Russian-style (lack of) Randomness

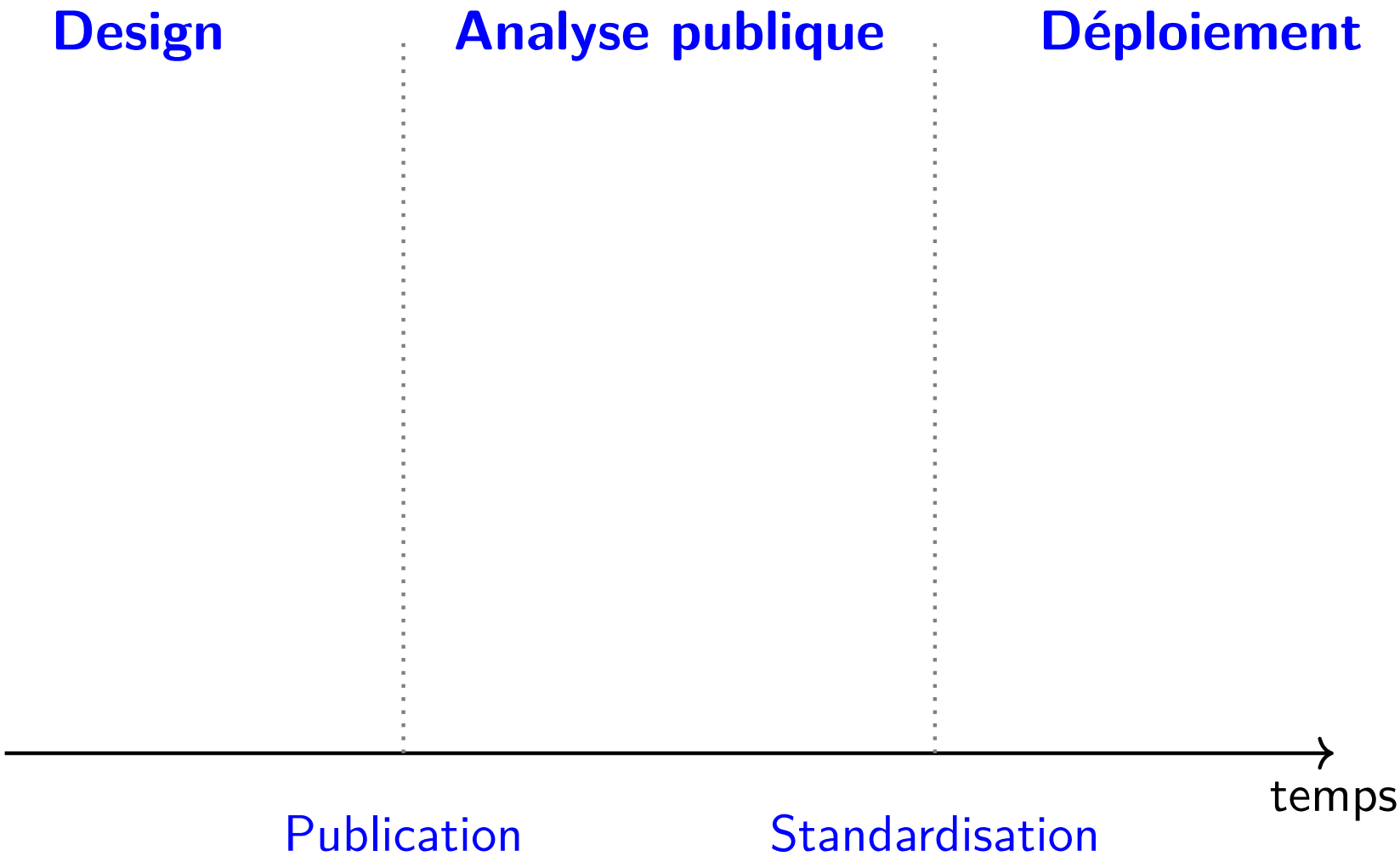
Léo Perrin, Xavier Bonnetain

Inria, France

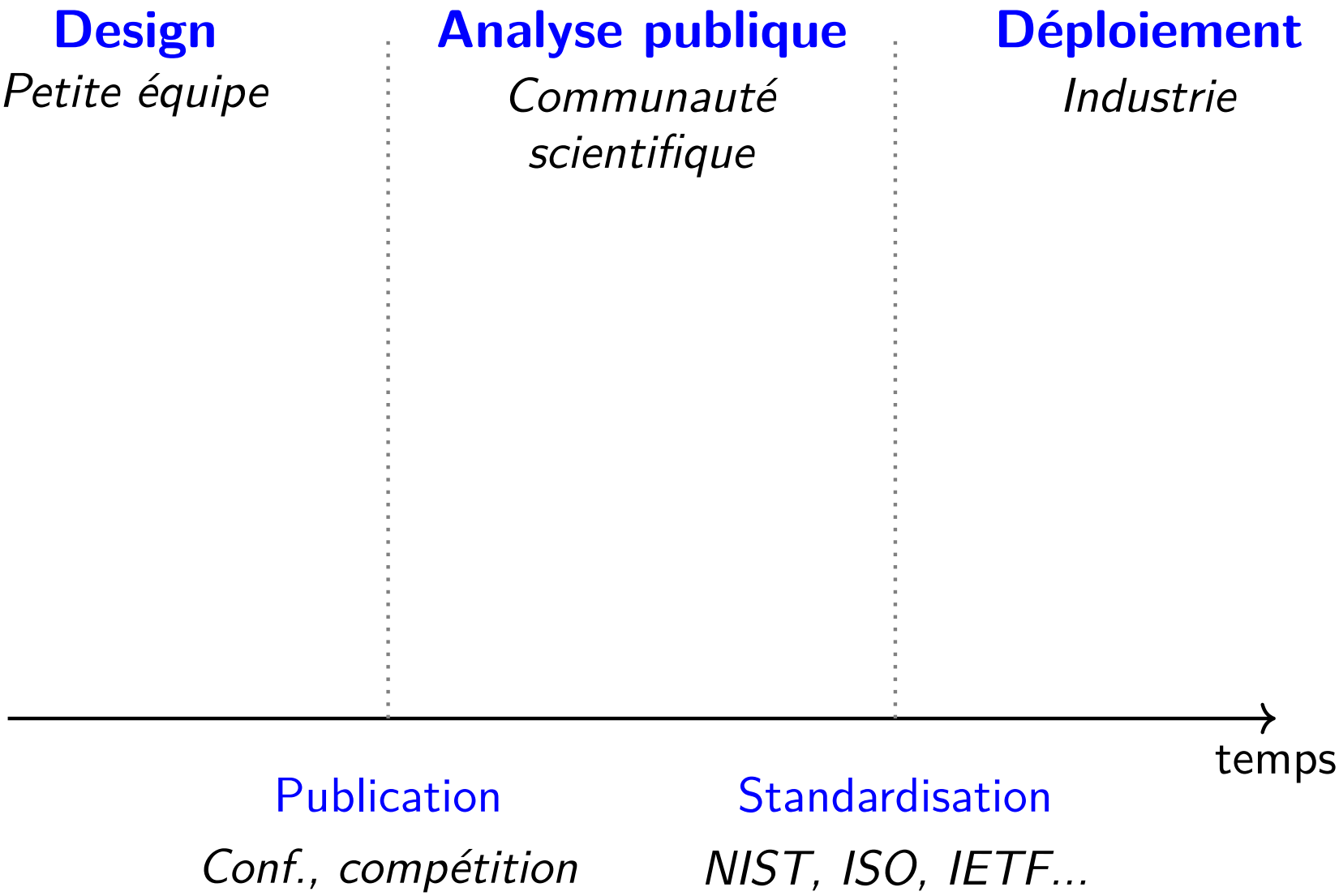
7 juin 2019

Plan

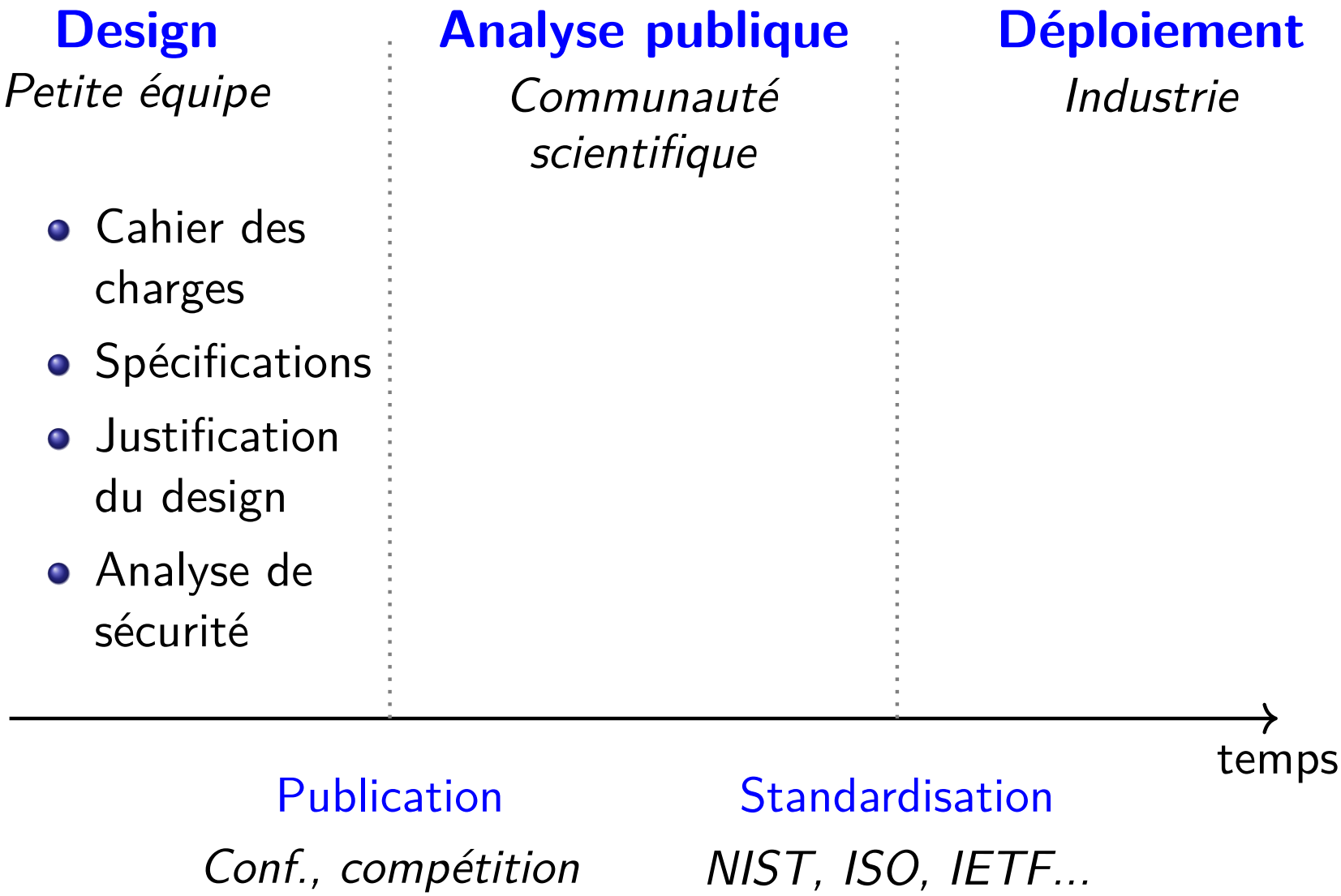
La standardisation en théorie



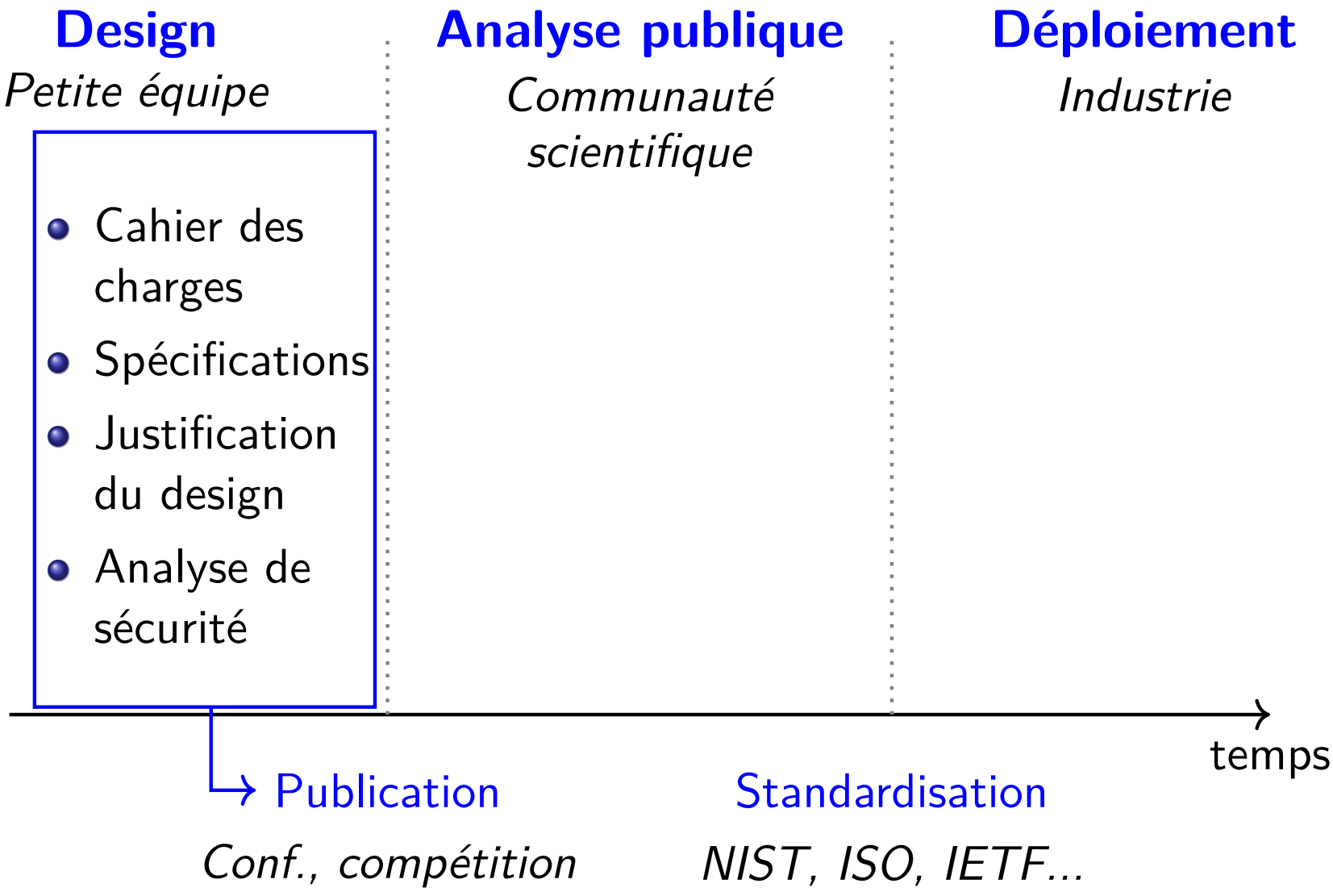
La standardisation en théorie



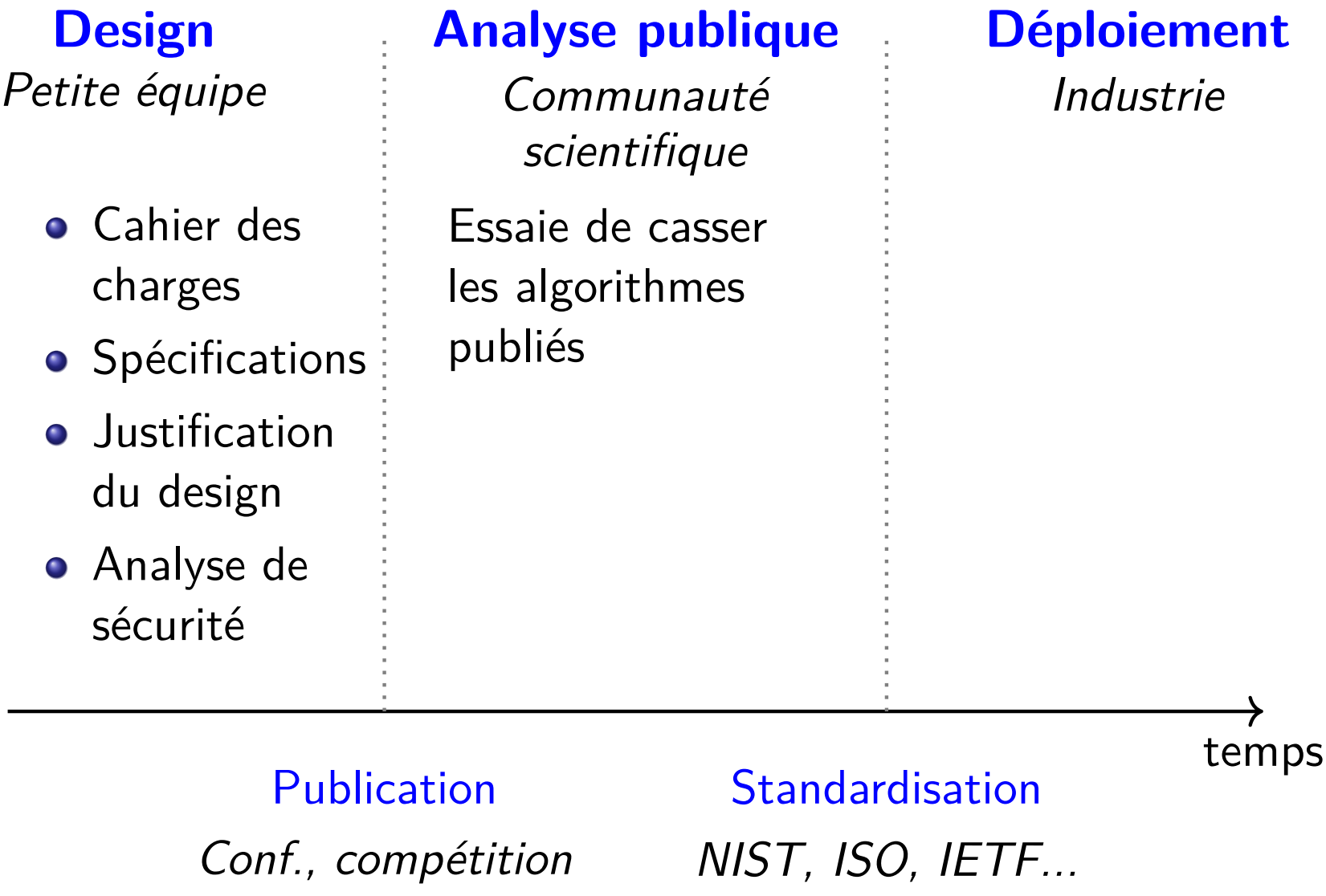
La standardisation en théorie



