La cryptographie symétrique légère (et sa standardisation)

Léo Perrin[1]

[1]Inria, France
leo.perrin@inria.fr

Vendredi 17 Décembre

Séminaire de Versailles

La cryptographie symétrique légère (et sa standardisation)

La cryptographie symétrique légère (et sa standardisation)

1 Rappels de cryptographie symétrique

La cryptographie symétrique légère (et sa standardisation)

1. Rappels de cryptographie symétrique
2. La légèreté en cryptographie

La cryptographie symétrique légère (et sa standardisation)

1. Rappels de cryptographie symétrique
2. La légèreté en cryptographie
3. La standardisation

Outline

1 Rappels de Cryptographie Symétrique

2 La légereté en cryptographie

3 La standardisation

4 Conclusion

Plan of this Section

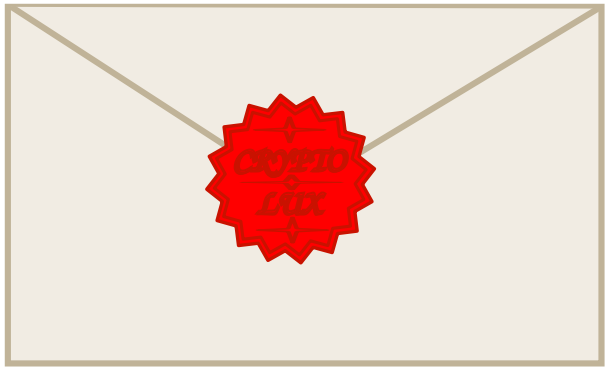
1 Rappels de Cryptographie Symétrique

2 La légereté en cryptographie

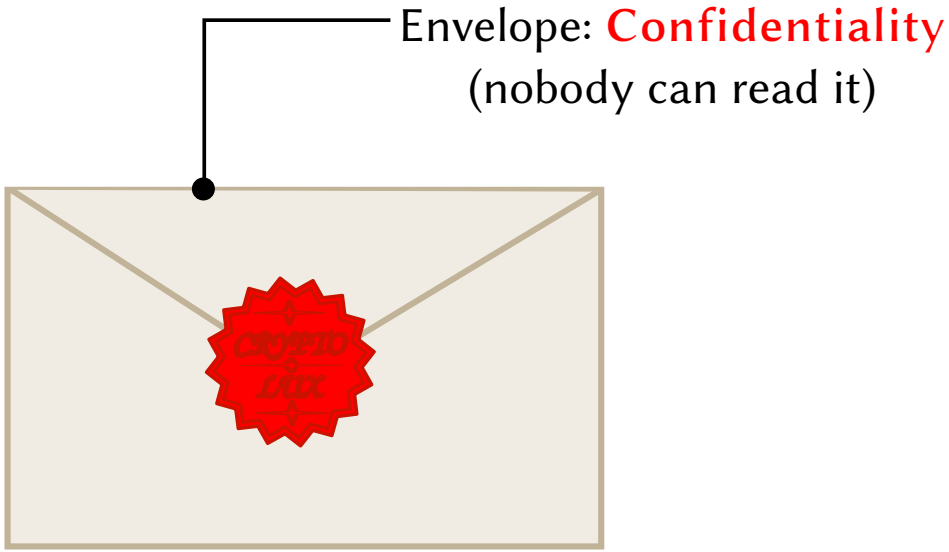
3 La standardisation

4 Conclusion

Le but de la cryptographie

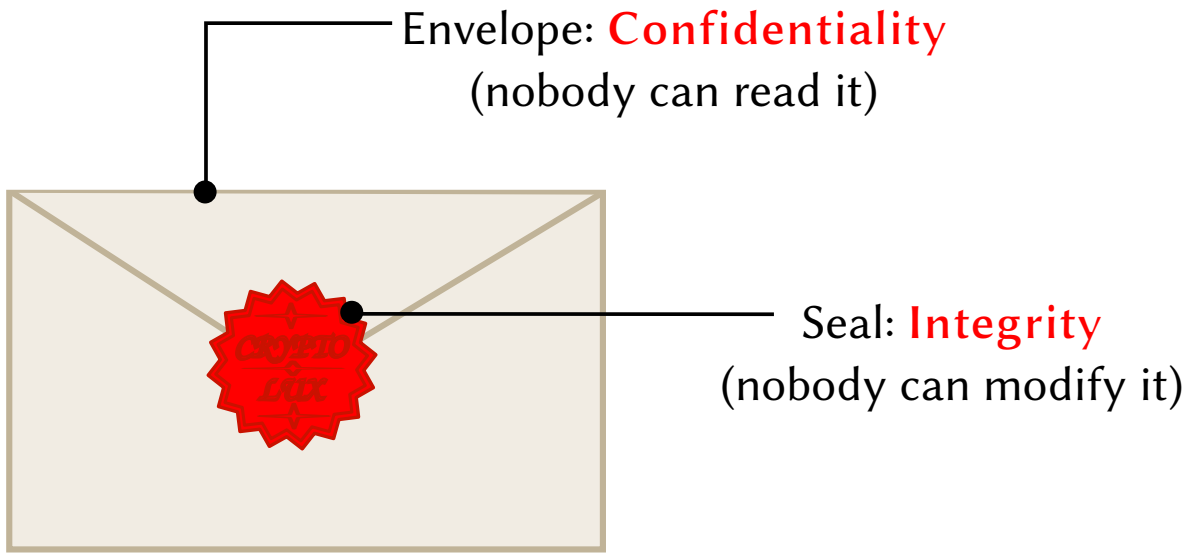


Le but de la cryptographie



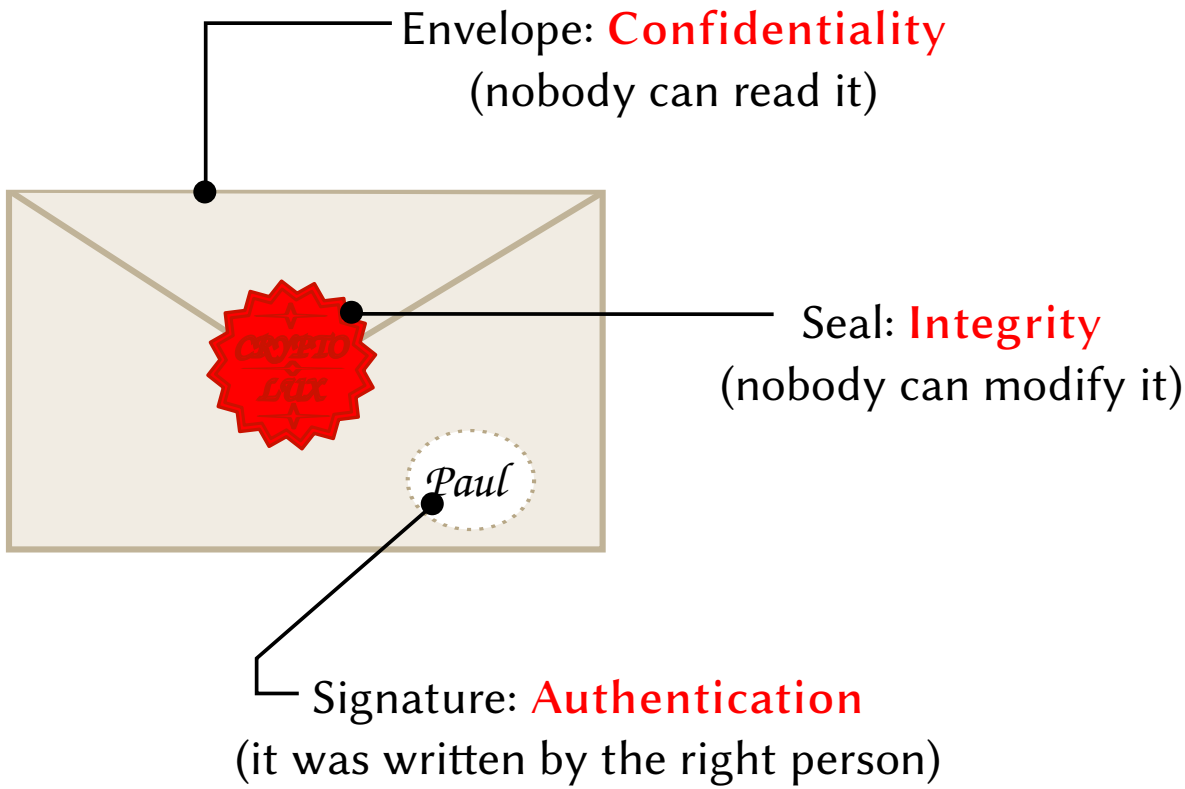
Confidentialité

Le but de la cryptographie



Confidentialité · Intégrité

Le but de la cryptographie



Confidentialité · Intégrité · Authentification

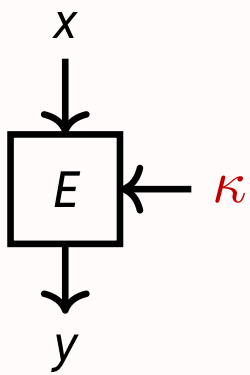
La cryptographie symétrique

On suppose qu'une clef est déjà partagée.

La cryptographie symétrique

On suppose qu'une clef est déjà partagée.

Primitives

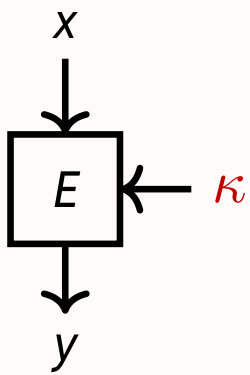


Chiffrement par bloc

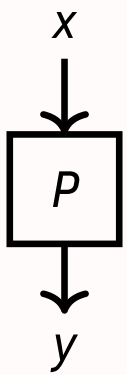
La cryptographie symétrique

