Chiffrement à clé symétrique distribuée sans confiance





POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

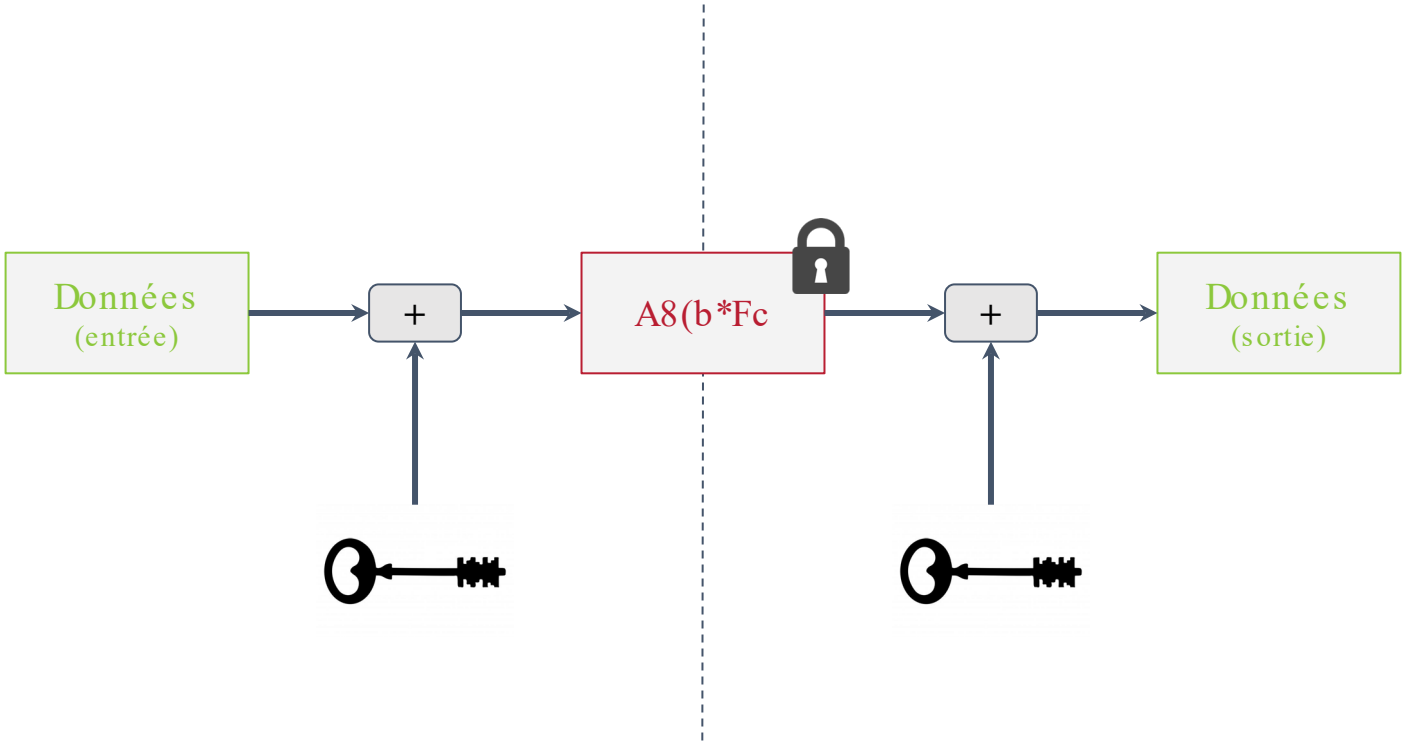
UQAC | Université du Québec à Chicoutimi

Florian Le Mouël
7 Mai 2025

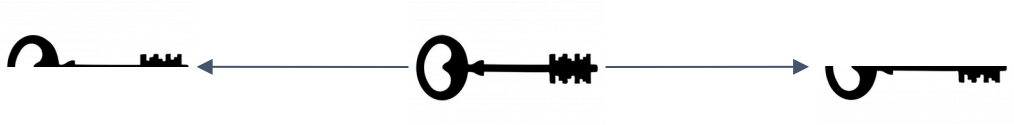
SOMMAIRE

1. **Notions de cryptographie**
2. Propriétés de notre protocole
3. Applications
4. Introduction au partage de secret