La standardisation en théorie



La standardisation en théorie



La standardisation en théorie

Design

Petite équipe

- Cahier des charges
- Spécifications
- Justification du design
- Analyse de sécurité

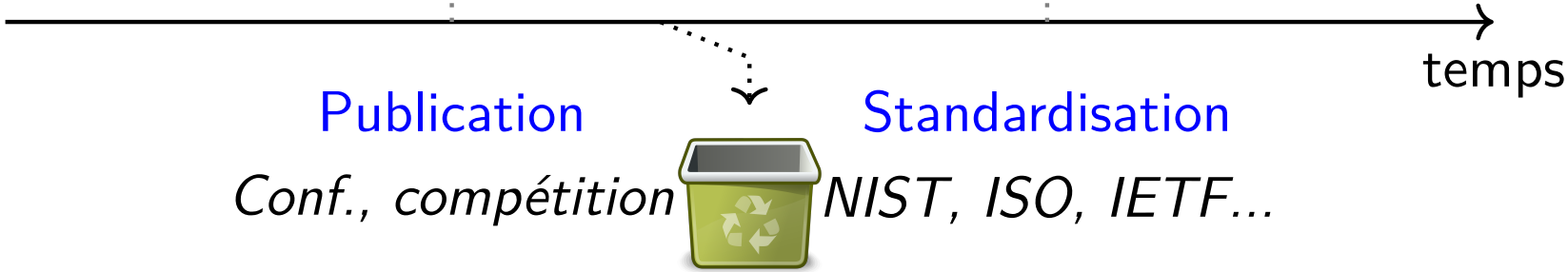
Analyse publique

Communauté scientifique

Essaie de casser les algorithmes publiés

Déploiement

Industrie



La standardisation en théorie

Design

Petite équipe

- Cahier des charges