On suppose qu'une clef est déjà partagée.

Primitives



Chiffrement par bloc

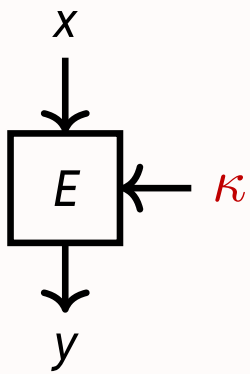


Permutation

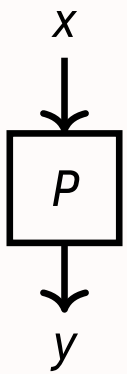
La cryptographie symétrique

On suppose qu'une clef est déjà partagée.

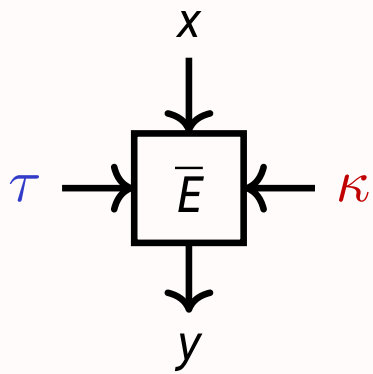
Primitives



Chiffrement par bloc



Permutation

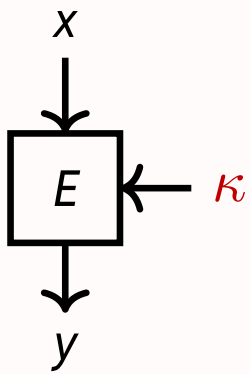


Chiffrement par bloc avec tweak

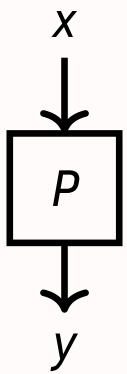
La cryptographie symétrique

On suppose qu'une clef est déjà partagée.

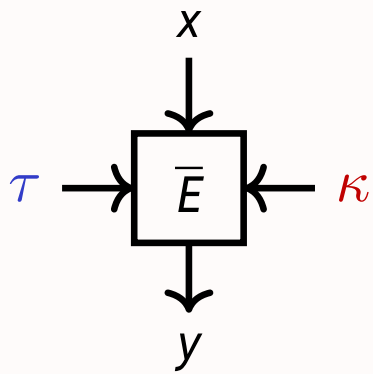
Primitives



Chiffrement par bloc



Permutation



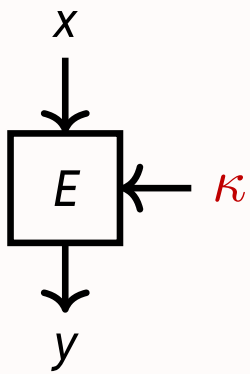
Chiffrement par bloc avec tweak

Modes

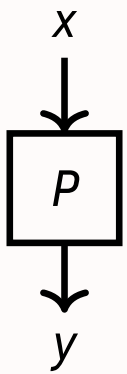
La cryptographie symétrique

On suppose qu'une clef est déjà partagée.

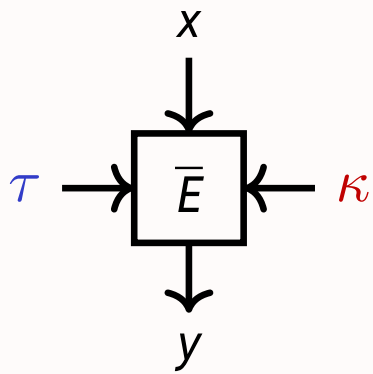
Primitives



Chiffrement par bloc



Permutation



Chiffrement par bloc avec tweak

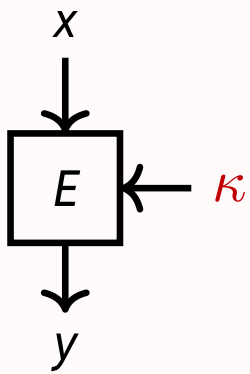
Modes

- GCM (chiffrement par bloc $\longrightarrow$ AEAD)

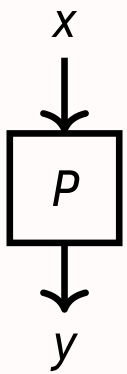
La cryptographie symétrique

On suppose qu'une clef est déjà partagée.

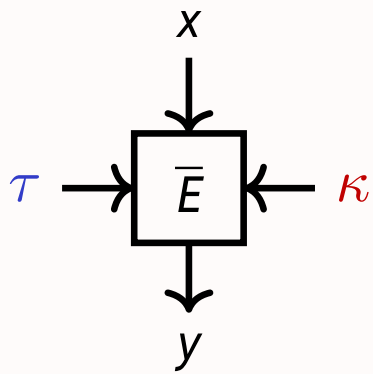
Primitives



Chiffrement par bloc



Permutation



Chiffrement par bloc avec tweak

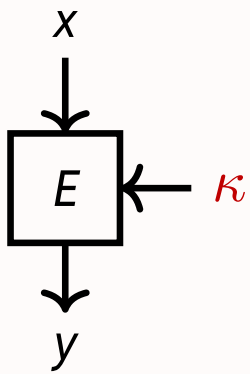
Modes

- GCM (chiffrement par bloc $\longrightarrow$ AEAD)
- Éponge (permutation $\longrightarrow$ fonction de hachage),

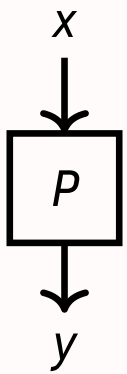
La cryptographie symétrique

On suppose qu'une clef est déjà partagée.