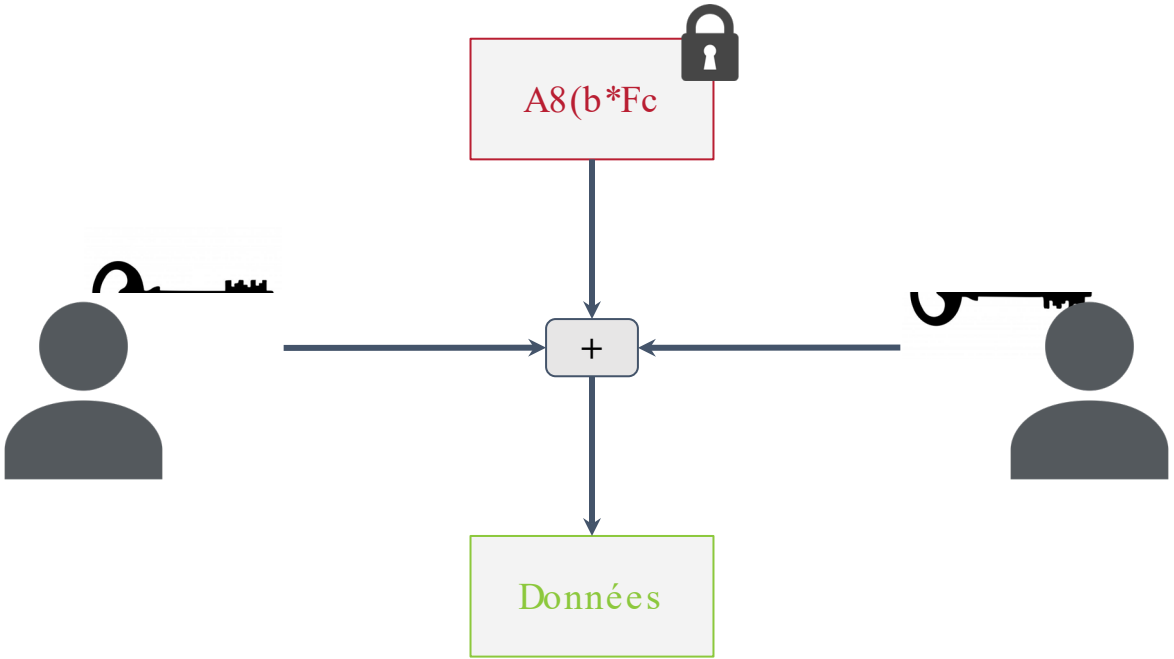
CHIFFREMENTÀ CLÉ SYMÉTRIQUE



CLÉ DISTRIBUÉE



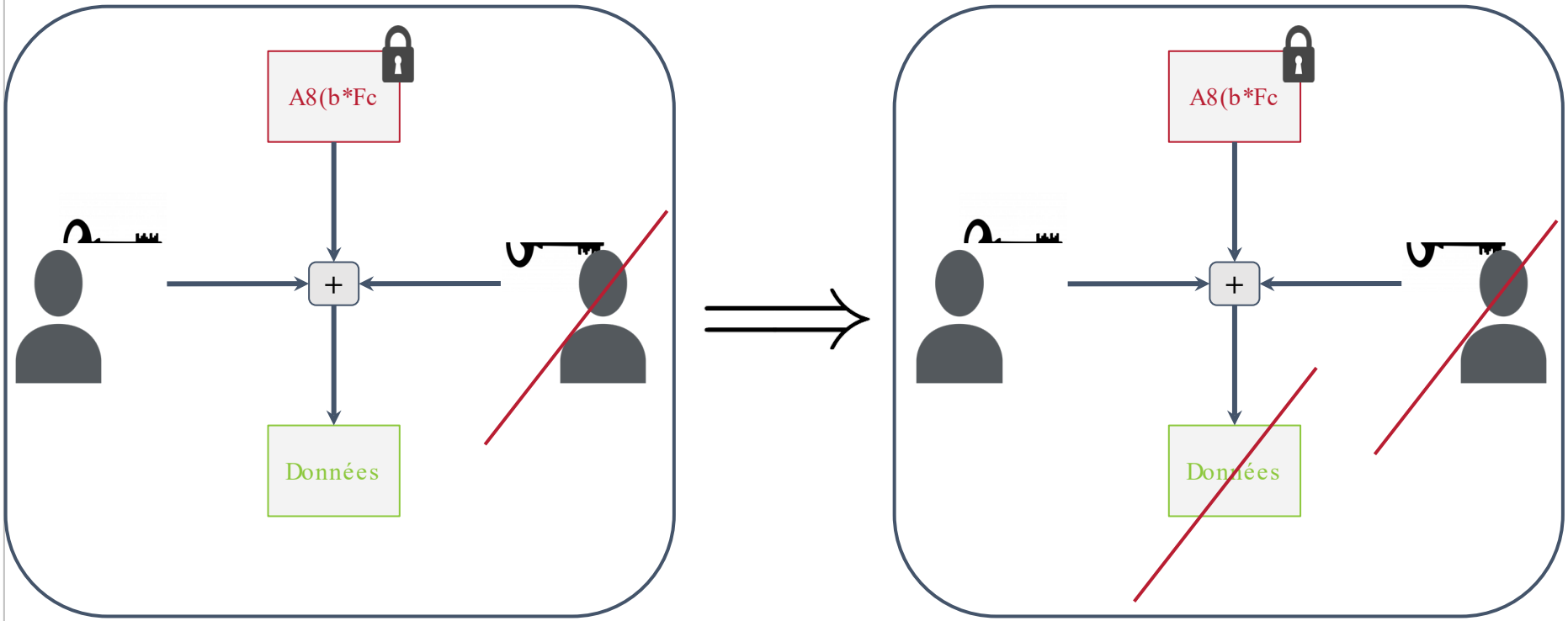
DÉCHIFFREMENTDISTRIBUÉ



SOMMAIRE

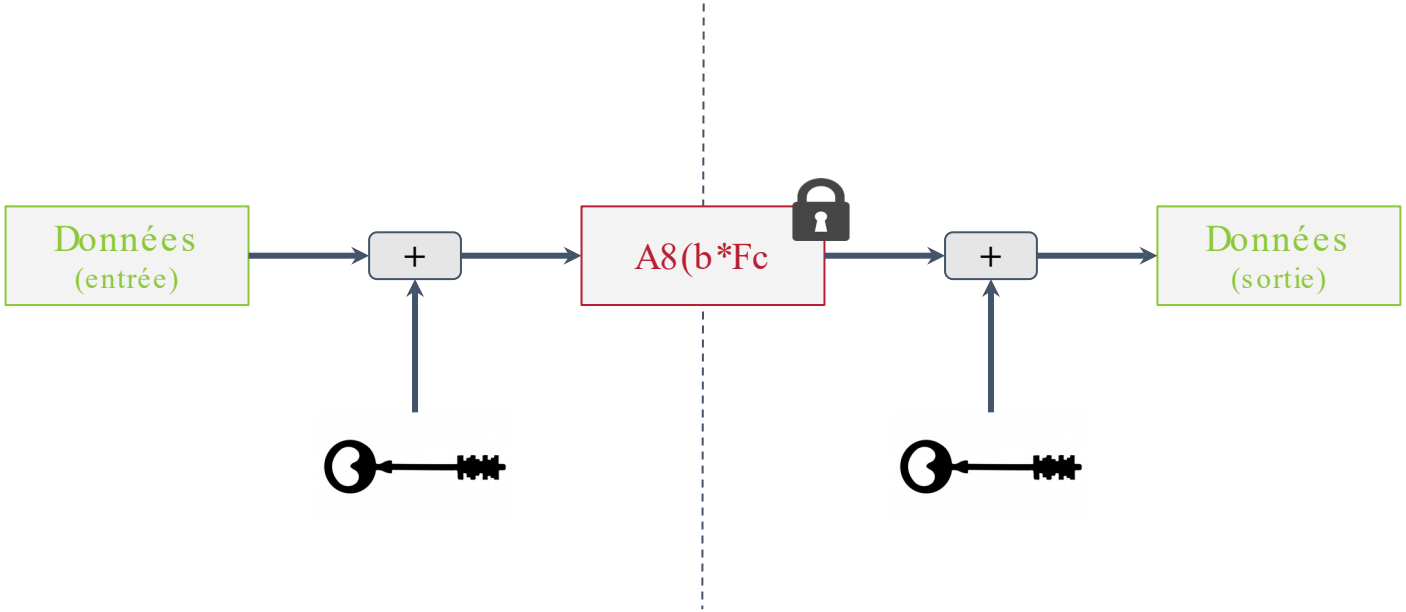
PROPRIÉTÉS DE SÉCURITÉ

CONFIDENTIALITÉ - AUTHENTICITÉ - CORRECTION - PAS DE TIER DE CONFIANCE



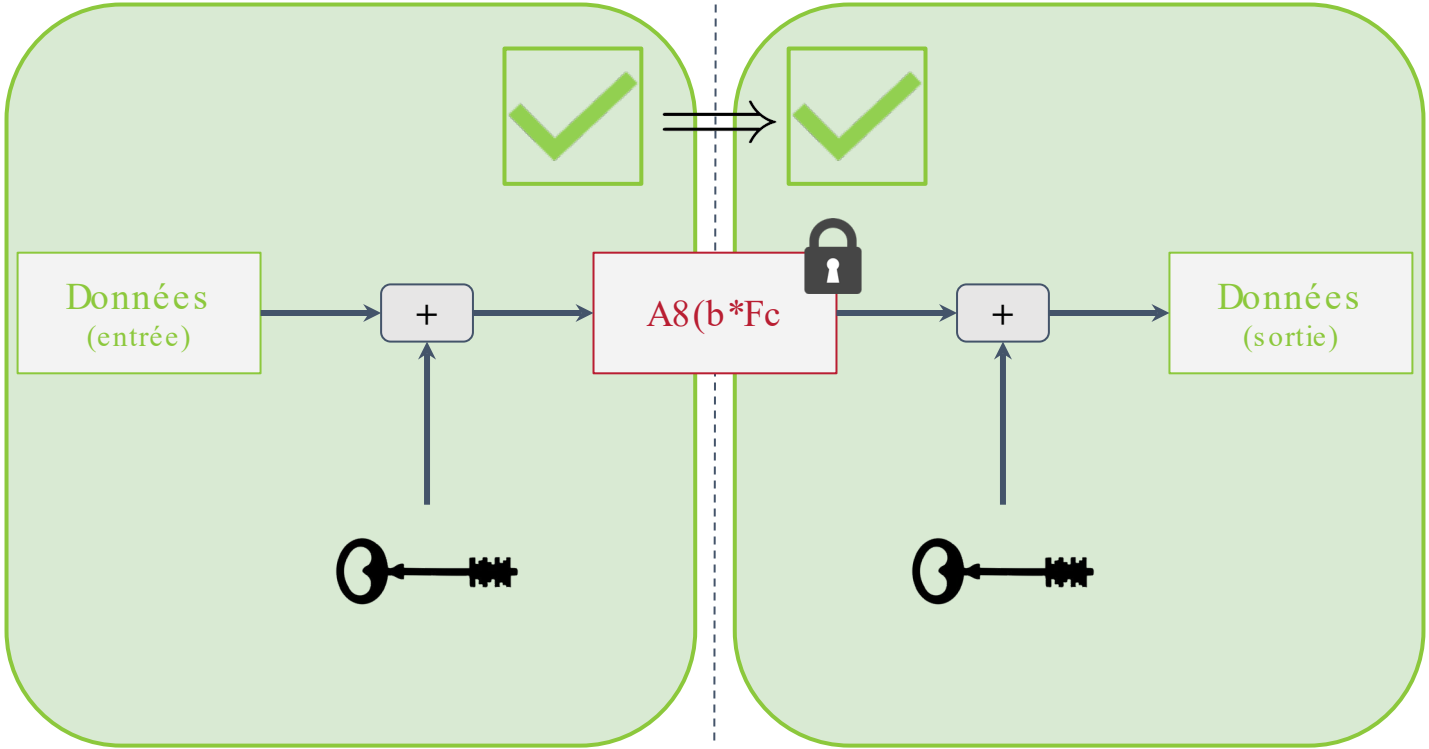
PROPRIÉTÉS DE SÉCURITÉ

