

Ma cryptographie au XXI^e siècle

avec un peu d'eau salée et du post-quantique

Guillaume Bonnoron



L'itinéraire pour notre discussion

01 PARTIE 1 Jusqu'à la thèse

2003–2010

Science et Vie Junior

2010–2013

Télécom Bretagne

2015–2018

Chaire Cyber Navale

02 PARTIE 2 Aujourd'hui

ENTREPRISE

La crypto dans une entreprise normale,
c'est quoi ?

POST-QUANTIQUE

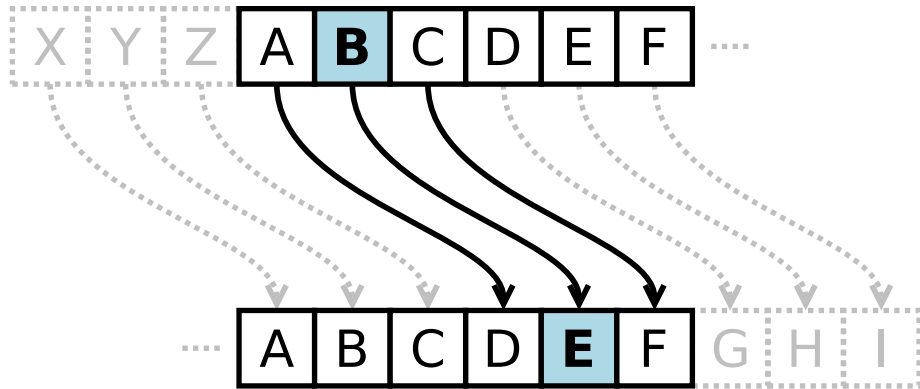
Et le post-quantique alors ?

Partie 1: Jusqu'à la thèse

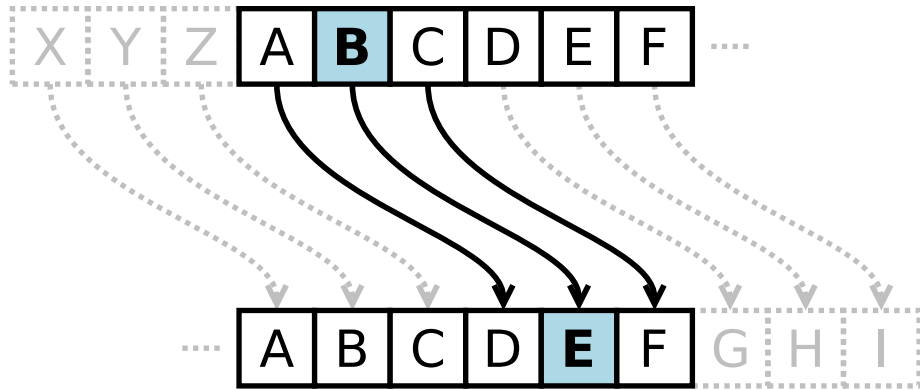
- Les années Science et Vie Junior (2003-2010)
- Les années Télécom Bretagne (2010-2013)
- Les années Chaire Cyber Navale (2015-2018)

2003-2010 – Science et Vie Junior

2003-2010 – Science et Vie Junior

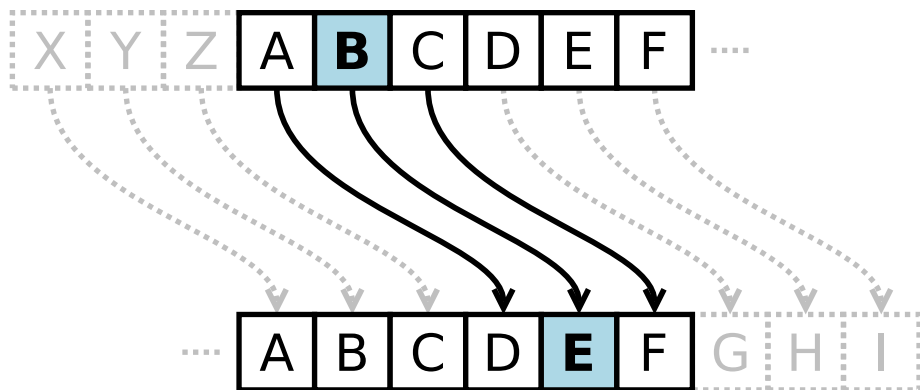


2003-2010 – Science et Vie Junior



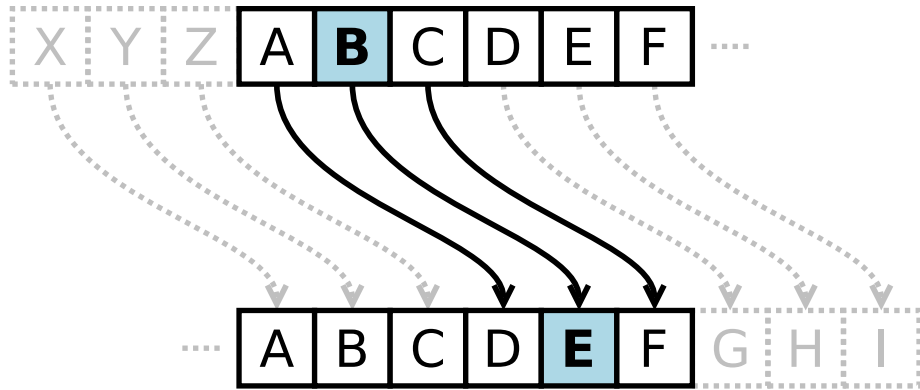
Le chiffre de César

2003-2010 – Science et Vie Junior



Le chiffre de César

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

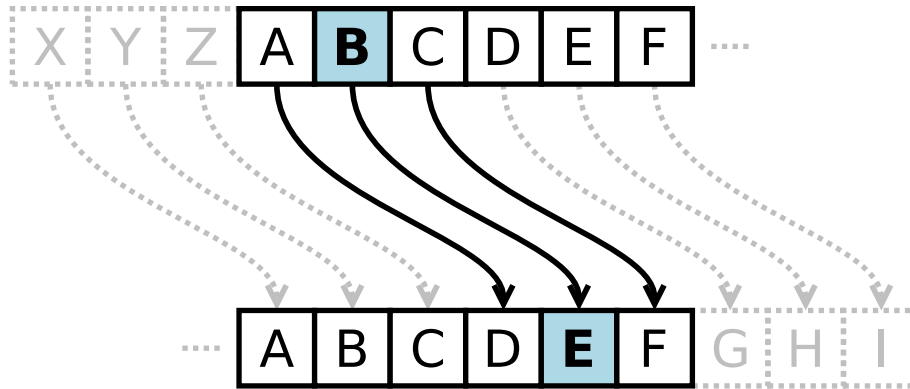


Le chiffre de César

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Le carré de Polybe

2003-2010 – Science et Vie Junior



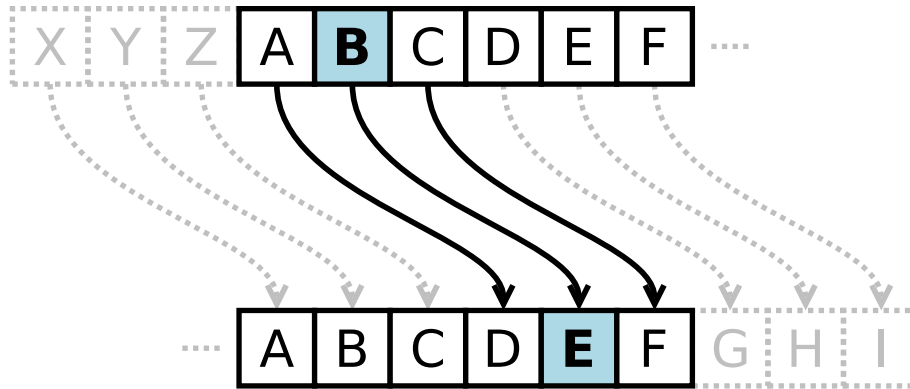
Le chiffre de César

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Le carré de Polybe



2003-2010 – Science et Vie Junior



Le chiffre de César

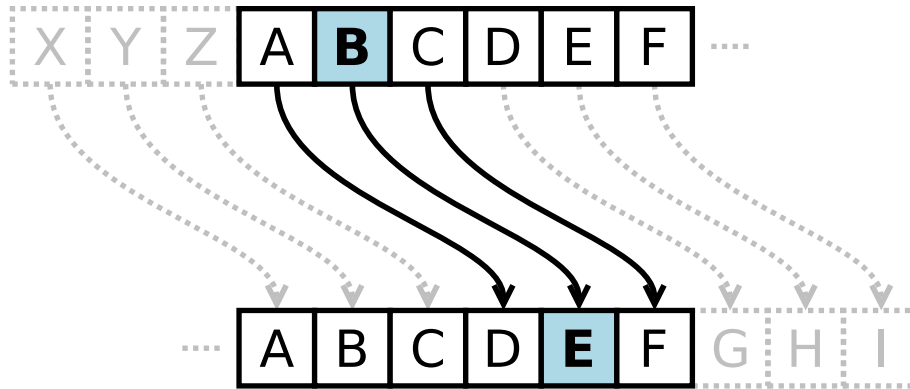
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Le carré de Polybe



Enigma, bien sûr!

2003-2010 – Science et Vie Junior



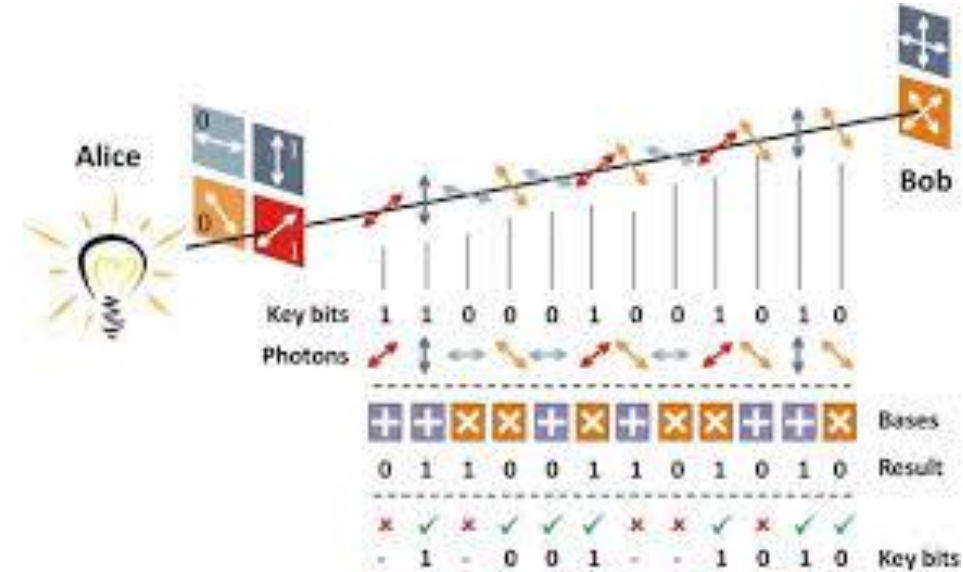
Le chiffre de César

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

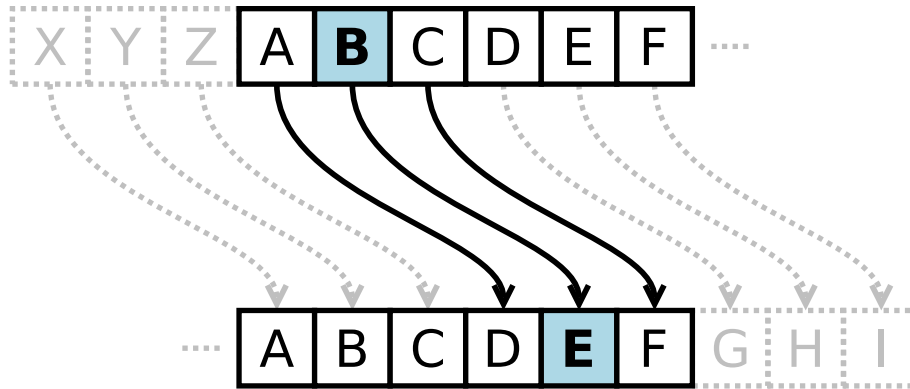
Le carré de Polybe



Enigma, bien sûr!