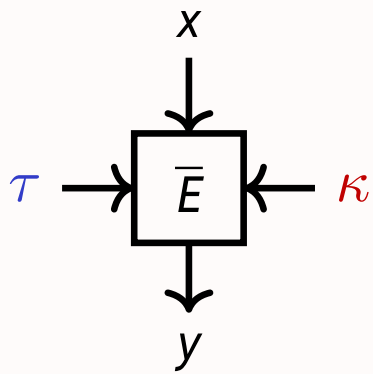
Primitives



Chiffrement par bloc



Permutation



Chiffrement par bloc avec tweak

Modes

- GCM (chiffrement par bloc $\longrightarrow$ AEAD)
- Éponge (permutation $\longrightarrow$ fonction de hachage),
- ...

Plan of this Section

1 Rappels de Cryptographie Symétrique

2 La légereté en cryptographie

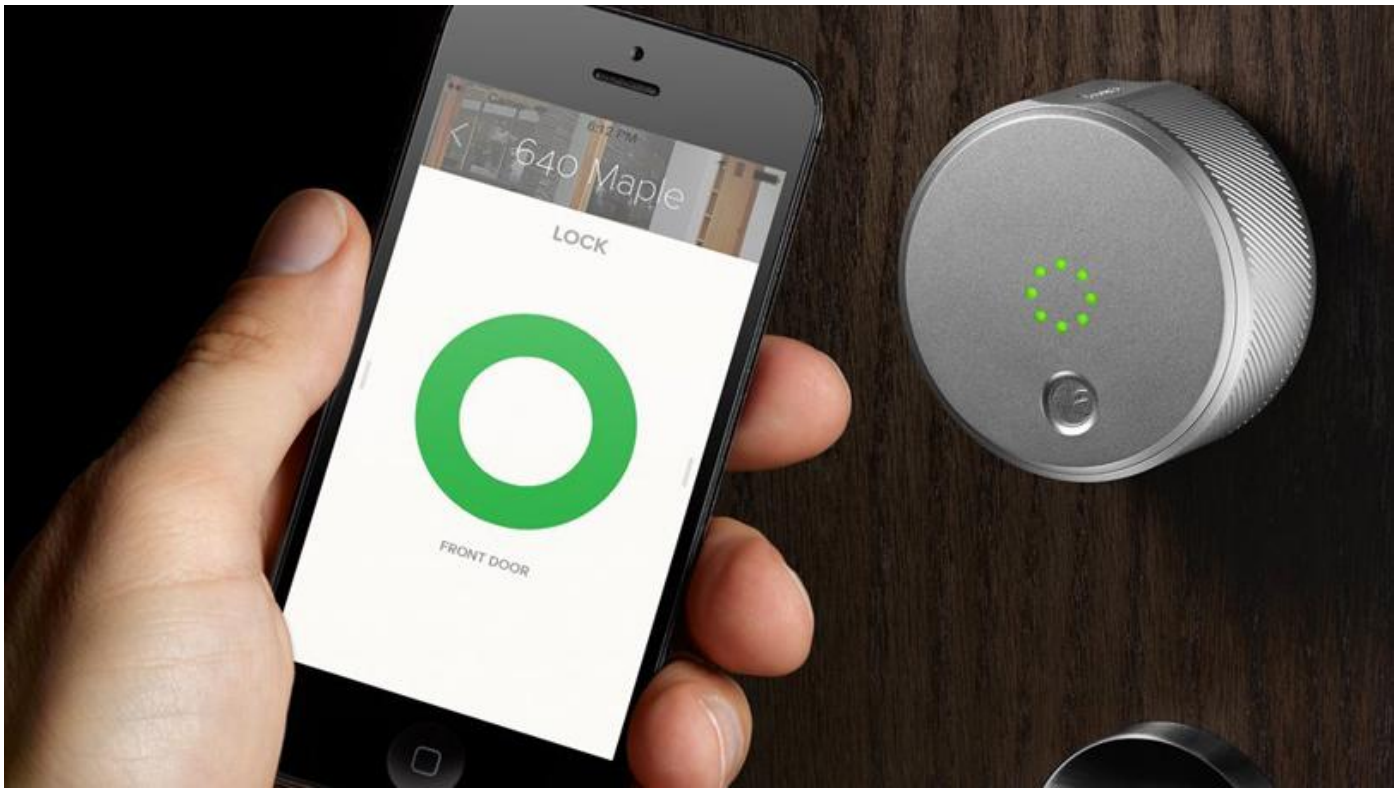
3 La standardisation

4 Conclusion

Les objets de “l’internet des objets”

Tout se fait connecter à internet

Les objets de “l’internet des objets”



Tout

Les objets de “l’internet des objets”

Tout

Les objets de “l’internet des objets”

TOUT

Securité

"In IoT, the S is for Security."

- Les objets connectés ont des failles de sécurité.
- La sécurité est en bas de la liste des priorités (si elle y est).
- La sécurité a un coût en terme de conception...
- ... et en terme de ressource (temps/mémoire) !

La cryptographie légère

La cryptographie légère utilise peu de ressources.

La cryptographie légère

La cryptographie légère utilise peu de ressources.

Ce qui ne veut pas dire grand chose !

Cibles d'optimisation

La cryptographie légère

La cryptographie légère utilise peu de ressources.

Ce qui ne veut pas dire grand chose !

Cibles d'optimisation

- Le logiciel ? Peu de RAM, peu de cycles, utilisation des instructions disponibles sur les micro-controlleurs...

La cryptographie légère

La cryptographie légère utilise peu de ressources.

Ce qui ne veut pas dire grand chose !

Cibles d'optimisation

- Le logiciel ? Peu de RAM, peu de cycles, utilisation des instructions disponibles sur les micro-controlleurs...
- Le matériel ? Évaluation parallèle, importance du chemin critique, différence de coût mémoire volatile/figée...

La cryptographie légère

La cryptographie légère utilise peu de ressources.

Ce qui ne veut pas dire grand chose !

Cibles d'optimisation

- Le logiciel ? Peu de RAM, peu de cycles, utilisation des instructions disponibles sur les micro-controlleurs...
- Le matériel ? Évaluation parallèle, importance du chemin critique, différence de coût mémoire volatile/figée...
- Le masquage ? Utilisation de sous-fonctions de bas degré algébrique, modes spécialisés...

La cryptographie légère de l'industrie

Chiffrements à flots, sauf †(CpB) ou ‡(MAC)

- A5/1
- A5/2
- Cmea †
- Oryx
- A5-GMR-1
- A5-GMR-2
- Dsc
- SecureMem.
- CryptoMem.
- Hitag2
- Megamos
- Keeloq †
- Dst40 †
- iClass
- Crypto-1
- Css
- Cryptomeria †
- Csa-BC †
- Csa-SC
- PC-1
- SecurID ‡
- E0
- RC4

La cryptographie légère de l'industrie

Chiffrements à flots, sauf †(CpB) ou ‡(MAC)

- A5/1
- A5/2
- Cmea †
- Oryx
- A5-GMR-1
- A5-GMR-2
- Dsc
- SecureMem.
- CryptoMem.
- Hitag2
- Megamos
- Keeloq †
- Dst40 †
- iClass
- Crypto-1
- Css
- Cryptomeria †
- Csa-BC †
- Csa-SC
- PC-1
- SecurID ‡
- E0
- RC4

Ils sont tous cassés (attaques en temps inférieur à 2^{64}).

