RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

Intégration de la Cryptographie Post-Quantique dans les Protocoles de Communication Sécurisés

Abdel Rahman Taleb

Agence nationale de la sécurité des systèmes d'information

24 avril 2025

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

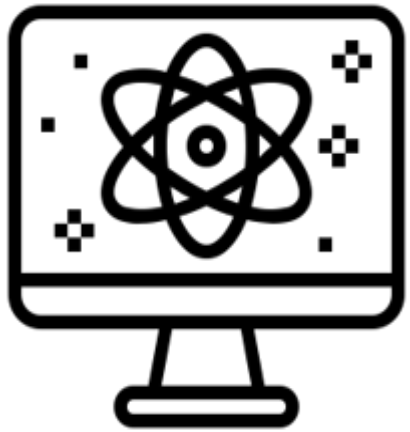
1. Cryptographie Post-Quantique

Menace Quantique sur la Cryptographie Moderne

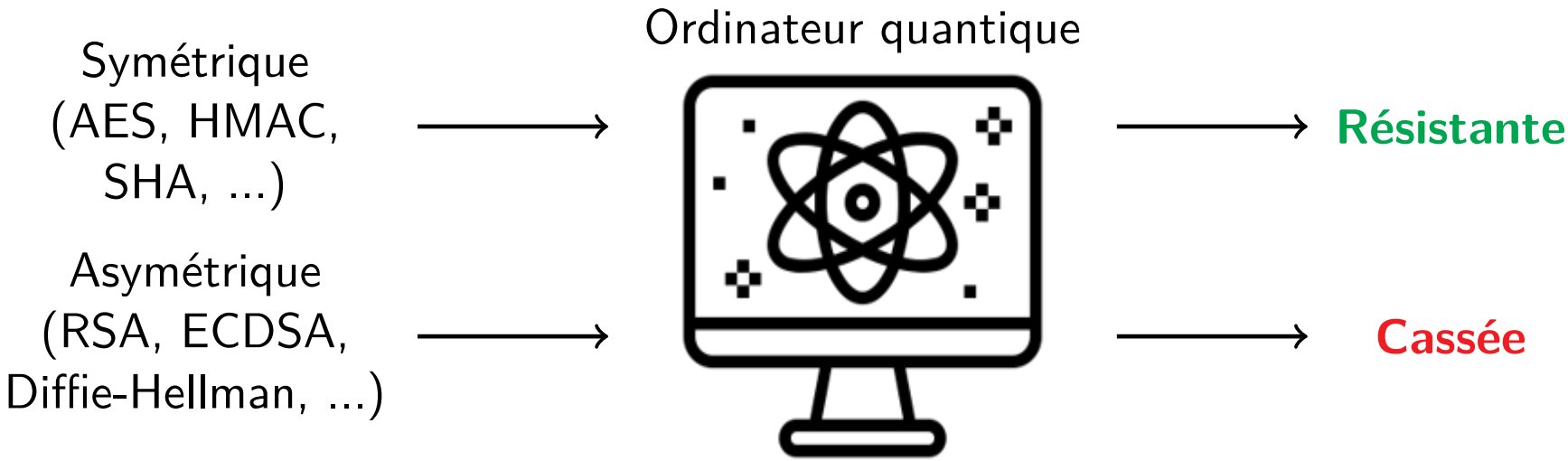
Ordinateur quantique

Symétrique (AES, HMAC, SHA, ...) → → **Résistante**

Asymétrique (RSA, ECDSA, Diffie-Hellman, ...) → → **Cassée**

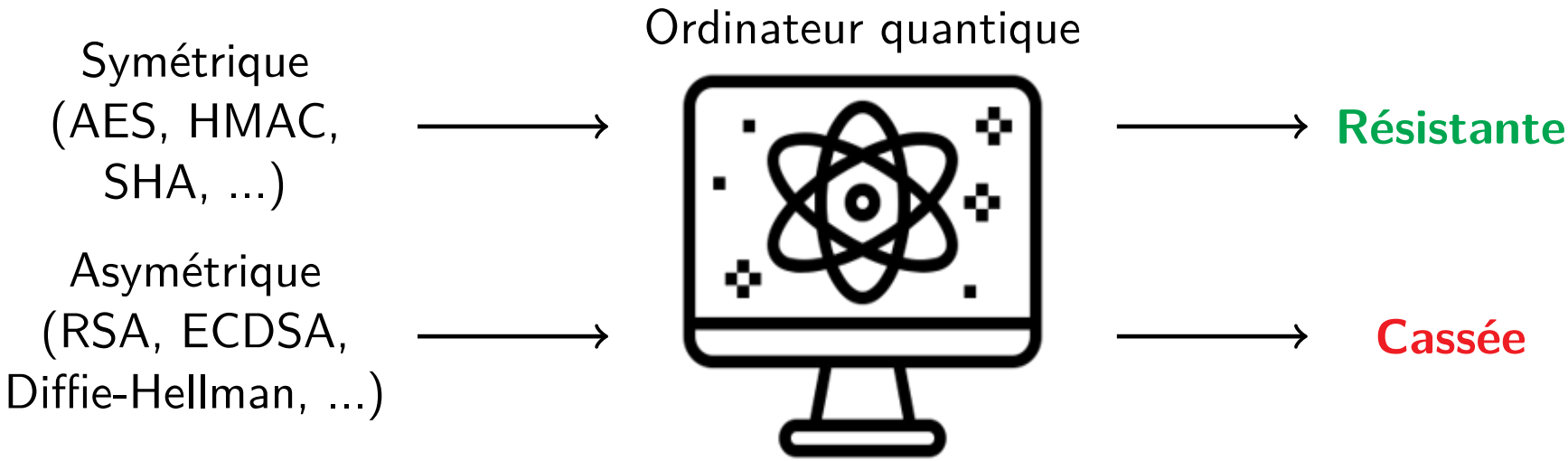


Menace Quantique sur la Cryptographie Moderne



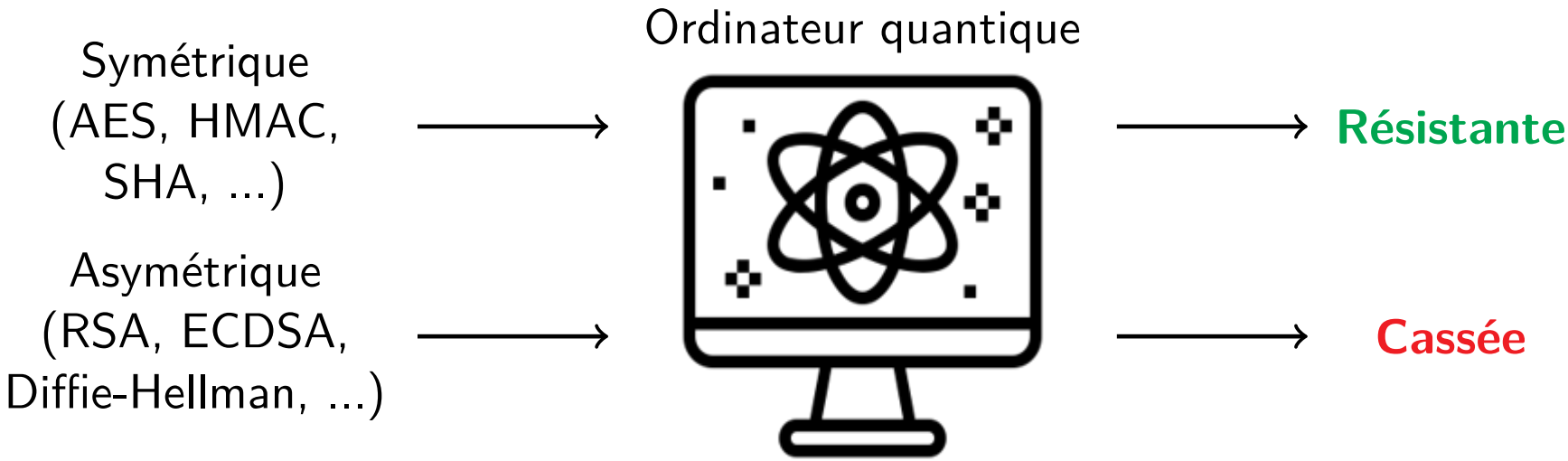
- Algo. de Grover : impact sur les primitives symétriques

Menace Quantique sur la Cryptographie Moderne



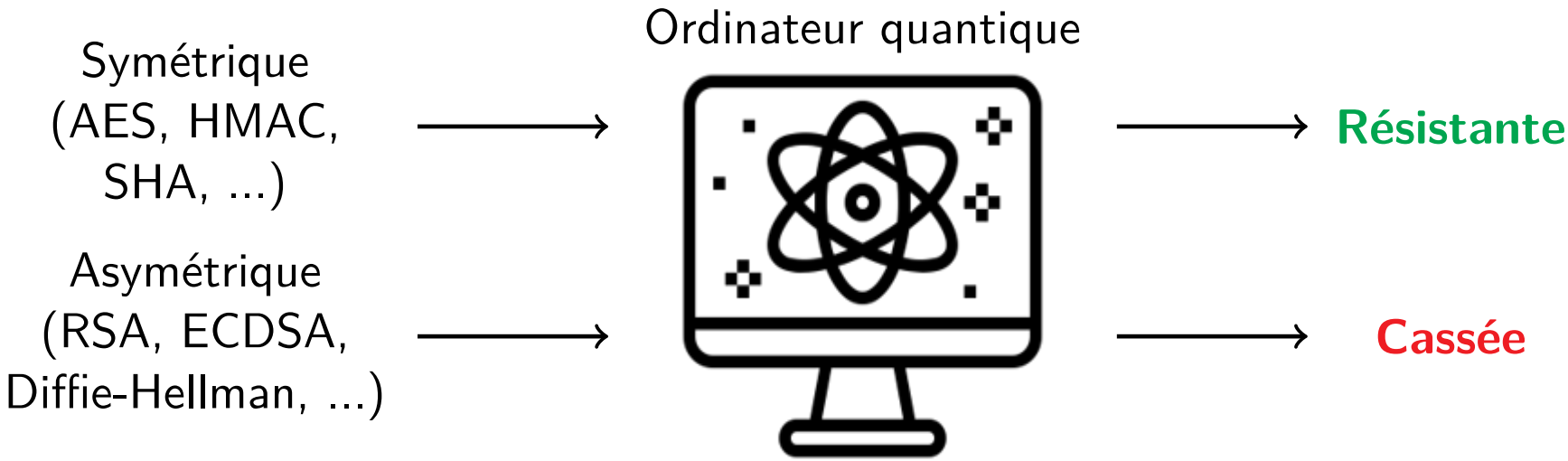
- Algo. de Grover : impact sur les primitives symétriques
  - **Augmenter la taille des clés, sorties des fonctions de hachage, ...**

Menace Quantique sur la Cryptographie Moderne



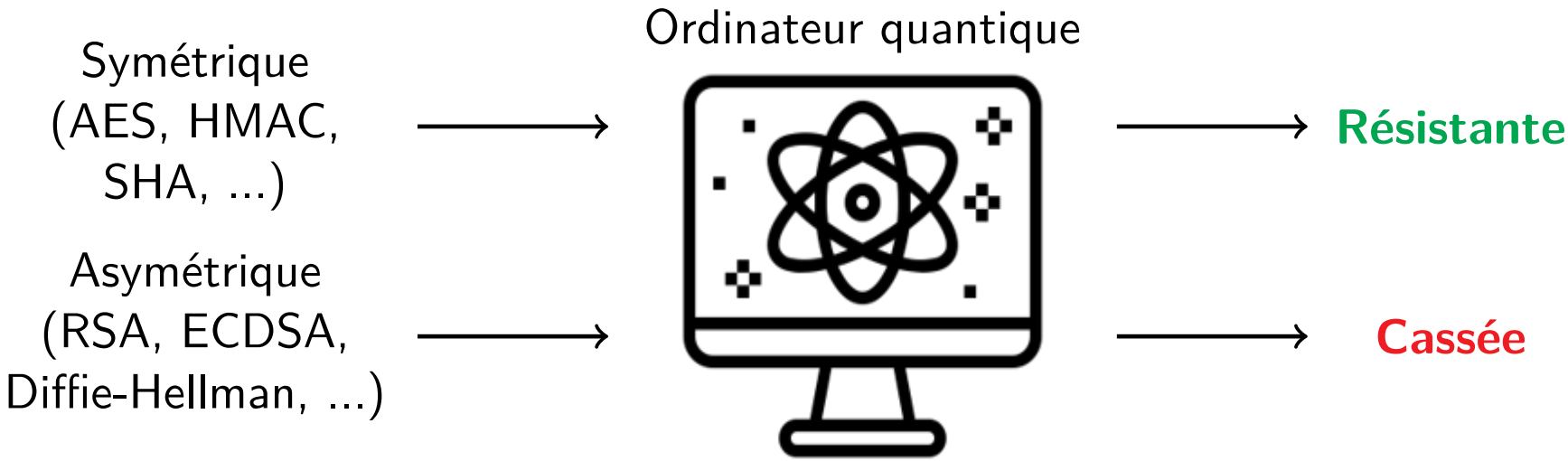
- Algo. de Grover : impact sur les primitives symétriques
  - **Augmenter la taille des clés, sorties des fonctions de hachage, ...**
  - Reco. : éventuellement passer de 128 bits à 256 bits de sécurité

Menace Quantique sur la Cryptographie Moderne



- Algo. de Grover : impact sur les primitives symétriques
  - **Augmenter la taille des clés, sorties des fonctions de hachage, ...**
  - Reco. : éventuellement passer de 128 bits à 256 bits de sécurité
- Algo. de Shor : compromission des primitives asymétriques actuelles

Menace Quantique sur la Cryptographie Moderne



- Algo. de Grover : impact sur les primitives symétriques
  - **Augmenter la taille des clés, sorties des fonctions de hachage, ...**
  - Reco. : éventuellement passer de 128 bits à 256 bits de sécurité
- Algo. de Shor : compromission des primitives asymétriques actuelles
  - **Besoin de nouvelles constructions asymétriques**

Construction d'un Ordinateur Quantique

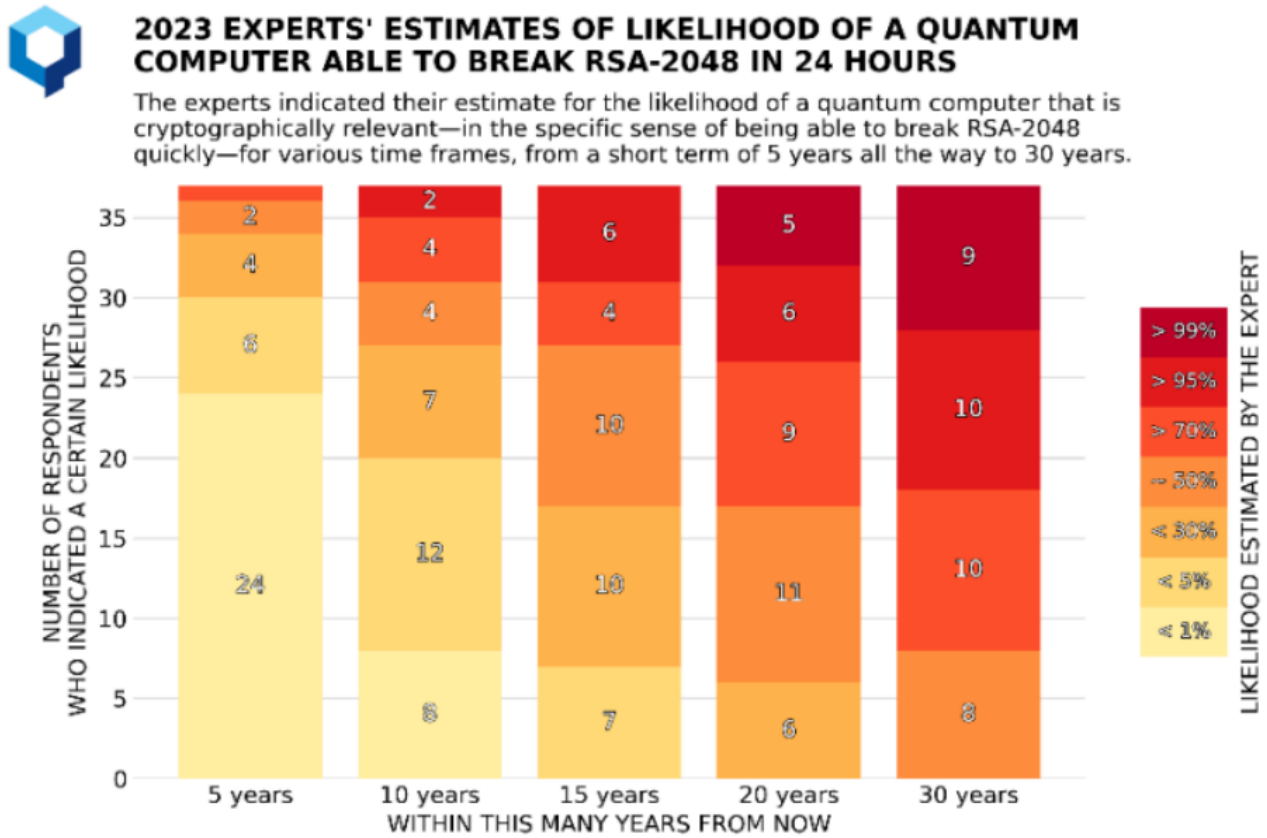
A date, pas de **CRQC** : Cryptographically Relevant Quantum Computer

Construction d'un Ordinateur Quantique

A date, pas de **CRQC** : Cryptographically Relevant Quantum Computer
Cf. "*The status of quantum computer development*" par le BSI
`https://bsi.bund.de/dok/study_status_quantum_computer`

Construction d'un Ordinateur Quantique

A date, pas de **CRQC** : Cryptographically Relevant Quantum Computer
Cf. "*The status of quantum computer development*" par le BSI
`https://bsi.bund.de/dok/study_status_quantum_computer`



`https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/`

Menace Quantique

- Attaques rétroactives **”store now, decrypt later”**

Menace Quantique

- Attaques rétroactives **"store now, decrypt later"**
- Forge de signature $\rightarrow$ usurpation d'identité

Menace Quantique

- Attaques rétroactives **"store now, decrypt later"** Risque immédiat !
- Forge de signature $\rightarrow$ usurpation d'identité Risque lorsqu'un CRQC existera (voire avant pour les signatures long-terme)

Menace Quantique

- Attaques rétroactives **"store now, decrypt later"** Risque immédiat !
- Forge de signature → usurpation d'identité Risque lorsqu'un CRQC existera (voire avant pour les signatures long-terme)

→ Besoin de remplacer les primitives asymétriques classiques !

Menace Quantique

- Attaques rétroactives **"store now, decrypt later"** Risque immédiat !
- Forge de signature $\rightarrow$ usurpation d'identité Risque lorsqu'un CRQC existera (voire avant pour les signatures long-terme)

$\rightarrow$ Besoin de remplacer les primitives asymétriques classiques !

Théorème de Mosca

Menace Quantique

- Attaques rétroactives **"store now, decrypt later"** Risque immédiat !
- Forge de signature $\rightarrow$ usurpation d'identité Risque lorsqu'un CRQC existera (voire avant pour les signatures long-terme)

$\rightarrow$ Besoin de remplacer les primitives asymétriques classiques !

Théorème de Mosca

Il faut que $X + Y \leq Z$

Menace Quantique

- Attaques rétroactives **"store now, decrypt later"** Risque immédiat !
- Forge de signature $\rightarrow$ usurpation d'identité Risque lorsqu'un CRQC existera (voire avant pour les signatures long-terme)

$\rightarrow$ Besoin de remplacer les primitives asymétriques classiques !

Théorème de Mosca

Il faut que $X + Y \leq Z$

X : années de protection des données

Menace Quantique

- Attaques rétroactives **"store now, decrypt later"** Risque immédiat !
- Forge de signature $\rightarrow$ usurpation d'identité Risque lorsqu'un CRQC existera (voire avant pour les signatures long-terme)

$\rightarrow$ Besoin de remplacer les primitives asymétriques classiques !

Théorème de Mosca

Il faut que $X + Y \leq Z$

X : années de protection des données

Y : années nécessaires pour la transition

Menace Quantique

- Attaques rétroactives **"store now, decrypt later"** Risque immédiat !
- Forge de signature → usurpation d'identité Risque lorsqu'un CRQC existera (voire avant pour les signatures long-terme)

→ Besoin de remplacer les primitives asymétriques classiques !

Théorème de Mosca

Il faut que $X + Y \leq Z$

- X : années de protection des données
- Y : années nécessaires pour la transition
- Z : années pour l'apparition d'un **CRQC**

Compétition du NIST : Niveaux de Sécurité

Niveau de sécurité	Complexité calculatoire équivalente
L1	recherche de clé sur l'AES-128
L2	recherche de collisions sur SHA-256
L3	recherche de clé sur l'AES-192
L4	recherche de collisions sur SHA-384
L5	recherche de clé sur l'AES-256

Performance des Signatures Post-Quantiques

3 schémas sélectionnés par le NIST

- DILITHIUM (ML-DSA), FALCON (FN-DSA), SPHINCS+ (SLH-DSA)

Performance des Signatures Post-Quantiques

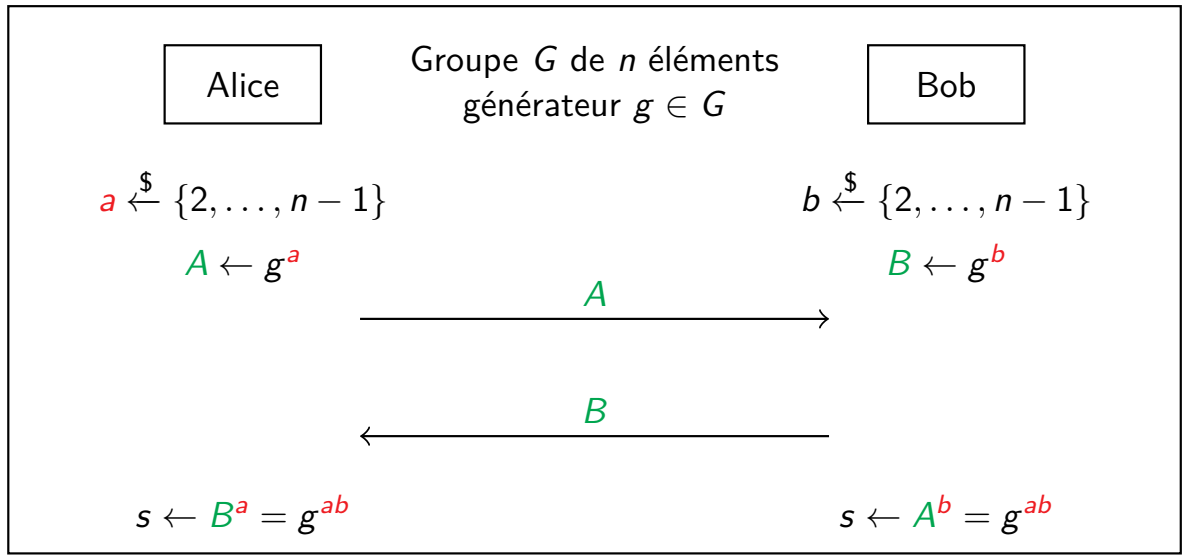
3 schémas sélectionnés par le NIST

- DILITHIUM (ML-DSA), FALCON (FN-DSA), SPHINCS+ (SLH-DSA)

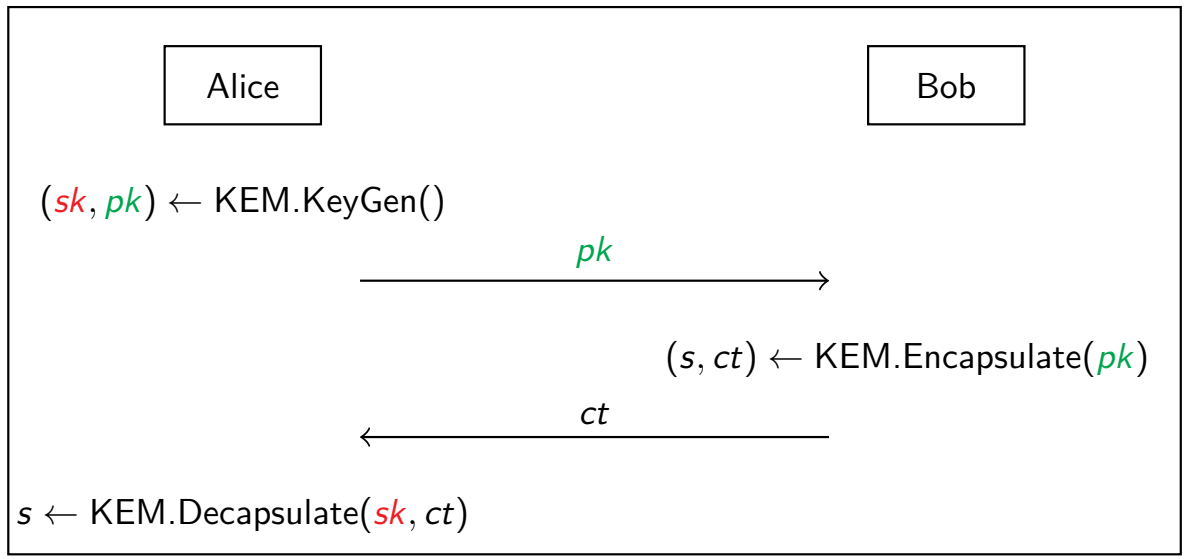
schéma de signature		taille (en octets)			temps (en ms)	
		clé privée	clé publique	signature	signature	vérification
niveau de sécurité L1						
ECDSA (brainpoolP256t1)		32	64	64	0.3	0.3
FALCON-512		1 281	897	666	0.216	0.037
SPHINCS+ (SHA2)	small	64	32	7 856	129.92	0.222
	fast			17 088	6.364	0.55
niveau de sécurité L5						
ECDSA (brainpoolP512t1)		64	128	128	1.2	1
ML-DSA-87		4 896	2 592	4 627	0.119	0.058
FALCON-1024		2 305	1 793	1 280	0.43	0.08
SPHINCS+ (SHA2)	small	128	64	29 792	227.62	0.45
	fast			49 856	22.82	0.8

Préliminaire : Échange de Clés

Diffie-Hellman
secret partagé: s



Key **E**ncapsulation **M**echanism (**KEM**)
secret partagé: s



Performance des KEMs Post-Quantiques

2 schémas sélectionnés par le NIST

- KYBER (ML-KEM), HQC

Performance des KEMs Post-Quantiques

2 schémas sélectionnés par le NIST

- KYBER (ML-KEM), HQC

schéma d'échange de clés	Alice → Bob (en octets)	Bob → Alice (en octets)	temps (en ms)	
			Alice	Bob
niveau de sécurité L1				
ECDH (brainpoolP256t1)	64	64	0.6	0.6
ML-KEM-512	800	768	0.014	0.007
HQC-128	2 249	4 497	6.15	3.04
niveau de sécurité L5				
ECDH (brainpoolP512t1)	128	128	2	2
ML-KEM-1024	1 568	1 568	0.033	0.016
HQC-256	7 245	14 485	33.53	16.7

