La Cryptographie

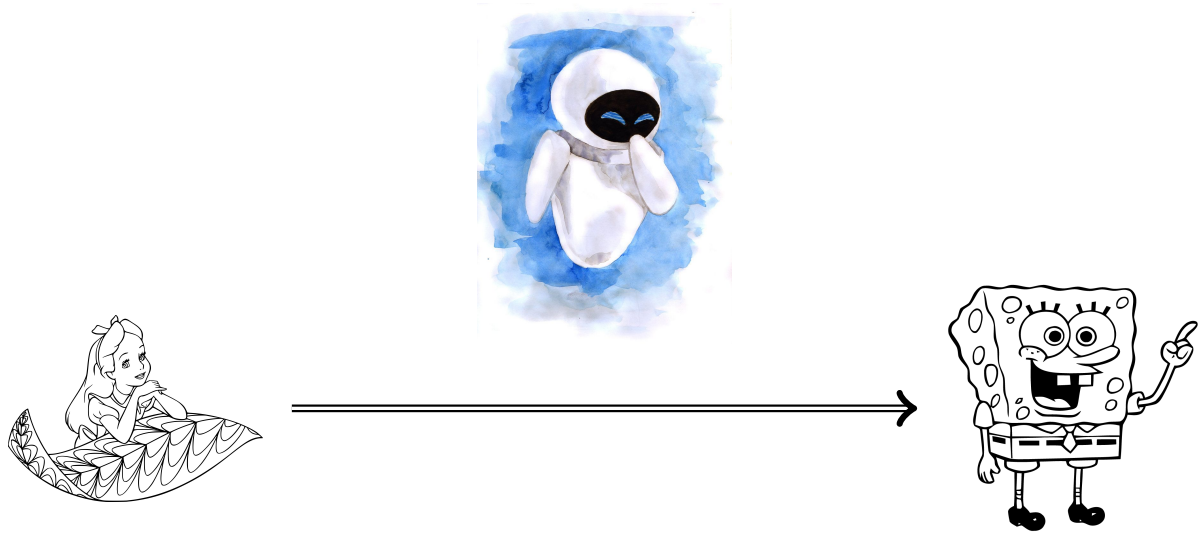
En quoi avons-nous confiance ?

Yann Rotella

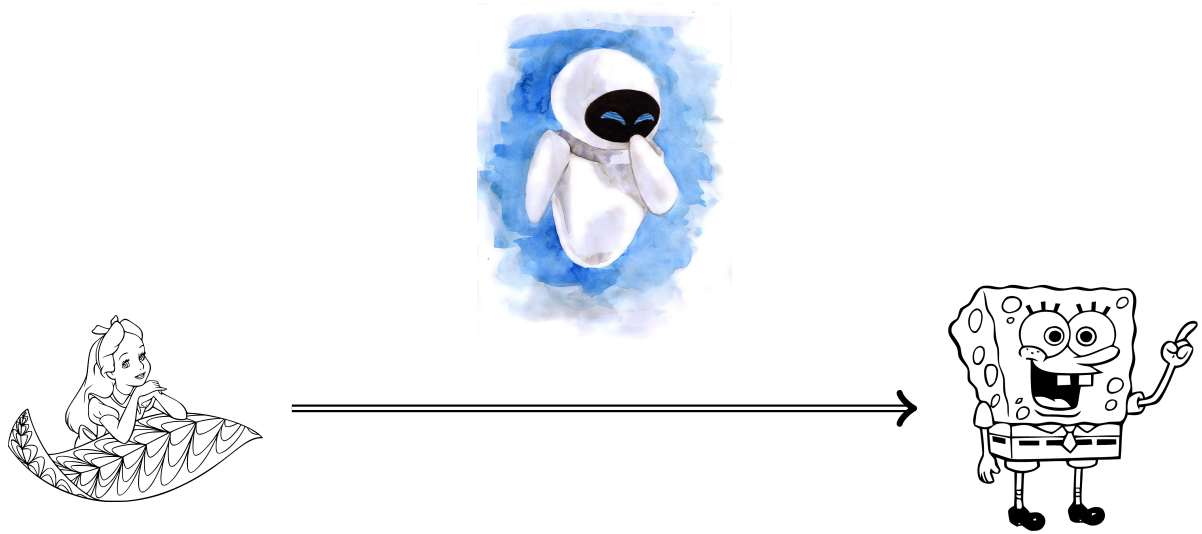
Université de Versailles Saint Quentin en Yvelines

Séminaire DAVID, 16 novembre 2023

DÉFINITION



Définition

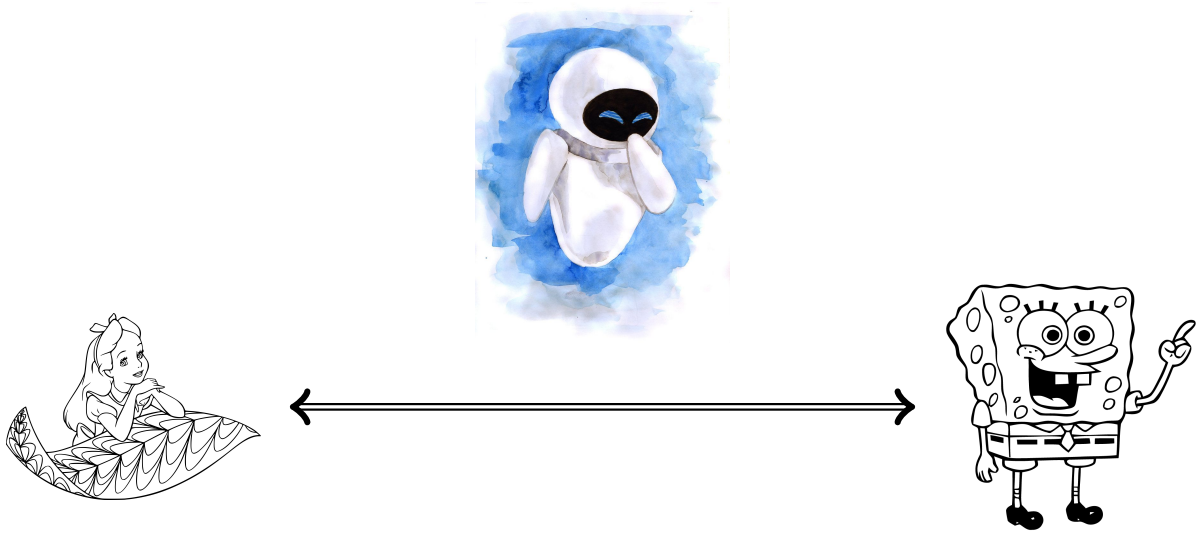


Enjeux

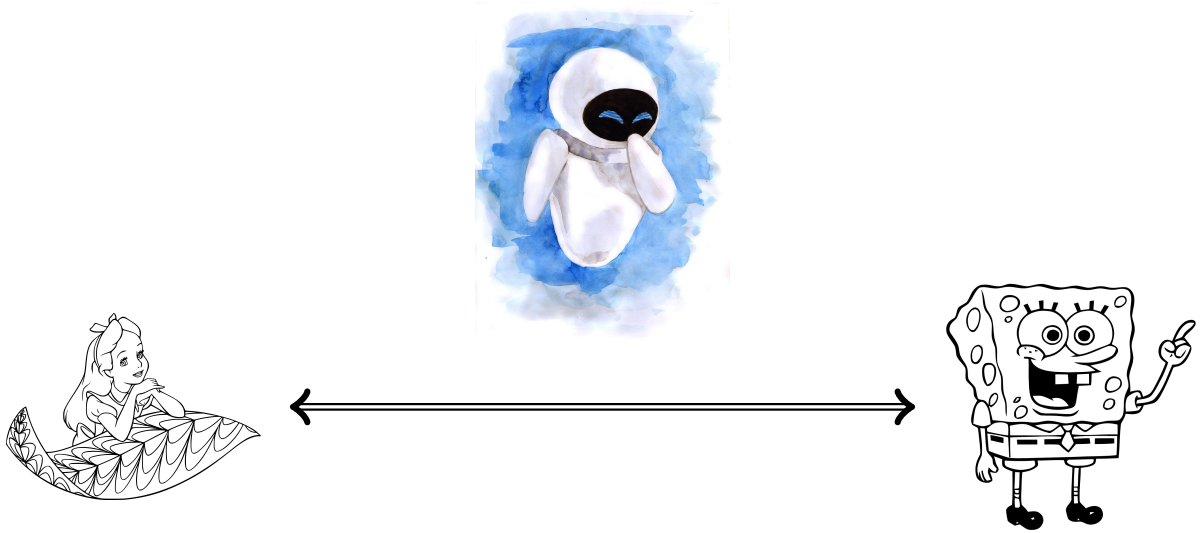
Confidentialité, authentification, intégrité, signatures.

Plan

La Cryptographie symétrique

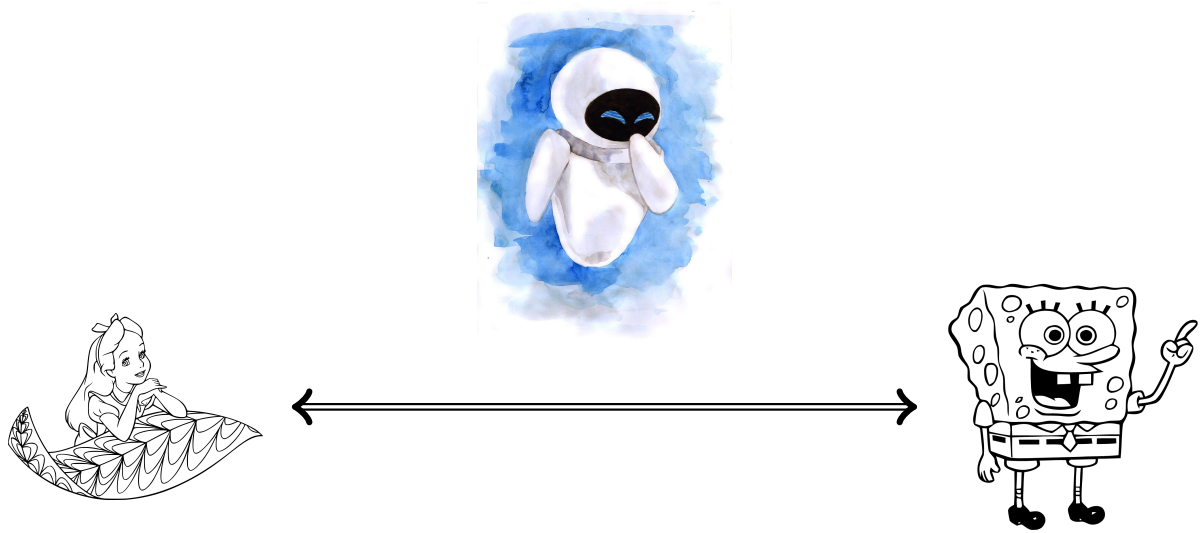


La Cryptographie symétrique



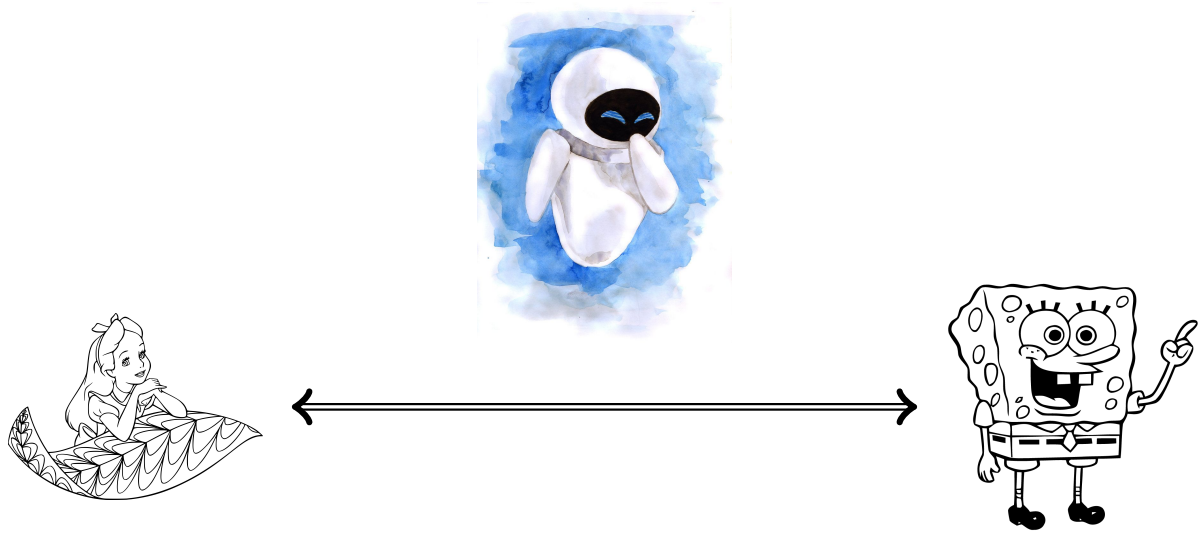
- Une seule clef K dans $\mathbb{F}_2^\kappa$

La Cryptographie symétrique



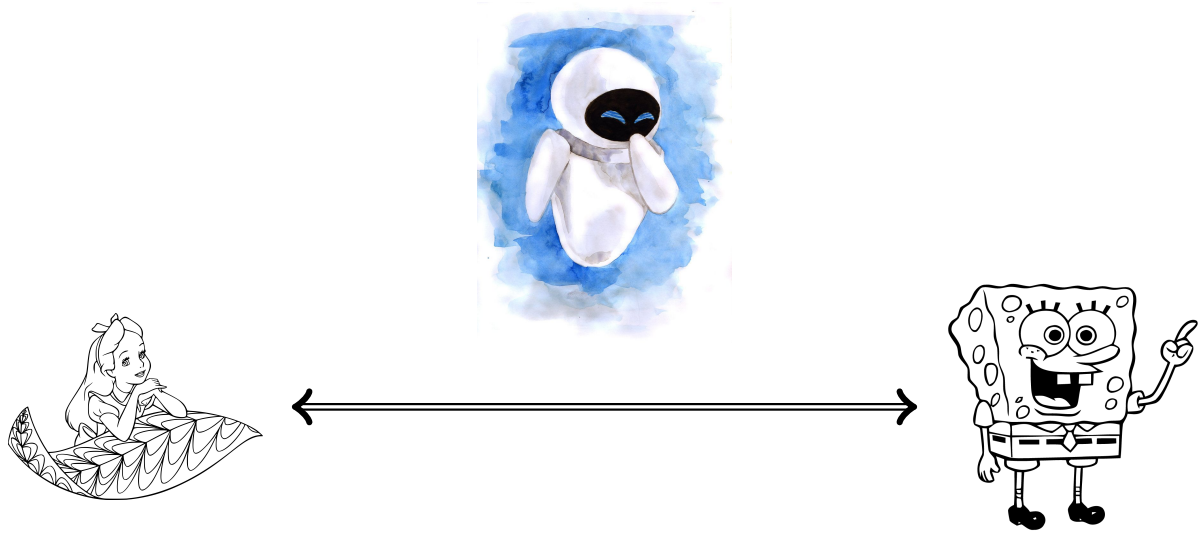
- Une seule clef K dans $\mathbb{F}_2^\kappa$
- Une fonction de chiffrement $E : \mathbb{F}_2^\kappa \times \mathbb{F}_2^* \to \mathbb{F}_2^*$

La Cryptographie symétrique



- Une seule clef K dans $\mathbb{F}_2^\kappa$
- Une fonction de chiffrement $E : \mathbb{F}_2^\kappa \times \mathbb{F}_2^* \to \mathbb{F}_2^*$
- Une fonction de déchiffrement $D : \mathbb{F}_2^\kappa \times \mathbb{F}_2^* \to \mathbb{F}_2^*$ telle que pour tout $M \in \mathbb{F}_2^*$ et pour tout $K \in \mathbb{F}_2^\kappa$, $D(K, E(K, M)) = M$

La Cryptographie symétrique



- Une seule clef K dans $\mathbb{F}_2^\kappa$
- Une fonction de chiffrement $E : \mathbb{F}_2^\kappa \times \mathbb{F}_2^* \to \mathbb{F}_2^*$
- Une fonction de déchiffrement $D : \mathbb{F}_2^\kappa \times \mathbb{F}_2^* \to \mathbb{F}_2^*$ telle que pour tout $M \in \mathbb{F}_2^*$ et pour tout $K \in \mathbb{F}_2^\kappa$, $D(K, E(K, M)) = M$
- On peut vouloir authentifier des messages avec une clef symétrique.