Plan of this Section

1 Rappels de Cryptographie Symétrique

2 La légereté en cryptographie

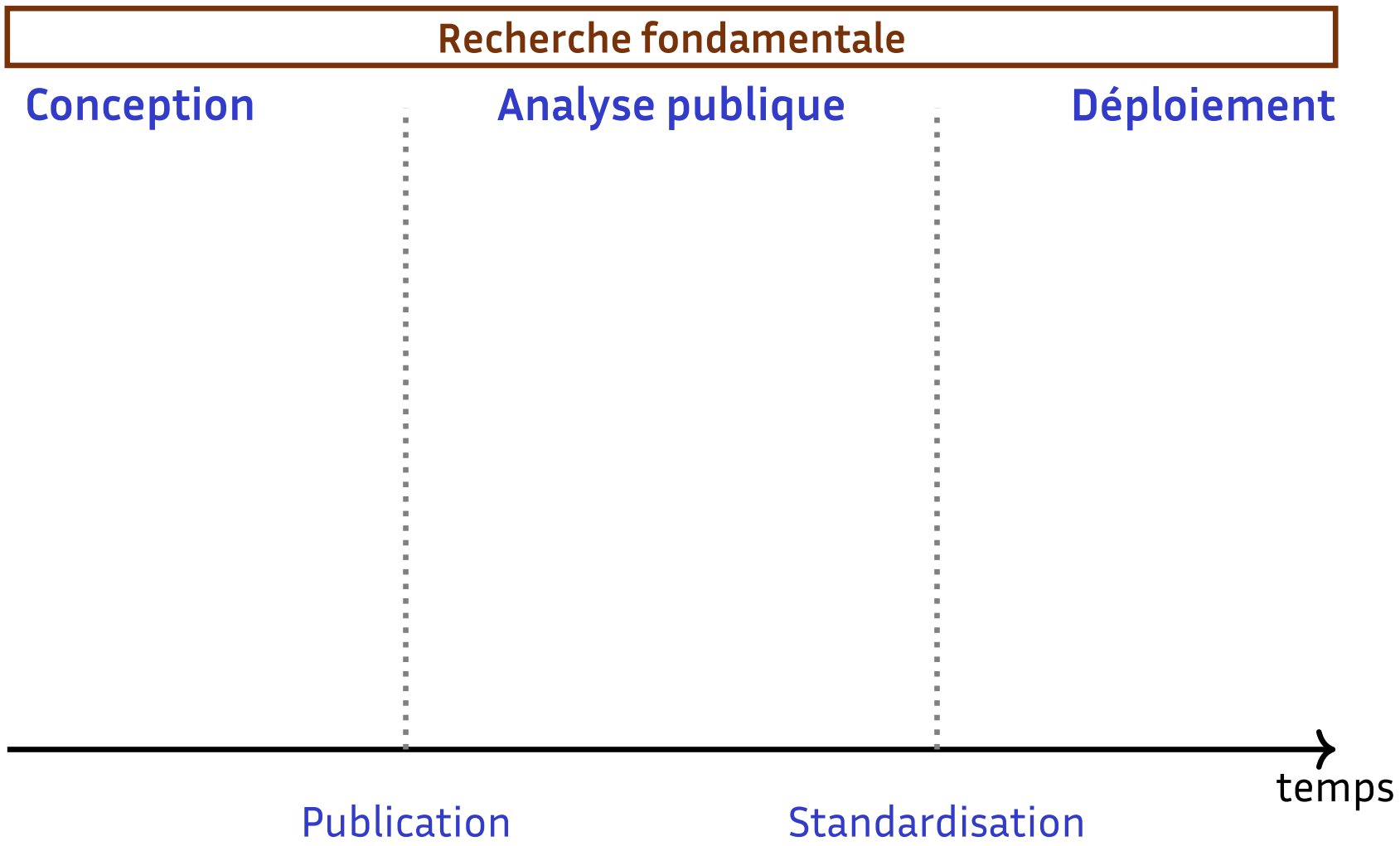
3 La standardisation

4 Conclusion

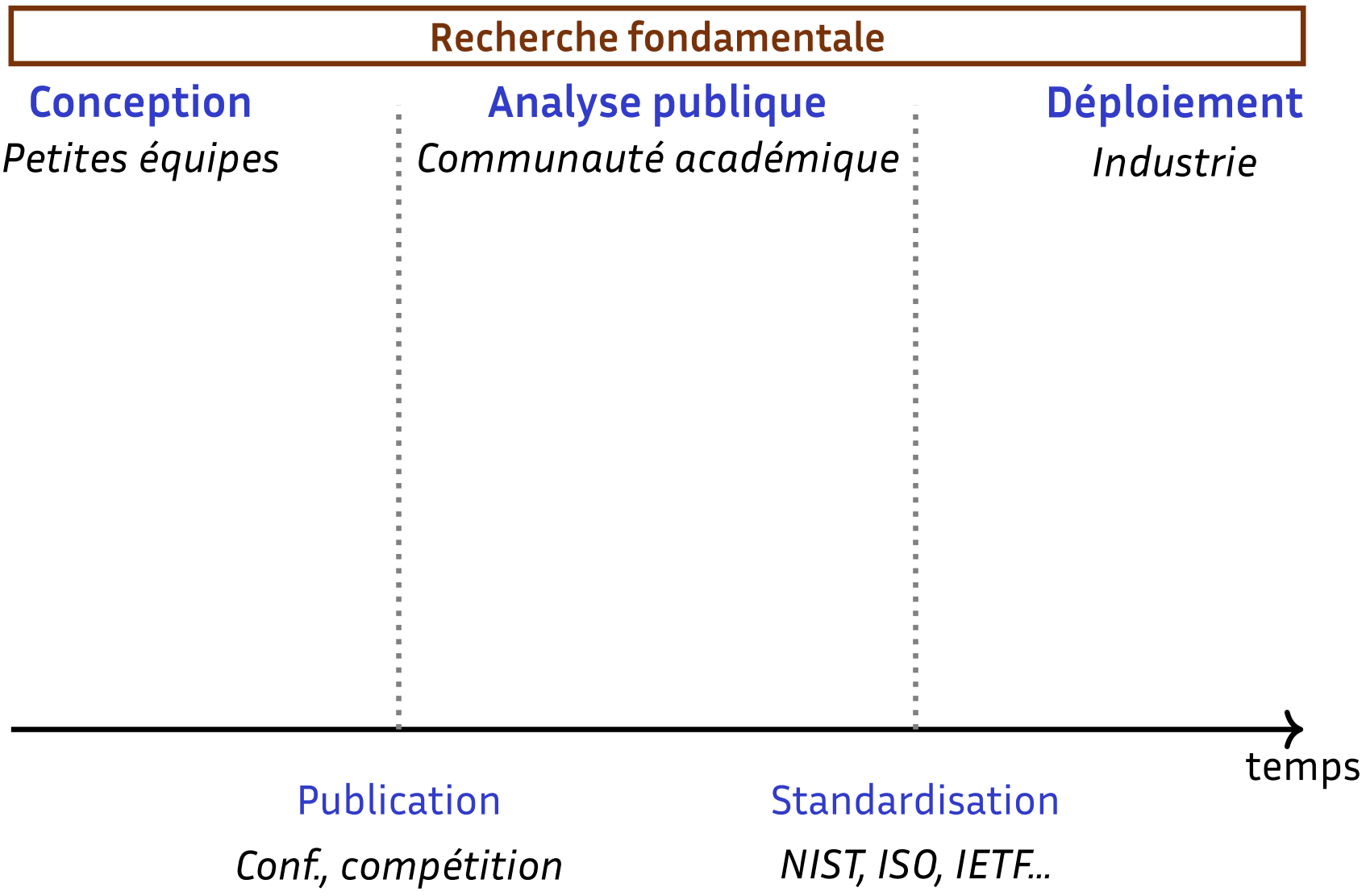
Le cycle de vie d'une primitive cryptographique