2003-2010 – Science et Vie Junior



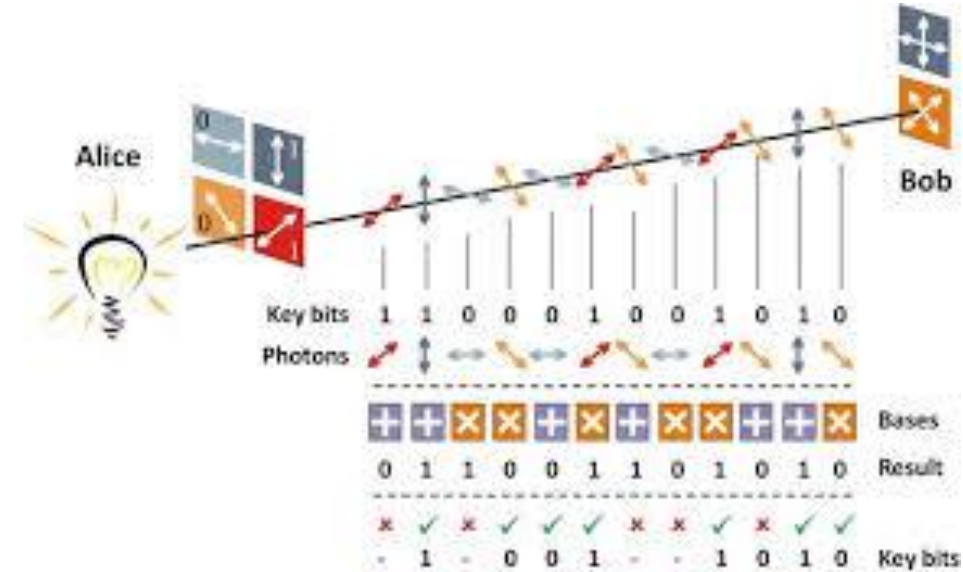
Le chiffre de César

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Le carré de Polybe

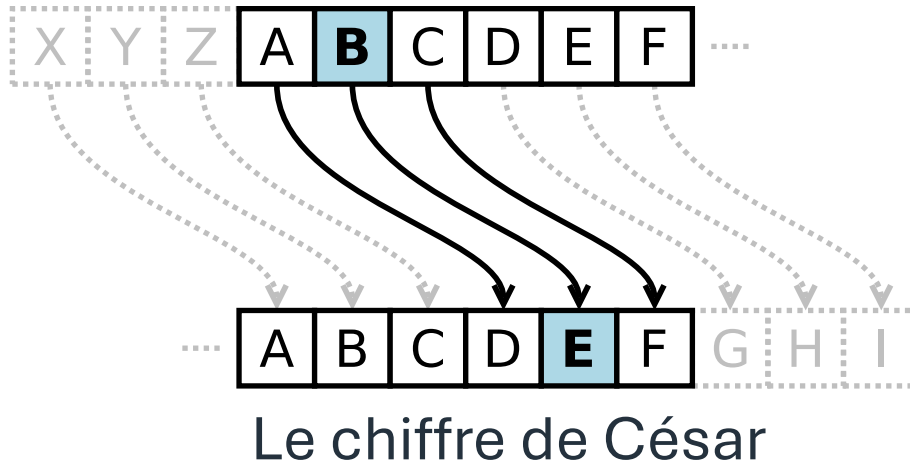


Enigma, bien sûr!



Echange de clés inviolable
[BB84]

2003-2010 – Science et Vie Junior

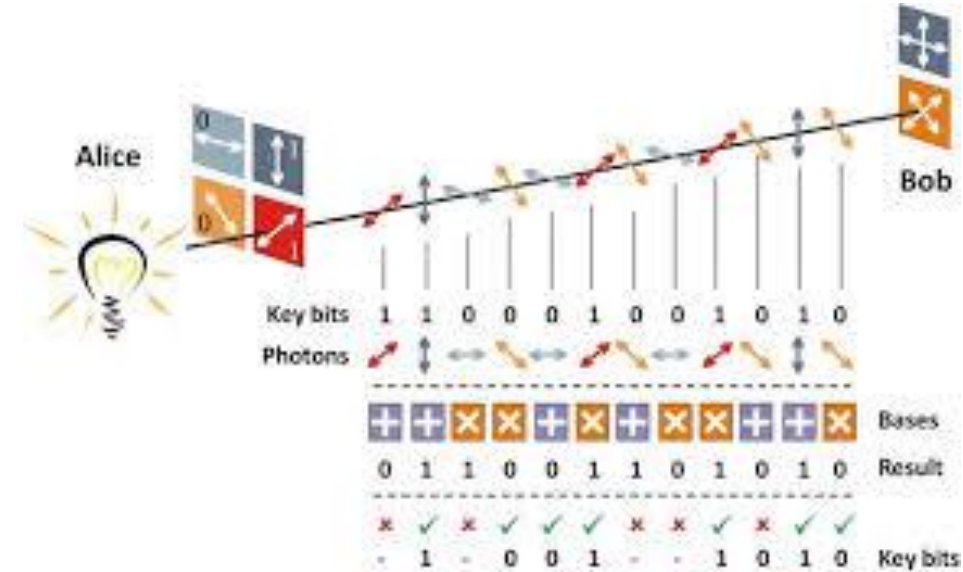


	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Le carré de Polybe



Enigma, bien sûr!



Echange de clés inviolable
[BB84]

RSA est sûr parce que

$p \times q \rightarrow N$ facile

$N \rightarrow p \times q$ difficile

2003-2010 – Science et Vie Junior

- 15 ans, premier contact avec la recherche
 - Première version simple

Algorithm 1: N , entier à factoriser

```
1:  $p \leftarrow \lfloor \sqrt{N} \rfloor$ 
2:  $q \leftarrow \lfloor \sqrt{N} \rfloor$ 
3: while  $p \times q \neq N$  do
4:   if  $p \times q > N$  then
5:      $p \leftarrow p - 1$ 
6:   else if  $p \times q < N$  then
7:      $q \leftarrow q + 1$ 
8:   end if
9: end while
```

2003-2010 – Science et Vie Junior

- 15 ans, premier contact avec la recherche
 - Première version simple
- Algorithme efficace?

Algorithm 1: N , entier à factoriser

```
1:  $p \leftarrow \lfloor \sqrt{N} \rfloor$ 
2:  $q \leftarrow \lfloor \sqrt{N} \rfloor$ 
3: while  $p \times q \neq N$  do
4:   if  $p \times q > N$  then
5:      $p \leftarrow p - 1$ 
6:   else if  $p \times q < N$  then
7:      $q \leftarrow q + 1$ 
8:   end if
9: end while
```

2003-2010 – Science et Vie Junior

- 15 ans, premier contact avec la recherche
 - Première version simple
- Algorithme efficace?
 - Linéaire en N 😊

Algorithm 1: N , entier à factoriser

```
1:  $p \leftarrow \lfloor \sqrt{N} \rfloor$ 
2:  $q \leftarrow \lfloor \sqrt{N} \rfloor$ 
3: while  $p \times q \neq N$  do
4:   if  $p \times q > N$  then
5:      $p \leftarrow p - 1$ 
6:   else if  $p \times q < N$  then
7:      $q \leftarrow q + 1$ 
8:   end if
9: end while
```

2003-2010 – Science et Vie Junior

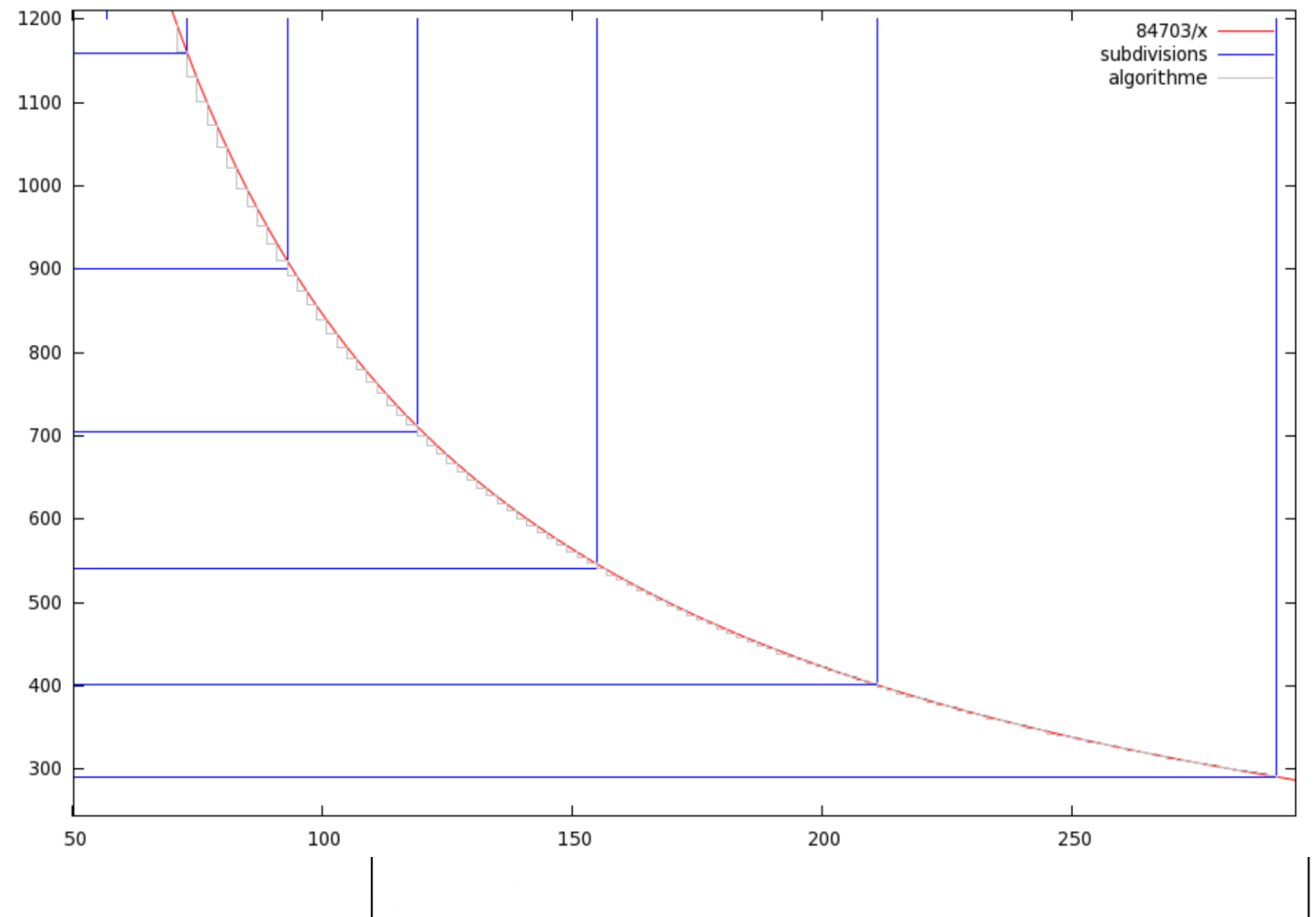
- 15 ans, premier contact avec la recherche
 - Première version simple
- Algorithme efficace?
 - Linéaire en N 😊
 - Exponentiel en la taille de N 😞

Algorithm 1: N , entier à factoriser

```
1:  $p \leftarrow \lfloor \sqrt{N} \rfloor$ 
2:  $q \leftarrow \lfloor \sqrt{N} \rfloor$ 
3: while  $p \times q \neq N$  do
4:   if  $p \times q > N$  then
5:      $p \leftarrow p - 1$ 
6:   else if  $p \times q < N$  then
7:      $q \leftarrow q + 1$ 
8:   end if
9: end while
```