L'ANCIEN MONDE

- Substitutions (César)
- Transpositions (Scytale)
- Substitutions polyalphabétiques
- Vigenere (16ème siècle)
- Machines à chiffrer (Enigma)

L'ANCIEN MONDE

- Substitutions (César)
- Transpositions (Scytale)
- Substitutions polyalphabétiques
- Vigenere (16ème siècle)
- Machines à chiffrer (Enigma)

Premier concept moderne : le principe de Kerckhoffs (1883) :

"La sécurité d'un système
ne doit pas exiger de secret autre que la clef"

L'ANCIEN MONDE

- Substitutions (César)
- Transpositions (Scytale)
- Substitutions polyalphabétiques
- Vigenere (16ème siècle)
- Machines à chiffrer (Enigma)

Premier concept moderne : le principe de Kerckhoffs (1883) :

"La sécurité d'un système
ne doit pas exiger de secret autre que la clef"

Qui est concepteur des chiffrements ?

CHIFFREMENT PAR BLOC

$$E : \mathbb{F}_2^k \times \mathbb{F}_2^s \to \mathbb{F}_2^s$$

CHIFFREMENT PAR BLOC

$$E : \mathbb{F}_2^\kappa \times \mathbb{F}_2^s \to \mathbb{F}_2^s$$

tel que pour tout K,

$$\begin{array}{rccc} f_K & : & \mathbb{F}_2^s & \to & \mathbb{F}_2^s \\ & & x & \mapsto & E(K, x) \end{array}$$

soit bijective.

CHIFFREMENT PAR BLOC

$$E : \mathbb{F}_2^\kappa \times \mathbb{F}_2^s \to \mathbb{F}_2^s$$

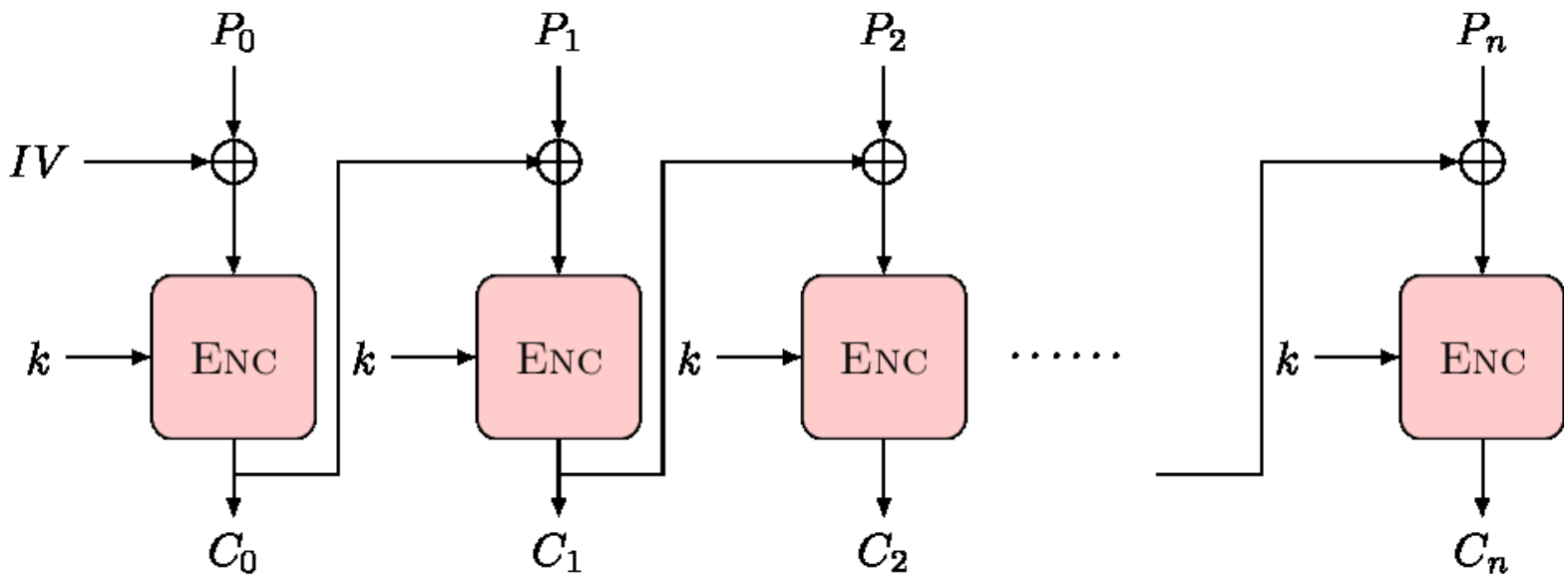
tel que pour tout K,

$$\begin{array}{rccc} f_K & : & \mathbb{F}_2^s & \to & \mathbb{F}_2^s \\ & & x & \mapsto & E(K, x) \end{array}$$

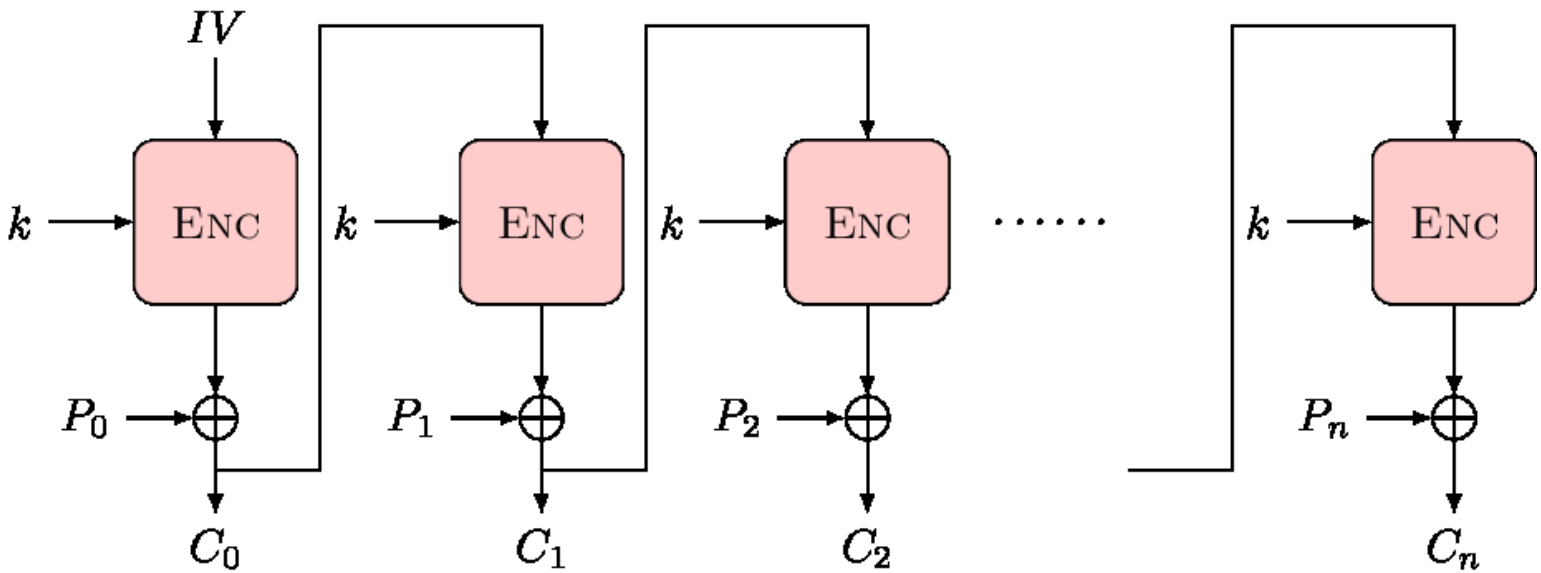
soit bijective.

Un chiffrement par bloc est la définition d'une famille de 2^κ permutations de $\mathbb{F}_2^s$

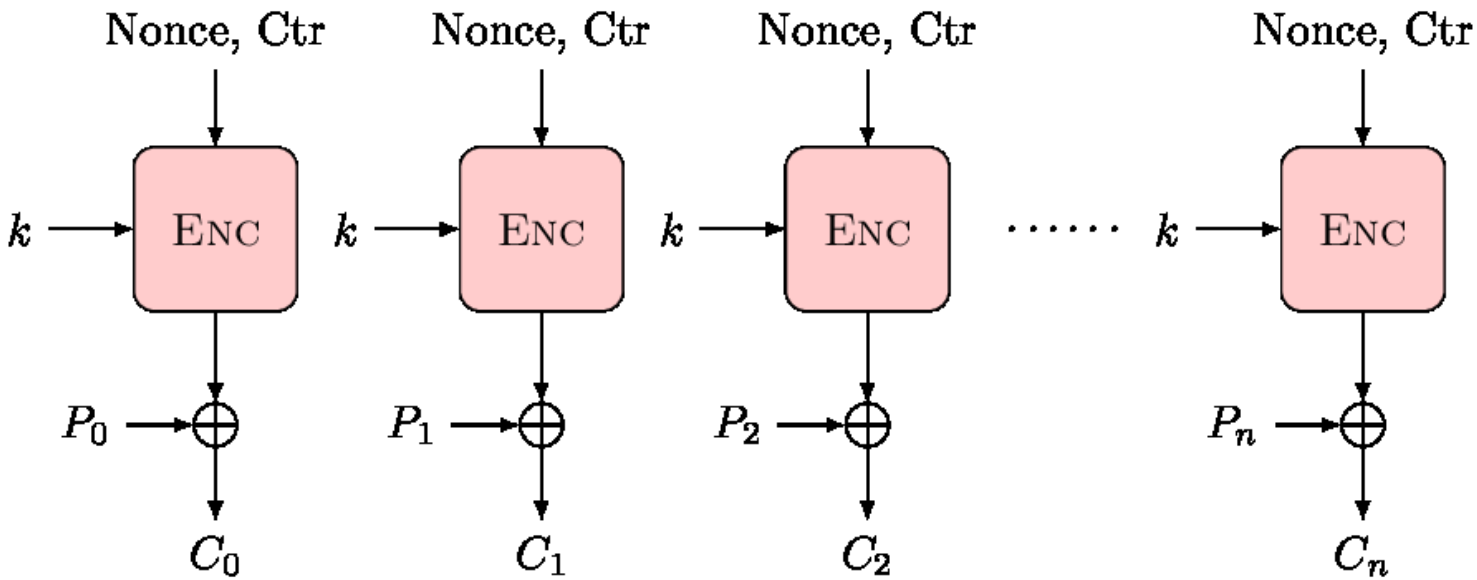
MODES OPÉRATOIRES



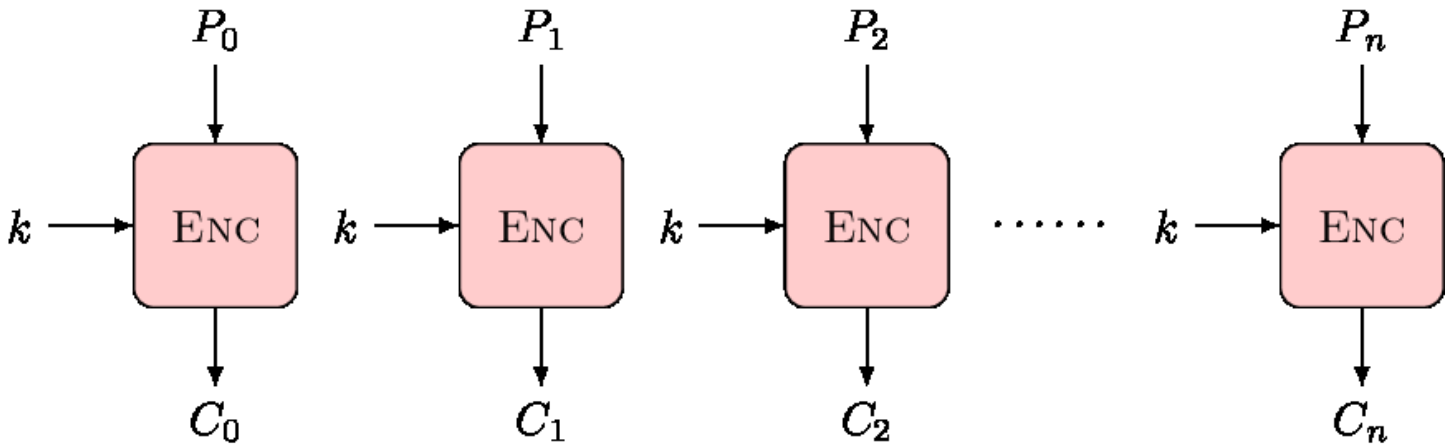
MODES OPÉRATOIRES



MODES OPÉRATOIRES



MODES OPÉRATOIRES



PROVABLE SECURITY

- E une famille de permutations
- F toutes les permutations

PROVABLE SECURITY

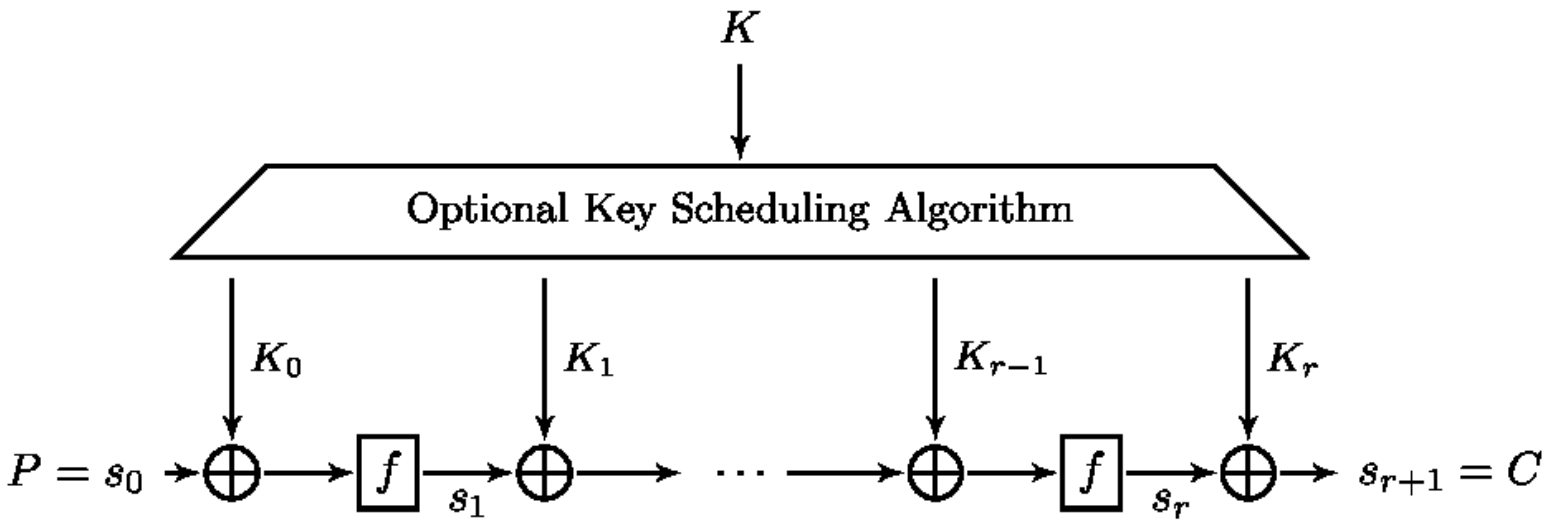
- E une famille de permutations
- F toutes les permutations
- Un algorithme $\mathcal{A}$ qui prend en entrée des entrées - sorties d'une permutation (sans le savoir) et renvoie vrai ou faux