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

2. Protocoles de Communication Sécurisés

Protocoles de Communication Sécurisés

Client - Serveur

Protocoles de Communication Sécurisés

Client - Serveur

- (D)TLS, QUIC

Protocoles de Communication Sécurisés

Client - Serveur

- (D)TLS, QUIC

Utilisateur - Machine Distante

Protocoles de Communication Sécurisés

Client - Serveur

- (D)TLS, QUIC

Utilisateur - Machine Distante

- SSH

Protocoles de Communication Sécurisés

Client - Serveur

- (D)TLS, QUIC

Utilisateur - Machine Distante

- SSH

Tunnel VPN

Protocoles de Communication Sécurisés

Client - Serveur

- (D)TLS, QUIC

Utilisateur - Machine Distante

- SSH

Tunnel VPN

- IPsec, WireGuard, OpenVPN

Protocoles de Communication Sécurisés

Client - Serveur

- (D)TLS, QUIC

Utilisateur - Machine Distante

- SSH

Tunnel VPN

- IPsec, WireGuard, OpenVPN

Messagerie sécurisée

Protocoles de Communication Sécurisés

Client - Serveur

- (D)TLS, QUIC

Utilisateur - Machine Distante

- SSH

Tunnel VPN

- IPsec, WireGuard, OpenVPN

Messagerie sécurisée

- Whatsapp, Signal, Olvid

Protocoles de Communication Sécurisés

Client - Serveur

- (D)TLS, QUIC

Utilisateur - Machine Distante

- SSH

Tunnel VPN

- IPsec, WireGuard, OpenVPN

Messagerie sécurisée

- Whatsapp, Signal, Olvid

Mails

Protocoles de Communication Sécurisés

Client - Serveur

- (D)TLS, QUIC

Utilisateur - Machine Distante

- SSH

Tunnel VPN

- IPsec, WireGuard, OpenVPN

Messagerie sécurisée

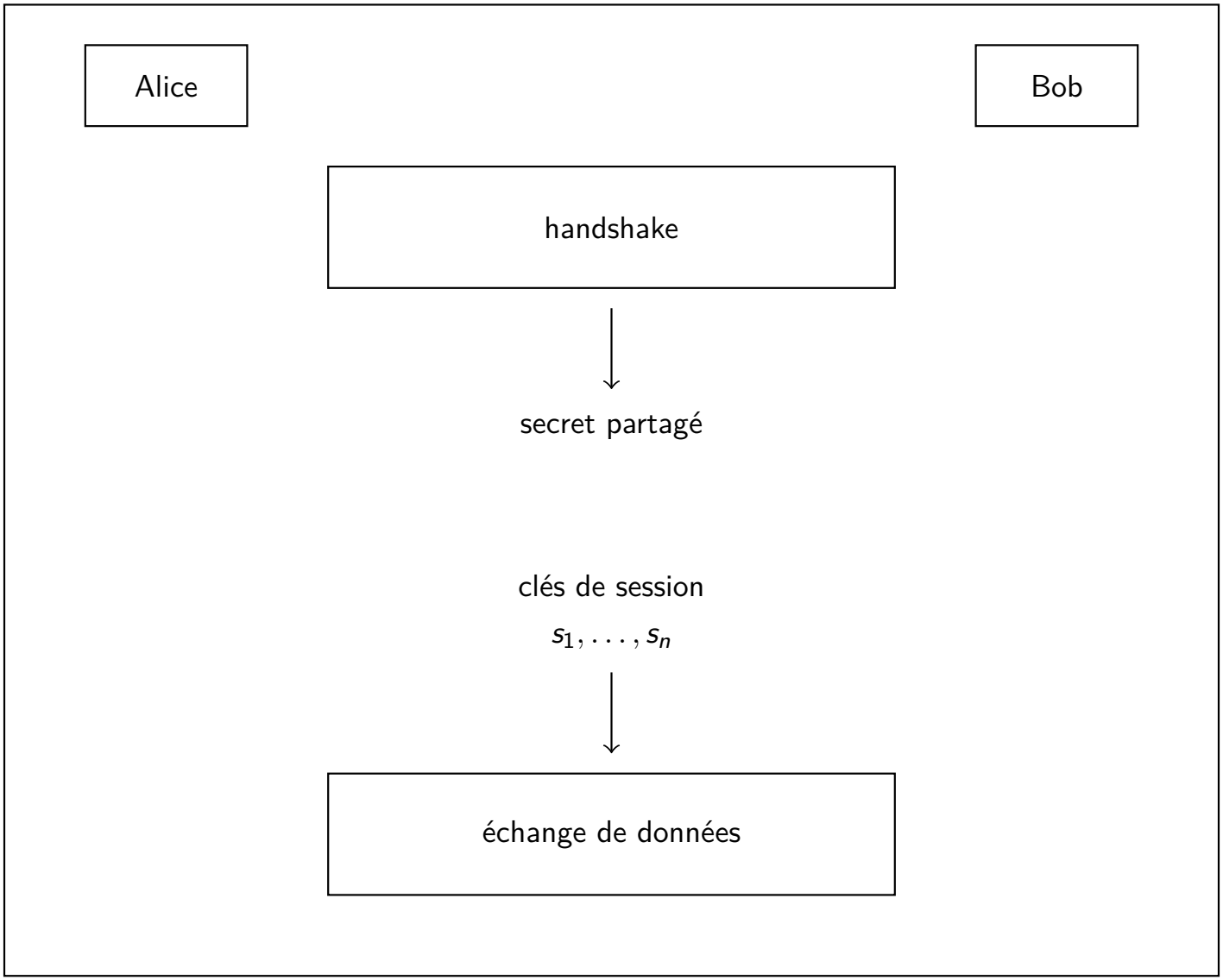
- Whatsapp, Signal, Olvid

Mails

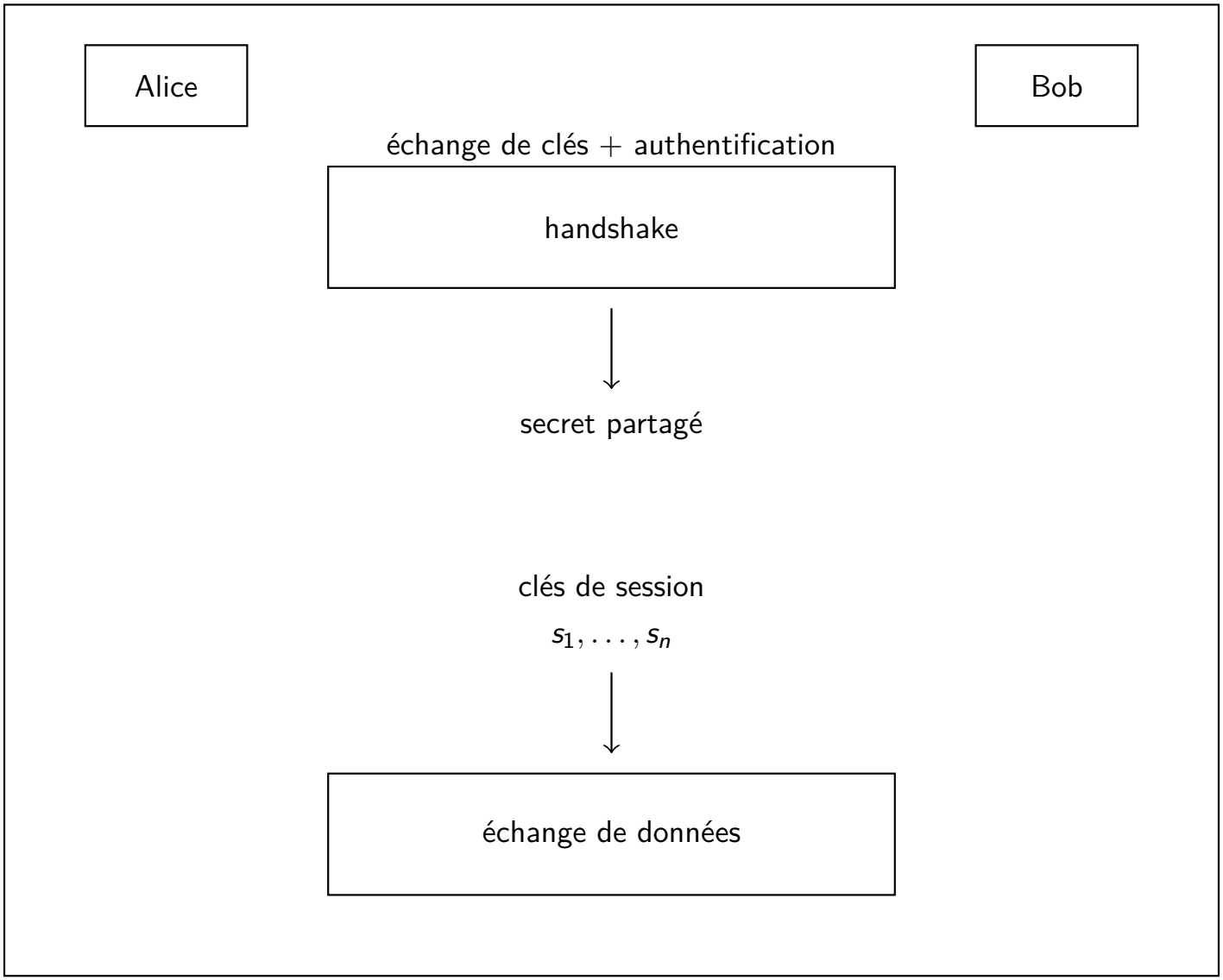
- S/MIME

...

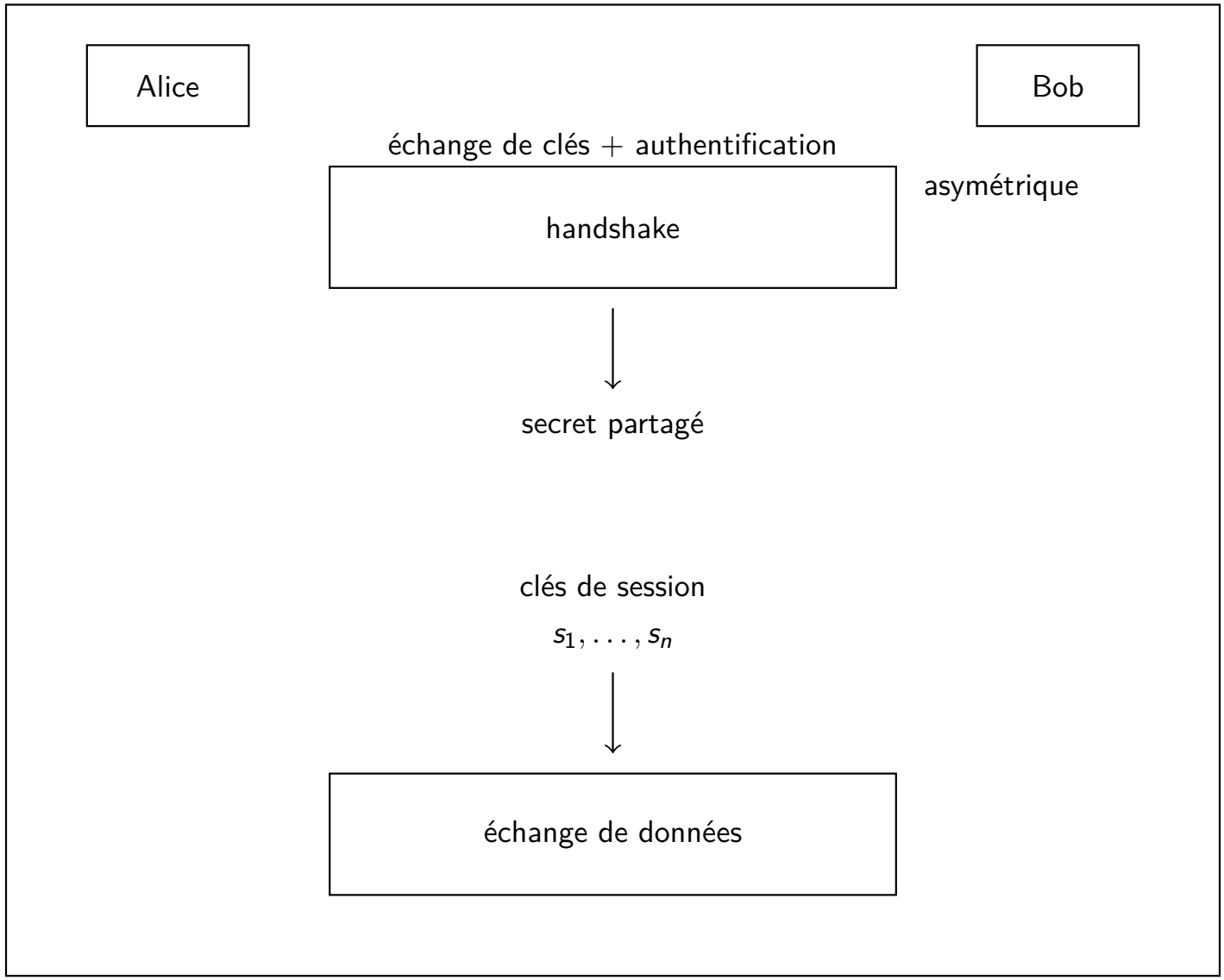
Protocoles de Communication Sécurisés



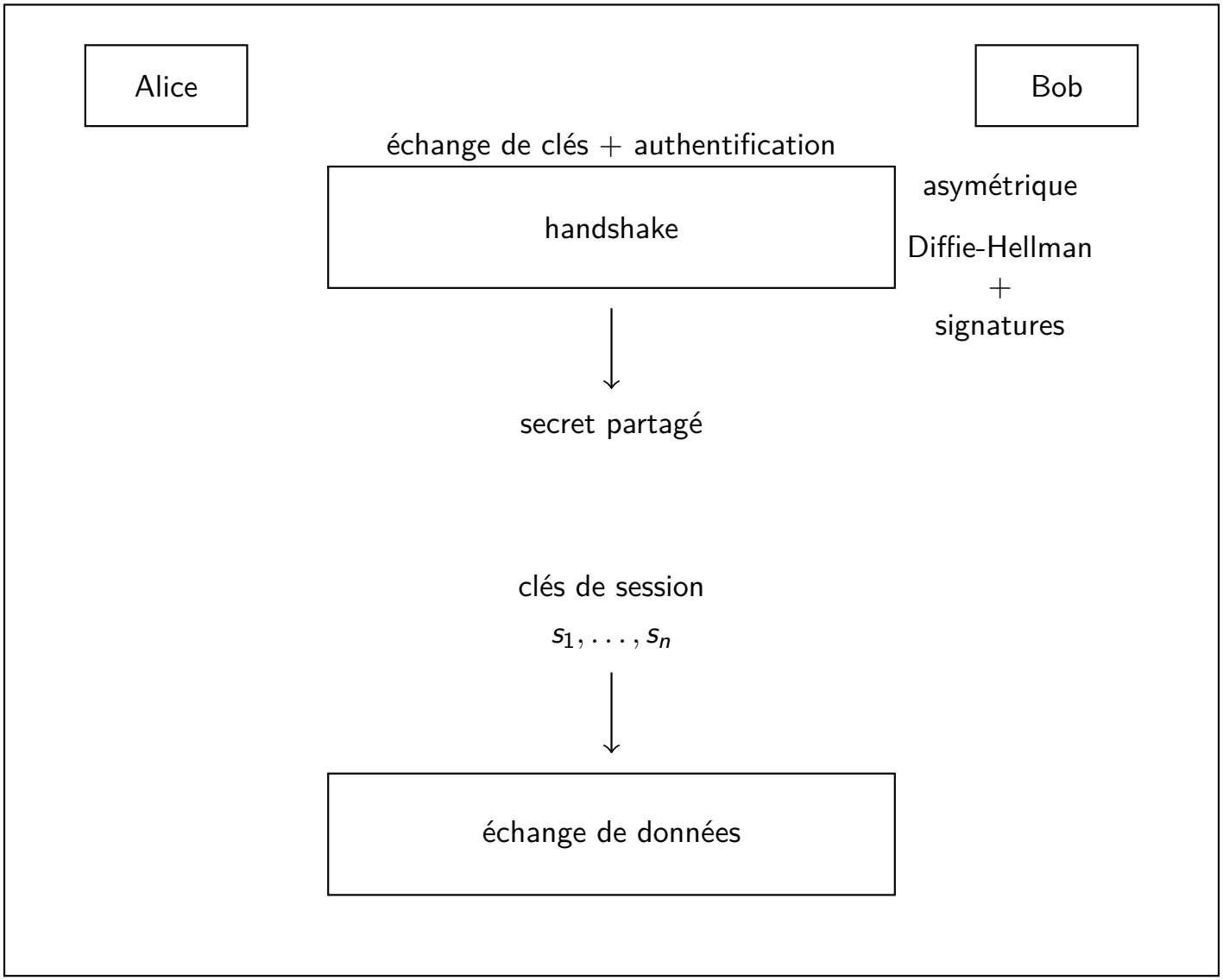
Protocoles de Communication Sécurisés



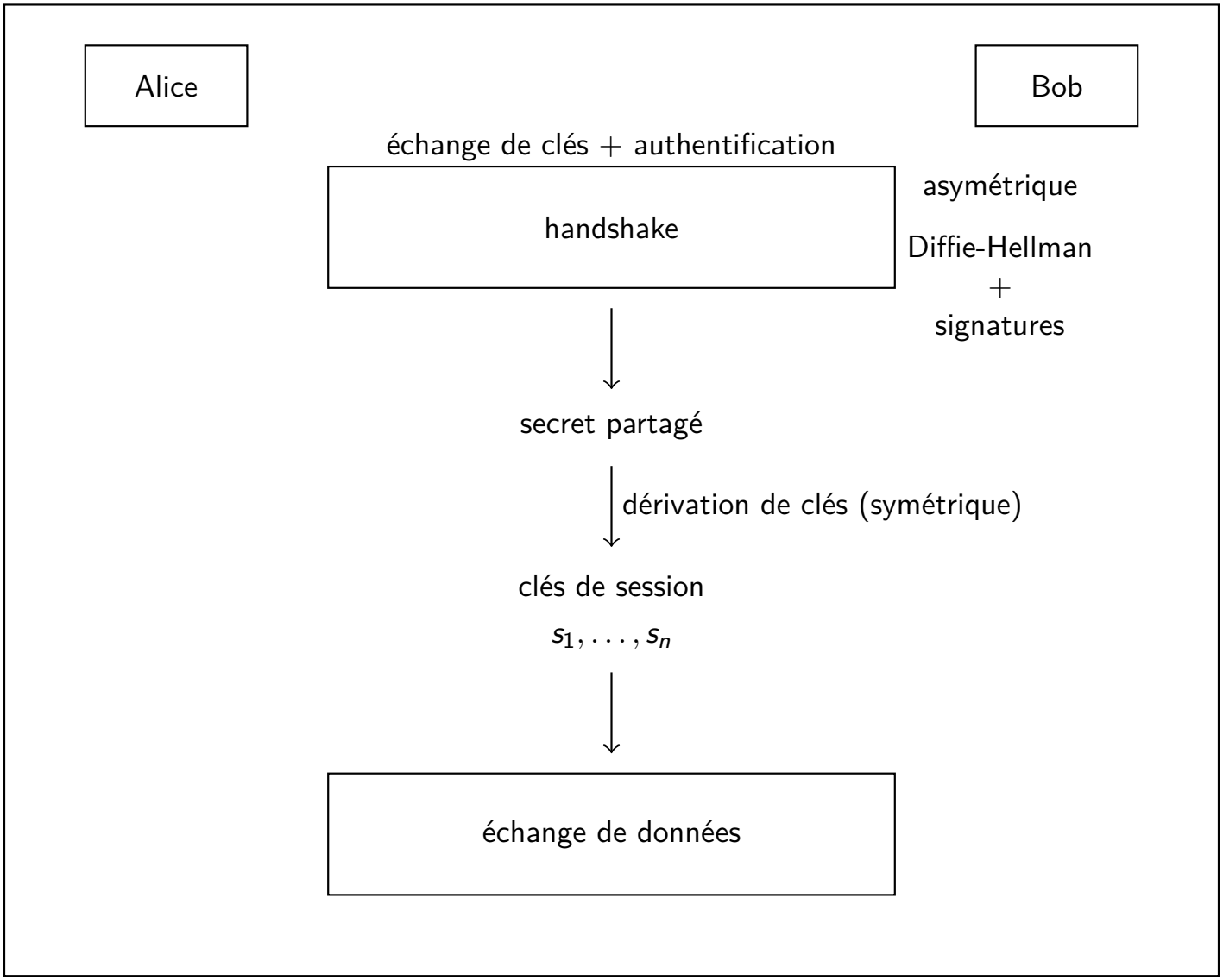
Protocoles de Communication Sécurisés



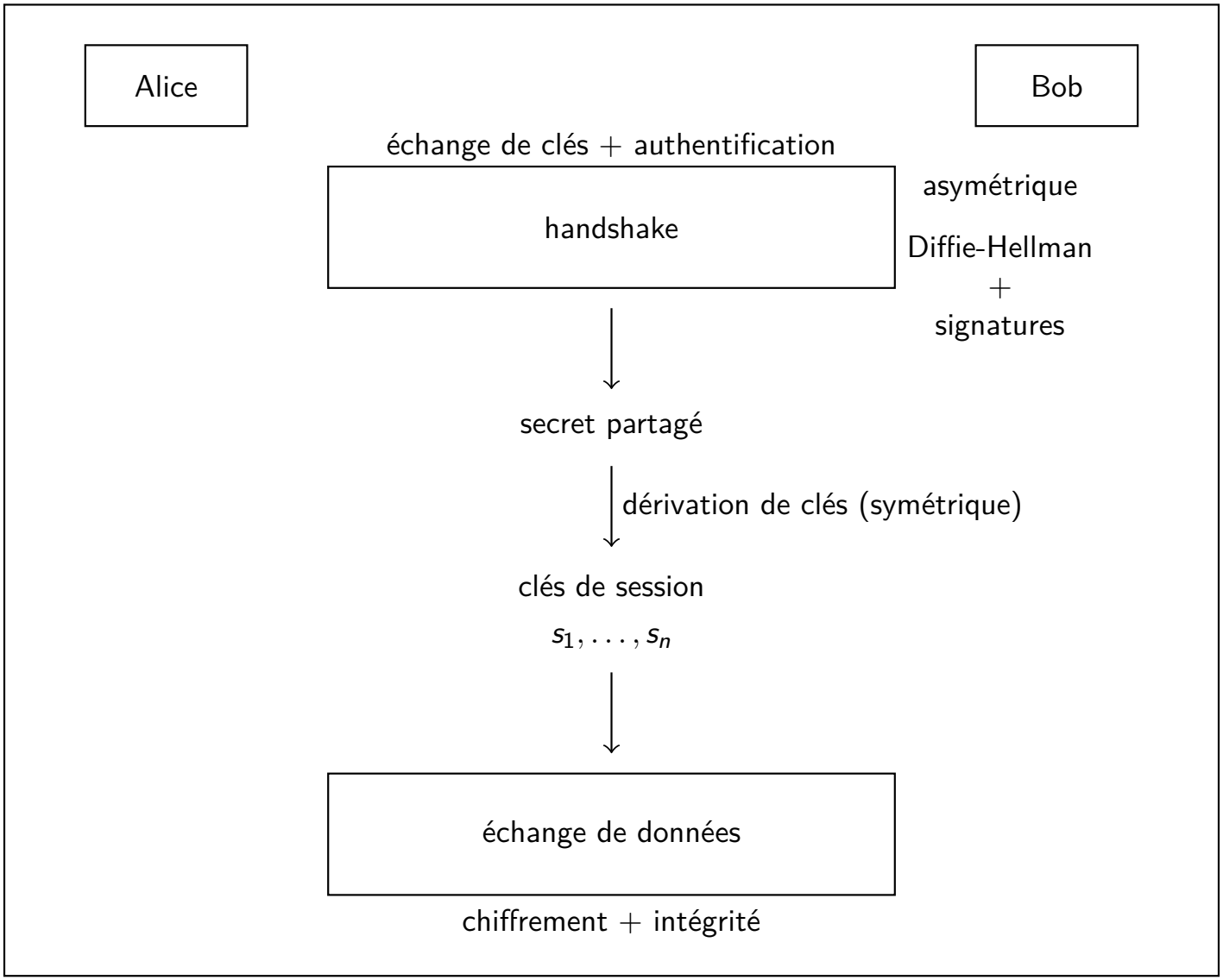
Protocoles de Communication Sécurisés



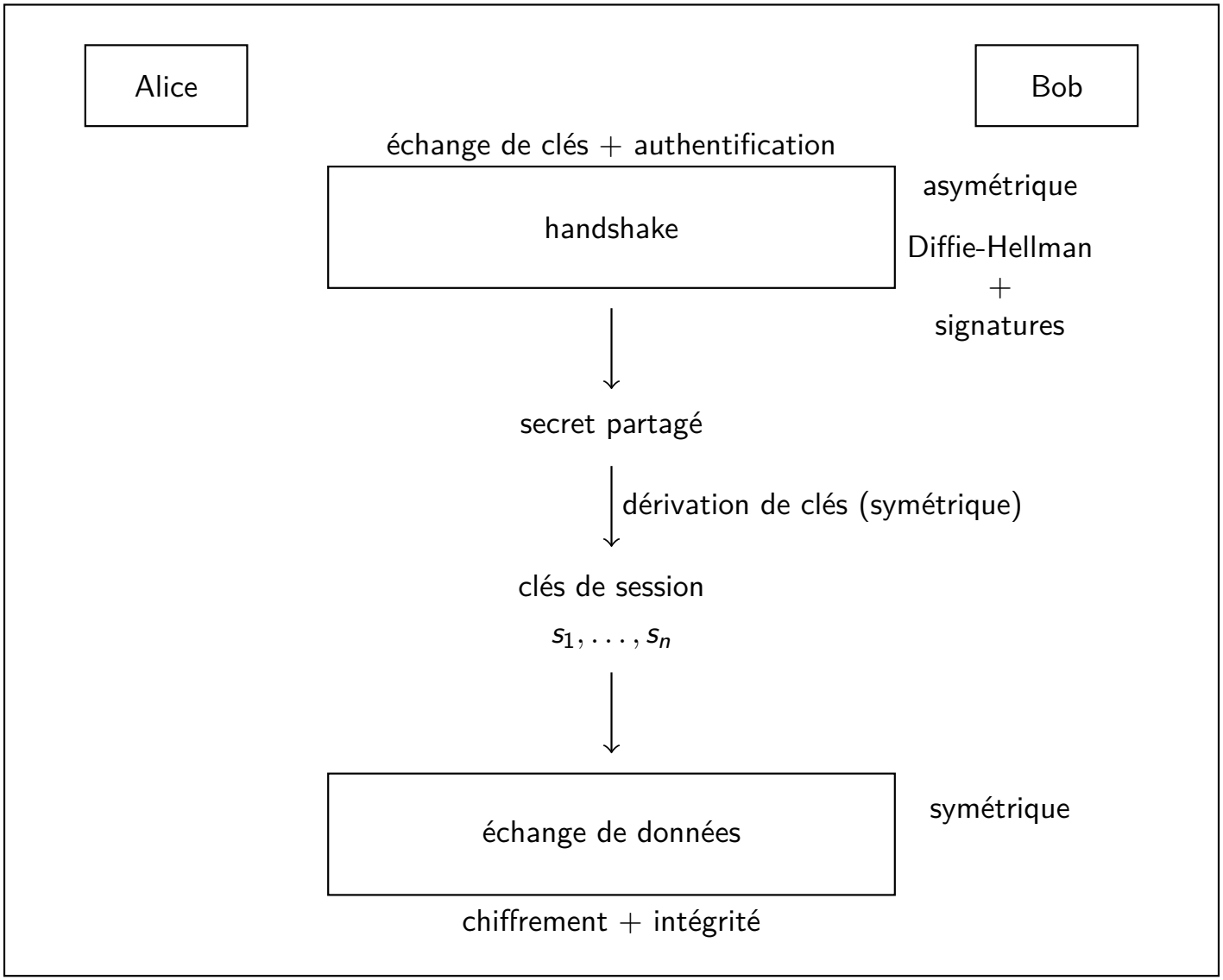
Protocoles de Communication Sécurisés



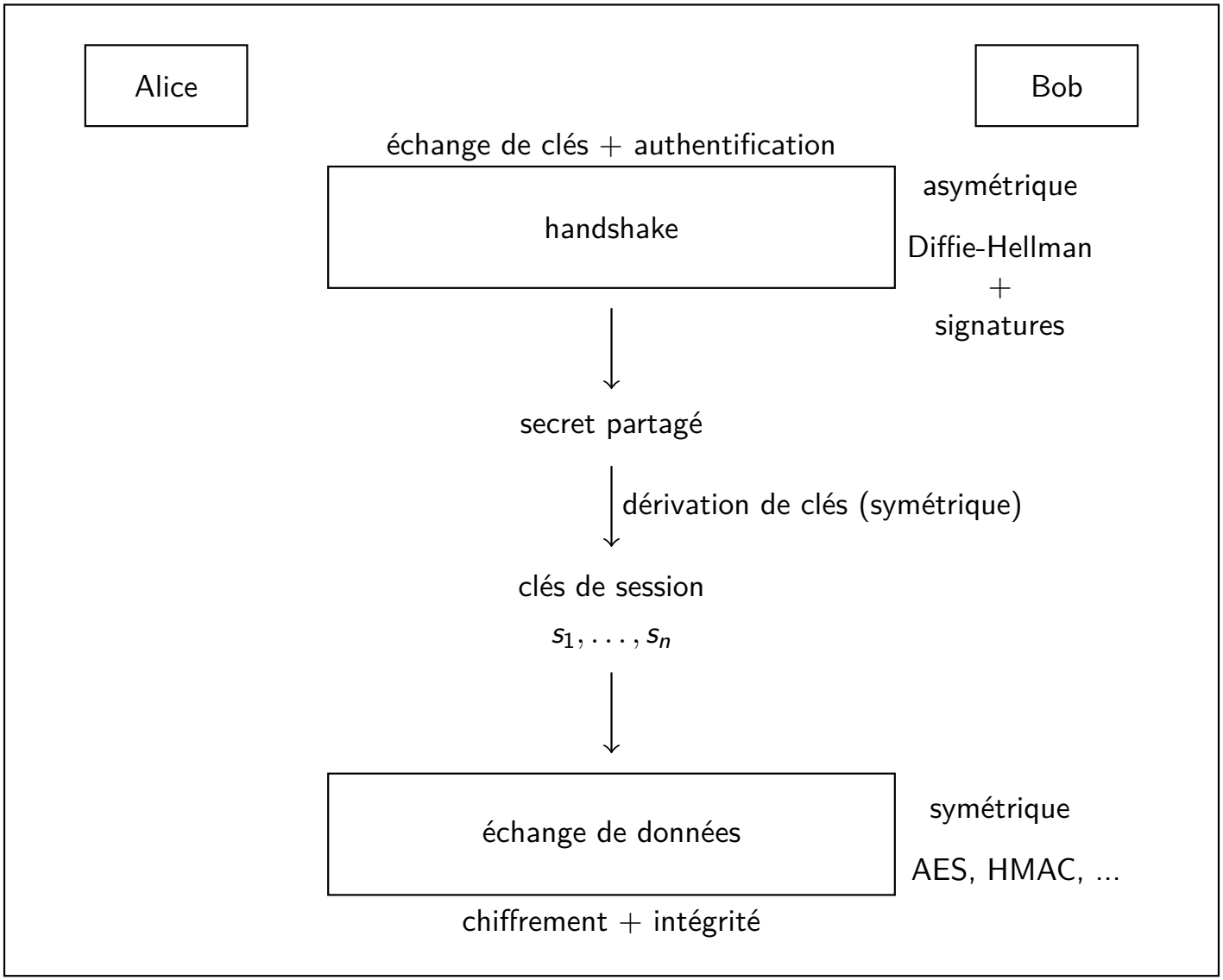
Protocoles de Communication Sécurisés



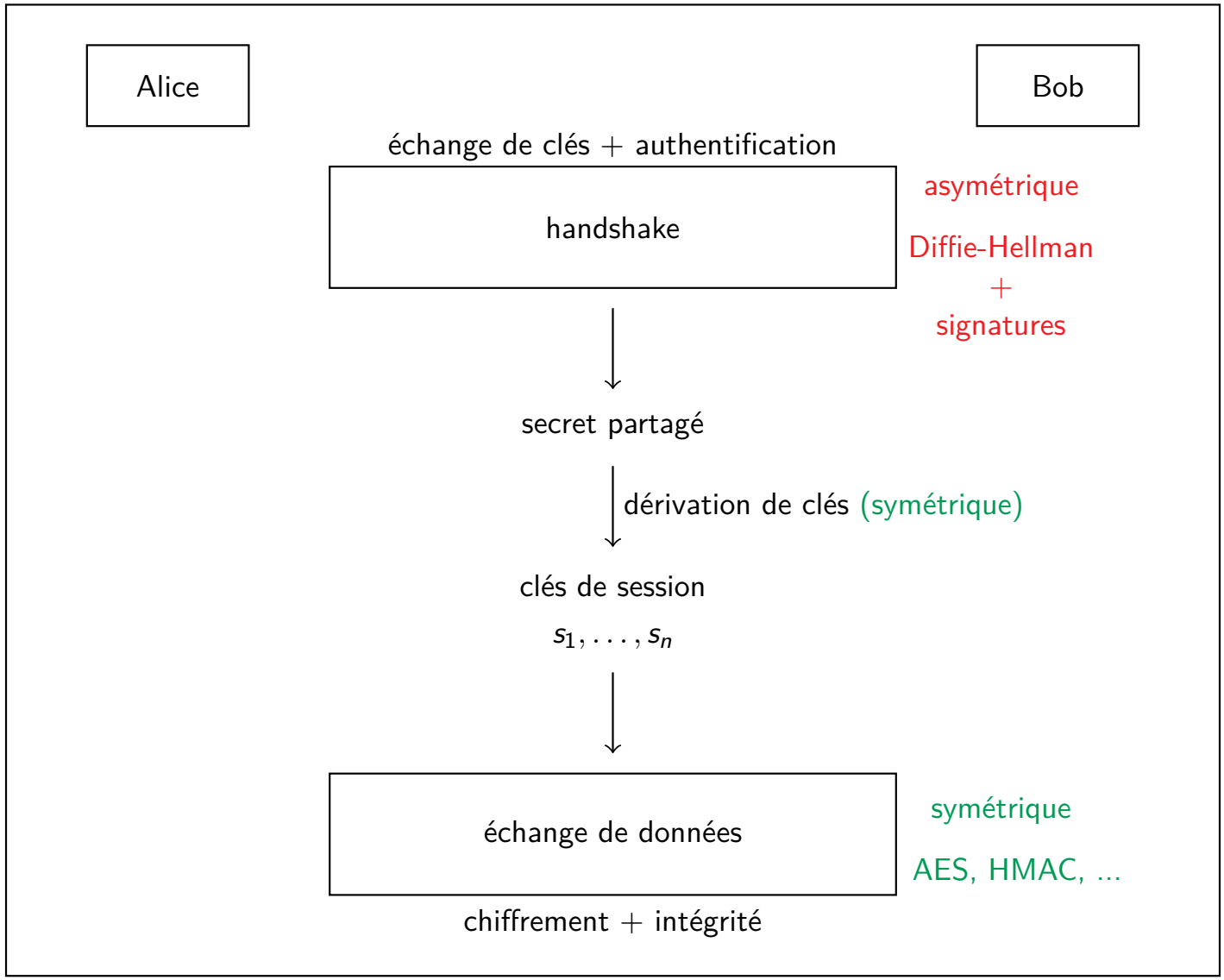
Protocoles de Communication Sécurisés



Protocoles de Communication Sécurisés



Menace Quantique sur les Protocoles



Menace Quantique sur les Protocoles

handshake

Diffie-Hellman

+

Signatures

Menace Quantique sur les Protocoles

handshake

Diffie-Hellman

+

Signatures

$\longrightarrow$

Remplacement de primitives

Menace Quantique sur les Protocoles

handshake

Diffie-Hellman
+
Signatures

Remplacement de primitives

handshake PQ

KEM PQ
+
Signatures PQ

Menace Quantique sur les Protocoles

handshake

Diffie-Hellman
+
Signatures

Remplacement de primitives

handshake PQ

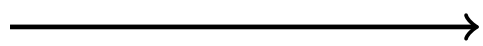
KEM PQ
+
Signatures PQ

The End !

