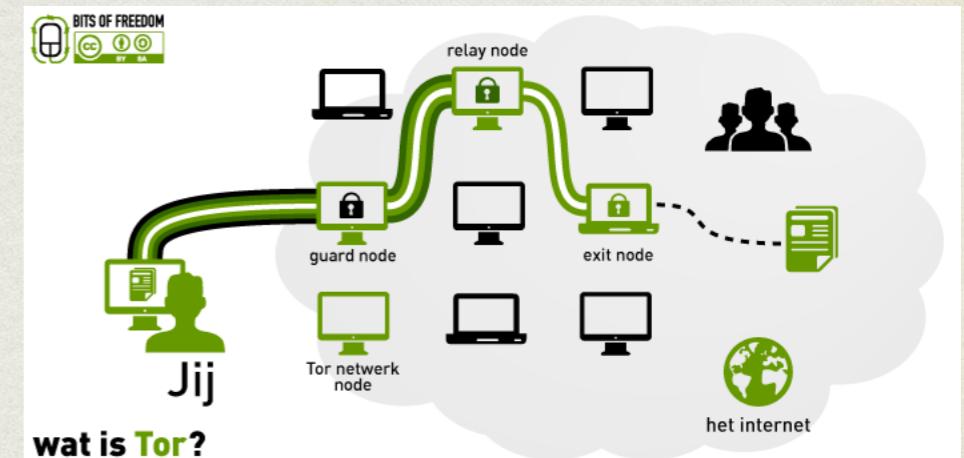
ROUTAGE ONION



wat is Tor?

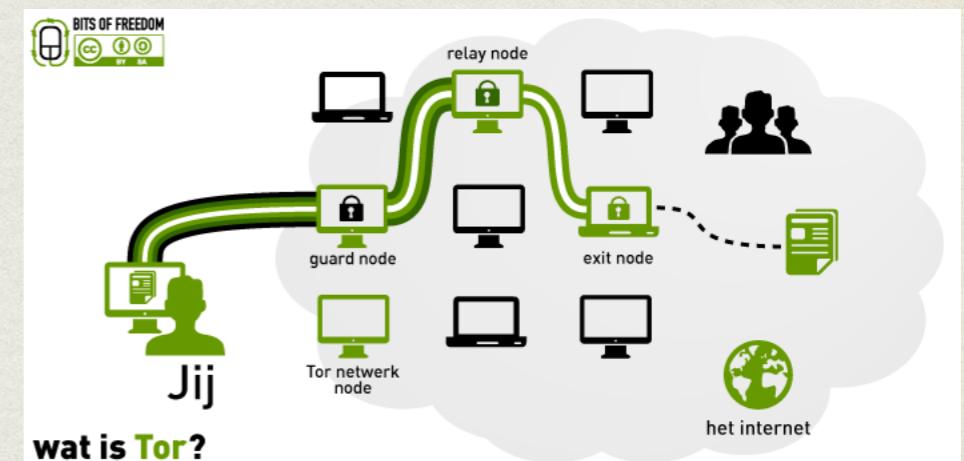
ROUTAGE ONION

- L'émetteur choisi la route de son message :
 $E, r_0, r_1, \dots, r_n, R$
- Il chiffre le message pour R :
 $m_R = enc(m, PK_R)$
- Il chiffre pour le routeur précédent un message qui contient le routeur suivant et le message : $m_{r_n} = enc(R, m_R)$
- Et ainsi de suite en marche arrière :
 $m_{r_i} = enc(r_{i+1}, m_{r_{i+1}})$



ROUTAGE ONION

- r_i ne sait pas si r_{i+1} est le récepteur final ou non
 - R doit faire semblant de router un message sortant lors d'une réception finale
- un observateur non plus



COMMUNICATIONS ANONYMES: QUEL TRILEMME

TABLE I

Latency vs. bandwidth vs. strong anonymity of AC protocols, with the number of protocol-nodes K , number of clients N , and message-threshold T , expected latency ℓ' per node, dummy-message rate β .

Protocol	Latency	Bandwidth	Strong Anonymity
Tor [10]	$\theta(1)$	$\theta(1/N)$	impossible
Hornet [47]	$\theta(1)$	$\theta(1/N)$	impossible
Herd [48]	$\theta(1)$	$\theta(N/N)$	possible
Riposte [49]	$\theta(N)$	$\theta(N/N)$	possible
Vuvuzula [20]	$\theta(K)$	$\theta(N/N)$	possible
Riffle [21]	$\theta(K)$	$\theta(N/N)$	possible
Threshold mixes [14]	$\theta(T \cdot K)$	$\theta(1/N)$	impossible*
Loopix [24]	$\theta(\sqrt{K} \cdot \ell')$	$\theta(\beta)$	possible
DC-Net [15], [46]	$\theta(1)$	$\theta(N/N)$	possible
Dissent-AT [22]	$\theta(1)$	$\theta(N/N)$	possible
DiceMix [16]	$\theta(1)$	$\theta(N/N)$	possible

* if T in $o(\text{poly}(\eta))$

de Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency---Choose Two

COMMUNICATIONS ANONYMES: QUEL TRILEMME

TABLE I

Latency vs. bandwidth vs. strong anonymity of AC protocols, with the number of protocol-nodes K , number of clients N , and message-threshold T , expected latency ℓ' per node, dummy-message rate β .

Protocol	Latency	Bandwidth	Strong Anonymity
Tor [10]	$\theta(1)$	$\theta(1/N)$	impossible
Hornet [47]	$\theta(1)$	$\theta(1/N)$	impossible
Herd [48]	$\theta(1)$	$\theta(N/N)$	possible
Riposte [49]	$\theta(N)$	$\theta(N/N)$	possible
Vuvuzula [20]	$\theta(K)$	$\theta(N/N)$	possible
Riffle [21]	$\theta(K)$	$\theta(N/N)$	possible
Threshold mixes [14]	$\theta(T \cdot K)$	$\theta(1/N)$	impossible*
Loopix [24]	$\theta(\sqrt{K} \cdot \ell')$	$\theta(\beta)$	possible
DC-Net [15], [46]	$\theta(1)$	$\theta(N/N)$	possible
Dissent-AT [22]	$\theta(1)$	$\theta(N/N)$	possible
DiceMix [16]	$\theta(1)$	$\theta(N/N)$	possible

* if T in $o(\text{poly}(\eta))$

non-obs \rightarrow bandwidth

sinon

de Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency---Choose Two

analyse de traffic

COMMUNICATIONS ANONYMES: QUEL TRILEMME

TABLE I

Latency vs. bandwidth vs. strong anonymity of AC protocols, with the number of protocol-nodes K , number of clients N , and message-threshold T , expected latency ℓ' per node, dummy-message rate β .

Protocol	Latency	Bandwidth	Strong Anonymity
Tor [10]	$\theta(1)$	$\theta(1/N)$	impossible
Hornet [47]	$\theta(1)$	$\theta(1/N)$	impossible
Herd [48]	$\theta(1)$	$\theta(N/N)$	possible
Riposte [49]	$\theta(N)$	$\theta(N/N)$	possible
Vuvuzula [20]	$\theta(K)$	$\theta(N/N)$	possible
Riffle [21]	$\theta(K)$	$\theta(N/N)$	possible
Threshold mixes [14]	$\theta(T \cdot K)$	$\theta(1/N)$	impossible*
Loopix [24]	$\theta(\sqrt{K} \cdot \ell')$	$\theta(\beta)$	possible
DC-Net [15], [46]	$\theta(1)$	$\theta(N/N)$	possible
Dissent-AT [22]	$\theta(1)$	$\theta(N/N)$	possible
DiceMix [16]	$\theta(1)$	$\theta(N/N)$	possible

* if T in $o(\text{poly}(\eta))$

de Anonymity Trilemma: Strong Anonymity, Low Bandwidth

NOMBREUSES SOLUTIONS

NE PASSENT PAS À L'ÉCHELLE

COMMUNICATIONS ANONYMES: QUEL TRILEMME

TABLE I

Latency vs. bandwidth vs. strong anonymity of AC protocols, with the number of protocol-nodes K , number of clients N , and message-threshold T , expected latency ℓ' per node, dummy-message rate β .

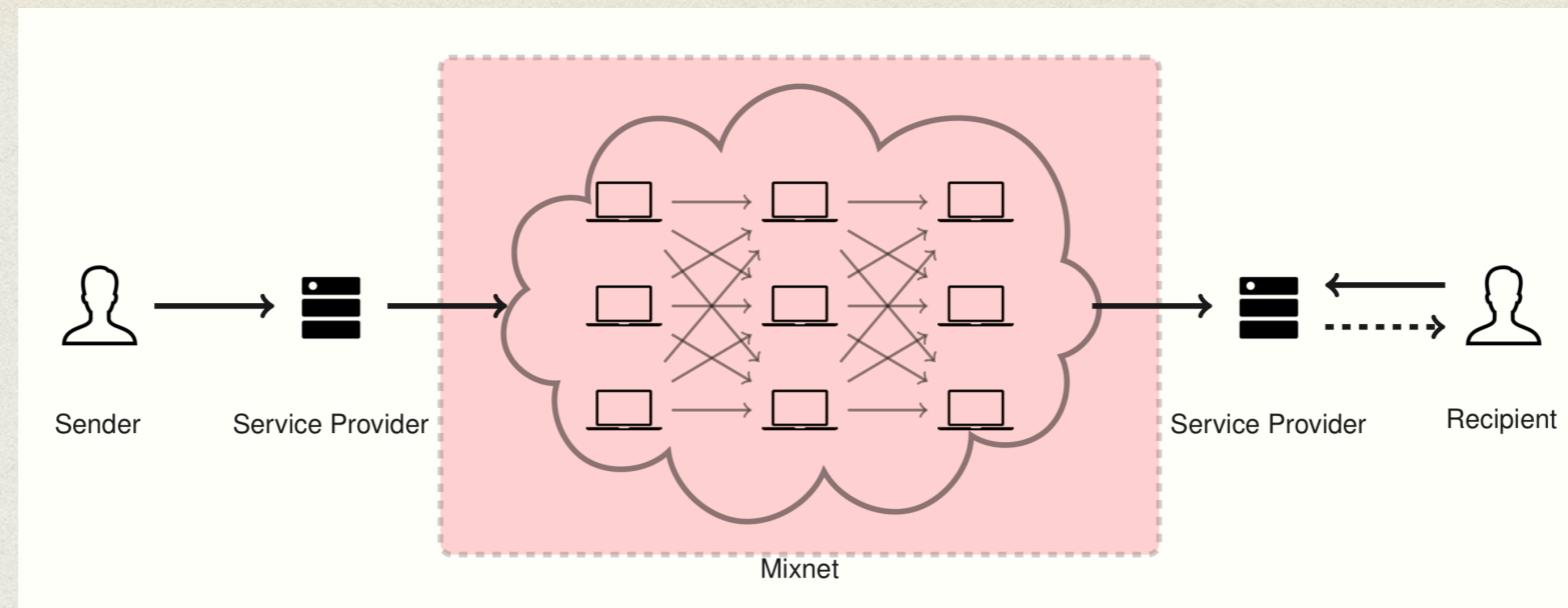
Protocol	Latency	Bandwidth	Strong Anonymity
Tor [10]	$\theta(1)$	$\theta(1/N)$	impossible
Hornet [47]	$\theta(1)$	$\theta(1/N)$	impossible
Herd [48]	$\theta(1)$	$\theta(N/N)$	possible
Riposte [49]	$\theta(N)$	$\theta(N/N)$	possible
Vuvuzula [20]	$\theta(K)$	$\theta(N/N)$	possible
Riffle [21]	$\theta(K)$	$\theta(N/N)$	possible
Threshold mixes [14]	$\theta(T \cdot K)$	$\theta($	
Loopix [24]	$\theta(\sqrt{K} \cdot \ell')$	$\theta($	
DC-Net [15], [46]	$\theta(1)$	$\theta($	
Dissent-AT [22]	$\theta(1)$	$\theta($	
DiceMix [16]	$\theta(1)$	$\theta(N/N)$	possible

* if T in $o(\text{poly}(\eta))$

TOR n'est PAS résistant
à un observateur global passif !

de Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency---Choose Two

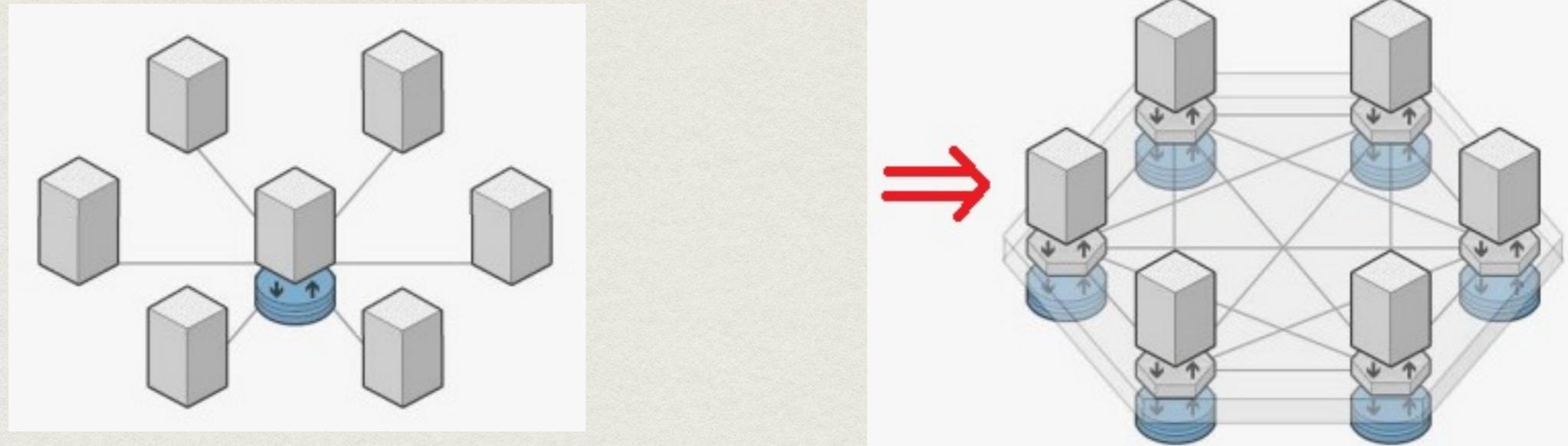
LOOPIX



- Mixnet 2.0 ([Piotrowska et al. 2017](#))
 - Traffic de masquage contre l'analyse de traffic (pas forcément à bande passante maximale, dépend du traffic réel)
 - Délais aléatoires (*Poisson mix*) dans le routage contre analyses temporelles
 - Protection contre un observateur passif global (Agences)
 - Protection contre attaques actives

BLOCKCHAIN ET CRYPTO- MONNAIES

CHAINE DE BLOCS / BLOCKCHAIN



- Système de gestion et de stockage de données distribué
 - pas d'organe de décision central
 - immuable
- Def: Registre répliqué et distribué, sans contrôle central et sécurisé par mécanismes cryptographiques

BLOCKCHAIN

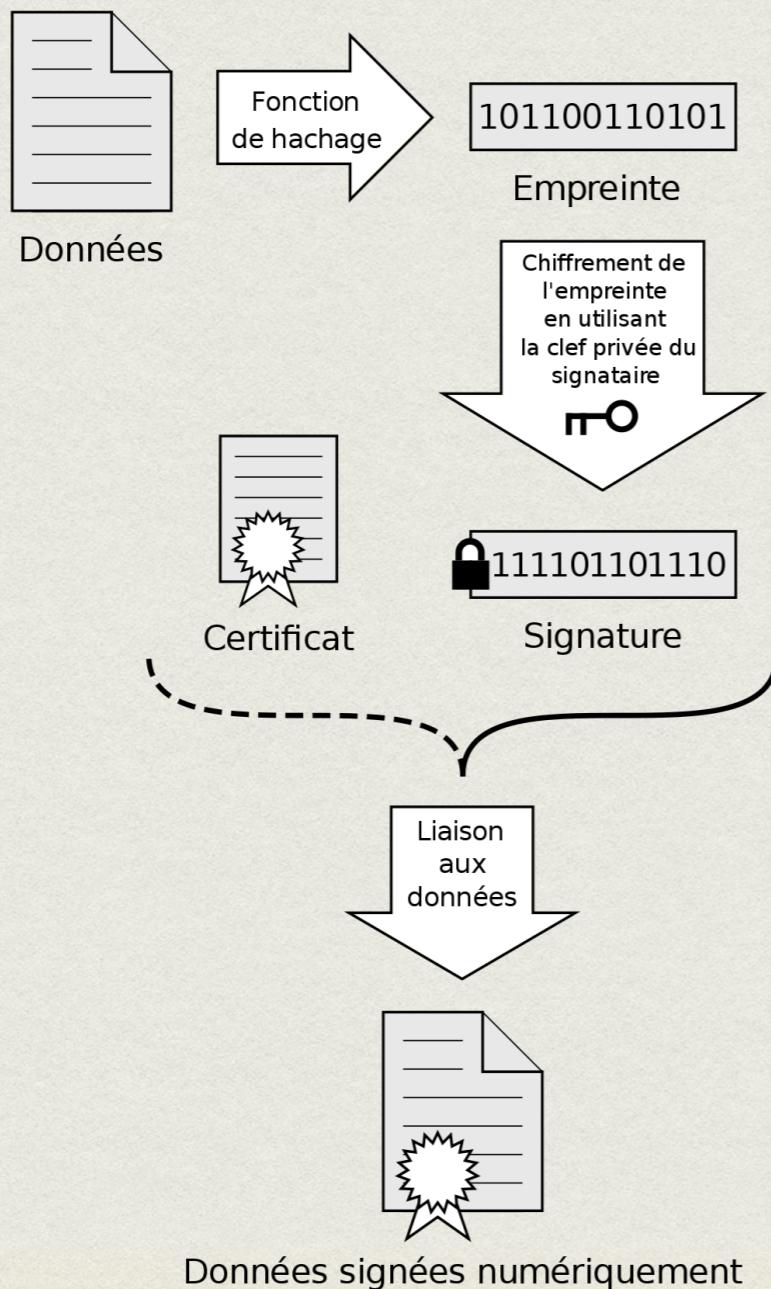
- Rien de nouveau techniquement
 - Stockage distribué P2P (1999: Napster, 2000: eDonkey, 2001: BitTorrent, etc.)
 - Consensus distribué
 - Chaînes d'horodatage
 - Dépense énergétique liée à la résolution de problèmes difficiles
- Basé sur des fonctions cryptographiques particulières (fonctions de hachage, signatures)

