Schémas de signature post-quantiques: Construction et cryptanalyse

Casser de la cryptographie post-quantique avec un ordinateur portable pour assurer la sécurité de vos communications.

Pierre Pébereau

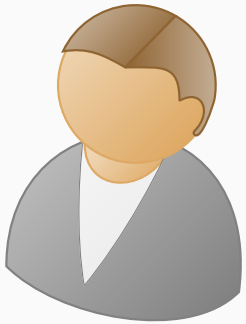
Thales SIX, Sorbonne Université, LIP6, CNRS

Thèse encadrée par Simon Abelard (Thales SIX) et Mohab Safey el Din (LIP6)

March, 2024

Cryptographie asymétrique

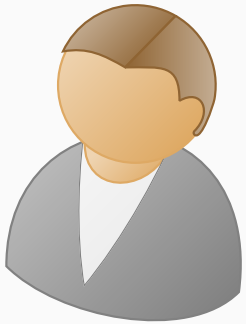
Alice



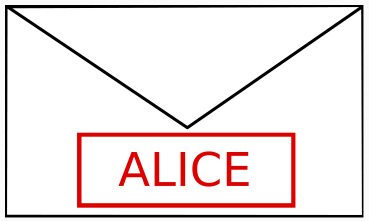
Bob

Cryptographie asymétrique

Alice

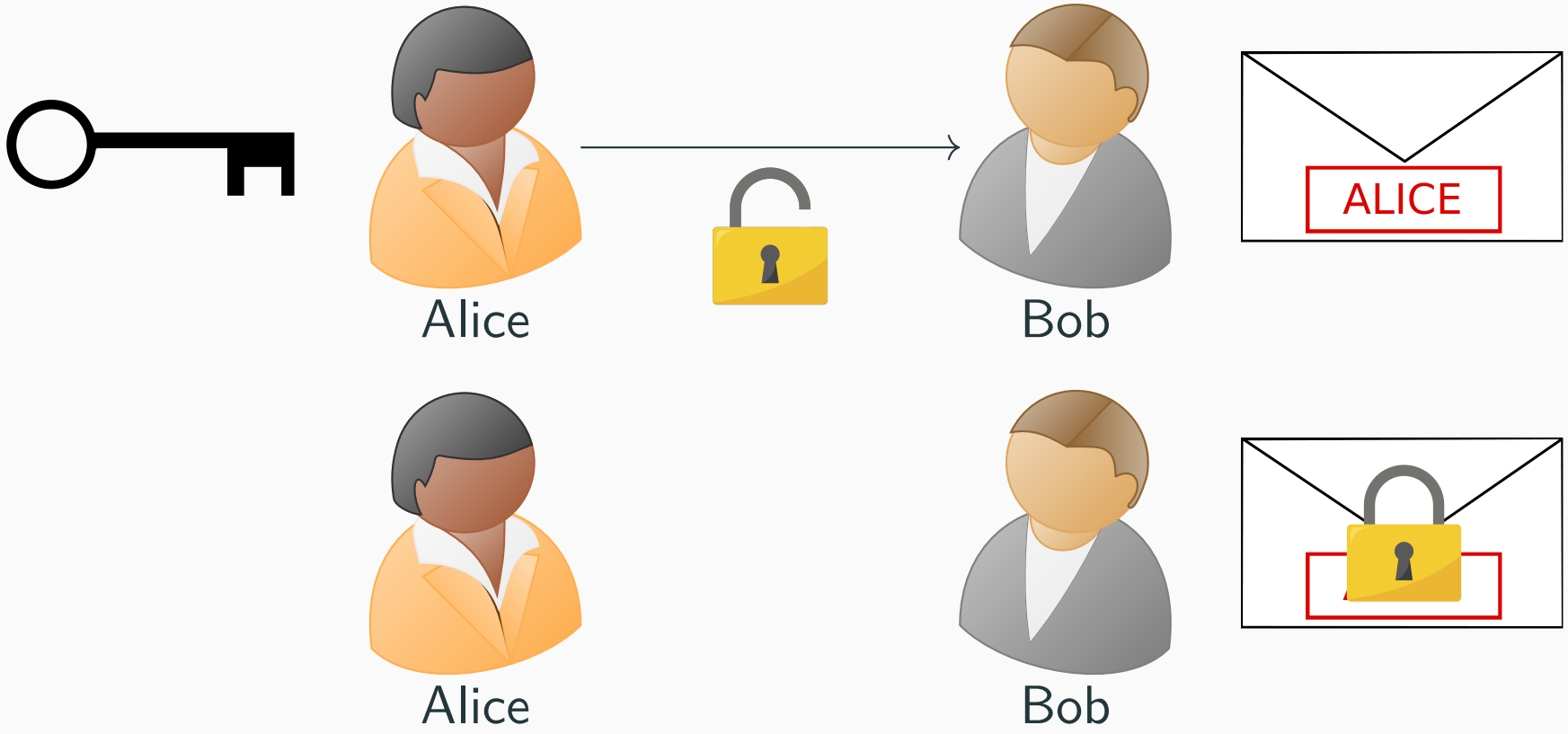


Bob

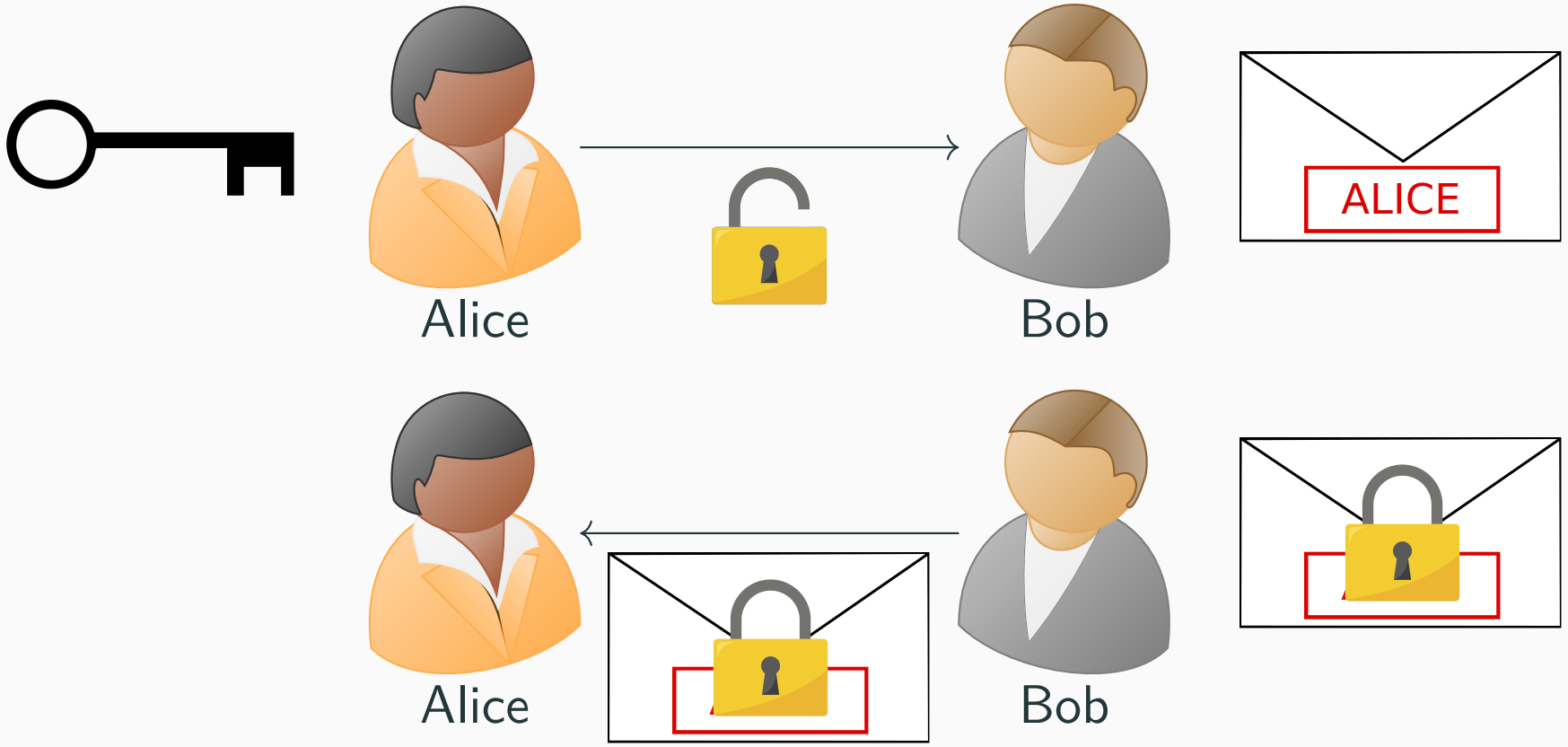


Cryptographie asymétrique

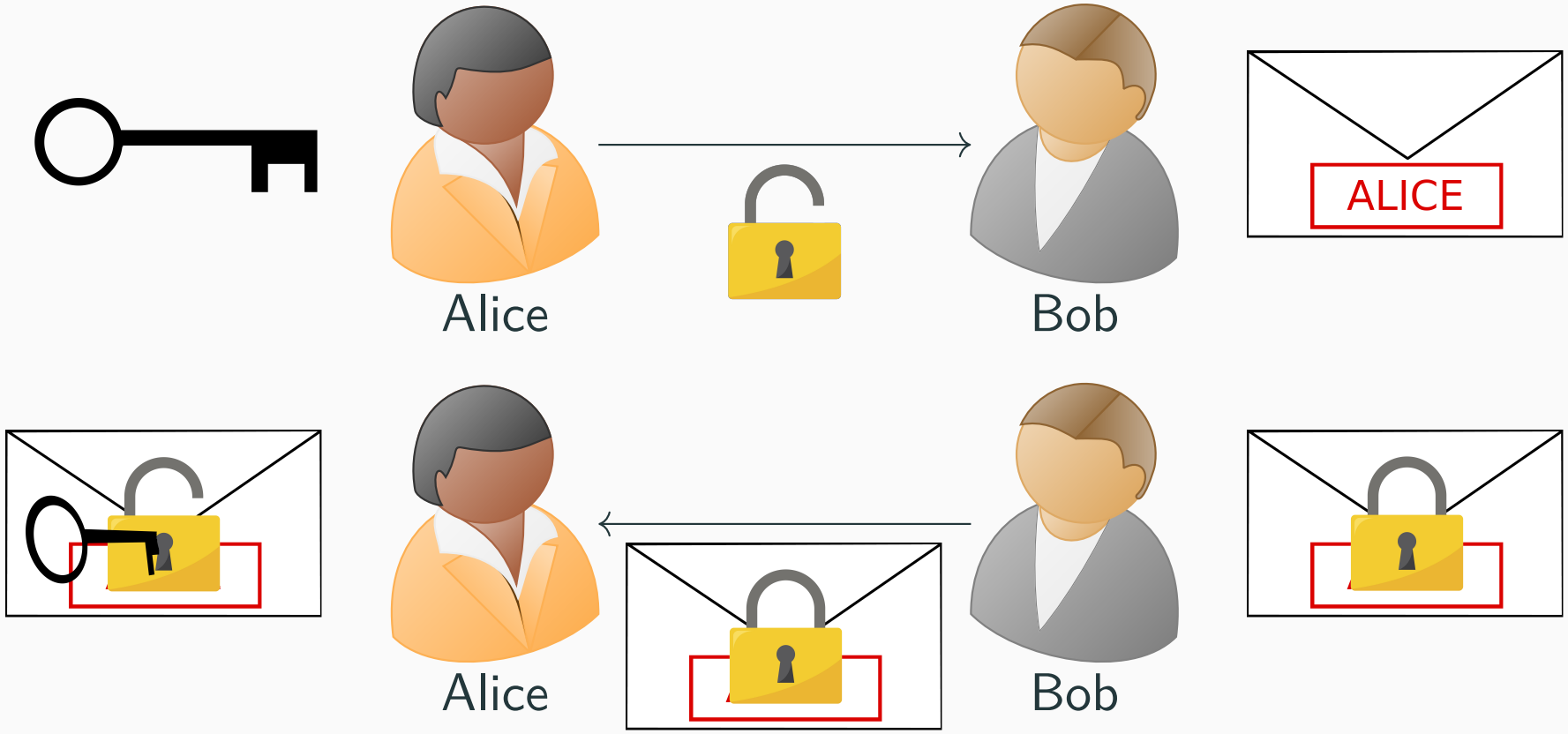
Cryptographie asymétrique



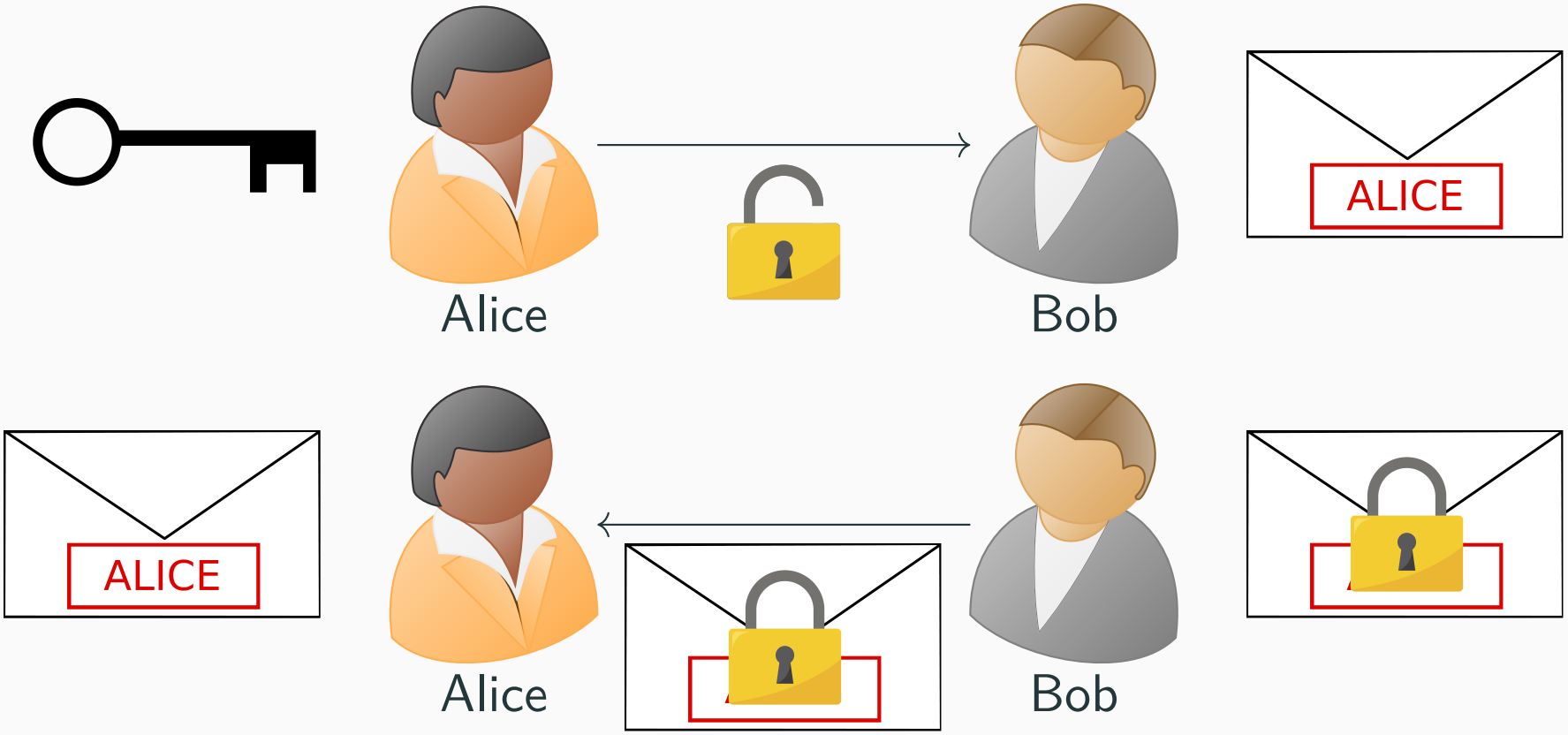
Cryptographie asymétrique



Cryptographie asymétrique

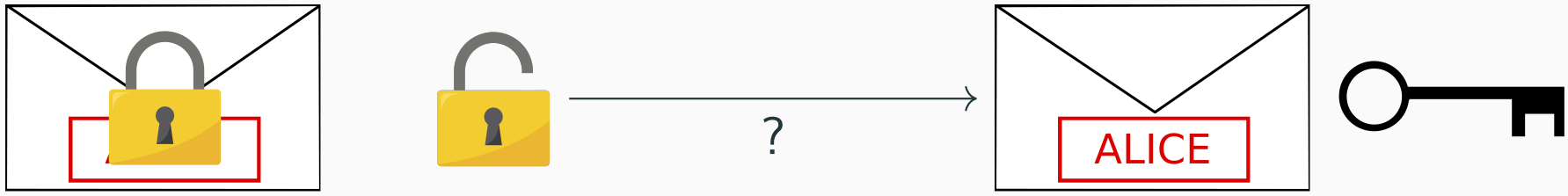


Cryptographie asymétrique



Cryptanalyse

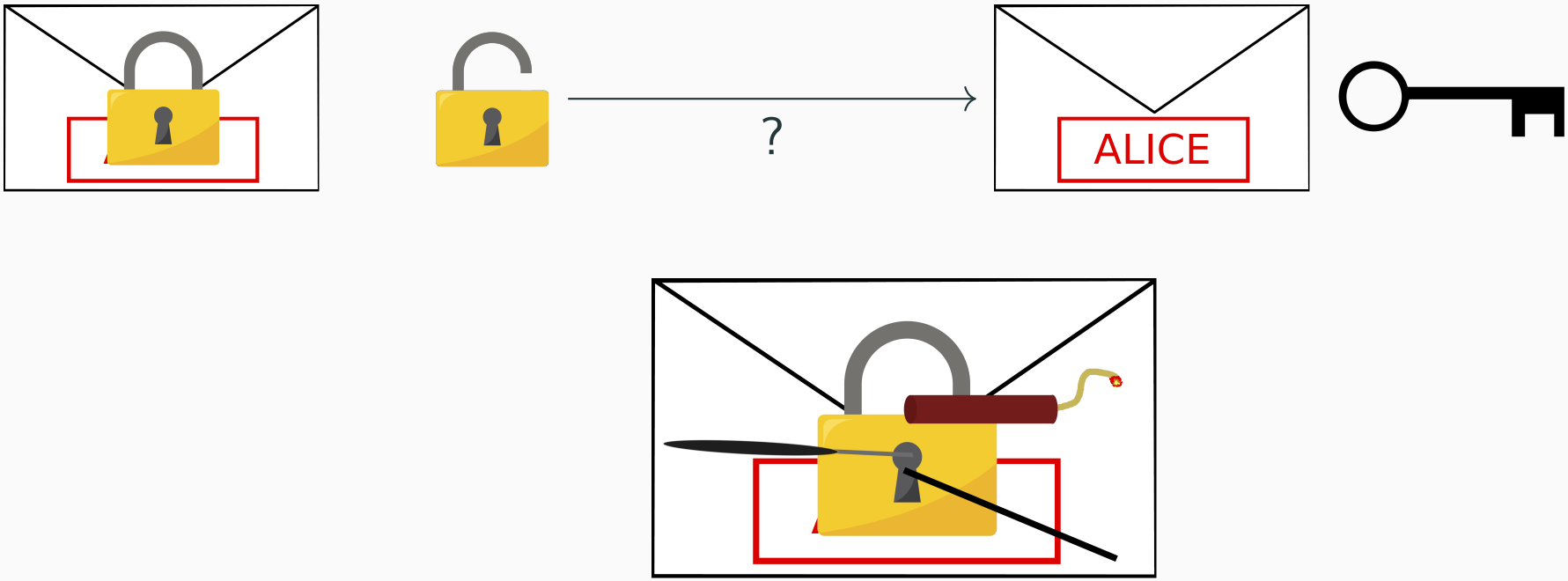
Cryptanalyse



Modéliser l'adversaire