Menace Quantique sur les Protocoles

handshake

Diffie-Hellman
+
Signatures



Remplacement de primitives

handshake PQ

KEM PQ
+
Signatures PQ

The End !

Pas vraiment ...

Impact de la Transition Post-Quantique des Protocoles

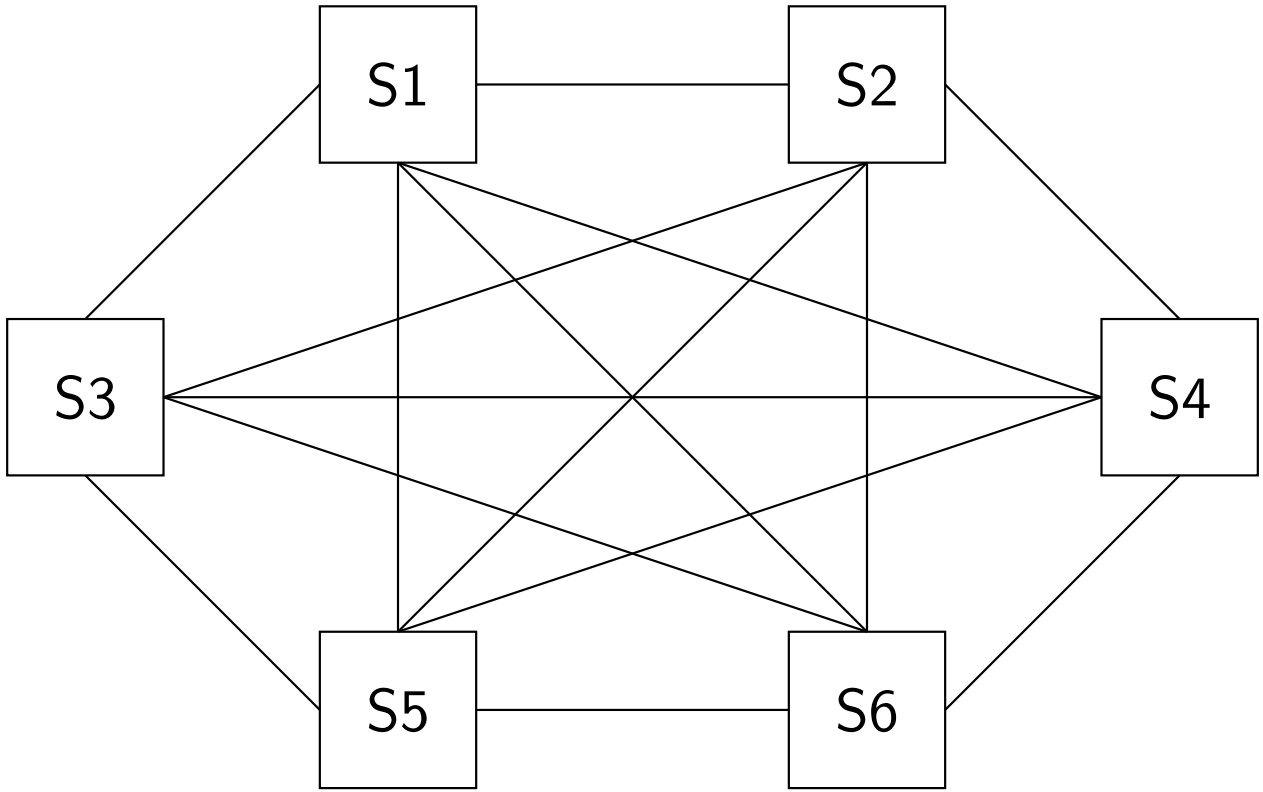
1. Transition progressive

Impact de la Transition Post-Quantique des Protocoles

1. Transition progressive
   - Synchronization des sytèmes
   - Rétro compatibilité

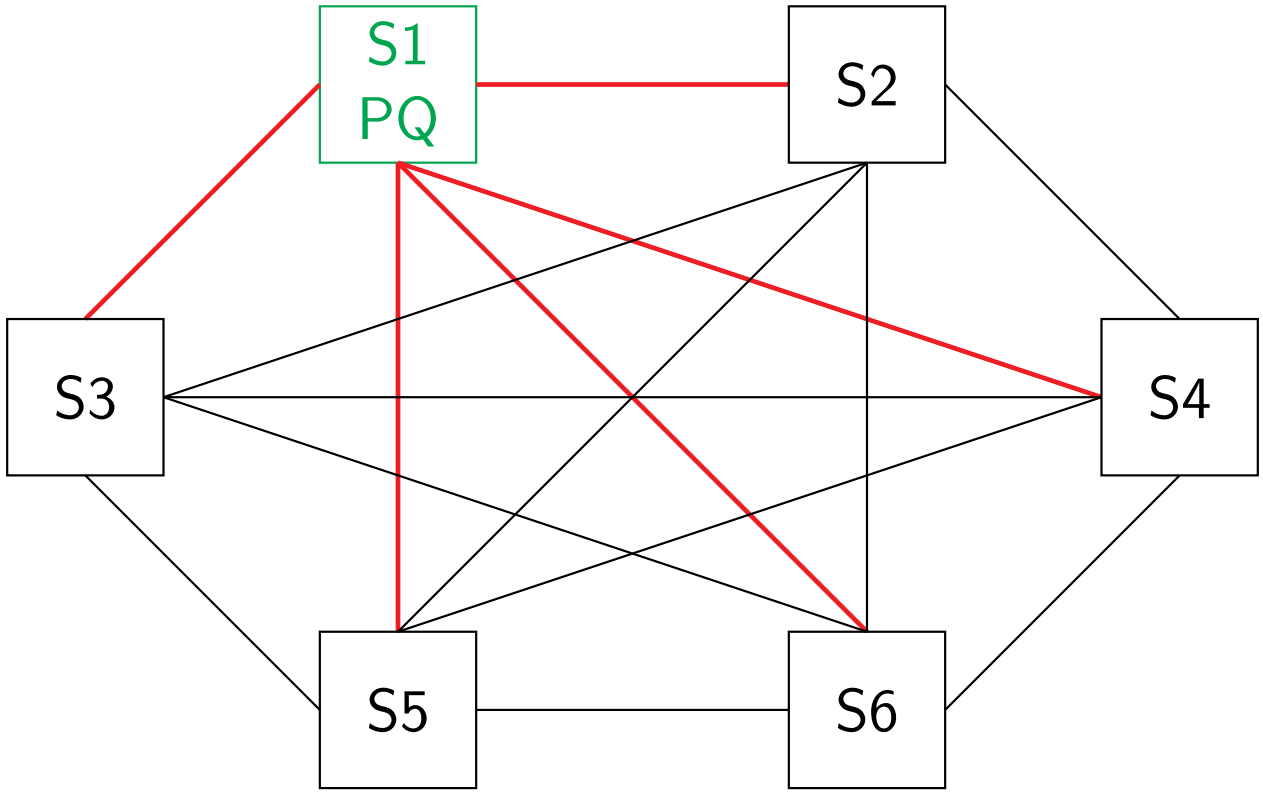
Impact de la Transition Post-Quantique des Protocoles

1. Transition progressive
   - Synchronization des sytèmes
   - Rétro compatibilité



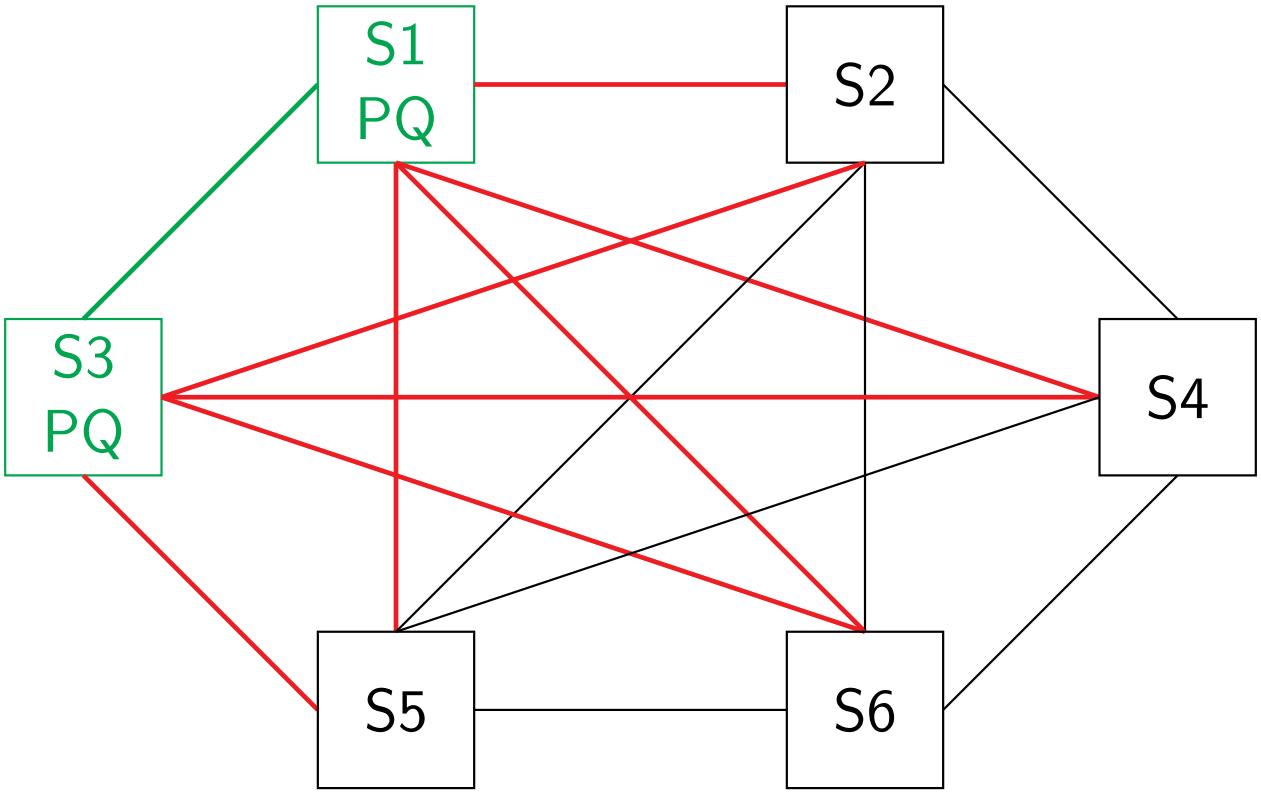
Impact de la Transition Post-Quantique des Protocoles

1. Transition progressive
   - Synchronization des sytèmes
   - Rétro compatibilité



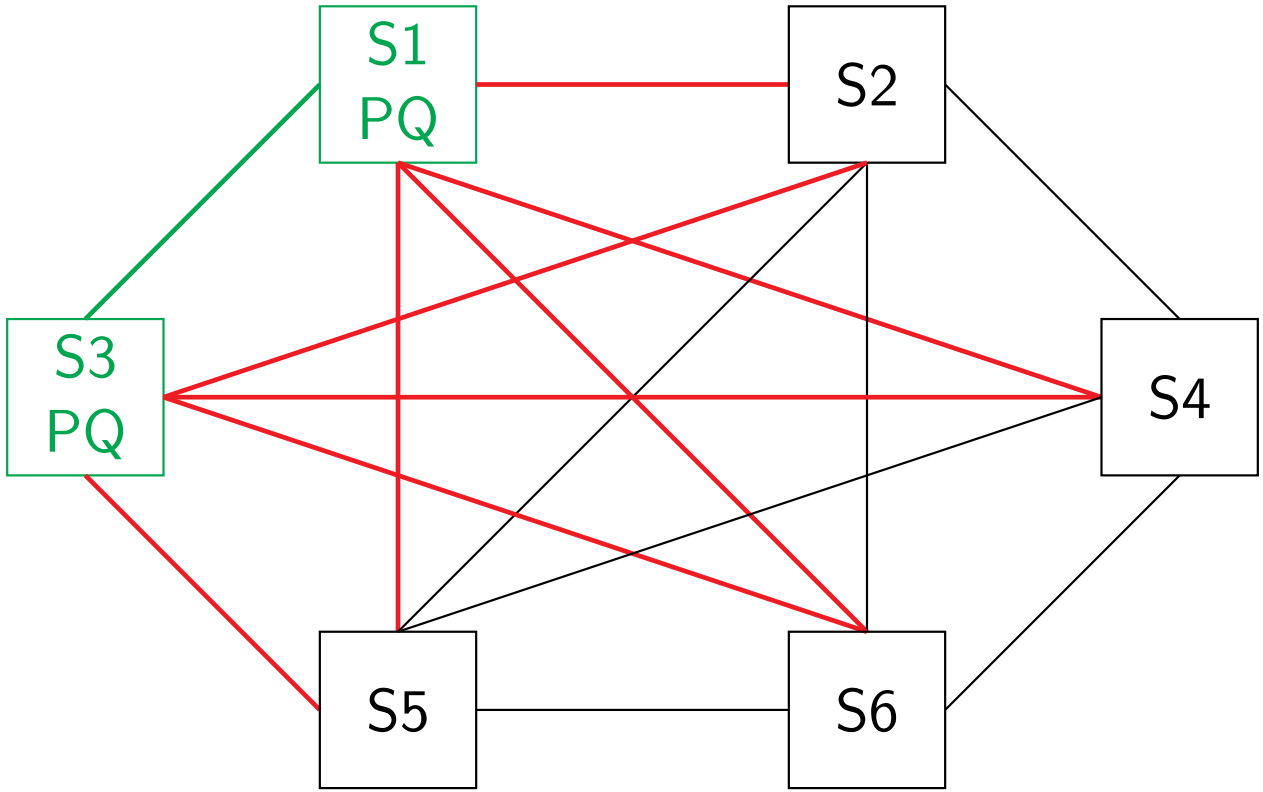
Impact de la Transition Post-Quantique des Protocoles

1. Transition progressive
   - Synchronization des sytèmes
   - Rétro compatibilité



Impact de la Transition Post-Quantique des Protocoles

1. Transition progressive
   - Synchronization des sytèmes
   - Rétro compatibilité



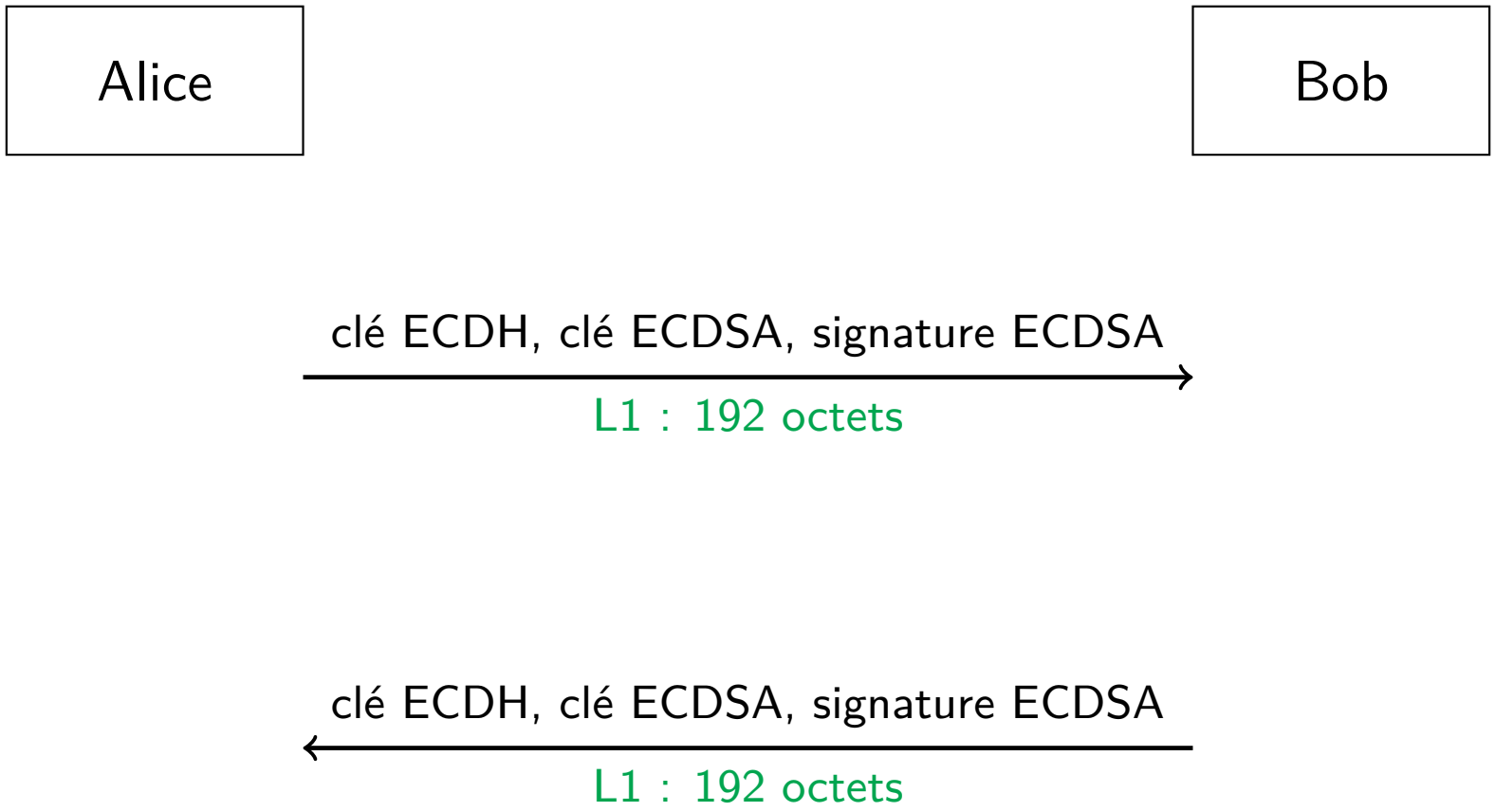
Besoin d'une stratégie de transition !

Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ

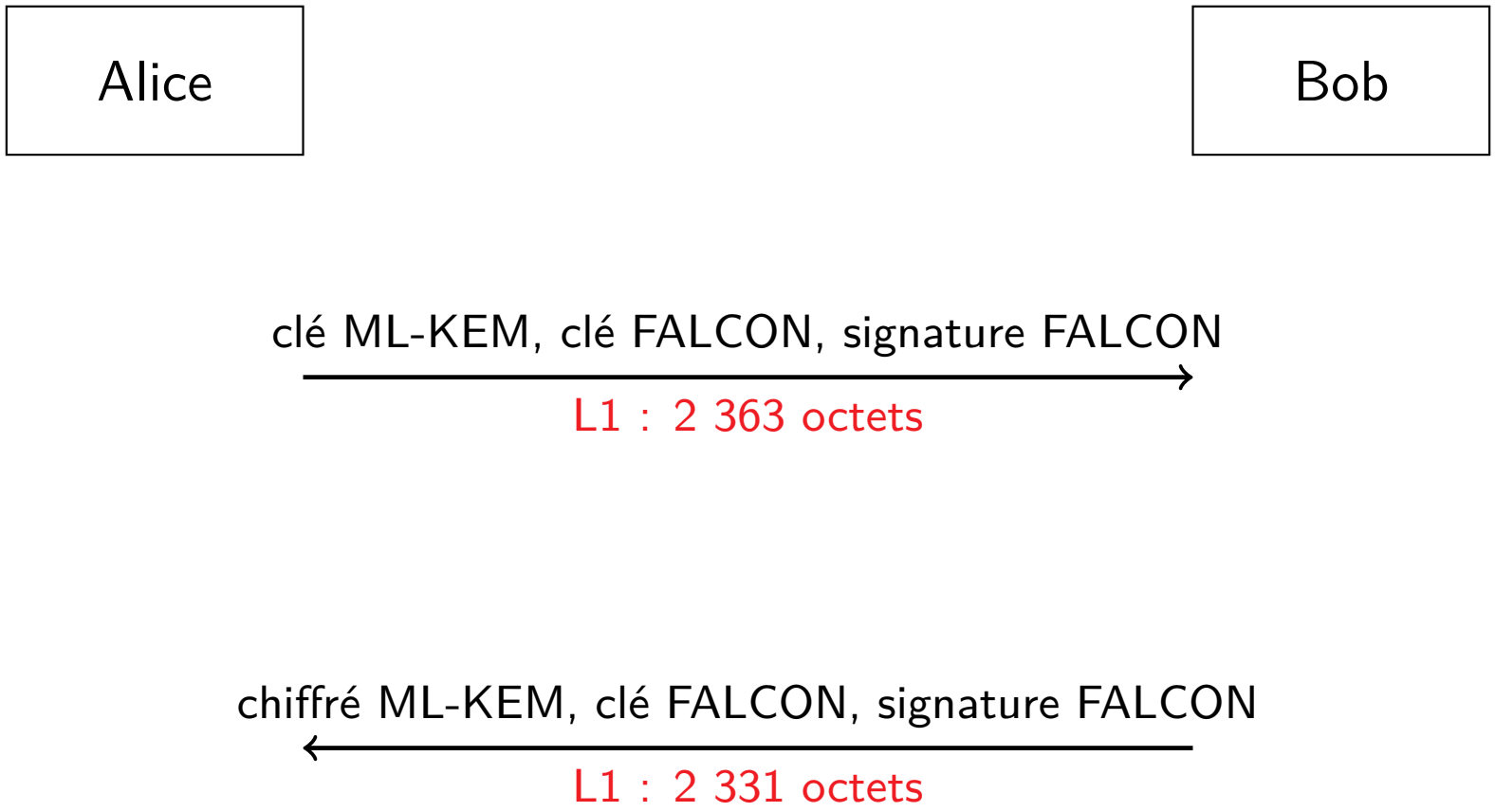
Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ



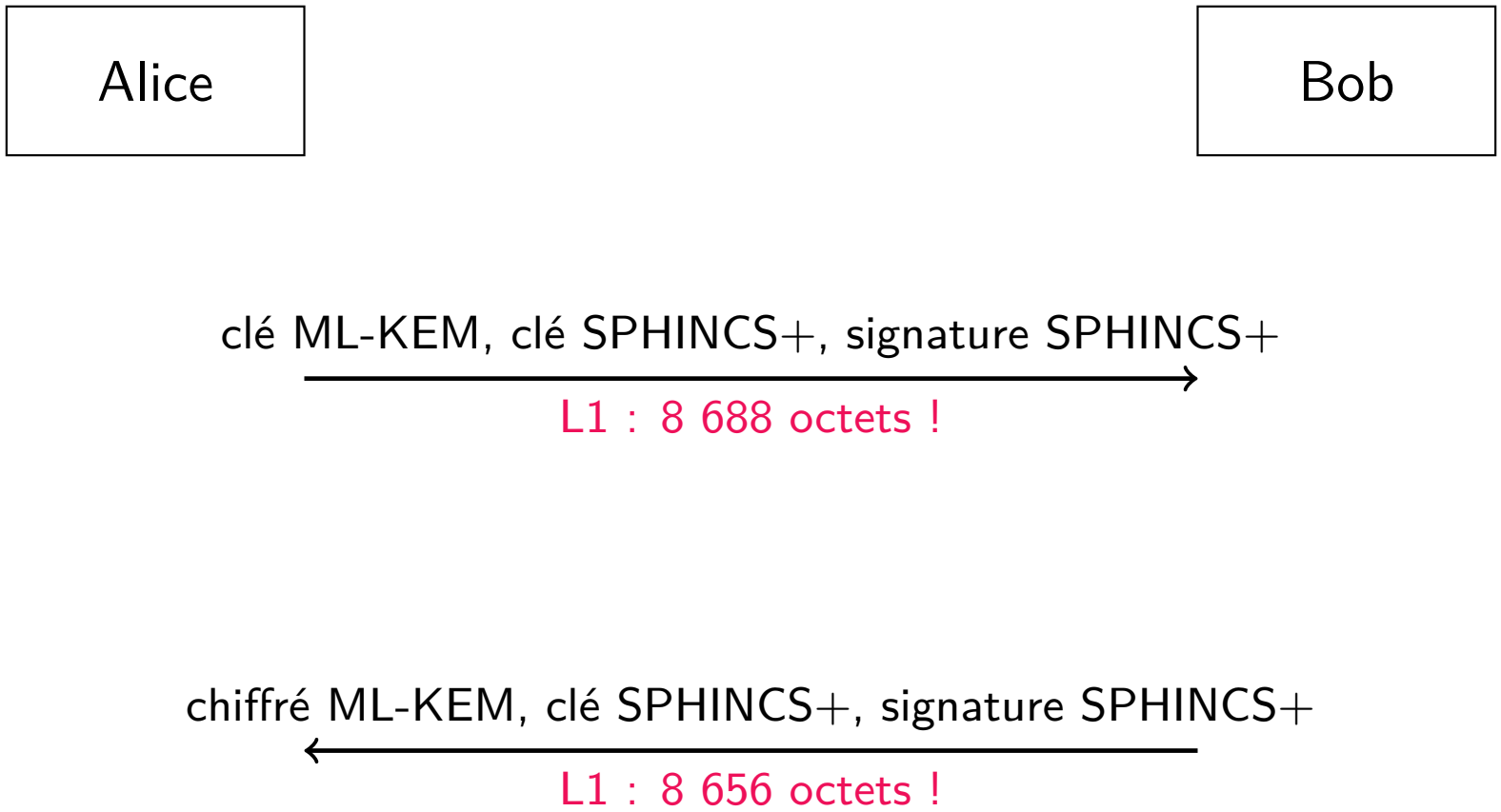
Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ



Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ



Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ

Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Toutes les primitives PQ ne sont pas adaptées à tous les scénarios

Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Toutes les primitives PQ ne sont pas adaptées à tous les scénarios
   - Systèmes embarqués

Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Toutes les primitives PQ ne sont pas adaptées à tous les scénarios
   - Systèmes embarqués
   - Latence réseau

Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Toutes les primitives PQ ne sont pas adaptées à tous les scénarios
   - Systèmes embarqués
   - Latence réseau
   - Surcharge des serveurs

Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Toutes les primitives PQ ne sont pas adaptées à tous les scénarios
   - Systèmes embarqués
   - Latence réseau
   - Surcharge des serveurs
   - Allocation de plus de ressources