FONCTION DE HACHAGE

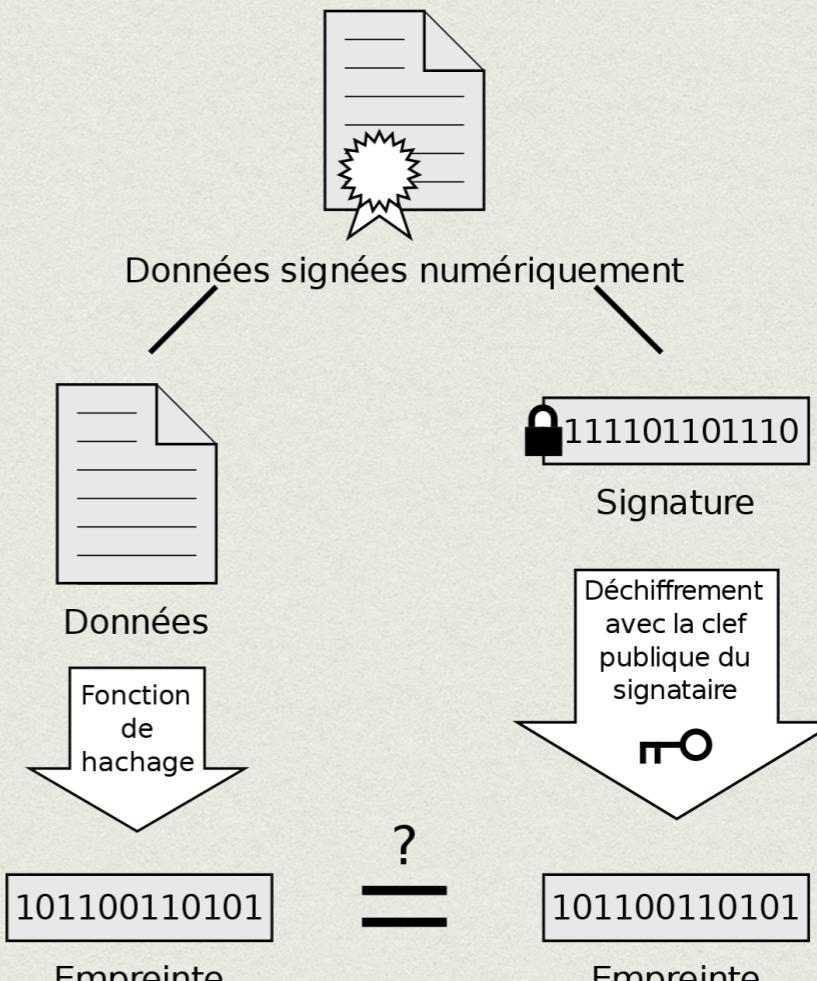
- $H(\text{document}) \rightarrow$ empreinte E de taille fixe (e.g. 256 bits)
 - Facile (rapide) de calculer $H(y)=x$
 - **Mono-directionnel**: « Difficile » de calculer $y=H^{-1}(x)$
 - **Résistant aux collisions**: « Difficile » de trouver y' tq $H(y)=H(y')=x$
- Principales fonctions de hachage : ~~MD5, SHA-1~~, SHA-256, SHA-512, SHA-3
- SHA1 : hashs de 160 bits, une infinité de y donnent un x mais trouver une collision force brute nécessite en moy. de calculer 2^{80} hachés mais une attaque a été trouvée en 2005 en 2^{69} calculs (2000x force brute)

SIGNATURES ÉLECTRONIQUES

Signature



Vérification



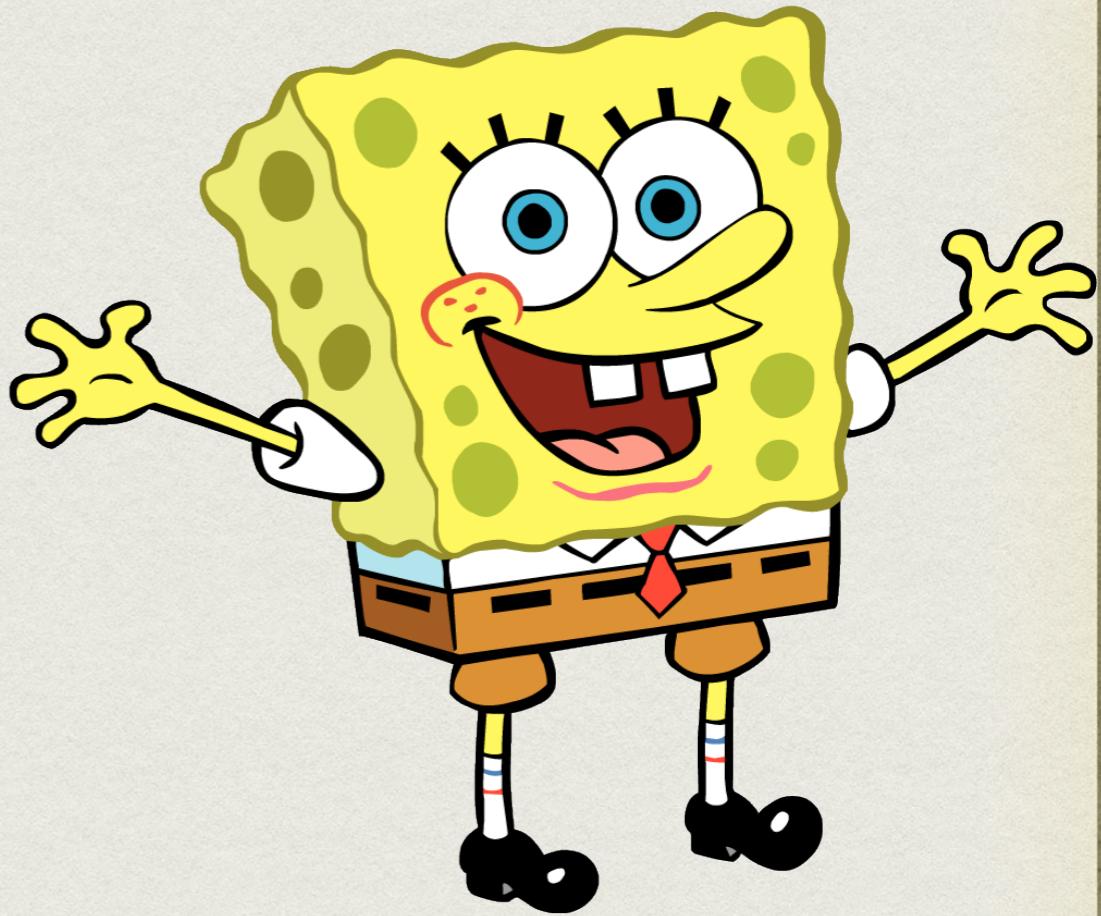
Si les empreintes sont identiques, la signature est valide

CRYPTO SYM/ ASYMÉTRIQUE

Alice



Bob



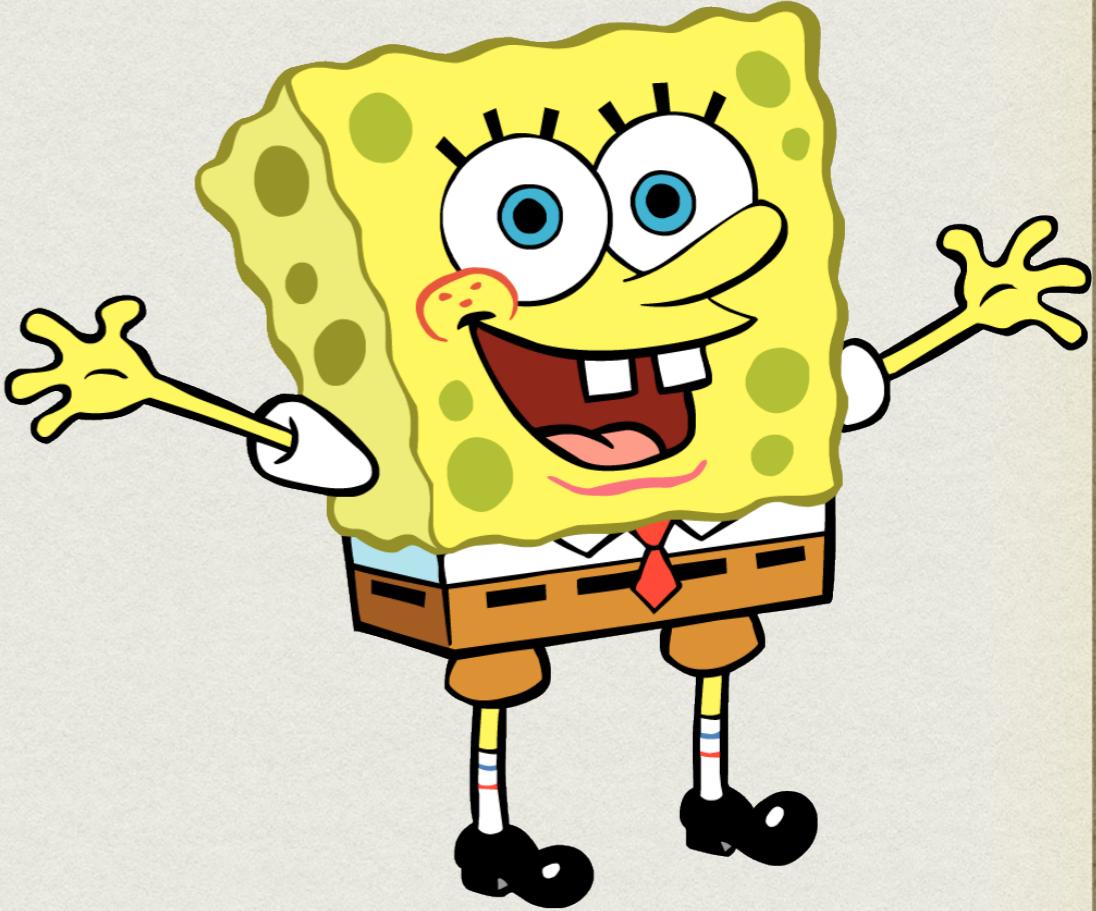
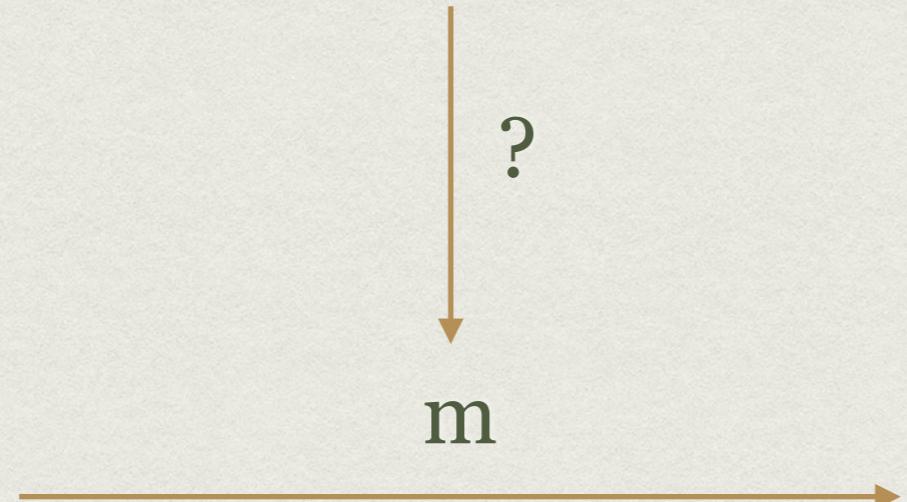
m

CRYPTO SYM/ ASYMÉTRIQUE

Alice

Charlie

Bob

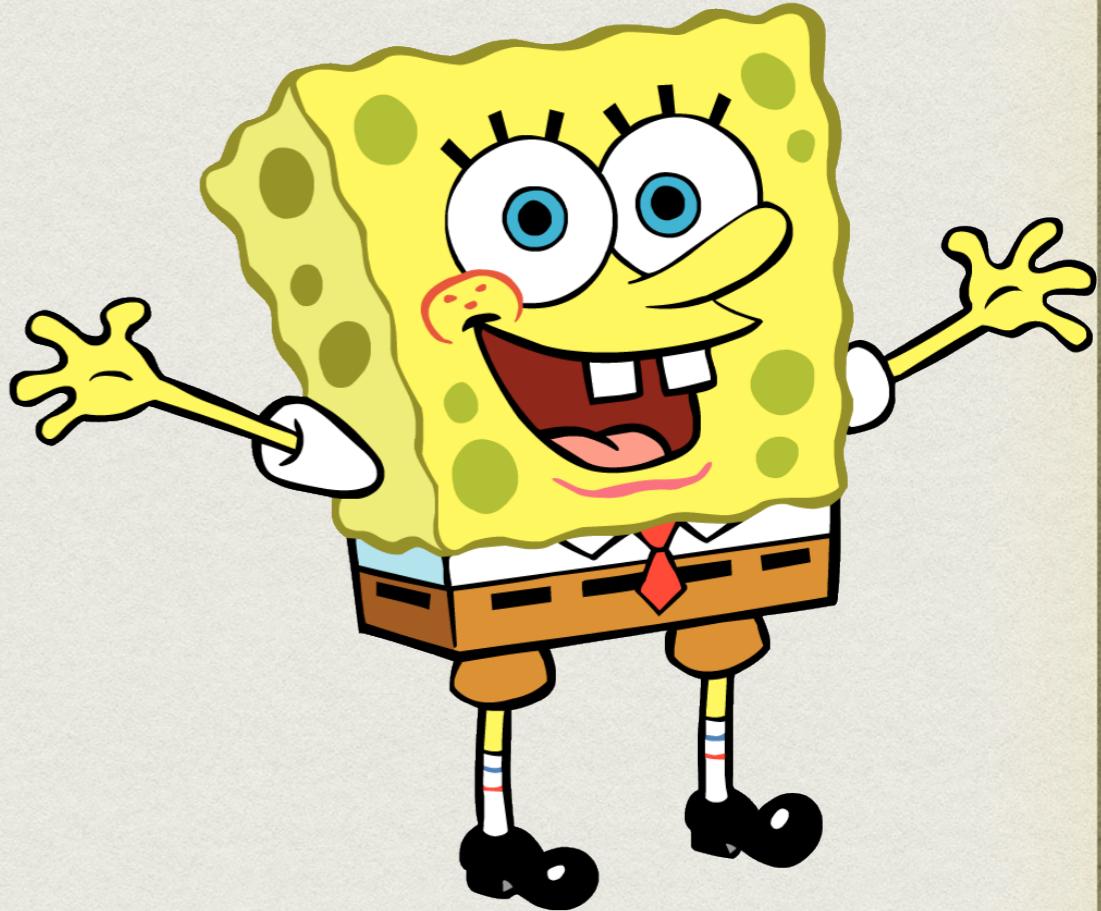
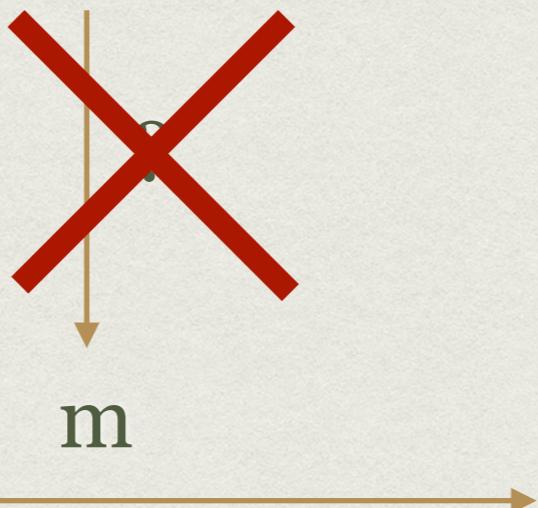