- Informations: données publiques, couples clair/chiffrés ...
- Budget de calcul: puissance, temps, dollar-cost ...

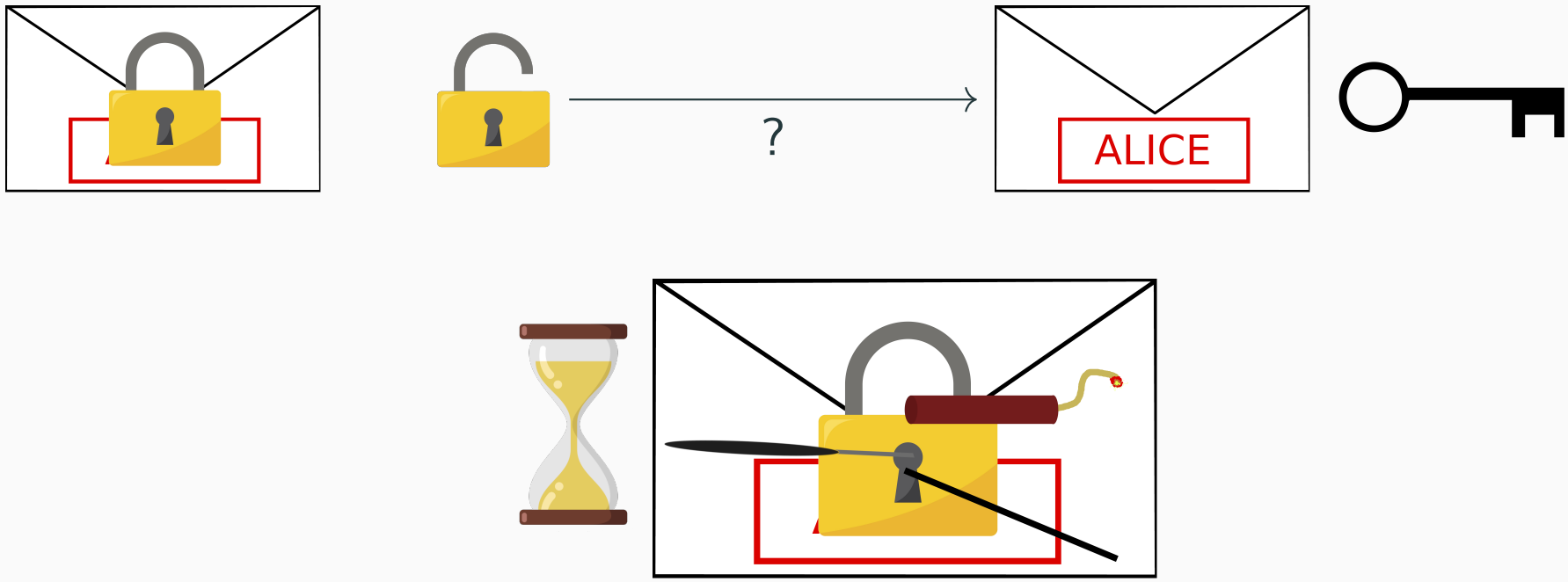
Cryptanalyse



Modéliser l'adversaire

- Informations: données publiques, couples clair/chiffrés ...
- Budget de calcul: puissance, temps, dollar-cost ...

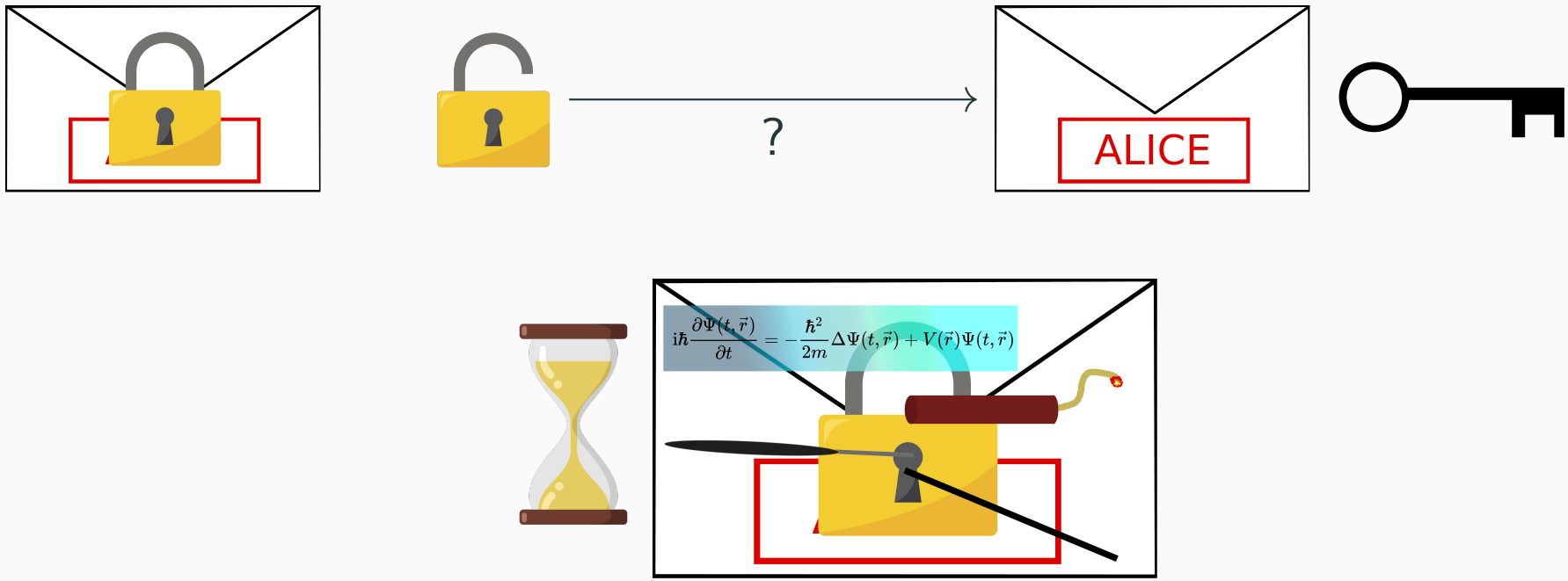
Cryptanalyse



Modéliser l'adversaire

- Informations: données publiques, couples clair/chiffrés ...
- Budget de calcul: puissance, temps, dollar-cost ...