Impact de la Transition Post-Quantique des Protocoles

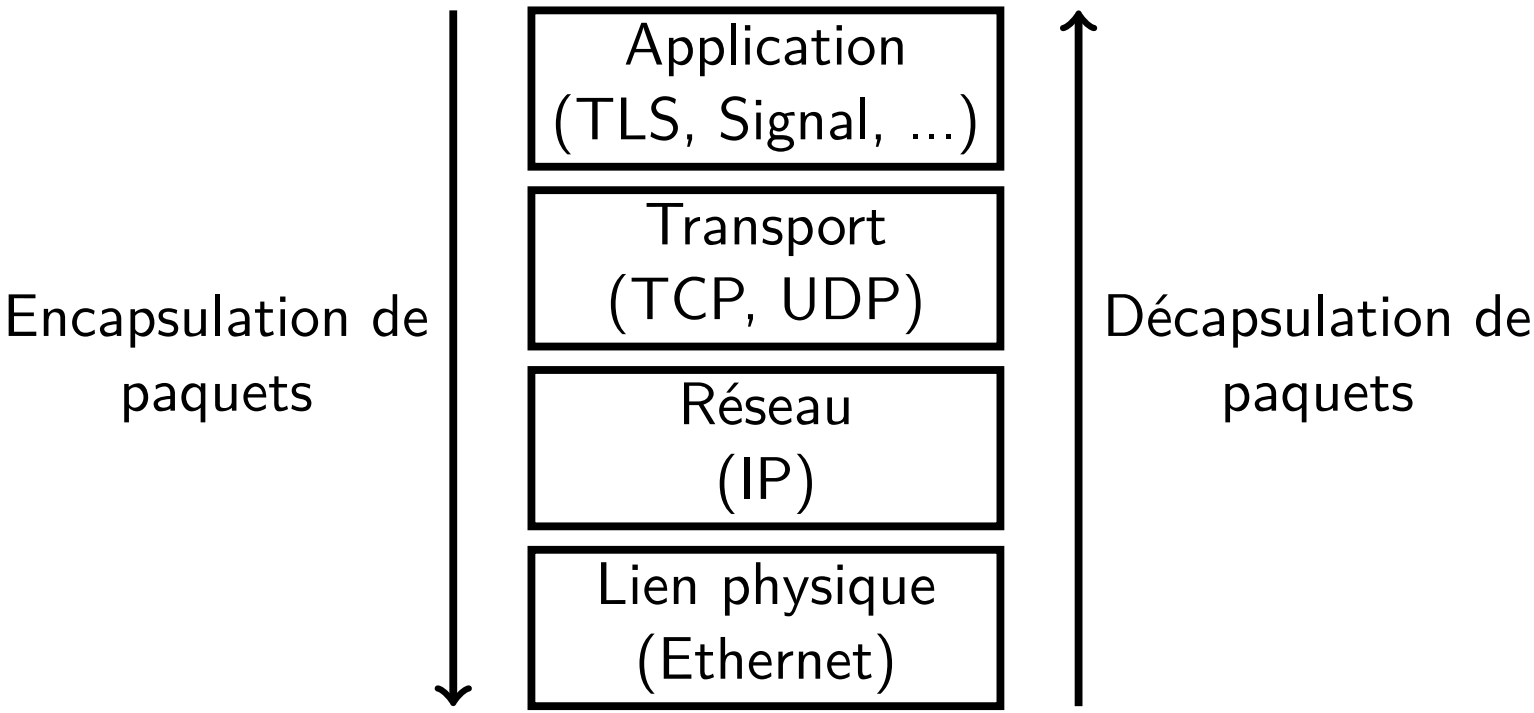
2. Taille importante des données PQ

Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Fragmentation

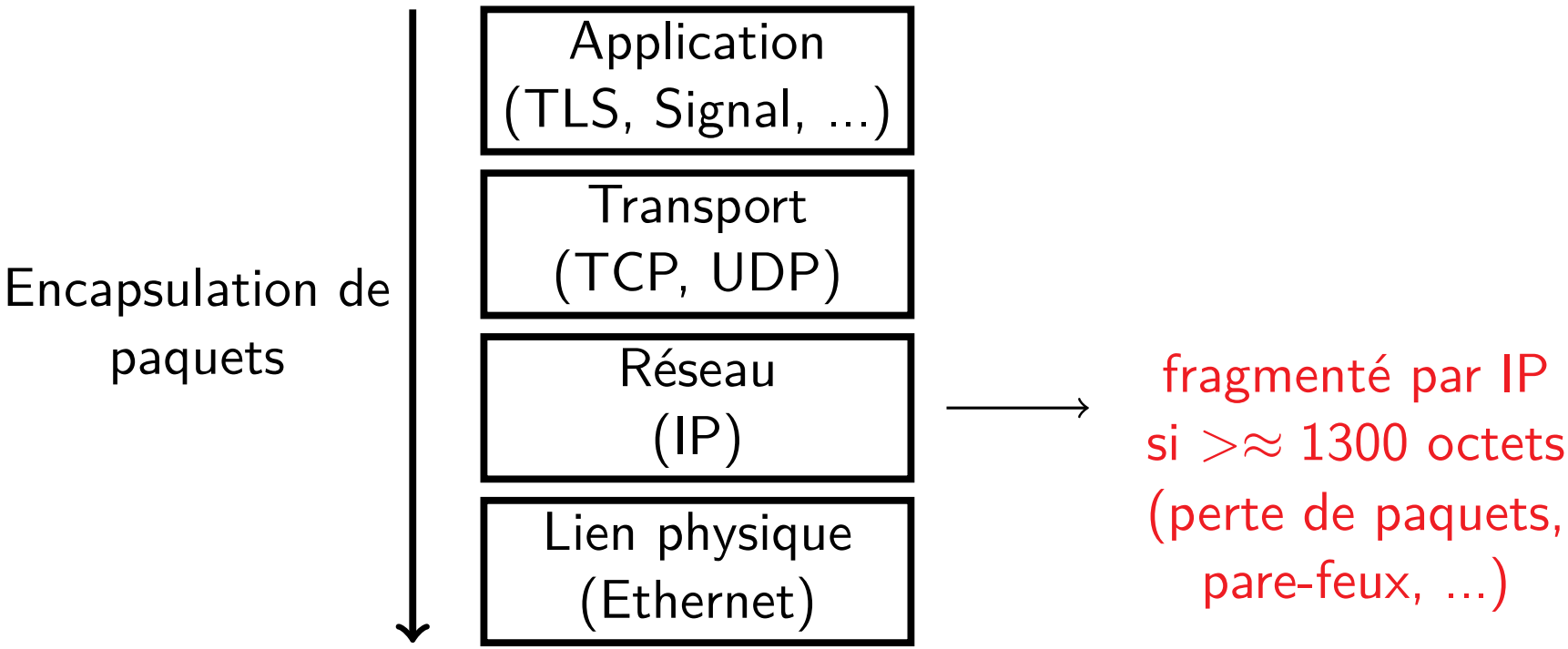
Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Fragmentation



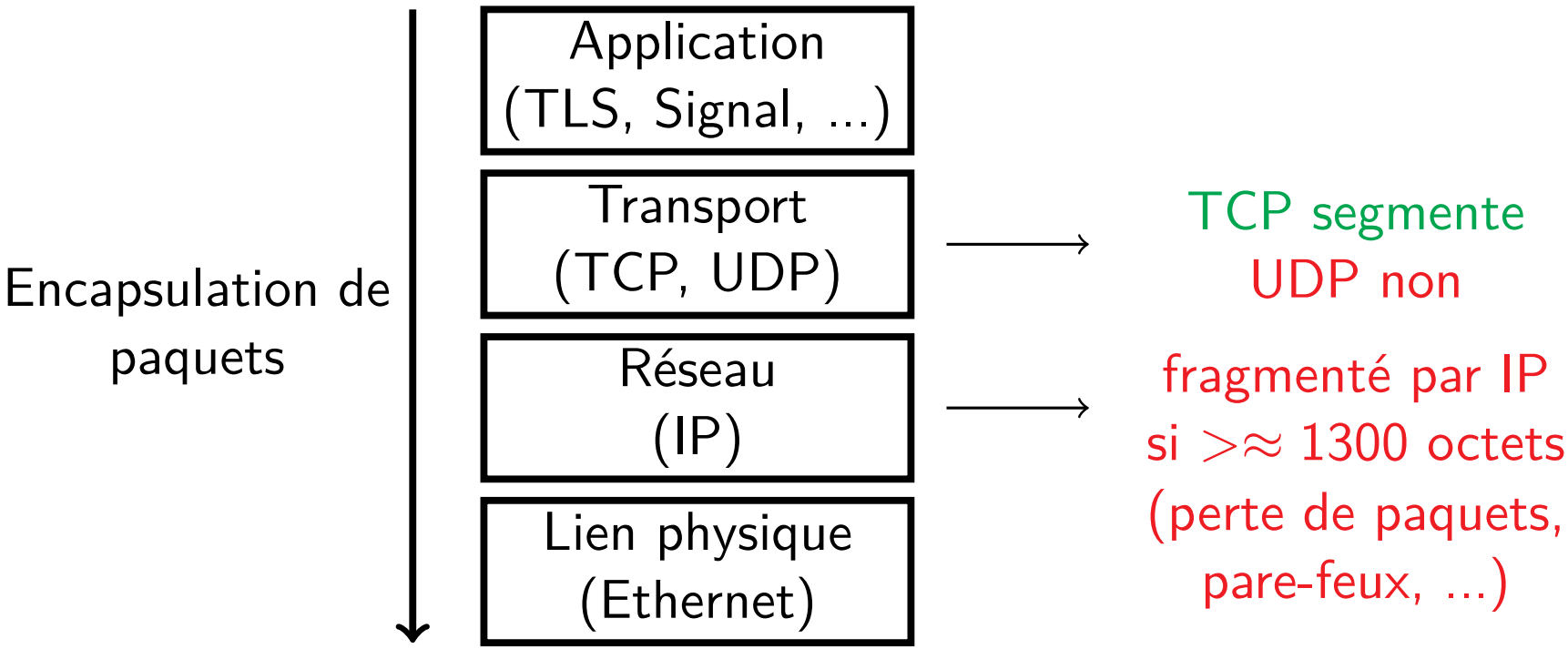
Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Fragmentation



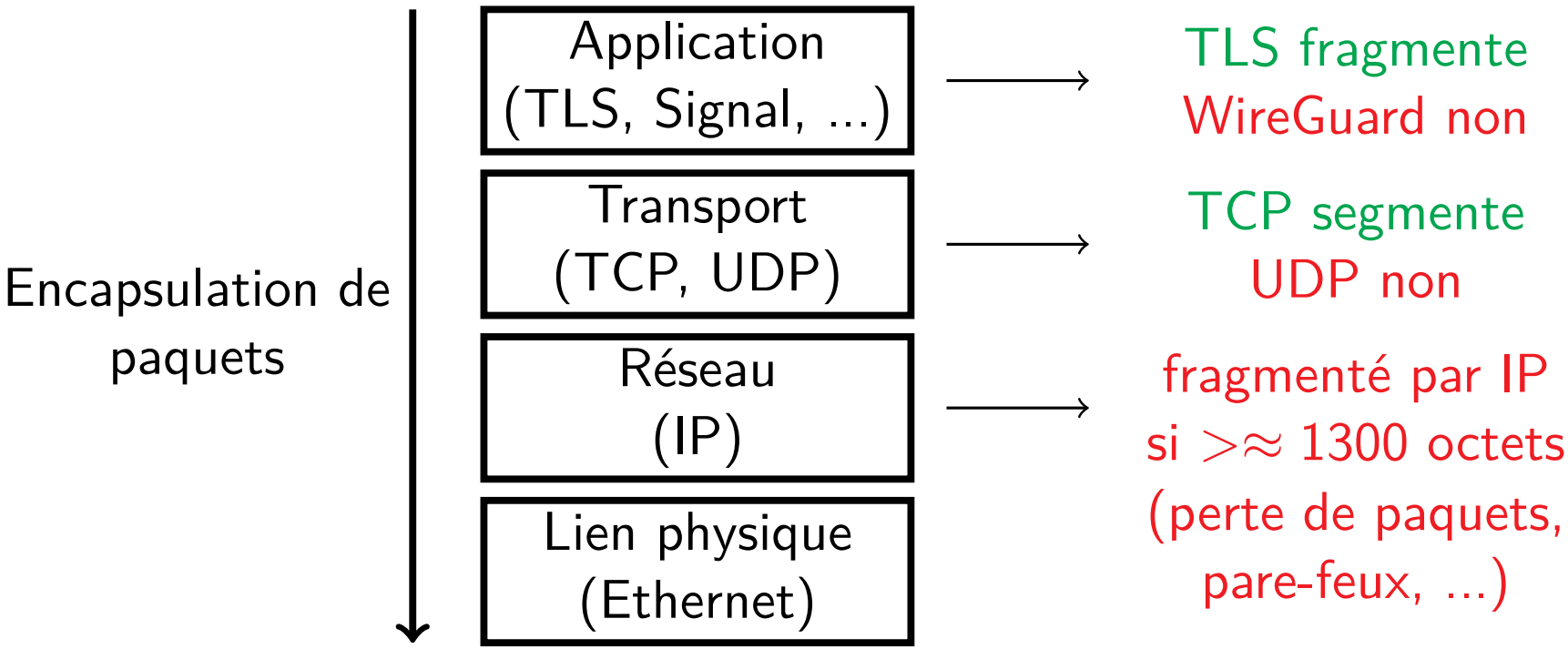
Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Fragmentation



Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Fragmentation



Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Fragmentation

Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Fragmentation
     - Protocoles qui ne gèrent pas nativement la fragmentation / fonctionnent sur UDP pour gagner en performance

Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Fragmentation
     - Protocoles qui ne gèrent pas nativement la fragmentation / fonctionnent sur UDP pour gagner en performance
     - Intégration de la cryptographie post-quantique $\rightarrow$ fragmentation inévitable

Impact de la Transition Post-Quantique des Protocoles

2. Taille importante des données PQ
   - Fragmentation
     - Protocoles qui ne gèrent pas nativement la fragmentation / fonctionnent sur UDP pour gagner en performance
     - Intégration de la cryptographie post-quantique $\rightarrow$ fragmentation inévitable
     - Modification potentielle de la structure du protocole !

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Cryptanalyse

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Cryptanalyse
   - Implémentation

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Cryptanalyse
   - Implémentation

Mais,

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Cryptanalyse
   - Implémentation

Mais,

   - Déploiement nécessaire dès aujourd'hui

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Cryptanalyse
   - Implémentation

Mais,

- Déploiement nécessaire dès aujourd'hui
- surtout pour les échanges de clés

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Cryptanalyse
   - Implémentation

Mais,

- Déploiement nécessaire dès aujourd'hui
- surtout pour les échanges de clés

Application classique

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Cryptanalyse
   - Implémentation

Mais,

- Déploiement nécessaire dès aujourd'hui
- surtout pour les échanges de clés

$$\text{Application classique} \xrightarrow{1\text{ an}} \text{Application post-quantique}$$

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Cryptanalyse
   - Implémentation

Mais,

- Déploiement nécessaire dès aujourd'hui
- surtout pour les échanges de clés

Application classique $\xrightarrow{1\text{ an}}$ Application post-quantique $\xrightarrow{6\text{ mois}}$ Schéma post-quantique cassé par un ordinateur classique

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - 2 recommandations :

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - 2 recommandations :
     - Agilité des implémentations

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - 2 recommandations :
     - Agilité des implémentations
       - Remplacer une primitive cassée par une autre **rapidement**

Impact de la Transition Post-Quantique des Protocoles

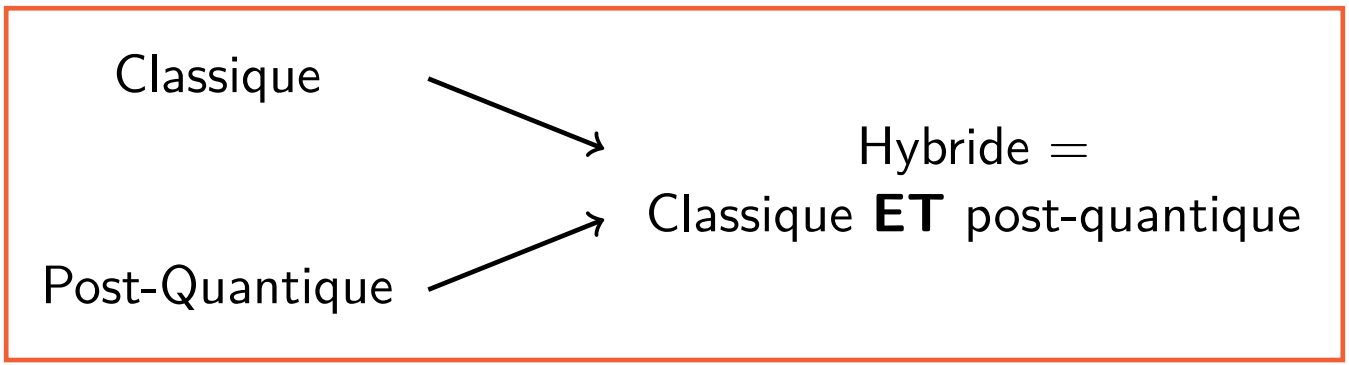
3. Maturité insuffisante des schémas post-quantiques
   - 2 recommandations :
     - Agilité des implémentations
       - Remplacer une primitive cassée par une autre **rapidement**
       - Pas toujours facile

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - 2 recommandations :
     - Agilité des implémentations
       - Remplacer une primitive cassée par une autre **rapidement**
       - Pas toujours facile
     - Hybridation

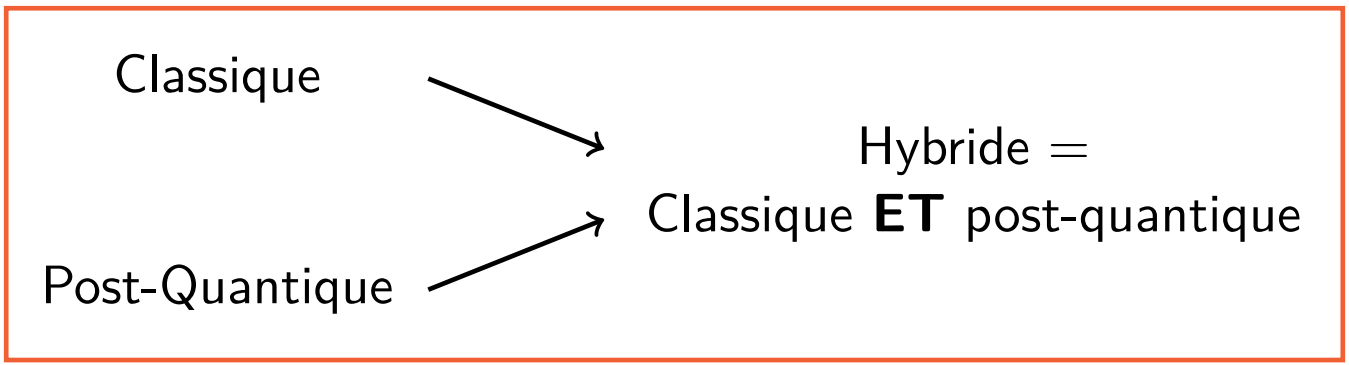
Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - 2 recommandations :
     - Agilité des implémentations
       - Remplacer une primitive cassée par une autre **rapidement**
       - Pas toujours facile
     - Hybridation



Impact de la Transition Post-Quantique des Protocoles

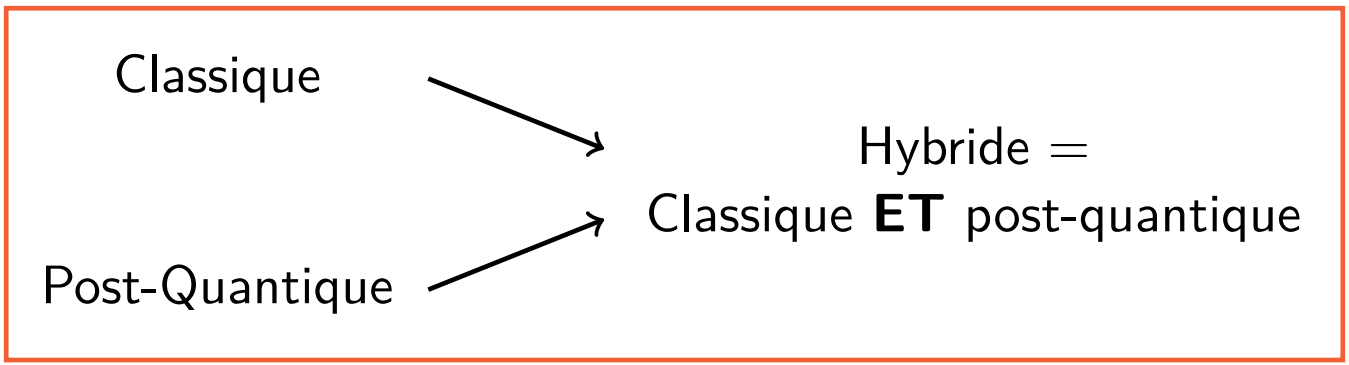
3. Maturité insuffisante des schémas post-quantiques
   - 2 recommandations :
     - Agilité des implémentations
       - Remplacer une primitive cassée par une autre **rapidement**
       - Pas toujours facile
     - Hybridation



Sécurité assurée si AU MOINS une des primitives n'est pas cassée

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - 2 recommandations :
     - Agilité des implémentations
       - Remplacer une primitive cassée par une autre **rapidement**
       - Pas toujours facile
     - Hybridation



Sécurité assurée si AU MOINS une des primitives n'est pas cassée

Recommandée par ANSSI, BSI (Allemagne), AIVD (Pays-bas), ENISA (Europe), CFDIR (Canada)

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Exemples d'hybridation

Impact de la Transition Post-Quantique des Protocoles

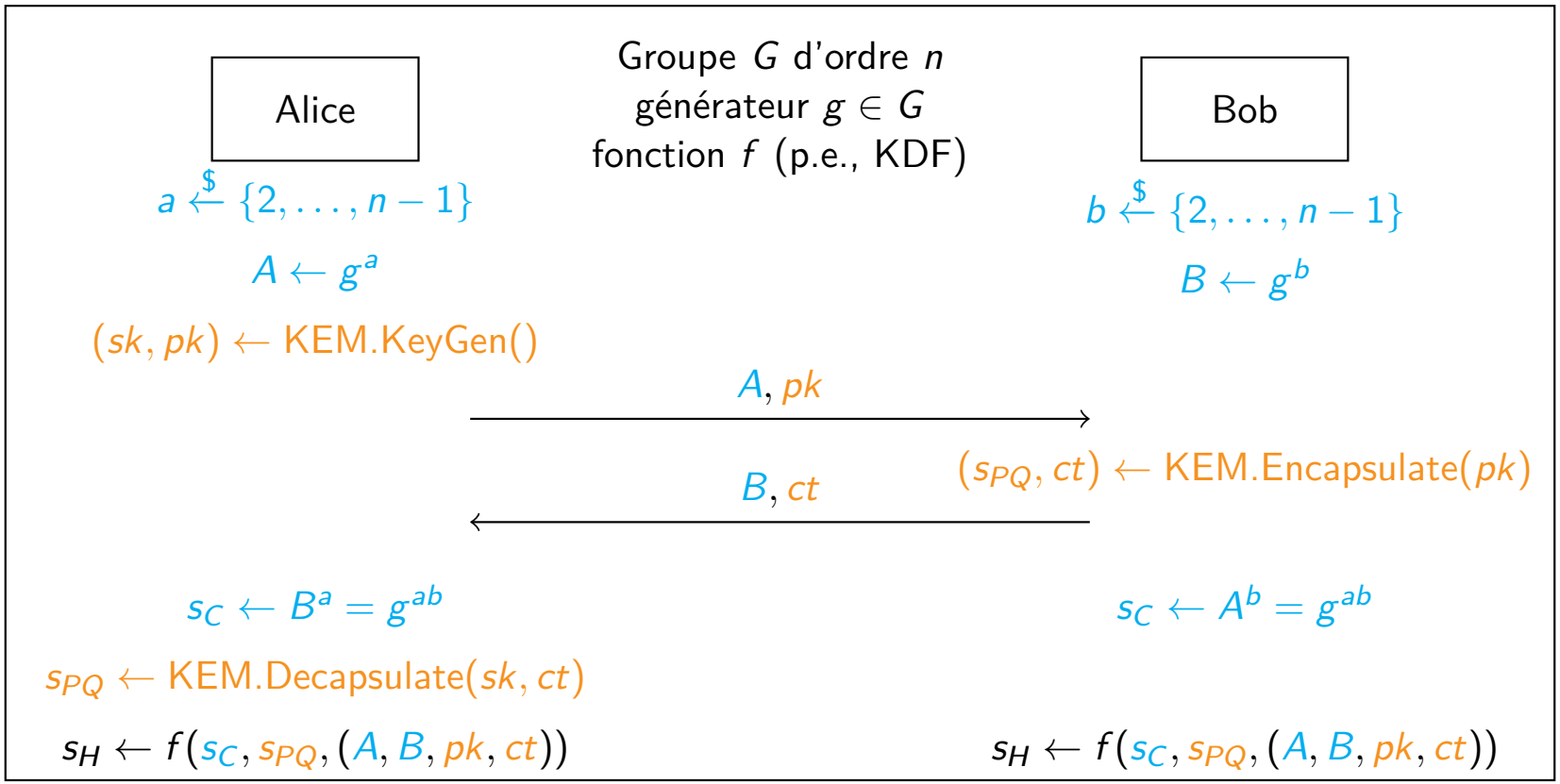
3. Maturité insuffisante des schémas post-quantiques
   - Exemples d'hybridation
     - signatures : concaténation

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Exemples d'hybridation
     - signatures : concaténation
     - échanges de clés :

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Exemples d'hybridation
     - signatures : concaténation
     - échanges de clés :



Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Tous les travaux existants font de l'hybridation

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Tous les travaux existants font de l'hybridation
     - Pas que pour des raisons de sécurité

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Tous les travaux existants font de l'hybridation
     - Pas que pour des raisons de sécurité
     - Aussi pour des raisons pratiques

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Tous les travaux existants font de l'hybridation
     - Pas que pour des raisons de sécurité
     - Aussi pour des raisons pratiques
       - Transition progressive

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Tous les travaux existants font de l'hybridation
     - Pas que pour des raisons de sécurité
     - Aussi pour des raisons pratiques
       - Transition progressive
       - Utilisation d'extensions pour les échanges post-quantiques

Impact de la Transition Post-Quantique des Protocoles

3. Maturité insuffisante des schémas post-quantiques
   - Tous les travaux existants font de l'hybridation
     - Pas que pour des raisons de sécurité
     - Aussi pour des raisons pratiques
       - Transition progressive
       - Utilisation d'extensions pour les échanges post-quantiques
       - Rétro compatibilité

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats
   - Gestion de certificats (beaucoup) plus grands

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats
   - Gestion de certificats (beaucoup) plus grands
     - Pire avec les chaines de certifications

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats
   - Gestion de certificats (beaucoup) plus grands
     - Pire avec les chaines de certifications
   - Certificats hybrides

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats
   - Gestion de certificats (beaucoup) plus grands
     - Pire avec les chaines de certifications
   - Certificats hybrides
     - Comment gérer les autorités de certifications ?

Impact de la Transition Post-Quantique des Protocoles

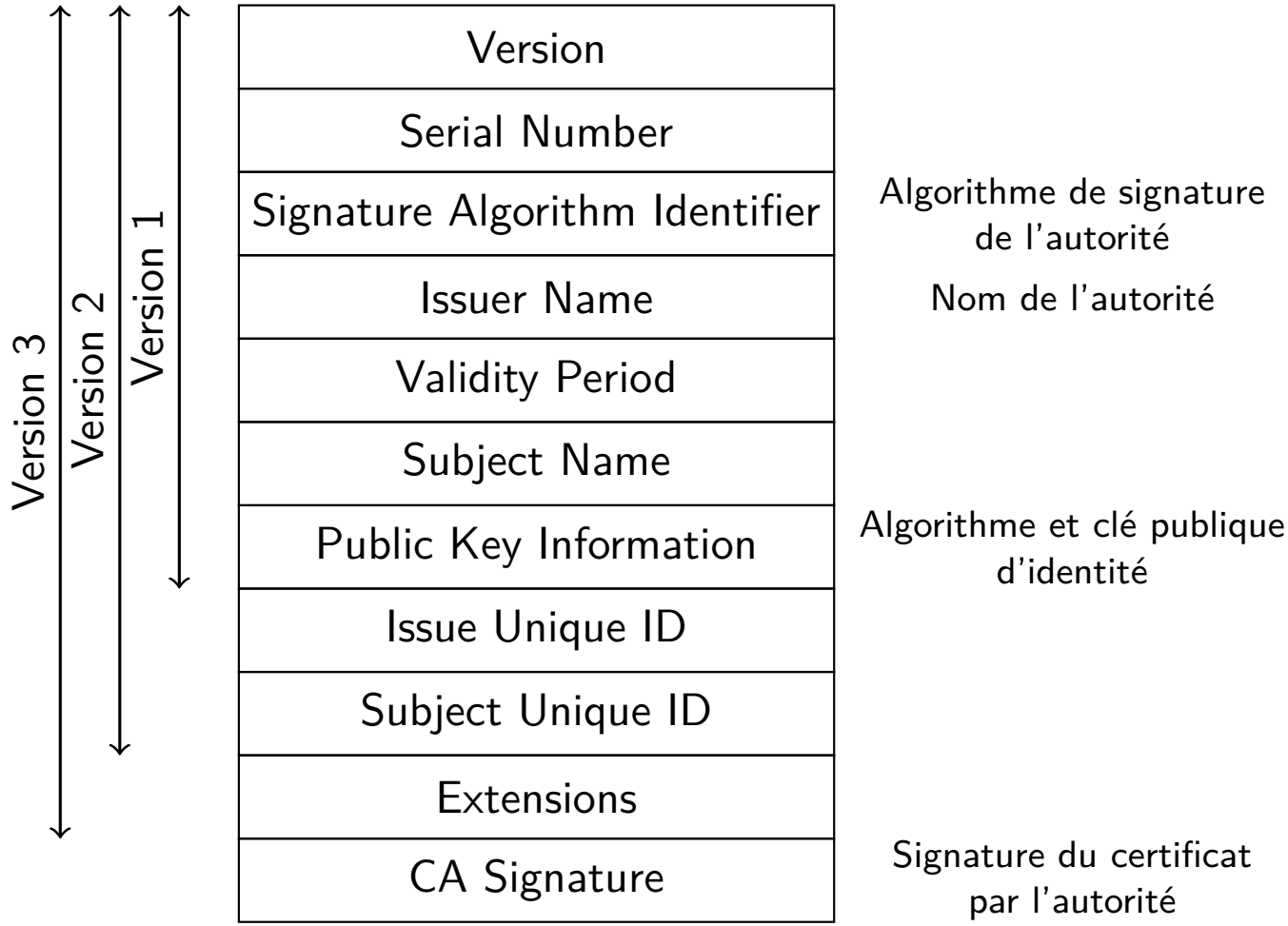
4. Modification des PKI + certificats
   - Gestion de certificats (beaucoup) plus grands
     - Pire avec les chaines de certifications
   - Certificats hybrides
     - Comment gérer les autorités de certifications ?
     - Quel format choisir ?