CRYPTO SYM/ ASYMÉTRIQUE

Alice

Charlie

Bob



CRYPTO SYMÉTRIQUE

Alice

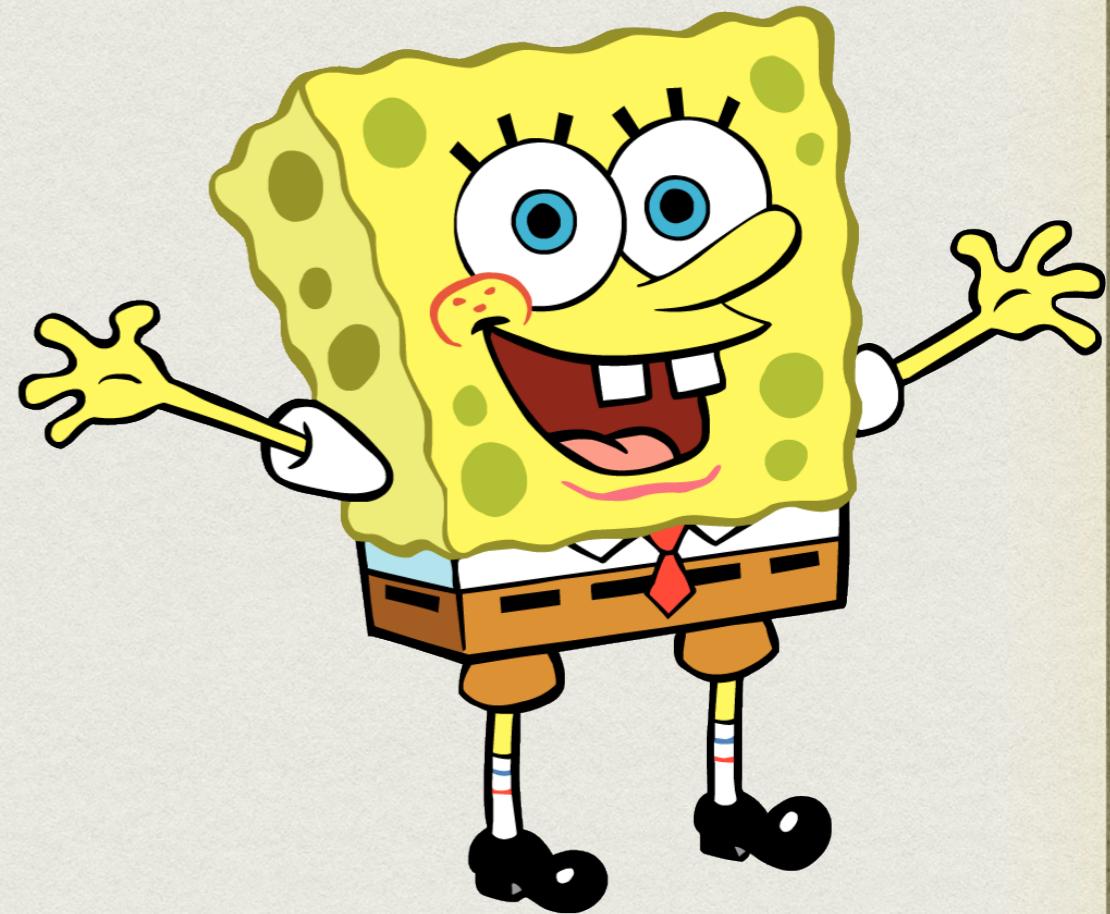
chiffré=Enc(m,k)



Bob

m=Dec(chiffré,k)

Dec=Enc⁻¹



chiffré



CRYPTO SYMÉTRIQUE

Alice

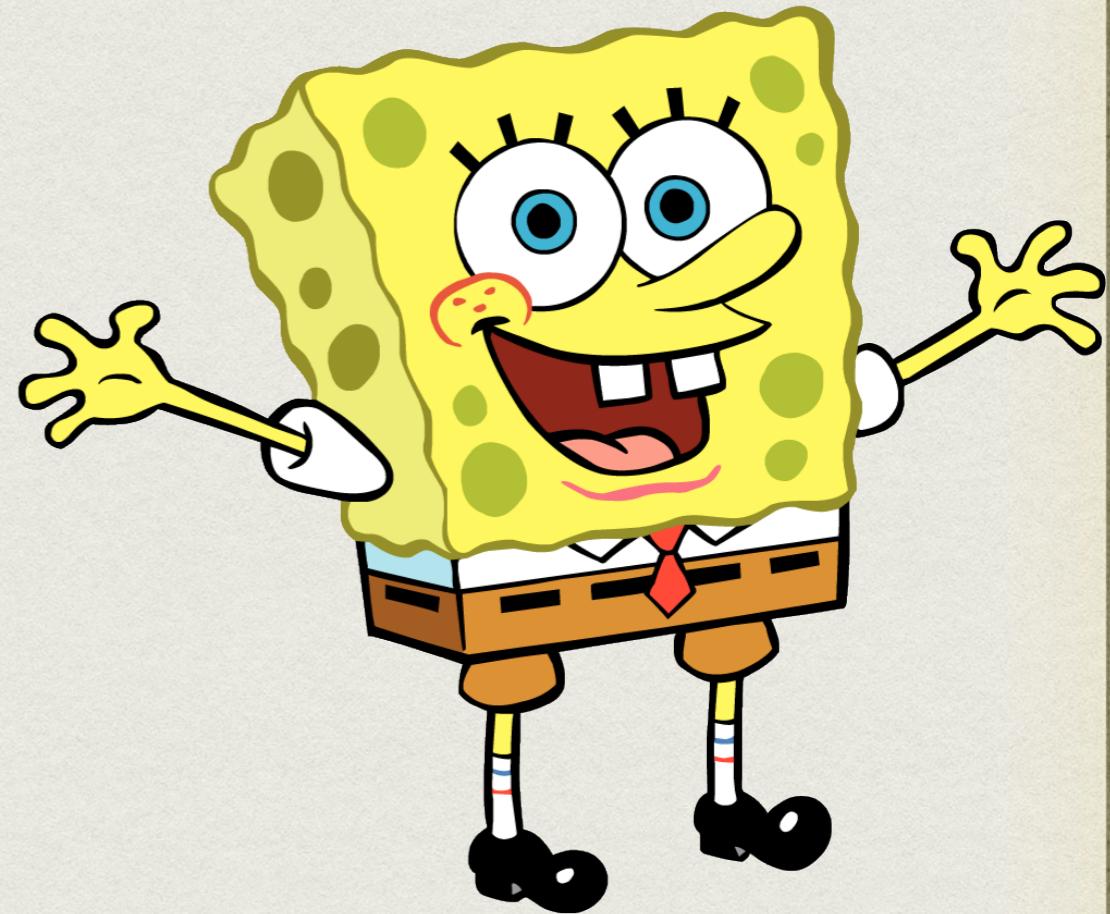
chiffré=Enc(m,k)



Bob

m=Dec(chiffré,k)

Dec=Enc⁻¹



chiffré



CRYPTO ASYMÉTRIQUE

Alice

chiffré=Enc(m, pub)

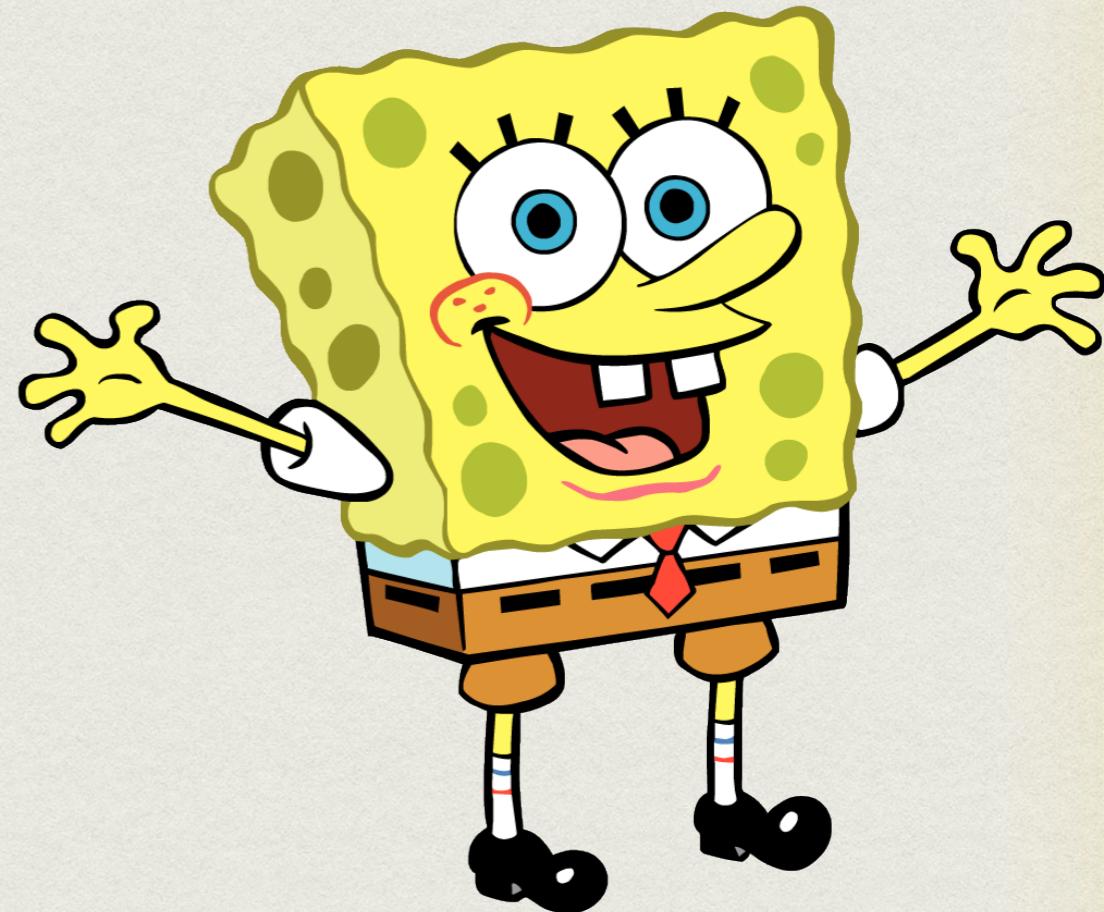


Bob

$m = \text{Dec}(\text{chiffré}, \text{priv})$

$\text{Dec} \neq \text{Enc}^{-1}$

chiffré



CRYPTO ASYMÉTRIQUE

Alice

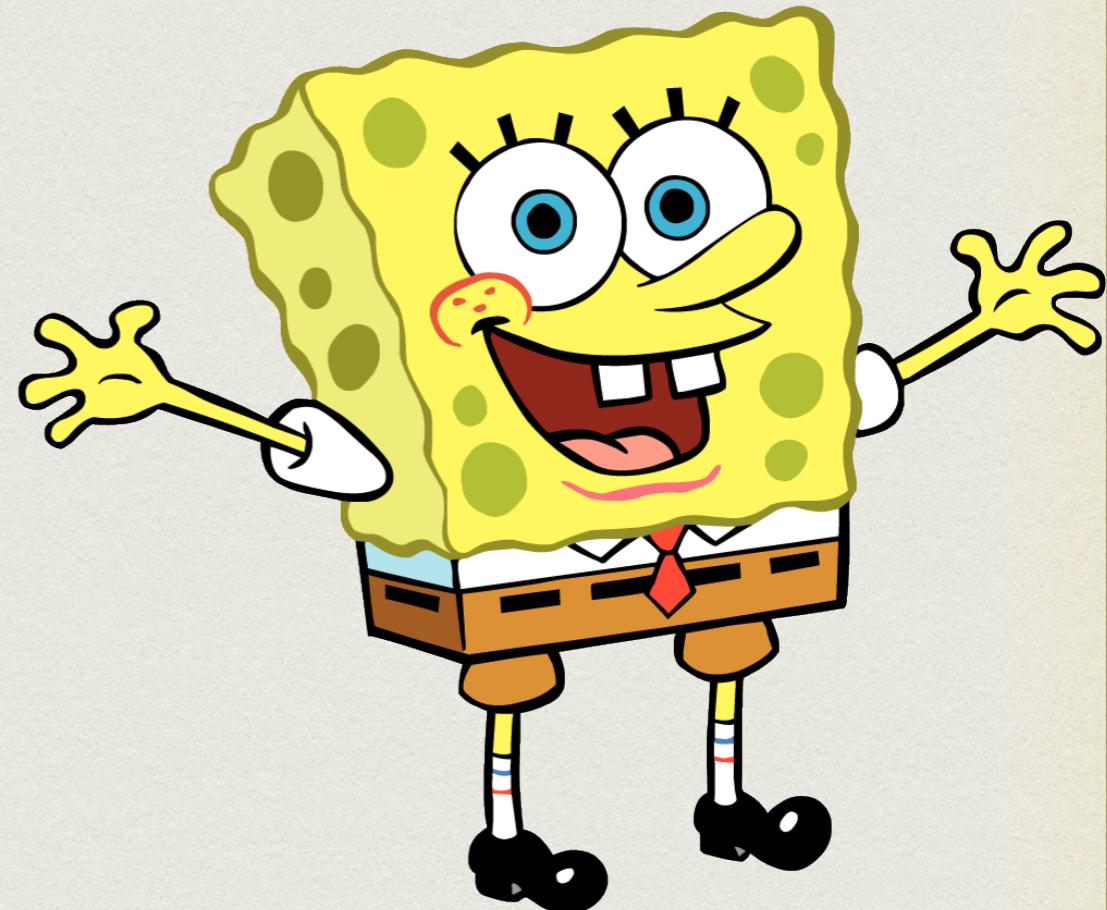
chiffré=Enc(m, pub)



Bob

$m = \text{Dec}(\text{chiffré}, \text{priv})$

$\text{Dec} \neq \text{Enc}^{-1}$



SIGNATURE

Alice

chiffré=Enc(H(m),priv)



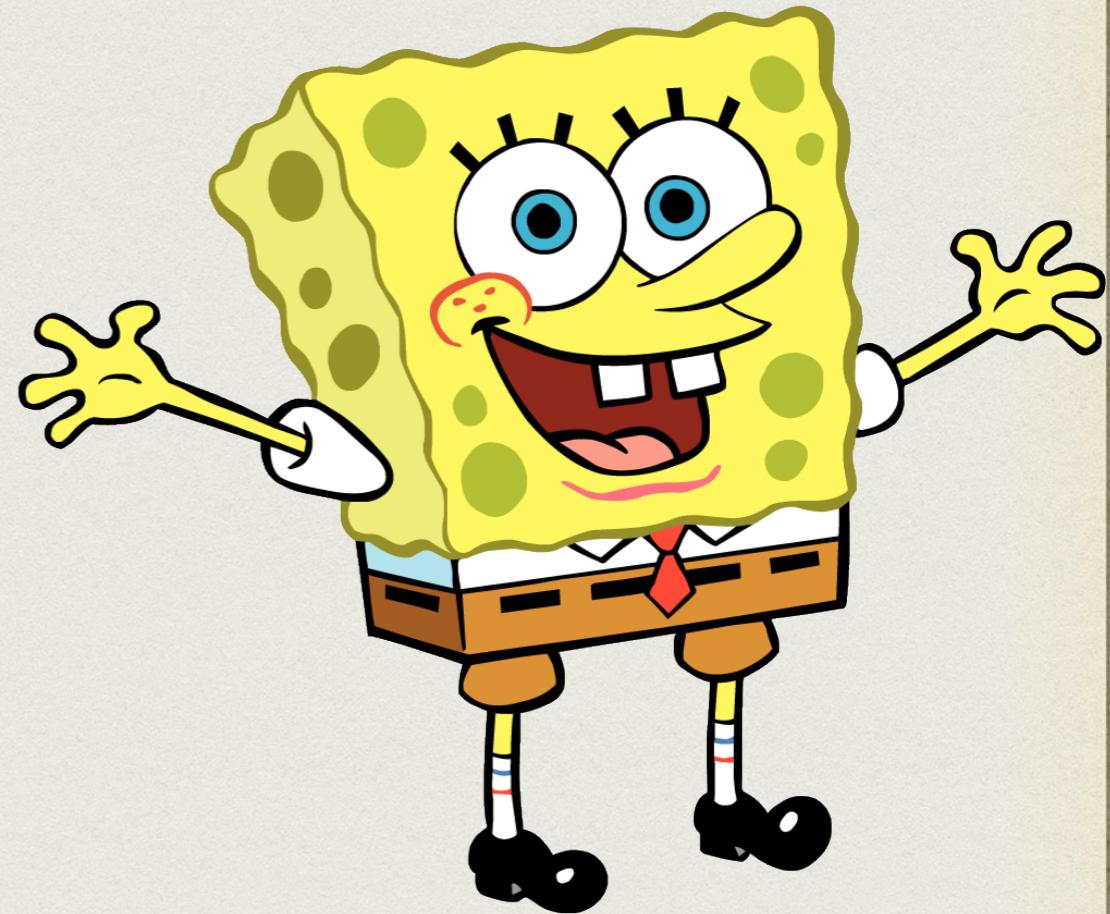
Bob

empreinte=Dec(chiffré, pub)

H(m) == empreinte ??