Cryptanalyse Post-Quantique



Modéliser l'adversaire

- Informations: données publiques, couples clair/chiffrés ...
- Budget de calcul: puissance, temps, dollar-cost ...

Contexte

https://cyber.gouv.fr/sites/default/files/document/Avis de l'ANSSI sur la migration vers la cryptographie.pdf

"L'ANSSI encourage toutes les industries à inclure la menace quantique dans leur analyse de risque et à envisager d'inclure des mesures de protection quantique dans les produits cryptographiques concernés."

Avis de l'ANSSI sur la migration vers la cryptographie post-quantique, 21 décembre 2023

Contexte

https://cyber.gouv.fr/sites/default/files/document/Avis de l'ANSSI sur la migration vers la cryptographie.pdf

"L'ANSSI encourage toutes les industries à inclure la menace quantique dans leur analyse de risque et à envisager d'inclure des mesures de protection quantique dans les produits cryptographiques concernés."

Avis de l'ANSSI sur la migration vers la cryptographie post-quantique, 21 décembre 2023

Produits cryptographiques

https://cyber.gouv.fr/sites/default/files/document/Avis de l'ANSSI sur la migration vers la cryptographie.pdf

Produits cryptographiques

https://cyber.gouv.fr/sites/default/files/document/Avis de l'ANSSI sur la migration vers la cryptographie.pdf

Produits cryptographiques

https://cyber.gouv.fr/sites/default/files/document/Avis de l'ANSSI sur la migration vers la cryptographie.pdf

Contraintes des systèmes

- Protocole web sécurisé $\rightarrow$ Nombre élevé d'échanges
- Systèmes satellitaires $\rightarrow$ Puissance de calcul/bande passante

Produits cryptographiques

https://cyber.gouv.fr/sites/default/files/document/Avis de l'ANSSI sur la migration vers la cryptographie.pdf

Contraintes des systèmes

- Protocole web sécurisé $\rightarrow$ Nombre élevé d'échanges
- Systèmes satellitaires $\rightarrow$ Puissance de calcul/bande passante

Performances des solutions

- Sûres face à des attaquants disposant de moyens importants

Produits cryptographiques

https://cyber.gouv.fr/sites/default/files/document/Avis de l'ANSSI sur la migration vers la cryptographie.pdf

Contraintes des systèmes

- Protocole web sécurisé $\rightarrow$ Nombre élevé d'échanges
- Systèmes satellitaires $\rightarrow$ Puissance de calcul/bande passante

Performances des solutions

- Sûres face à des attaquants disposant de moyens importants
- Coûts de communication limités en temps et en taille

Puissance de calcul

Modèle scientifique

On définit la sécurité selon les capacités de l'adversaire:

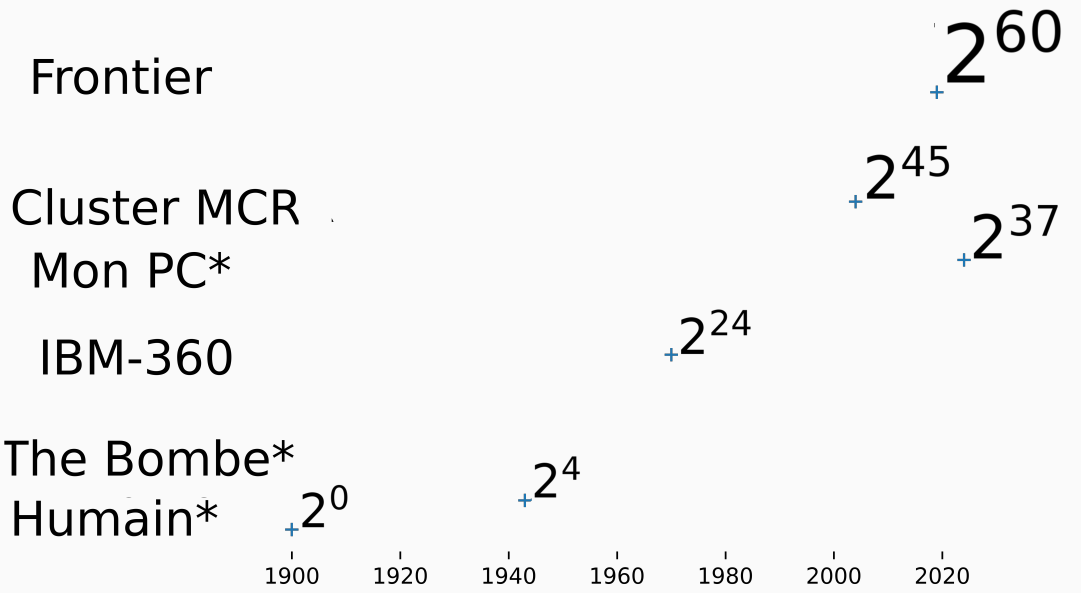
Puissance des supercalculateurs, hashrate du Bitcoin, ...

Puissance de calcul

Modèle scientifique

On définit la sécurité selon les capacités de l'adversaire:

Puissance des supercalculateurs, hashrate du Bitcoin, ...



Nombre d'opérations en virgule flottante par seconde ($\log_2$)

Puissance de calcul

Modèle scientifique

On définit la sécurité selon les capacités de l'adversaire:

Puissance des supercalculateurs, hashrate du Bitcoin, ...

Niveau	Nombre d'opérations*	Temps de calcul pour Frontier
I	2^{143}	$\approx 10^{17}$ années
III	2^{192}	$\approx 10^{32}$ années
V	2^{272}	$\approx 10^{56}$ années

Niveau de sécurité selon le NIST.

Puissance de calcul

Modèle scientifique

On définit la sécurité selon les capacités de l'adversaire:

Puissance des supercalculateurs, hashrate du Bitcoin, ...

Niveau	Nombre d'opérations*	Temps de calcul pour Frontier
I	2^{143}	$\approx 10^{17}$ années
III	2^{192}	$\approx 10^{32}$ années
V	2^{272}	$\approx 10^{56}$ années

Niveau de sécurité selon le NIST.

Repère

Âge de l'univers: $\approx 10^{10}$ années

Équation Polynomiale Multivariée

$$\mathcal{P}(\boldsymbol{x}) = \boldsymbol{t} \iff \begin{cases} P_1(x_1, \ldots, x_n) = t_1 \\ \vdots \\ P_m(x_1, \ldots, x_n) = t_m \end{cases}$$

Équation Polynomiale Multivariée

$$\mathcal{P}(\boldsymbol{x}) = \boldsymbol{t} \iff \begin{cases} P_1(x_1, \ldots, x_n) = t_1 \\ \vdots \\ P_m(x_1, \ldots, x_n) = t_m \end{cases}$$

Problème NP-difficile

- Avec $x_1, \ldots, x_n$, il est facile de vérifier $\mathcal{P}(x_1, \ldots, x_n) = (t_1, \ldots, t_m)$

Équation Polynomiale Multivariée

$$\mathcal{P}(\boldsymbol{x}) = \boldsymbol{t} \iff \begin{cases} P_1(x_1, \ldots, x_n) = t_1 \\ \vdots \\ P_m(x_1, \ldots, x_n) = t_m \end{cases}$$

Problème NP-difficile

- Avec $x_1, \ldots, x_n$, il est facile de vérifier $\mathcal{P}(x_1, \ldots, x_n) = (t_1, \ldots, t_m)$
- Avec $t_1, \ldots, t_m$, il est difficile de trouver $x_1, \ldots, x_n$ tels que $\mathcal{P}(x_1, \ldots, x_n) = (t_1, \ldots, t_m)$

Exemple générique

Un système de 2 équations à 3 trois inconnues

$$\mathcal{P}(x,y,z) : \begin{cases} xy + xz + z^2 + x + y + z + 3 & = 0 \\ 5xy - xz + 3z^2 - x - y - z + 2 & = 0 \end{cases}$$

Exemple générique

Un système de 2 équations à 3 trois inconnues

$$\mathcal{P}(x,y,z) : \begin{cases} xy + xz + z^2 + x + y + z + 3 & = 0 \\ 5xy - xz + 3z^2 - x - y - z + 2 & = 0 \end{cases}$$

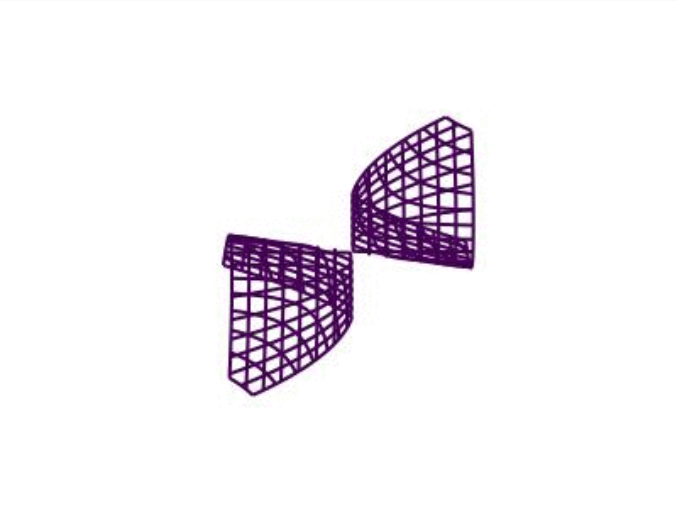


Figure 1: Hypersurface définie par le système $\mathcal{P}(x,y,z)$ dans $\mathbb{R}^3$.