CONFIDENTIALITÉ - AUTHENTICITÉ - CORRECTION - PAS DE TIER DE CONFIANCE



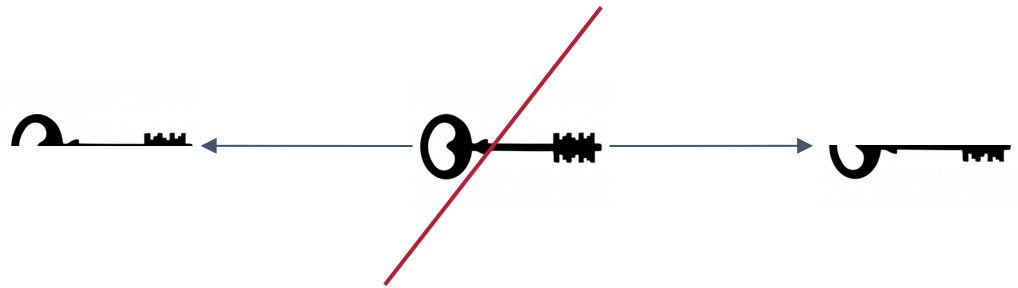
PROPRIÉTÉS DE SÉCURITÉ

CONFIDENTIALITÉ - AUTHENTICITÉ - CORRECTION - PAS DE TIER DE CONFIANCE



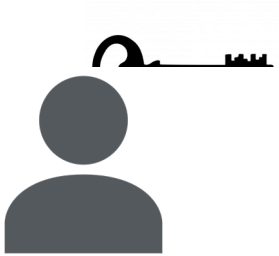
PROPRIÉTÉS DE SÉCURITÉ

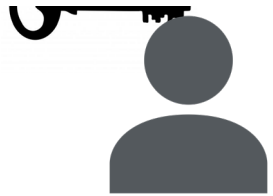
CONFIDENTIALITÉ - AUTHENTICITÉ - CORRECTION - PAS DE TIER DE CONFIANCE