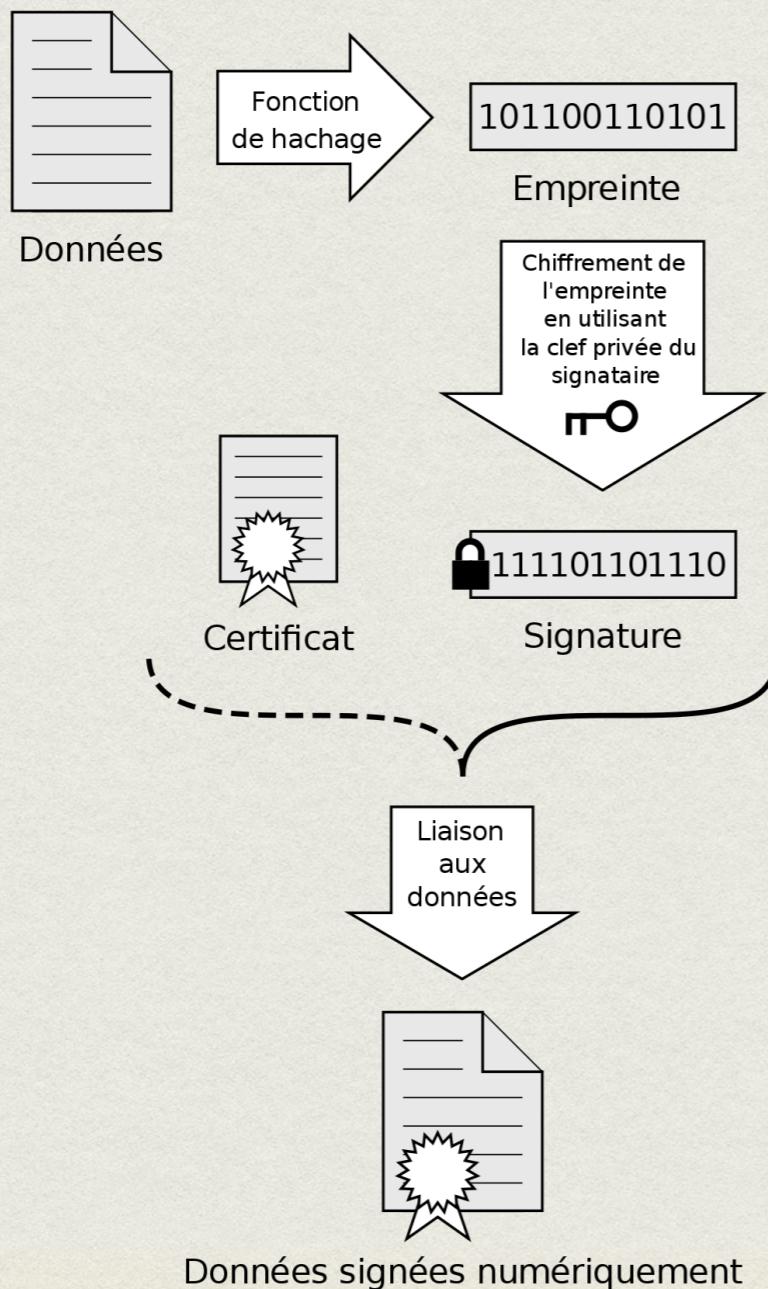
pub

m+chiffré

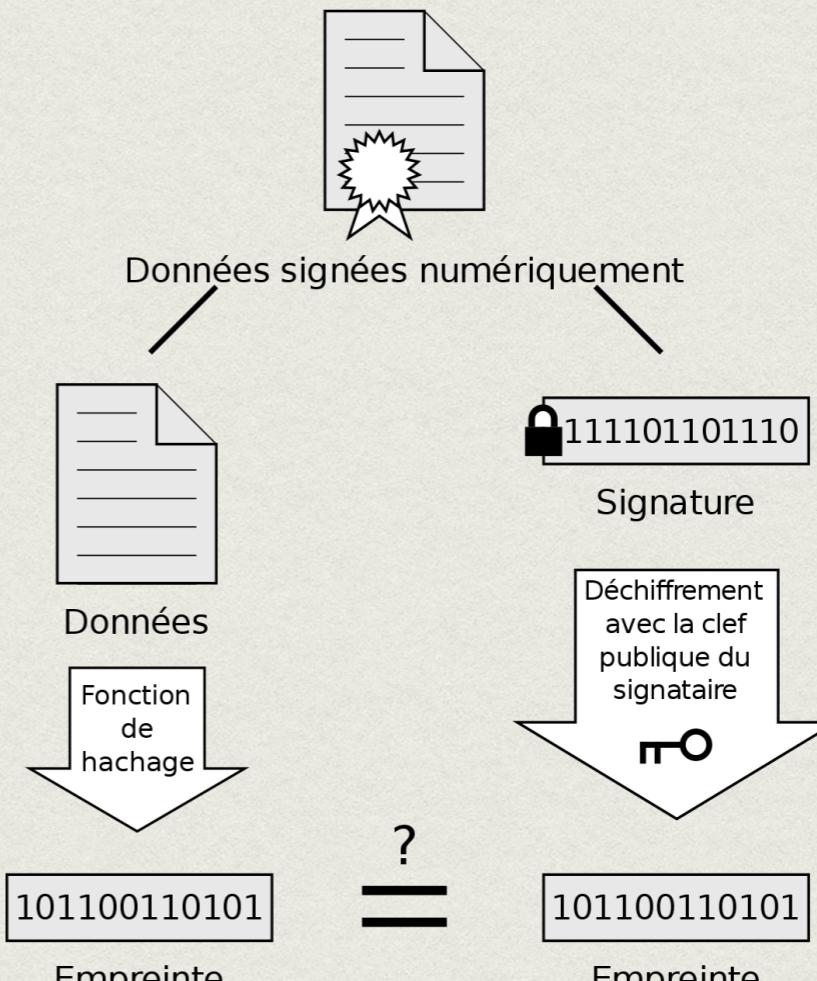


SIGNATURES ÉLECTRONIQUES

Signature



Vérification

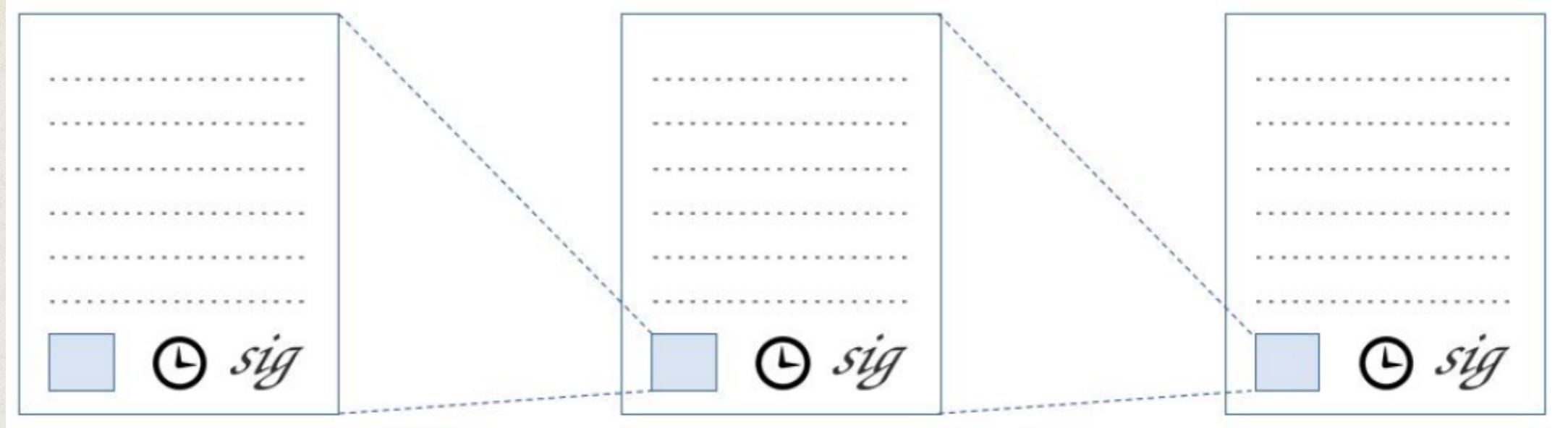


Si les empreintes sont identiques, la signature est valide

BLOCKCHAIN

- Rien de nouveau techniquement
 - stockage distribué P2P (1999: Napster, 2000: eDonkey, 2001: BitTorrent, etc.)
 - consensus distribué
 - **Chaînes d'horodatage**
 - Dépense énergétique liée à la résolution de problèmes difficiles
- Basé sur des fonctions cryptographiques particulières (fonctions de hachage, signatures)

CHAINE D'HORODATÉE



- Chaque nouveau message incorpore le document, sa date de génération, le haché du message précédent et une signature
- Cela forme une chaîne
- A partir d'un bloc on peut valider tous les blocs précédents
- On doit disposer (distribuer) toute la chaîne depuis le premier bloc

DÉPENSE ÉNERGÉTIQUE (PROOF-OF-WORK)

- Objectif: s'assurer qu'une entité a « payé » pour obtenir un résultat
- On définit un pb mathématique qu'on ne peut résoudre qu'en dépensant une certaine quantité d'énergie (de calcul)
- Hashcash introduit pour lutter contre le spam (si le cout d'envoi d'un message est non nul, plus de spam)
- Réutilisé pour les crypto monnaies

APPLICATIONS DE LA CHAINE DE BLOCS

- Crypto-monnaies
- Assurer la transparence d'un livre de comptes certifiés, de transactions, etc
 - Cadastre ; certification des diplômes ; signature des logiciels/ pilotes certifiés/signés
 - **Le contraire de l'anonymat !**
- On peut imaginer que cela puisse remplacer tout intermédiaire qui n'a pas de valeur ajoutée (notaires...?)

APPLICATIONS DE LA CHAINE DE BLOCS



APPLICATION FORM DE LA

A.T.A. CARNET / CARNET A.T.A.

FOR TEMPORARY ADMISSION OF GOODS

POUR L'ADMISSION TEMPORAIRE DES MARCHANDISES

CUSTOMS CONVENTION ON THE A.T.A. CARNET FOR THE TEMPORARY ADMISSION OF GOODS

CONVENTION DOUANIÈRE SUR LE CARNET A.T.A. POUR L'ADMISSION TEMPORAIRE DES MARCHANDISES

CONVENTION ON TEMPORARY ADMISSION / CONVENTION RELATIVE À L'ADMISSION TEMPORAIRE

(Before completing the Carnet, please read Notes on cover page 3 / Avant de remplir le carnet, lire la notice en page 3 de la couverture)

INTERNATIONAL GUARANTEE CHAIN
CHAÎNE DE GARANTIE INTERNATIONALE

W.C.F.

A. HOLDER AND ADDRESS / Titulaire et adresse

B. REPRESENTED BY* / Représenté par*

C. INTENDED USE OF GOODS / Utilisation prévue des marchandises

G. FOR ISSUING ASSOCIATION USE / Réservé à l'association émettrice
FRONT COVER / Couverture

a) CARNET No.
Carnet N° _____
Number of continuation sheets:
Nombre de feuilles supplémentaires: _____

b) ISSUED BY / Délivré par _____

c) VALID UNTIL / Valable jusqu'au
year / année month / mois day (inclusive) / jour (inclus)
_____/_____/_____

P. This Carnet may be used in the following countries/Customs territories under the guarantee of the associations listed on page four of the cover: / Ce carnet est valable dans les pays/territoires douaniers ci-après, sous la garantie des associations reprises en page quatre de la couverture:

ALGERIA (DZ)
ANDORRE (AD)
AUSTRALIA (AU)
AUSTRIA (AT)
BELARUS (BY)
BELGIUM/LUXEMBOURG (BE)
BOSNIA AND HERZEGOVINA (BA)
BULGARIA (BG)
CANADA (CA)
CHILE (CL)
CHINA (CN)
CÔTE D'IVOIRE (CI)
CROATIA (HR)
CYPRUS (CY)
CZECH REPUBLIC (CZ)
DENMARK (DK)
ESTONIA (EE)
FINLAND (FI)
FRANCE (FR)
GERMANY (DE)
GIBRALTAR (GI)
GREECE (GR)
HONG KONG, CHINA (HK)
HUNGARY (HU)
ICELAND (IS)
INDIA (IN)
IRAN (IR)

IRELAND (IE)
ISRAEL (IL)
ITALY (IT)
JAPAN (JP)
KOREA (REP. OF) (KR)
LATVIA (LV)
LEBANON (LB)
LITHUANIA (LT)
MACAO, CHINA (MO)
REPUBLIC OF MACEDONIA (MK)
MALAYSIA (MY)
MALTA (MT)
MAURITIUS (MU)
MEXICO (MX)
MOLDOVA (MD)
MONGOLIA (MN)
MONTENEGRO (ME)
MOROCCO (MA)
NETHERLANDS (NL)
NEW ZEALAND (NZ)
NORWAY (NO)
PAKISTAN (PK)
POLAND (PL)
PORTUGAL (PT)
ROMANIA (RO)
RUSSIA (RU)
SENEGAL (SN)

SERBIA (CS)
SINGAPORE (SG)
SLOVAK REPUBLIC (SK)
SLOVENIA (SI)
REPUBLIC OF SOUTH AFRICA (ZA)
SPAIN (ES)
SRI LANKA (LK)
SWEDEN (SE)
SWITZERLAND (CH)
THAILAND (TH)
TUNISIE (TN)
TURKEY (TR)
UKRAINE (UA)
UNITED ARAB EMIRATES (AE)
UNITED KINGDOM (GB)
UNITED STATES (US)

The holder of this Carnet and his representative will be held responsible for compliance with the laws and regulations of the country/Customs territory of departure and the countries/Customs territories of importation. / A charge pour le titulaire et son représentant de se conformer aux lois et règlements du pays/territoire douanier de départ et des pays/territoires douaniers d'importation.

H. CERTIFICATE BY CUSTOMS AT DEPARTURE
Attestation de la douane, au départ

a) Identification marks have been affixed as indicated in column 7 against the following item No(s), of the General List
Apposé les marques d'identification mentionnées dans la colonne 7 en regard du (des) numéro(s) d'ordre suivant(s) de la liste générale

b) GOODS EXAMINED* / Vérifié les marchandises*
Yes / Oui No / Non

c) Registered under Reference No.*
Enregistré sous le numéro*

d) Customs Office _____ Place _____ Date (year/month/day) _____ Signature and Stamp
Bureau de douane _____ Lieu _____ Date (année/mois/jour) _____ Signature et timbre

i. Signature of authorised official and Issuing Association stamp / Signature du délégué et timbre de l'association émettrice

Place and Date of Issue (year/month/day)
Lieu et date d'émission (année/mois/jour)

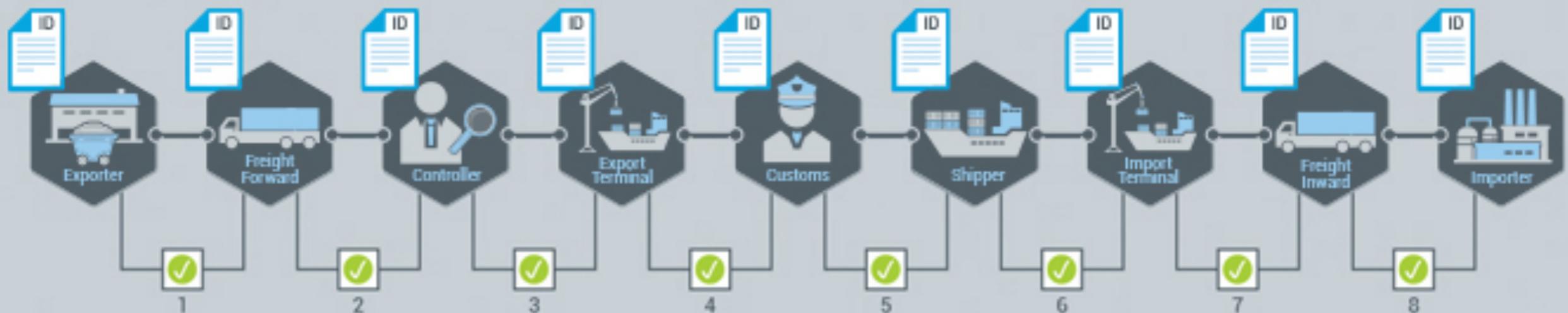
J. _____ X _____
Signature of Holder / Signature du titulaire