PROVABLE SECURITY

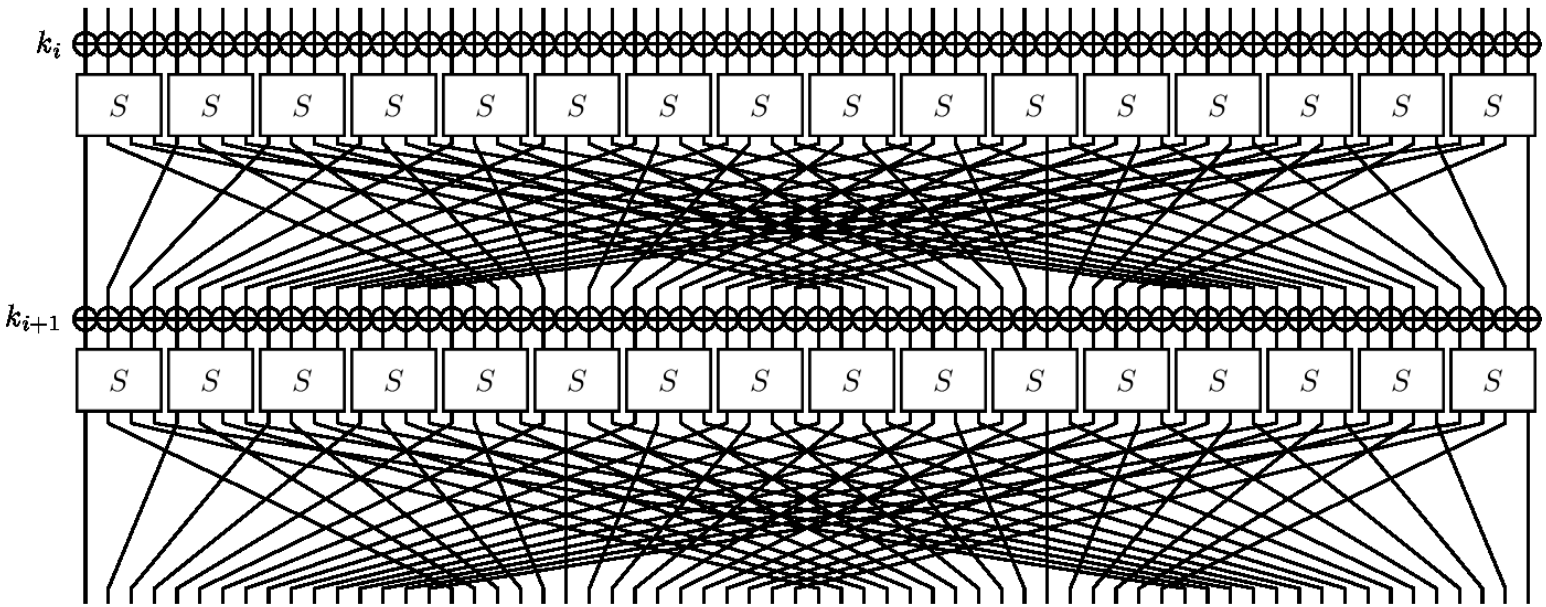
- E une famille de permutations
- F toutes les permutations
- Un algorithme $\mathcal{A}$ qui prend en entrée des entrées - sorties d'une permutation (sans le savoir) et renvoie vrai ou faux

$$\mathrm{Adv}(\mathcal{A}) = |\Pr[\mathcal{A}(F)] = 1 - \Pr[\mathcal{A}(E)] = 1| < \varepsilon$$

CONSTRUCTION



CONSTRUCTION

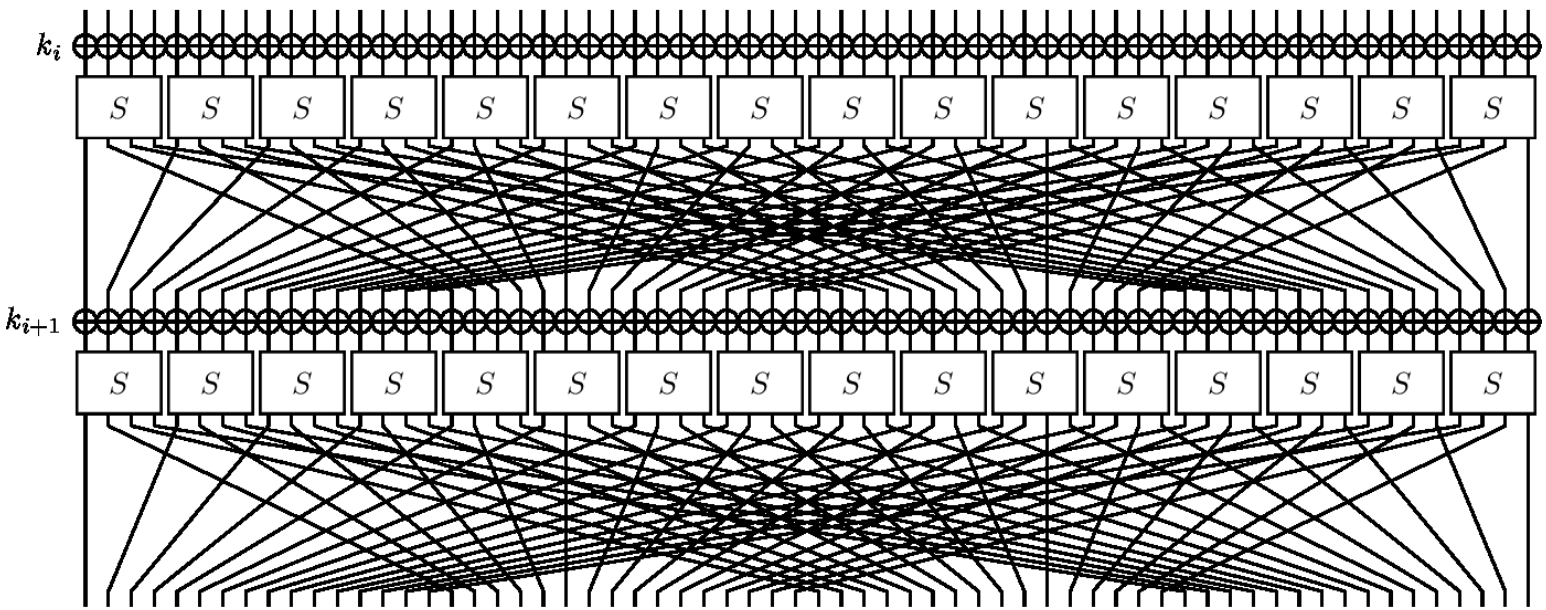


Arguments de sécurité

- On analyse uniquement le chiffrement par bloc
- Aucune preuve absolue
- Cryptanalyse différentielle
- Cryptanalyse algébrique et intégrale
- Cryptanalyse linéaire
- Attaques par invariant
- ...

ARGUMENTS DE SÉCURITÉ

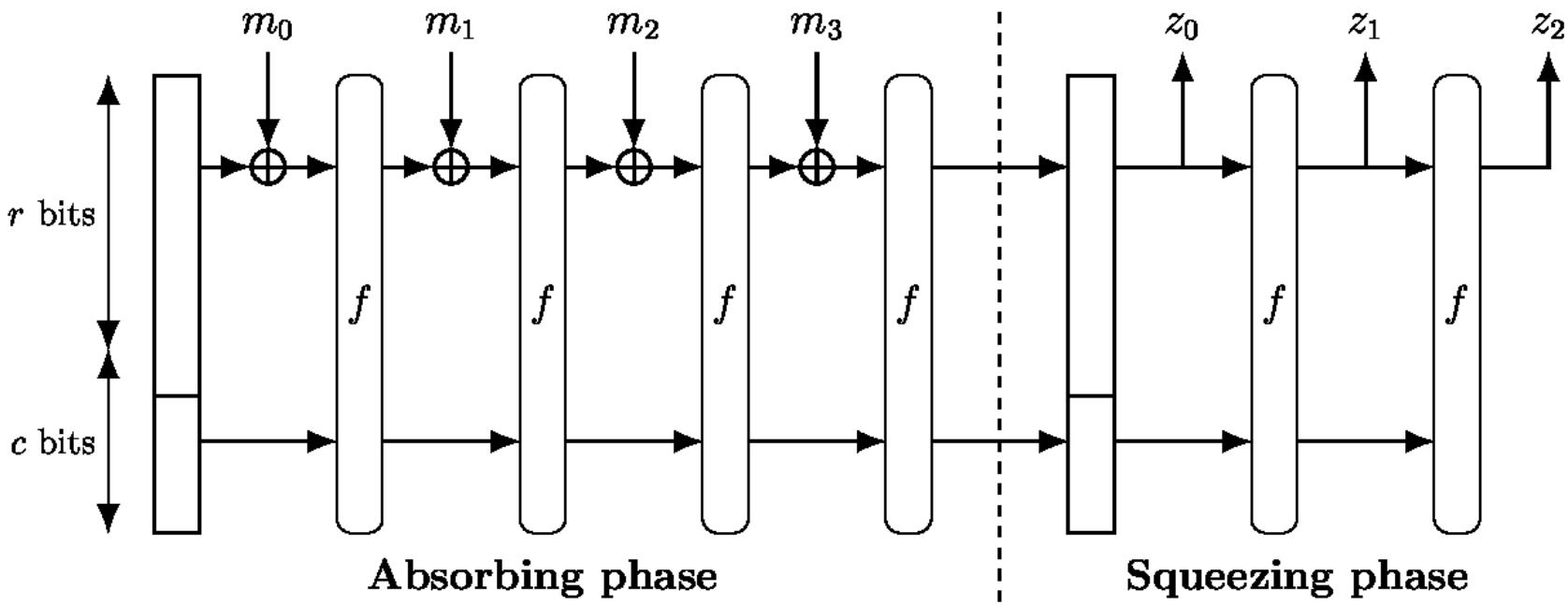
- On analyse uniquement le chiffrement par bloc
- Aucune preuve absolue
- Cryptanalyse différentielle
- Cryptanalyse algébrique et intégrale
- Cryptanalyse linéaire
- Attaques par invariant
- ...



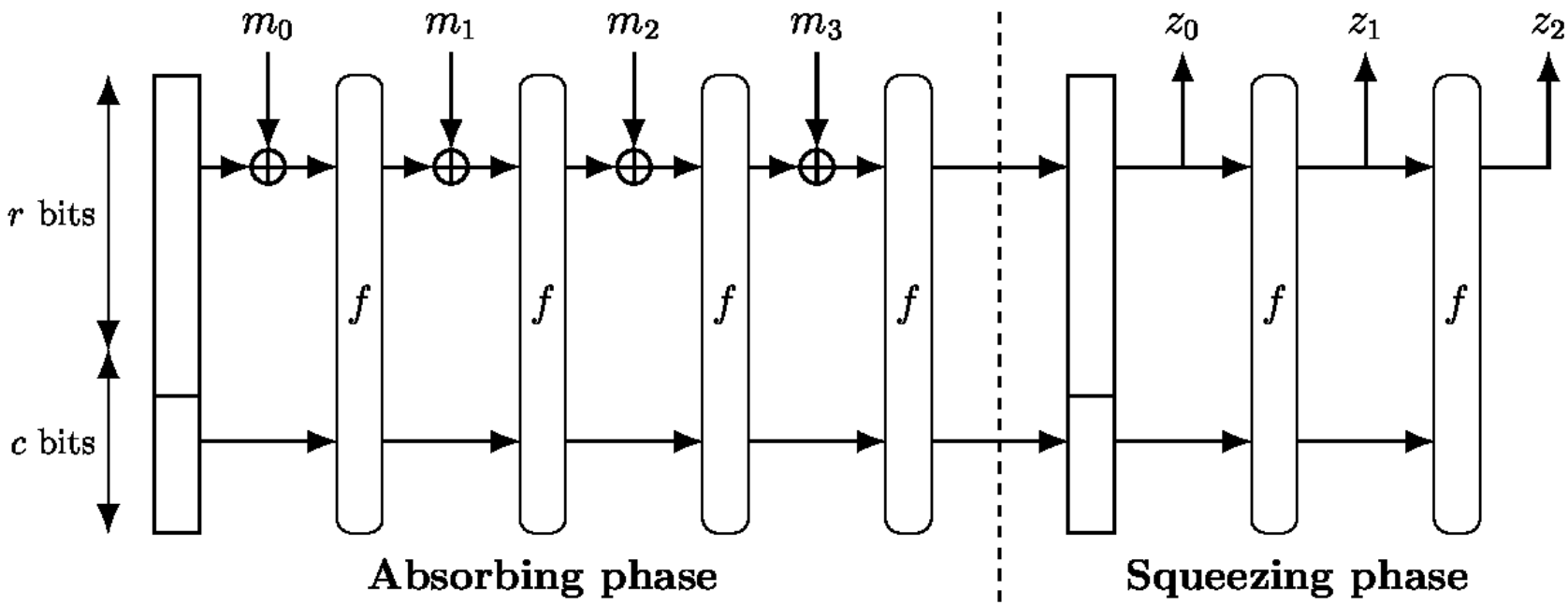
Outils automatiques pour les attaques

- MILP (Mixed Integer Linear Programming)
- SAT solvers
- Outils dédiés

CRYPTOGRAPHIE BASÉE SUR LES PERMUTATIONS

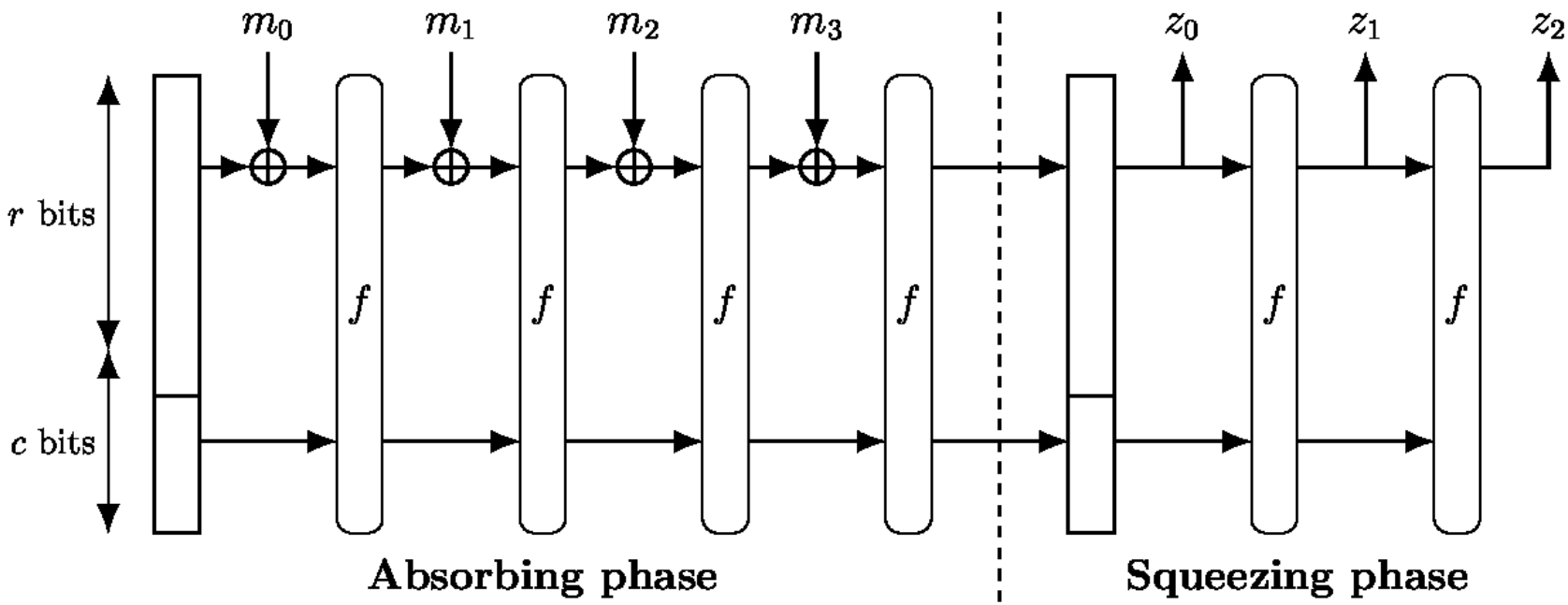


CRYPTOGRAPHIE BASÉE SUR LES PERMUTATIONS



Problème : Construction sûre si la permutation f est choisie au hasard...