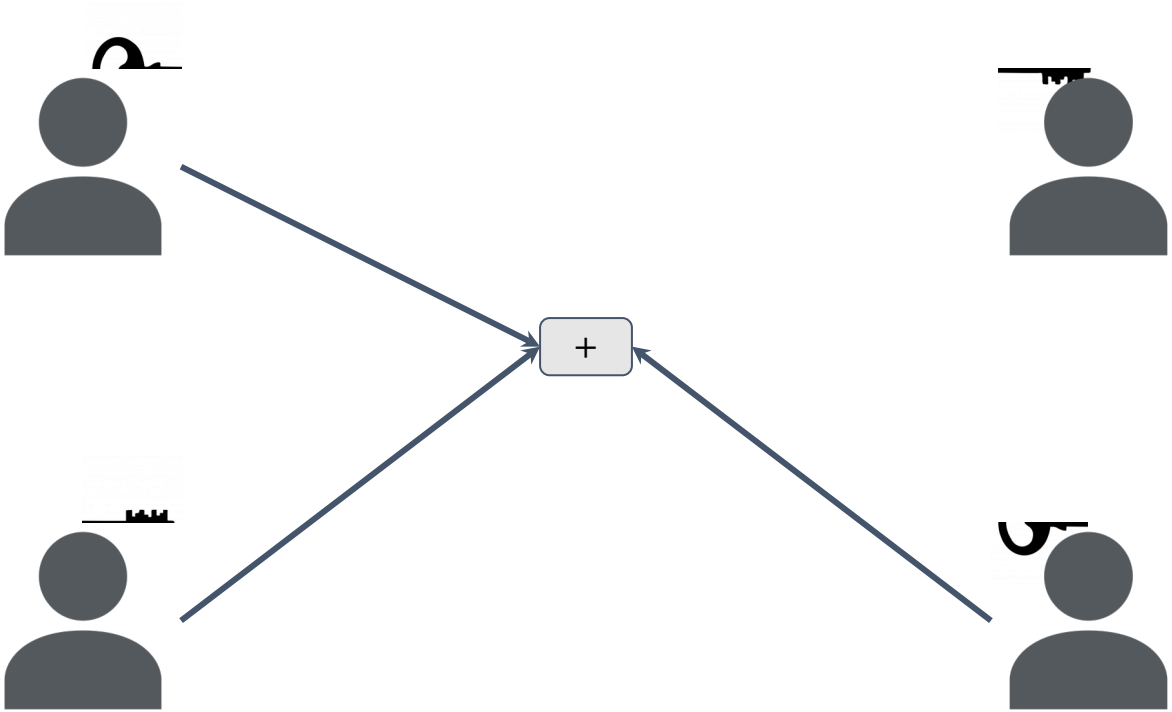
PROPRIÉTÉS DE SÉCURITÉ

CONFIDENTIALITÉ - AUTHENTICITÉ - CORRECTION - PAS DE TIER DE CONFIANCE

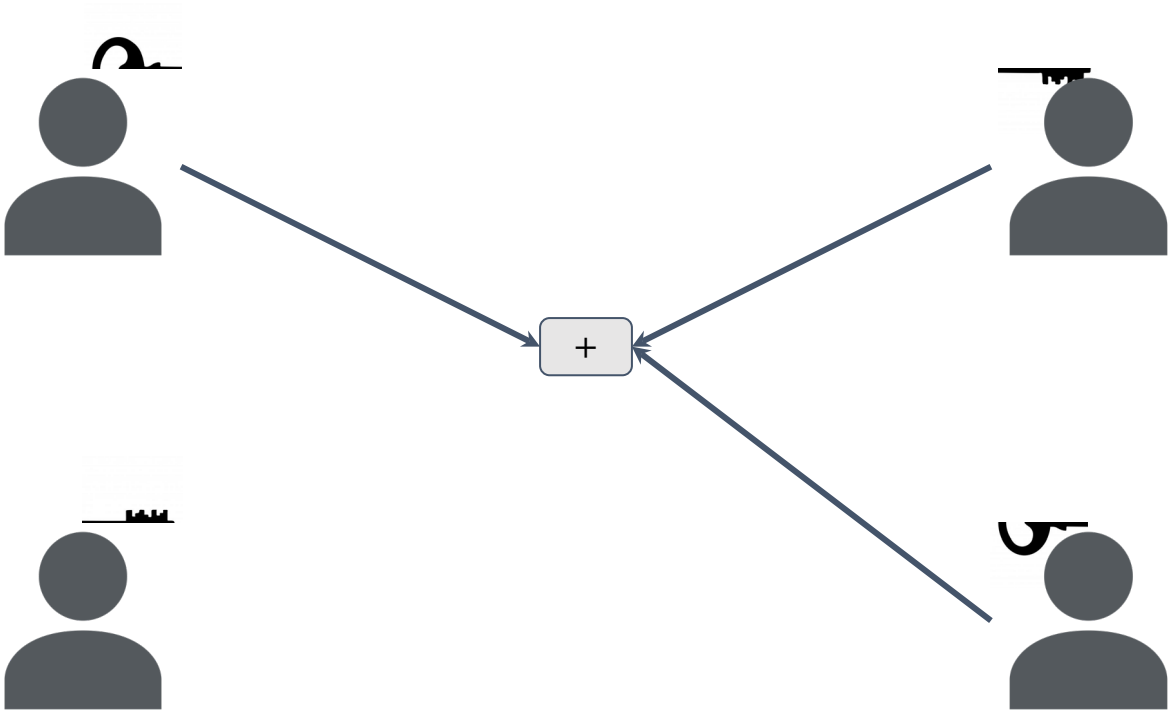




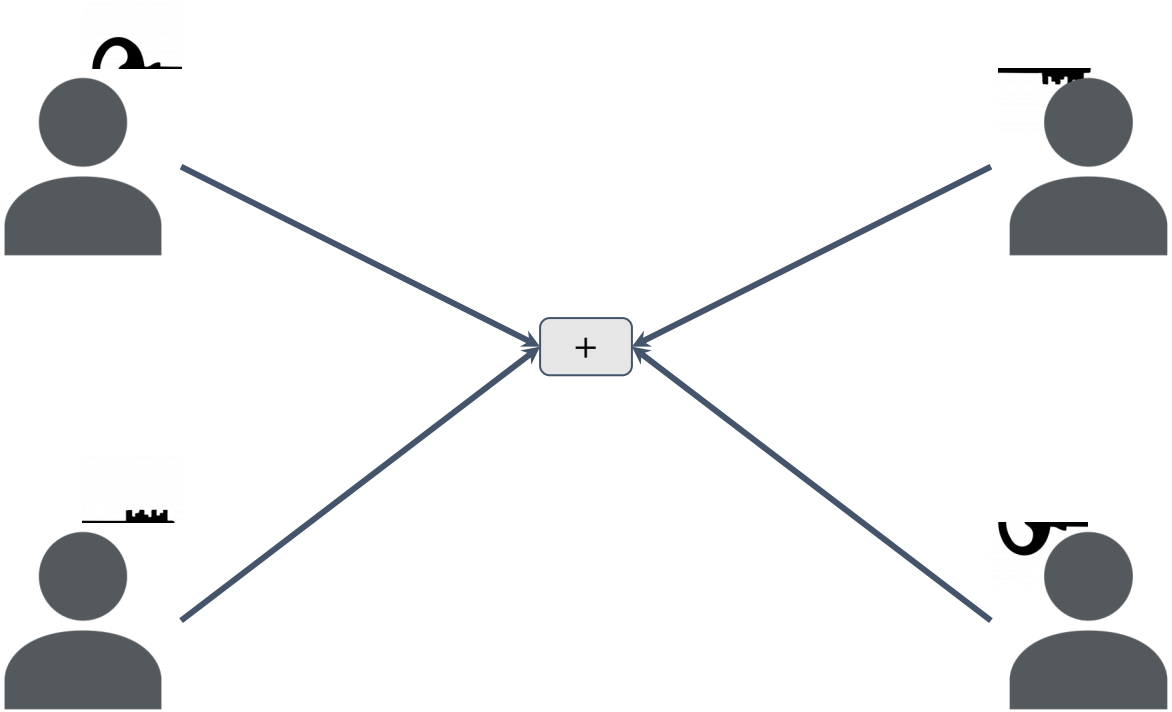
PROPRIÉTÉADDITIONNELLE CLÉ DISTRIBUÉEÀ SEUIL



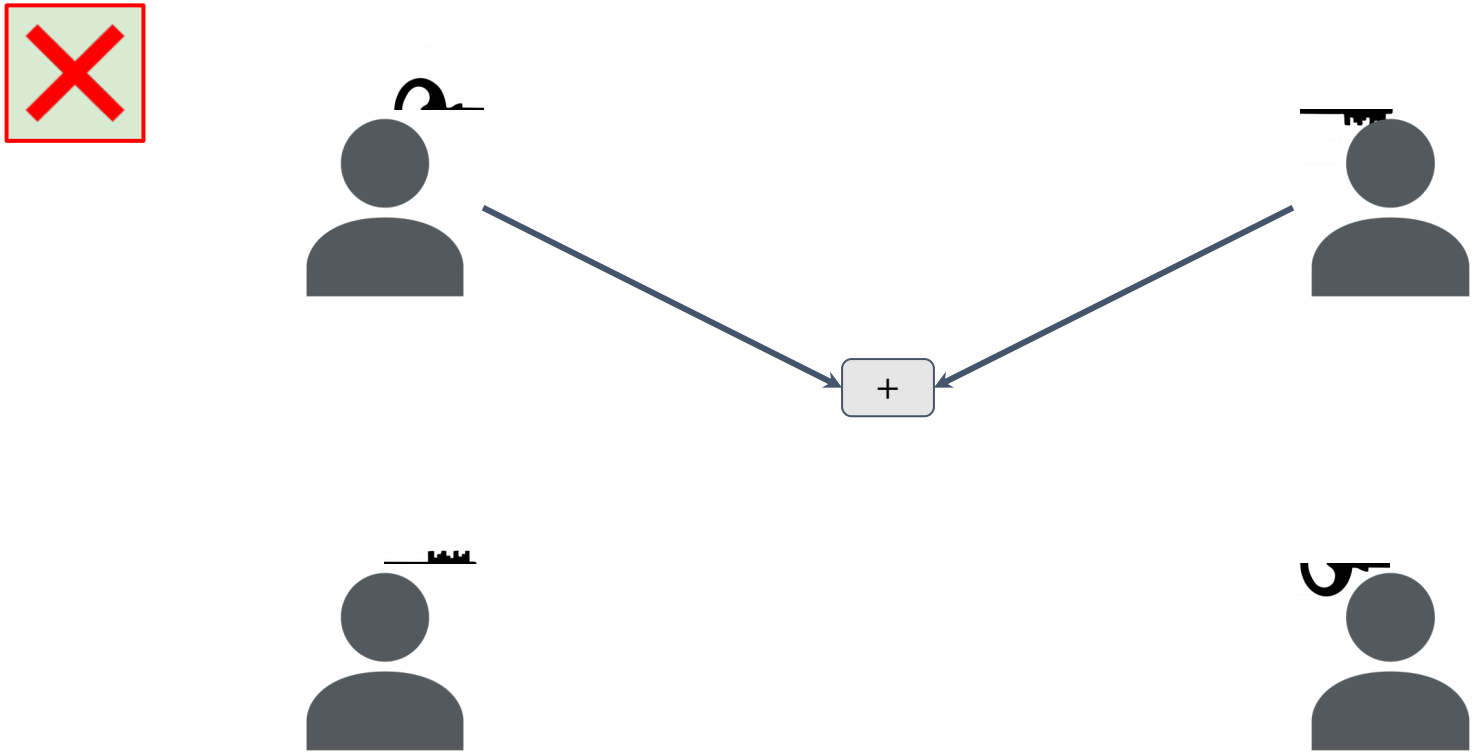
PROPRIÉTÉADDITIONELLE CLÉ DISTRIBUÉEÀ SEUIL