- Spécifications
- Justification du design
- Analyse de sécurité

Analyse publique

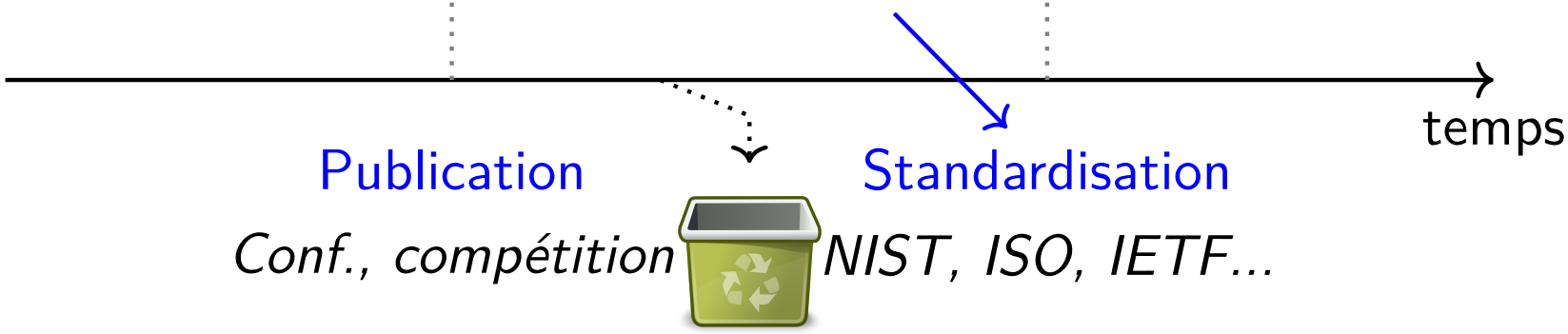
Communauté scientifique

Essaie de casser les algorithmes publiés

On finit par faire confiance à un algorithme bien étudié

Déploiement

Industrie



La standardisation en théorie

Design

Petite équipe

- Cahier des charges
- Spécifications
- Justification du design
- Analyse de sécurité