CRYPTOGRAPHIE BASÉE SUR LES PERMUTATIONS



Problème : Construction sûre si la permutation f est choisie au hasard...

Avantage : Très performant, NIST LWC finalists : 7/10 permutation-based, 2/10 BlockCiphers, 1/10 streamcipher

ETAT DE LA RECHERCHE

- On ne peut pas se passer de la cryptanalyse

ETAT DE LA RECHERCHE

- On ne peut pas se passer de la cryptanalyse
- Outils automatiques

ETAT DE LA RECHERCHE

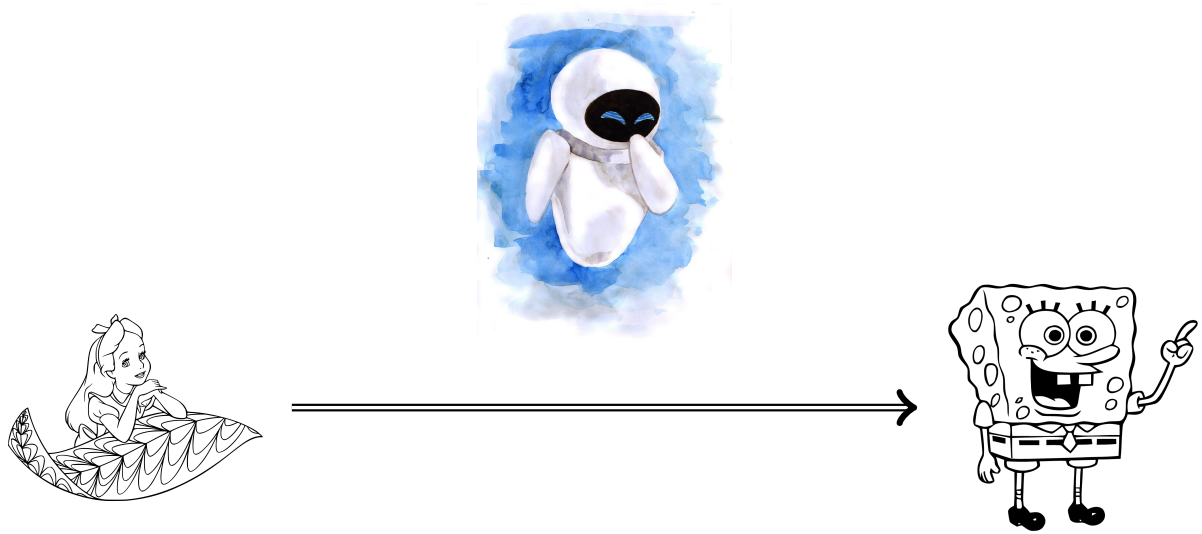
- On ne peut pas se passer de la cryptanalyse
- Outils automatiques
- Meilleurs arguments de sécurité

ETAT DE LA RECHERCHE

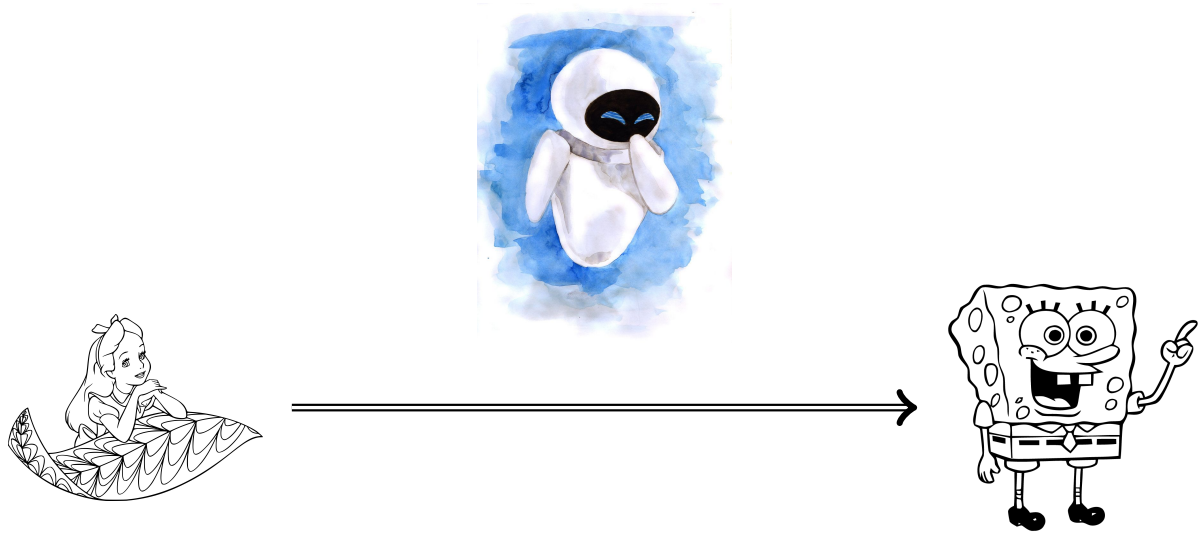
- On ne peut pas se passer de la cryptanalyse
- Outils automatiques
- Meilleurs arguments de sécurité
- Besoin de nouvelles constructions ?

Plan

CRPYTOGRAPHIE ASYMÉTRIQUE

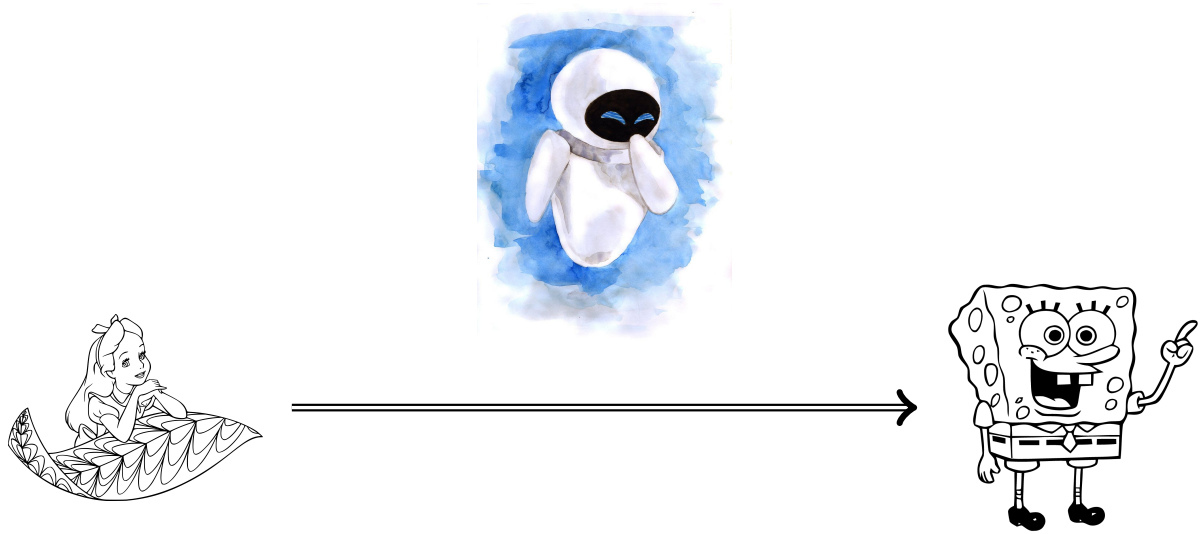


CRPYTOGRAPHIE ASYMÉTRIQUE



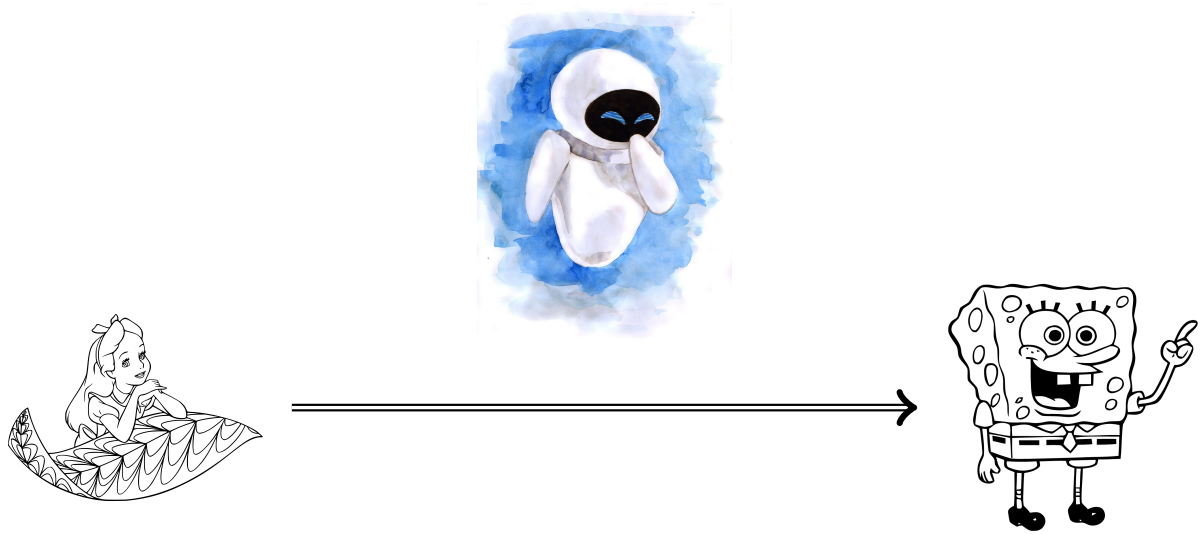
- Une clef privé *sk* dans $\mathcal{S}$ et une clef publique *pk* dans $\mathcal{P}$

CRPYTOGRAPHIE ASYMÉTRIQUE



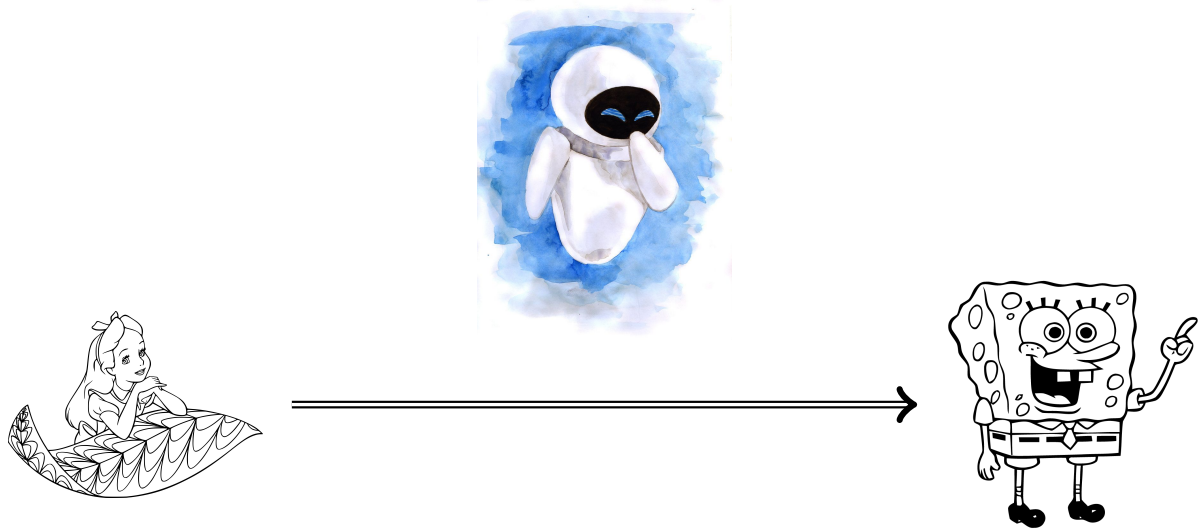
- Une clef privé *sk* dans $\mathcal{S}$ et une clef publique *pk* dans $\mathcal{P}$
- Une fonction de chiffrement $E : \mathcal{P} \times \mathcal{M} \to \mathcal{C}$

CRPYTOGRAPHIE ASYMÉTRIQUE

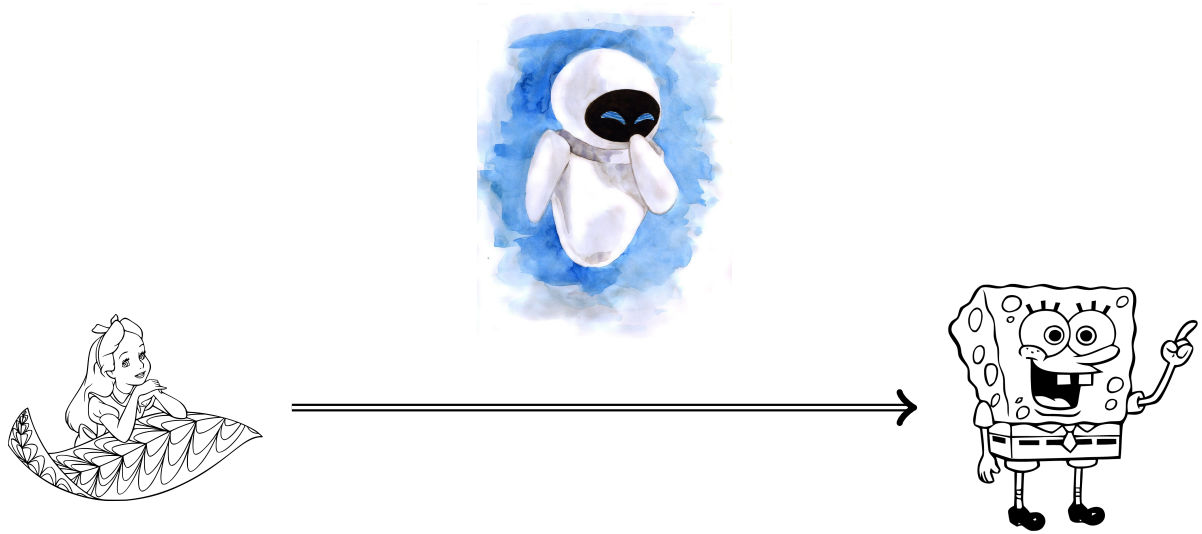


- Une clef privé *sk* dans $\mathcal{S}$ et une clef publique *pk* dans $\mathcal{P}$
- Une fonction de chiffrement $E : \mathcal{P} \times \mathcal{M} \to \mathcal{C}$
- Une fonction de déchiffrement $D : \mathcal{S} \times \mathcal{C} \to \mathcal{M}$