PROPRIÉTÉADDITIONELLE CLÉ DISTRIBUÉEÀ SEUIL

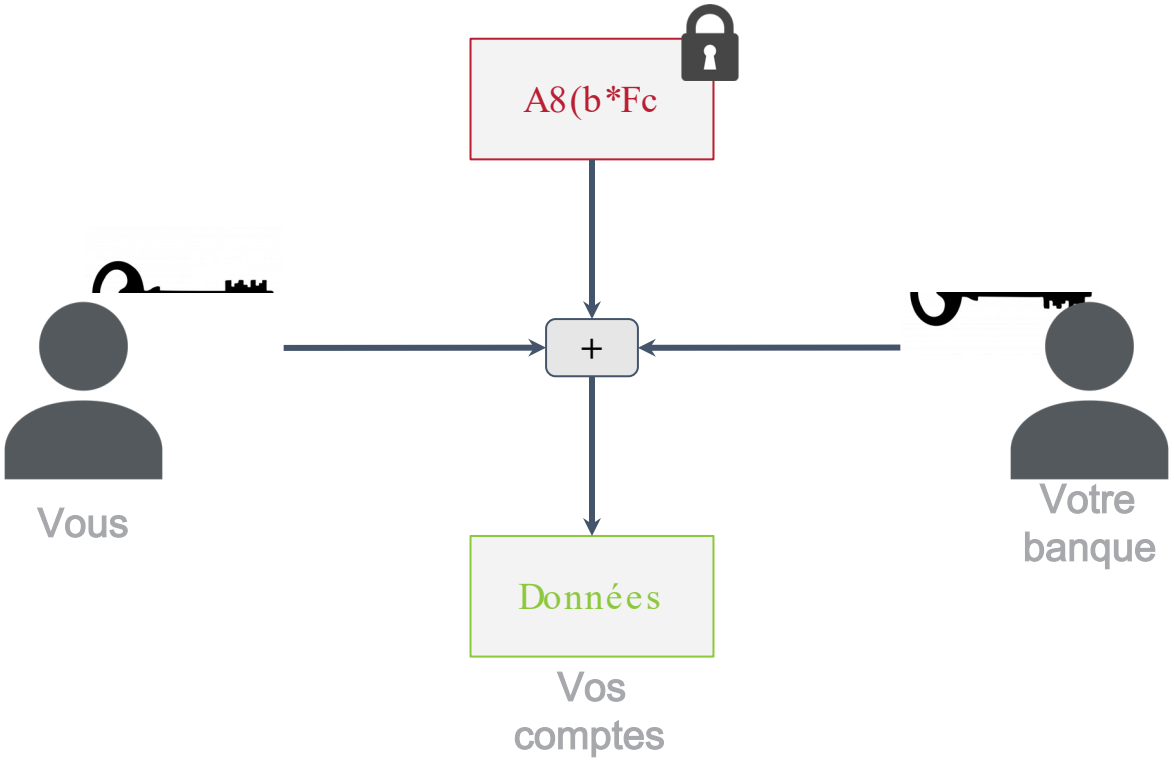


PROPRIÉTÉADDITIONELLE CLÉ DISTRIBUÉEÀ SEUIL

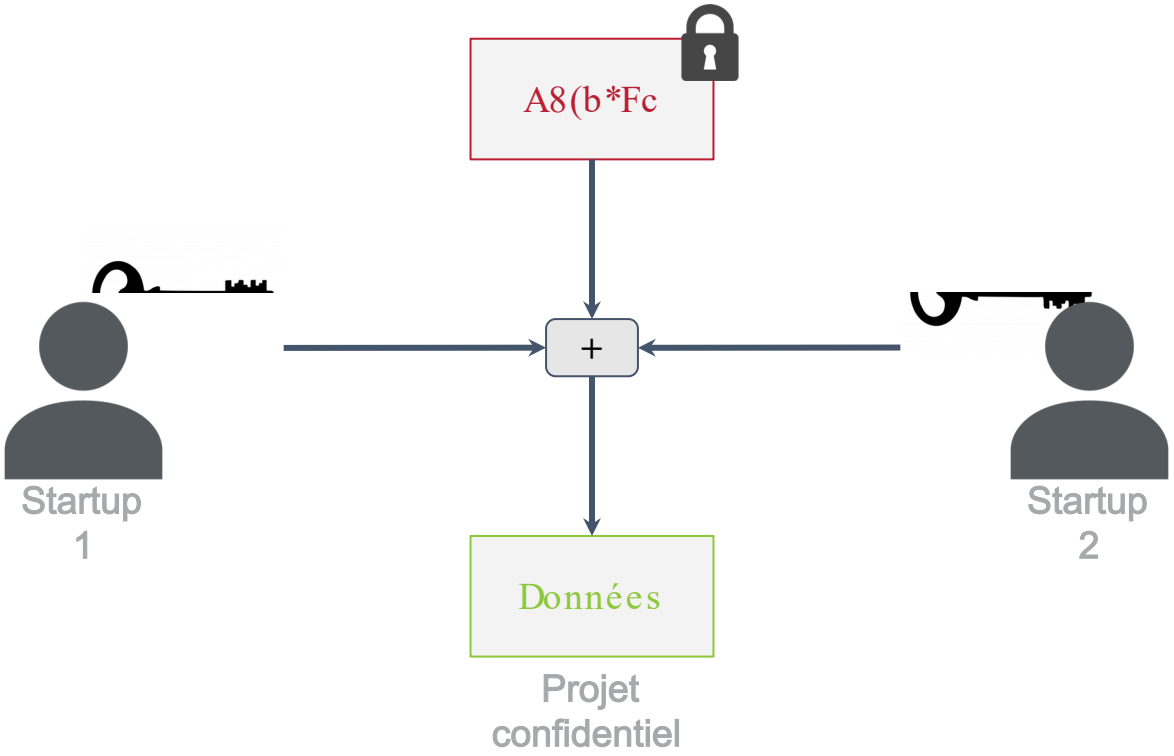


SOMMAIRE

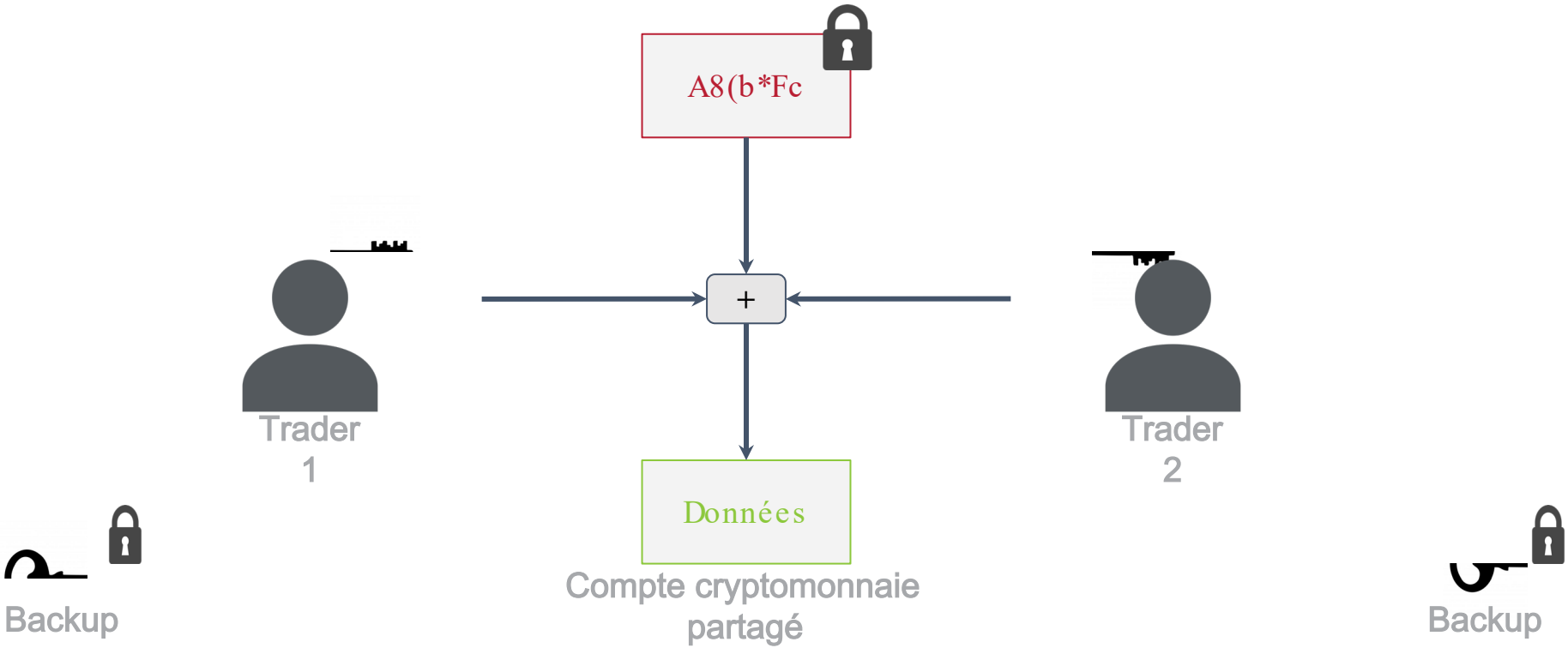
APPLICATION 1



APPLICATION 2

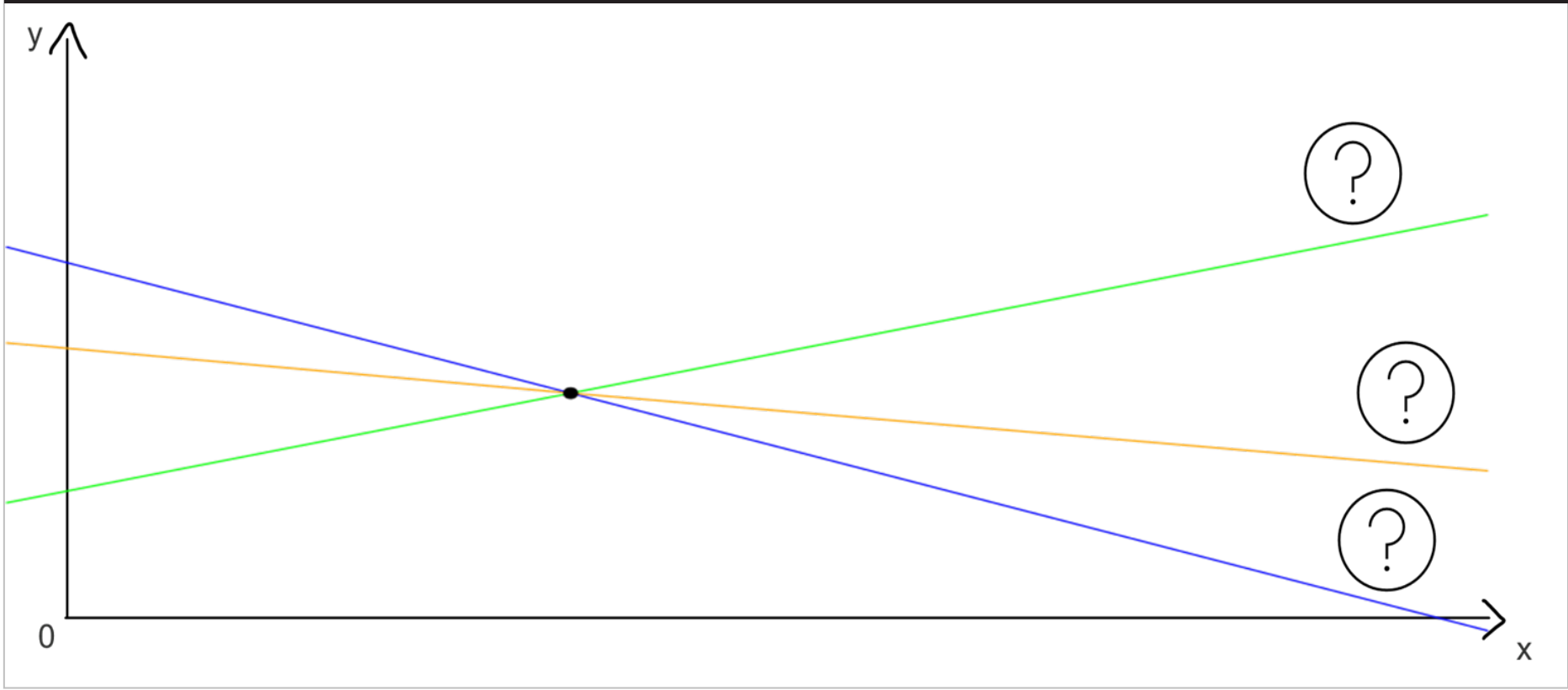


APPLICATION 3

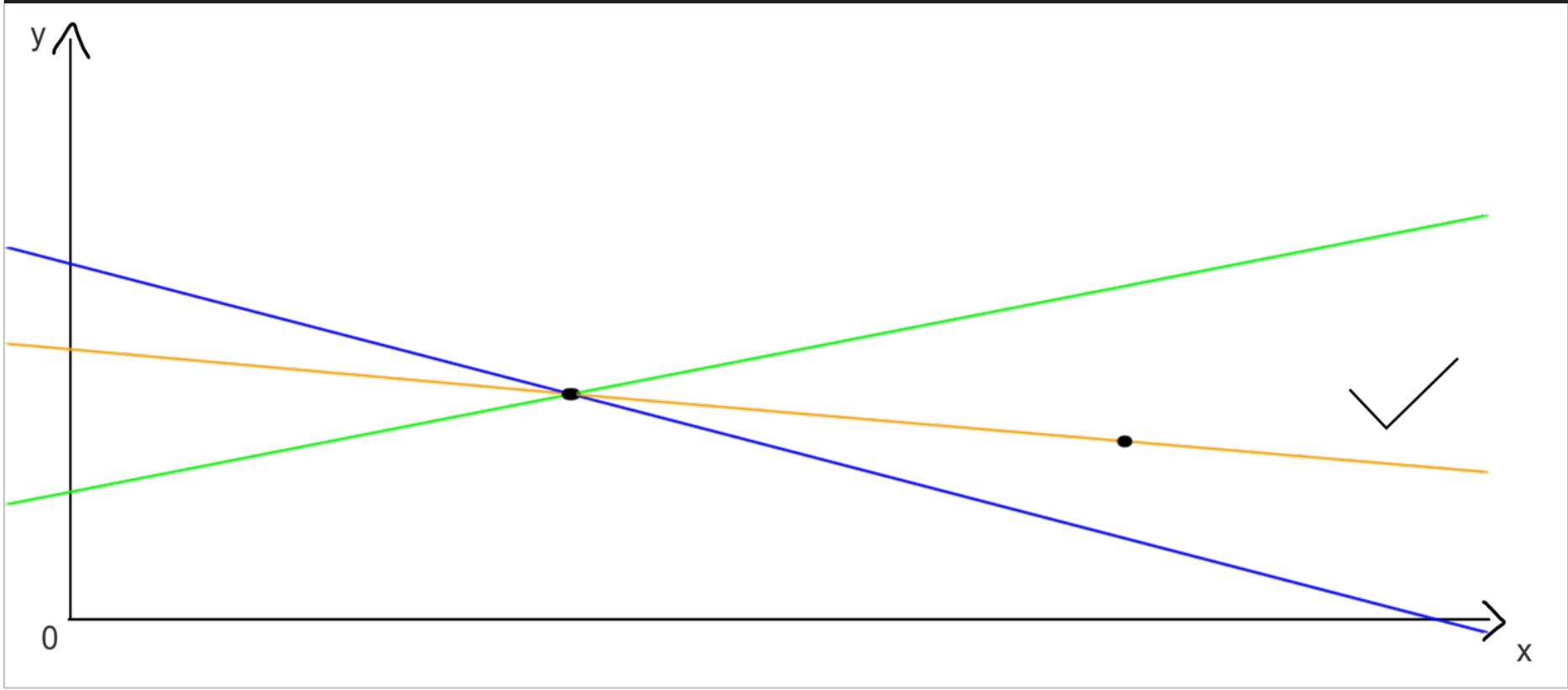


SOMMAIRE

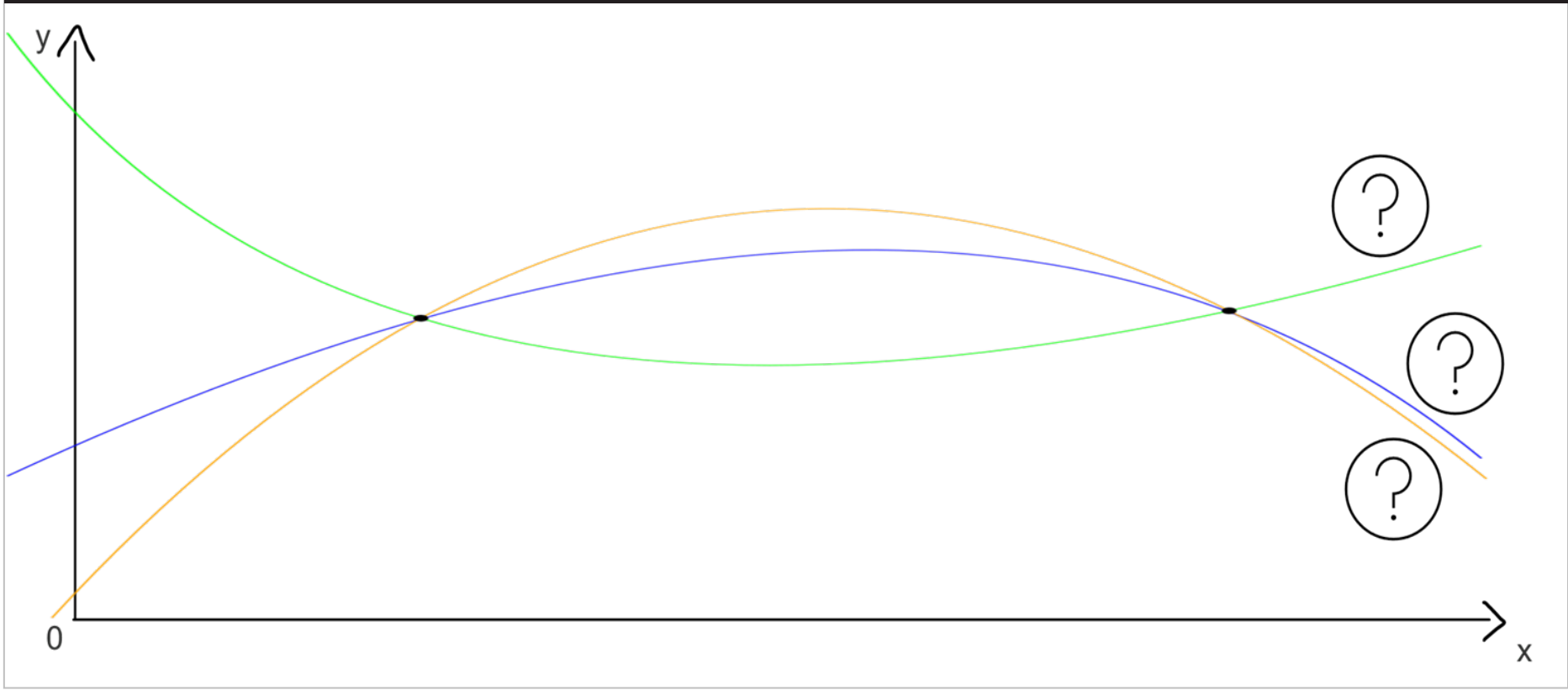