Impact de la Transition Post-Quantique des Protocoles

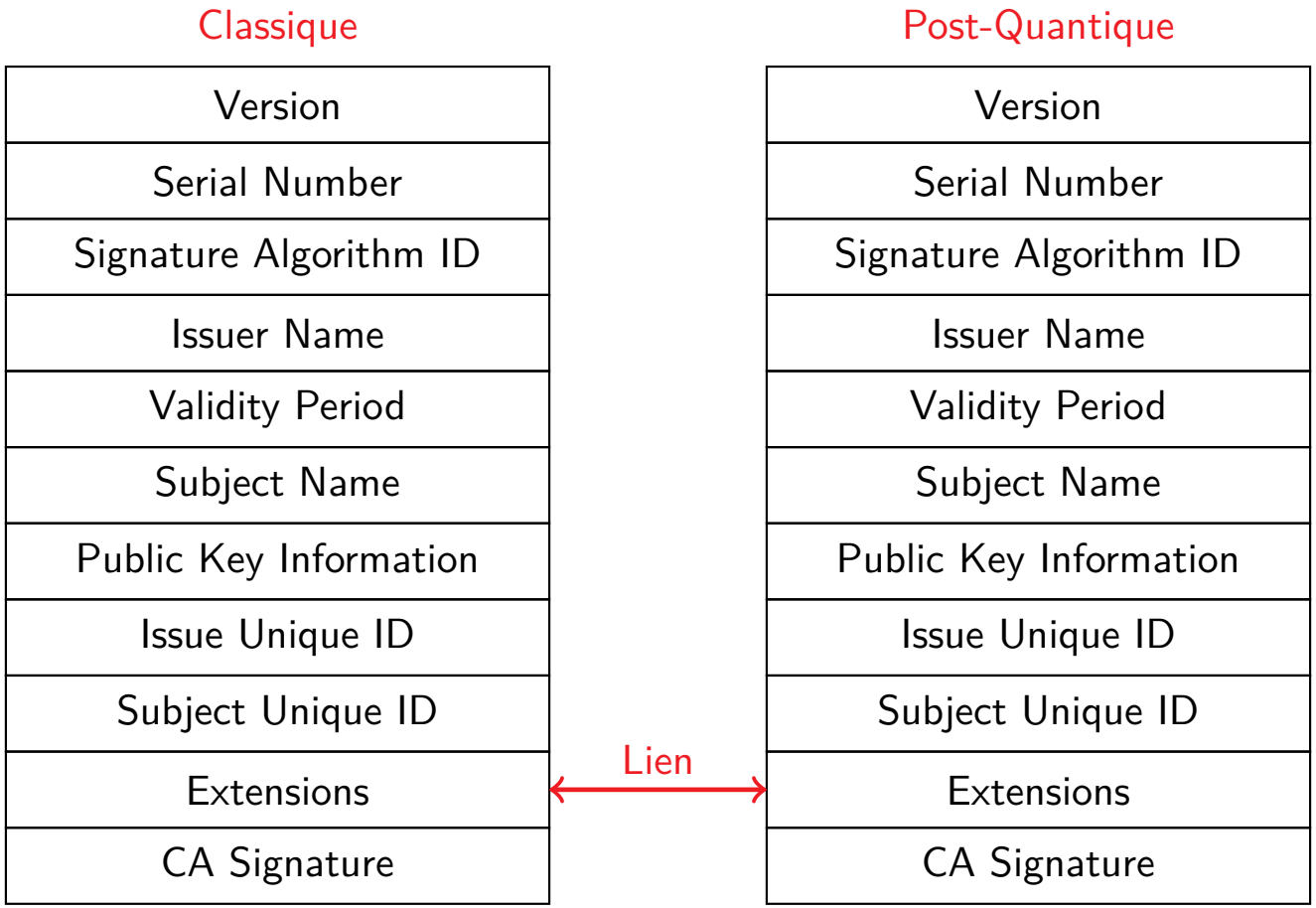
4. Modification des PKI + certificats

Impact de la Transition Post-Quantique des Protocoles

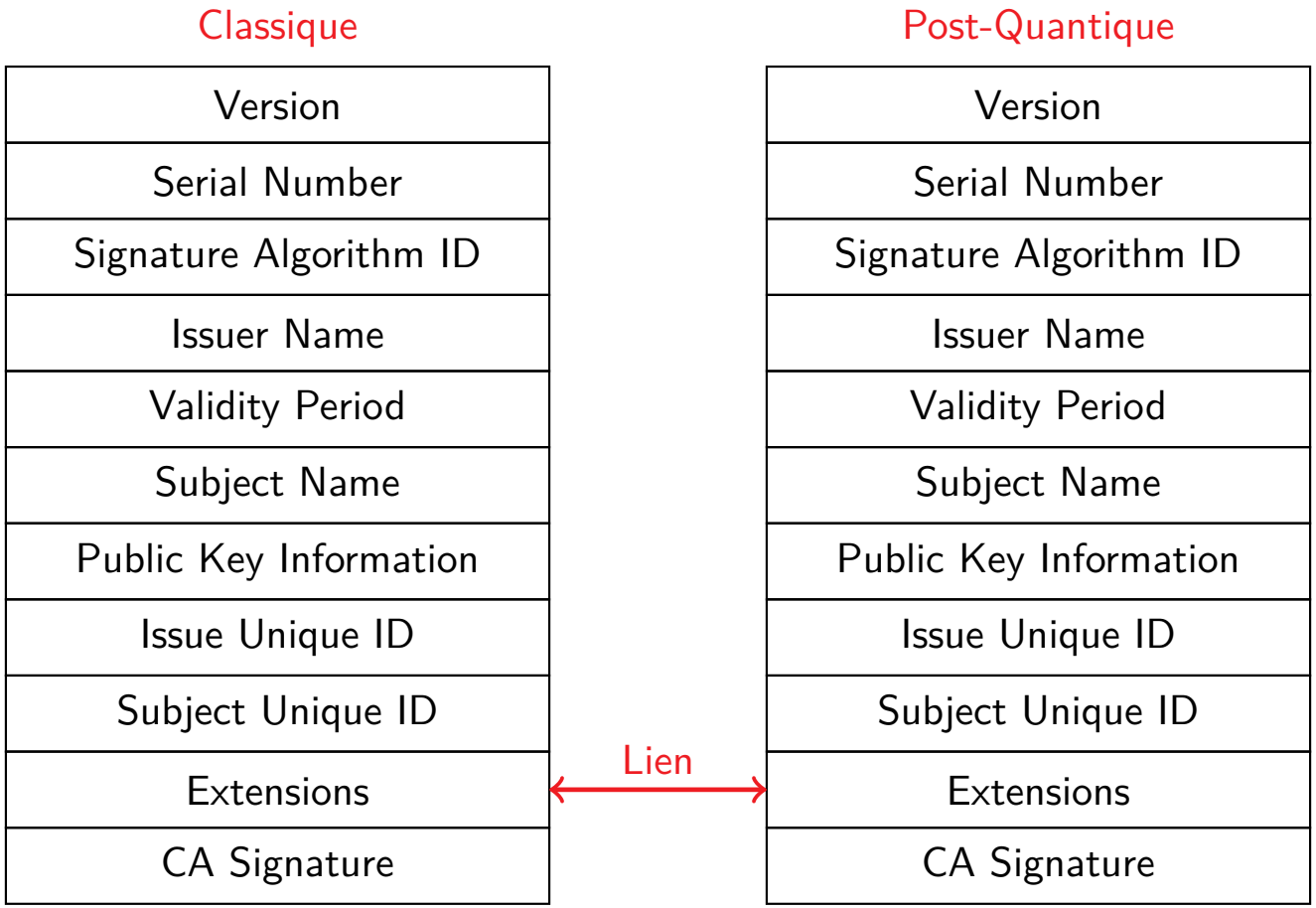
4. Modification des PKI + certificats



Impact de la Transition Post-Quantique des Protocoles

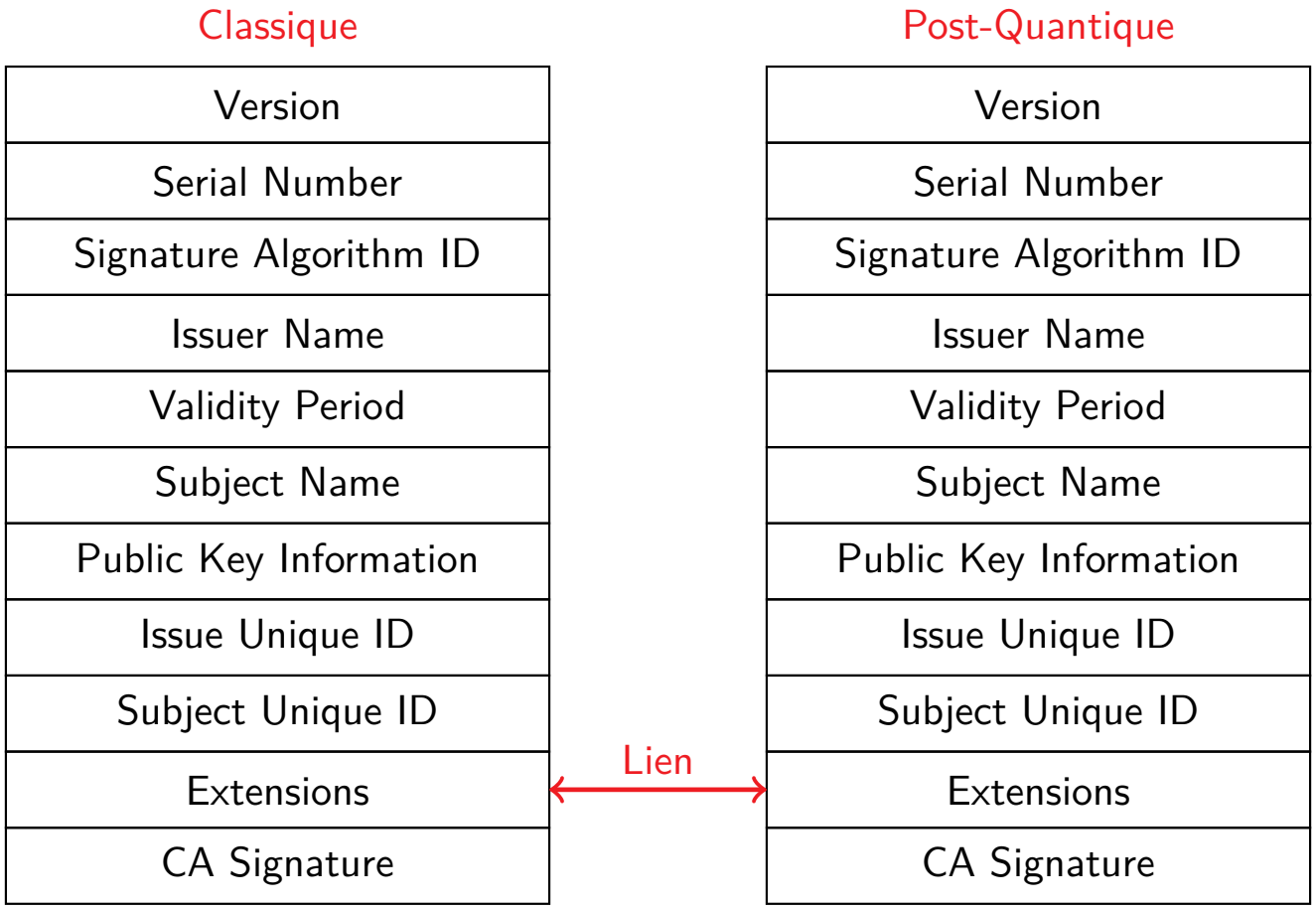


Impact de la Transition Post-Quantique des Protocoles



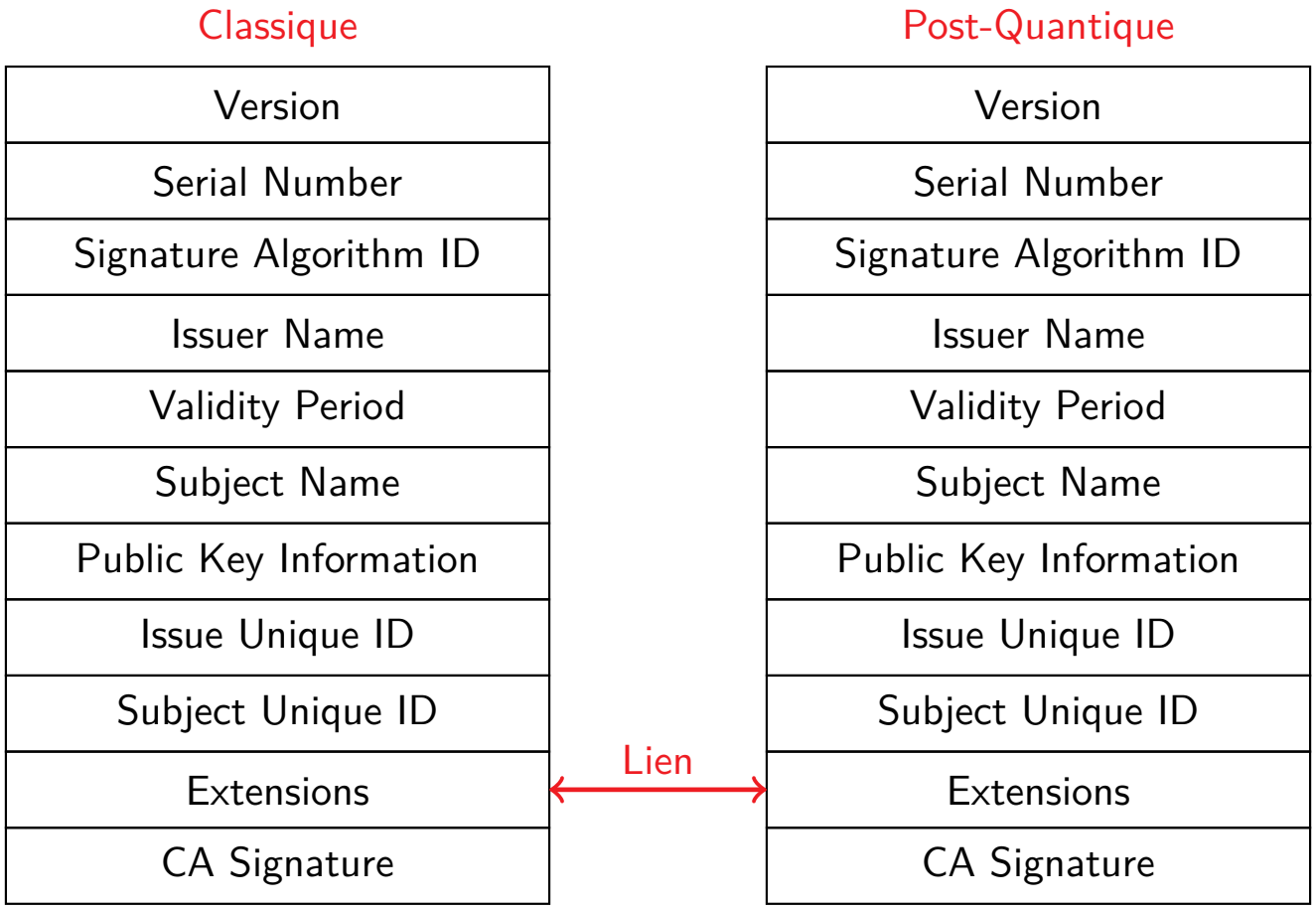
- Facile à implémenter

Impact de la Transition Post-Quantique des Protocoles



- Facile à implémenter
- Rétro compatible

Impact de la Transition Post-Quantique des Protocoles



- Facile à implémenter
- Rétro compatible
- Certificats séparables : point d'attention dans les implémentations

Impact de la Transition Post-Quantique des Protocoles

Version	
Serial Number	
Signature Algorithm Identifier	Identifiant de l'algorithme hybride
Issuer Name	
Validity Period	
Subject Name	
Public Key Information	$pk^C \mid\mid pk^{PQ}$
Issue Unique ID	
Subject Unique ID	
Extensions	
CA Signature	$\text{signature}^C \mid\mid \text{signature}^{PQ}$

Impact de la Transition Post-Quantique des Protocoles

Version	
Serial Number	
Signature Algorithm Identifier	Identifiant de l'algorithme hybride
Issuer Name	
Validity Period	
Subject Name	
Public Key Information	$pk^C \mid\mid pk^{PQ}$
Issue Unique ID	
Subject Unique ID	
Extensions	
CA Signature	$\text{signature}^C \mid\mid \text{signature}^{PQ}$

- Certificats non-séparables

Impact de la Transition Post-Quantique des Protocoles

Version	
Serial Number	
Signature Algorithm Identifier	Identifiant de l'algorithme hybride
Issuer Name	
Validity Period	
Subject Name	
Public Key Information	$pk^C \mid\mid pk^{PQ}$
Issue Unique ID	
Subject Unique ID	
Extensions	
CA Signature	$\text{signature}^C \mid\mid \text{signature}^{PQ}$

- Certificats non-séparables
- Nécessite une ré-implémentation des certificats

Impact de la Transition Post-Quantique des Protocoles

Version	
Serial Number	
Signature Algorithm Identifier	Identifiant de l'algorithme hybride
Issuer Name	
Validity Period	
Subject Name	
Public Key Information	$pk^C \mid\mid pk^{PQ}$
Issue Unique ID	
Subject Unique ID	
Extensions	
CA Signature	$\text{signature}^C \mid\mid \text{signature}^{PQ}$

- Certificats non-séparables
- Nécessite une ré-implémentation des certificats
- Non rétro compatible

Impact de la Transition Post-Quantique des Protocoles

Version
Serial Number
Signature Algorithm Identifier
Issuer Name
Validity Period
Subject Name
Public Key Information
Issue Unique ID
Subject Unique ID
Extensions
CA Signature

Identifiant de l'algorithme pq

pk^{PQ}

signature^{PQ}

Impact de la Transition Post-Quantique des Protocoles

Version
Serial Number
Signature Algorithm Identifier
Issuer Name
Validity Period
Subject Name
Public Key Information
Issue Unique ID
Subject Unique ID
Extensions
CA Signature

Identifiant de l'algorithme pq
pk^{PQ}
signature^{PQ}

- Facile à implémenter

Impact de la Transition Post-Quantique des Protocoles

Version
Serial Number
Signature Algorithm Identifier
Issuer Name
Validity Period
Subject Name
Public Key Information
Issue Unique ID
Subject Unique ID
Extensions
CA Signature

Identifiant de l'algorithme pq
pk^{PQ}
signature^{PQ}

- Facile à implémenter
- Rétro compatible

Impact de la Transition Post-Quantique des Protocoles

Version
Serial Number
Signature Algorithm Identifier
Issuer Name
Validity Period
Subject Name
Public Key Information
Issue Unique ID
Subject Unique ID
Extensions
CA Signature

Identifiant de l'algorithme pq
pk^{PQ}
signature^{PQ}

- Facile à implémenter
- Rétro compatible
- Vérification des extensions : point d'attention

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats
   - Plusieurs solutions d'hybridation de certificats existent

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats
   - Plusieurs solutions d'hybridation de certificats existent
   - Compromis

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats
   - Plusieurs solutions d'hybridation de certificats existent
   - Compromis
     - Rétro compatibilité

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats
   - Plusieurs solutions d'hybridation de certificats existent
   - Compromis
     - Rétro compatibilité
     - Sécurité & Séparabilité

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats
   - Plusieurs solutions d'hybridation de certificats existent
   - Compromis
     - Rétro compatibilité
     - Sécurité & Séparabilité
     - PKI et gestion de clés

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats
   - Plusieurs solutions d'hybridation de certificats existent
   - Compromis
     - Rétro compatibilité
     - Sécurité & Séparabilité
     - PKI et gestion de clés
   - Pas de solution choisie aujourd'hui

Impact de la Transition Post-Quantique des Protocoles

4. Modification des PKI + certificats
   - Plusieurs solutions d'hybridation de certificats existent
   - Compromis
     - Rétro compatibilité
     - Sécurité & Séparabilité
     - PKI et gestion de clés
   - Pas de solution choisie aujourd'hui
   - Intégration de l'échange de clés plus urgent

Travaux Existants

SSH

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**
  - v8.9 : SSH avec échange de clés hybride (DH, NTRU Prime)

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**
  - v8.9 : SSH avec échange de clés hybride (DH, NTRU Prime)
  - v9.9 : SSH avec échange de clés hybride (DH, ML-KEM)

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**
  - v8.9 : SSH avec échange de clés hybride (DH, NTRU Prime)
  - v9.9 : SSH avec échange de clés hybride (DH, ML-KEM)

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**
  - v8.9 : SSH avec échange de clés hybride (DH, NTRU Prime)
  - v9.9 : SSH avec échange de clés hybride (DH, ML-KEM)

IPsec

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**
  - v8.9 : SSH avec échange de clés hybride (DH, NTRU Prime)
  - v9.9 : SSH avec échange de clés hybride (DH, ML-KEM)

IPsec

- RFC 9370 : Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**
  - v8.9 : SSH avec échange de clés hybride (DH, NTRU Prime)
  - v9.9 : SSH avec échange de clés hybride (DH, ML-KEM)

IPsec

- RFC 9370 : Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)
- Strongswan version 6.0.0 : échange de clés hybride (RFC 9370) avec ML-KEM

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**
  - v8.9 : SSH avec échange de clés hybride (DH, NTRU Prime)
  - v9.9 : SSH avec échange de clés hybride (DH, ML-KEM)

IPsec

- RFC 9370 : Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)
- Strongswan version 6.0.0 : échange de clés hybride (RFC 9370) avec ML-KEM
- RFC 8784 : Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**
  - v8.9 : SSH avec échange de clés hybride (DH, NTRU Prime)
  - v9.9 : SSH avec échange de clés hybride (DH, ML-KEM)

IPsec

- RFC 9370 : Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)
- Strongswan version 6.0.0 : échange de clés hybride (RFC 9370) avec ML-KEM
- RFC 8784 : Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**
  - v8.9 : SSH avec échange de clés hybride (DH, NTRU Prime)
  - v9.9 : SSH avec échange de clés hybride (DH, ML-KEM)

IPsec

- RFC 9370 : Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)
- Strongswan version 6.0.0 : échange de clés hybride (RFC 9370) avec ML-KEM
- RFC 8784 : Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

NordVPN

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**
  - v8.9 : SSH avec échange de clés hybride (DH, NTRU Prime)
  - v9.9 : SSH avec échange de clés hybride (DH, ML-KEM)

IPsec

- RFC 9370 : Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)
- Strongswan version 6.0.0 : échange de clés hybride (RFC 9370) avec ML-KEM
- RFC 8784 : Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

NordVPN

- NordLynx (WireGuard) + échange de clés ML-KEM

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**
  - v8.9 : SSH avec échange de clés hybride (DH, NTRU Prime)
  - v9.9 : SSH avec échange de clés hybride (DH, ML-KEM)

IPsec

- RFC 9370 : Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)
- Strongswan version 6.0.0 : échange de clés hybride (RFC 9370) avec ML-KEM
- RFC 8784 : Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

NordVPN

- NordLynx (WireGuard) + échange de clés ML-KEM

Certificats X.509

Travaux Existants

SSH

- Doc de l'IETF : SSH avec échange de clés hybride
- **OpenSSH**
  - v8.9 : SSH avec échange de clés hybride (DH, NTRU Prime)
  - v9.9 : SSH avec échange de clés hybride (DH, ML-KEM)

IPsec

- RFC 9370 : Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)
- Strongswan version 6.0.0 : échange de clés hybride (RFC 9370) avec ML-KEM
- RFC 8784 : Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security

NordVPN

- NordLynx (WireGuard) + échange de clés ML-KEM

Certificats X.509

- RFC 8773 : TLS 1.3 Extension for Certificate-Based Authentication with an External Pre-Shared Key

Travaux Existants

TLS

Travaux Existants

TLS

- Google Chrome : TLS avec échange de clés hybride avec ML-KEM (bureau uniquement)

Travaux Existants

TLS

- Google Chrome : TLS avec échange de clés hybride avec ML-KEM (bureau uniquement)
- Amazon : TLS avec échange de clés hybride dans certains services

Travaux Existants

TLS

- Google Chrome : TLS avec échange de clés hybride avec ML-KEM (bureau uniquement)
- Amazon : TLS avec échange de clés hybride dans certains services
- Meta : TLS avec échange de clés hybride pour services internes

Travaux Existants

TLS

- Google Chrome : TLS avec échange de clés hybride avec ML-KEM (bureau uniquement)
- Amazon : TLS avec échange de clés hybride dans certains services
- Meta : TLS avec échange de clés hybride pour services internes
- Pas de RFC, mais des drafts par l'IETF pour l'échange de clés hybride

Travaux Existants

TLS

- Google Chrome : TLS avec échange de clés hybride avec ML-KEM (bureau uniquement)
- Amazon : TLS avec échange de clés hybride dans certains services
- Meta : TLS avec échange de clés hybride pour services internes
- Pas de RFC, mais des drafts par l'IETF pour l'échange de clés hybride
- **OpenSSL** v3.5 : intégration de ML-KEM, ML-DSA, SLH-DSA

Travaux Existants

TLS

- Google Chrome : TLS avec échange de clés hybride avec ML-KEM (bureau uniquement)
- Amazon : TLS avec échange de clés hybride dans certains services
- Meta : TLS avec échange de clés hybride pour services internes
- Pas de RFC, mais des drafts par l'IETF pour l'échange de clés hybride
- **OpenSSL** v3.5 : intégration de ML-KEM, ML-DSA, SLH-DSA

Bibliothèques open-source

Travaux Existants

TLS

- Google Chrome : TLS avec échange de clés hybride avec ML-KEM (bureau uniquement)
- Amazon : TLS avec échange de clés hybride dans certains services
- Meta : TLS avec échange de clés hybride pour services internes
- Pas de RFC, mais des drafts par l'IETF pour l'échange de clés hybride
- **OpenSSL** v3.5 : intégration de ML-KEM, ML-DSA, SLH-DSA

Bibliothèques open-source

- liboqs : C, algo et certs X.509 PQ, KEM hybride pour TLS et SSH

Travaux Existants

TLS

- Google Chrome : TLS avec échange de clés hybride avec ML-KEM (bureau uniquement)
- Amazon : TLS avec échange de clés hybride dans certains services
- Meta : TLS avec échange de clés hybride pour services internes
- Pas de RFC, mais des drafts par l'IETF pour l'échange de clés hybride
- **OpenSSL** v3.5 : intégration de ML-KEM, ML-DSA, SLH-DSA

Bibliothèques open-source

- liboqs : C, algo et certs X.509 PQ, KEM hybride pour TLS et SSH
- CIRCL : Go, algo PQ

Travaux Existants

TLS

- Google Chrome : TLS avec échange de clés hybride avec ML-KEM (bureau uniquement)
- Amazon : TLS avec échange de clés hybride dans certains services
- Meta : TLS avec échange de clés hybride pour services internes
- Pas de RFC, mais des drafts par l'IETF pour l'échange de clés hybride
- **OpenSSL** v3.5 : intégration de ML-KEM, ML-DSA, SLH-DSA

Bibliothèques open-source

- liboqs : C, algo et certs X.509 PQ, KEM hybride pour TLS et SSH
- CIRCL : Go, algo PQ
- AWS libcrypto : C, algo PQ

Travaux Existants

TLS

- Google Chrome : TLS avec échange de clés hybride avec ML-KEM (bureau uniquement)
- Amazon : TLS avec échange de clés hybride dans certains services
- Meta : TLS avec échange de clés hybride pour services internes
- Pas de RFC, mais des drafts par l'IETF pour l'échange de clés hybride
- **OpenSSL** v3.5 : intégration de ML-KEM, ML-DSA, SLH-DSA

Bibliothèques open-source

- liboqs : C, algo et certs X.509 PQ, KEM hybride pour TLS et SSH
- CIRCL : Go, algo PQ
- AWS libcrypto : C, algo PQ

Autres

Travaux Existants

TLS

- Google Chrome : TLS avec échange de clés hybride avec ML-KEM (bureau uniquement)
- Amazon : TLS avec échange de clés hybride dans certains services
- Meta : TLS avec échange de clés hybride pour services internes
- Pas de RFC, mais des drafts par l'IETF pour l'échange de clés hybride
- **OpenSSL** v3.5 : intégration de ML-KEM, ML-DSA, SLH-DSA

Bibliothèques open-source

- liboqs : C, algo et certs X.509 PQ, KEM hybride pour TLS et SSH
- CIRCL : Go, algo PQ
- AWS libcrypto : C, algo PQ

Autres

- messagerie sécurisée: Signal, Apple iMessage PQ3

Travaux Existants

TLS

- Google Chrome : TLS avec échange de clés hybride avec ML-KEM (bureau uniquement)
- Amazon : TLS avec échange de clés hybride dans certains services
- Meta : TLS avec échange de clés hybride pour services internes
- Pas de RFC, mais des drafts par l'IETF pour l'échange de clés hybride
- **OpenSSL** v3.5 : intégration de ML-KEM, ML-DSA, SLH-DSA

Bibliothèques open-source

- liboqs : C, algo et certs X.509 PQ, KEM hybride pour TLS et SSH
- CIRCL : Go, algo PQ
- AWS libcrypto : C, algo PQ

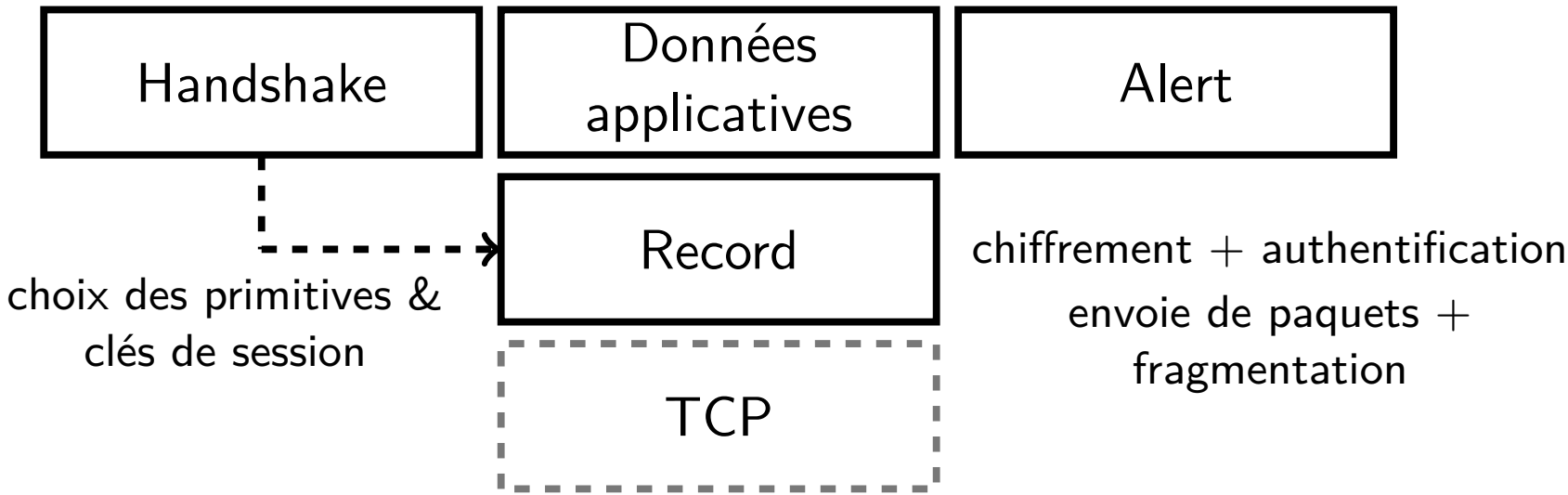
Autres

- messagerie sécurisée: Signal, Apple iMessage PQ3
- ...