Recherche fondamentale

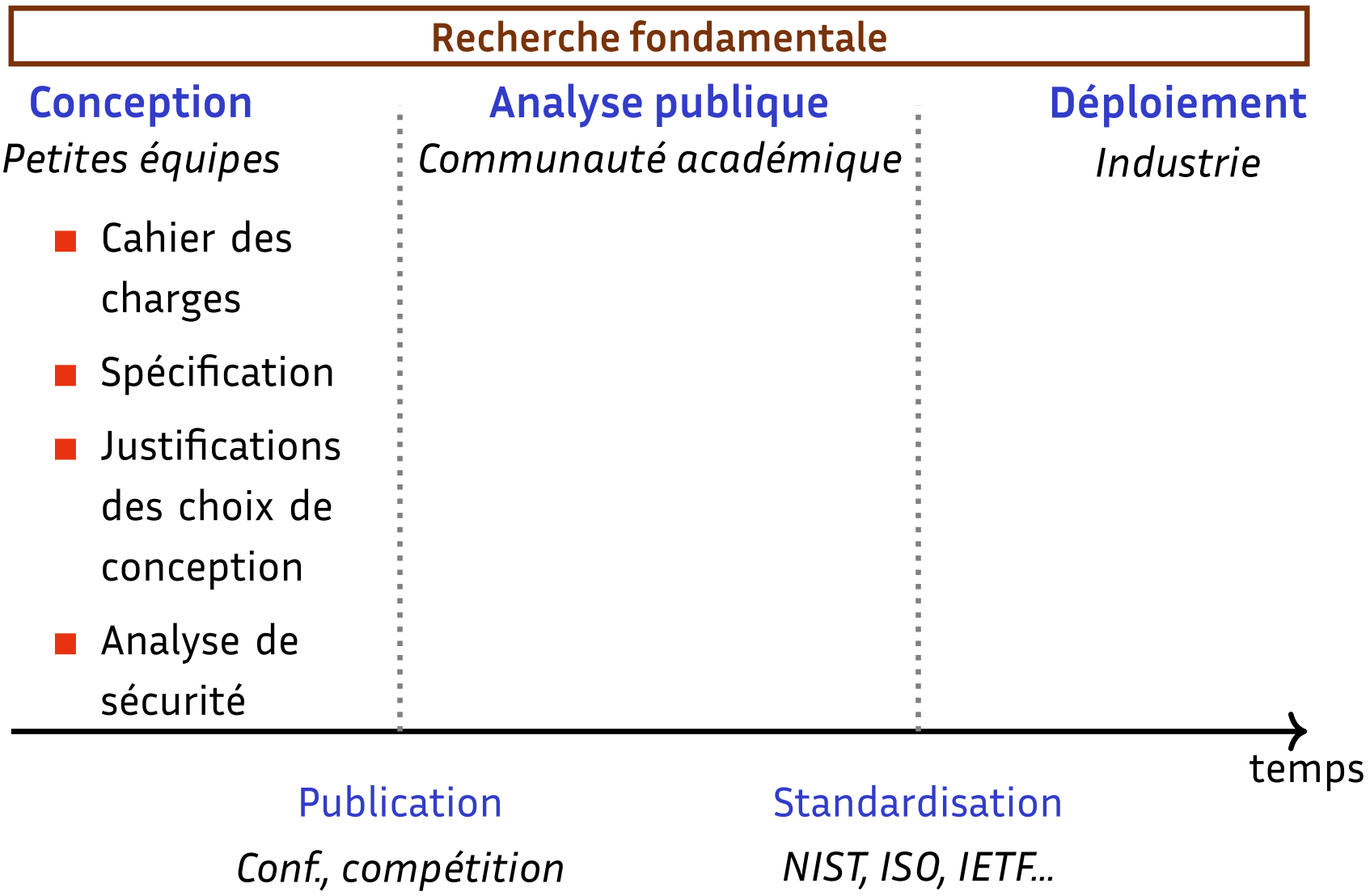
Le cycle de vie d'une primitive cryptographique



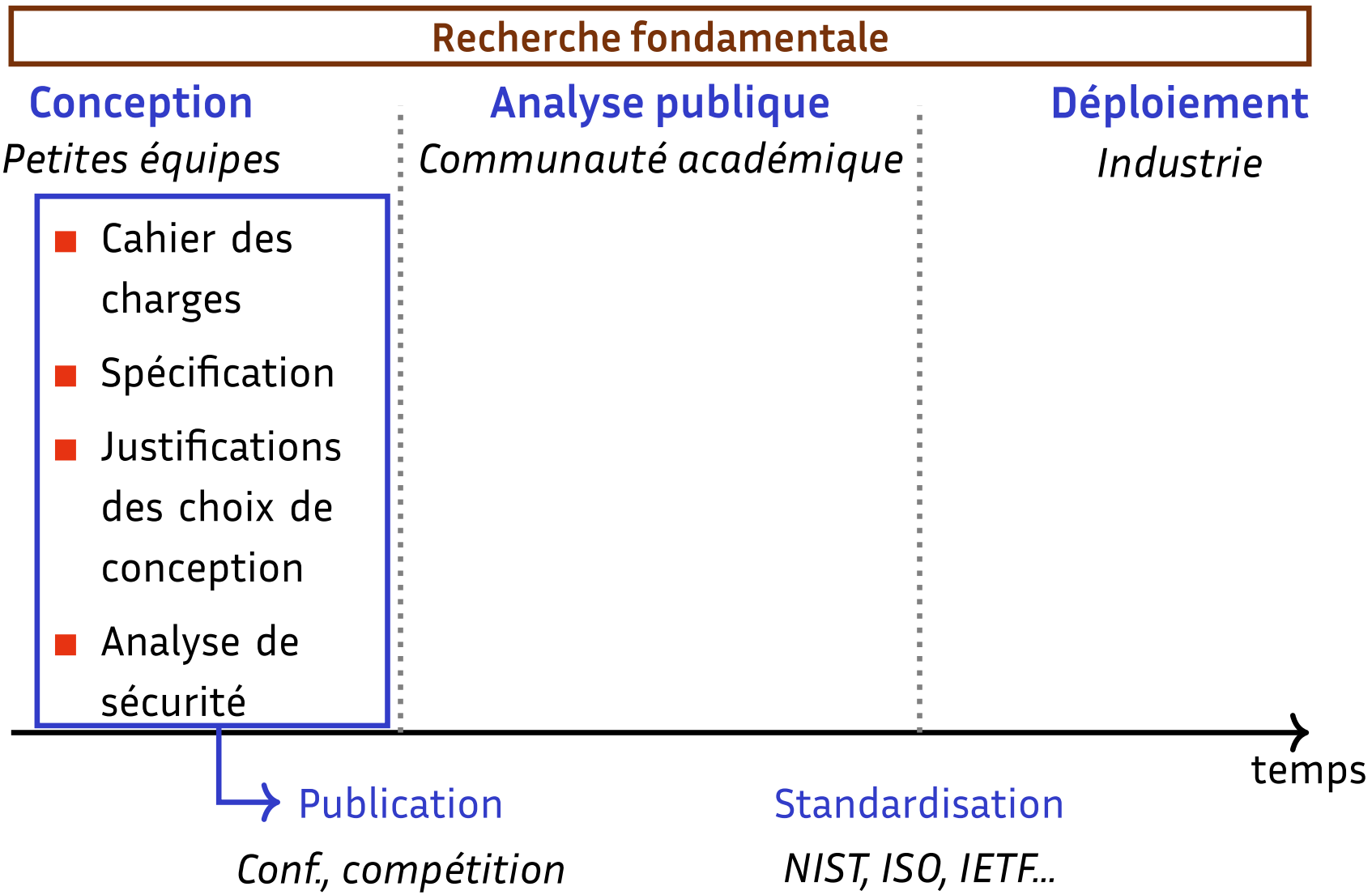
Le cycle de vie d'une primitive cryptographique