Exemple singulier

Un autre système de 2 équations à 3 trois inconnues

$$\mathcal{P}(x,y,z) : \begin{cases} zy + xz + z^2 + x + y + z + 3 & = 0 \\ 5zy - xz + 3z^2 - x - y - z + 2 & = 0 \end{cases}$$

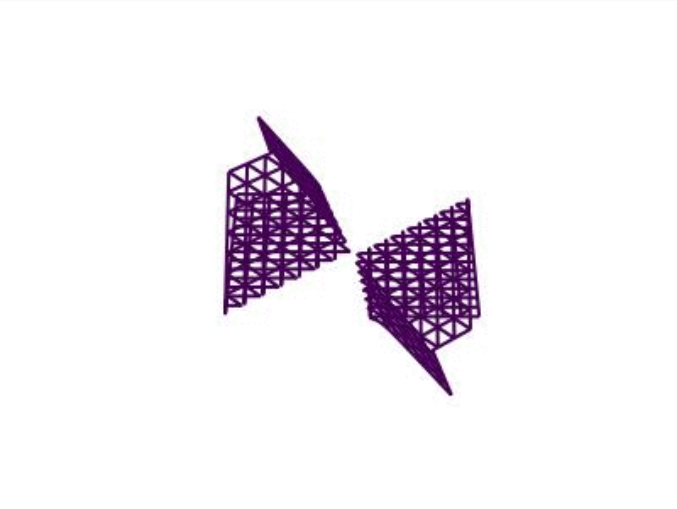
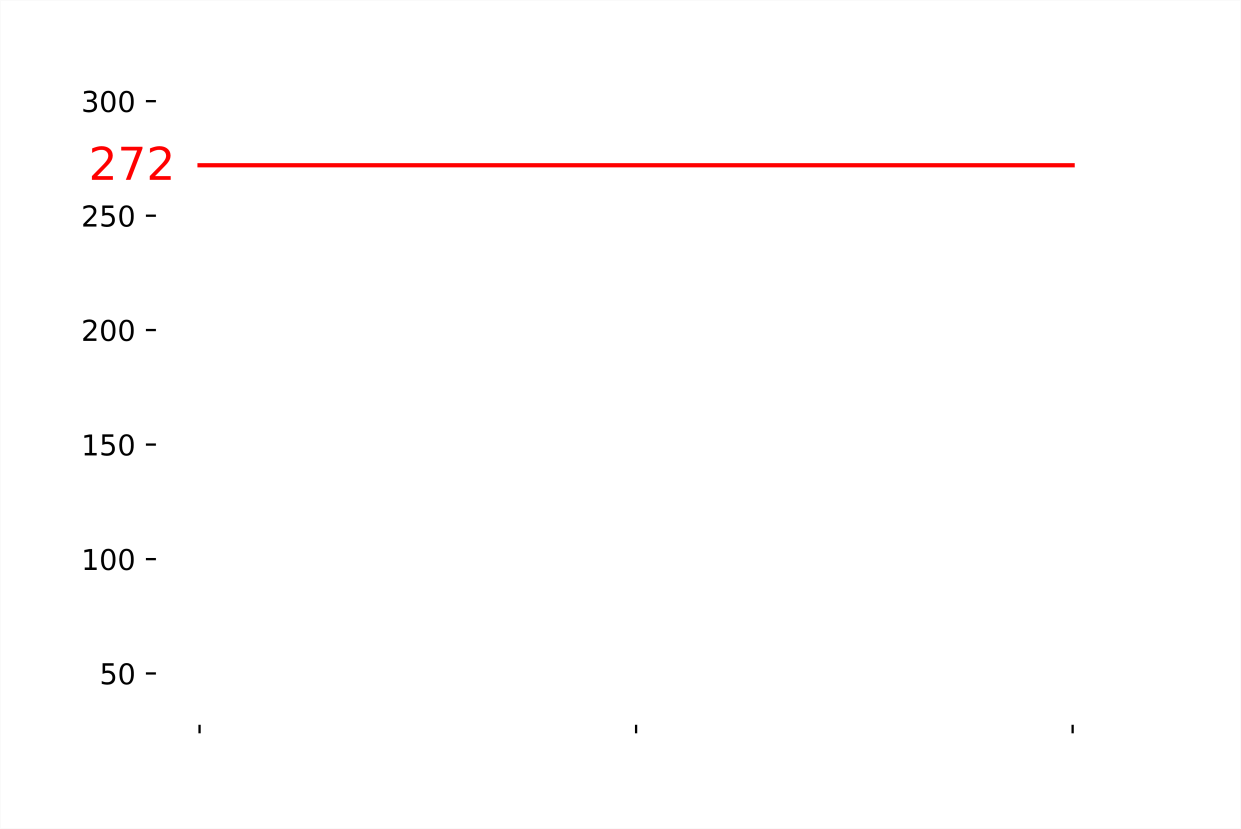


Figure 2: Hypersurface définie par le système $\mathcal{P}(x,y,z)$ dans $\mathbb{R}^3$.