2003-2010 – Science et Vie Junior

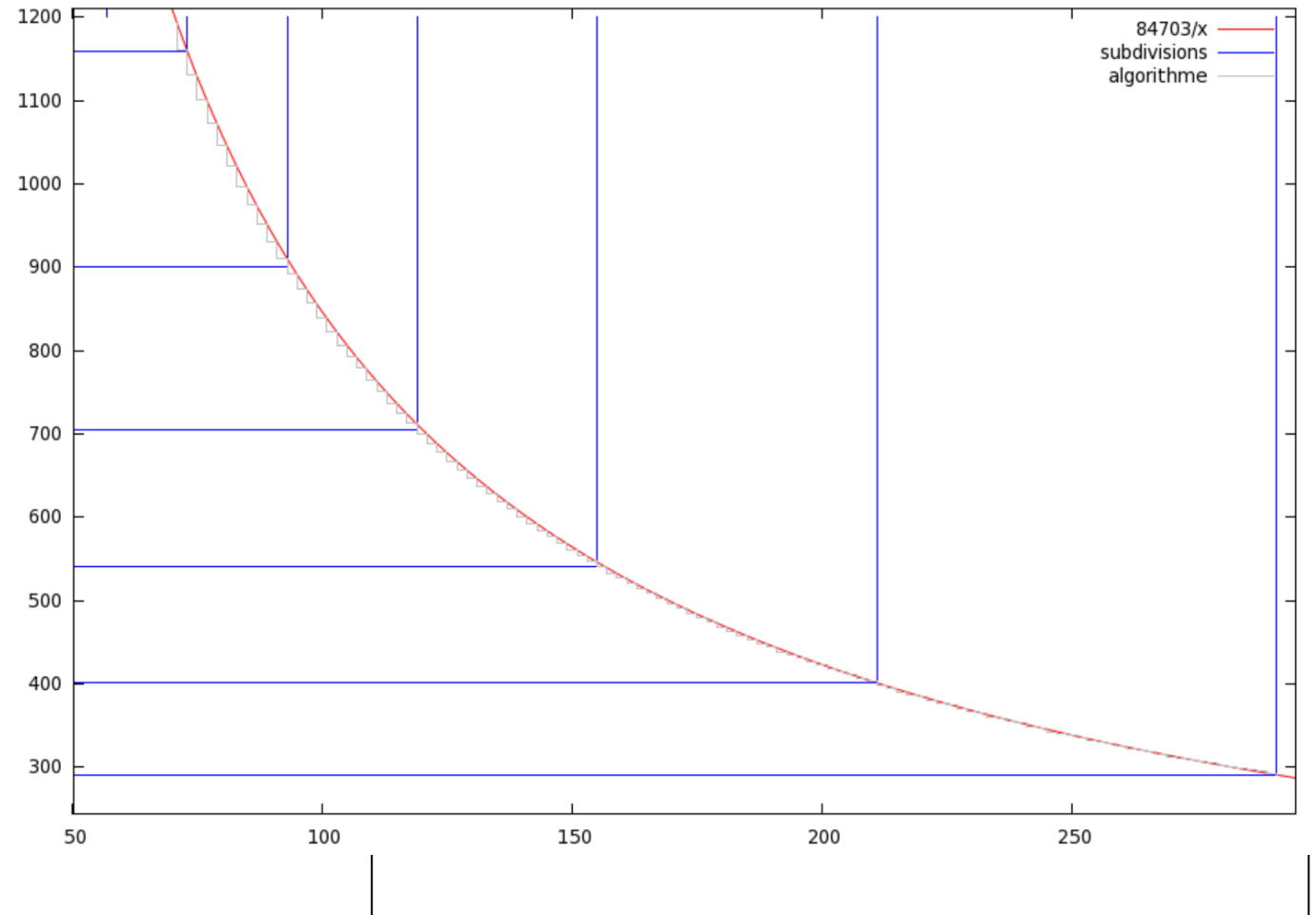
- 15 ans, premier contact avec la recherche
 - Première version simple
 - Version parallélisée en classe prépa
- Algorithme efficace?
 - Linéaire en N 😊
 - Exponentiel en la taille de N 😞



2003-2010 – Science et Vie Junior

- 15 ans, premier contact avec la recherche
 - Première version simple
 - Version parallélisée en classe prépa
- Algorithme efficace?
 - Linéaire en N 😊
 - Exponentiel en la taille de N 😞

Hash basé sur le mélange d'un Rubik's Cube

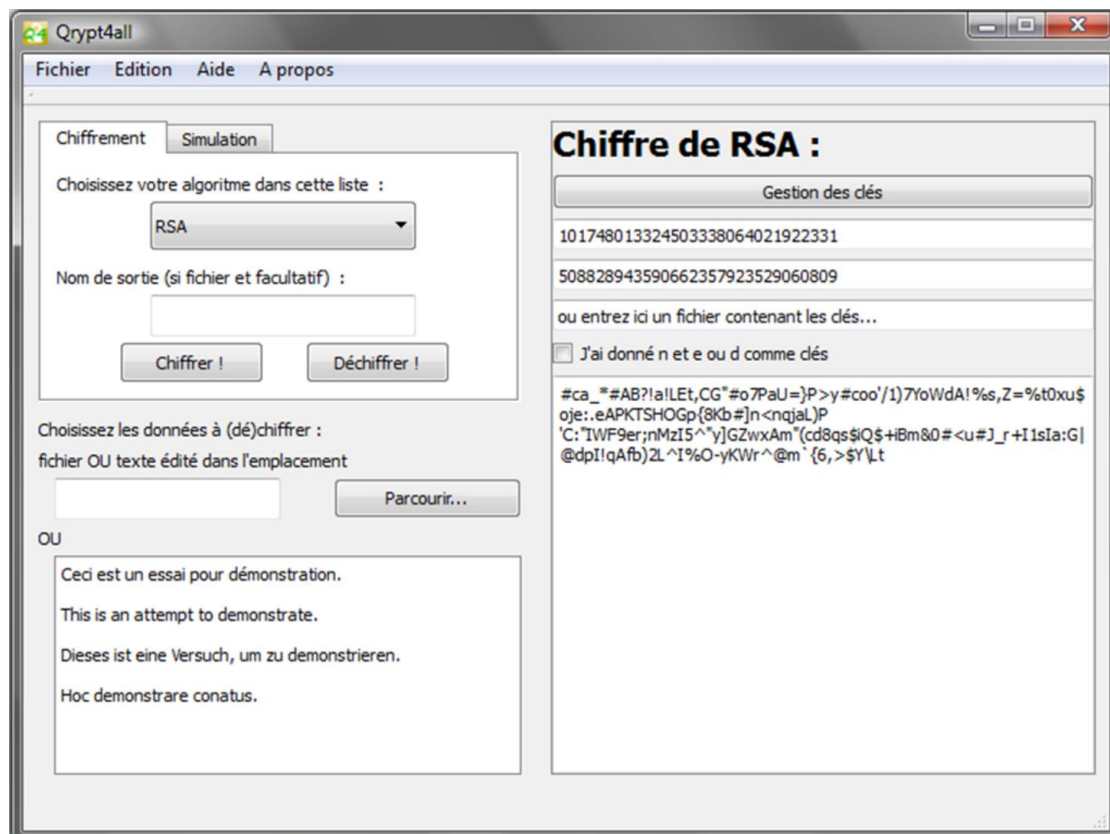


| 2010-2013 – Télécom Bretagne

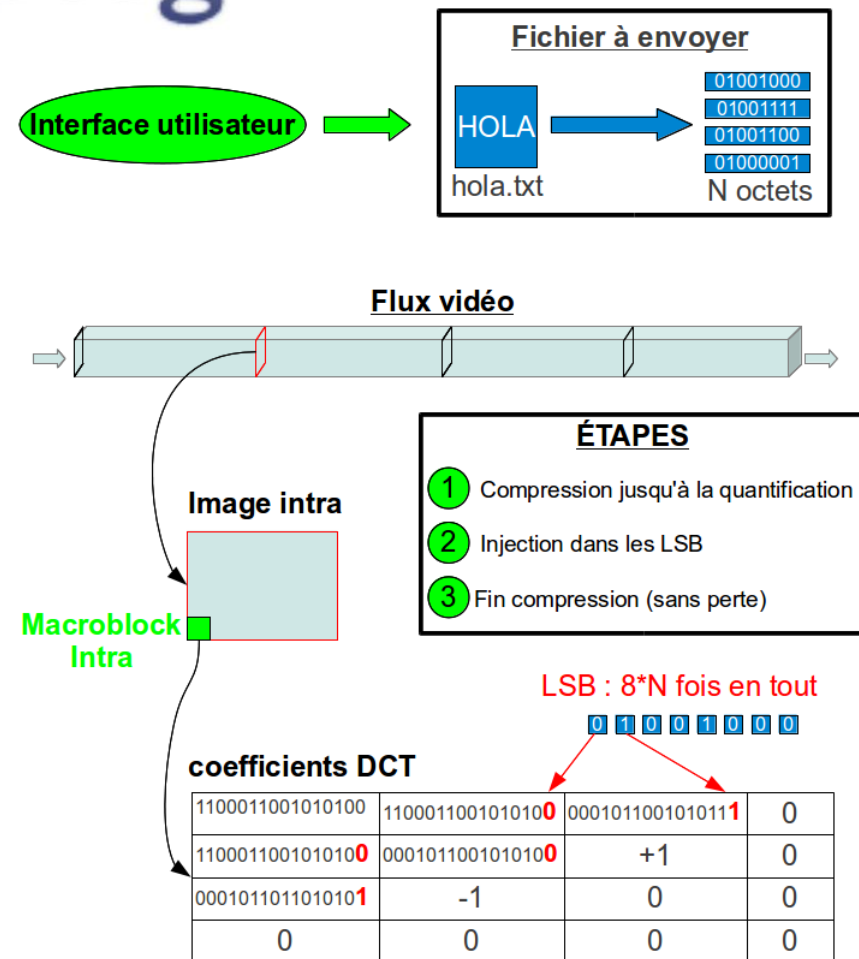
2010-2013 – Télécom Bretagne



2010-2013 – Télécom Bretagne



VisiSteg



2015-2018 – Chaire Cyber Navale

– S4 –

Protection des données en environnement naval
sur les bus et dans les systèmes embarqués

Guillaume Bonnoron

2 décembre 2016
4ème journée scientifique – Brest

2015-2018 – Chaire Cyber Navale

– S4 –

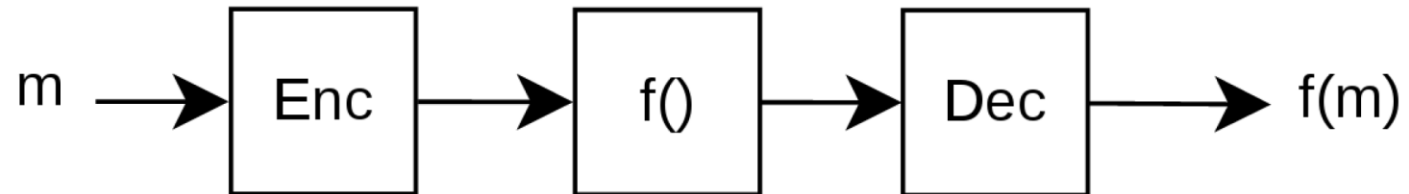
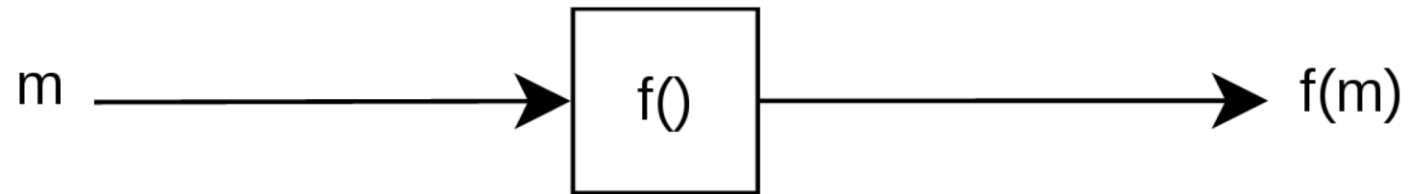
Protection des données en environnement naval
sur les bus et dans les systèmes embarqués

Guillaume Bonnoron

2 décembre 2016
4ème journée scientifique – Brest

- ▶ La cryptographie homomorphe (*FHE*)
→ Mettre le focus sur cet aspect, le plus avancé
- ▶ L'obfuscation de programmes (*méthodes proches FHE*)
→ Travail de second plan, ponctuel
- ▶ Multi-niveau de communication sur canal physique unique
→ Conclure par un rapport de recherche

FHE – Fully Homomor... quoi ?



FHE (*Fully homomorphic encryption*) = pas de contraintes sur f

Imaginé en 1978, réalisé en 2009.

Schémas étudiés, à base de réseaux (*lattices*)

2015-2018 – Chaire Cyber Navale

2015-2018 – Chaire Cyber Navale

Début de thèse en avril 2015.

- ▶ septembre 2015: Premiers résultats avec la nouvelle attaque
- ▶ octobre 2015: Présentation à C2
- ▶ mars 2016: Attaque bien maîtrisée, limitations comprises
- ▶ avril 2016: <https://eprint.iacr.org/2016/385>
- ▶ juin 2016: fp111 days #1 (L. Ducas)
- ▶ juillet 2016: Présentation à WHEAT
- ▶ août 2016: Attaque finalement très limitée
- ▶ décembre 2016: fp111 days #2 (L. Ducas)

Invitation au C.W.I. par L. Ducas (printemps 2017)

2015-2018 – Chaire Cyber Navale

Début de thèse en avril 2015

- ▶ septembre
- ▶ octobre 2015
- ▶ mars 2016:
- ▶ avril 2016:
- ▶ juin 2016:
- ▶ juillet 2016
- ▶ août 2016:
- ▶ décembre 2016

Invitation au C.