Analyse publique

Communauté scientifique

Essaie de casser les algorithmes publiés

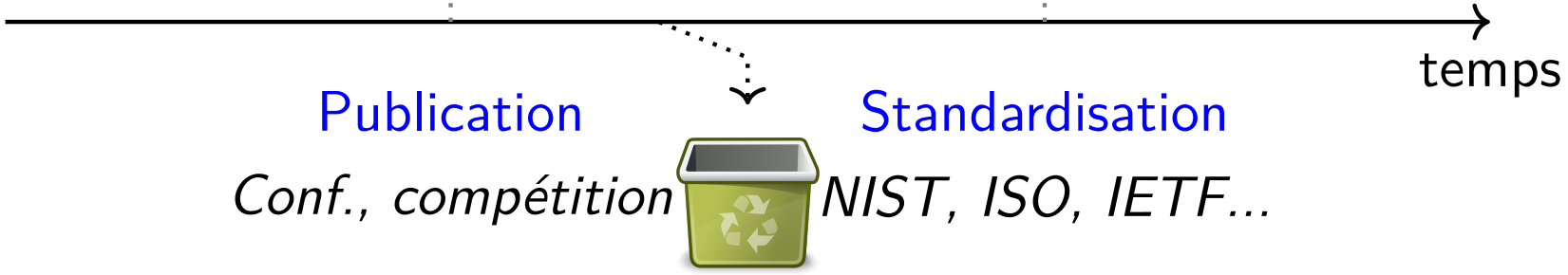
On finit par faire confiance à un algorithme bien étudié

Déploiement

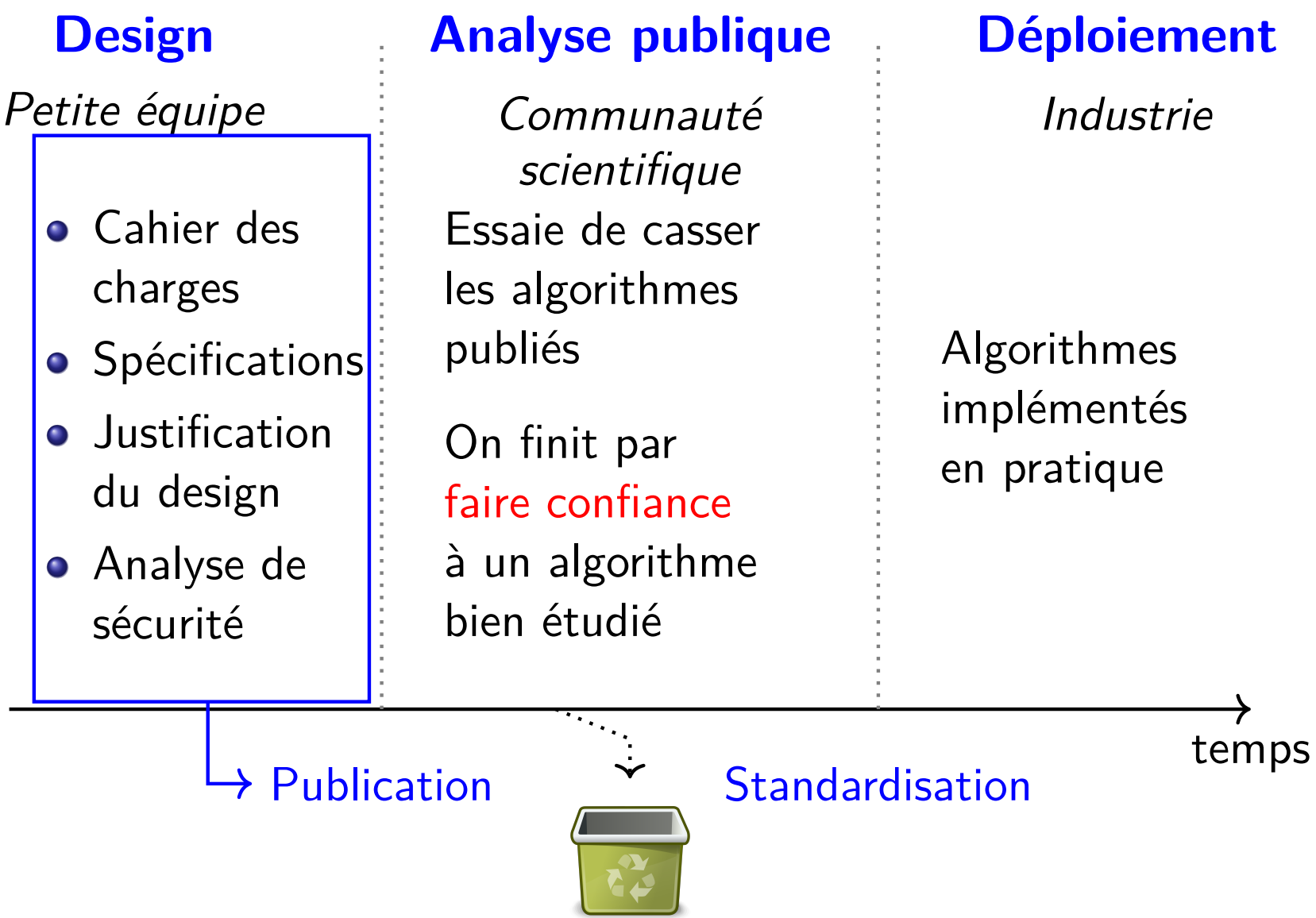
Industrie

Algorithmes implémentés en pratique...

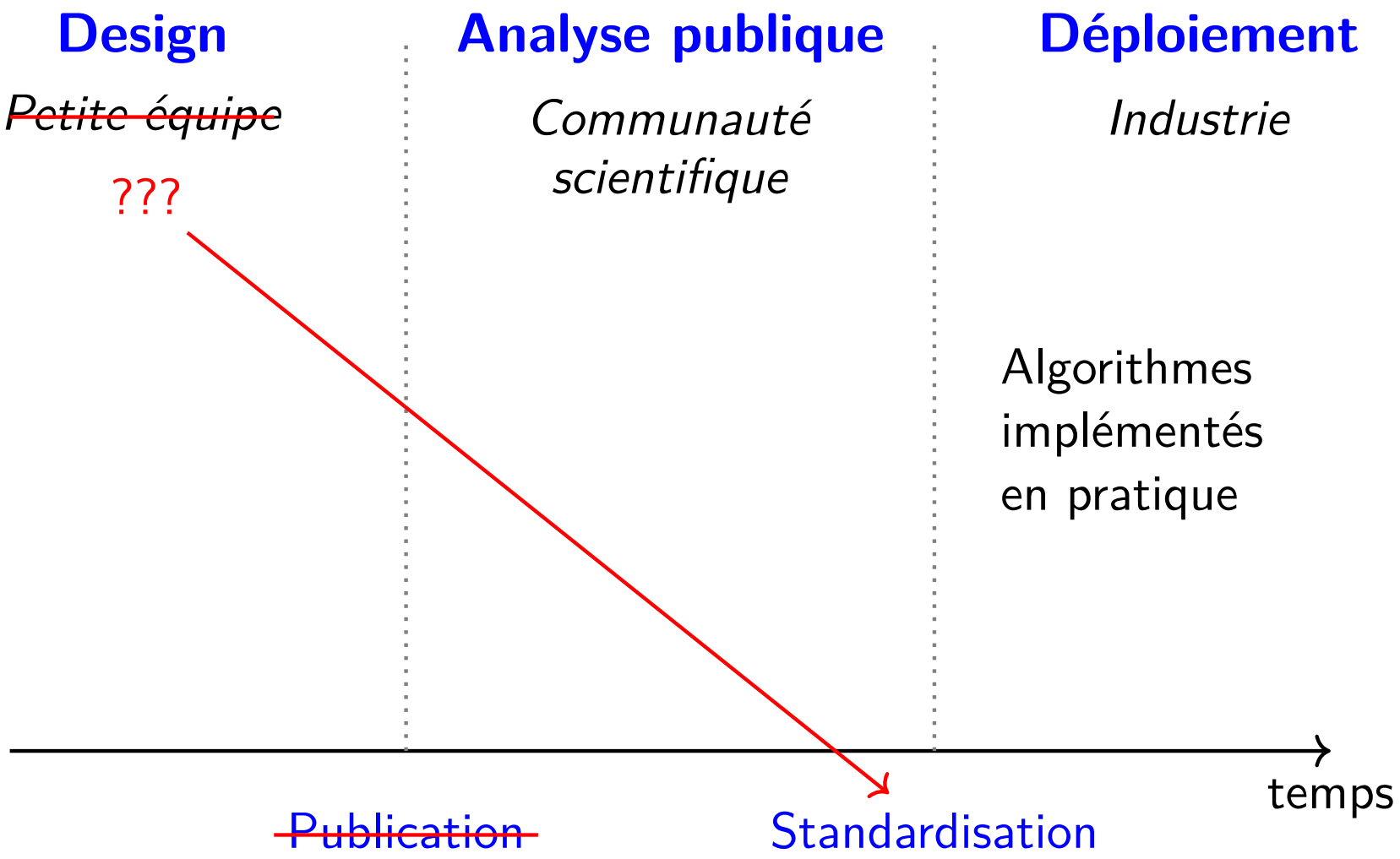
...Jusqu'à ce qu'une nouvelle attaque soit trouvée