Cryptanalyse d'un schéma de signature multivarié: VOX

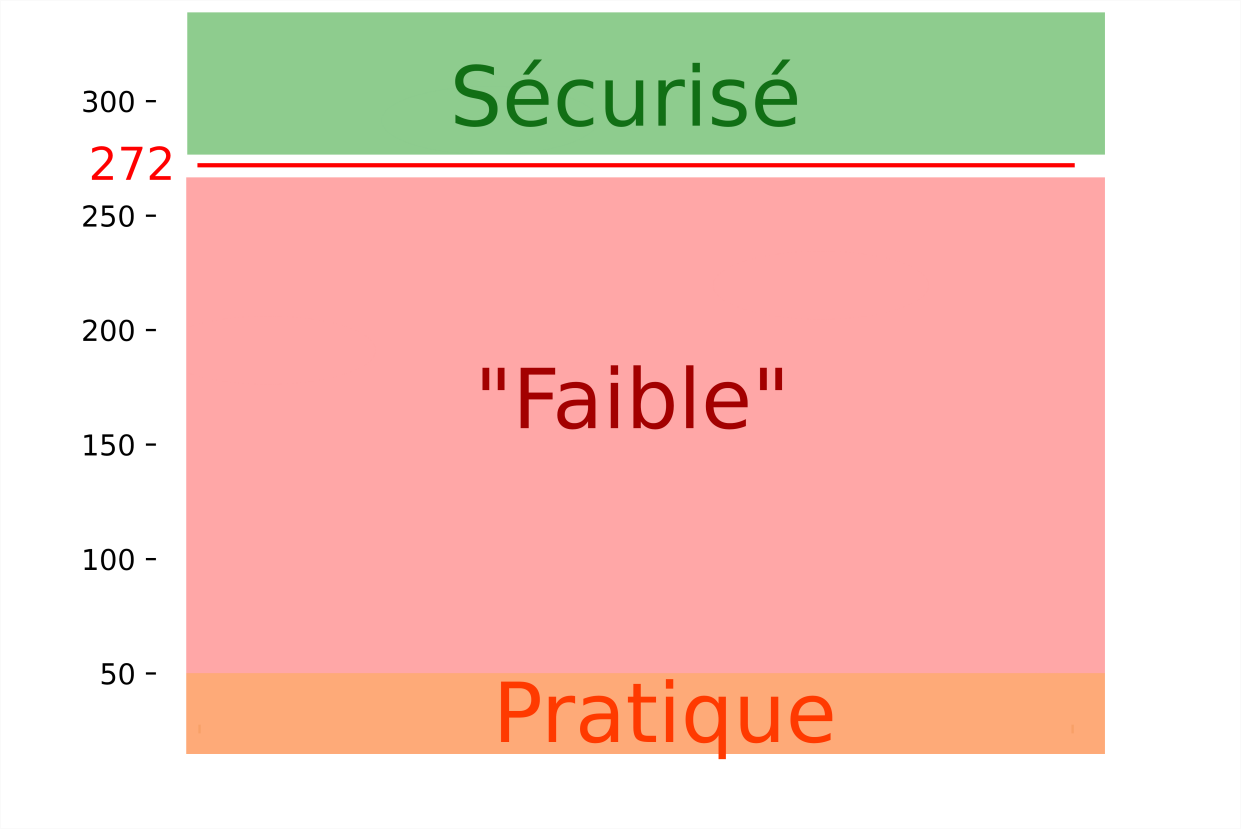


Échelle logarithmique du niveau de sécurité

Références

Niveau de sécurité V: 2^{272} opérations au moins

Cryptanalyse d'un schéma de signature multivarié: VOX

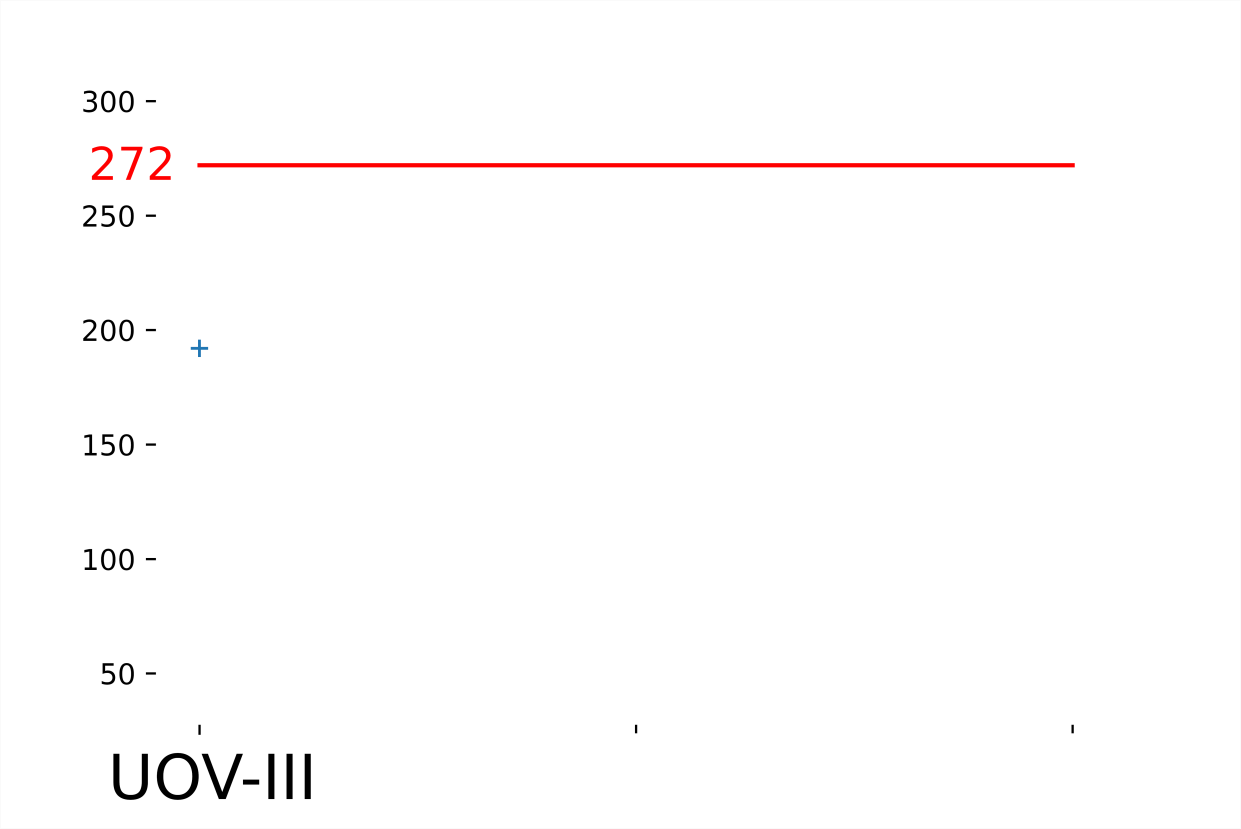


Échelle logarithmique du niveau de sécurité

Références

Niveau de sécurité V: 2^{272} opérations au moins

Cryptanalyse d'un schéma de signature multivarié: VOX

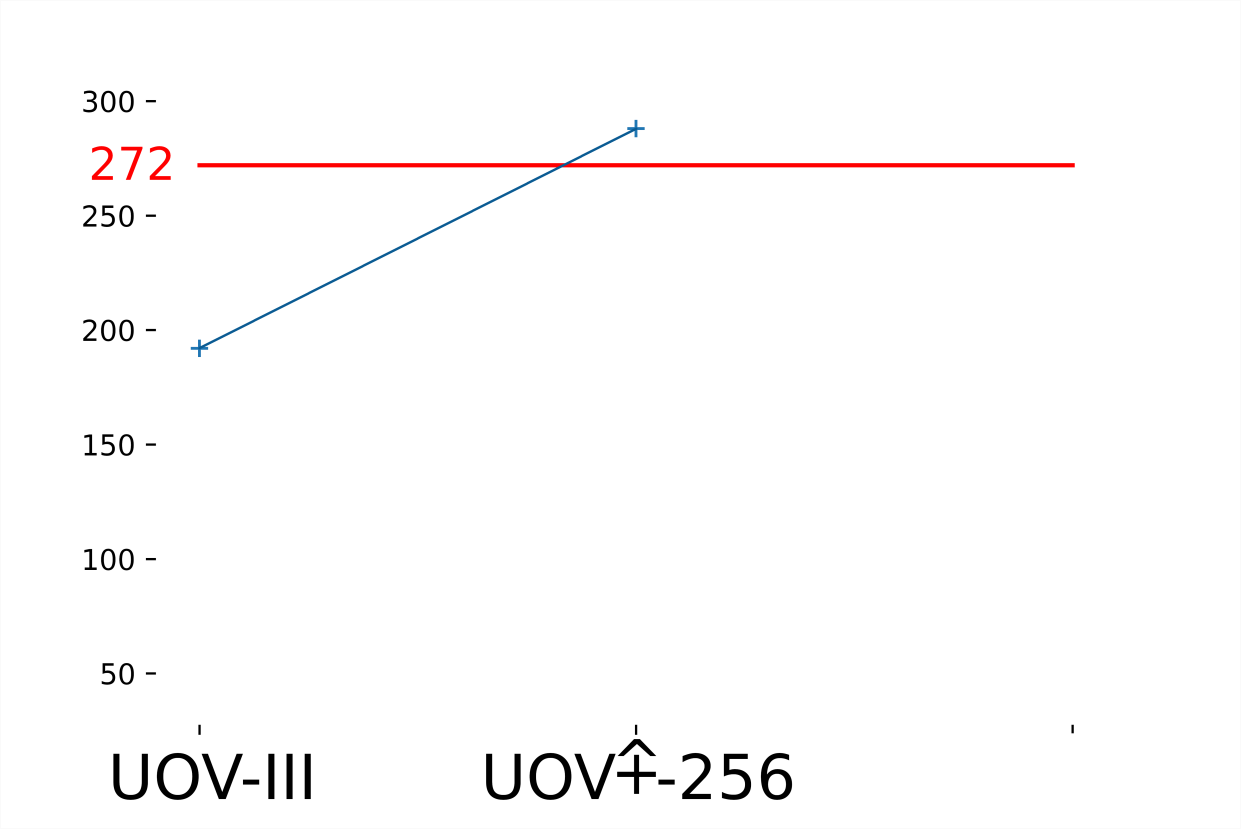


Échelle logarithmique du niveau de sécurité

Références

Unbalanced Oil and Vinegar [Kipnis, Patarin, Goubin, 1999]