Papier avec Vincent Migliore, avril-septembre 2016

→ <https://hal.archives-ouvertes.fr/hal-01394362v1>

Determination and exploration of practical parameters for the latest *Somewhat* Homomorphic Encryption (SHE) Schemes.

Vincent Migliore*, Guillaume Bonnoron†

*Université Bretagne Sud, vincent.migliore@univ-ubs.fr

†Chair of Naval Cyber Defense, guillaume.bonnoron@ecole-navale.fr

Table 5: Parameters size for FV and SHIELD, where λ is the security level and L the multiplicative depth. Binary key, $\sigma_{err} = 2\sqrt{n}$.

(a) FV

L	$\lambda = 80$ bits				$\lambda = 128$ bits			
	$\omega = 32$ bits		$\omega = 64$ bits		$\omega = 32$ bits		$\omega = 64$ bits	
	C, P_{key}	γ	C, P_{key}	γ	C, P_{key}	γ	C, P_{key}	γ
5	121.4 KB	607 KB	181.1 KB	543.3 KB	165.8 KB	994.8 KB	245.2 KB	1 MB
10	442.5 KB	4.3 MB	552.8 KB	3.2 MB	613.9 KB	6 MB	758.4 KB	4.4 MB
15	999.5 KB	13.7 MB	1.1 MB	9 MB	1.4 MB	20.3 MB	1.6 MB	12.5 MB

(b) SHIELD. Optimized circuit.

L	$\lambda = 80$ bits				$\lambda = 128$ bits			
	No batching		Batching		No batching		Batching	
	C	P_{key}	C	P_{key}	C	P_{key}	C	P_{key}
5	488.6 KB	6.4 KB	5.2 MB	32.3 KB	667.7 KB	8.6 KB	7.4 MB	44.3 KB
10	531 KB	6.8 KB	30 MB	105.1 KB	721.1 KB	9 KB	43 MB	145.9 KB
15	575 KB	7.2 KB	94.8 MB	226.8 KB	777.3 KB	9.5 KB	136.6 MB	316.5 KB

→ Benchmark de schémas en 2017

2015-2018 – Chaire Cyber Navale

Début de thèse en avril 2015

- ▶ septembre
- ▶ octobre 2015
- ▶ mars 2016:
- ▶ avril 2016:
- ▶ juin 2016:
- ▶ juillet 2016
- ▶ août 2016:
- ▶ décembre 2016

Invitation au C.

Papier avec Vincent Migliore avril septembre 2016

→ <https://hal.archives-ouvertes.fr/hal-01171111>

Determination and exploration of parameters for the latest *Somewhat* Homomorphic Encryption (SHE) Schemes.

Vincent Migliore*, Guillaume Bonnoron†

*Université Bretagne Sud, vincent.migliore@univ-ubs.fr

†Chair of Naval Cyber Defense, guillaume.bonnoron@ecole-navale.fr

Détails

- ▶ Du 1er mars au 30 mai
- ▶ Collaboration avec Léo Ducas et Max Fillinger
- ▶ Nouveau schéma homomorphe
 - ▶ Contribution théorique (Léo et Max)
 - ▶ Implémentation (Guillaume)

Valorisations

- ▶ Pre-print : <https://ia.cr/2017/996>
- ▶ Soumis à PKC 2017 (verdict le 15 décembre)
- ▶ Implémentation libre : <https://github.com/gbonnoron/Borogrove>

→ Doctorat à label européen possible !

→ Benchmark de schéma

2015-2018 – Chaire Cyber Navale

Début de thèse en avril 2015

- ▶ septembre
- ▶ octobre 2015
- ▶ mars 2016:
- ▶ avril 2016:
- ▶ juin 2016:
- ▶ juillet 2016
- ▶ août 2016:
- ▶ décembre 2016

Invitation au C.

Papier avec Vincent Migliore, avril 2016

→ <https://hal.archives-ouvertes.fr/hal-01121111>

Determination and exploration of parameters for the latest *Somewhat Homomorphic* Encryption (SHE) Schemes.

Vincent Migliore*, Guillaume Bonnoron†

*Université Bretagne Sud, vincent.migliore@univ-ubs.fr

†Chair of Naval Cyber Defense, guillaume.bonnoron@ecole-navale.fr

→ Benchmark de schéma

Début de la compétition NIST
en février 2016

Détails

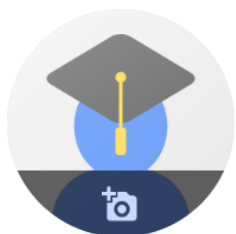
- ▶ Du 1er mars au 30 mai
- ▶ Collaboration avec Léo Ducas et Max Fillinger
- ▶ Nouveau schéma homomorphe
 - ▶ Contribution théorique (Léo et Max)
 - ▶ Implémentation (Guillaume)

Valorisations

- ▶ Pre-print : <https://ia.cr/2017/996>
- ▶ Soumis à PKC 2017 (verdict le 15 décembre)
- ▶ Implémentation libre :
<https://github.com/gbonnoron/Borogrove>

→ Doctorat à label européen possible !

2015-2018 – Chaire Cyber Navale



Guillaume Bonnoron

Chair of Naval Cyber Defence
Verified email at imt-atlantique.fr

Cybersecurity

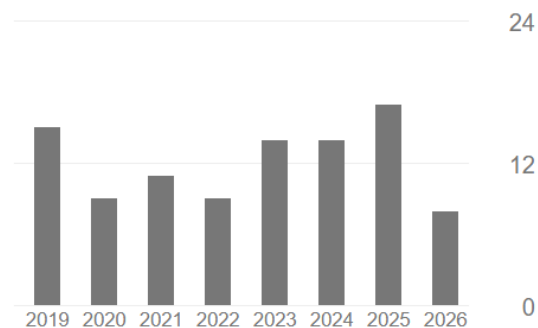


☐	TITLE			CITED BY	YEAR
☐	Large FHE gates from tensored homomorphic accumulator G Bonnoron, L Ducas, M Fillinger International Conference on Cryptology in Africa, 217-251			61	2018
☐	Practical Parameters for <i>Somewhat</i> Homomorphic Encryption Schemes on Binary Circuits V Migliore, G Bonnoron, C Fontaine IEEE Transactions on Computers 67 (11), 1550-1560			22 *	2018
☐	Somewhat/fully homomorphic encryption: Implementation progresses and challenges G Bonnoron, C Fontaine, G Gogniat, V Herbert, V Lapôte, V Migliore, ... International Conference on Codes, Cryptology, and Information Security, 68-82			22	2017
☐	A note on ring-LWE security in the case of fully homomorphic encryption G Bonnoron, C Fontaine International Conference on Cryptology in India, 27-43			11	2017

Cited by

[VIEW ALL](#)

	All	Since 2021
Citations	125	73
h-index	4	3
i10-index	4	3



Public access

[VIEW ALL](#)

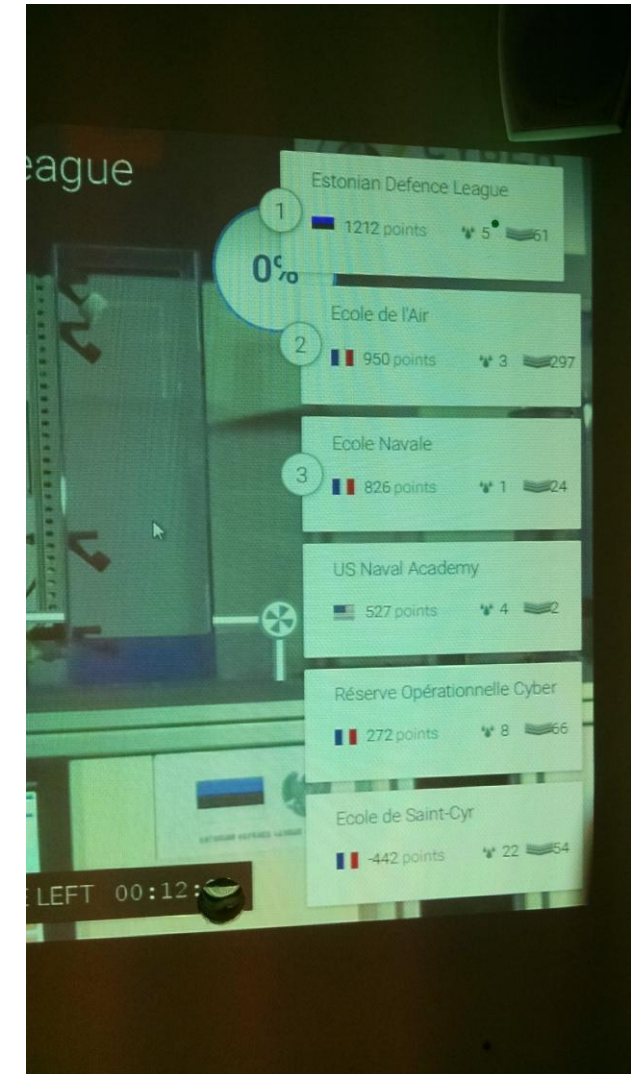
0 articles

2 articles

2015-2018 – Chaire Cyber Navale



2015-2018 – Chaire Cyber Navale

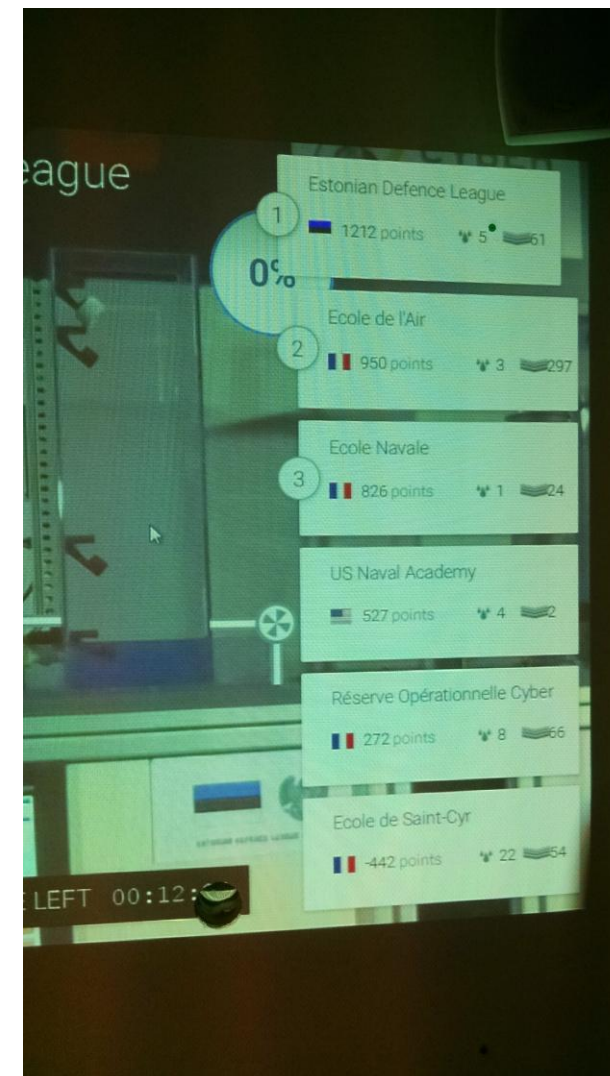


#CyberDef2015

2015-2018 – Chaire Cyber Navale



Challenge CSAW: (pas) qualifié



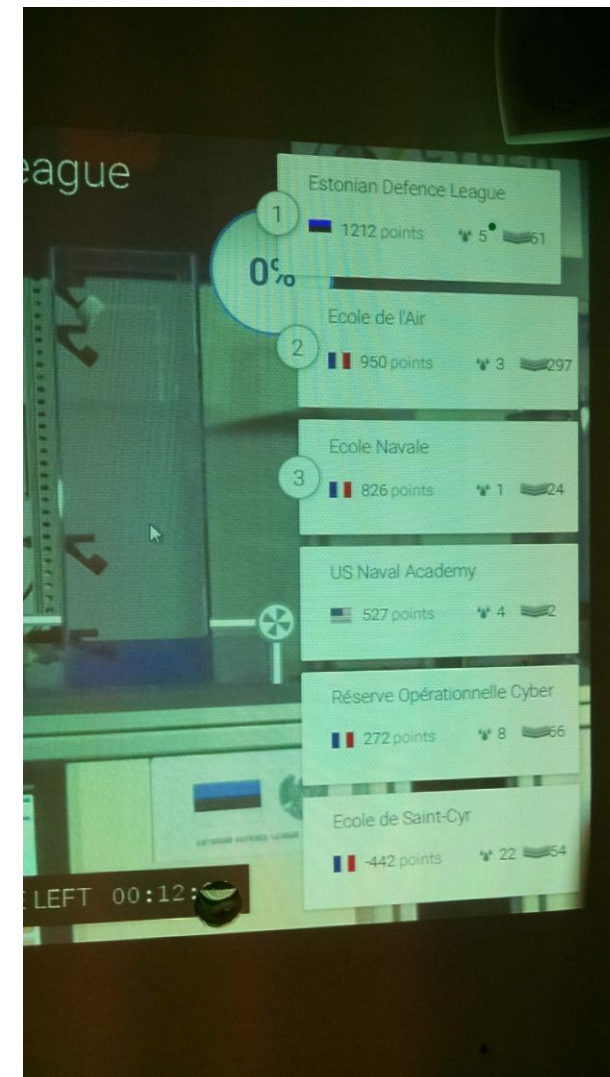
#CyberDef2015

2015-2018 – Chaire Cyber Navale

CyberCamp RCD



Challenge CSAW: (pas) qualifié



#CyberDef2015

Partie 2: Aujourd'hui

- La cryptographie dans une entreprise normale
- Et le post-quantique alors ?