Passage en force

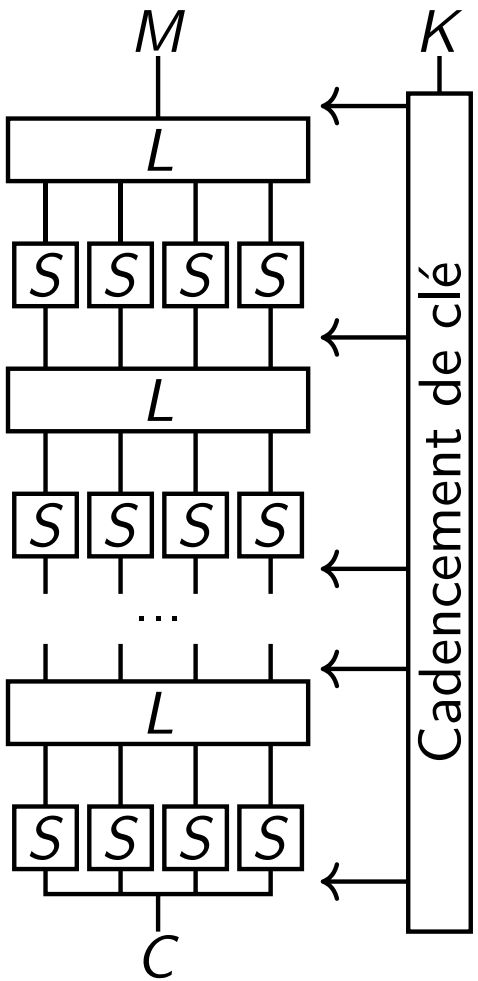


Passage en force



Plan

Réseau de substitution-permutation



Construction standard

- Utilisée par AES, Kuznyechik,. . .
- L (couche linéaire) : diffusion
- S (boîte-S) : confusion

La boîte-S π

π' = (252, 238, 221, 17, 207, 110, 49, 22, 251, 196, 250, 218, 35, 197, 4, 77, 233, 119, 240, 219, 147, 46, 153, 186, 23, 54, 241. 187, 20, 205, 95, 193, 249, 24, 101, 90, 226, 92, 239, 33, 129, 28, 60, 66, 139, 1, 142, 79, 5, 132, 2, 174, 227, 106, 143, 160, 6, 11, 237, 152, 127, 212, 211, 31, 235, 52, 44, 81, 234, 200, 72, 171, 242, 42, 104, 162, 253, 58, 206, 204, 181, 112, 14, 86, 8, 12, 118, 18, 191, 114, 19, 71, 156, 183, 93, 135, 21, 161, 150, 41, 16, 123, 154, 199, 243, 145, 120, 111, 157, 158, 178, 177, 50, 117, 25, 61, 255, 53, 138, 126, 109, 84, 198, 128, 195, 189, 13, 87, 223, 245, 36, 169, 62, 168, 67, 201, 215, 121, 214, 246, 124, 34, 185, 3, 224, 15, 236, 222, 122, 148, 176, 188, 220, 232, 40, 80, 78, 51, 10, 74, 167, 151, 96, 115, 30, 0, 98, 68, 26, 184, 56, 130, 100, 159, 38, 65, 173, 69, 70, 146, 39, 94, 85, 47, 140, 163, 165, 125, 105, 213, 149, 59, 7, 88, 179, 64, 134, 172, 29, 247, 48, 55, 107, 228, 136, 217, 231, 137, 225, 27, 131, 73, 76, 63, 248, 254, 141, 83, 170, 144, 202, 216, 133, 97, 32, 113, 103, 164, 45, 43, 9, 91, 203, 155, 37, 208, 190, 229, 108, 82, 89, 166, 116, 210, 230, 244, 180, 192, 209, 102, 175, 194, 57, 75, 99, 182).

Extrait de la spécification de ***Kuznyechik*** *(2015).*

Justification des designers : choisie aléatoirement

- Propriétés cryptographiques sous-optimales
- Pas de structure mathématique forte

Historique

Juillet 2012 Spécification/Standardisation en Russie de Streebog

Juin 2015 Spécification/Standardisation en Russie de Kuznyechik

Historique

Juillet 2012	Spécification/Standardisation en Russie de Streebog
Aout 2013	RFC de Streebog (RFC6986)
Juin 2015	Spécification/Standardisation en Russie de Kuznyechik
Mars 2016	RFC de Kuznyechik (RFC7801)
Octobre 2018	Streebog à l'ISO (ISO 10118-3)

Historique

Juillet 2012	Spécification/Standardisation en Russie de Streebog	
Aout 2013	RFC de Streebog (RFC6986)	
Juin 2015	Spécification/Standardisation en Russie de Kuznyechik	
Mars 2016	RFC de Kuznyechik (RFC7801)	
Mai 2016	Première décomposition de π	[BPU16]
Octobre 2018	Streebog à l'ISO (ISO 10118-3)	
Janvier 2019	Décomposition finale π	[Per19]

Historique

Juillet 2012	Spécification/Standardisation en Russie de Streebog	
Aout 2013	RFC de Streebog (RFC6986)	
Juin 2015	Spécification/Standardisation en Russie de Kuznyechik	
Mars 2016	RFC de Kuznyechik (RFC7801)	
Mai 2016	Première décomposition de π	[BPU16]
Octobre 2018	Streebog à l'ISO (ISO 10118-3)	
Janvier 2019	Décomposition finale π	[Per19]
Avril 2019	Les designers insistent, π est aléatoire	

Historique

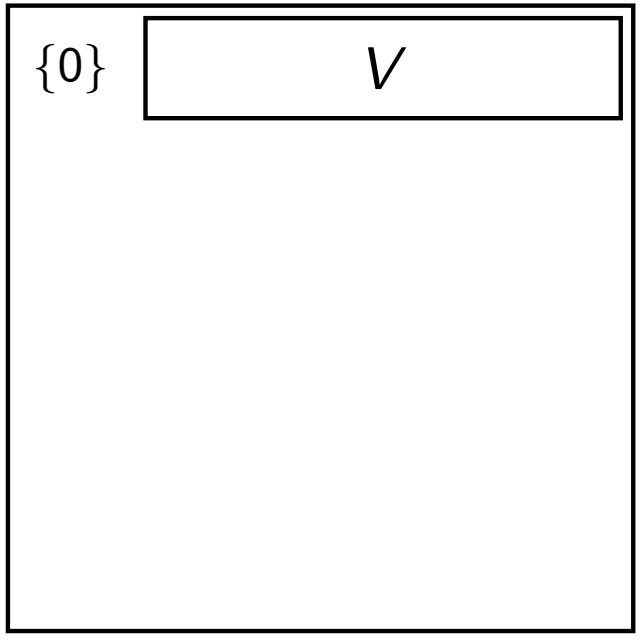
Juillet 2012	Spécification/Standardisation en Russie de Streebog	
Aout 2013	RFC de Streebog (RFC6986)	
Juin 2015	Spécification/Standardisation en Russie de Kuznyechik	
Mars 2016	RFC de Kuznyechik (RFC7801)	
Mai 2016	Première décomposition de π	[BPU16]
Octobre 2018	Streebog à l'ISO (ISO 10118-3)	
Janvier 2019	Décomposition finale π	[Per19]
Avril 2019	Les designers insistent, π est aléatoire	
Septembre 2019 ?	Kuznyechik à l'ISO	