INTRODUCTION AU PARTAGE DE SECRET



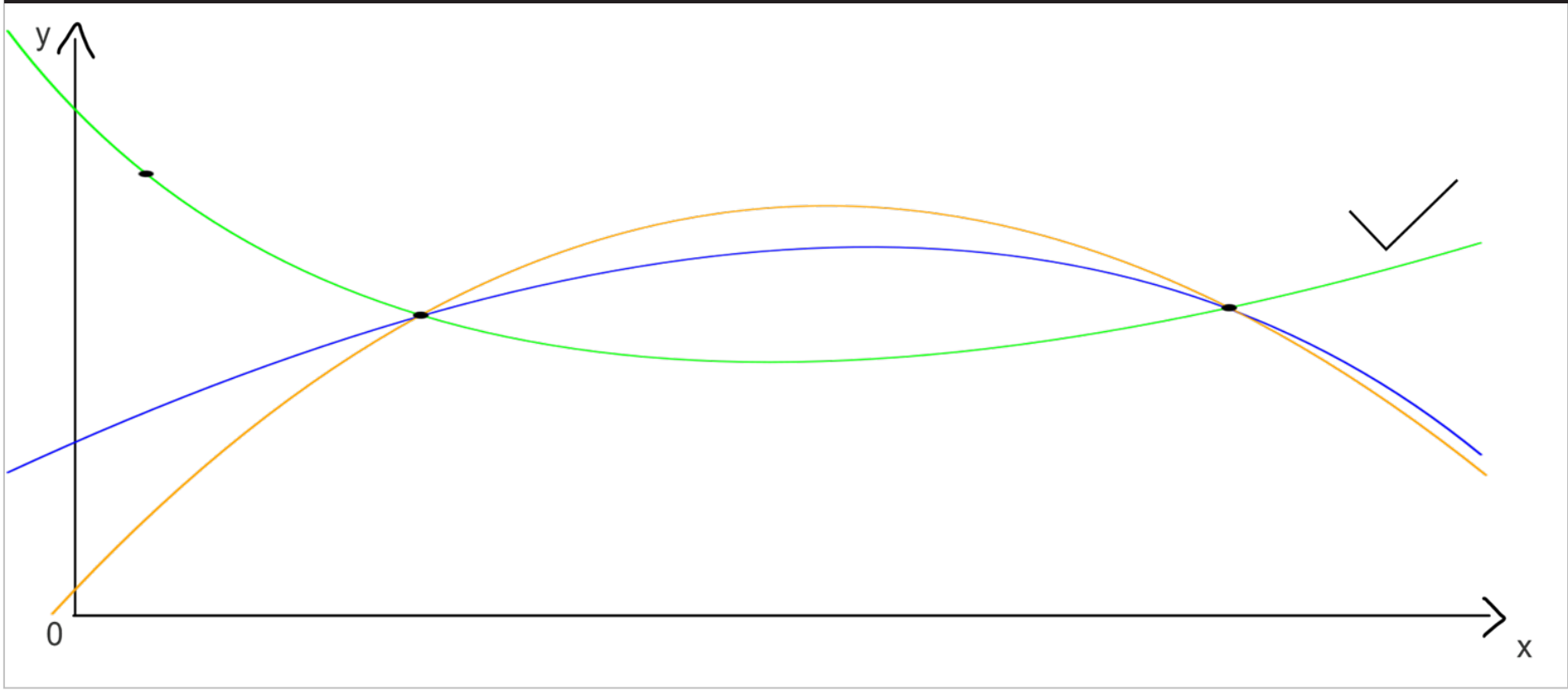
INTRODUCTION AU PARTAGE DE SECRET



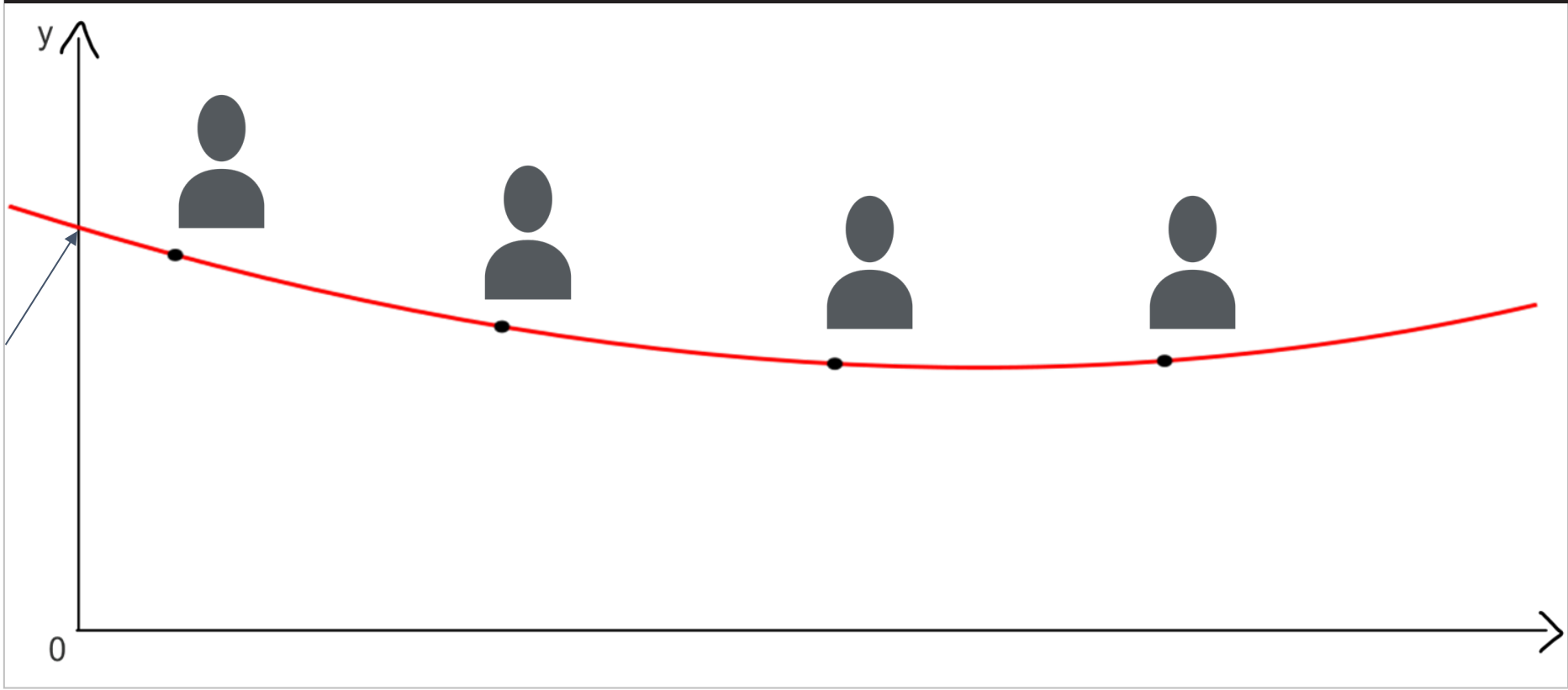
INTRODUCTION AU PARTAGE DE SECRET



INTRODUCTION AU PARTAGE DE SECRET



INTRODUCTION AU PARTAGE DE SECRET



TRAVAUX FUTURS

- Chiffrement à clé distribuée post-quantique (sans tier de confiance)
- Chiffrement à clé distribuée dans le modèle standard (sans tier de confiance)
- Preuve formelle de notre chiffrement dans un modèle plus fort

RÉFÉRENCES

- F. L. Mouël, M. Godon, R. Brien, E. Beurier, N. Boulahia-Cuppens, and F. Cuppens, "Trustless distributed symmetric-key encryption," 2024. [Online]. Available: https://arxiv.org/abs/2408.16137

- A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

- S. Agrawal, P. Mohassel, P. Mukherjee, and P. Rindal, "Dise: distributed symmetric-key encryption," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 1993–2010.

- S. Agrawal, W. Dai, A. Luykx, P. Mukherjee, and P. Rindal, "Paradise: efficient threshold authenticated encryption in fully malicious model," in International Conference on Cryptology in India. Springer, 2022, pp. 26–51.

GÉNÉRATIONDISTRIBUÉEDE CLÉ