Hilti en bref

- **Leader mondial**, secteur de la construction.
- Fondée en **1941**.
- Environ **34,000 employés** dans le monde
- Activités dans **120 pays, 750 sites**.
- **CHF 6.3 milliards** chiffre d'affaires (2025).



Hilti en bref

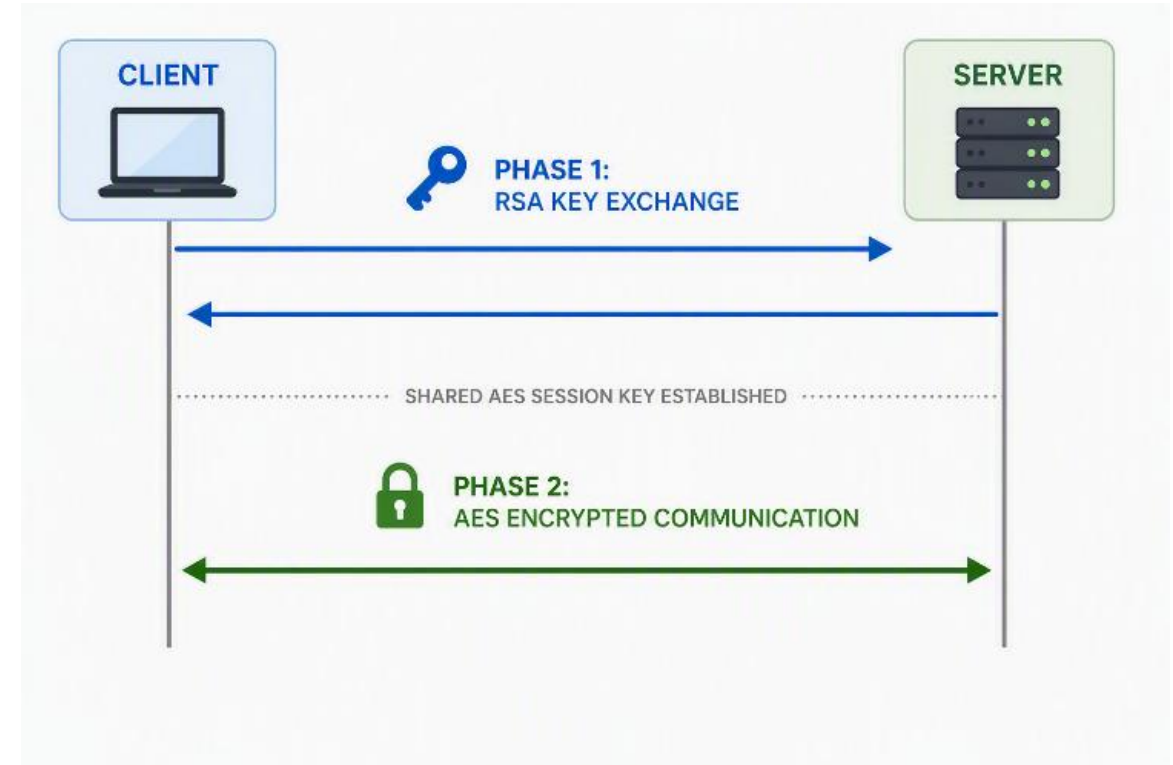
- **Leader mondial**, secteur de la construction.
- Fondée en **1941**.
- Environ **34,000 employés** dans le monde
- Activités dans **120 pays, 750 sites**.
- **CHF 6.3 milliards** chiffre d'affaires (2025).



Et la crypto dans tout ça ?



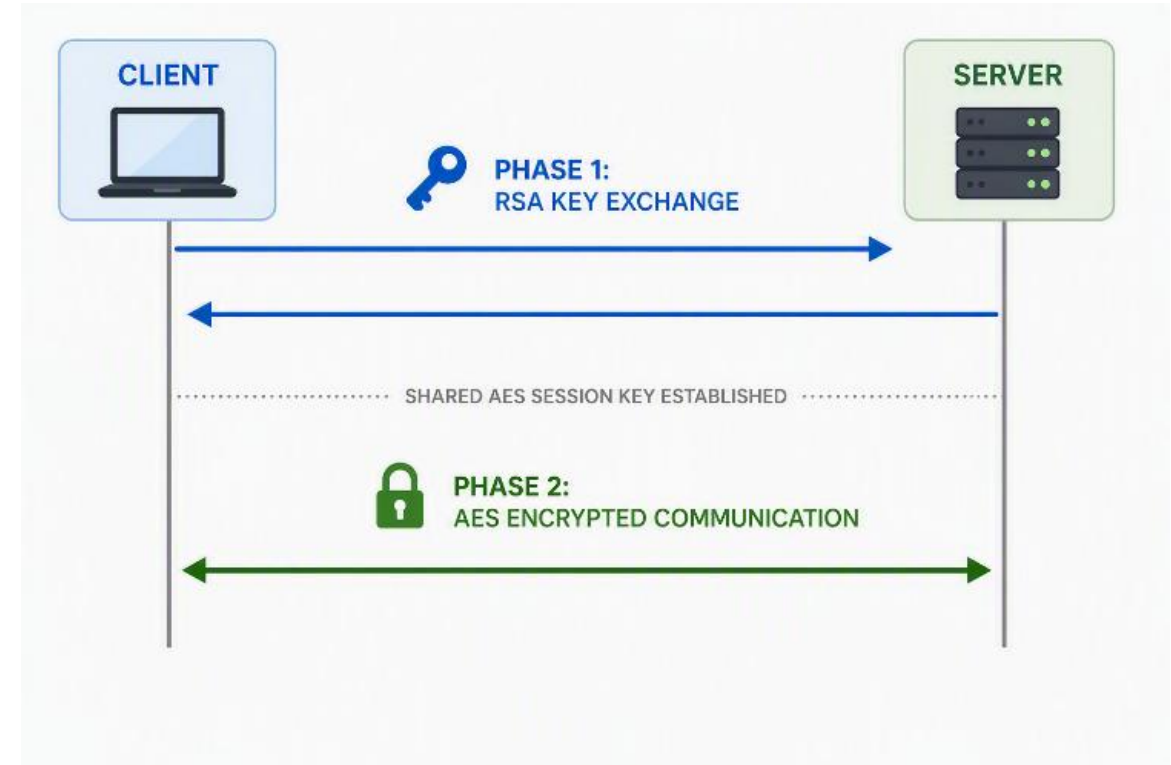
Le cas typique: https (merci E. Snowden !)



Le cas typique: https (merci E. Snowden !)

Pendant la phase 1

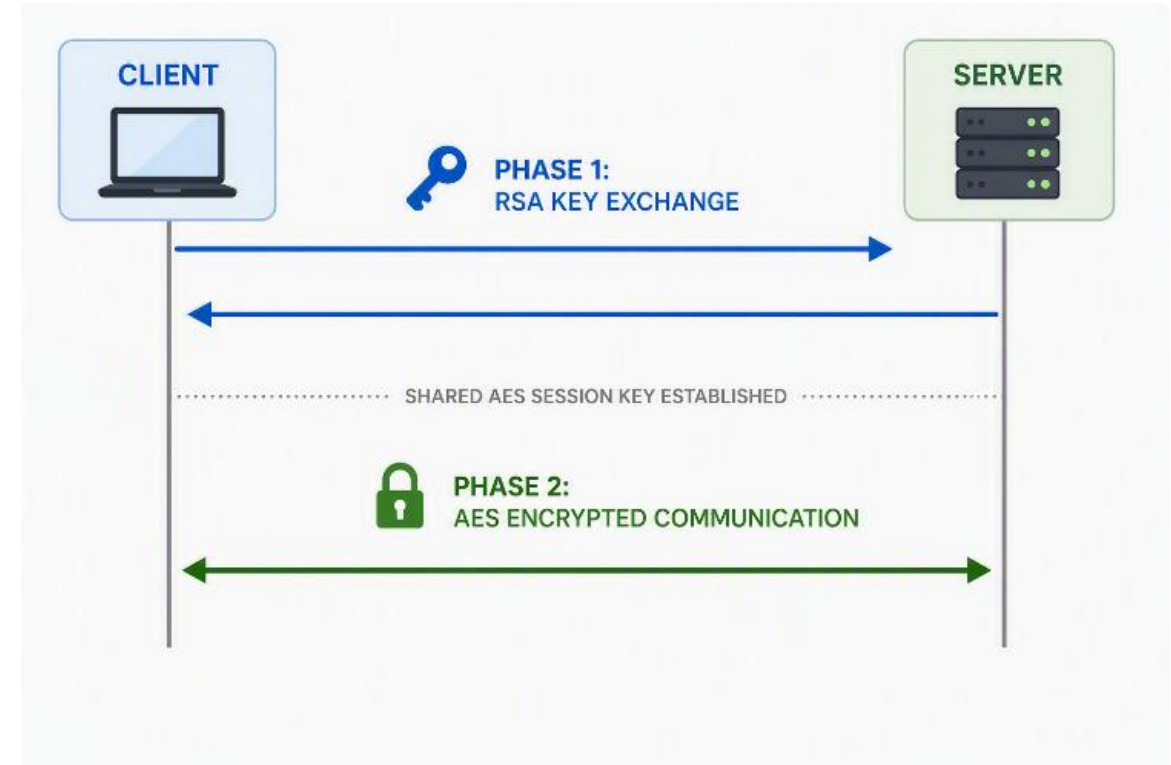
1. Le serveur présente son certificat



Le cas typique: https (merci E. Snowden !)

Pendant la phase 1

1. Le serveur présente son certificat
 - a) Fournit la clé publique au client pour chiffrement

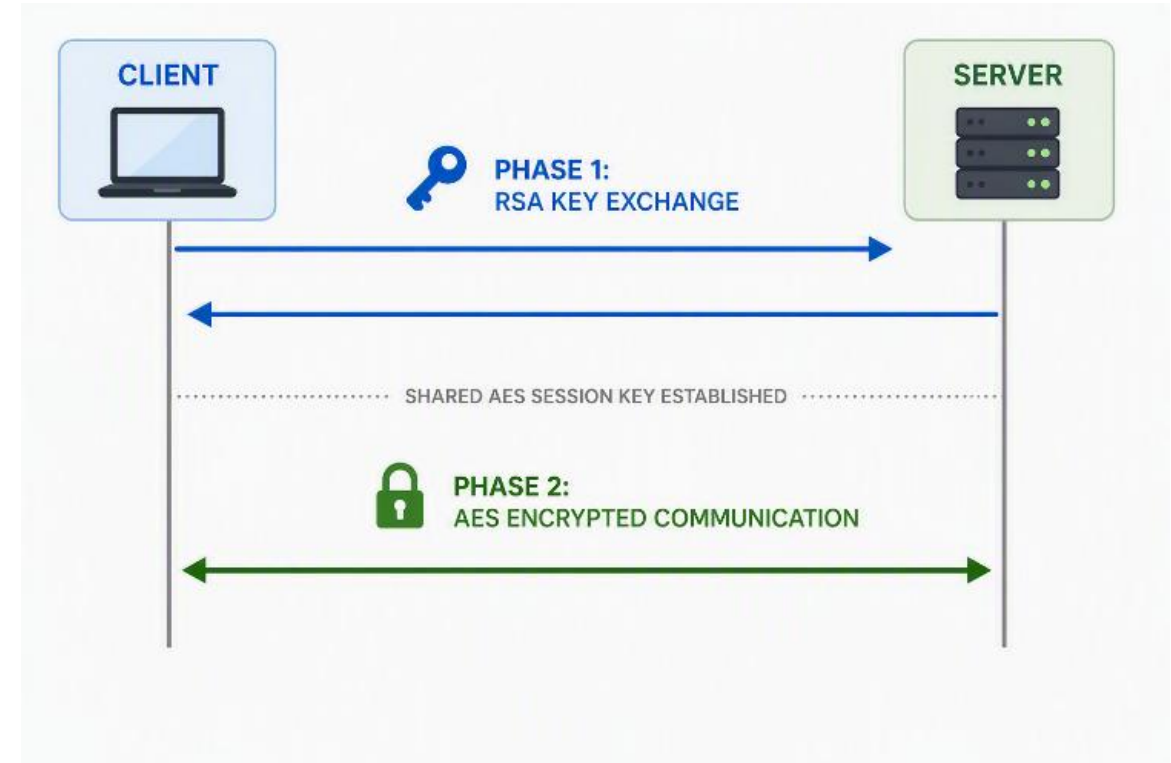


Le cas typique: https (merci E. Snowden !)