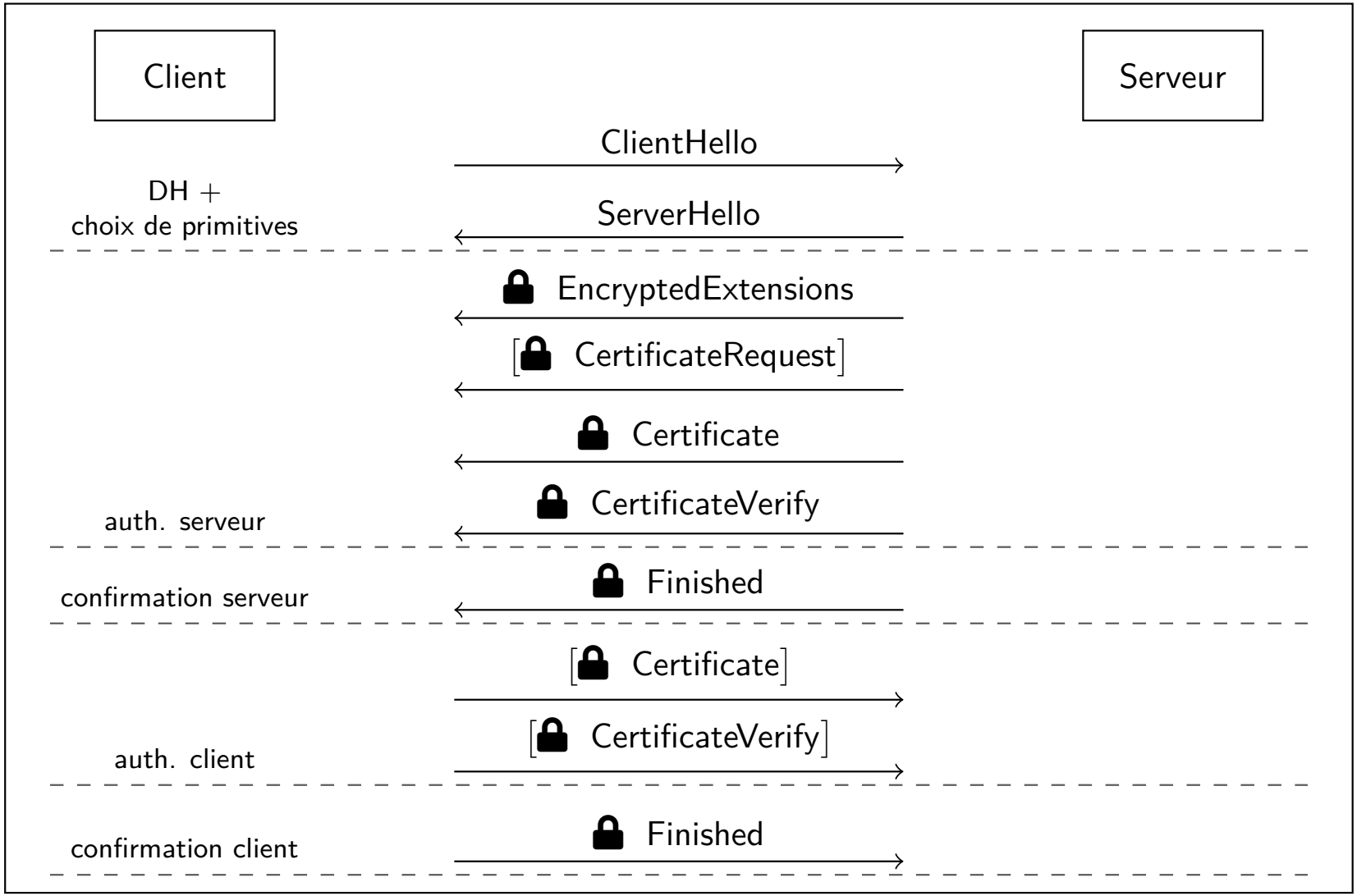
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

3. Application à TLS

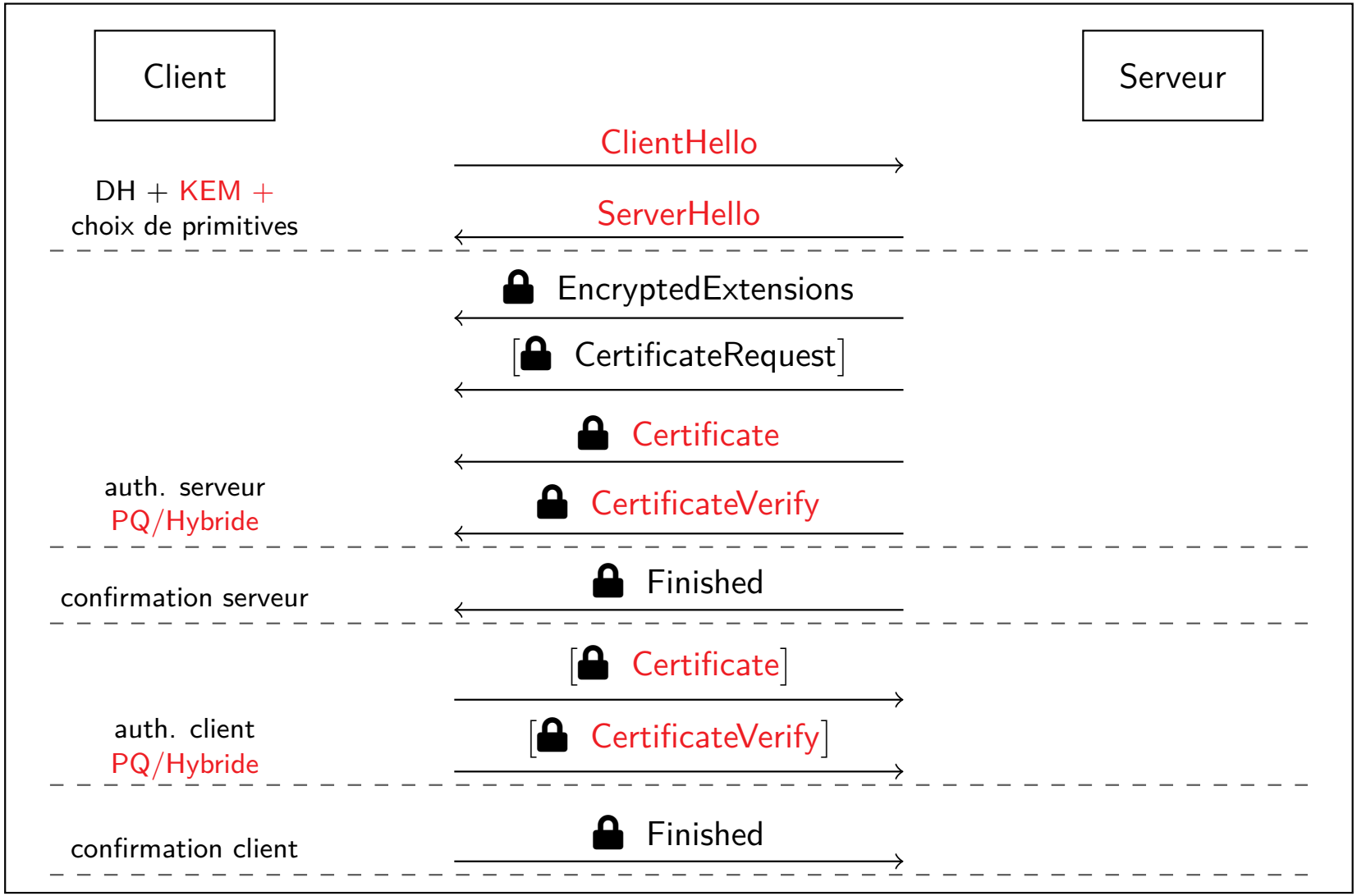
TLS 1.3


Handshake
Données applicatives
Alert
Record
TCP
choix des primitives & clés de session
chiffrement + authentification
envoie de paquets + fragmentation

TLS 1.3 : Handshake



TLS 1.3 : Handshake PQ/Hybride



TLS 1.3 : Handshake PQ/Hybride

TLS 1.3 : cas où ça se passe bien

TLS 1.3 : Handshake PQ/Hybride

TLS 1.3 : cas où ça se passe bien

- Fragmentation gérée par défaut

TLS 1.3 : Handshake PQ/Hybride

TLS 1.3 : cas où ça se passe bien

- Fragmentation gérée par défaut
- Messages bien structurés

TLS 1.3 : Handshake PQ/Hybride

TLS 1.3 : cas où ça se passe bien

- Fragmentation gérée par défaut
- Messages bien structurés
- Utilisation de DH et de signatures bien identifiée

TLS 1.3 : Handshake PQ/Hybride

TLS 1.3 : cas où ça se passe bien

- Fragmentation gérée par défaut
- Messages bien structurés
- Utilisation de DH et de signatures bien identifiée
- Rétro compatibilité échange de clés

TLS 1.3 : Handshake PQ/Hybride

TLS 1.3 : cas où ça se passe bien

- Fragmentation gérée par défaut
- Messages bien structurés
- Utilisation de DH et de signatures bien identifiée
- Rétro compatibilité échange de clés
  - Possibilité d'utiliser les extensions dans ClientHello et ServerHello pour l'échange KEM

TLS 1.3 : Handshake PQ/Hybride

TLS 1.3 : cas où ça se passe bien

- Fragmentation gérée par défaut
- Messages bien structurés
- Utilisation de DH et de signatures bien identifiée
- Rétro compatibilité échange de clés
  - Possibilité d'utiliser les extensions dans ClientHello et ServerHello pour l'échange KEM
- Possibilité de faire de l'hybride ou du post-quantique pure

TLS 1.3 : Handshake PQ/Hybride

Autre proposition : KEMTLS [SSW:CCS20]

TLS 1.3 : Handshake PQ/Hybride

Autre proposition : KEMTLS [SSW:CCS20]

- Authentification en utilisant des **KEM**s à la place des **signatures**

TLS 1.3 : Handshake PQ/Hybride

Autre proposition : KEMTLS [SSW:CCS20]

- Authentification en utilisant des **KEM**s à la place des **signatures**
- Certificats authentifiant des clés KEMs
- Les KEMs post-quantiques ont des tailles plus petites que les signatures post-quantiques

TLS 1.3 : Handshake PQ/Hybride

Autre proposition : KEMTLS [SSW:CCS20]

- Authentification en utilisant des **KEM**s à la place des **signatures**
- Certificats authentifiant des clés KEMs
- Les KEMs post-quantiques ont des tailles plus petites que les signatures post-quantiques
- Idée déjà utilisée en classique : KEM basé sur RSA, clés DH statiques, ...

4. Application à IKEv2

IPsec/IKEv2

IPsec

IPsec/IKEv2

IPsec

- Protocole VPN

IPsec/IKEv2

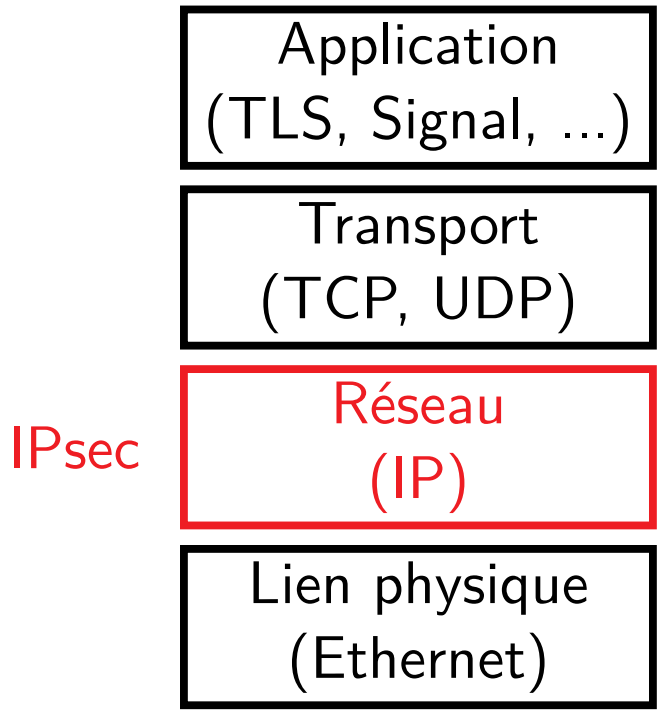
IPsec

- Protocole VPN
- Assure la confidentialité, l'intégrité et l'authentification des paquets IP

IPsec/IKEv2

IPsec

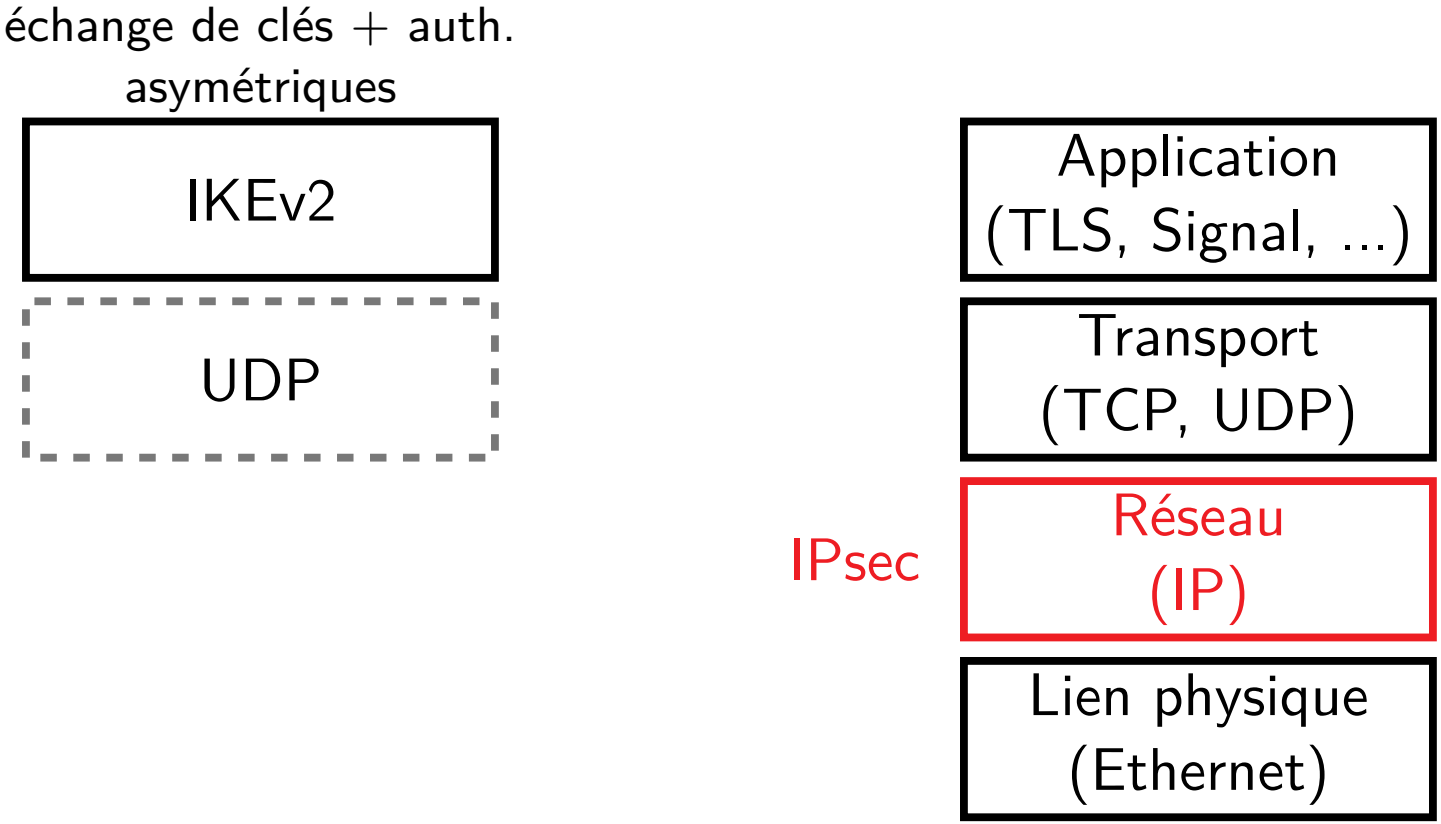
- Protocole VPN
- Assure la confidentialité, l'intégrité et l'authentification des paquets IP



IPsec/IKEv2

IPsec

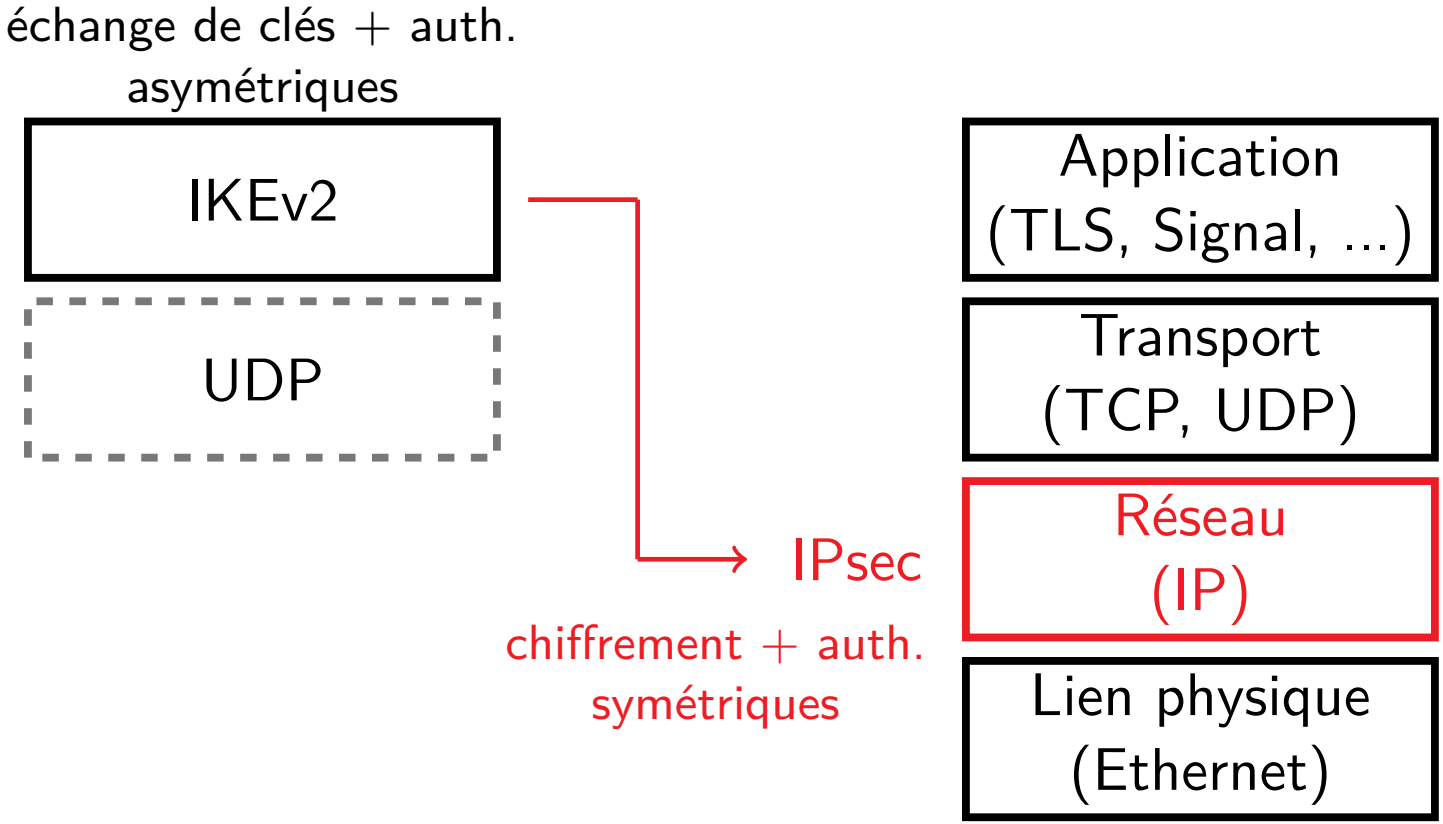
- Protocole VPN
- Assure la confidentialité, l'intégrité et l'authentification des paquets IP



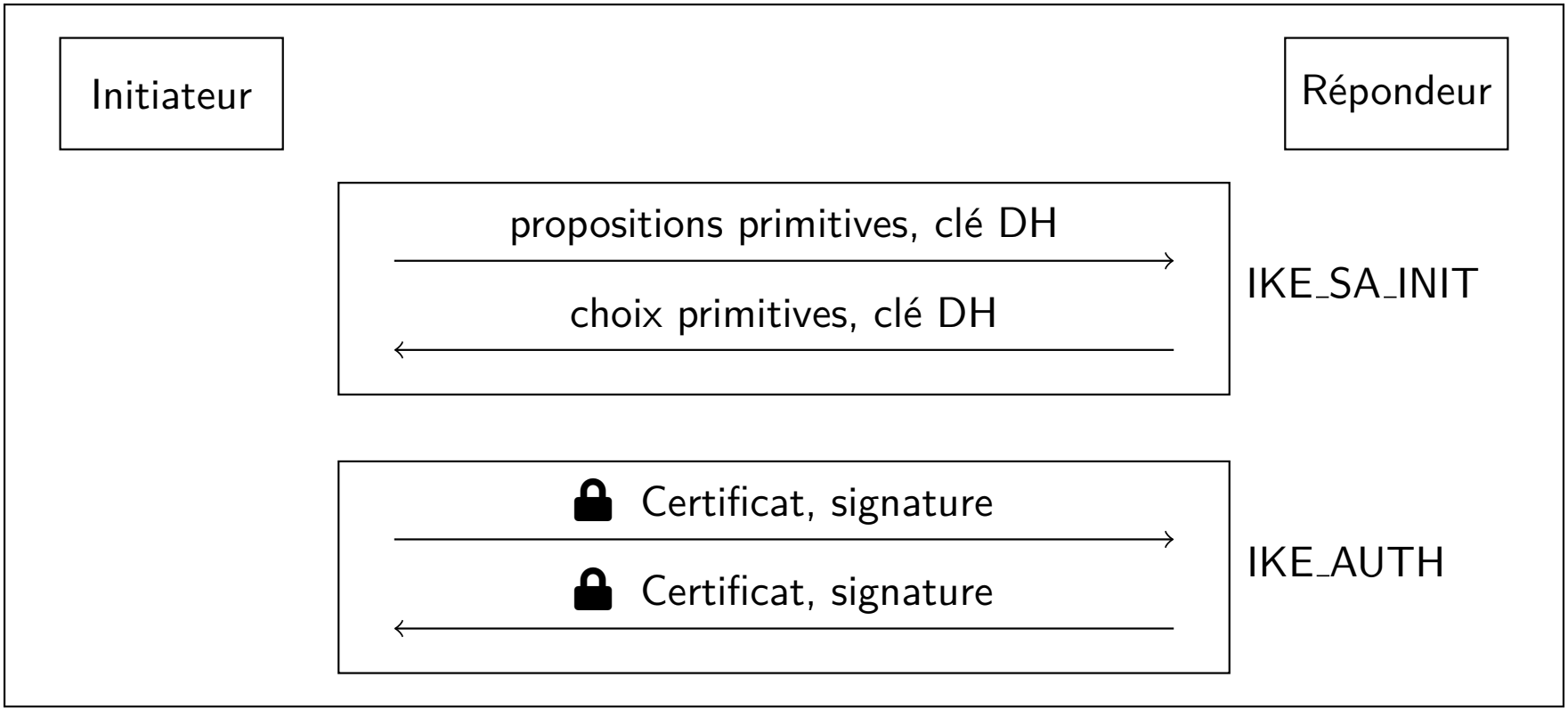
IPsec/IKEv2

IPsec

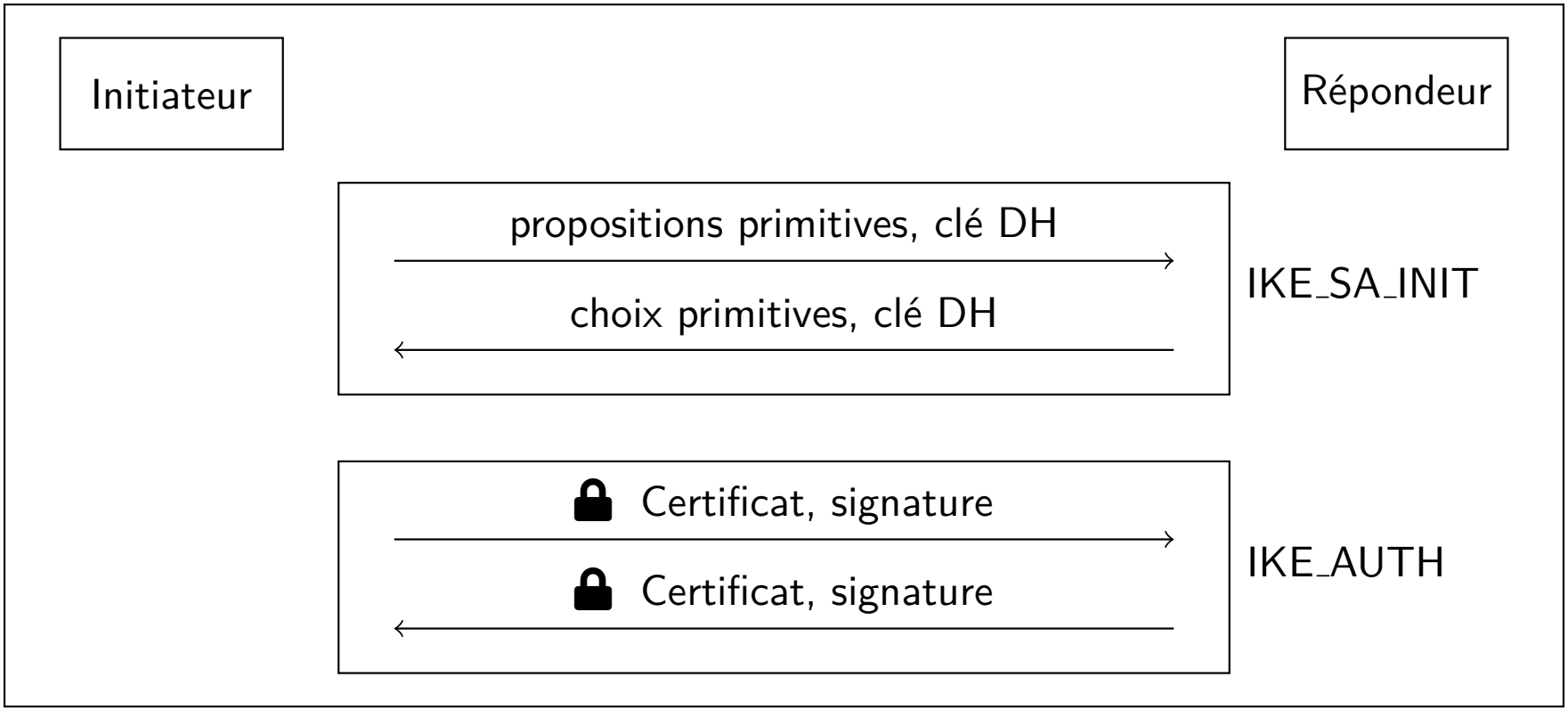
- Protocole VPN
- Assure la confidentialité, l'intégrité et l'authentification des paquets IP



IKEv2

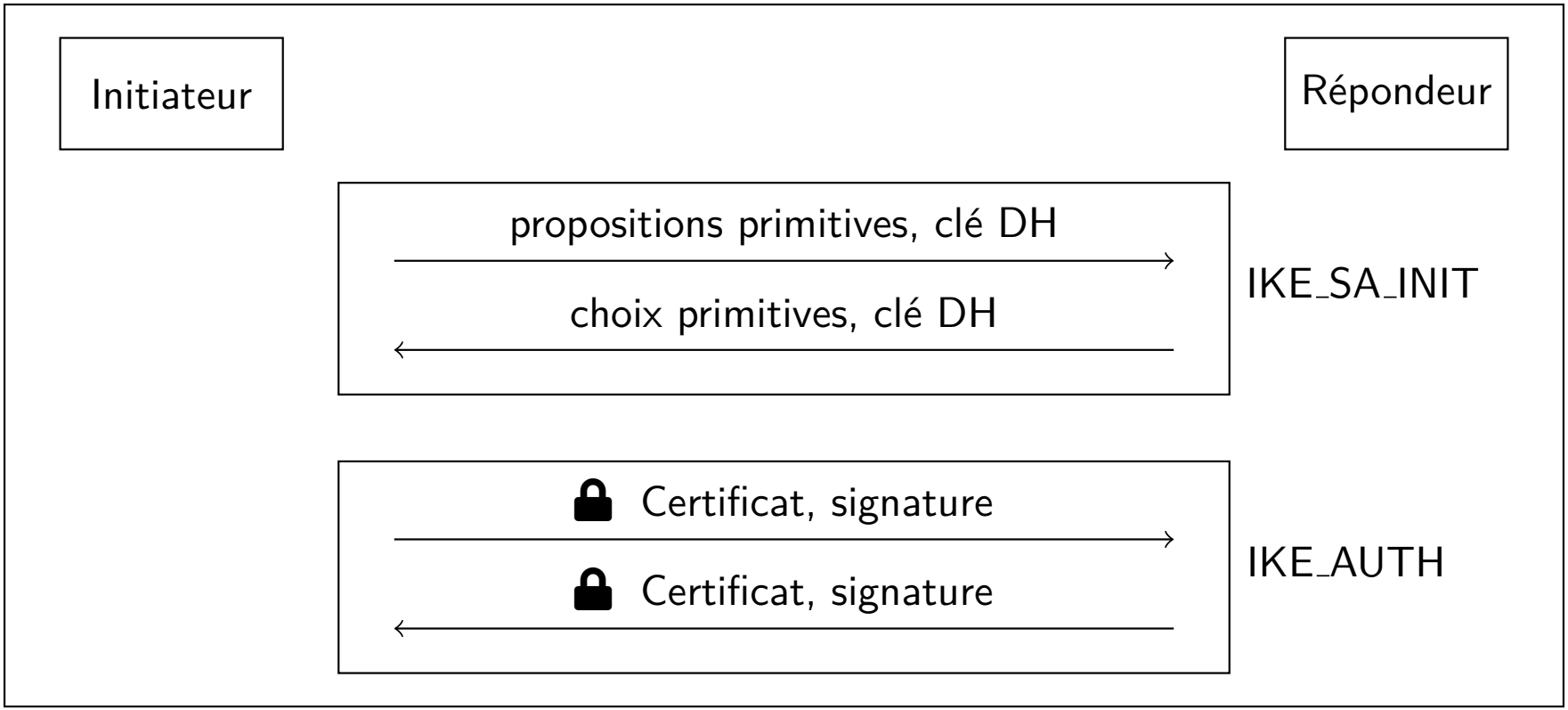

Initiateur
Répondeur
propositions primitives, clé DH
choix primitives, clé DH
IKE_SA_INIT
Certificat, signature
Certificat, signature
IKE_AUTH