*If applicable / *S'il y a lieu

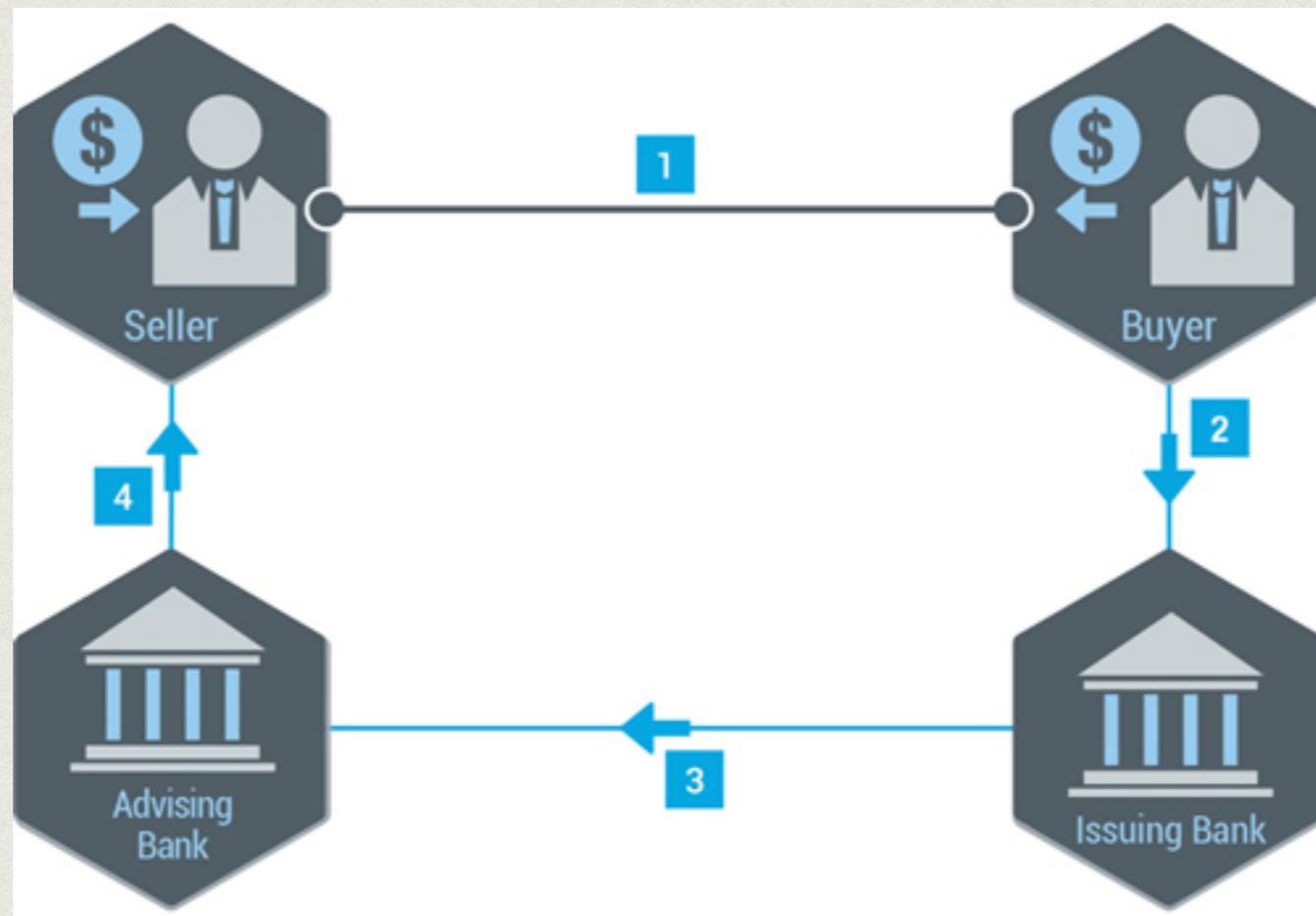
TO BE RETURNED TO THE ISSUING CHAMBER IMMEDIATELY AFTER USE
A RETOURNER À LA CHAMBRE ÉMETTRICE IMMÉDIATEMENT APRÈS UTILISATION

APPLICATIONS DE LA CHAINE DE BLOCS

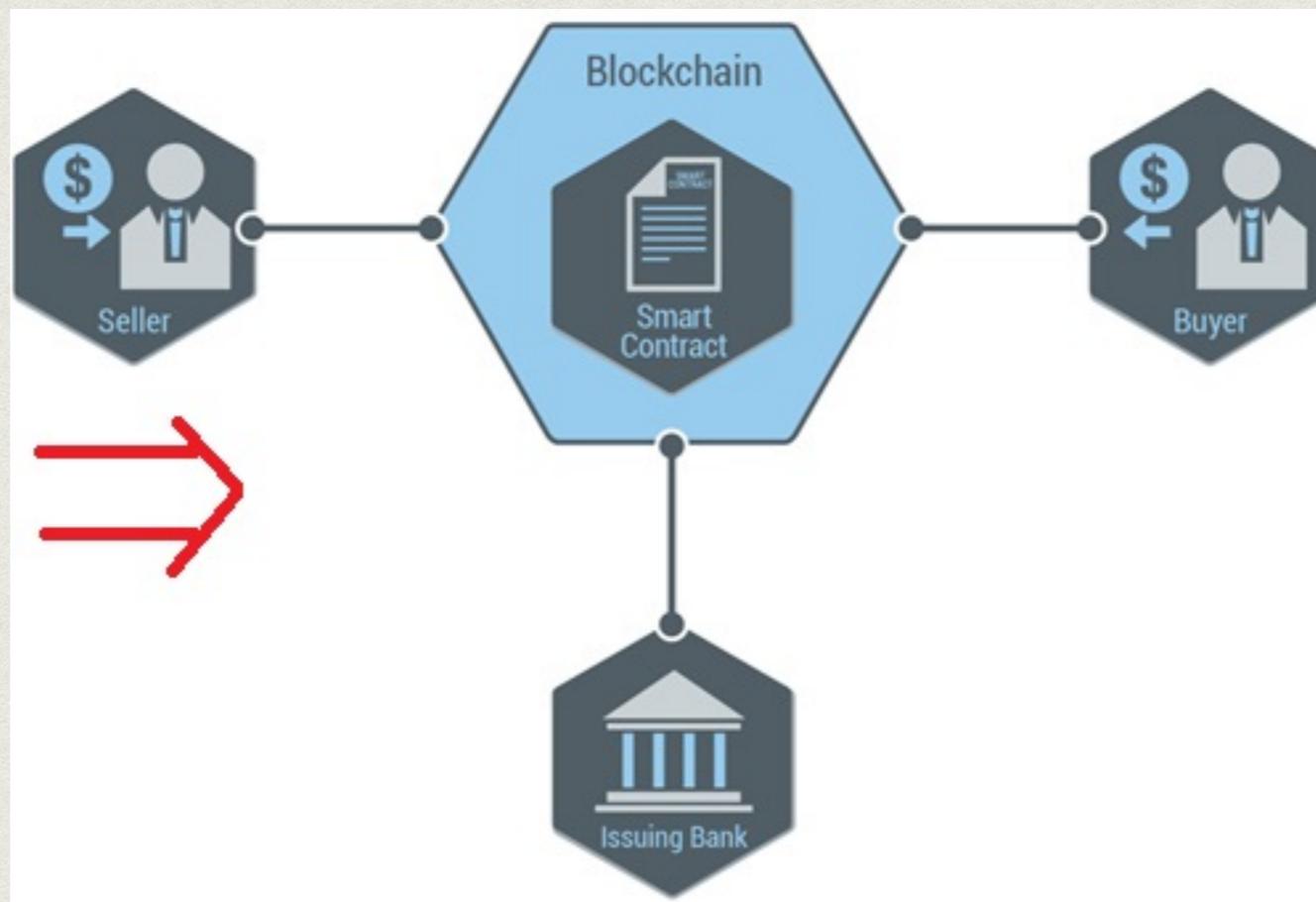
Supply Chain Logistics



APPLICATIONS DE LA CHAINE DE BLOCS



APPLICATIONS DE LA CHAINE DE BLOCS



PRO/CONS

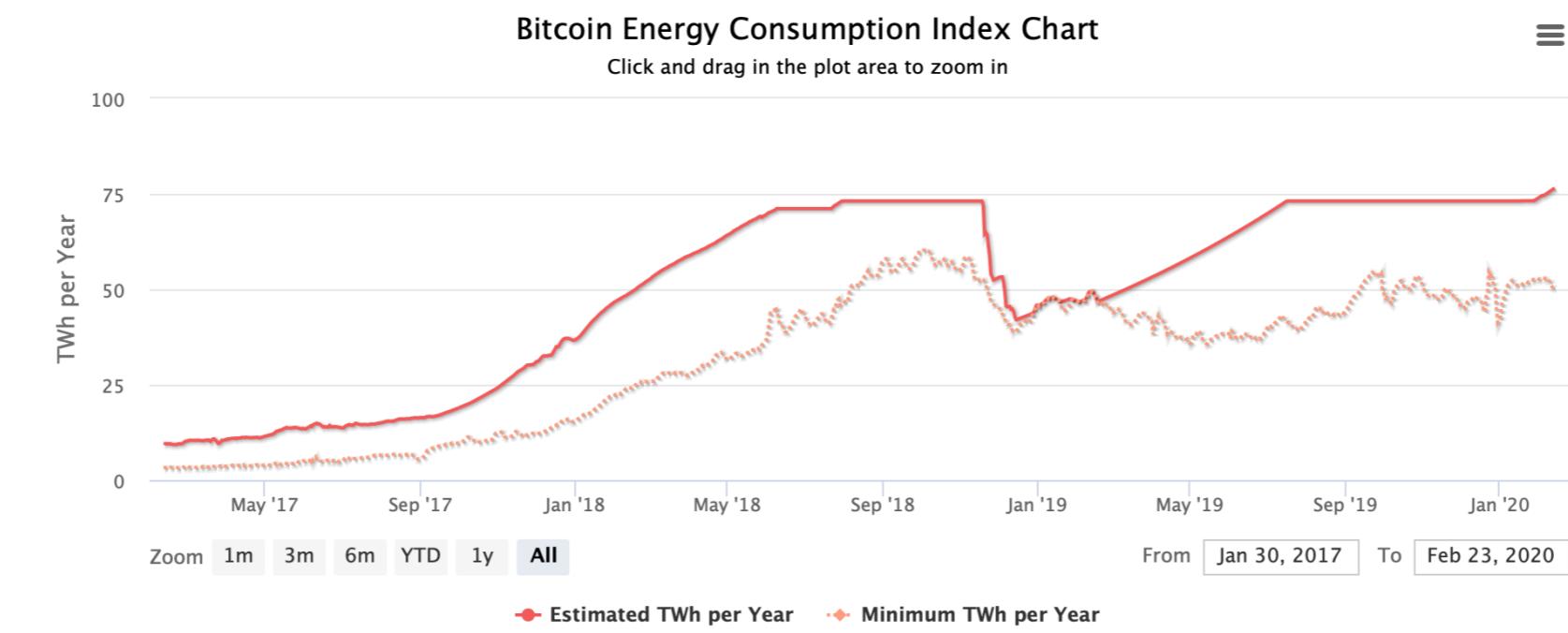
- Magnifique !
 - Moins d'intermédiaires inutiles/peu scrupuleux
 - De la confiance entre entités (numériques)
- Mais
 - Que se passe t'il si un opérateur contrôle plus de 50% des noeuds ?
 - Jusqu'à quand grandit la chaîne de blocs ?
actuellement 200 Go/noeud, 11.000 noeuds actifs début 2020, 1 validation de bloc toutes les 10min.
 - Beaucoup d'énergie dépensée pour « rien », cf ici ou là
entre 30 et 80 TWh/an ; empreinte carbone de 15 à 40 MtCO₂-eq, comparables à celle de l'Autriche, la Belgique ou le Danemark
- Alternatives : problèmes utiles ou pas de proof-of-work mais proof-of-stake (preuve d'enjeu, de possession)
NB: Ethereum doit passer en 2020 à une preuve d'enjeu, gain estimé facteur 1.000 ou 10.000

PRO/CONS

- Magnifique
- Moins
- De la c
- Mais
- Que se
- Jusqu'
- actuel
- Beaucou entre l'Autri
- Alternative

Bitcoin Energy Consumption Index

NEW: Bitcoin Electronic Waste Monitor



Download data.

Annualized Total Footprints

Carbon Footprint

36.34 Mt CO₂



Comparable to the carbon footprint of New Zealand.

Electrical Energy

76.51 TWh



Comparable to the power consumption of Chile.

Electronic Waste

10.79 kt



Comparable to the e-waste generation of Luxembourg.

CRYPTO-JACKING

- Miner de la crypto-monnaie à l'insu du propriétaire d'un ordinateur
 - logiciel malveillant, virus, etc ?
 - une librairie qui se cache dans un logiciel ou un site web
 - jeux gratuits, site de streaming « pirate »

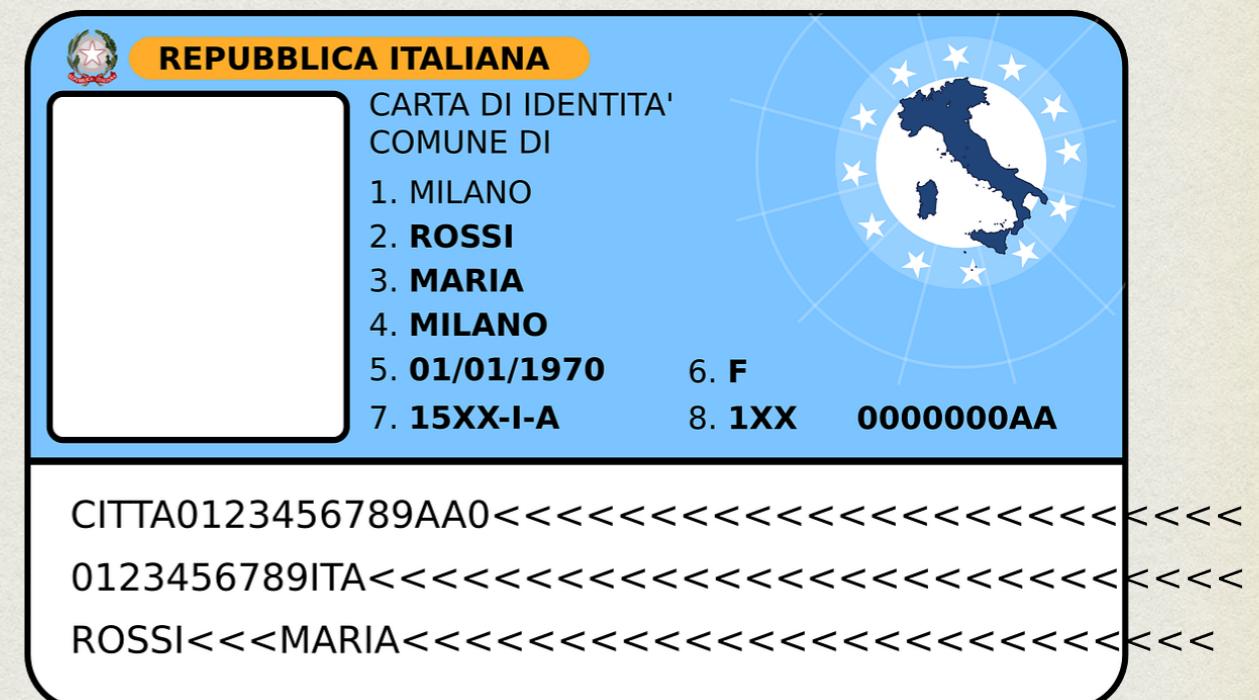
ANONYMAT ET BTC ?

- Pourquoi on croit qu'on est **anonyme** avec des **Bitcoin** ?
 - alors que c'est plutôt la **transparence** la propriété principale !
 - **pseudonymes**/signatures, pas directement des IDs
- Autres crypto-monnaies plus anonymes
 - Monero : anneaux de signatures et adresses furtives
 - Zcash : base sur preuves à divulgation nulle (ZKP) permet de cacher les montants et IDs d'une transaction

ACCREDITATIONS ANONYMES

ACCREDITATION

- Preuve de qualification, de compétence ou d'autorisation
 - émis par une autorité pour un individu
 - ex : passeport, permis de conduire, carte de bibliothèque, carte de transport
 - Généralement nominative, contient des données personnelles (adresse, date de naissance, profil biométrique etc.)



ACCRÉDITATION ANONYME

- Version **anonyme** : preuve d'une propriété, sans révéler son identité
 - Anonymat (**prouveur**), voire parfois non-chainabilité
- Souvent sous la forme d'un **jeton cryptographique**
 - Crée et certifié par une autorité de confiance
 - Vérifiable par d'autres entités (**vérificateurs**)



DIFFÉRENTS USAGES

- Usage unique : monnaie électronique, ticket de transport, place de concert
- Usage multiple : pas de non-chainabilité
 - Plusieurs accréditations à usage unique ? combien ?