Pendant la phase 1

1. Le serveur présente son certificat

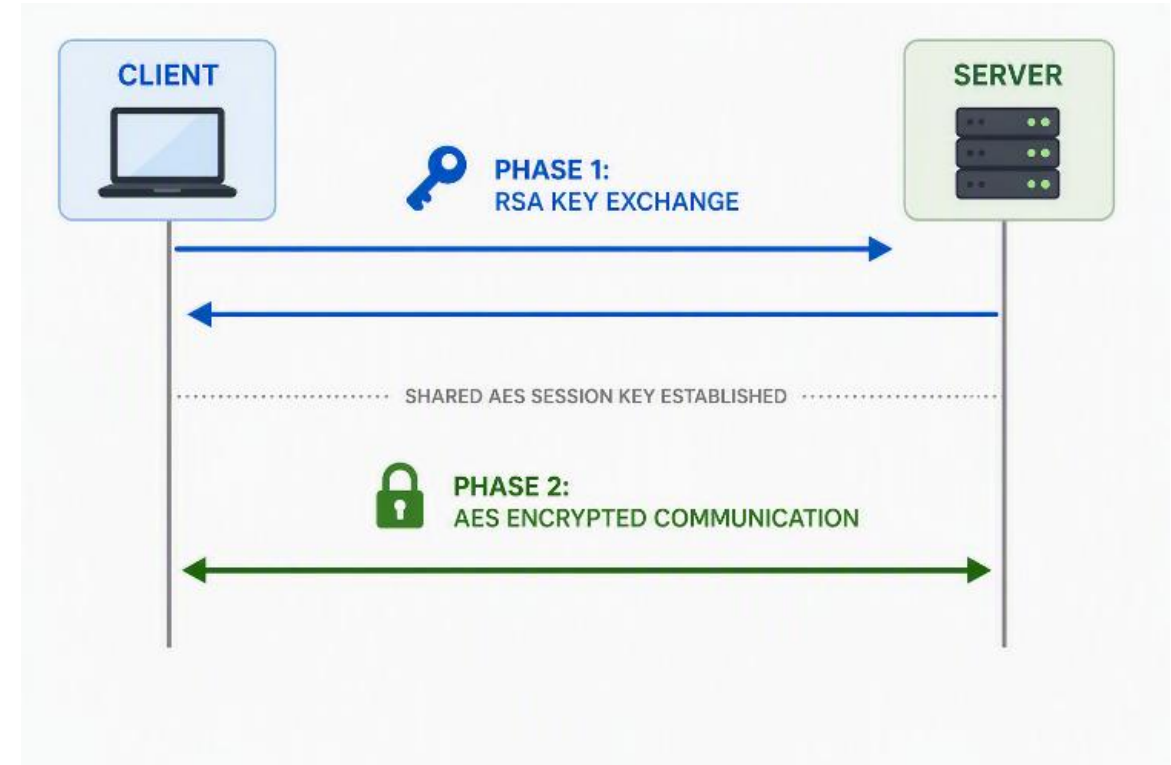
- a) Fournit la clé publique au client pour chiffrement
- b) Prouve son identité grâce à la signature du certificat



Le cas typique: https (merci E. Snowden !)

Pendant la phase 1

1. Le serveur présente son certificat
 - a) Fournit la clé publique au client pour chiffrement
 - b) Prouve son identité grâce à la signature du certificat
2. Client et serveur s'accordent sur la clé à utiliser pour la suite



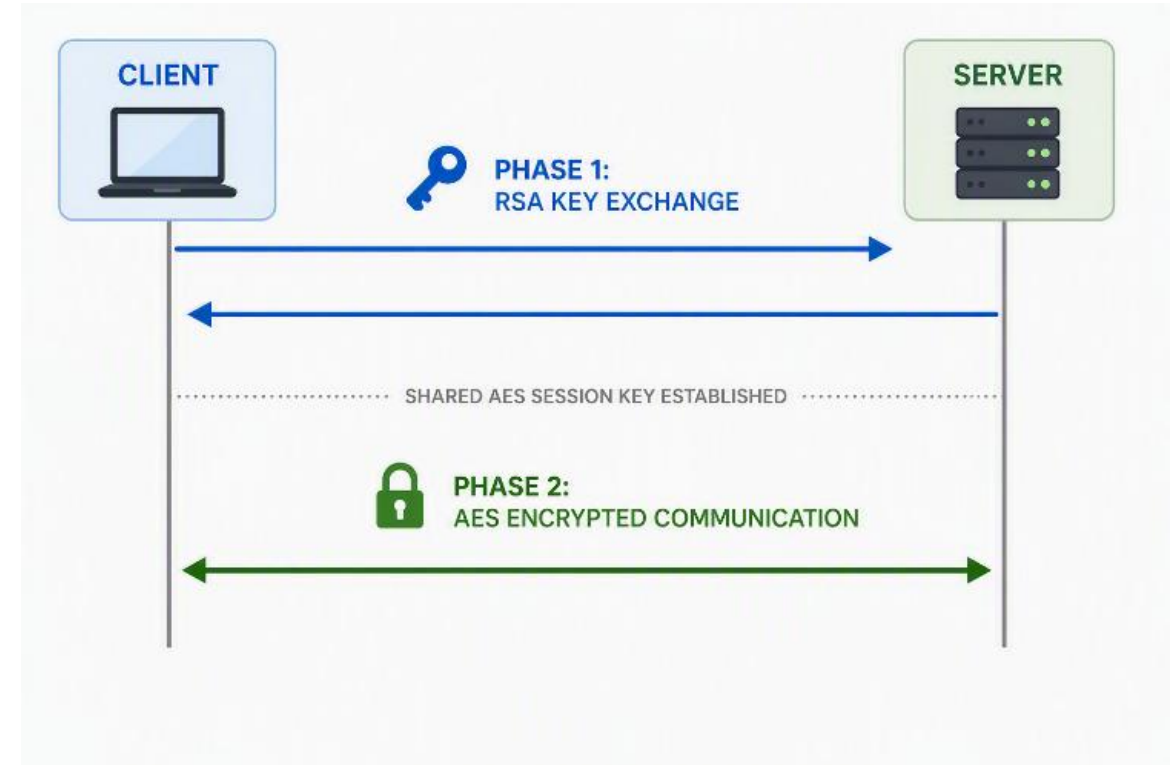
Le cas typique: https (merci E. Snowden !)

Pendant la phase 1

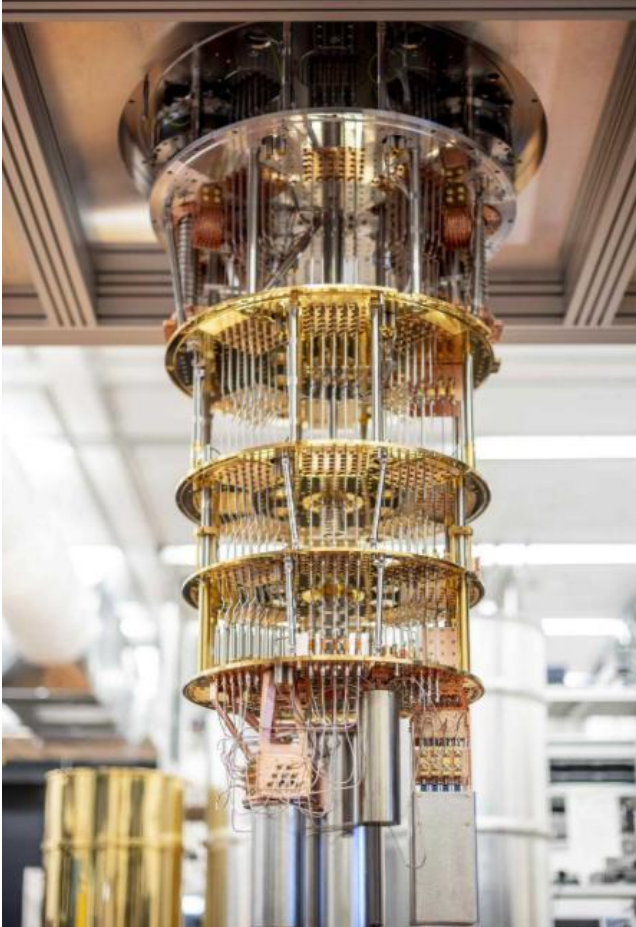
1. Le serveur présente son certificat
 - a) Fournit la clé publique au client pour chiffrement
 - b) Prouve son identité grâce à la signature du certificat
2. Client et serveur s'accordent sur la clé à utiliser pour la suite

Echange de clés (KEM) et signature reposent sur la cryptographie **assymétrique**

Le chiffrement des données qui suit utilise des algorithmes de chiffrement **symétriques**

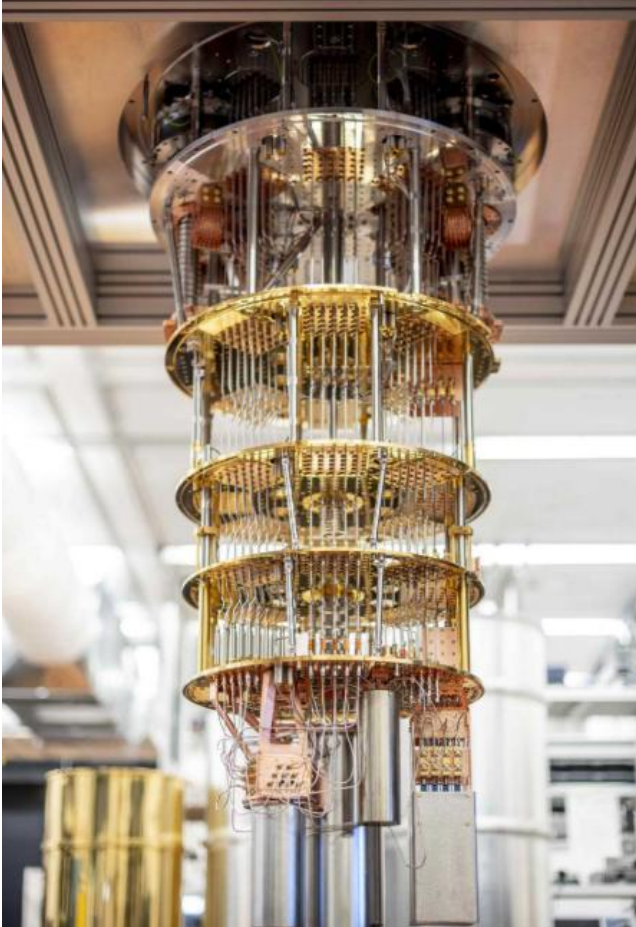


L'ordinateur quantique va tout casser!

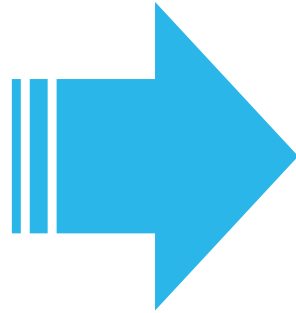


Quantum Lab de l'ETH Zurich

L'ordinateur quantique va tout casser!