Cryptanalyse d'un schéma de signature multivarié: VOX

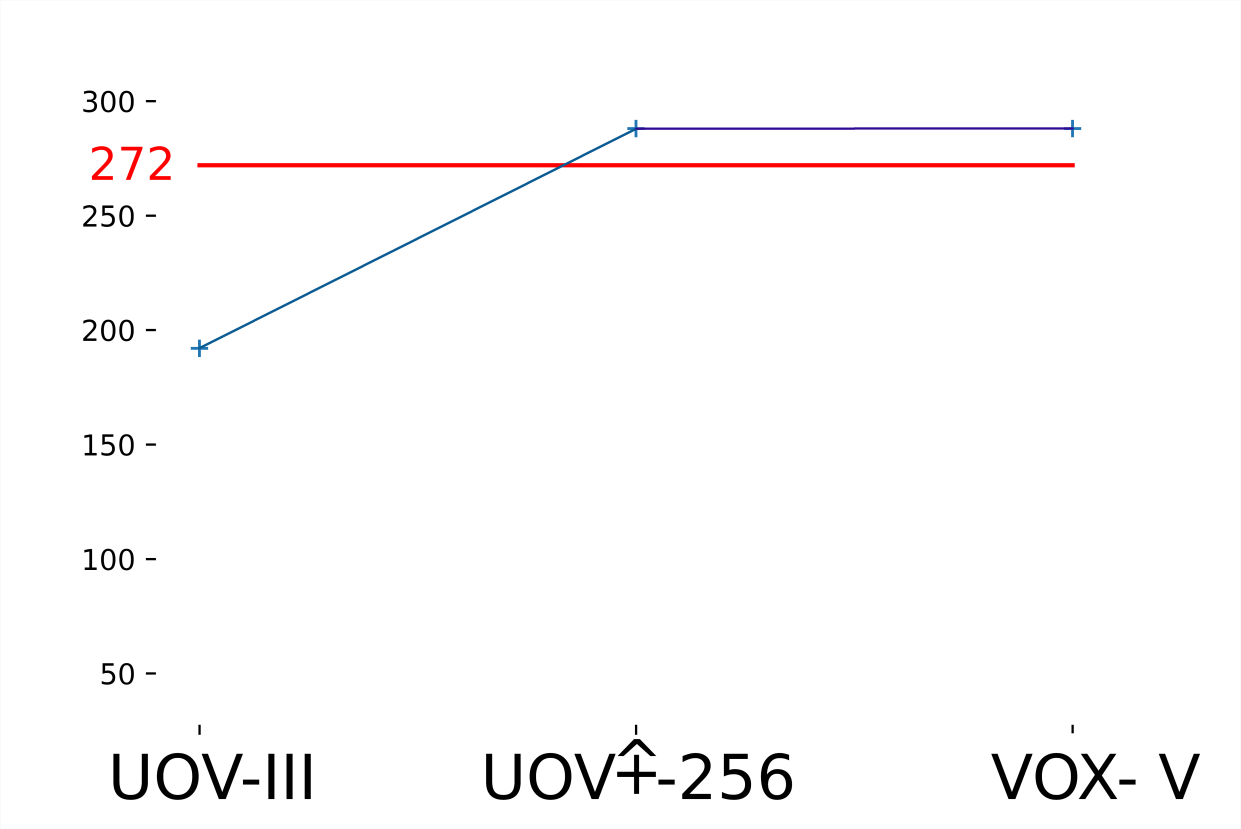


Échelle logarithmique du niveau de sécurité

Références

UOV "Hat Plus" [Faugère, Macario-Rat, Patarin, Perret, 2022]

Cryptanalyse d'un schéma de signature multivarié: VOX



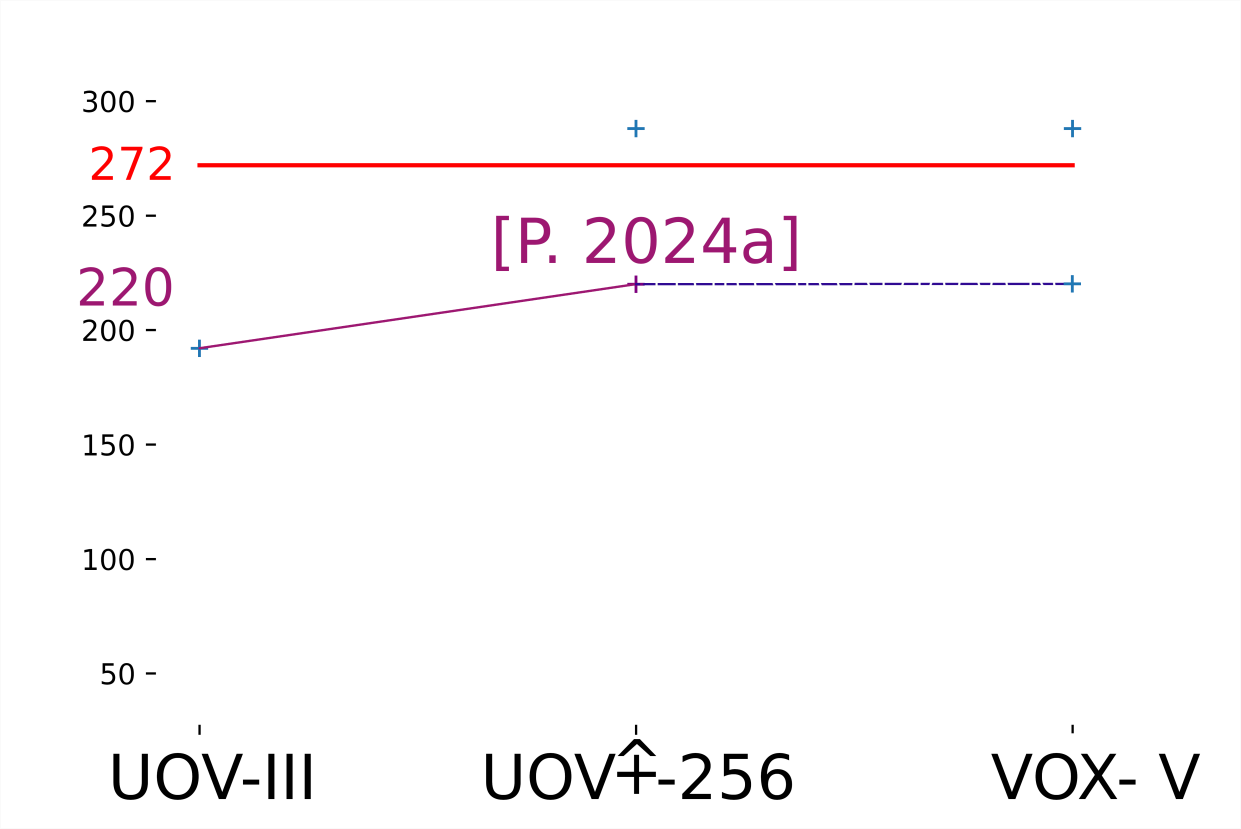
Échelle logarithmique du niveau de sécurité

Références

QR-UOV [Furue, Ikematsu, Kiyomura, Takagi, 2021]

VOX[Cogliati, Faugère, Fouque, Goubin, Larrieu, Macario-Rat, Minaud, Patarin, '23]