MONNAIE PHYSIQUE

#série → étagable



pas de #série



MONNAIE DIGITALE

- Equivalent numérique de la monnaie physique mais comment empêcher de « copier » une pièce digitale ?
- Propriétés :
 - Anonyme
 - Une seule dépense ou détection (probabilité non-négligeable)
 - On ne peut pas forger de nouvelles pièces
 - Possible avec des accréditations anonymes



ACCRÉDITATIONS ANONYMES

- Propriétés
 - Anonymat de l'utilisateur
 - Non-chainabilité (ré-utilisation de l'accréditation)
 - Dévoilement partiel
 - Non-forgeable
 - Non-partageable
- Preuves à divulgation nulle
 - Je prouve (crypto) que je connais un secret sans le dévoiler
 - Signatures aveugles
 - L'autorité m'a signé (crypto) un certificat sans le voir
 - une partie du message qu'elle a signé était cachée
 - par ex. $D(S(C(m)))$

SIGNATURE AVEUGLE

- Faire signer un message sans le voir (Chaum'83)

- Donc pas un haché du message

- Vérifiable grâce à une clé publique

- Vote électronique, argent digital anonyme

- Exemple avec RSA :

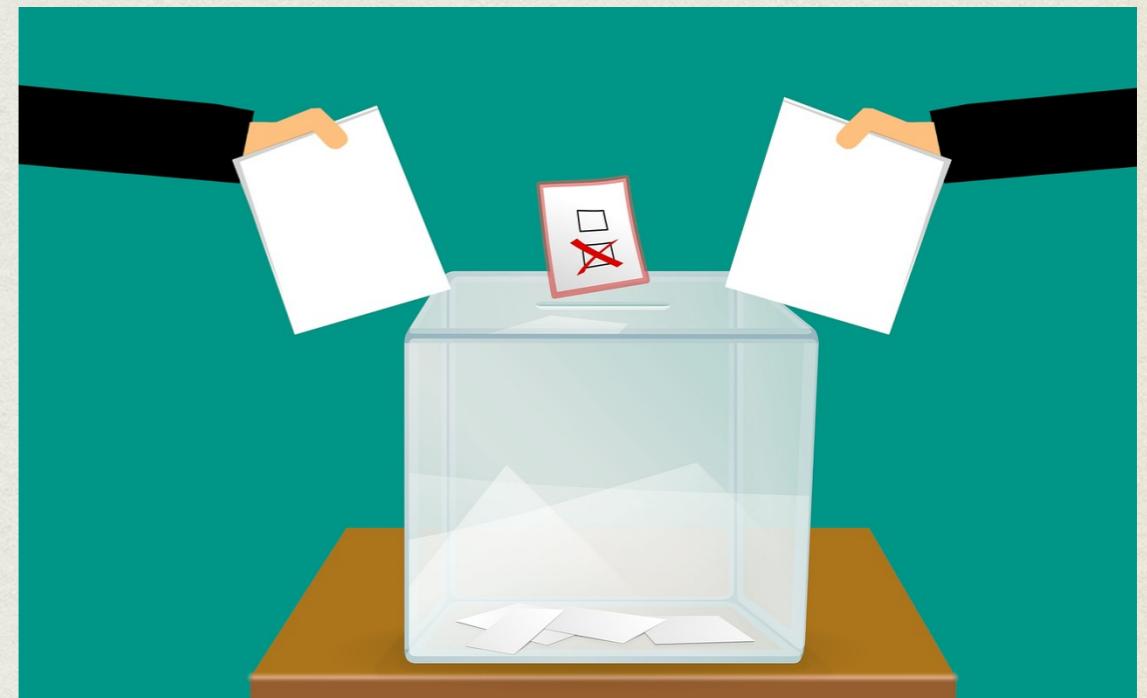
$$S(m) \cong m^d \pmod{n} \implies S(r \cdot m) \cong (r \cdot m)^d \pmod{n} \implies S(m) \cong \frac{S(r \cdot m)}{r}$$

- Attention: signer RSA équivaut à déchiffrer, un adv peut l'exploiter pour faire déchiffrer des chiffrés RSA. Faire signer un haché du message ?



VOTE PAR SIGNATURE AVEUGLE

- Propriétés :
 - Un électeur ne vote qu'une fois
 - Les votes sont secrets
- Exemple de protocole simplifié :
 - Vote avec accréditation à usage unique
 - Bulletin de vote signé en aveugle
 - Bulletin envoyé dans l'urne par un réseau de communication anonyme



SIGNATURE DE GROUPE

- Méthode qui prouve l'appartenance à un groupe (Chaum et Van Heyst'91)
- Signer anonymement un message de la part du groupe
 - clés privées de signatures SK_i (on ne peut retrouver i à partir d'une signature)
 - clé publique de vérification VK
- Permet de s'authentifier anonymement de façon non-chainable
- Option : révocation de l'anonymat

PROPRIÉTÉS DES SIGNATURE DE GROUPE

- **Consistance et solidité** : signature valide -> vérifiée correctement et invalide -> rejetée
- **Résistance à la contrefaçon** : seuls les membres du groupe peuvent produire des signatures valides
- **Anonymat** : impossible de retrouver quel membre du groupe a signé
- **Non-chainabilité** : impossible de savoir si deux messages signés l'ont été par le même membre du groupe
- **Non-coalition** : impossible de générer une signature au nom d'un autre membre du groupe, même en cas de coopération entre plusieurs membres

RETRAIT D'INFORMATION PRIVÉ

RETRAIT D'INFORMATION PRIVÉ

- **PIR** pour *Private Information Retrieval*
- **Définition informelle:** protocole qui permet à un utilisateur de récupérer un élément dans une base de données sans révéler son choix
- Retrait d' {Information Privée} : non l'**information** est a priori **publique**
- {Retrait privé} d'information : c'est la **sélection** qui est **privée**
- Ex: Netflix, Stock Exchange, License et brevets, etc.

RETRAIT D'INFORMATION PRIVÉ

- **PIR Naïf** : le serveur envoie au client toute la base de données
 - Généralement pas faisable, on veut faire mieux : $O < |DB|$
- **PIR Informationnel** : le client demande des informations à plusieurs serveurs pour cacher son choix
- **PIR Calculatoire** (computationnel) : le serveur doit effectuer un calcul sur toute la base de données pour construire la réponse à la requête du client

CHIFFREMENT HOMOMORPHE 101

- **Chiffrement non-homomorphe**

- $D_k(C_k(m)) = m$
- $D_k(C_k(m_1) + C_k(m_2)) = \text{noise}$

- **Chiffrement homomorphe**

- $D_k(C_k(m)) = m$
- $D_k(C_k(m_1) \oplus C_k(m_2)) = m_1 + m_2$ (**additif**)
- $D_k(C_k(m_1) \odot C_k(m_2)) = m_1 \cdot m_2$ (**multiplicatif**)

- **Complètement** homomorphe vs. **Partiellement** homomorphe

- Nombre d'opérations homomorphes bornées ou non
- Info-nuagique sur données chiffrées, chiffrement cherchable, etc..

RETRAIT D'INFORMATION PRIVÉ

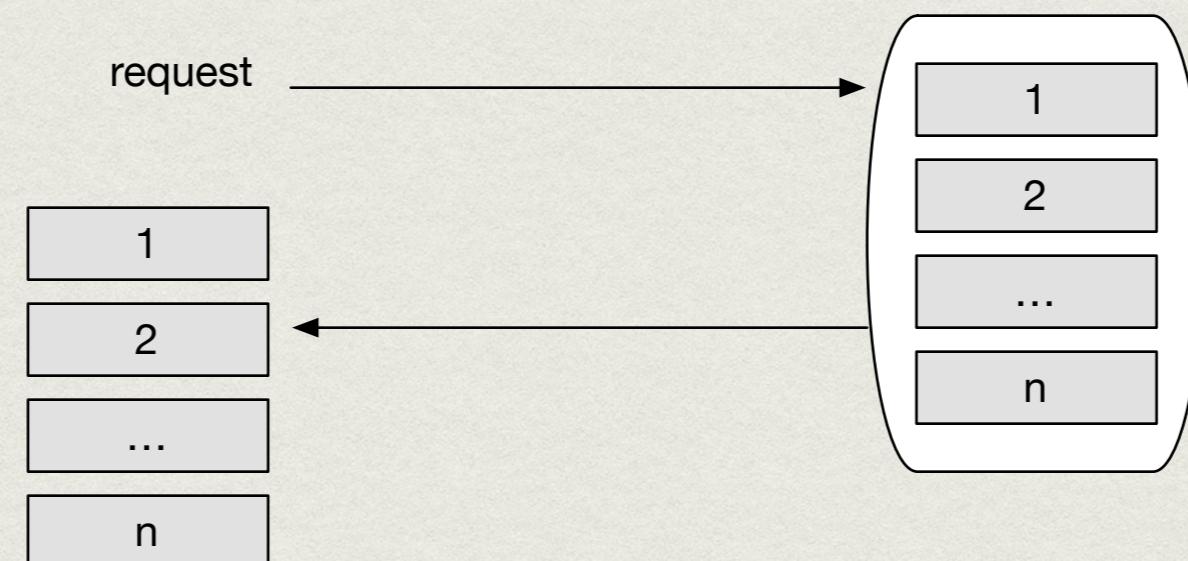
- Ce que l'on veut



- C envoie i et reçoit l'élément i

RETRAIT D'INFORMATION PRIVÉ

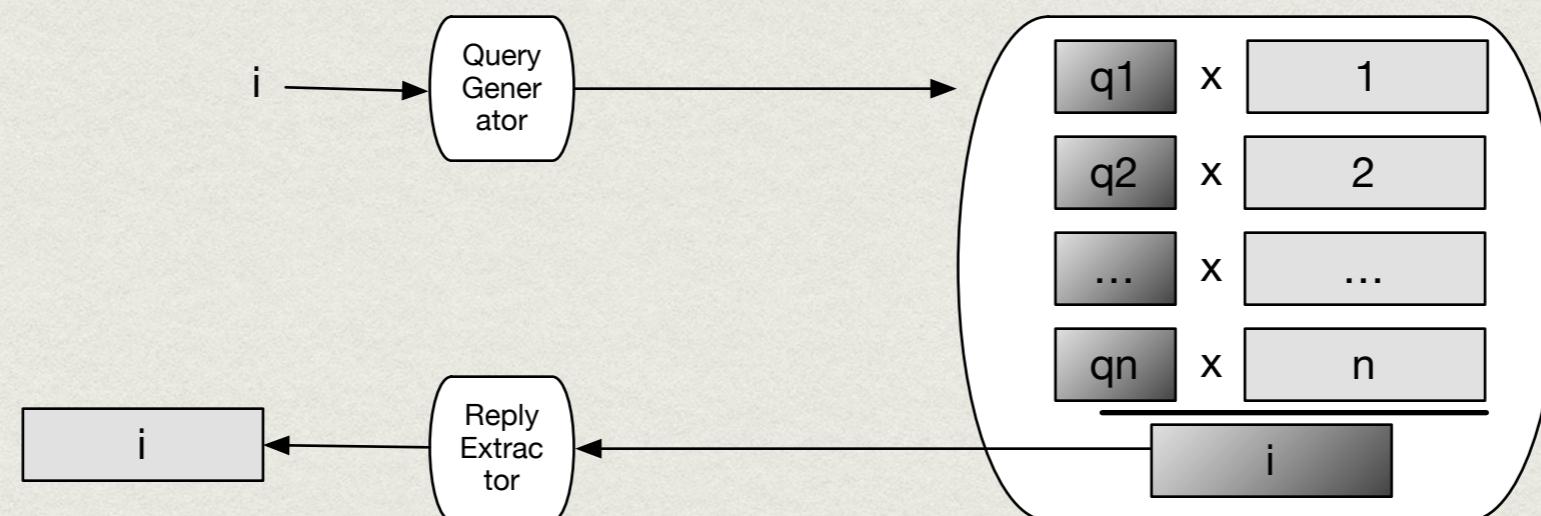
- Ce que l'on ne veut pas



- C reçoit toute la base de données

RETRAIT D'INFORMATION PRIVÉ

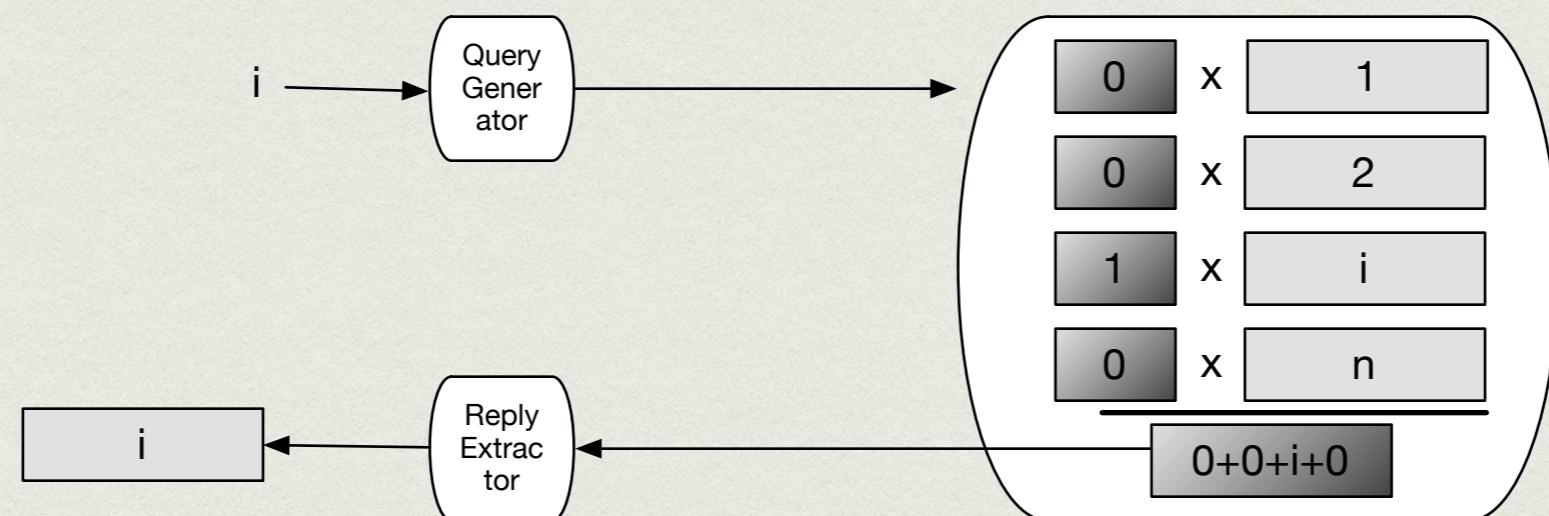
- PIR à base de chiffrement homomorphe



- Calcul: n additions et 1 multiplication
Espace: $O(\text{taille d'un élément})$

RETRAIT D'INFORMATION PRIVÉ

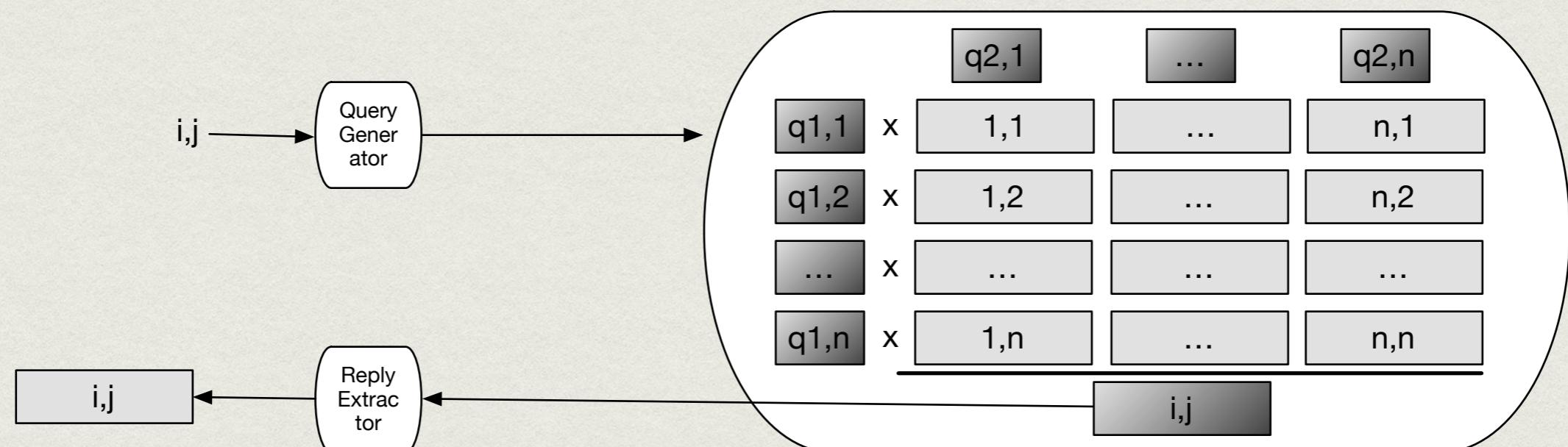
- PIR à base de chiffrement homomorphe



- Calcul: n additions et 1 multiplication
Espace: $O(\text{taille d'un élément})$

RETRAIT D'INFORMATION PRIVÉ

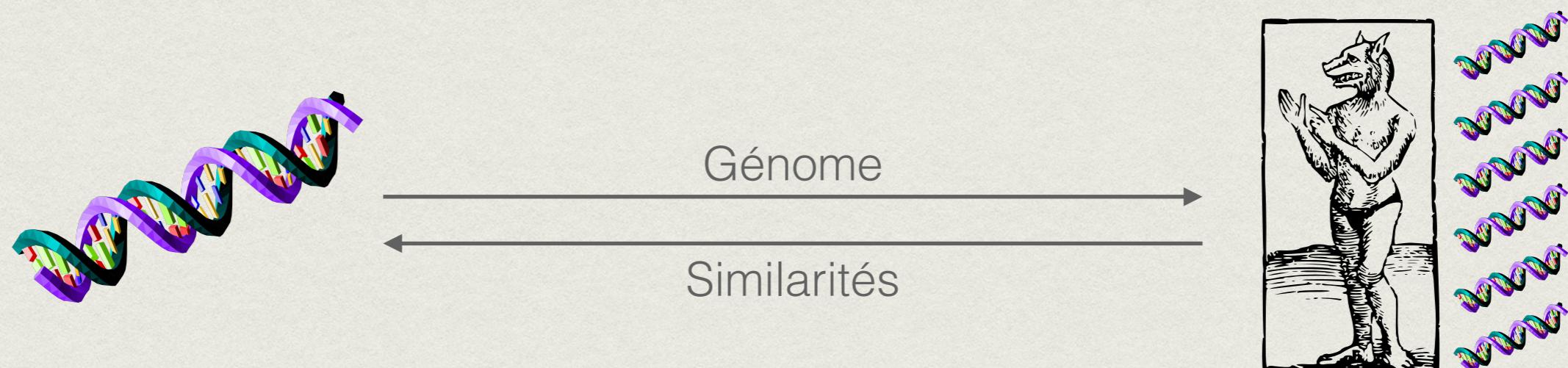
- Généralisation à plusieurs dimensions



- Taille de la requête diminue de $O(n)$ à $O(\sqrt{n})$

AUTRES TACS GRACE AUX CHIFFREMENT HOMOMORPHE

- Le chiffrement homomorphe permet d'envisager toute sorte de TAC
 - **Intersection ensembliste privée** (PSI): quels sont les contacts WhatsApp que nous avons en commun ?
 - Similarité entre un génome et une base de données : mon génome est-il proche de celui des Lycantropes ?