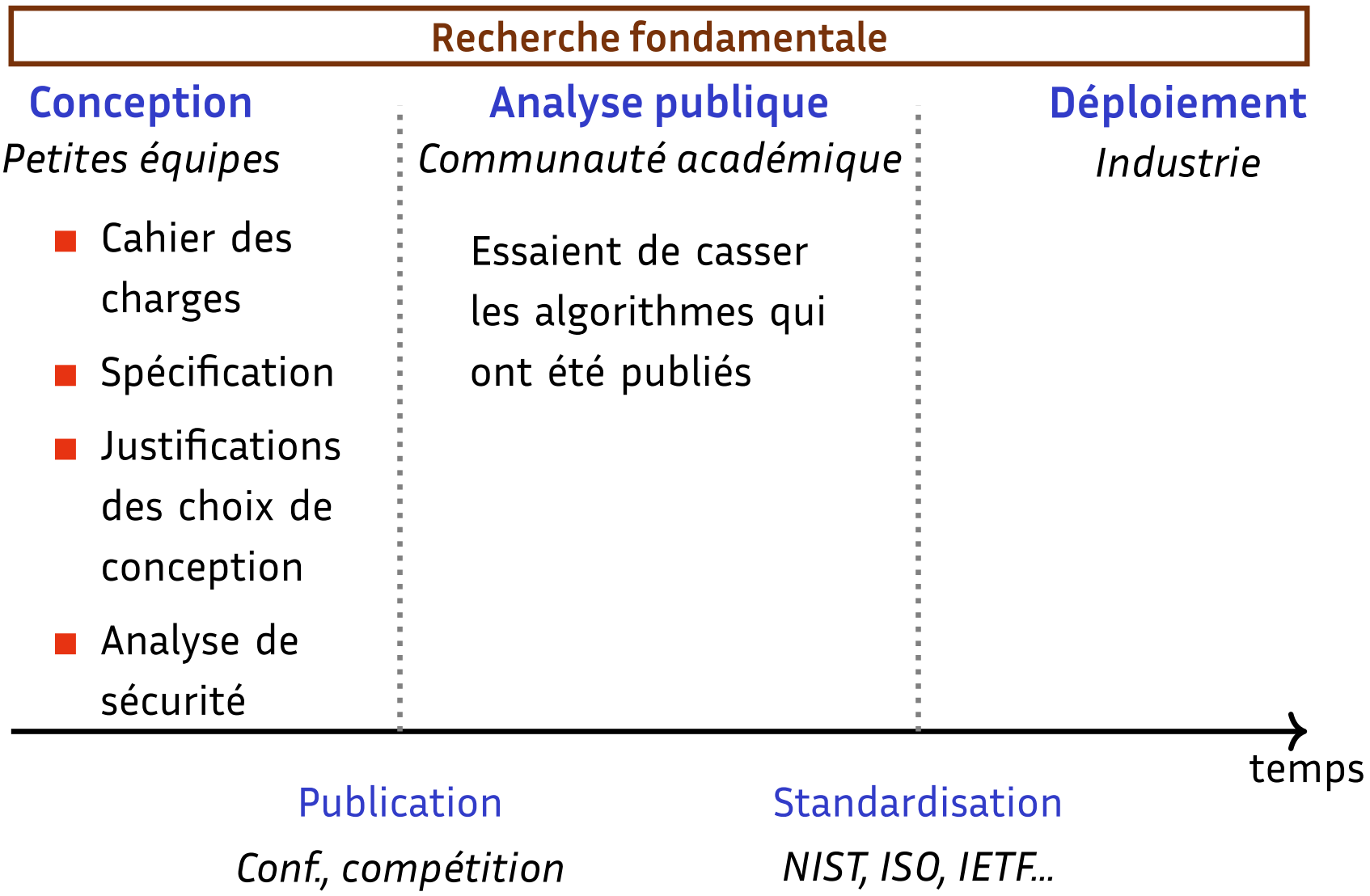
Le cycle de vie d'une primitive cryptographique



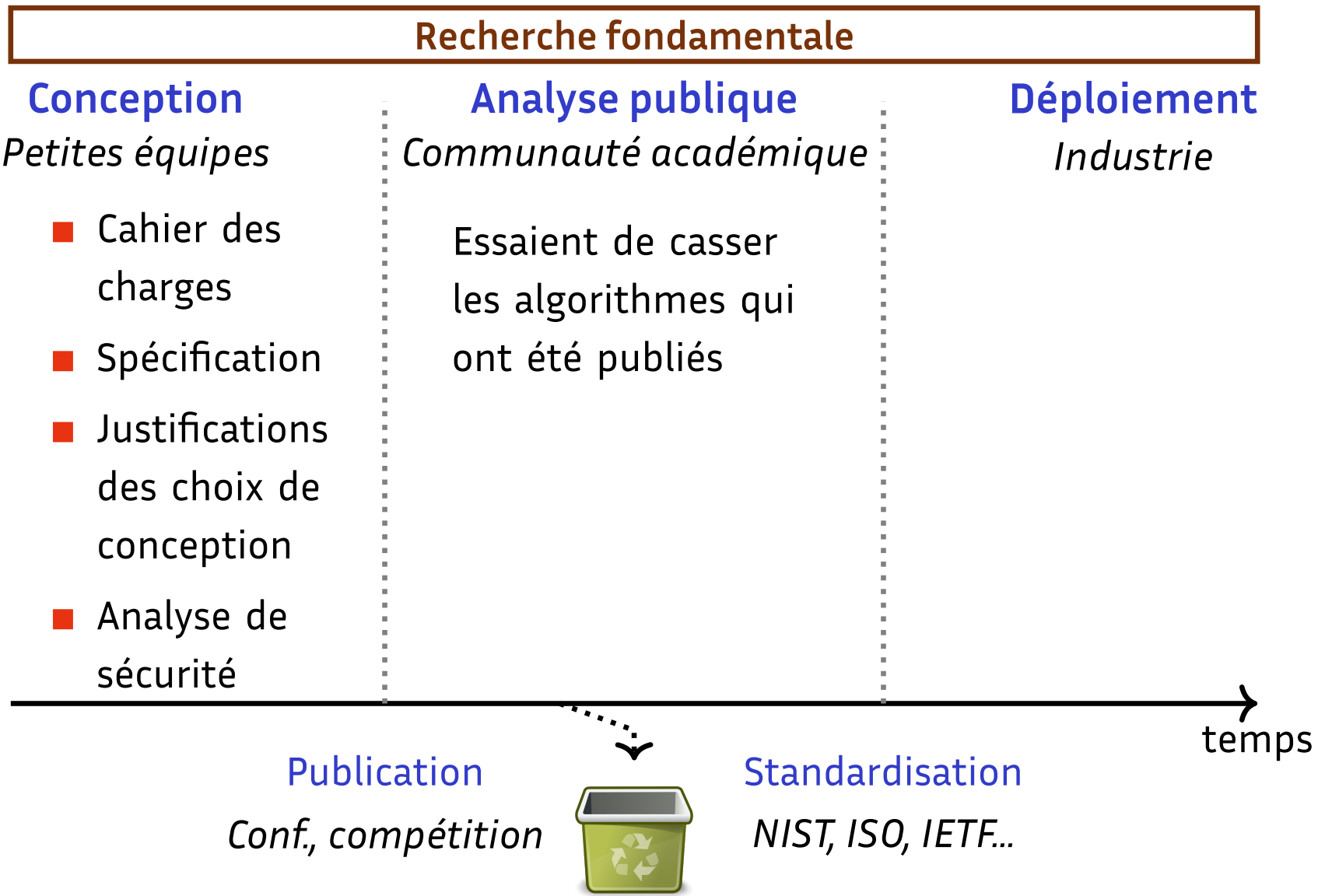
Le cycle de vie d'une primitive cryptographique