IKEv2



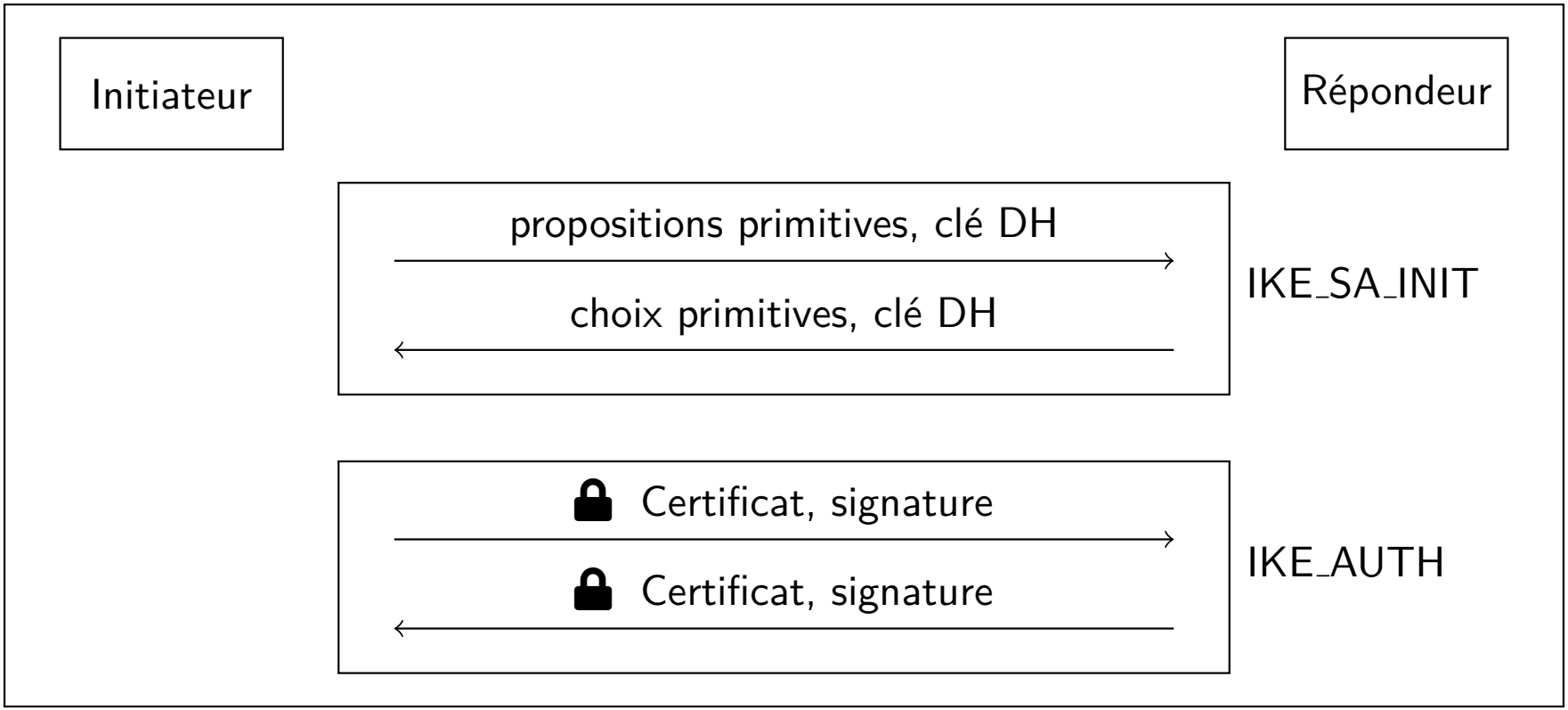
- fonctionne sur UDP

IKEv2



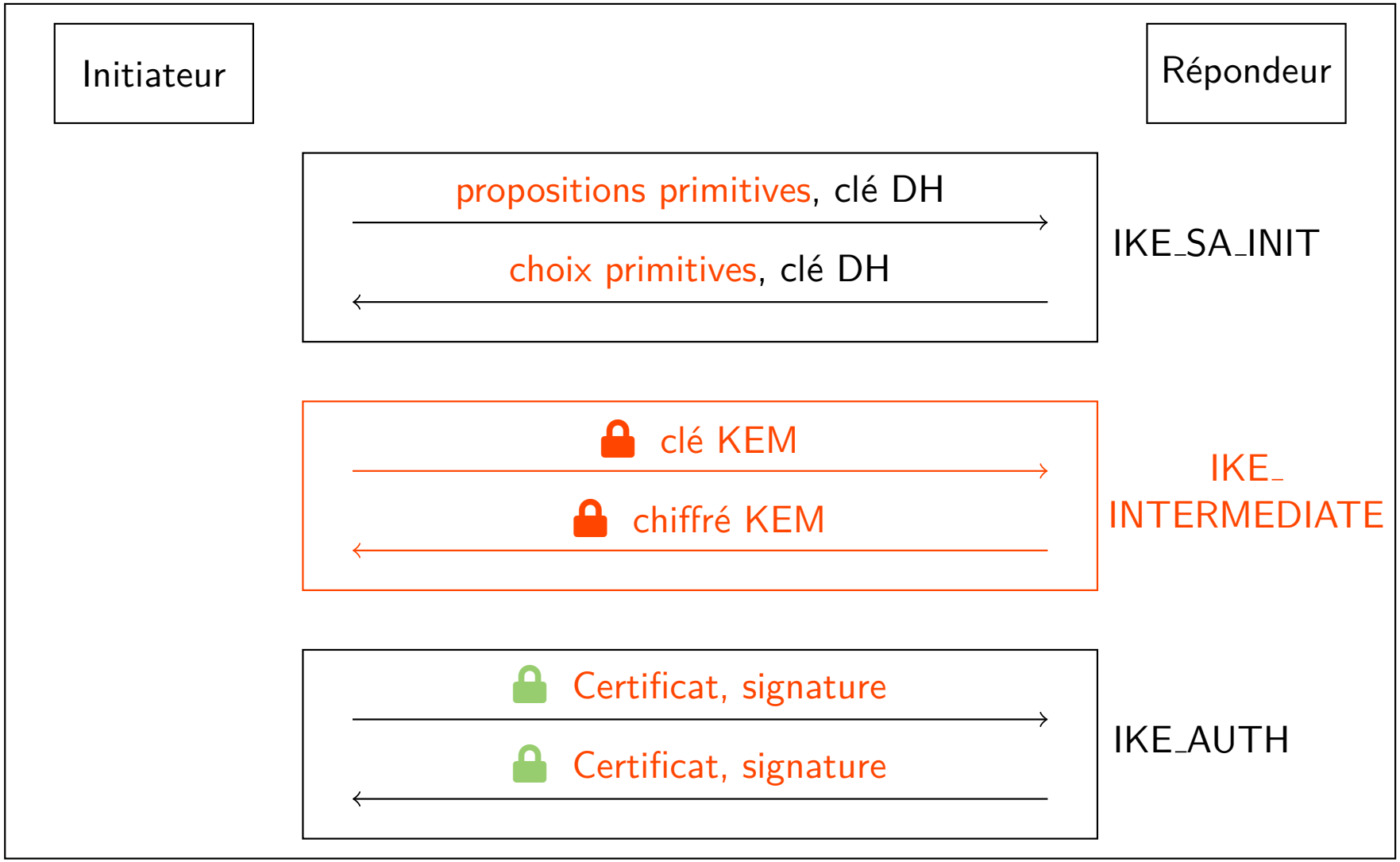
- fonctionne sur UDP
- gère uniquement la fragmentation des messages (🔒) chiffrés

IKEv2

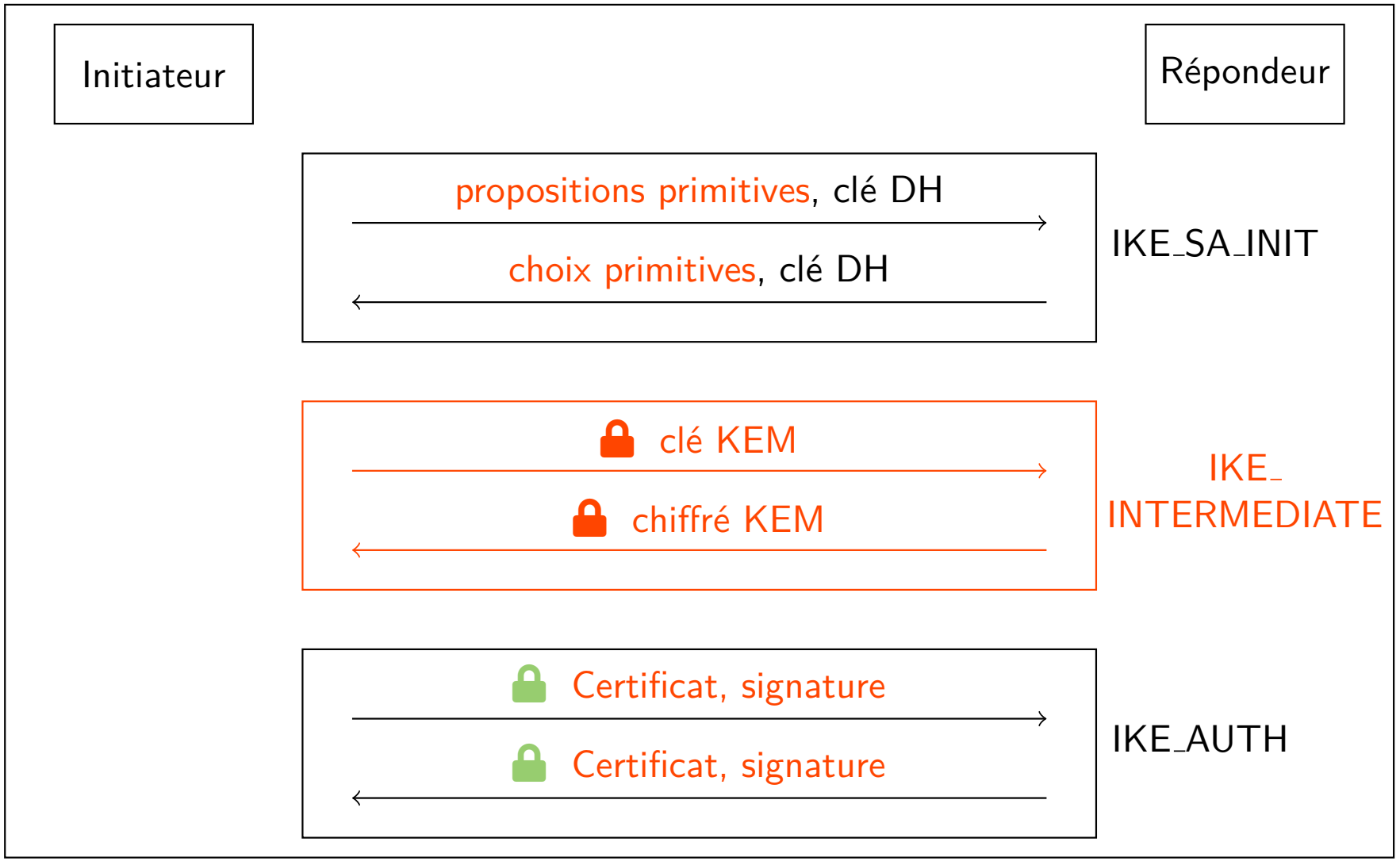


- fonctionne sur UDP
- gère uniquement la fragmentation des messages (🔒) chiffrés
- échange de clés KEM post-quantique impossible dans IKE_SA_INIT initial

IKEv2 Hybride

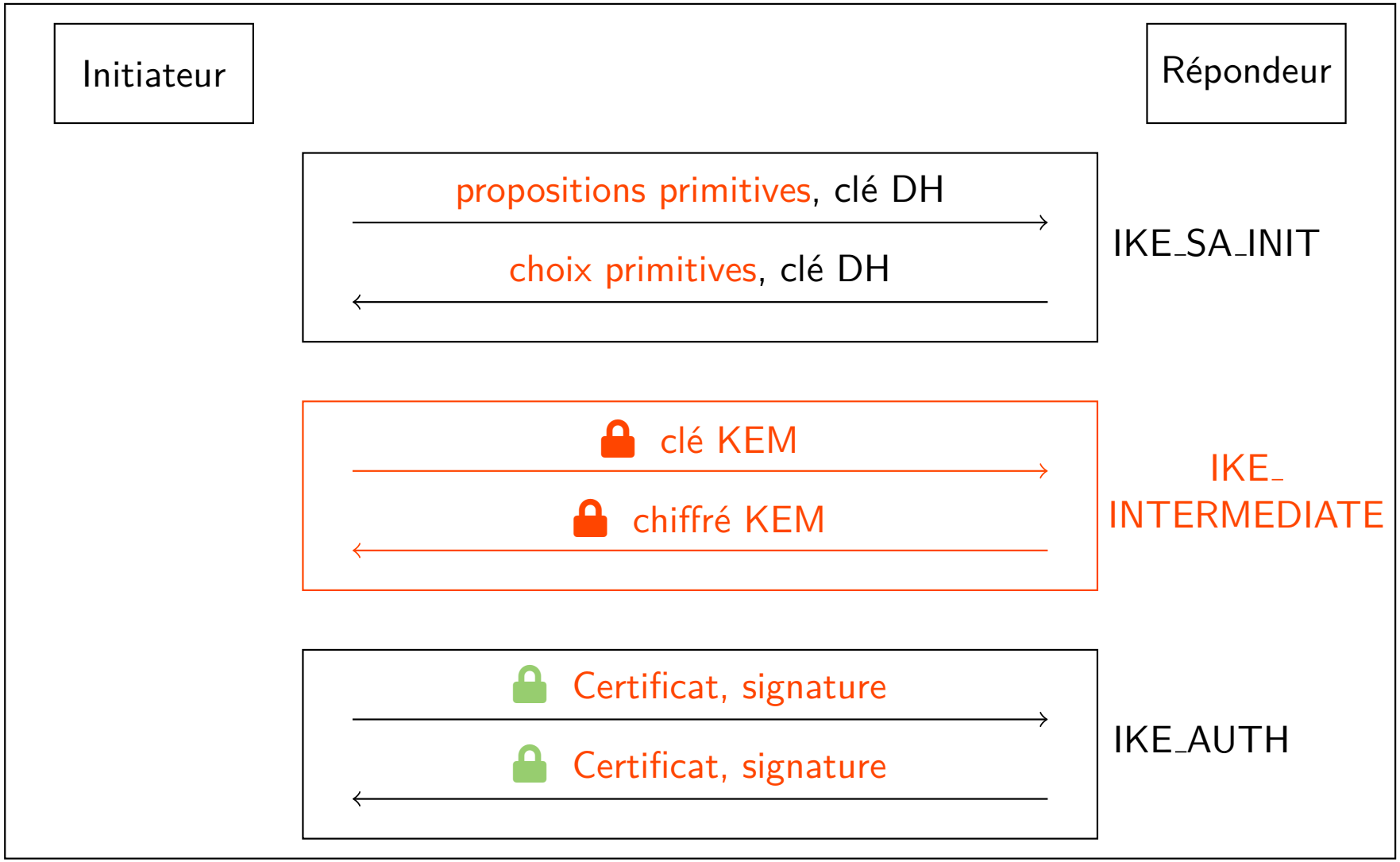


IKEv2 Hybride



- : protégé avec la clé DH

IKEv2 Hybride



- : protégé avec la clé DH
- : protégé en hybride avec les clés DH et KEM

IKEv2 Hybride

IKEv2 : cas moins idéal que TLS 1.3

IKEv2 Hybride

IKEv2 : cas moins idéal que TLS 1.3

- Fonctionne sur UDP

IKEv2 Hybride

IKEv2 : cas moins idéal que TLS 1.3

- Fonctionne sur UDP
- Nécessite une gestion particulière de la fragmentation

IKEv2 Hybride

IKEv2 : cas moins idéal que TLS 1.3

- Fonctionne sur UDP
- Nécessite une gestion particulière de la fragmentation
- Fragmentation possible uniquement pour les messages chiffrés

IKEv2 Hybride

IKEv2 : cas moins idéal que TLS 1.3

- Fonctionne sur UDP
- Nécessite une gestion particulière de la fragmentation
- Fragmentation possible uniquement pour les messages chiffrés
- Echange de clés KEM impossible dès le premier échange

IKEv2 Hybride

IKEv2 : cas moins idéal que TLS 1.3

- Fonctionne sur UDP
- Nécessite une gestion particulière de la fragmentation
- Fragmentation possible uniquement pour les messages chiffrés
- Echange de clés KEM impossible dès le premier échange
- Transition post-quantique pure d'IKEv2 ?

IKEv2 Hybride

IKEv2 : cas moins idéal que TLS 1.3

- Fonctionne sur UDP
- Nécessite une gestion particulière de la fragmentation
- Fragmentation possible uniquement pour les messages chiffrés
- Echange de clés KEM impossible dès le premier échange
- Transition post-quantique pure d'IKEv2 ?
  - **Modification du protocole**

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

5. Application à WireGuard

WireGuard

- Protocole VPN conçu en 2017

WireGuard

- Protocole VPN conçu en 2017
- Objectifs: Efficacité et simplicité de code

WireGuard

- Protocole VPN conçu en 2017
- Objectifs: Efficacité et simplicité de code
- Alternative à IPsec/IKEv2

WireGuard

- Protocole VPN conçu en 2017
- Objectifs: Efficacité et simplicité de code
- Alternative à IPsec/IKEv2
- Handshake de 2 messages

WireGuard

- Protocole VPN conçu en 2017
- Objectifs: Efficacité et simplicité de code
- Alternative à IPsec/IKEv2
- Handshake de 2 messages
- Fonctionne sur UDP

WireGuard

- Protocole VPN conçu en 2017
- Objectifs: Efficacité et simplicité de code
- Alternative à IPsec/IKEv2
- Handshake de 2 messages
- Fonctionne sur UDP
  - Ne gère pas la fragmentation

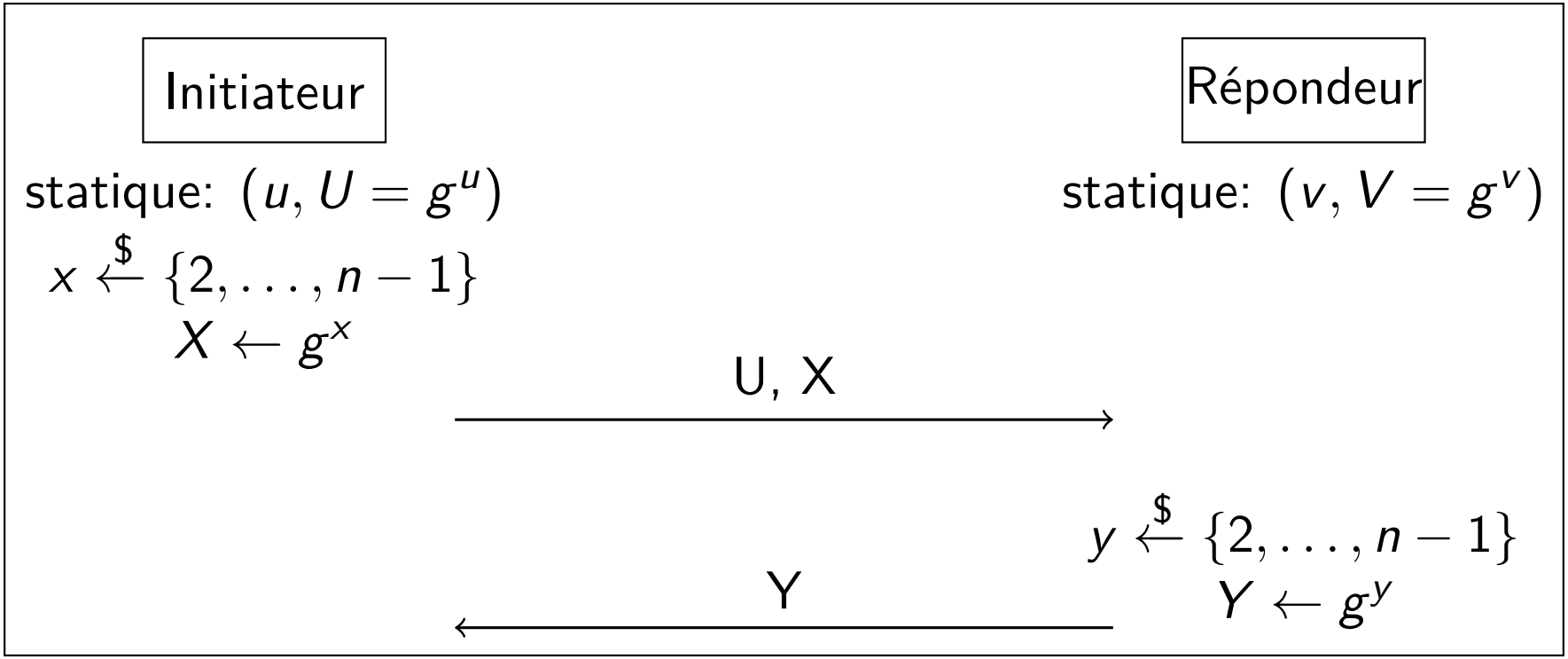
WireGuard

- Protocole VPN conçu en 2017
- Objectifs: Efficacité et simplicité de code
- Alternative à IPsec/IKEv2
- Handshake de 2 messages
- Fonctionne sur UDP
  - Ne gère pas la fragmentation
- Authentification des parties

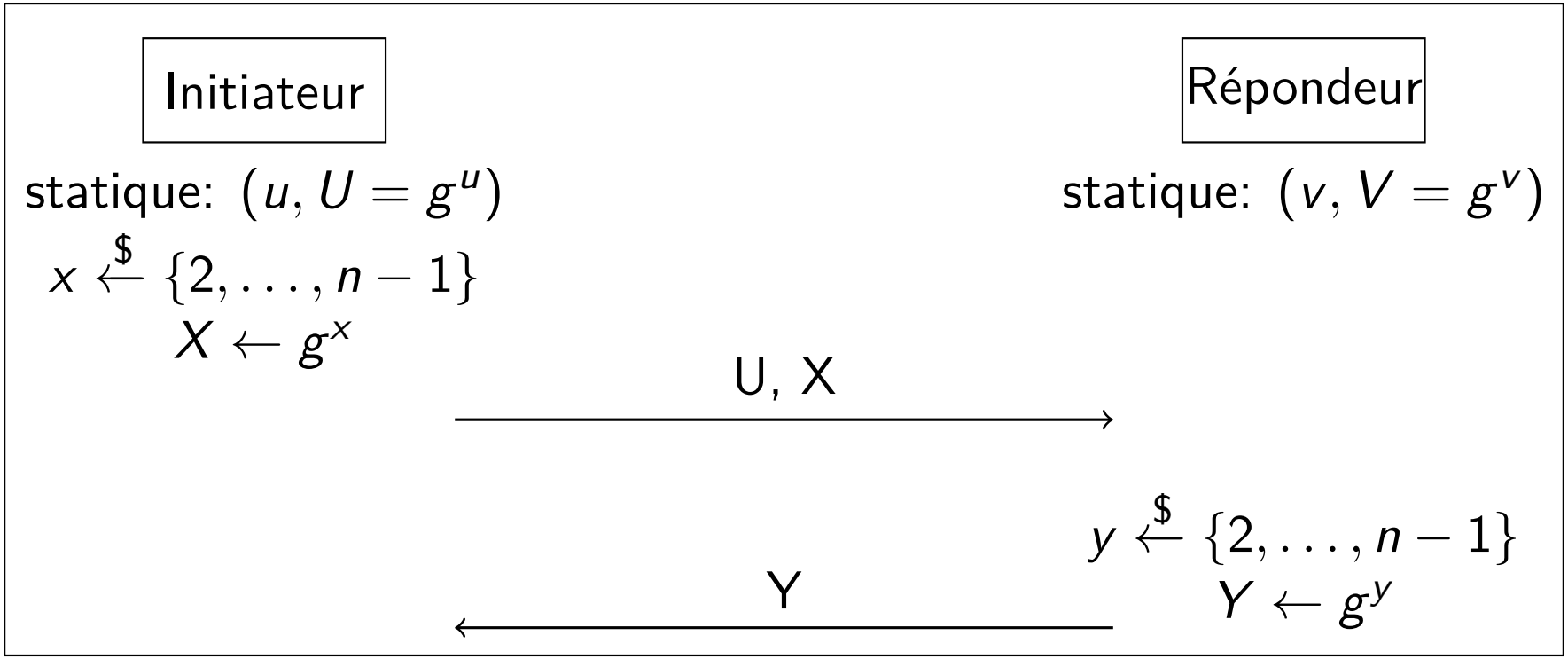
WireGuard

- Protocole VPN conçu en 2017
- Objectifs: Efficacité et simplicité de code
- Alternative à IPsec/IKEv2
- Handshake de 2 messages
- Fonctionne sur UDP
  - Ne gère pas la fragmentation
- Authentification des parties
  - Clés Diffie-Hellman

WireGuard : Handshake (Très Simplifié)

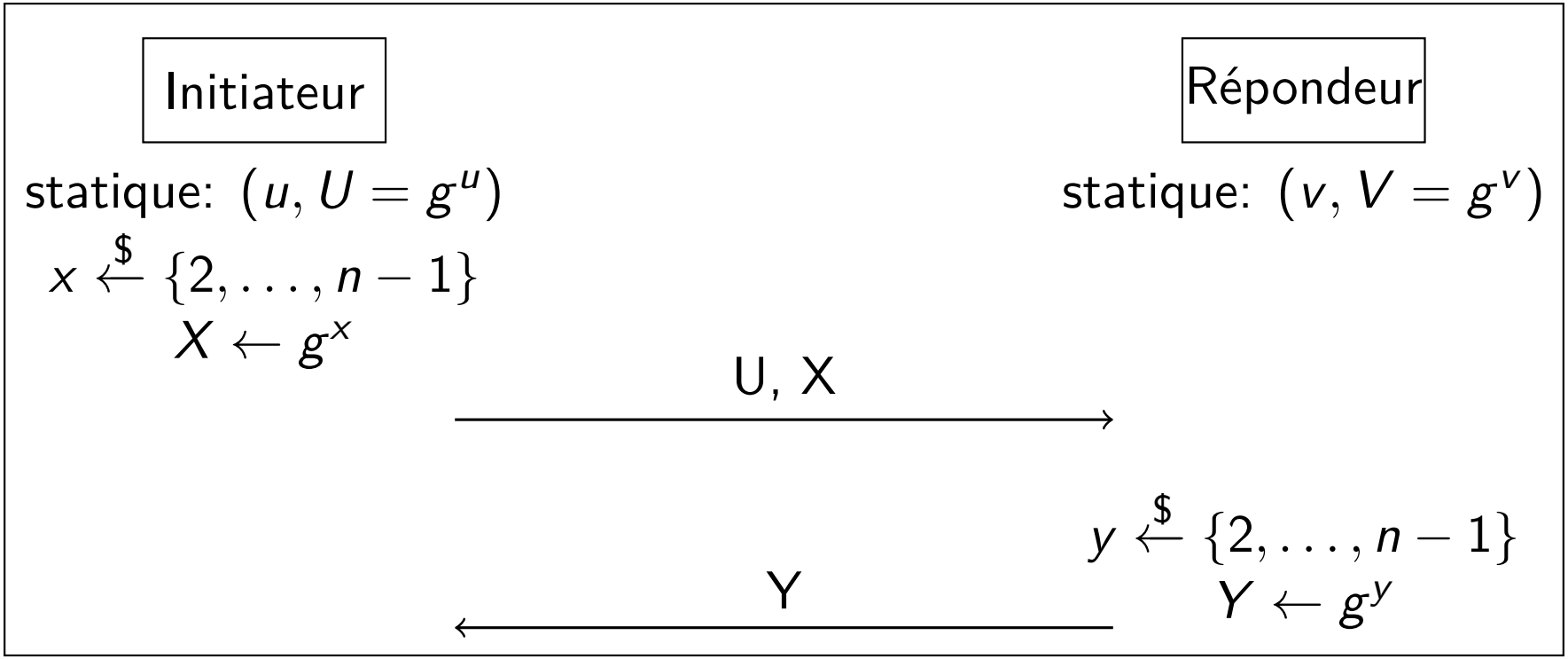


WireGuard : Handshake (Très Simplifié)



4 secrets partagés DH sont générés

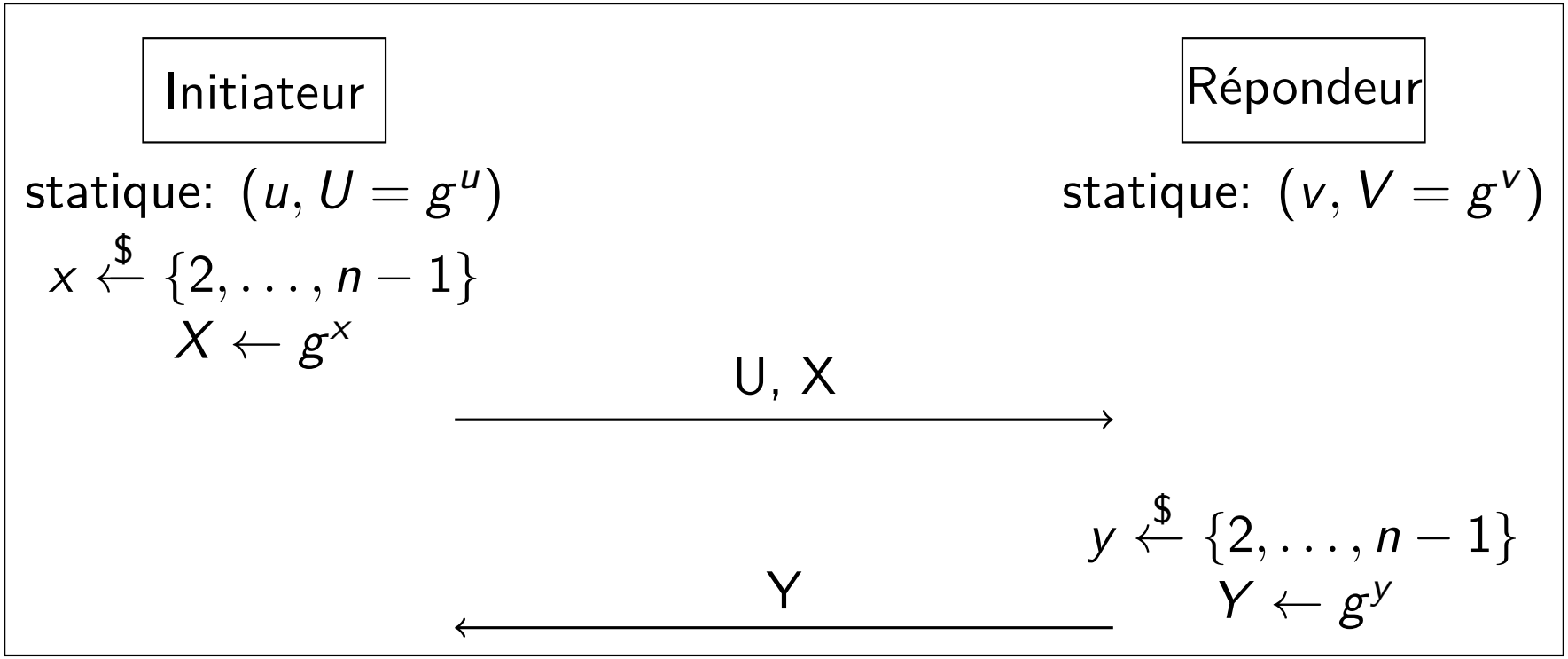
WireGuard : Handshake (Très Simplifié)