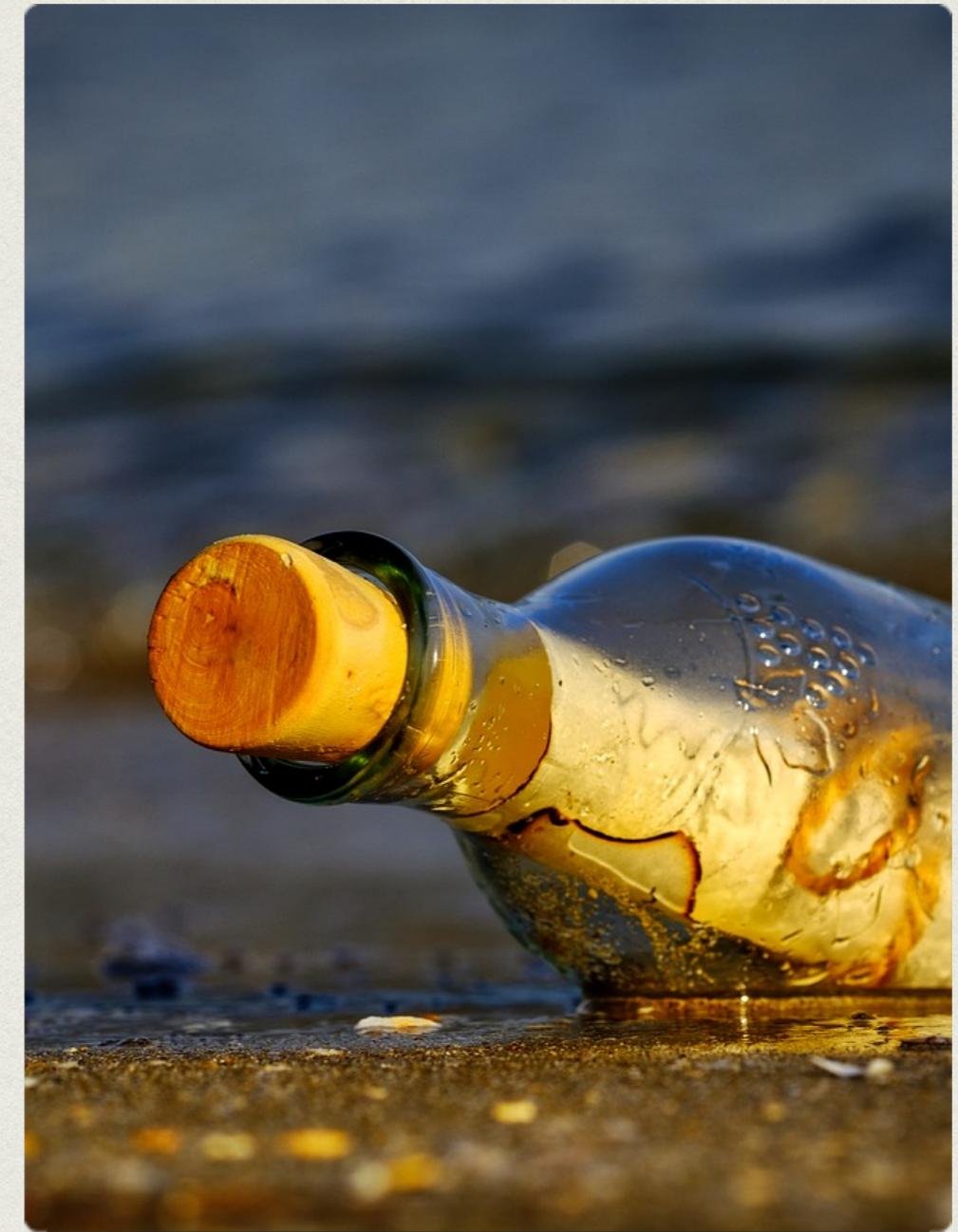


- En particulier, un cryptosystème homomorphe avec des clairs en binaire :
 - Multiplication = AND ; Addition = XOR **Tout est possible ! (mais peut-être un peu lent...)**

MESSAGERIES SÉCURISÉES

MESSAGES INSTANTANÉS

- WhatsApp, FB Messenger, Telegram, Signal, Skype, etc.
- Quelle confidentialité ?
 - chiffrement transport ou bout-en-bout ?
- Contre quel adversaire ?
 - Curieux ? Malveillants ? Agences étatiques ?



QUELLE CONFIDENTIALITÉ ?

- Au niveau transport : ce qui transite sur le réseau est chiffré, ce qui est sur les dispositifs ou les serveurs non.
 - Protection contre les écoutes réseau. HTTPS, VPNs, etc.
- Bout-en-bout : ce qui sort de l'application est chiffré jusqu'à l'appli réceptrice
 - Protection contre le fournisseur du service, ses employés, son gouvernement/agences
 - Pas de protection si le dispositif est compromis (PWDN)
 - Pas de protection des métadonnées (qui communique avec qui, quand, périodicité, volume d'échange, etc.)

COMPARAISON

Secure Msg

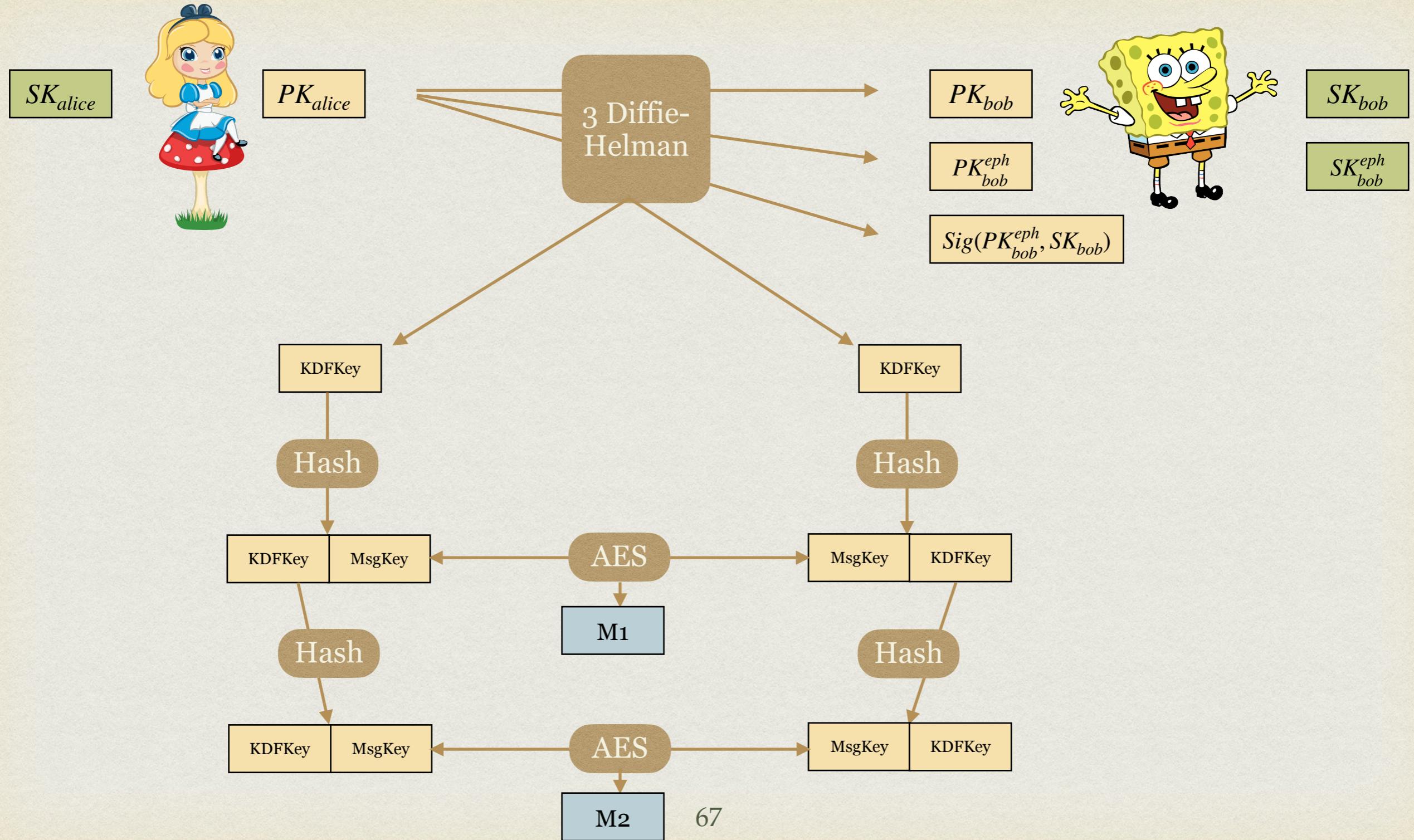
	#users/month	Messages	Group msg	Voice	Video	Web/Other clients	Metadata	Protocol	Owner
WhatsApp	2000000000	E2E	E2E	E2E	E2E	E2E	-	Signal	Facebook
Telegram	400000000	E2E optional	-	-	-	-	-	MTProto (closed source)	frères Durov
Signal	20000000	E2E	E2E	E2E	E2E	E2E	E2E	Signal + Sealed Sender	Signal Foundation

Pour plus de critères/messageries : [SecureMessagingApps](#)

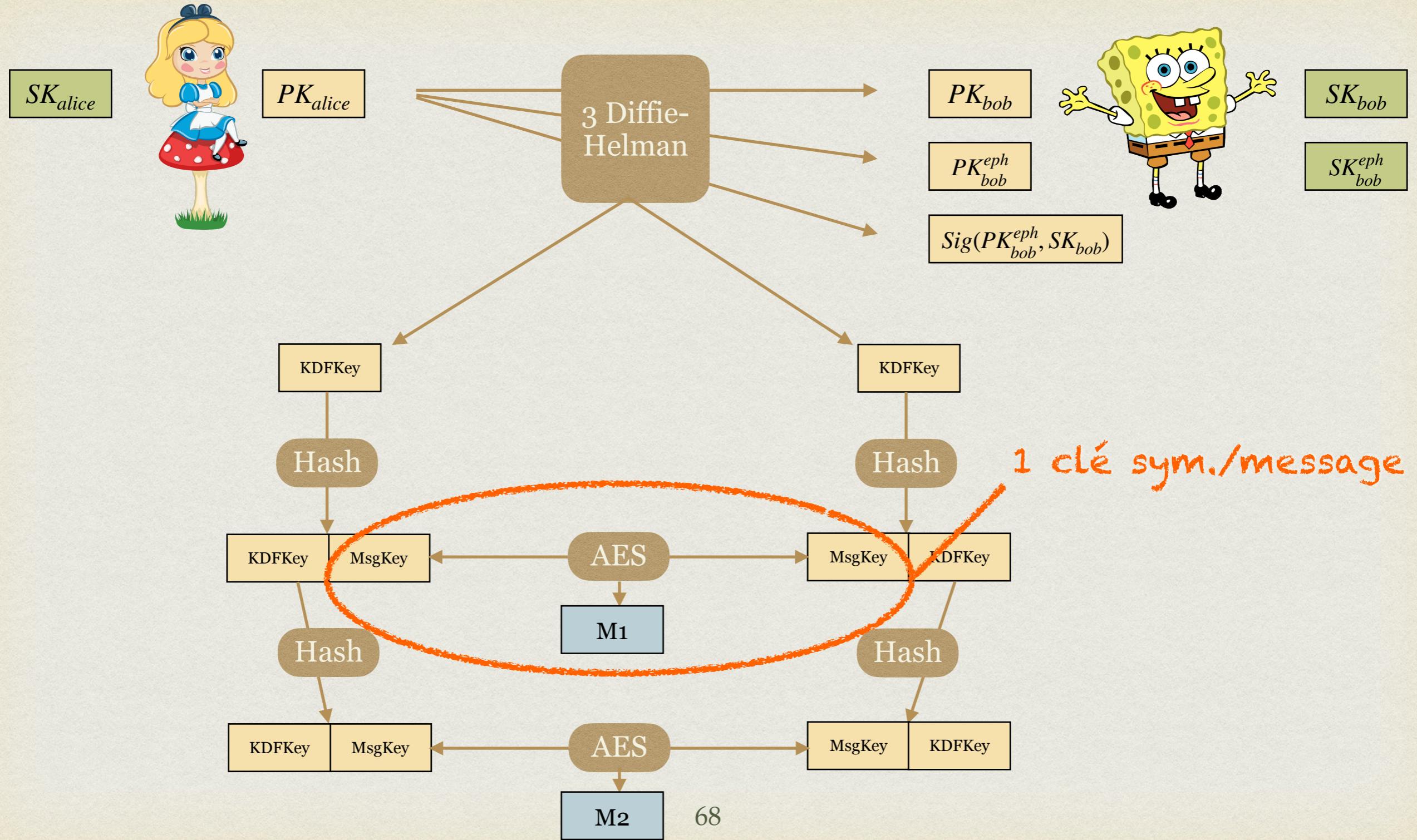
CONFIDENTIALITÉ PERSISTANTE

- *Forward Secrecy*
- Propriété : la découverte de la clé privée par l'adversaire ne compromet pas la confidentialité des messages passés, uniquement les futurs
- Signal: perte du téléphone (ou pwn ou ...) -> les messages passés ne sont plus accessibles
- SSH, OTR, TLS/SSLv3 mais rarement implémenté (OpenSSL oui)

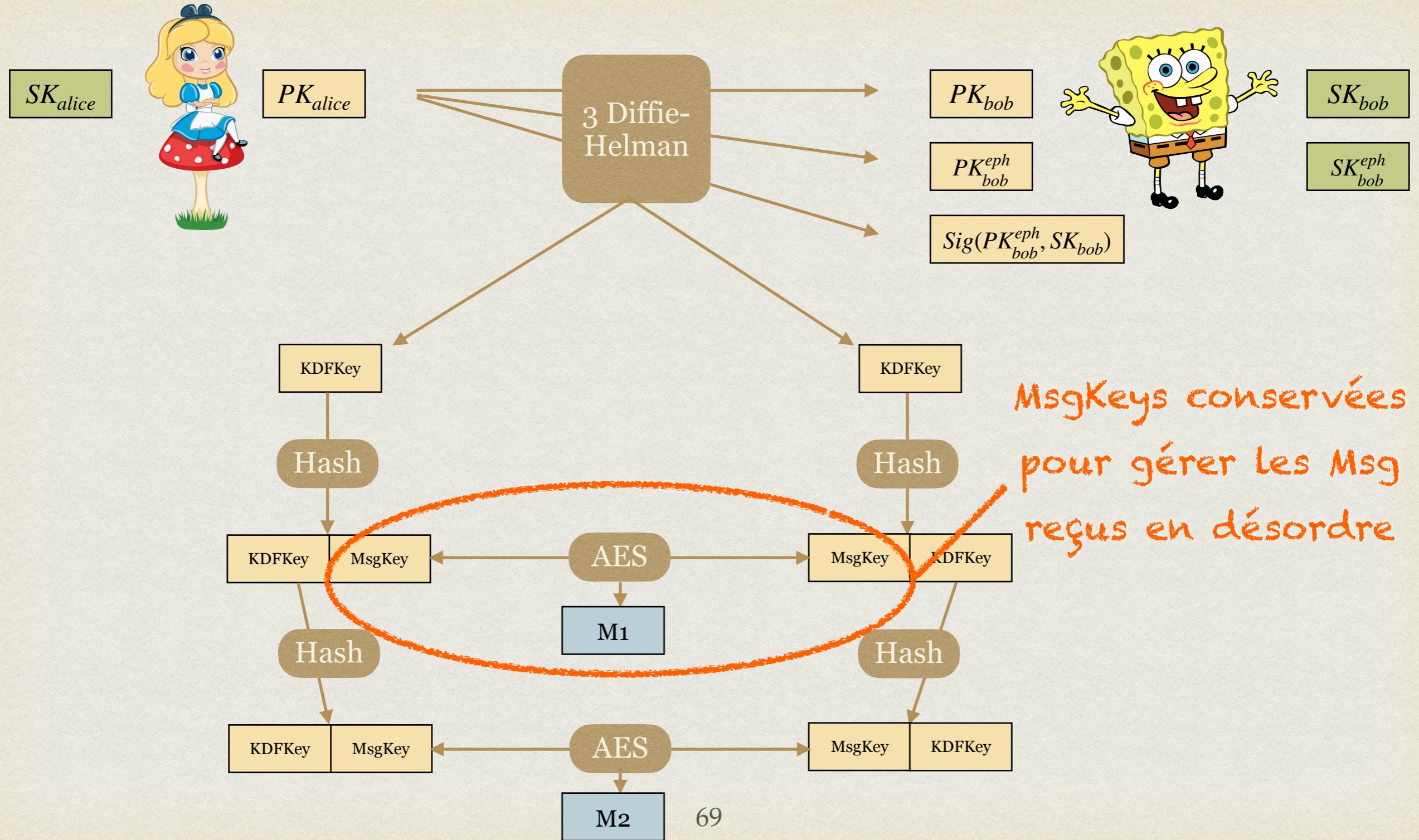
DANS SIGNAL (SIMPLIFIÉ)