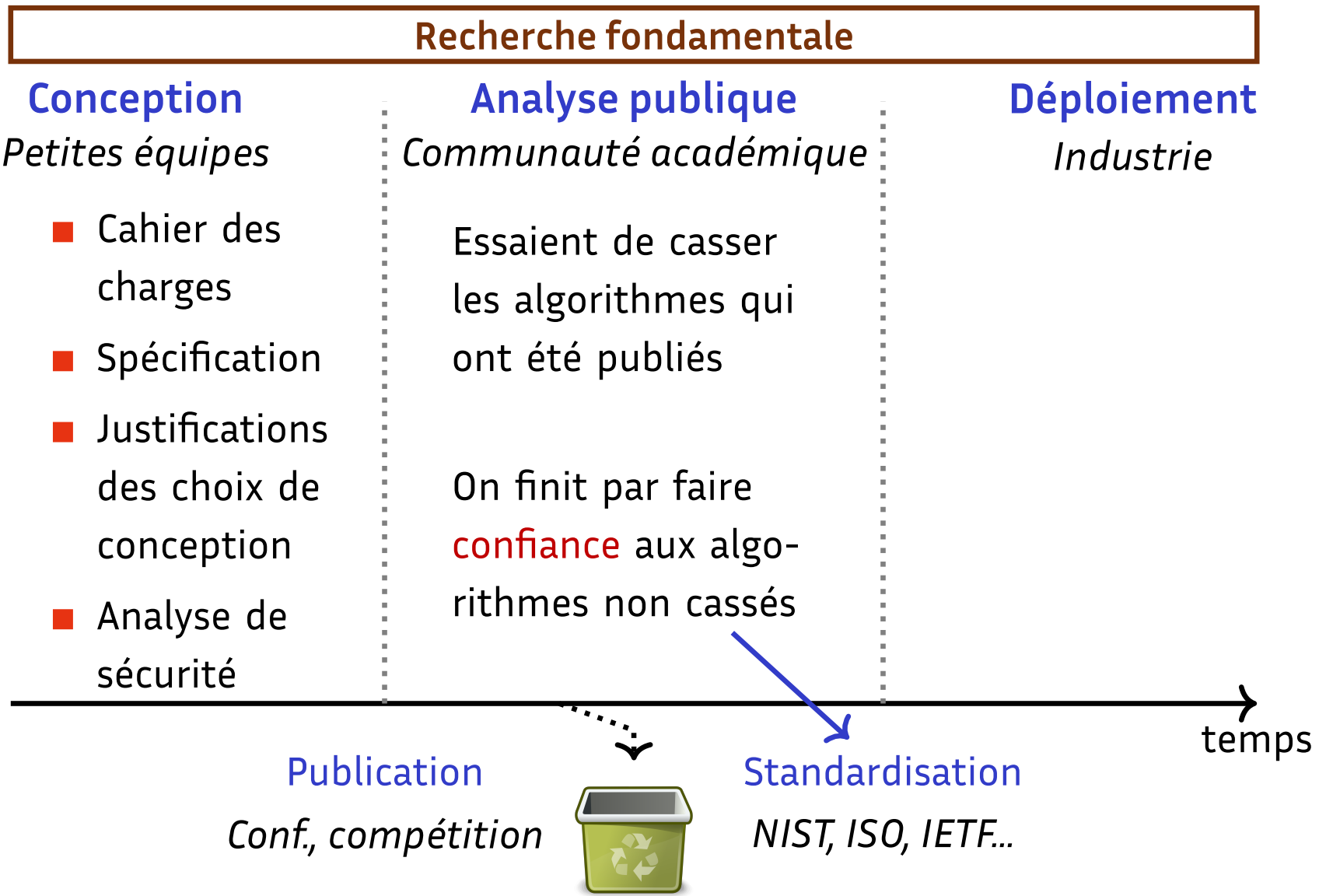
Le cycle de vie d'une primitive cryptographique



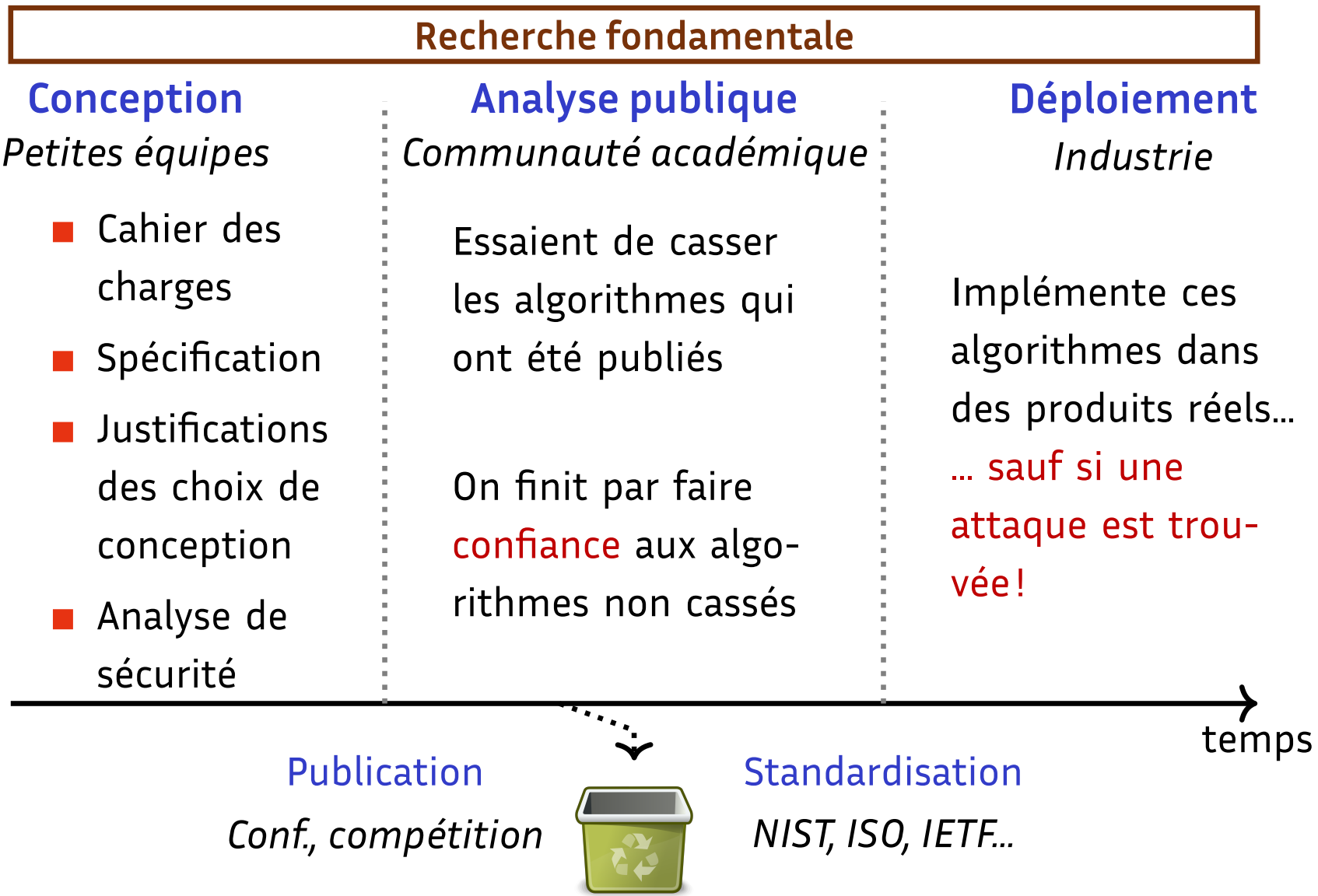
Le cycle de vie d'une primitive cryptographique