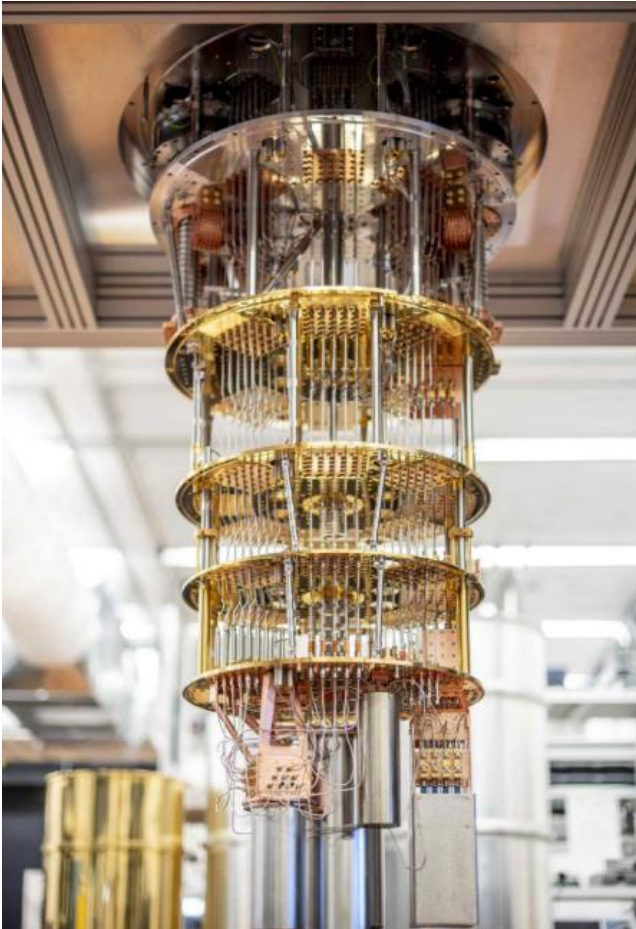
Quantum Lab de l'ETH Zurich



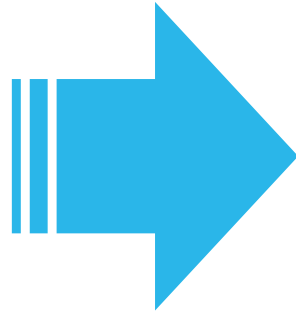
Impact sur la cryptographie symétrique

- L'algorithme de **Grover** apporte une **accélération quadratique** aux attaques sur ordinateur quantique
- **Doubler la taille des clés** compenser ce gain, ie AES-256 offre la même sécurité (contre les attaques quantique) que AES-128 (contre les attaques classiques)

L'ordinateur quantique va tout casser!



Quantum Lab de l'ETH Zurich



Impact sur la cryptographie symétrique

- L'algorithme de **Grover** apporte une **accélération quadratique** aux attaques sur ordinateur quantique
- **Doubler la taille des clés** compenser ce gain, ie AES-256 offre la même sécurité (contre les attaques quantique) que AES-128 (contre les attaques classiques)

Impact sur la cryptographie asymétrique

- L'algorithme de **Shor** apporte une **accélération exponentielle** aux attaques sur ordinateur quantique
- C'est impossible d'adapter la crypto actuelle pour compenser. Il faut inventer une nouvelle crypto: la **cryptographie "post-quantique"**

Oui mais quand ? Et quand agir?

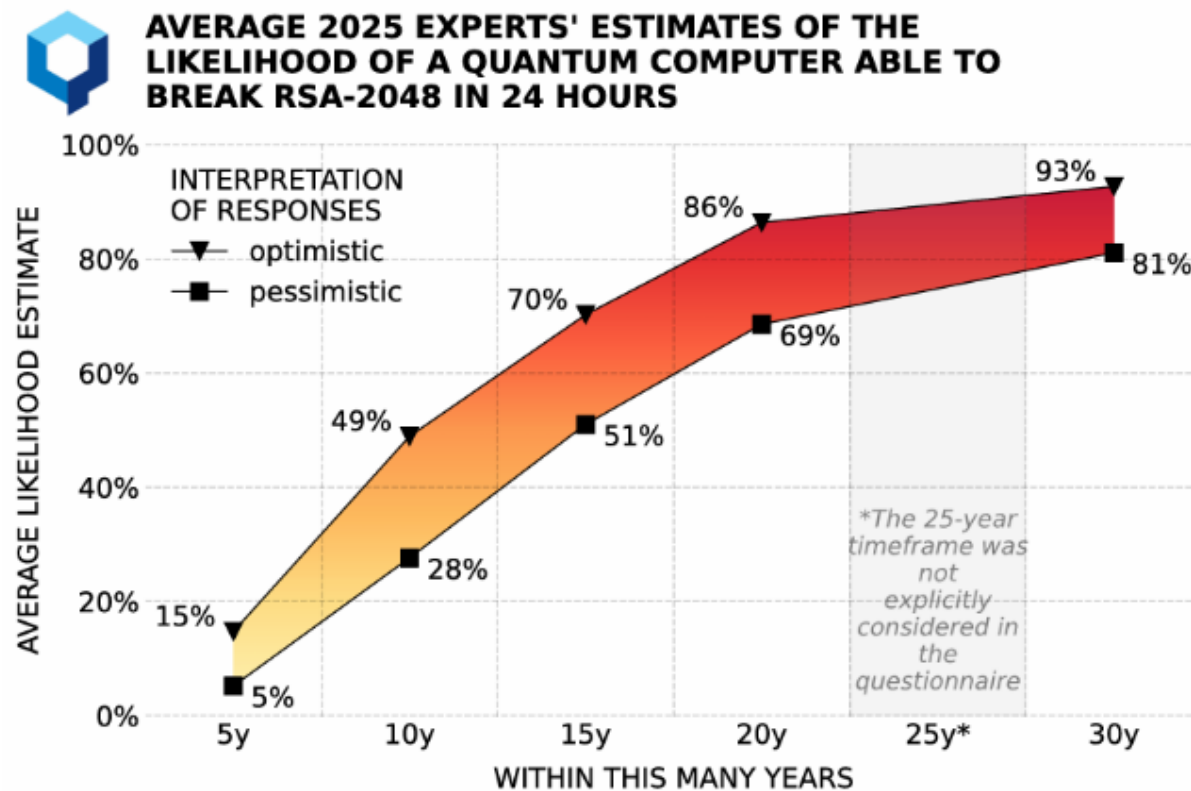


Figure 3 Averaged experts' likelihood estimates by timeframe.

Oui mais quand ? Et quand agir ?

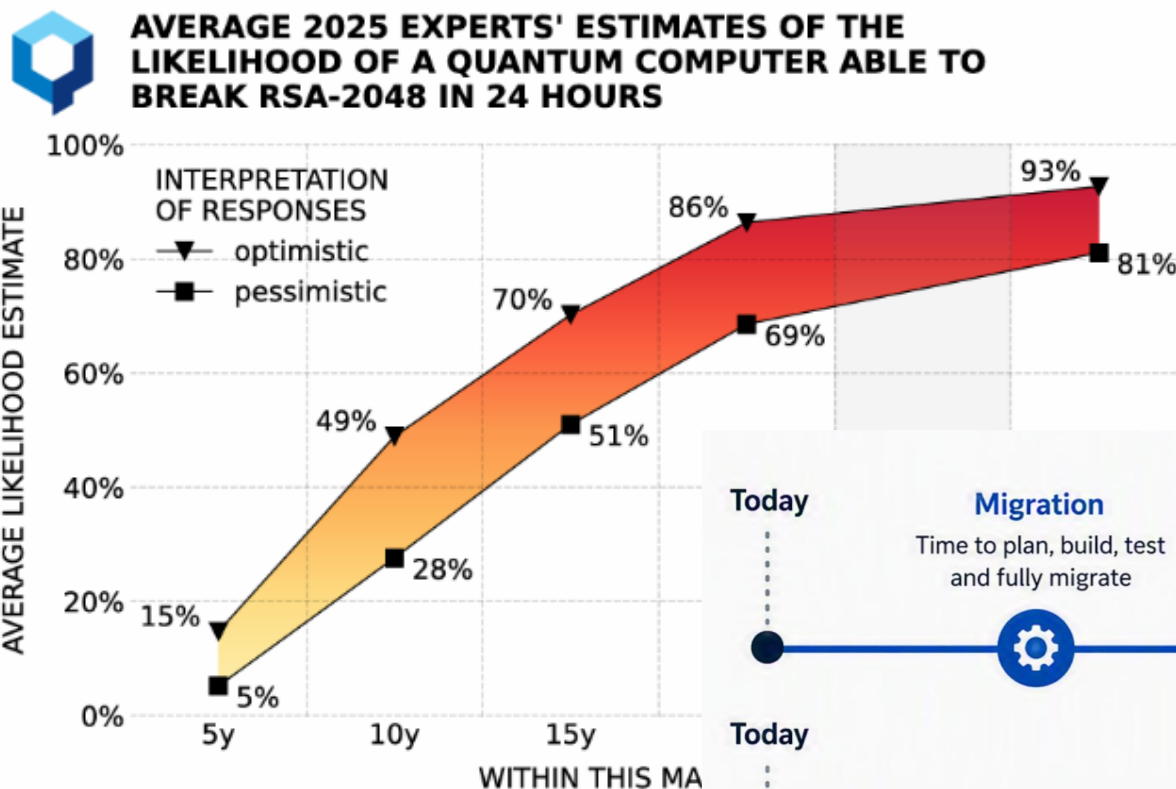
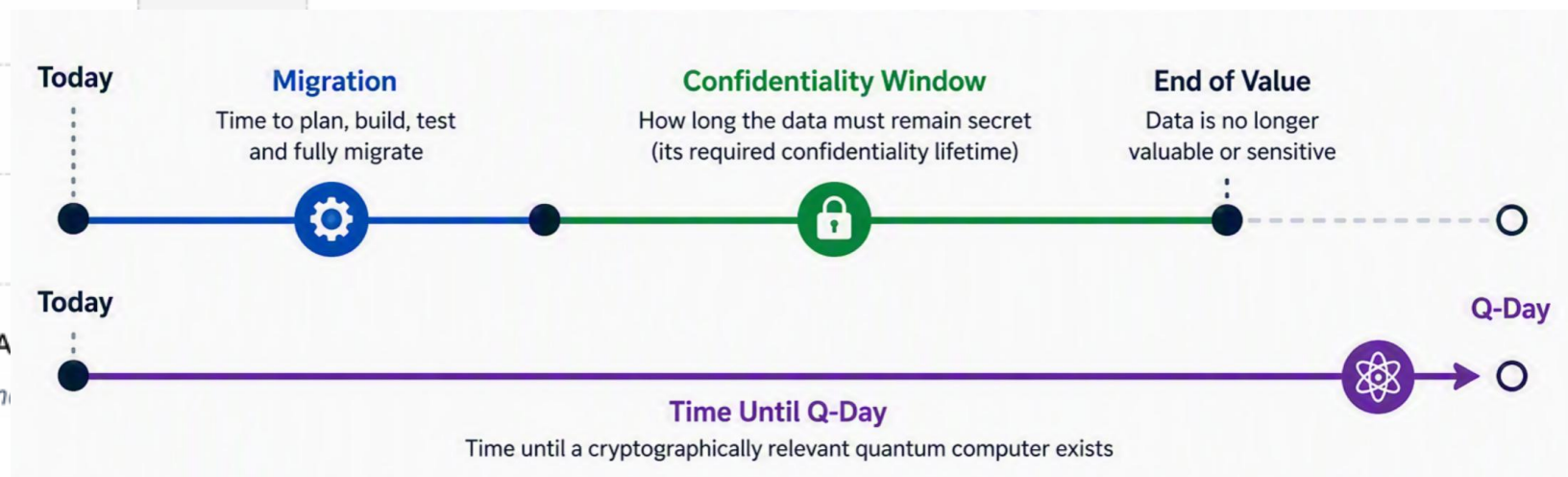


Figure 3 Averaged experts' likelihood estimates by time



Oui mais quand ? Et quand agir ?