Plan

Des classes vers des classes

$$(\{0, 1, \ldots 255\}, \oplus, \times)$$

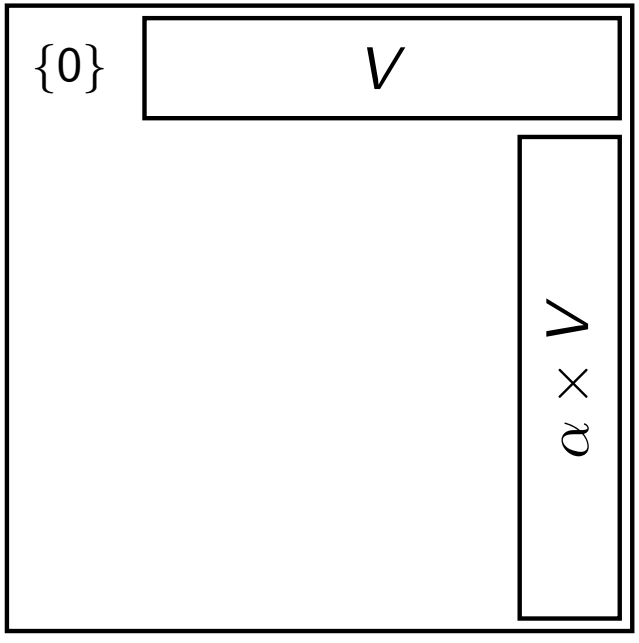
$$|V| = 15$$



Des classes vers des classes

$$(\{0, 1, \ldots 255\}, \oplus, \times)$$

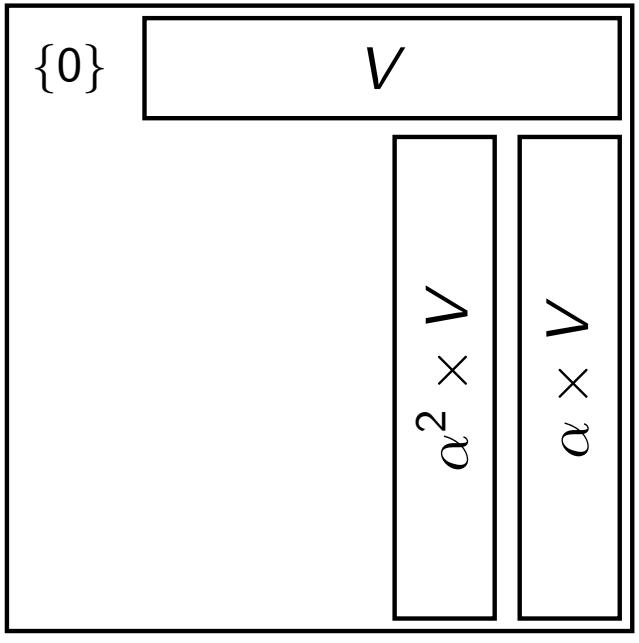
$$|V| = 15$$



Des classes vers des classes

$$(\{0, 1, \ldots 255\}, \oplus, \times)$$

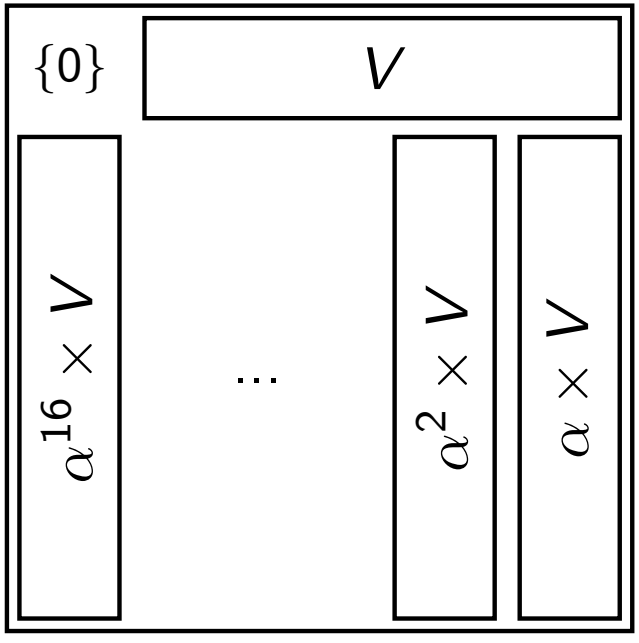
$$|V| = 15$$



Des classes vers des classes

$$(\{0, 1, \ldots 255\}, \oplus, \times)$$

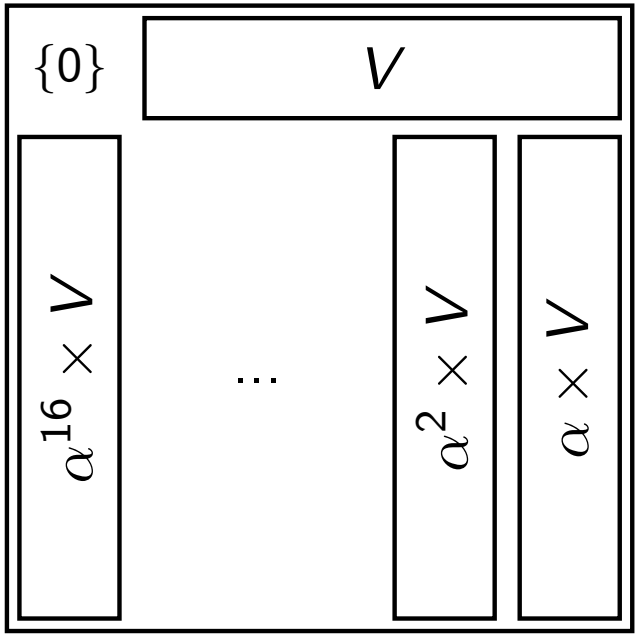
$$|V| = 15$$

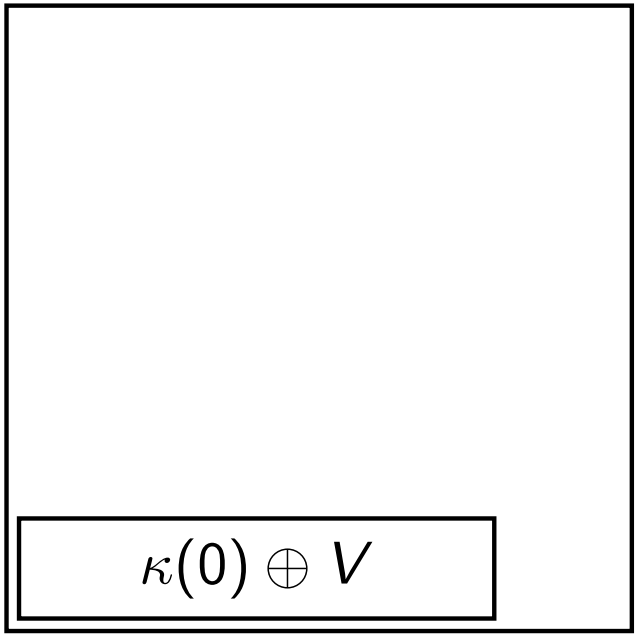


Des classes vers des classes

$$(\{0, 1, \ldots 255\}, \oplus, \times)$$

$$|V| = 15$$

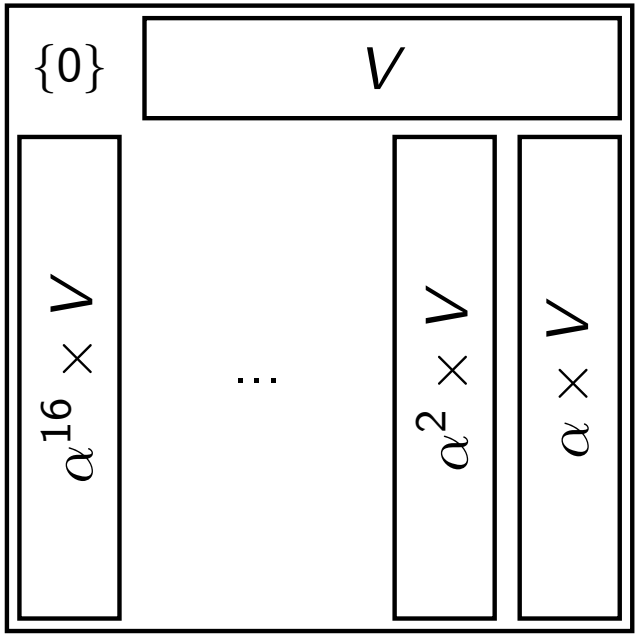


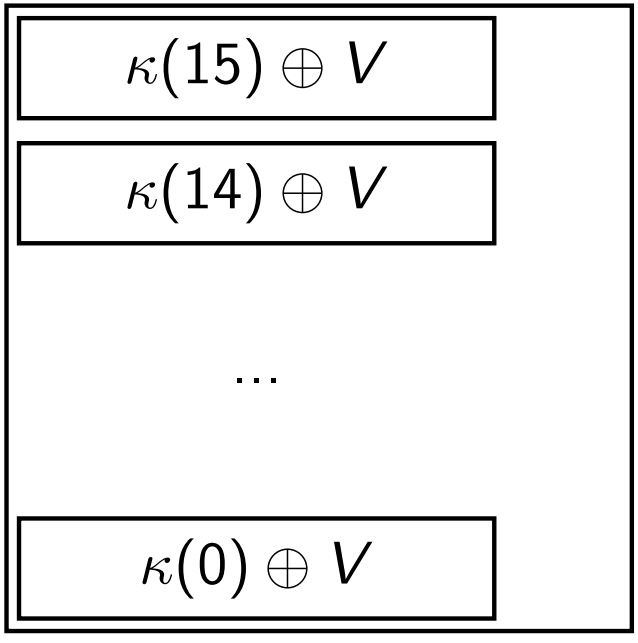


Des classes vers des classes

$$(\{0, 1, \ldots 255\}, \oplus, \times)$$

$$|V| = 15$$

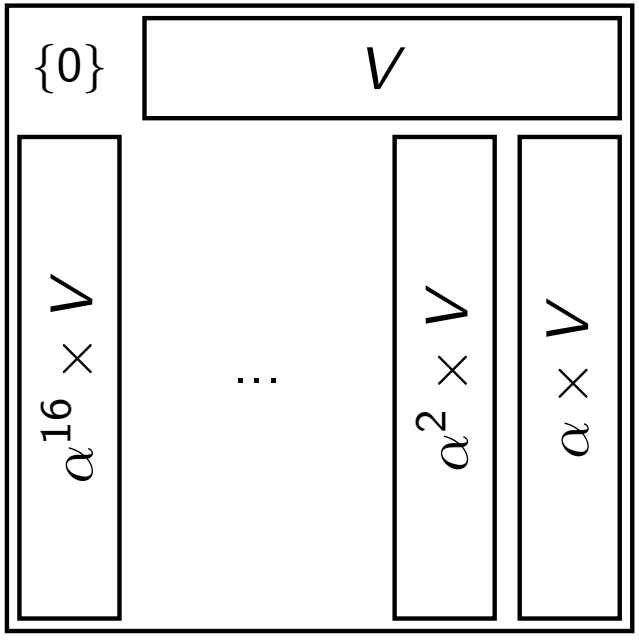


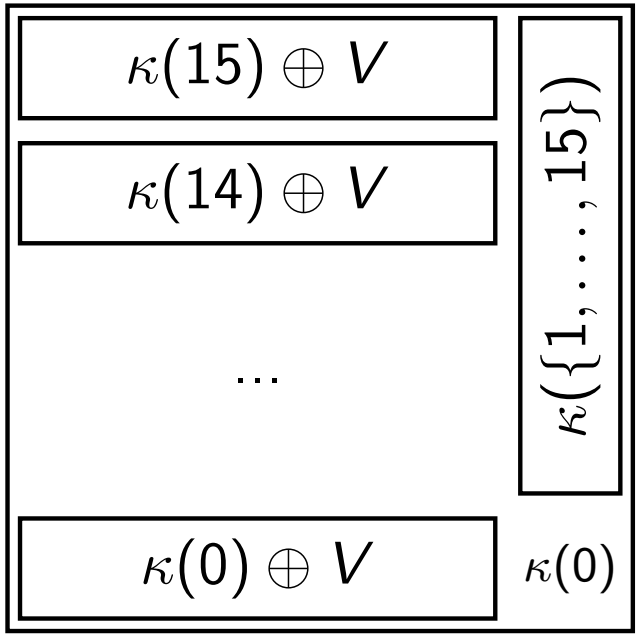


Des classes vers des classes

$$(\{0, 1, \ldots 255\}, \oplus, \times)$$

$$|V| = 15$$

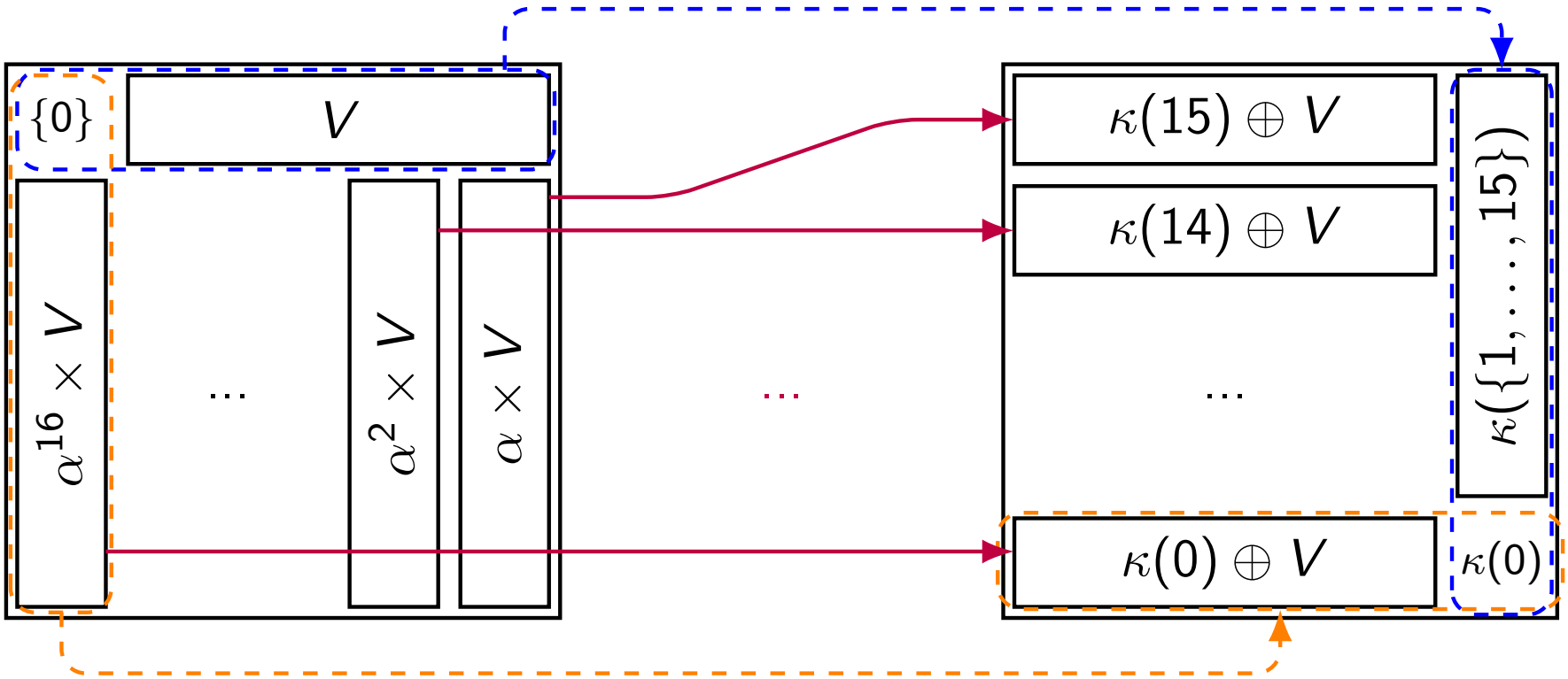




Des classes vers des classes

$$(\{0, 1, \ldots 255\}, \oplus, \times)$$