Cryptanalyse d'un schéma de signature multivarié: VOX

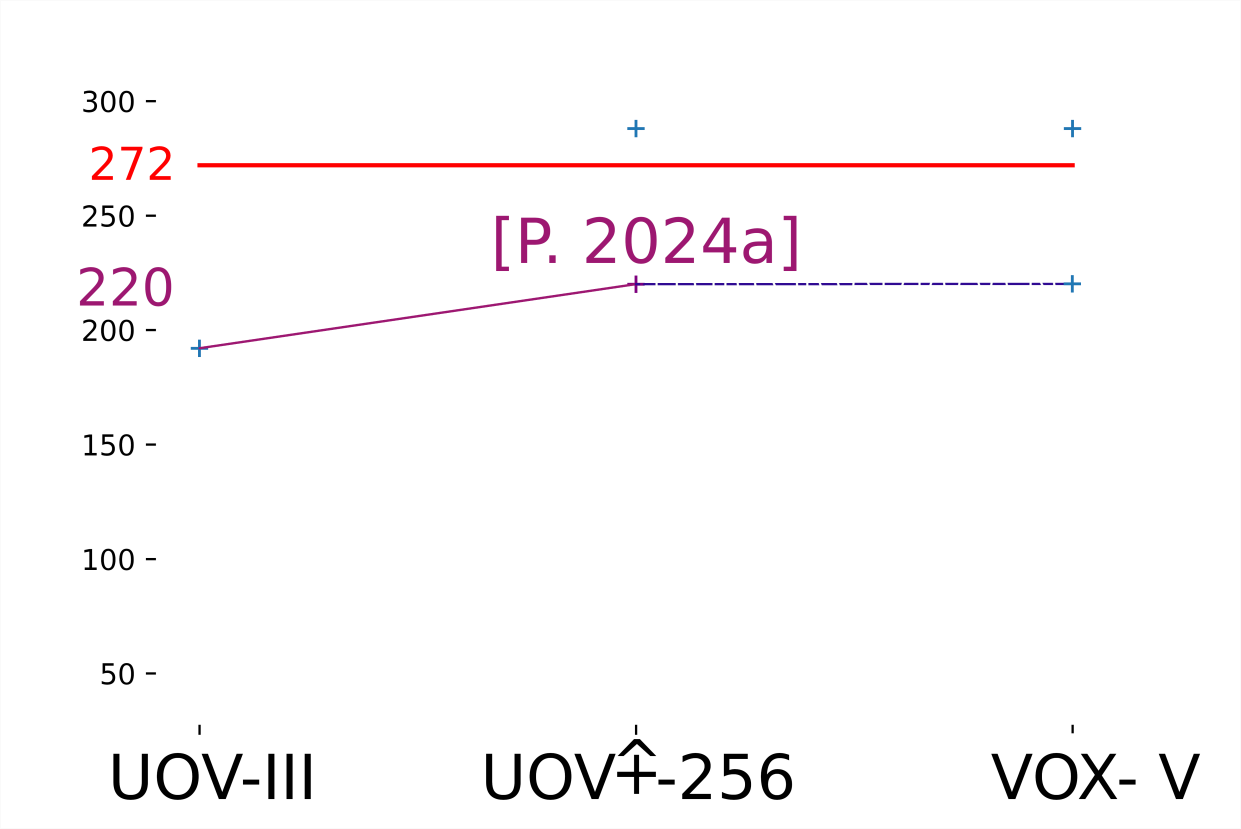


Échelle logarithmique du niveau de sécurité

Références

Singular points of UOV and VOX **[P. 2024]**

Cryptanalyse d'un schéma de signature multivarié: VOX



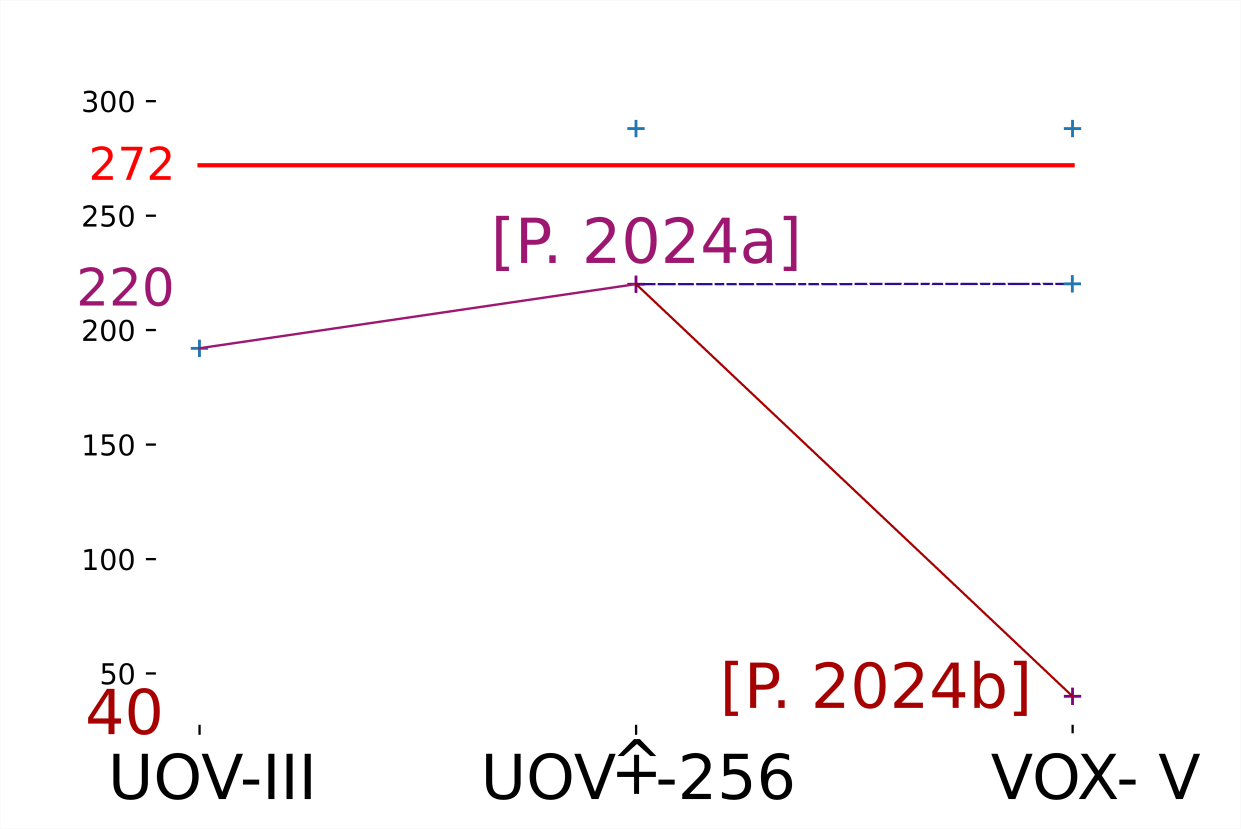
Échelle logarithmique du niveau de sécurité

Références

Singular points of UOV and VOX **[P. 2024]**

2^{50} fois plus facile qu'annoncé.

Cryptanalyse d'un schéma de signature multivarié: VOX

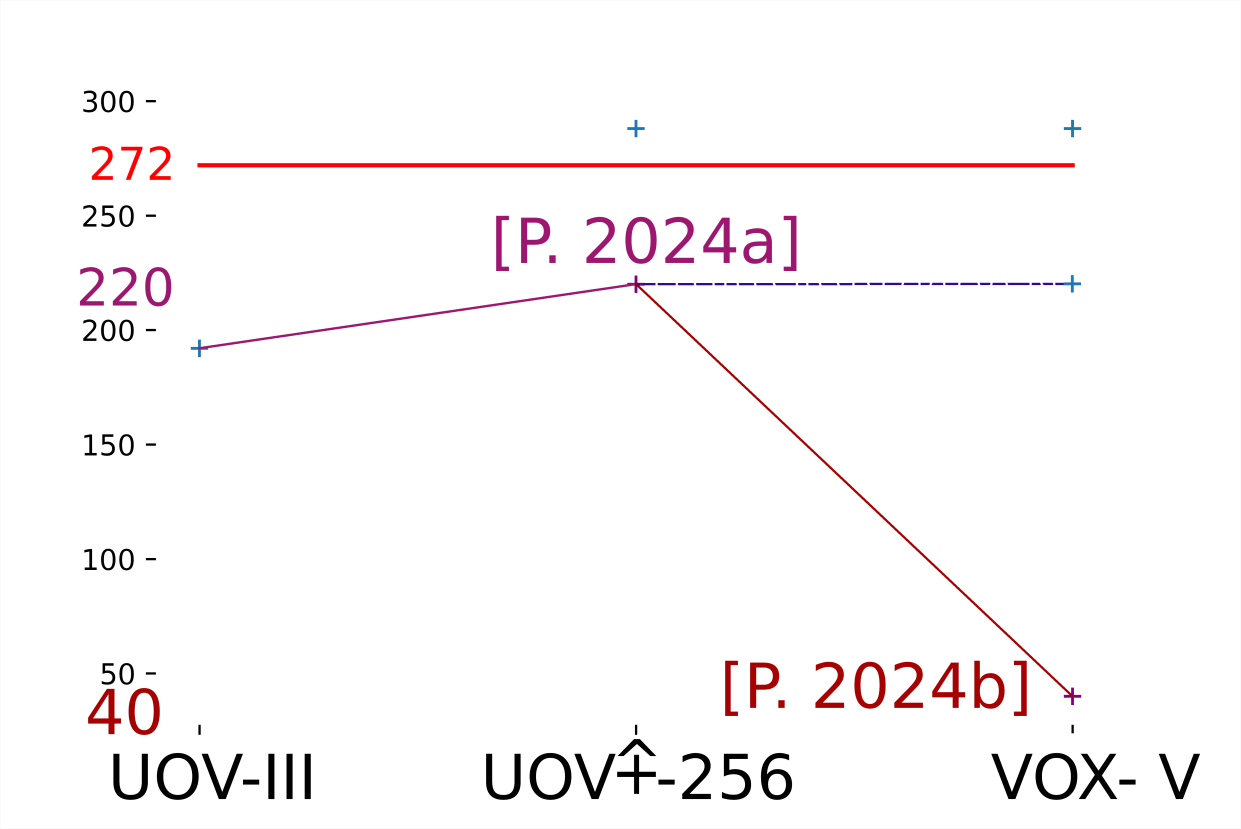


Échelle logarithmique du niveau de sécurité

Références

Subfield attack[...][P. 2024]

Cryptanalyse d'un schéma de signature multivarié: VOX



Échelle logarithmique du niveau de sécurité

Références

Subfield attack[...]**[P. 2024]**

2^{230} fois plus facile qu'annoncé: 0.5s sur mon laptop