Entreprise privée

- Q-Day : dans 30 ans
 - Temps de migration : 5 ans
 - Durée de confidentialité : 5 ans
- ⇒ 20 ans de marge

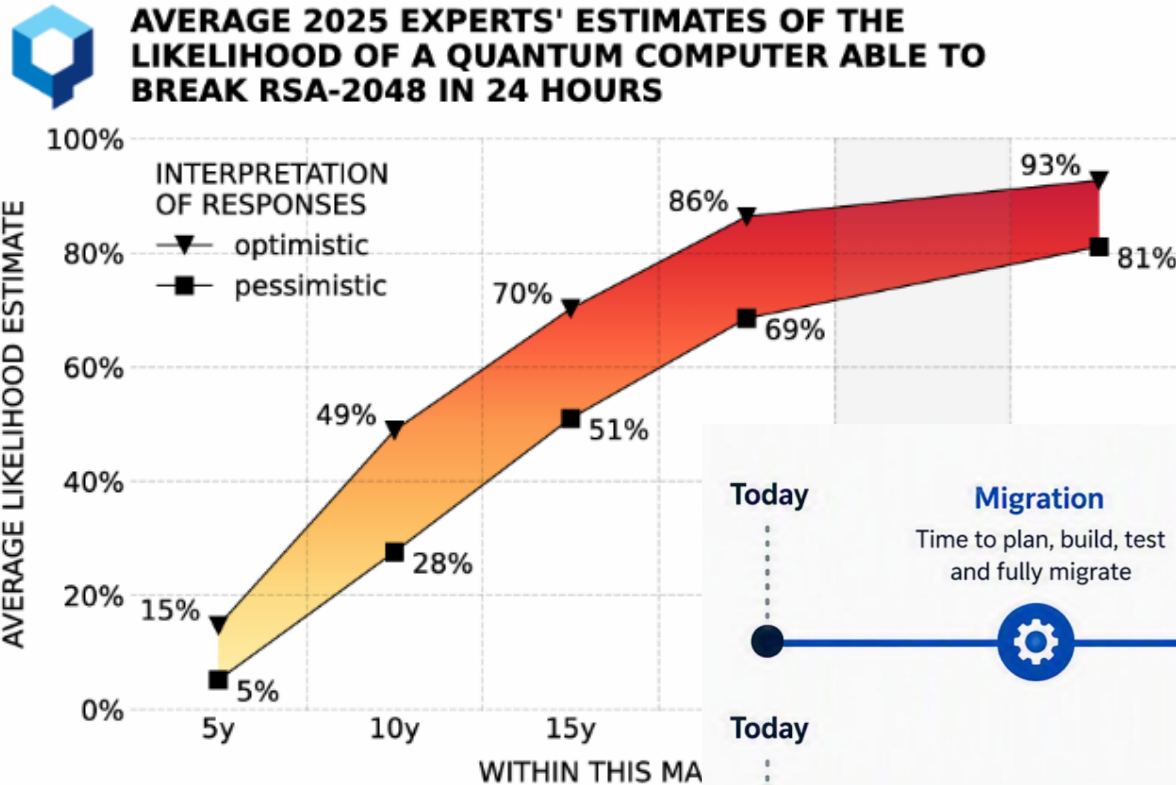
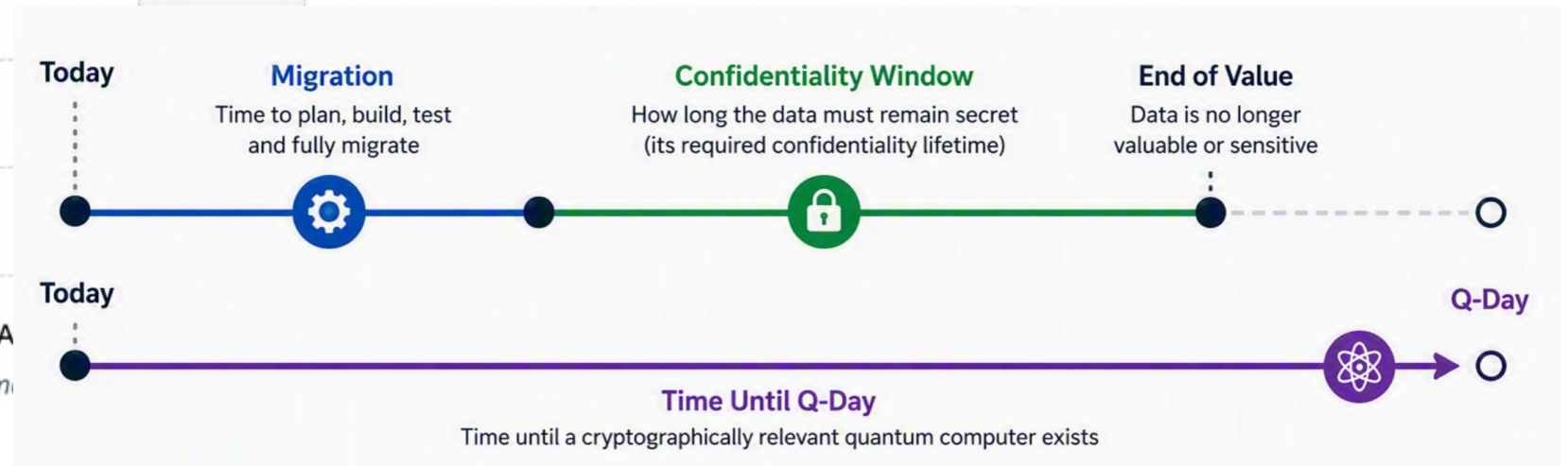


Figure 3 Averaged experts' likelihood estimates by time



Oui mais quand ? Et quand agir ?

Entreprise privée

- Q-Day : dans 30 ans
 - Temps de migration : 5 ans
 - Durée de confidentialité : 5 ans
- ⇒ 20 ans de marge

Organisme étatique

- Q-Day: dans 10 ans
 - Temps de migration : 2 ans
 - Durée de confidentialité : 20 ans
- ⇒ Déjà trop tard!

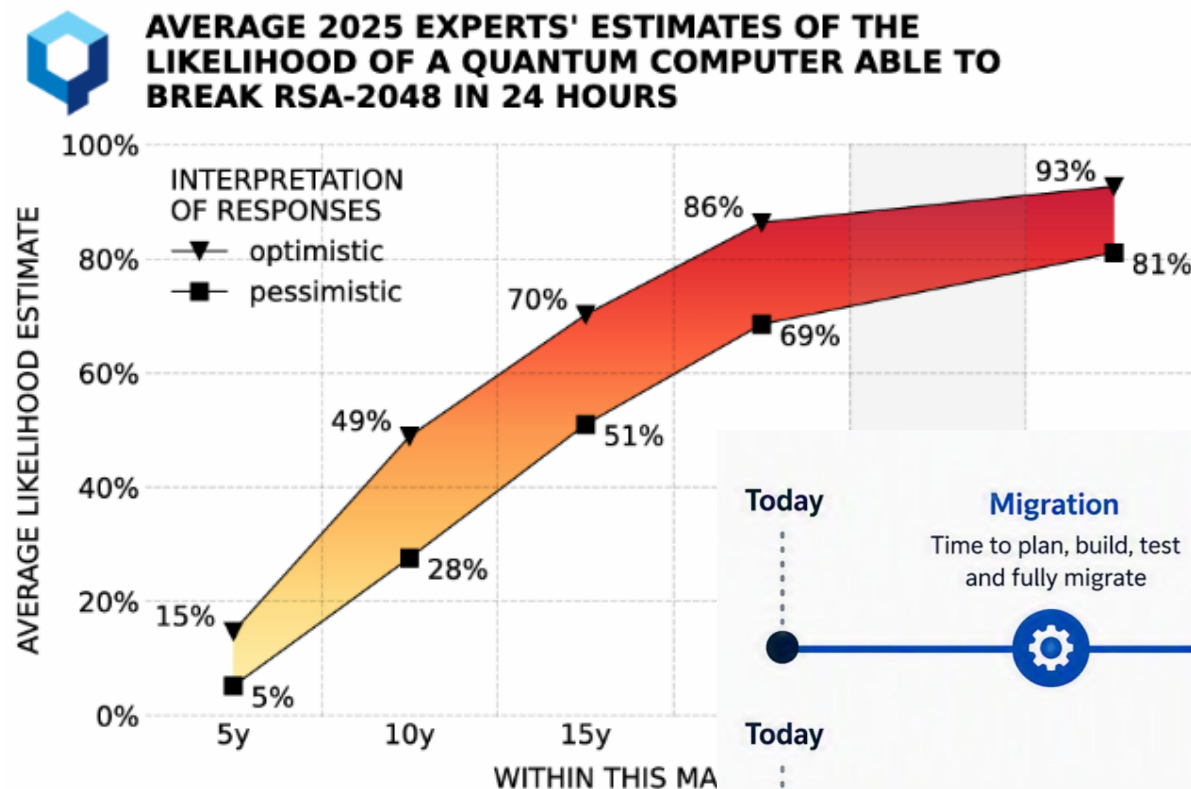
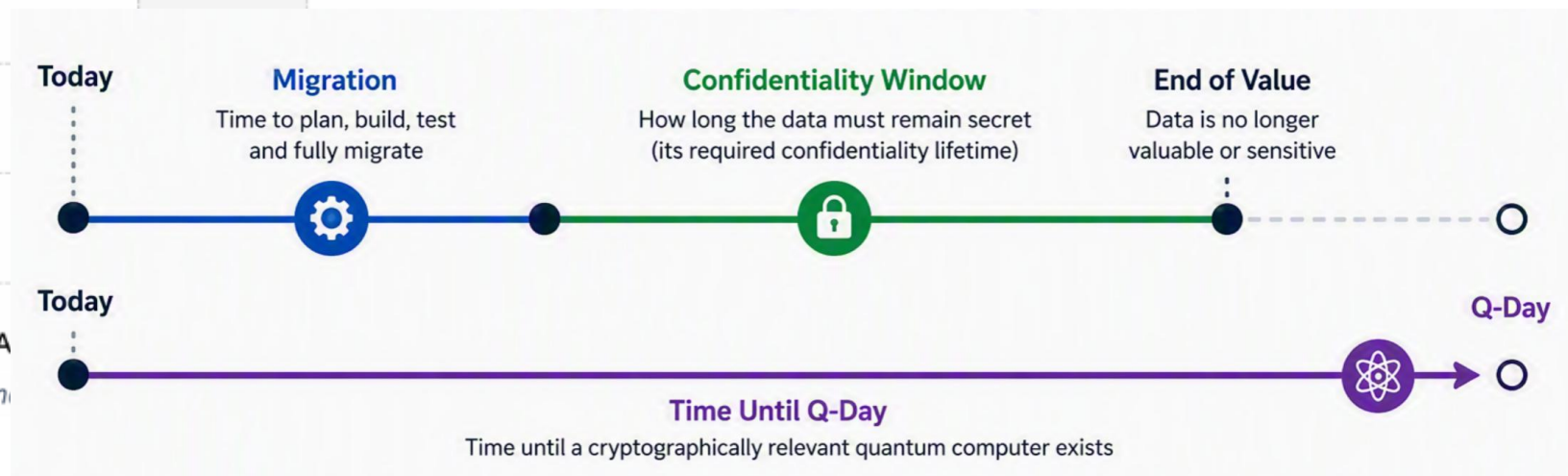


Figure 3 Averaged experts' likelihood estimates by time



| Ok, donc concrètement ?

Faible

Incertitude; complexité à migrer; impact sur la performance

Elevé

Ok, donc concrètement ?

Cryptographie symétrique

- **Doublement de la taille des clés AES.**

Idéalement on remplace AES-256 partout (sauf là où AES-128 peut être encore suffisant)

Faible

Incertitude; complexité à migrer; impact sur la performance

Elevé

Ok, donc concrètement ?

Cryptographie symétrique

- **Doublement de la taille des clés AES.**

Idéalement on remplace AES-256 partout (sauf là où AES-128 peut être encore suffisant)

Echange de clés

- Utilisation du **FIPS-203 ML-KEM**, standard NIST basé sur des lattices
- Il semble déjà **bien accepté**, et aussi standardisé par ISO 18033 rev2
- **Partie intégrante de TLS 1.3** (RFC-9954) et implémenté dans les solutions commerciales

Faible

Incertitude; complexité à migrer; impact sur la performance

Elevé

Ok, donc concrètement ?

Cryptographie symétrique

- **Doublement de la taille des clés AES.**
Idéalement on remplace AES-256 partout (sauf là où AES-128 peut être encore suffisant)

Echange de clés

- Utilisation du **FIPS-203 ML-KEM**, standard NIST basé sur des lattices
- Il semble déjà **bien accepté**, et aussi standardisé par ISO 18033 rev2
- **Partie intégrante de TLS 1.3** (RFC-9954) et implémenté dans les solutions commerciales

Pour les signatures

- **Pas de gagnants pour l'instant** du fait des impacts sur les performances
- NIST propose FIPS-204 ML-DSA and FIPS-205 SLH-DSA.
- Mais l'ISO n'a pour l'instant rien validé
- Google et d'autres étudient d'autres approches

Faible

Incertitude; complexité à migrer; impact sur la performance

Elevé

Merci de votre attention !

Merci de votre attention !

- Merci Caroline

Merci de votre attention !

- Merci Caroline
- Merci à toute l'équipe de la chaire

Merci de votre attention !

- Merci Caroline
- Merci à toute l'équipe de la chaire
- Merci à tous les autres que j'ai eu la chance de côtoyer