La Cryptographie asymétrique

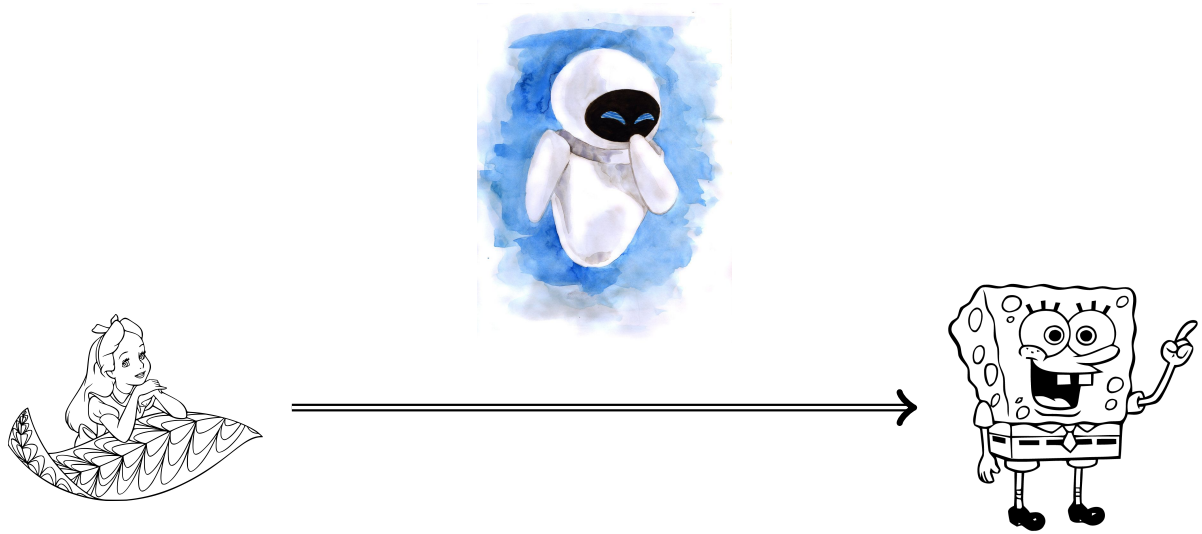


La Cryptographie asymétrique



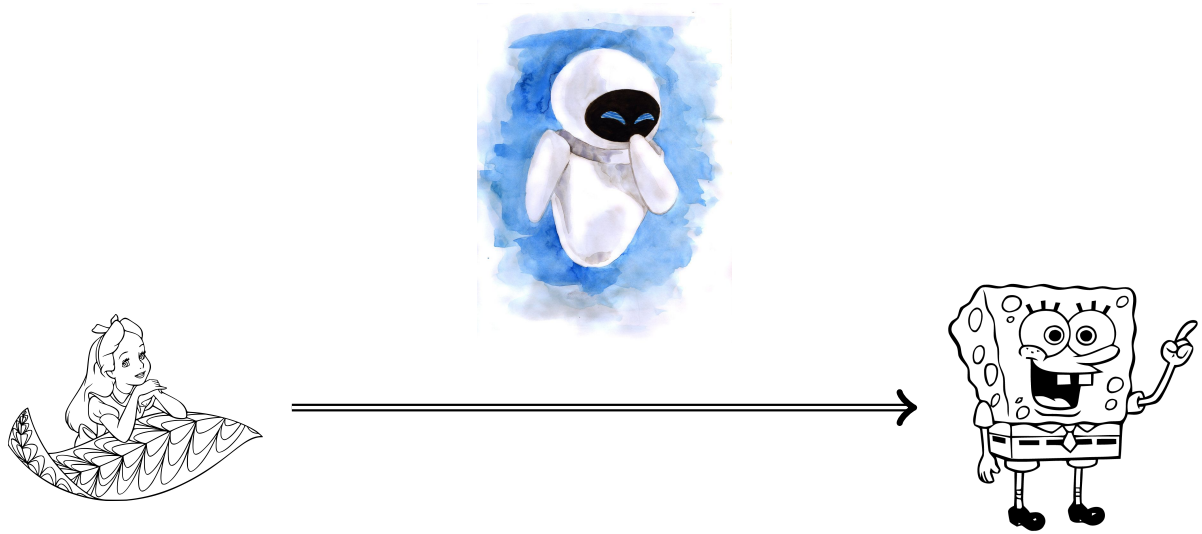
- Une clef privé sk_B dans $\mathcal{S}$ et une clef publique pk_B dans $\mathcal{P}$

La Cryptographie asymétrique



- Une clef privé sk_B dans $\mathcal{S}$ et une clef publique pk_B dans $\mathcal{P}$
- Une fonction de chiffrement $E : \mathcal{P} \times \mathcal{M} \to \mathcal{C}$

La Cryptographie asymétrique



- Une clef privé sk_B dans $\mathcal{S}$ et une clef publique pk_B dans $\mathcal{P}$
- Une fonction de chiffrement $E : \mathcal{P} \times \mathcal{M} \to \mathcal{C}$
- Une fonction de déchiffrement $D : \mathcal{S} \times \mathcal{C} \to \mathcal{M}$

L'ÉCHANGE DE CLEFS DIFFIE HELLMAN

Question : comment se mettre d'accord sur un secret commun sans se voir ?

L'ÉCHANGE DE CLEFS DIFFIE HELLMAN

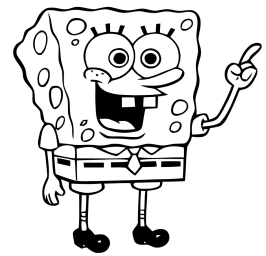
Question : comment se mettre d'accord sur un secret commun sans se voir ?

Un groupe G généré par $g \in G$ public

L'ÉCHANGE DE CLEFS DIFFIE HELLMAN

Question : comment se mettre d'accord sur un secret commun sans se voir ?

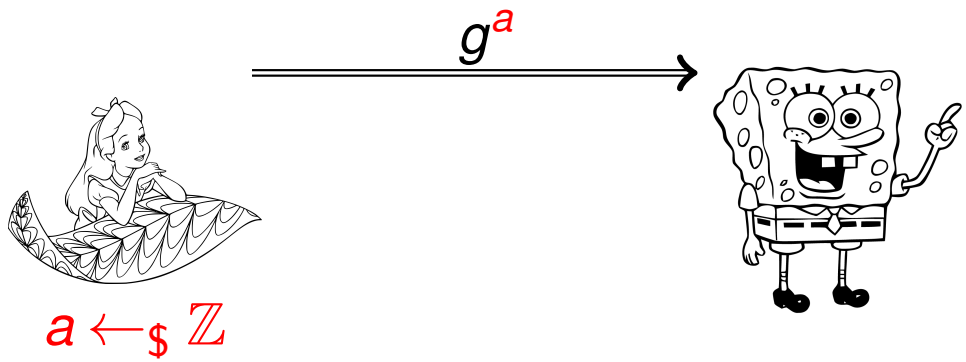
Un groupe G généré par $g \in G$ public



L'ÉCHANGE DE CLEFS DIFFIE HELLMAN

Question : comment se mettre d'accord sur un secret commun sans se voir ?

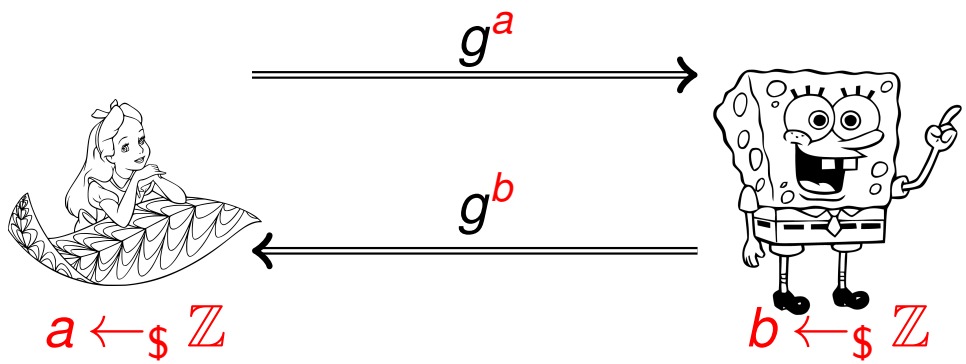
Un groupe G généré par $g \in G$ public



L'ÉCHANGE DE CLEFS DIFFIE HELLMAN

Question : comment se mettre d'accord sur un secret commun sans se voir ?

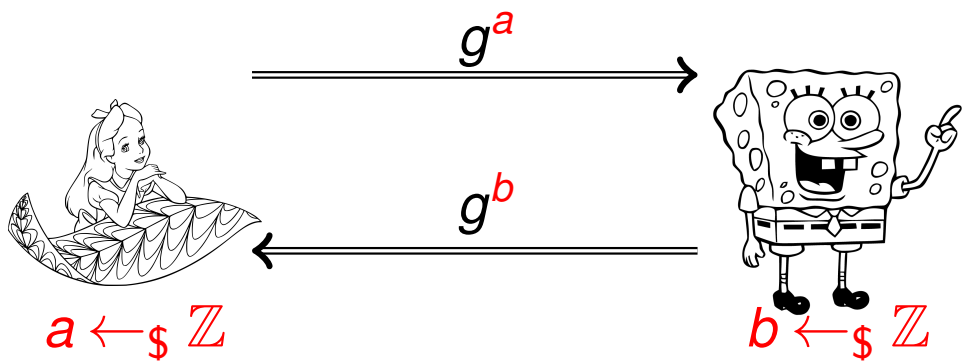
Un groupe G généré par $g \in G$ public



L'ÉCHANGE DE CLEFS DIFFIE HELLMAN

Question : comment se mettre d'accord sur un secret commun sans se voir ?

Un groupe G généré par $g \in G$ public

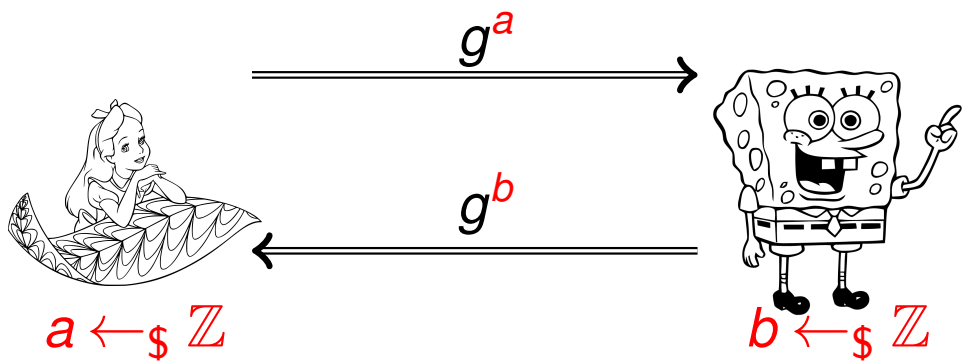


- Chacun peut calculer g^{ab}.

L'ÉCHANGE DE CLEFS DIFFIE HELLMAN

Question : comment se mettre d'accord sur un secret commun sans se voir ?

Un groupe G généré par $g \in G$ public

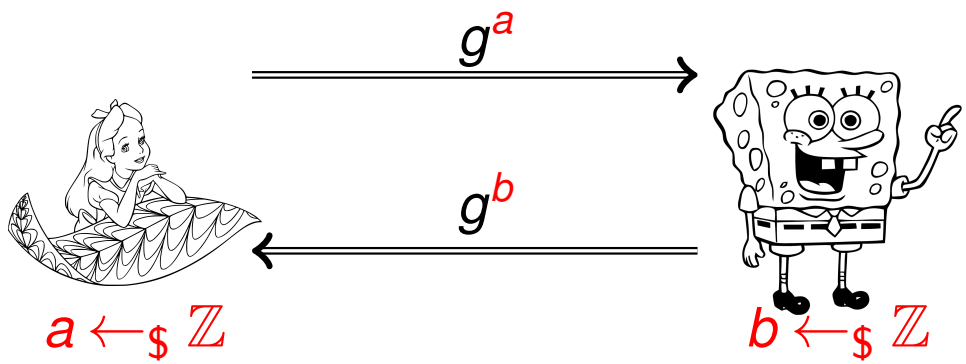


- Chacun peut calculer g^{ab}.
- Conception de protocoles cryptographiques

L'ÉCHANGE DE CLEFS DIFFIE HELLMAN

Question : comment se mettre d'accord sur un secret commun sans se voir ?

Un groupe G généré par $g \in G$ public



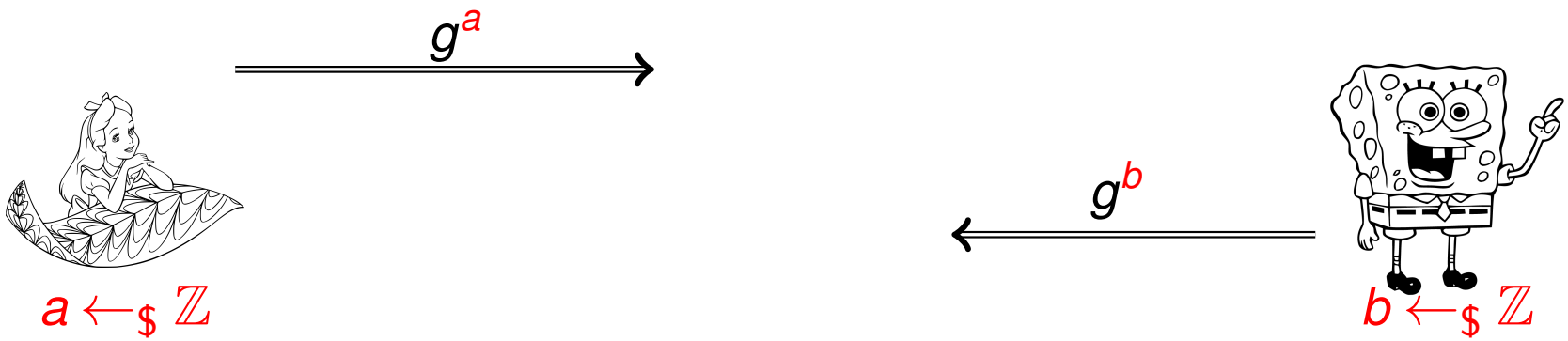
- Chacun peut calculer g^{ab}.
- Conception de protocoles cryptographiques
- Ce schéma est-il sûr ?

PREMIER PROBLÈME : L'AUTHENTIFICATION

Question : Comment Alice est-elle sûre de parler à Bob ?

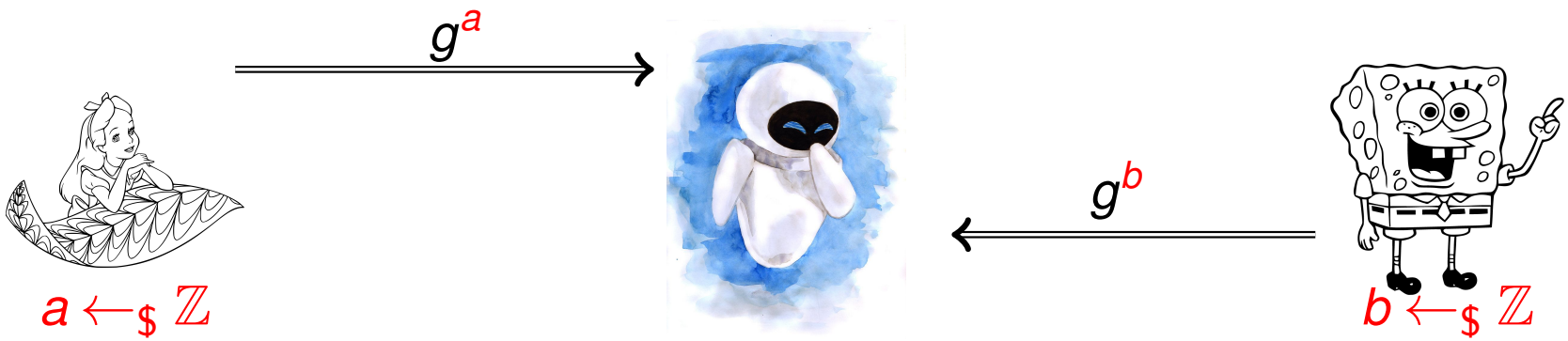
PREMIER PROBLÈME : L'AUTHENTIFICATION

Question : Comment Alice est-elle sûre de parler à Bob ?