$$|V| = 15$$



Coincidence ? [BPT19]

Coincidence ? [BPT19]

```
p(x){unsigned char*k="@`rFTDVbpPB
vdtfR@\xacp?\xe2>4\xa6\xe9{z\xe3q
5\xa7\xe8",a=2,l=0,b=17;while(x&&
(l++,a^x))a=2*a^a/128*29;return l
%b?k[l%b]^k[b+l/b]^b:k[l/b]^188;}
```

Coincidence ? [BPT19]

```
p(x){unsigned char*k="@`rFTDVbpPB
vdtfR@\xacp?\xe2>4\xa6\xe9{z\xe3q
5\xa7\xe8",a=2,l=0,b=17;while(x&&
(l++,a^x))a=2*a^a/128*29;return l
%b?k[l%b]^k[b+l/b]^b:k[l/b]^188;}
```

code C

- Permutations sur 8 bits : 2^{1684}
- Nombre de programmes d'au plus 165 caractères : 2^{1156}
- Probabilité d'une implémentation aussi courte $\leq 2^{-528}$

Coincidence ? [BPT19]

```
p(x){unsigned char*k="@`rFTDVbpPB
vdtfR@\xacp?\xe2>4\xa6\xe9{z\xe3q
5\xa7\xe8",a=2,l=0,b=17;while(x&&
(l++,a^x))a=2*a^a/128*29;return l
%b?k[l%b]^k[b+l/b]^b:k[l/b]^188;}
```

code C

- Permutations sur 8 bits : 2^{1684}
- Nombre de programmes d'au plus 165 caractères : 2^{1156}
- Probabilité d'une implémentation aussi courte $\leq 2^{-528}$

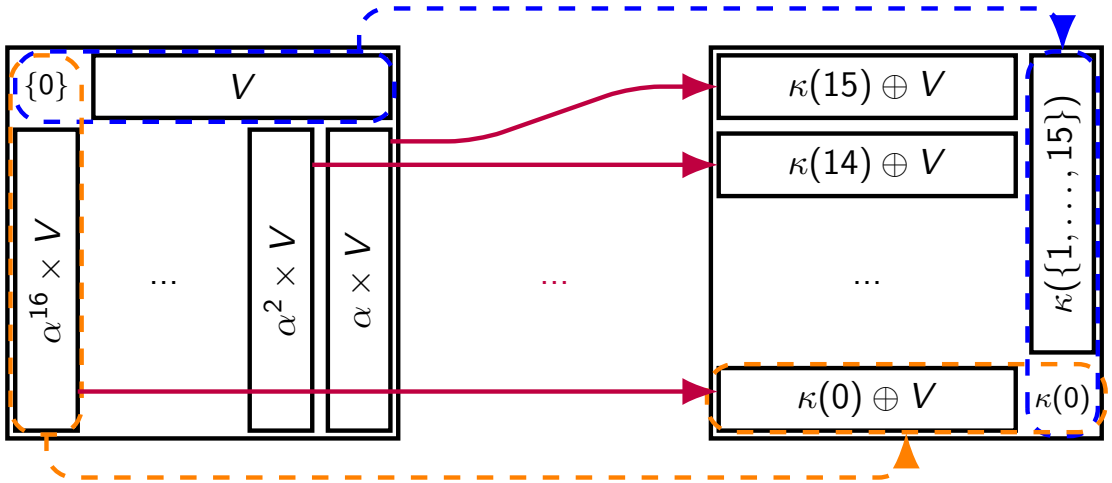
Concours d'implémentations courtes :

`https://who.paris.inria.fr/Leo.Perrin/short-implem.html`