Le cycle de vie d'une primitive cryptographique



Le cycle de vie d'une primitive cryptographique



La “compétition” du NIST

NIST has initiated a process to solicit, evaluate, and standardize lightweight cryptographic algorithms that are suitable for use in constrained environments where the performance of current NIST cryptographic standards is not acceptable.

La “compétition” du NIST (historique)

Mars 2017. Décision de créer un portfolio d’algorithmes légers

La “compétition” du NIST (historique)

Mars 2017. Décision de créer un portfolio d’algorithmes légers

25 Fév. 2019. Date butoir pour soumettre un algorithme

La “compétition” du NIST (historique)

Mars 2017. Décision de créer un portfolio d’algorithmes légers

25 Fév. 2019. Date butoir pour soumettre un algorithme

56 algorithmes soumis !

La “compétition” du NIST (historique)

Mars 2017.	Décision de créer un portfolio d’algorithmes légers
25 Fév. 2019.	Date butoir pour soumettre un algorithme 56 algorithmes soumis !
30 Août 2019.	Annonce des candidats admis au 2ème tour

La “compétition” du NIST (historique)

Mars 2017.	Décision de créer un portfolio d’algorithmes légers
25 Fév. 2019.	Date butoir pour soumettre un algorithme 56 algorithmes soumis !
30 Août 2019.	Annonce des candidats admis au 2ème tour 32 algorithmes sont passés

La “compétition” du NIST (historique)

Mars 2017.	Décision de créer un portfolio d’algorithmes légers
25 Fév. 2019.	Date butoir pour soumettre un algorithme 56 algorithmes soumis !
30 Août 2019.	Annonce des candidats admis au 2ème tour 32 algorithmes sont passés
Août 2020.	Annonce des candidats admis au 3ème tour

La “compétition” du NIST (historique)

Mars 2017.	Décision de créer un portfolio d’algorithmes légers
25 Fév. 2019.	Date butoir pour soumettre un algorithme 56 algorithmes soumis !
30 Août 2019.	Annonce des candidats admis au 2ème tour 32 algorithmes sont passés
Août 2020.	Annonce des candidats admis au 3ème tour [ANNULÉ]

La “compétition” du NIST (historique)

Mars 2017.	Décision de créer un portfolio d’algorithmes légers
25 Fév. 2019.	Date butoir pour soumettre un algorithme 56 algorithmes soumis !
30 Août 2019.	Annonce des candidats admis au 2ème tour 32 algorithmes sont passés
Août 2020.	Annonce des candidats admis au 3ème tour [ANNULÉ]
Déc. 2020.	Annonce des candidats admis au 3ème tour

La “compétition” du NIST (historique)

Mars 2017.	Décision de créer un portfolio d’algorithmes légers
25 Fév. 2019.	Date butoir pour soumettre un algorithme 56 algorithmes soumis !
30 Août 2019.	Annonce des candidats admis au 2ème tour 32 algorithmes sont passés
Août 2020.	Annonce des candidats admis au 3ème tour [ANNULÉ]
Déc. 2020.	Annonce des candidats admis au 3ème tour [ANNULÉ]

La “compétition” du NIST (historique)

Mars 2017.	Décision de créer un portfolio d’algorithmes légers
25 Fév. 2019.	Date butoir pour soumettre un algorithme 56 algorithmes soumis !
30 Août 2019.	Annonce des candidats admis au 2ème tour 32 algorithmes sont passés
Août 2020.	Annonce des candidats admis au 3ème tour [ANNULÉ]
Déc. 2020.	Annonce des candidats admis au 3ème tour [ANNULÉ]
Fév. 2021.	Annonce des candidats admis au 3ème tour ?

La “compétition” du NIST (historique)

Mars 2017.	Décision de créer un portfolio d’algorithmes légers
25 Fév. 2019.	Date butoir pour soumettre un algorithme 56 algorithmes soumis !
30 Août 2019.	Annonce des candidats admis au 2ème tour 32 algorithmes sont passés
Août 2020.	Annonce des candidats admis au 3ème tour [ANNULÉ]
Déc. 2020.	Annonce des candidats admis au 3ème tour [ANNULÉ]
Fév. 2021.	Annonce des candidats admis au 3ème tour ?

La “compétition” du NIST (futur ?)

Le NIST doit faire un choix !

La “compétition” du NIST (futur ?)

Le NIST doit faire un choix !

Un algorithme à tout faire

- moyen dans tous les contextes
- très bon nulle part...
- très mauvais nulle part !
- un standard plus facile à gérer/analyser
- l’AES ?

La “compétition” du NIST (futur ?)

Le NIST doit faire un choix !

Un algorithme à tout faire

- moyen dans tous les contextes
- très bon nulle part...
- très mauvais nulle part !
- un standard plus facile à gérer/analyser
- l’AES ?

Plusieurs algorithmes

- optimisés pour un usage précis
- très bons dans quelques contextes...
- très mauvais dans les autres !
- standard plus compliqué à gérer/analyser

Plan of this Section

1 Rappels de Cryptographie Symétrique

2 La légereté en cryptographie

3 La standardisation

4 Conclusion

Conclusion : le programme du jour

Présentation d'algorithmes

- Forkcipher (hardware)
- Saturnin (général)
- Sparkle (software)
- Spook (implémentation protégée)
- Subterranean (hardware)

Présentation d'attaques

MixFeed · Gimli · Xoodyak

Conclusion : le programme du jour

Présentation d'algorithmes

- Forkcipher (hardware)
- Saturnin (général)
- Sparkle (software)
- Spook (implémentation protégée)
- Subterranean (hardware)

Présentation d'attaques

MixFeed · Gimli · Xoodyak

À tout à l'heure !