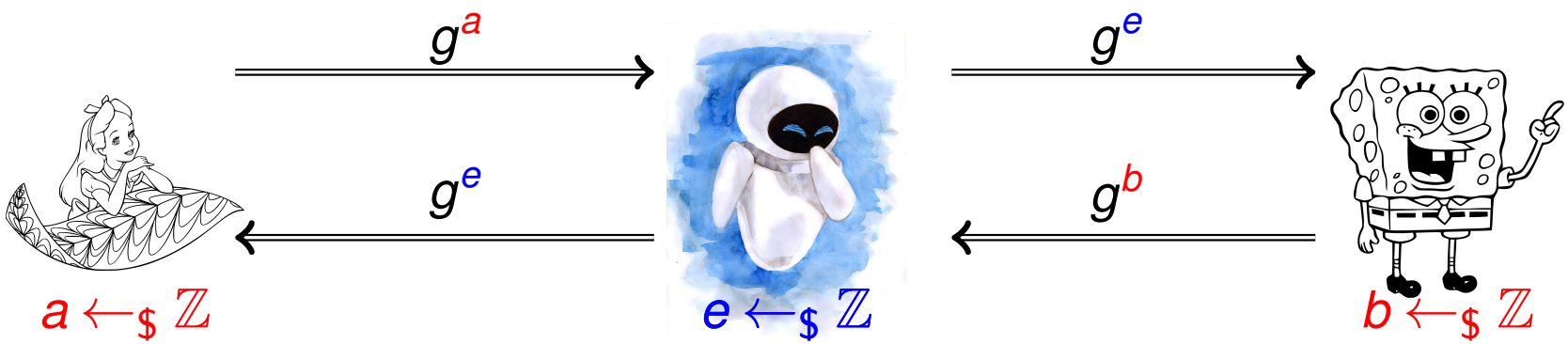
PREMIER PROBLÈME : L'AUTHENTIFICATION

Question : Comment Alice est-elle sûre de parler à Bob ?



PREMIER PROBLÈME : L'AUTHENTIFICATION

Question : Comment Alice est-elle sûre de parler à Bob ?



Solutions

- Autorité de certification (TLS)
- Web of Trust (PGP)

Solutions

- Autorité de certification (TLS)
- Web of Trust (PGP)

Pour réaliser cela on a besoin de **signatures**

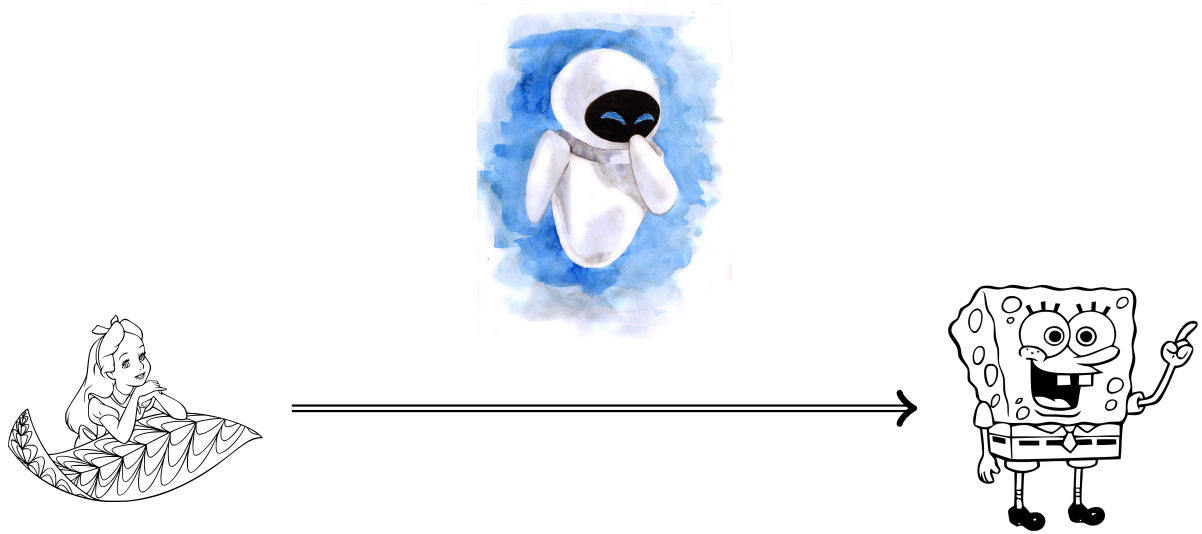
Solutions

- Autorité de certification (TLS)
- Web of Trust (PGP)

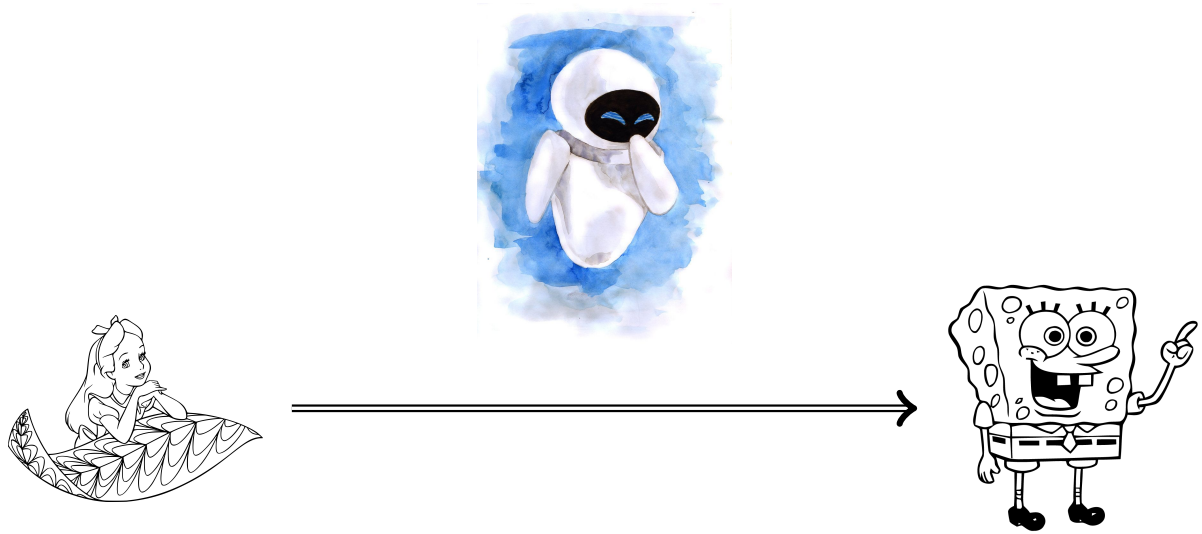
Pour réaliser cela on a besoin de **signatures**

- Participant à des protocoles : honnête, semi-honnête, malicieux

Les signatures numériques

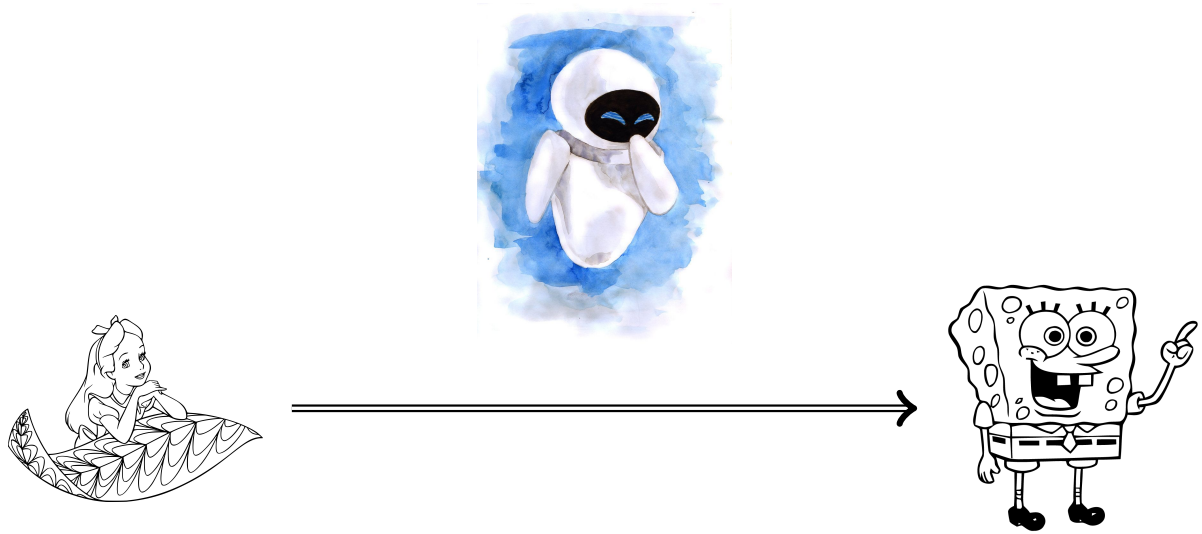


Les signatures numériques



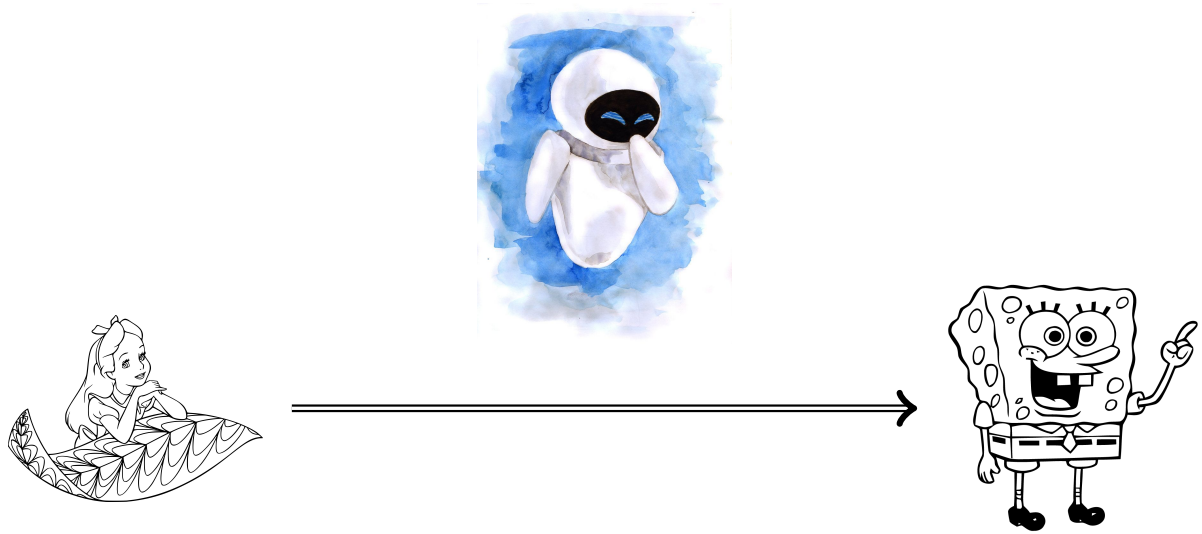
- Une clef privé sk_A dans $\mathcal{S}$ et une clef publique pk_A dans $\mathcal{P}$

Les signatures numériques



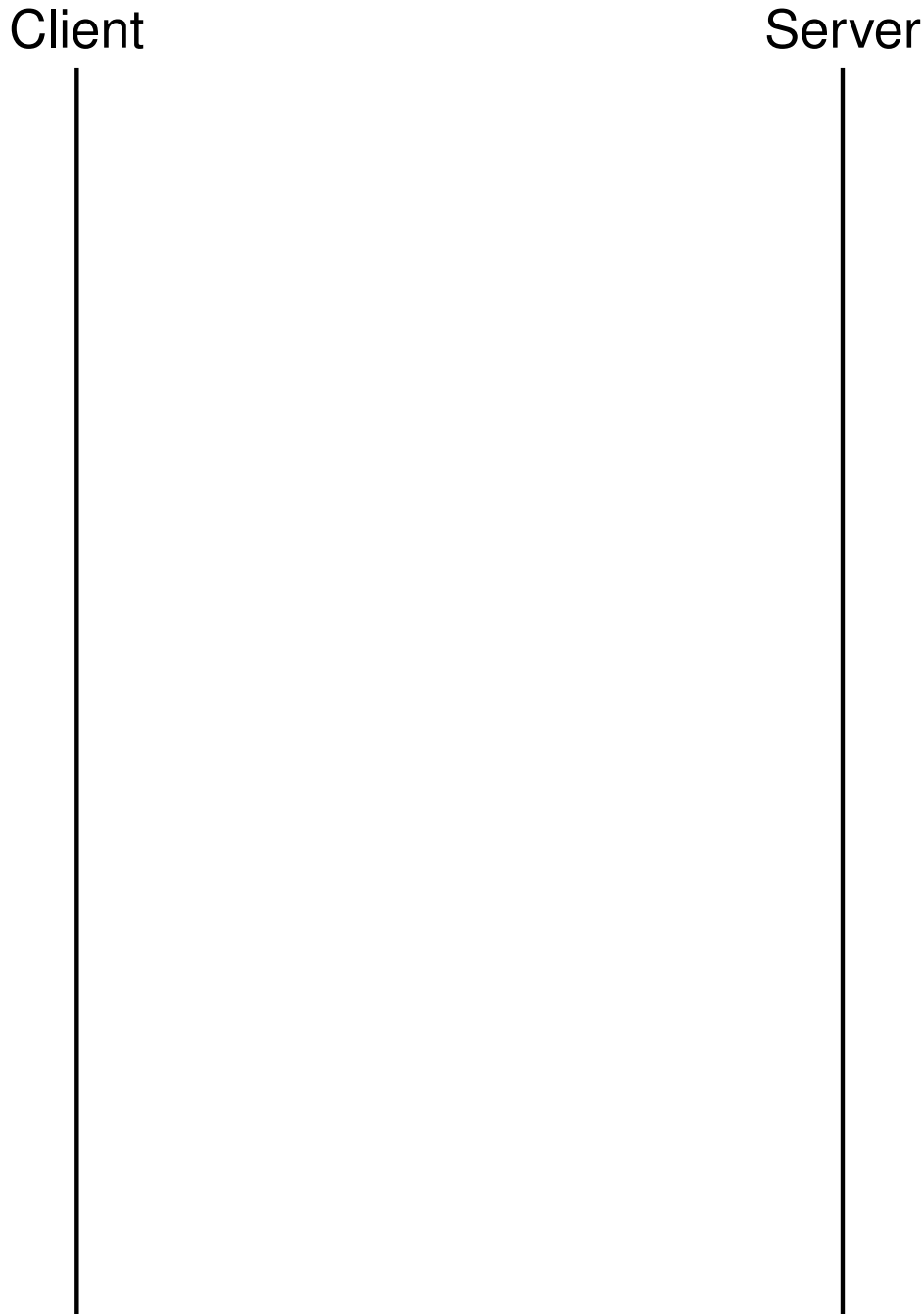
- Une clef privé sk_A dans $\mathcal{S}$ et une clef publique pk_A dans $\mathcal{P}$
- Une fonction de signature $\texttt{Sign} : \mathcal{S} \times \mathcal{M} \to \mathbb{F}_2^n$