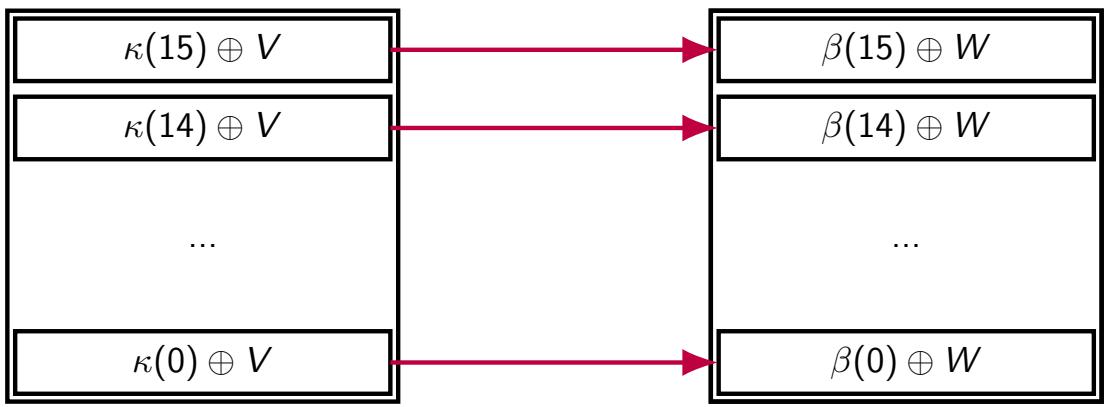
`https://codegolf.stackexchange.com/questions/186498/`

Une backdoor ?

π



Boite S de chiffrement avec backdoor [BBF16]



Conclusion

- La boîte-S de Streebog et Kuznyechik a une structure mathématique
- Contrairement à ce que disent les designers, cette structure est délibérée
- N'utilisez ni Streebog, ni Kuznyechik
- Standard $\neq$ bon

Références I

Arnaud Bannier, Nicolas Bodin, and Eric Filiol.
Partition-based trapdoor ciphers.
Cryptology ePrint Archive, Report 2016/493, 2016.
http://eprint.iacr.org/2016/493.

Xavier Bonnetain, Léo Perrin, and Shizhu Tian.
Anomalies and vector space search : Tools for s-box reverse-engineering.
Cryptology ePrint Archive, Report 2019/528, 2019.
https://eprint.iacr.org/2019/528.

Références II


Alex Biryukov, Léo Perrin, and Aleksei Udovenko.
Reverse-engineering the S-box of streebog, kuznyechik and STRIBOBr1.
In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 372–402. Springer, Heidelberg, May 2016.


Léo Perrin.
Partitions in the S-box of Streebog and Kuznyechik.
IACR Trans. Symm. Cryptol., 2019(1) :302–329, 2019.