4 secrets partagés DH sont générés

- éphémère - éphémère : g^{xy}

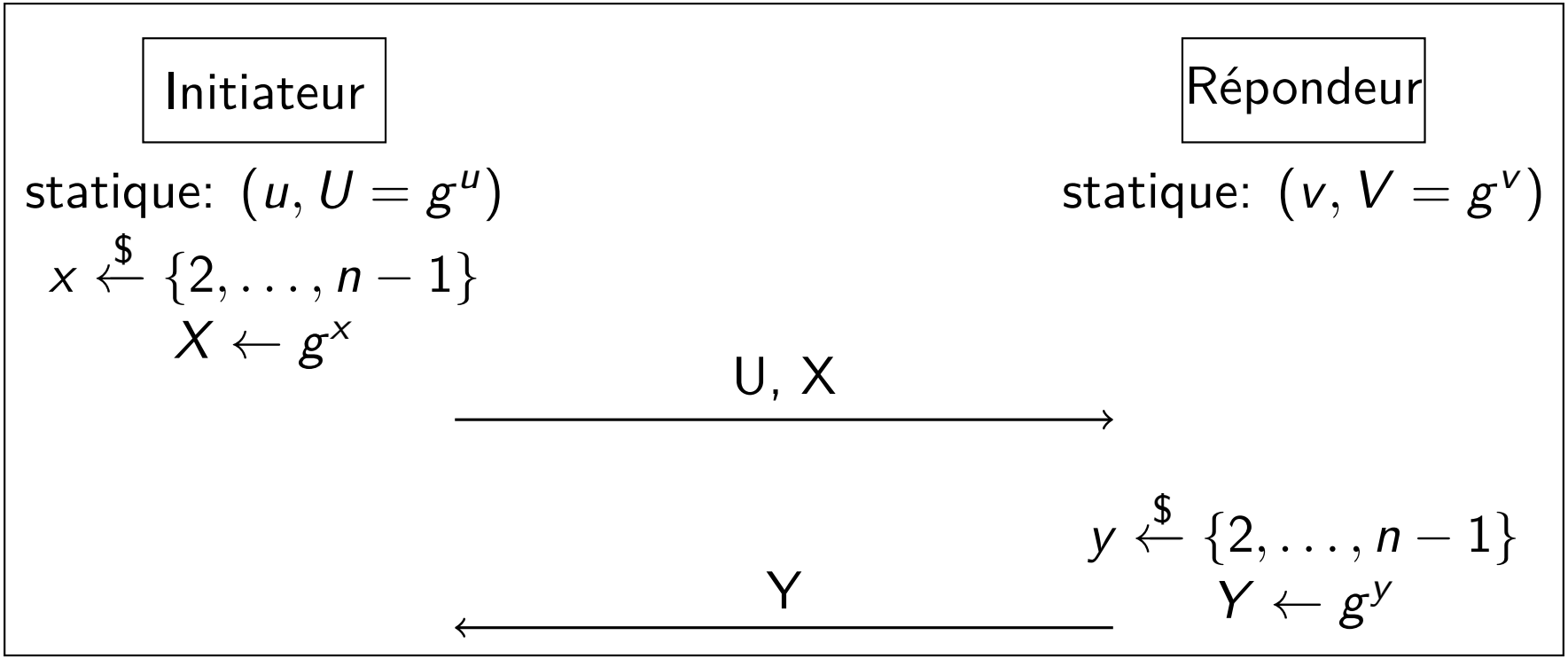
WireGuard : Handshake (Très Simplifié)



4 secrets partagés DH sont générés

- éphémère - éphémère : g^{xy}
- éphémère - statique : g^{xv}

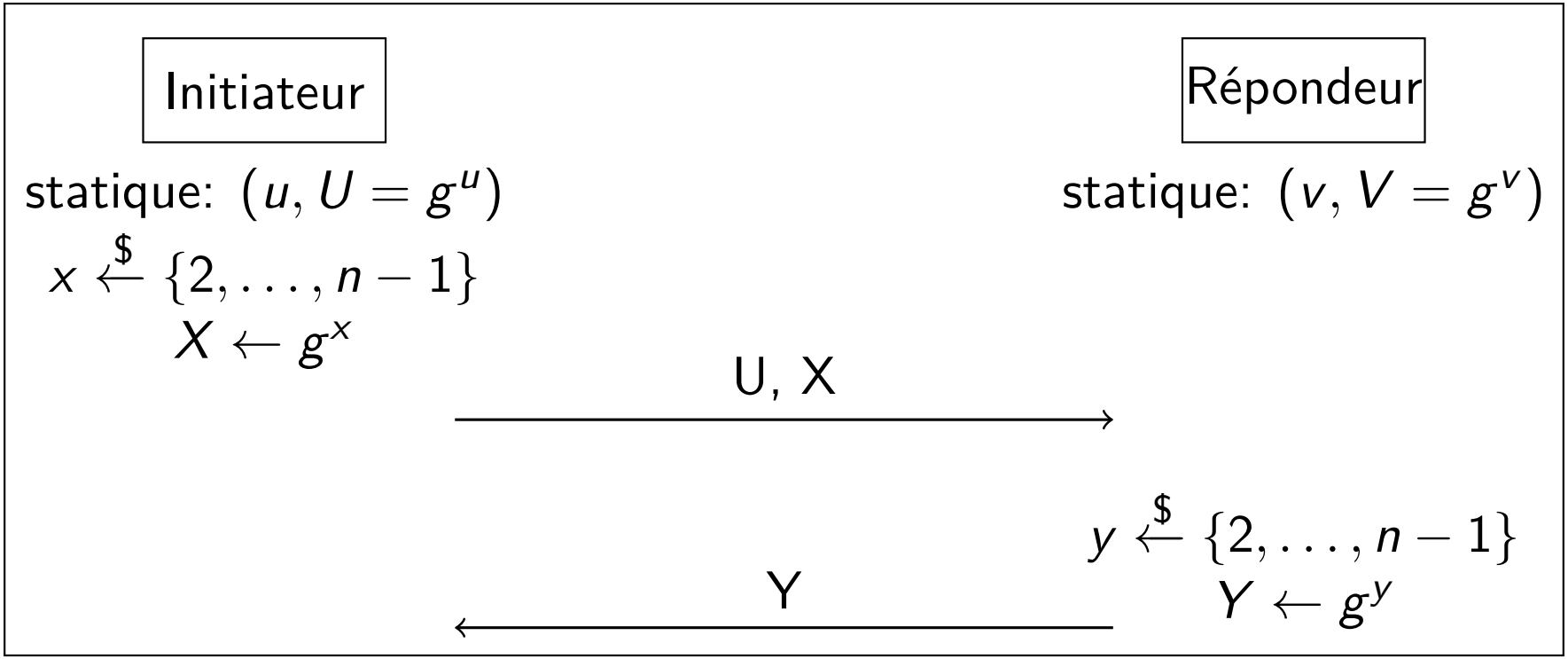
WireGuard : Handshake (Très Simplifié)



4 secrets partagés DH sont générés

- éphémère - éphémère : g^{xy}
- éphémère - statique : g^{xv}
- statique - éphémère : g^{uy}

WireGuard : Handshake (Très Simplifié)



4 secrets partagés DH sont générés

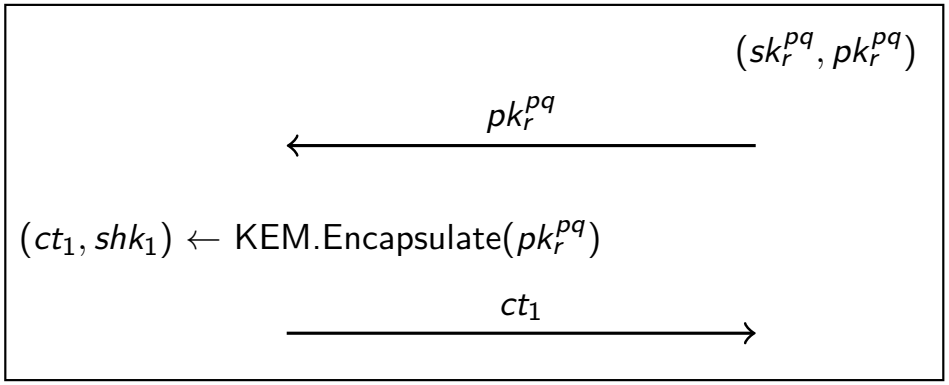
- éphémère - éphémère : g^{xy}
- éphémère - statique : g^{xv}
- statique - éphémère : g^{uy}
- statique - statique : g^{uv} (authentification mutuelle implicite)

WireGuard Post-Quantique [HNSWZ:S&P21]

Remplacer les secrets DH par des secrets KEM

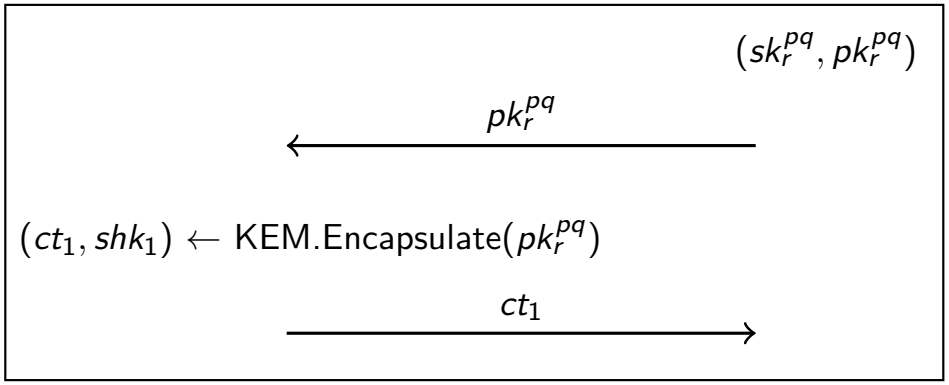
WireGuard Post-Quantique [HNSWZ:S&P21]

Remplacer les secrets DH par des secrets KEM



WireGuard Post-Quantique [HNSWZ:S&P21]

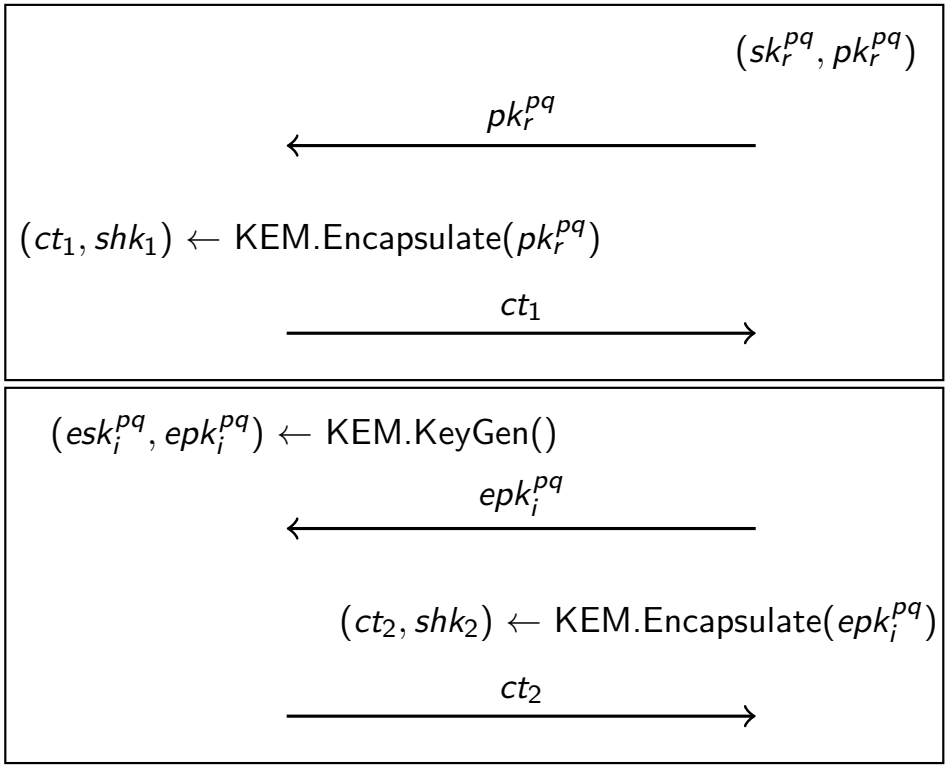
Remplacer les secrets DH par des secrets KEM



- éphémère - statique
- shk_1 remplace g^{xv}

WireGuard Post-Quantique [HNSWZ:S&P21]

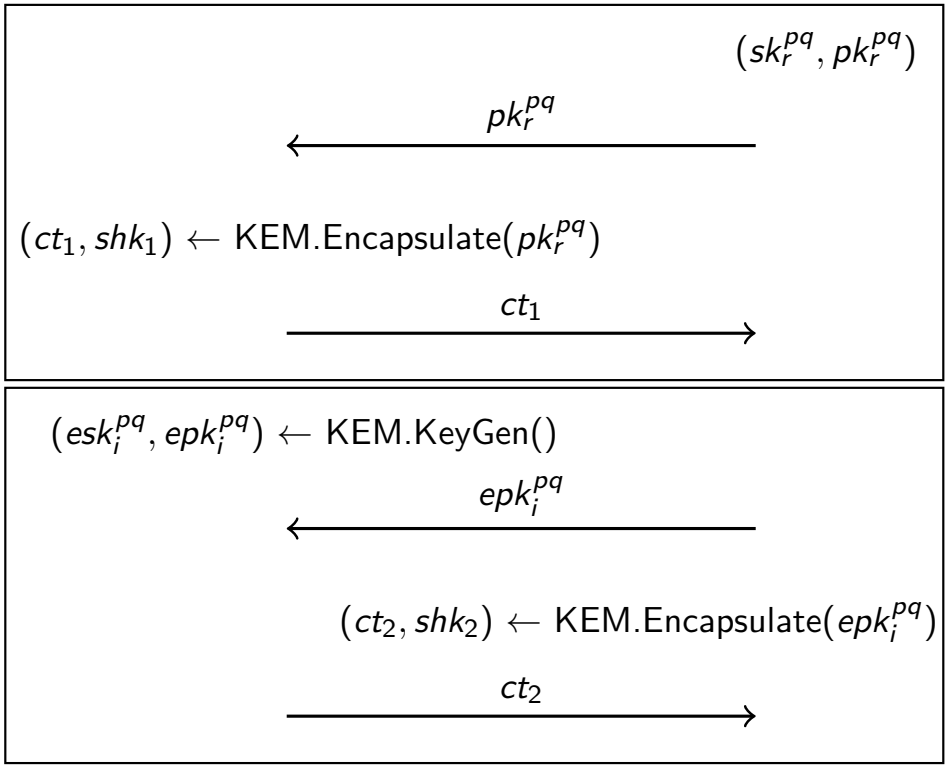
Remplacer les secrets DH par des secrets KEM



- éphémère - statique
- shk_1 remplace g^{xv}

WireGuard Post-Quantique [HNSWZ:S&P21]

Remplacer les secrets DH par des secrets KEM

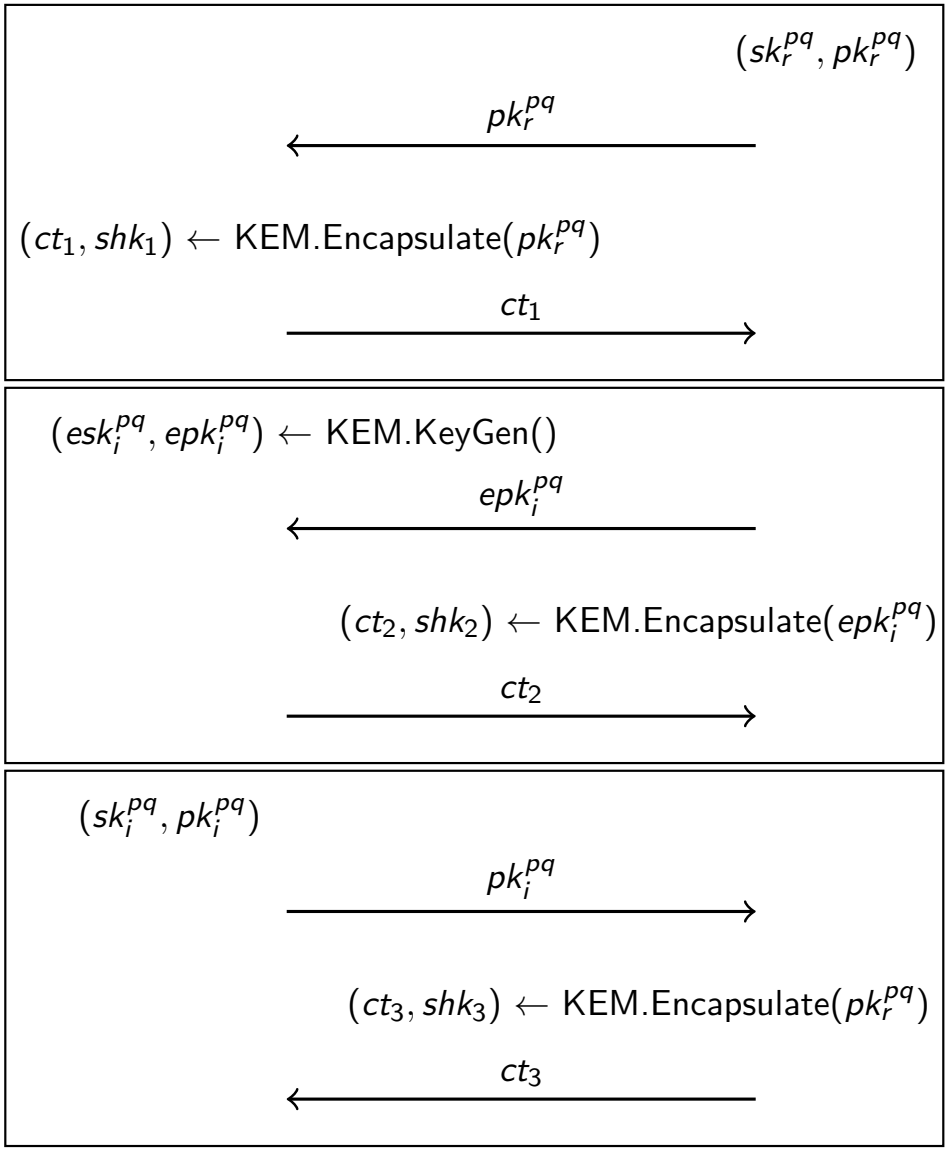


- éphémère - statique
- shk_1 remplace g^{xv}

- éphémère - éphémère
- shk_2 remplace g^{xy}

WireGuard Post-Quantique [HNSWZ:S&P21]

Remplacer les secrets DH par des secrets KEM

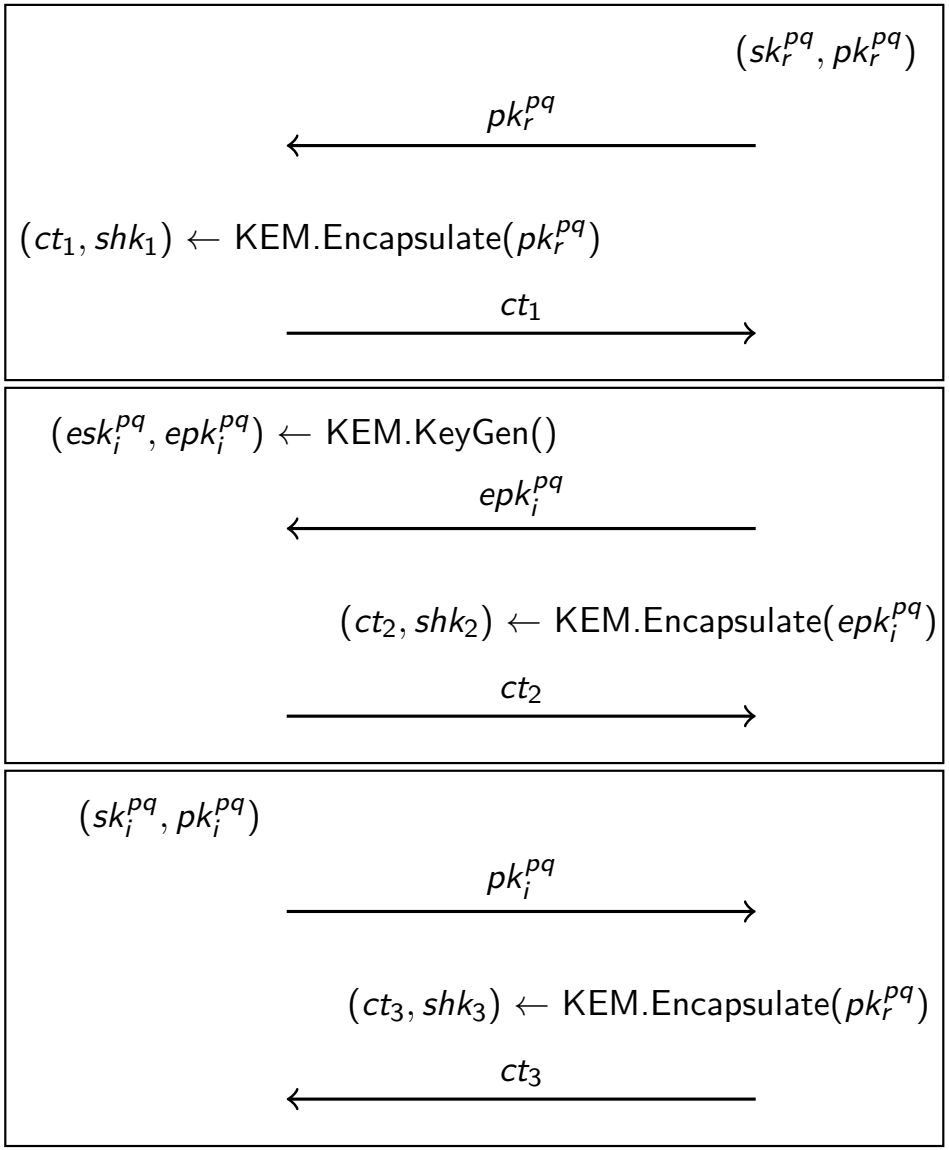


- éphémère - statique
- shk_1 remplace g^{xv}

- éphémère - éphémère
- shk_2 remplace g^{xy}

WireGuard Post-Quantique [HNSWZ:S&P21]

Remplacer les secrets DH par des secrets KEM



- éphémère - statique
- shk_1 remplace g^{xv}

- éphémère - éphémère
- shk_2 remplace g^{xy}

- statique - éphémère
- shk_3 remplace g^{uy}

WireGuard Post-Quantique [HNSWZ:S&P21]

g^{uv} ?

WireGuard Post-Quantique [HNSWZ:S&P21]

g^{uv} ?

- Secret DH statique - statique $\rightarrow$ non-interactive

WireGuard Post-Quantique [HNSWZ:S&P21]

g^{uv} ?

- Secret DH statique - statique $\rightarrow$ non-interactive
- Secret KEM $\rightarrow$ nécessite **au moins** une interaction

WireGuard Post-Quantique [HNSWZ:S&P21]

g^{uv} ?

- Secret DH statique - statique $\rightarrow$ non-interactive
- Secret KEM $\rightarrow$ nécessite **au moins** une interaction
- Besoin de solution alternative

WireGuard Post-Quantique [HNSWZ:S&P21]

g^{uv} ?

- Secret DH statique - statique $\rightarrow$ non-interactive
- Secret KEM $\rightarrow$ nécessite **au moins** une interaction
- Besoin de solution alternative
  - Clé pré-partagée

WireGuard Post-Quantique [HNSWZ:S&P21]

g^{uv} ?

- Secret DH statique - statique $\rightarrow$ non-interactive
- Secret KEM $\rightarrow$ nécessite **au moins** une interaction
- Besoin de solution alternative
  - Clé pré-partagée

WireGuard : cas où ça se passe mal ...

WireGuard Post-Quantique [HNSWZ:S&P21]

g^{uv} ?

- Secret DH statique - statique $\rightarrow$ non-interactive
- Secret KEM $\rightarrow$ nécessite **au moins** une interaction
- Besoin de solution alternative
  - Clé pré-partagée

WireGuard : cas où ça se passe mal ...

- Fragmentation non-gérée

WireGuard Post-Quantique [HNSWZ:S&P21]

g^{uv} ?

- Secret DH statique - statique $\rightarrow$ non-interactive
- Secret KEM $\rightarrow$ nécessite **au moins** une interaction
- Besoin de solution alternative
  - Clé pré-partagée

WireGuard : cas où ça se passe mal ...

- Fragmentation non-gérée
  - Modification du protocole,

WireGuard Post-Quantique [HNSWZ:S&P21]

g^{uv} ?

- Secret DH statique - statique $\rightarrow$ non-interactive
- Secret KEM $\rightarrow$ nécessite **au moins** une interaction
- Besoin de solution alternative
  - Clé pré-partagée

WireGuard : cas où ça se passe mal ...

- Fragmentation non-gérée
  - Modification du protocole,
  - ou choix de KEMs contraints

WireGuard Post-Quantique [HNSWZ:S&P21]

g^{uv} ?

- Secret DH statique - statique $\rightarrow$ non-interactive
- Secret KEM $\rightarrow$ nécessite **au moins** une interaction
- Besoin de solution alternative
  - Clé pré-partagée

WireGuard : cas où ça se passe mal ...

- Fragmentation non-gérée
  - Modification du protocole,
  - ou choix de KEMs contraints
- DH statique - statique

WireGuard Post-Quantique [HNSWZ:S&P21]

g^{uv} ?

- Secret DH statique - statique $\rightarrow$ non-interactive
- Secret KEM $\rightarrow$ nécessite **au moins** une interaction
- Besoin de solution alternative
  - Clé pré-partagée

WireGuard : cas où ça se passe mal ...

- Fragmentation non-gérée
  - Modification du protocole,
  - ou choix de KEMs contraints
- DH statique - statique
  - Besoin de réfléchir à d'autres solutions

6. Conclusion

Conclusion

Cryptographie Post-Quantique

Conclusion

Cryptographie Post-Quantique

- de nombreux nouveaux schémas d'échanges de clés et de signatures

Conclusion

Cryptographie Post-Quantique

- de nombreux nouveaux schémas d'échanges de clés et de signatures
- perte au niveau des tailles de données et complexité des implémentations

Conclusion

Cryptographie Post-Quantique

- de nombreux nouveaux schémas d'échanges de clés et de signatures
- perte au niveau des tailles de données et complexité des implémentations
- perte négligeable entre pure post-quantique et hybride

Conclusion

Cryptographie Post-Quantique

- de nombreux nouveaux schémas d'échanges de clés et de signatures
- perte au niveau des tailles de données et complexité des implémentations
- perte négligeable entre pure post-quantique et hybride
- pas / peu de perte au niveau des temps

Conclusion

Cryptographie Post-Quantique

- de nombreux nouveaux schémas d'échanges de clés et de signatures
- perte au niveau des tailles de données et complexité des implémentations
- perte négligeable entre pure post-quantique et hybride
- pas / peu de perte au niveau des temps

Transition des Protocoles de Communication

Conclusion

Cryptographie Post-Quantique

- de nombreux nouveaux schémas d'échanges de clés et de signatures
- perte au niveau des tailles de données et complexité des implémentations
- perte négligeable entre pure post-quantique et hybride
- pas / peu de perte au niveau des temps

Transition des Protocoles de Communication

- de nombreux études en cours pour l'utilisation de schémas PQ + hybridation

Conclusion

Cryptographie Post-Quantique

- de nombreux nouveaux schémas d'échanges de clés et de signatures
- perte au niveau des tailles de données et complexité des implémentations
- perte négligeable entre pure post-quantique et hybride
- pas / peu de perte au niveau des temps

Transition des Protocoles de Communication

- de nombreux études en cours pour l'utilisation de schémas PQ + hybridation
- de plus en plus d'implémentations et de propositions de standard

Conclusion

Cryptographie Post-Quantique

- de nombreux nouveaux schémas d'échanges de clés et de signatures
- perte au niveau des tailles de données et complexité des implémentations
- perte négligeable entre pure post-quantique et hybride
- pas / peu de perte au niveau des temps

Transition des Protocoles de Communication

- de nombreux études en cours pour l'utilisation de schémas PQ + hybridation
- de plus en plus d'implémentations et de propositions de standard
- plusieurs industriels intègrent déjà des échanges de clés hybrides (plus urgent que l'authentification)

Conclusion

Cryptographie Post-Quantique

- de nombreux nouveaux schémas d'échanges de clés et de signatures
- perte au niveau des tailles de données et complexité des implémentations
- perte négligeable entre pure post-quantique et hybride
- pas / peu de perte au niveau des temps

Transition des Protocoles de Communication

- de nombreux études en cours pour l'utilisation de schémas PQ + hybridation
- de plus en plus d'implémentations et de propositions de standard
- plusieurs industriels intègrent déjà des échanges de clés hybrides (plus urgent que l'authentification)
- Des protocoles mieux adaptés à la transition que d'autres

Conclusion

Cryptographie Post-Quantique

- de nombreux nouveaux schémas d'échanges de clés et de signatures
- perte au niveau des tailles de données et complexité des implémentations
- perte négligeable entre pure post-quantique et hybride
- pas / peu de perte au niveau des temps

Transition des Protocoles de Communication

- de nombreux études en cours pour l'utilisation de schémas PQ + hybridation
- de plus en plus d'implémentations et de propositions de standard
- plusieurs industriels intègrent déjà des échanges de clés hybrides (plus urgent que l'authentification)
- Des protocoles mieux adaptés à la transition que d'autres
- Protocoles avec d'autres primitives asymétriques que les échanges de clés et les signatures ?