Les signatures numériques

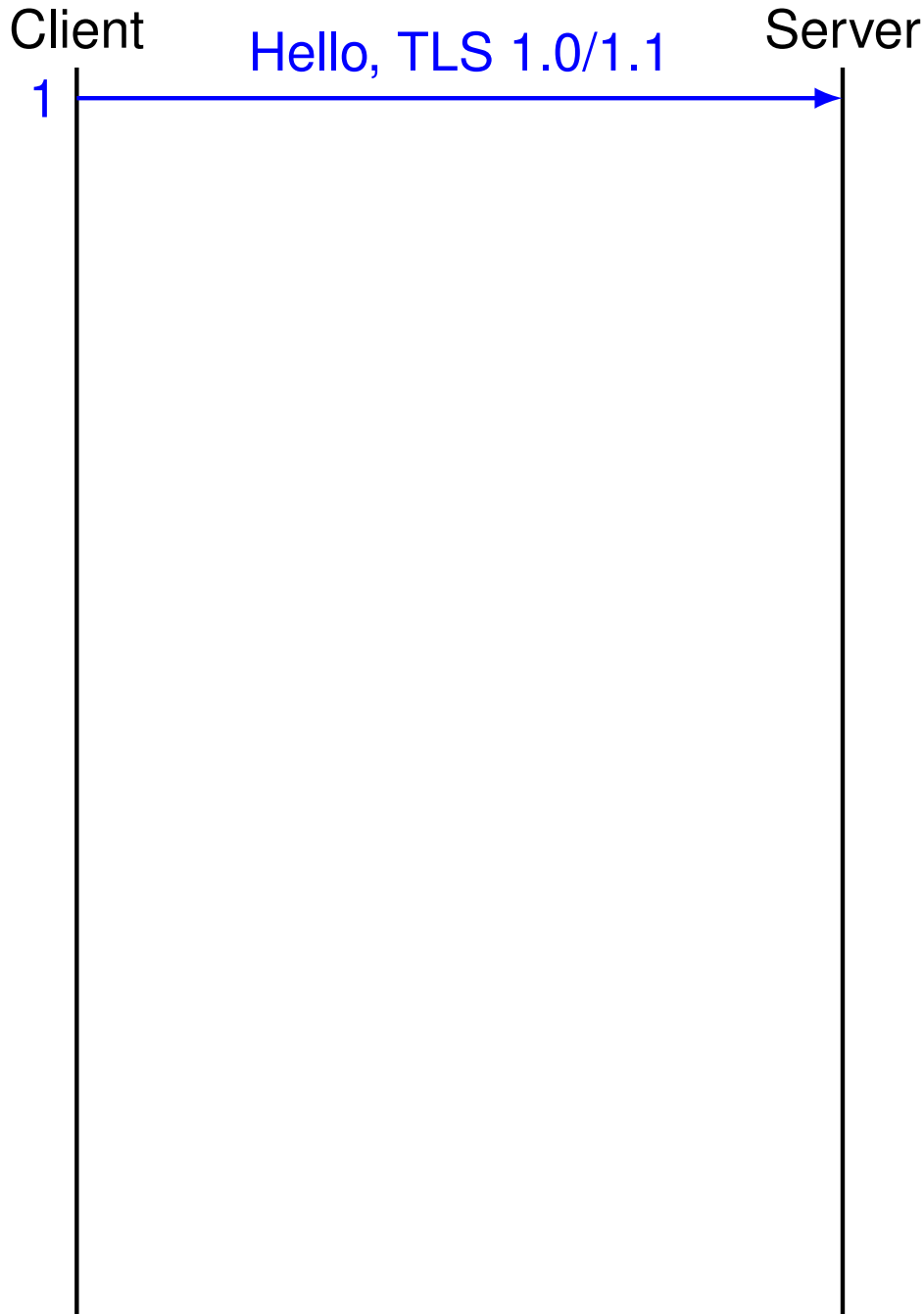


- Une clef privé sk_A dans $\mathcal{S}$ et une clef publique pk_A dans $\mathcal{P}$
- Une fonction de signature $\texttt{Sign} : \mathcal{S} \times \mathcal{M} \to \mathbb{F}_2^n$
- Une fonction de vérification $\texttt{Verif} : \mathcal{P} \times \mathcal{M} \times \mathbb{F}_2^n \to \{\texttt{Vrai}, \texttt{Faux}\}$