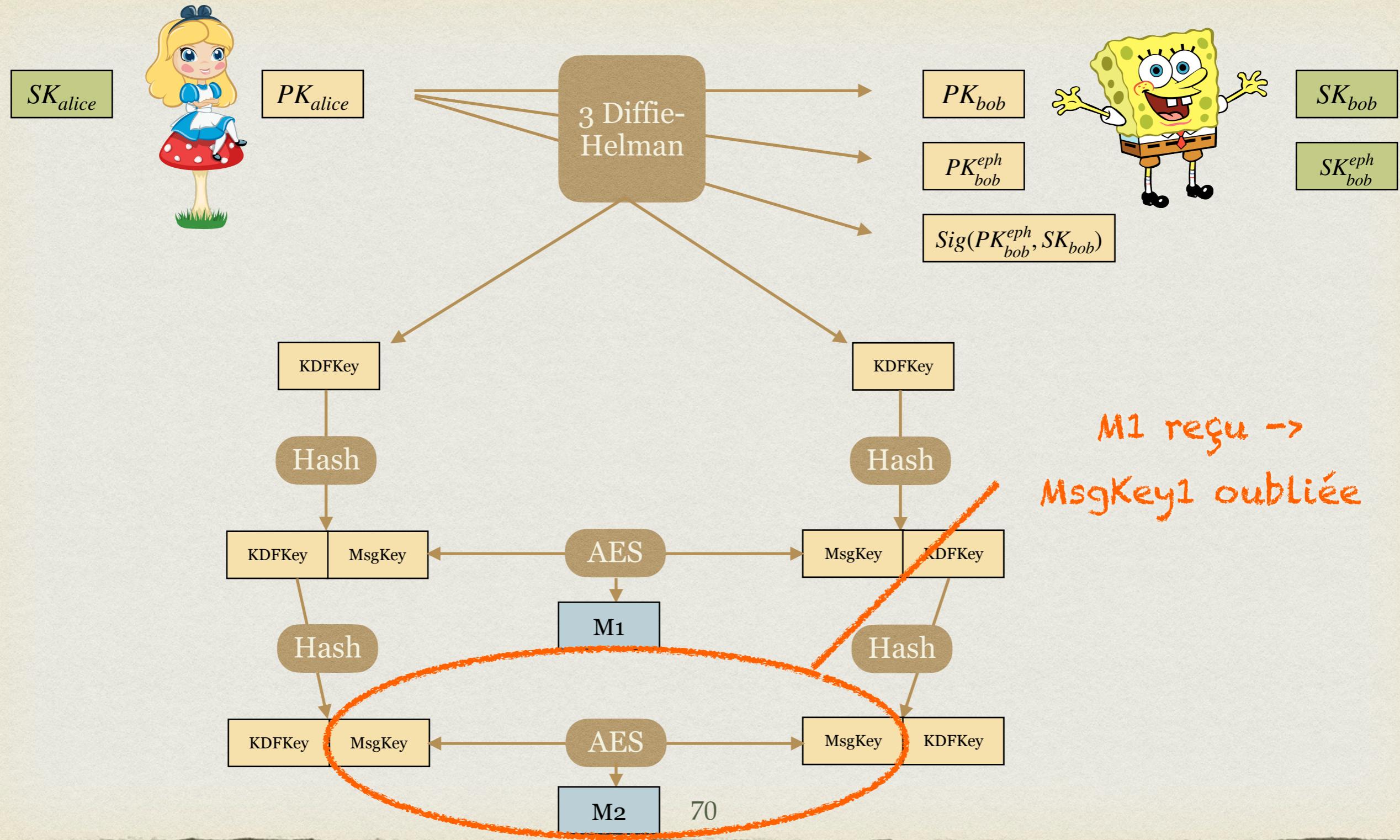
DANS SIGNAL (SIMPLIFIÉ)



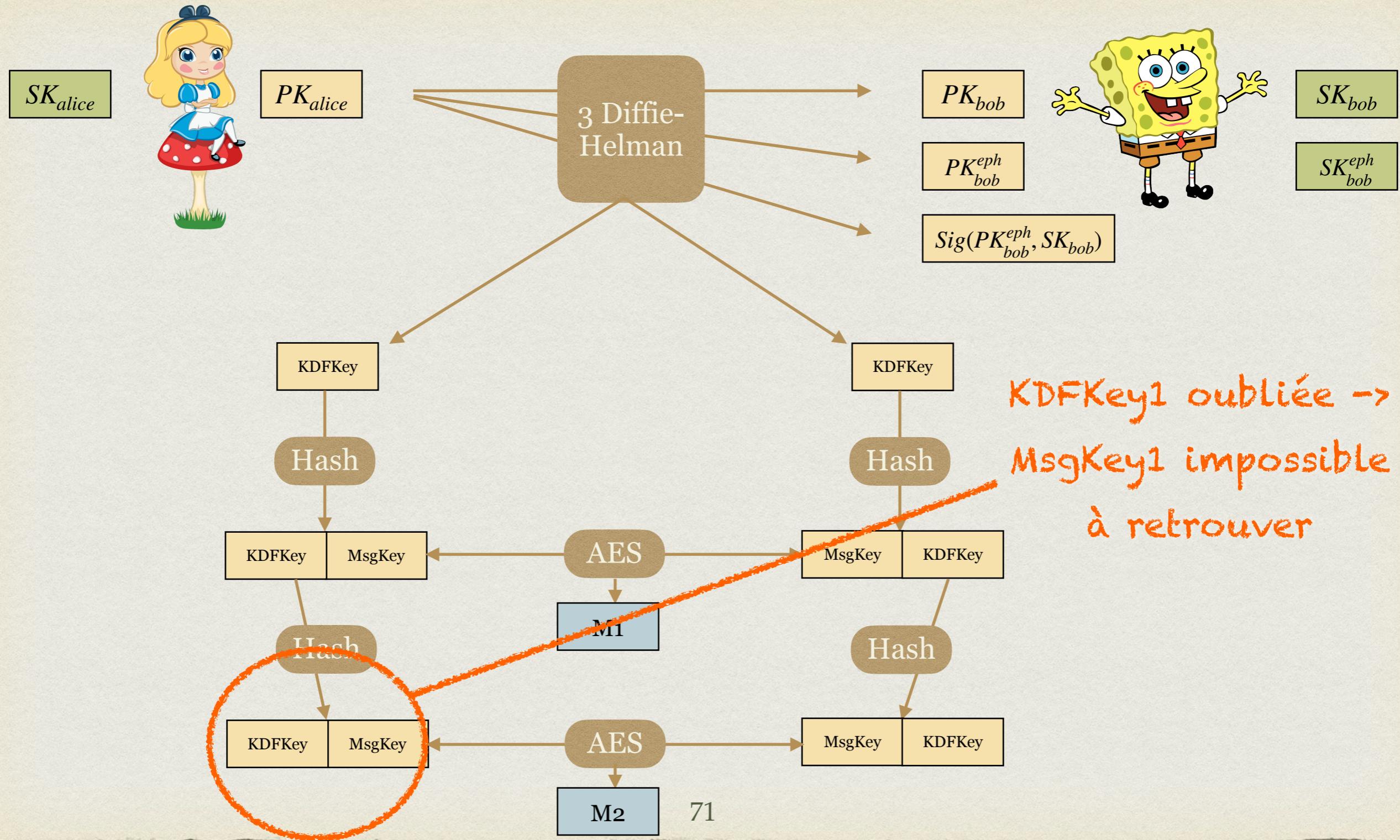
DANS SIGNAL (SIMPLIFIÉ)



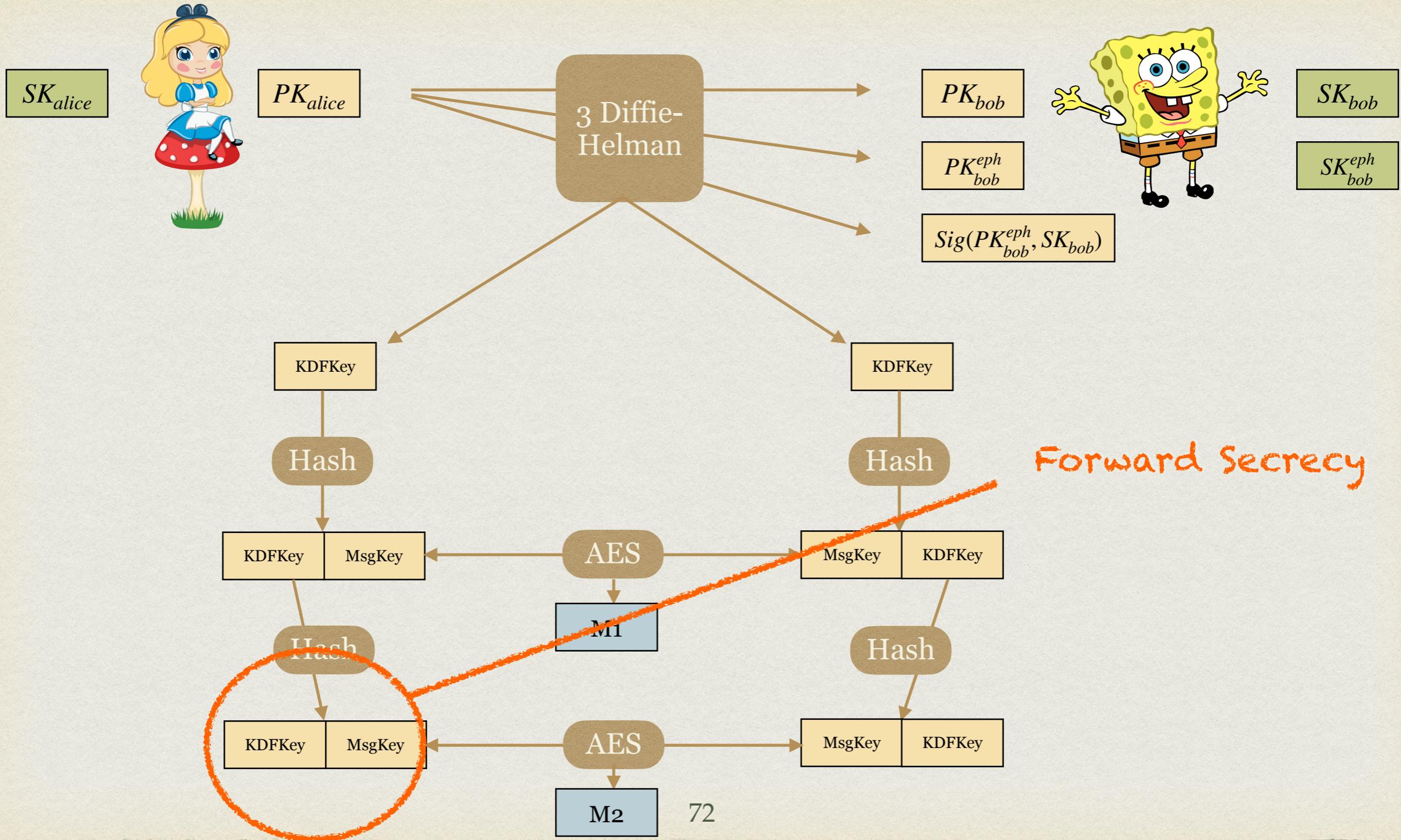
DANS SIGNAL (SIMPLIFIÉ)



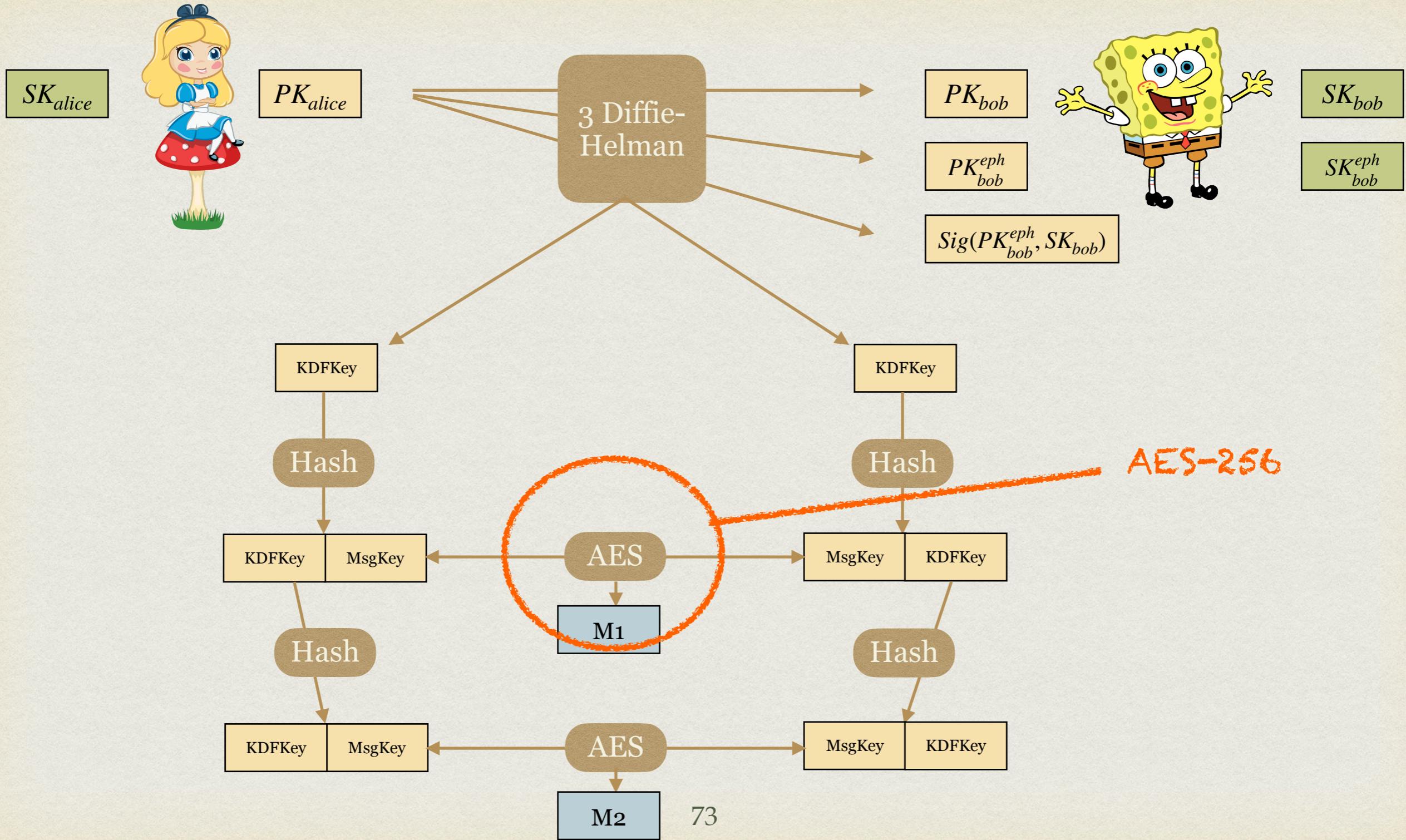
DANS SIGNAL (SIMPLIFIÉ)



RATCHET DANS SIGNAL (SIMPLIFIÉ)



RATCHET DANS SIGNAL (SIMPLIFIÉ)



RATCHET DANS SIGNAL (SIMPLIFIÉ)