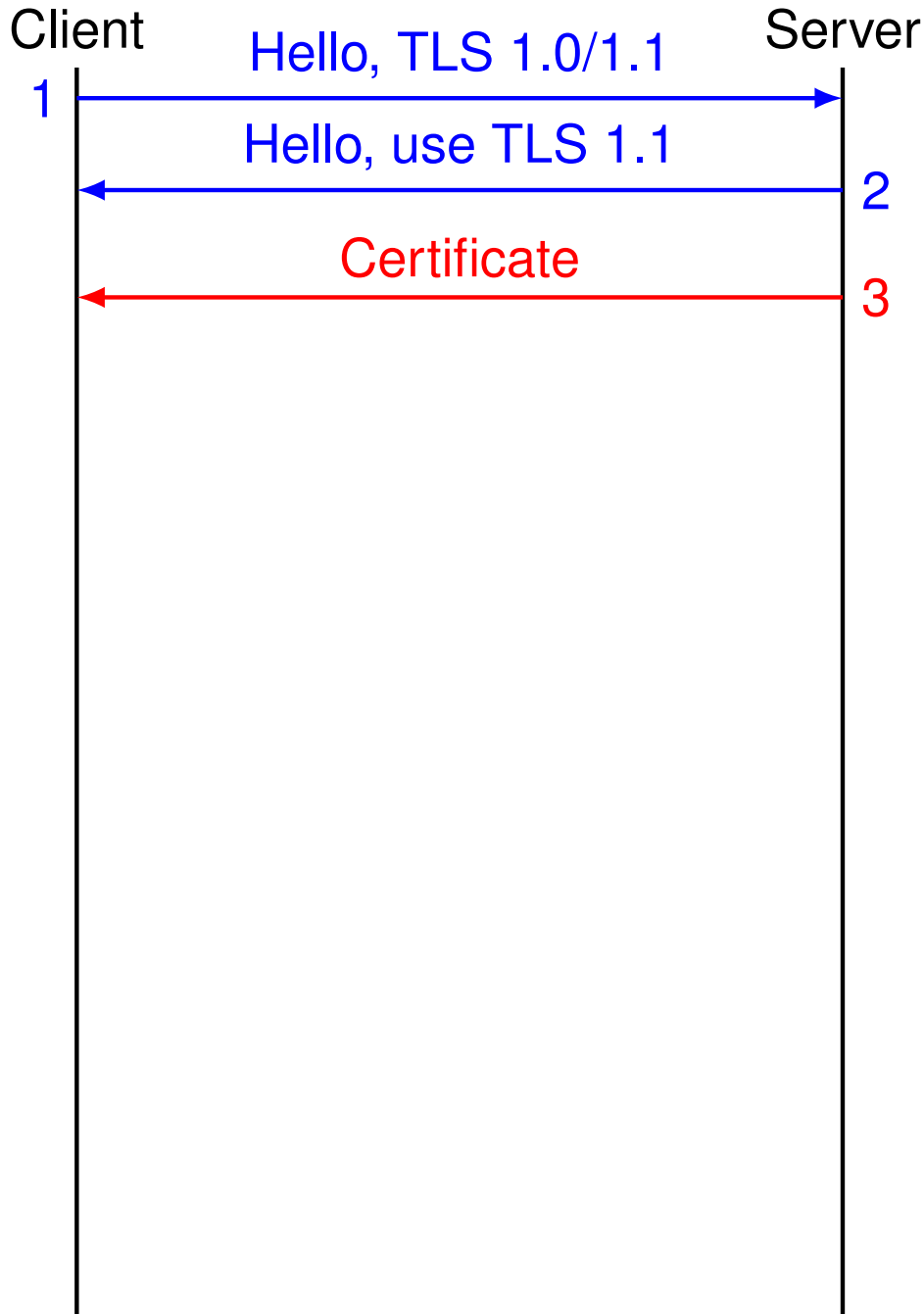
LE PROTOCOLE TLS



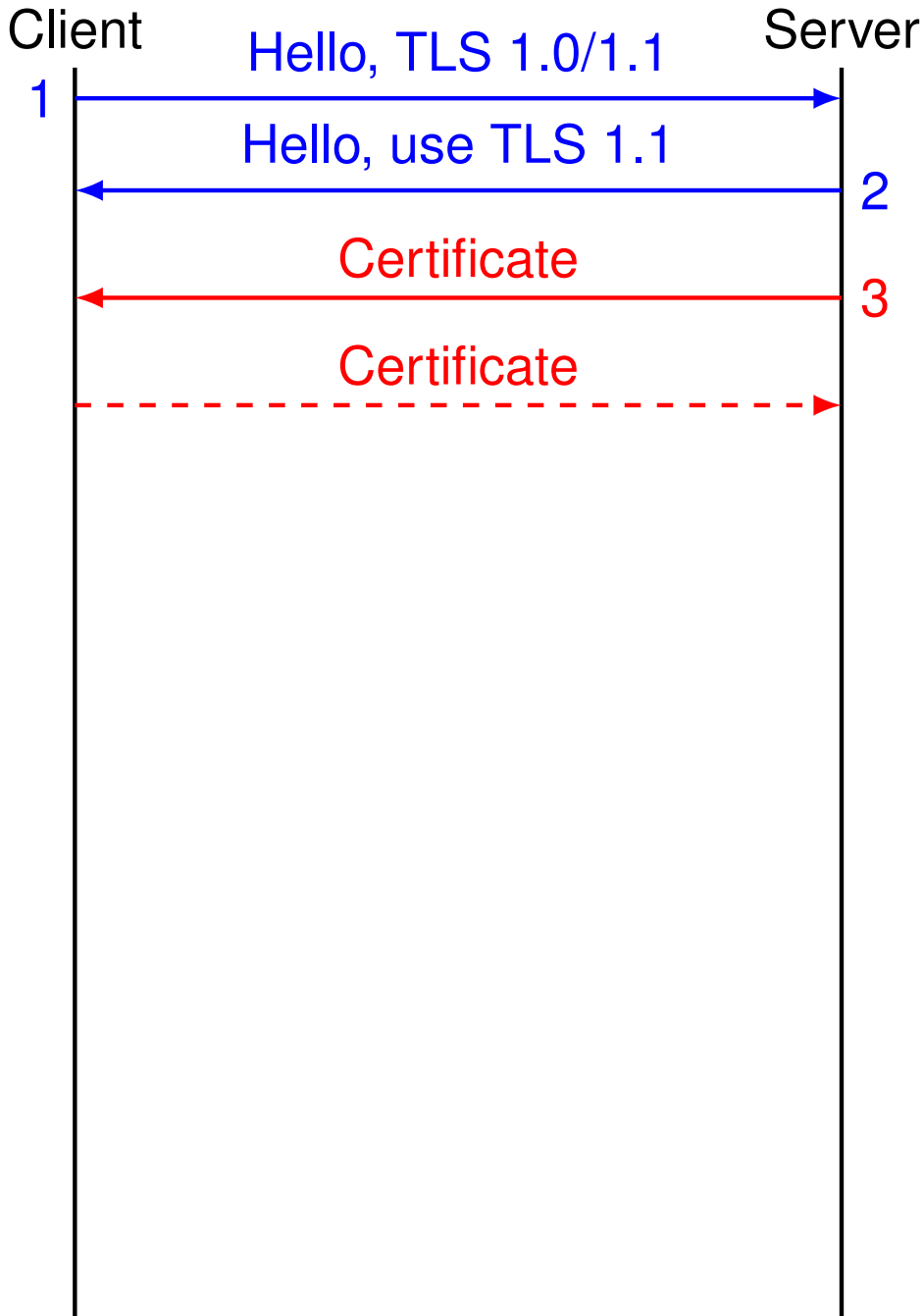
LE PROTOCOLE TLS



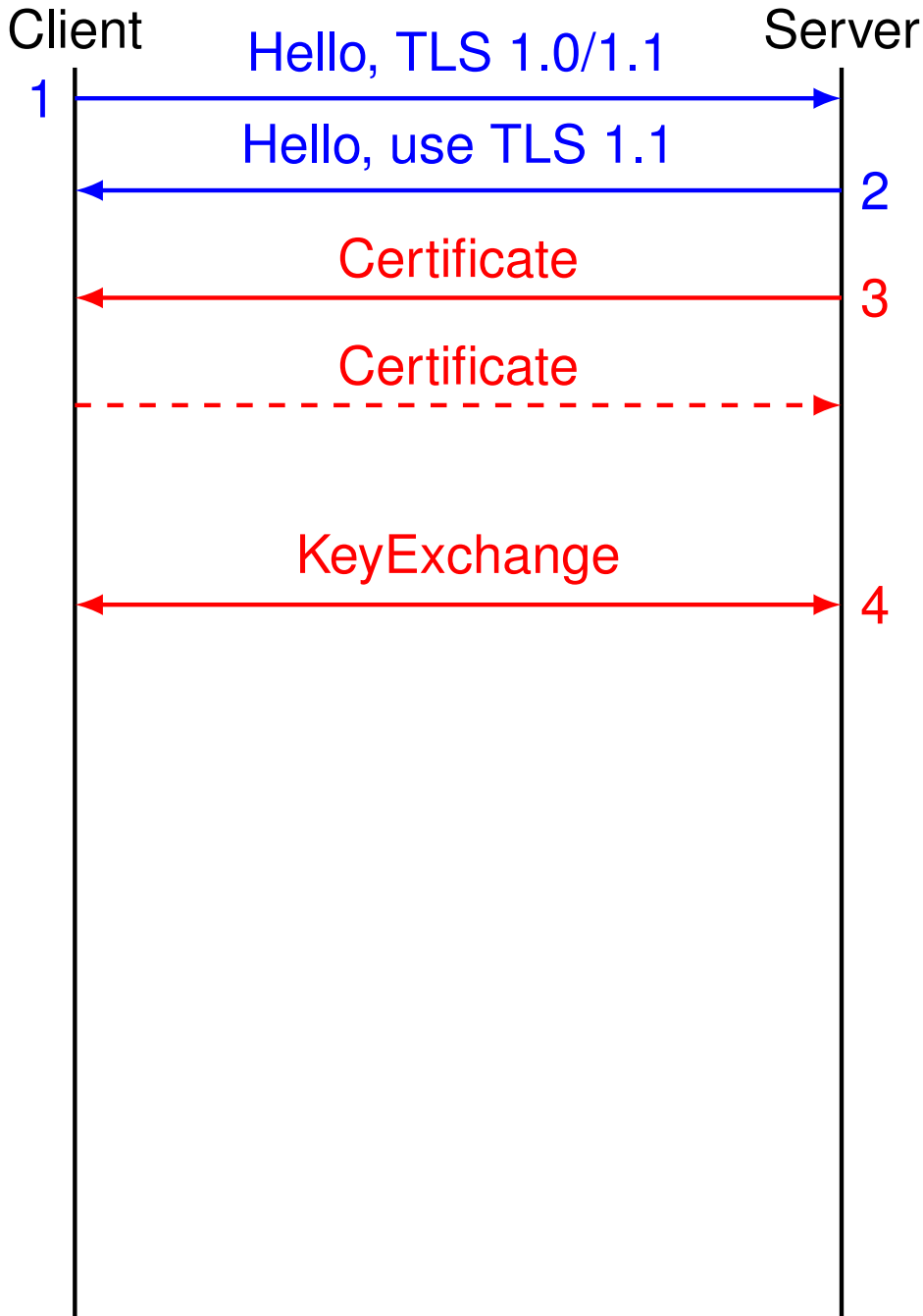
LE PROTOCOLE TLS



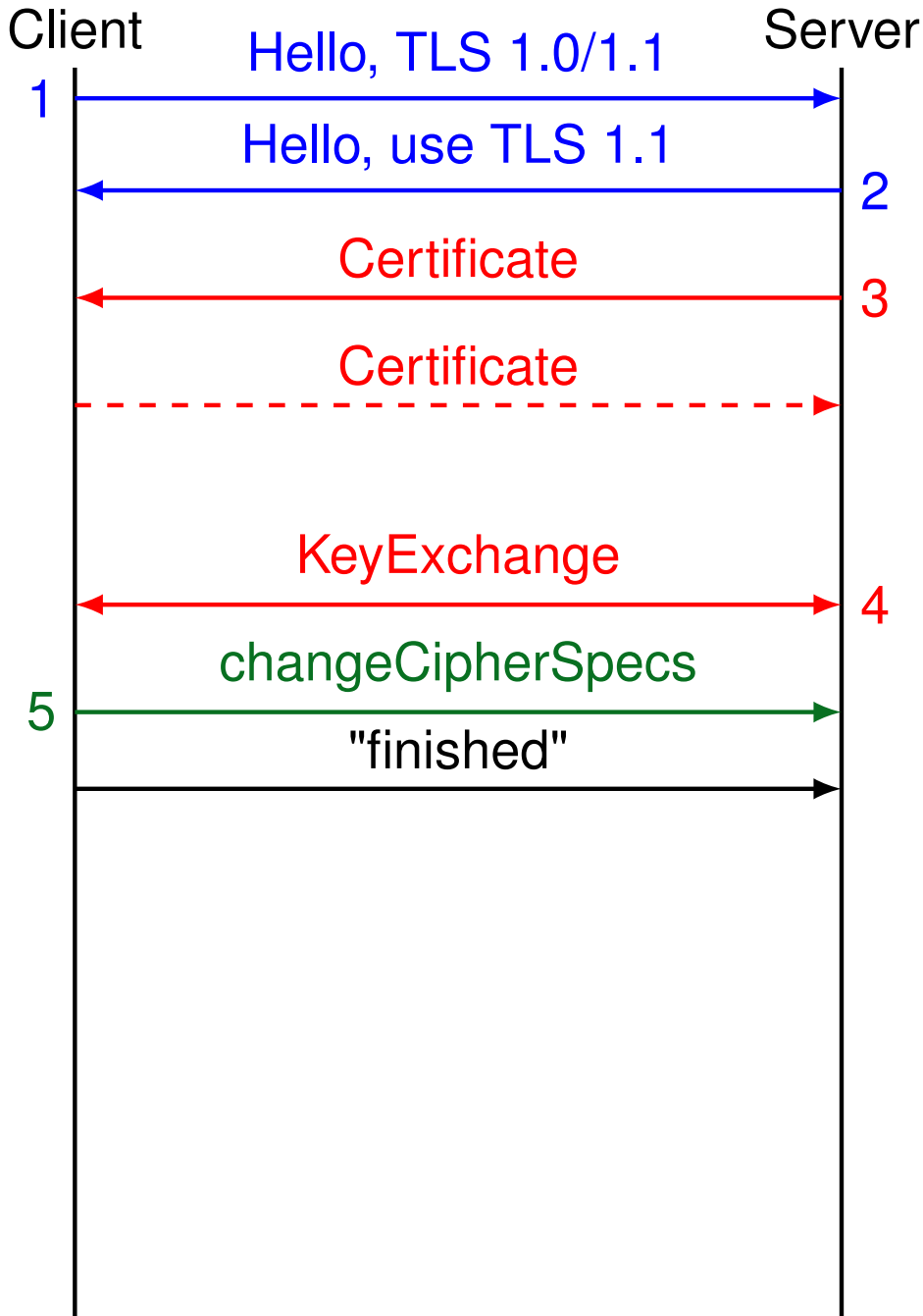
LE PROTOCOLE TLS



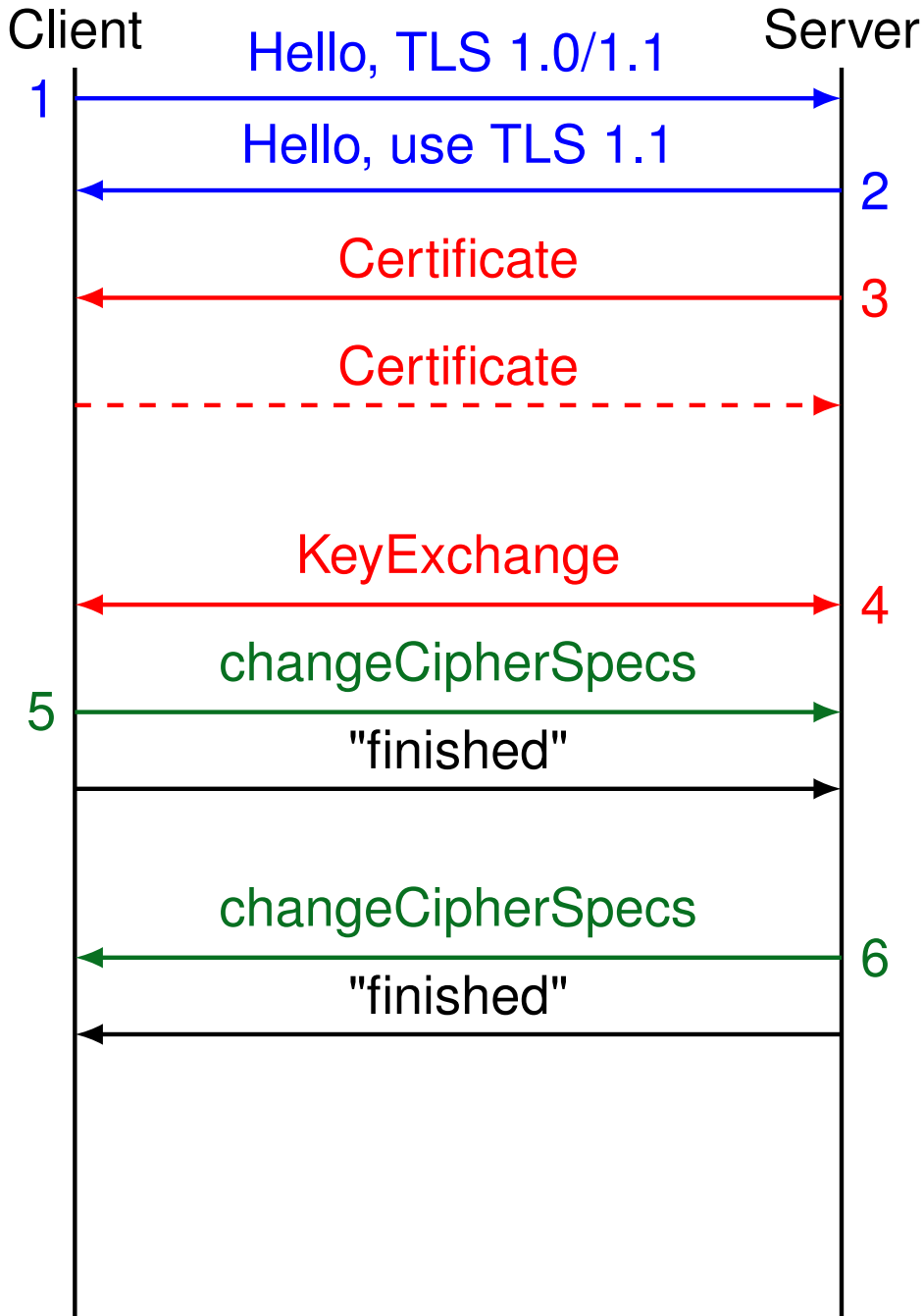
LE PROTOCOLE TLS



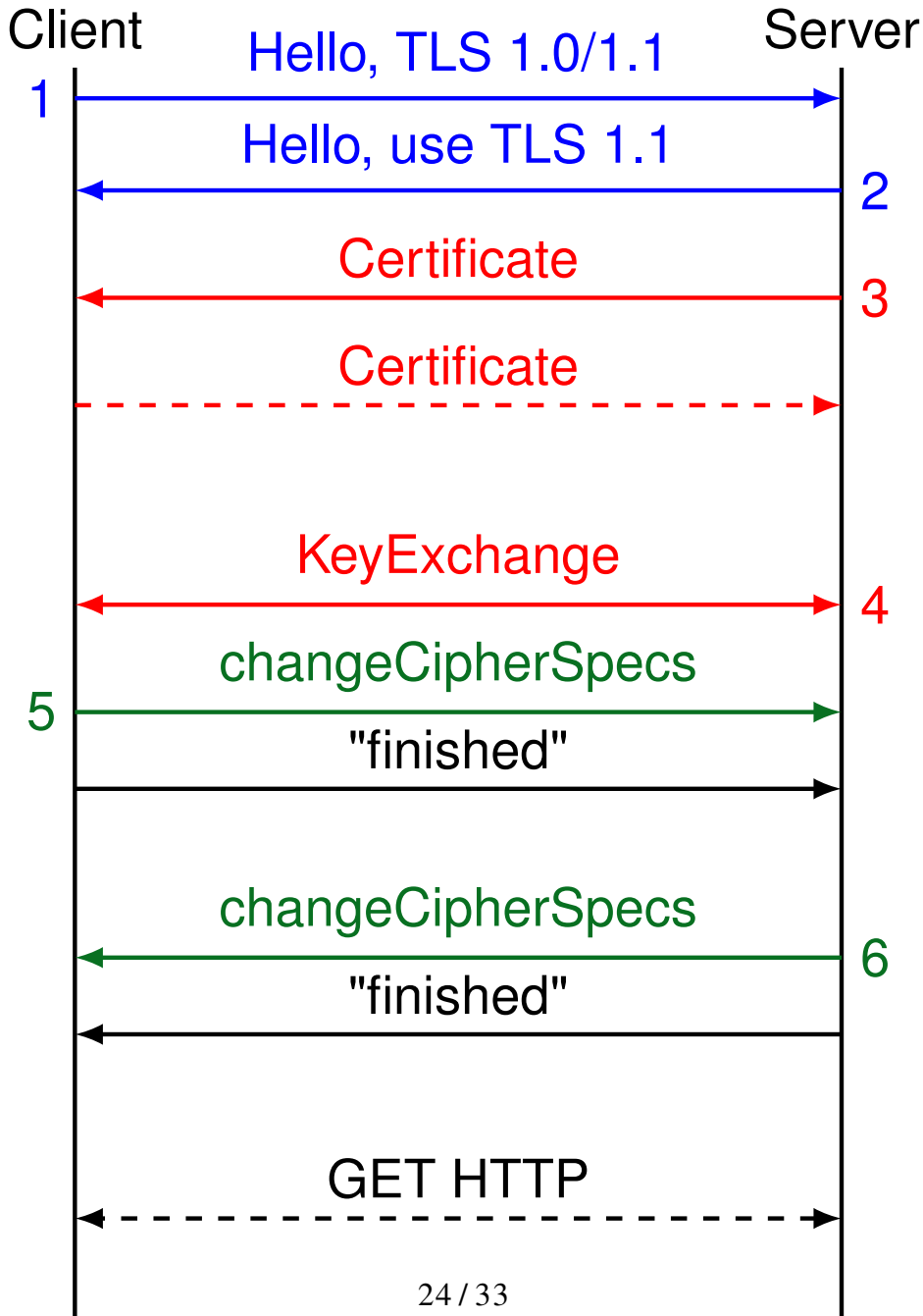
LE PROTOCOLE TLS



LE PROTOCOLE TLS



LE PROTOCOLE TLS



Deuxième problème : la réduction à des problèmes supposés difficiles

L'attaquant connaît G, g, g^a et g^b

Deuxième problème : la réduction à des problèmes supposés difficiles

L'attaquant connaît G, g, g^a et g^b
On peut donc montrer que l'attaquant potentiel, en observant les données transmises ne peut pas connaître les secrets a et b si le problème DLOG est dur.

La réduction à des problèmes supposés difficiles

$\mathcal{E}$

Attaquant

La réduction à des problèmes supposés difficiles

$\mathcal{P}$ $\mathcal{E}$

Attaquant

La réduction à des problèmes supposés difficiles

$$\mathcal{P} \quad \prec \quad \mathcal{E}$$

Attaquant

La réduction à des problèmes supposés difficiles

$$\mathcal{P} \quad \prec \quad \mathcal{E}$$

Scientifiques Attaquant

La réduction à des problèmes supposés difficiles

$$\mathcal{P} \quad \prec \quad \mathcal{E}$$

Scientifiques $\prec$ Attaquant

QUELS POBLÈMES DANS NOS PROBLÈMES ?

- RSA : $E_k(m) = m^e \mod pq$

QUELS POBLÈMES DANS NOS PROBLÈMES ?

- RSA : $E_k(m) = m^e \mod pq$
- Log discret : Calculer a à partir de g et g^a

QUELS POBLÈMES DANS NOS PROBLÈMES ?

- RSA : $E_k(m) = m^e \mod pq$
- Log discret : Calculer a à partir de g et g^a
- Lattice-based crypto

Quels poblèmes dans nos problèmes ?

- RSA : $E_k(m) = m^e \mod pq$
- Log discret : Calculer a à partir de g et g^a
- Lattice-based crypto
- Code-based crypto

Quels poblèmes dans nos problèmes ?

- RSA : $E_k(m) = m^e \mod pq$
- Log discret : Calculer a à partir de g et g^a
- Lattice-based crypto
- Code-based crypto
- Isogeny-based crypto

Quels poblèmes dans nos problèmes ?

- RSA : $E_k(m) = m^e \mod pq$
- Log discret : Calculer a à partir de g et g^a
- Lattice-based crypto
- Code-based crypto
- Isogeny-based crypto
- Multivariate crypto

UN EXEMPLE : CODE-BASED CRYPTO

On prend un code $\mathcal{C} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, et on prend deux matrices S et P qui définissent le code.

- Chiffrement : $c = P(m) + e$

UN EXEMPLE : CODE-BASED CRYPTO

On prend un code $\mathcal{C} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, et on prend deux matrices S et P qui définissent le code.

- Chiffrement : $c = P(m) + e$
- Déchiffrement : $\mathcal{D}_S(c)$

UN SECOND EXEMPLE : MULTIVARIATE CRYPTO

On prend un polynôme $\mathcal{Q}$: $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ inversible et deux applications linéaires L_1 et L_2 sur $\mathbb{F}_{q^n}$. On rend public l'application $\mathcal{A}=L_1 \circ \mathcal{Q} \circ L_2$.

- Chiffrement : $C = \mathcal{A}(m)$

UN SECOND EXEMPLE : MULTIVARIATE CRYPTO

On prend un polynôme $\mathcal{Q}$: $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ inversible et deux applications linéaires L_1 et L_2 sur $\mathbb{F}_{q^n}$. On rend public l'application $\mathcal{A}=L_1 \circ \mathcal{Q} \circ L_2$.

- Chiffrement : $C = \mathcal{A}(m)$
- Déchiffrement : ${L_1}^{-1} \circ Q^{-1} \circ {L_2}^{-1}(c)$

Difficulté des problèmes

- Si les problèmes sont NP-durs : problème de la trappe
- S'il y a réduction dans le cas général : pas NP-dur

Plan

Les différents domaines de recherche

- Conception et analyse de primitives symétriques (chiffrements par bloc, permutations, fonctions de hachage)

Les différents domaines de recherche

- Conception et analyse de primitives symétriques (chiffrements par bloc, permutations, fonctions de hachage)
- Protocoles et preuves formelles

Les différents domaines de recherche

- Conception et analyse de primitives symétriques (chiffrements par bloc, permutations, fonctions de hachage)
- Protocoles et preuves formelles
- Conception et analyse de chiffrements et signatures (asymétriques)

Les différents domaines de recherche

- Conception et analyse de primitives symétriques (chiffrements par bloc, permutations, fonctions de hachage)
- Protocoles et preuves formelles
- Conception et analyse de chiffrements et signatures (asymétriques)
- Analyse de problèmes supposés difficiles

Les différents domaines de recherche

- Conception et analyse de primitives symétriques (chiffrements par bloc, permutations, fonctions de hachage)
- Protocoles et preuves formelles
- Conception et analyse de chiffrements et signatures (asymétriques)
- Analyse de problèmes supposés difficiles
- Réduction de problèmes

Les différents domaines de recherche

- Conception et analyse de primitives symétriques (chiffrements par bloc, permutations, fonctions de hachage)
- Protocoles et preuves formelles
- Conception et analyse de chiffrements et signatures (asymétriques)
- Analyse de problèmes supposés difficiles
- Réduction de problèmes
- Analyse et conception résistants aux attaques par canaux auxiliaires

QUELQUES CHAMPS DE RECHERCHE ACTUELS

- Multi-Parti Computation

QUELQUES CHAMPS DE RECHERCHE ACTUELS

- Multi-Parti Computation
- Fully Homomorphic Encryption

Quelques champs de recherche actuels

- Multi-Parti Computation
- Fully Homomorphic Encryption
- En lien avec la cryptographie symétrique

Quelques champs de recherche actuels

- Multi-Parti Computation
- Fully Homomorphic Encryption
- En lien avec la cryptographie symétrique
- Zero-Knowledge Proofs

Quelques champs de recherche actuels

- Multi-Parti Computation
- Fully Homomorphic Encryption
- En lien avec la cryptographie symétrique
- Zero-Knowledge Proofs
- La cryptographie en boîte blanche

Quelques champs de recherche actuels

- Multi-Parti Computation
- Fully Homomorphic Encryption
- En lien avec la cryptographie symétrique
- Zero-Knowledge Proofs
- La cryptographie en boîte blanche
- La cryptographie symétrique à bas coût