Calcul Sécurisé sur des Réseaux à Grande Échelle

Geoffroy Couteau

Parcours et Domaine de Recherche

ENS Paris

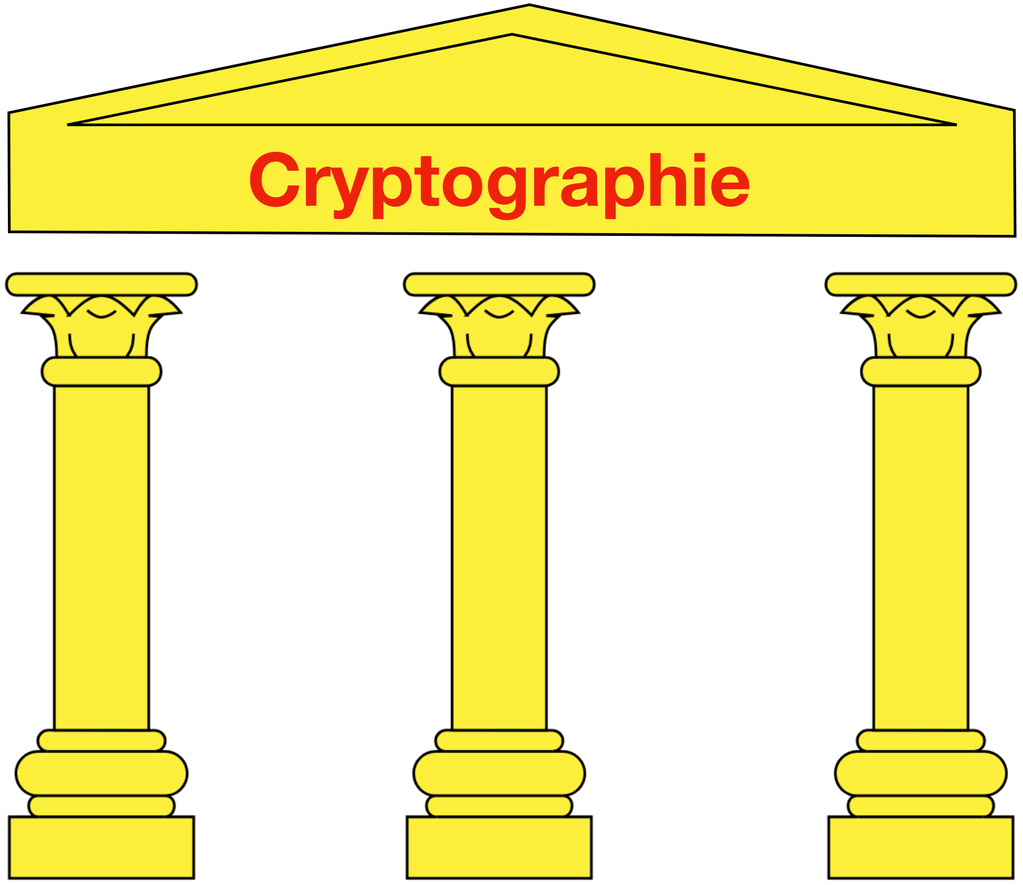
2014 - 2017

Karlsruhe Institute of Technology

2017 - 2019

CNRS
IRIF - UPCité

2019 - aujourd'hui



Calcul sécurisé

Cette présentation

Preuves à divulgation nulle de connaissance

Fondations théoriques de la cryptographie

Activités de Recherche et d’Encadrement

Publications

70 publications (**+2** depuis janvier), dont

- **47** : FOCS, Crypto, Eurocrypt, Asiacrypt, JoC, CCS, S&P
- **40** : avec les étudiant·e·s et post-doctorant·e·s que j'encadre

Projets

Porteur ou coordinateur :

- ERC Starting Grant **OBELiSC** (2024—2029)
- PEPR Cybersécurité **SecureCompute** (2022—2028)
- **(Nouveau)** Amazon Research Award **PCTC** (2026—)

Terminés :

- *ANR JCJC **SCENE** (2021—2024)*
- *DIM RFSI **LICENCED** (2022—2023)*

Dépôts comme porteur ou coordinateur :

- ERC Proof of Concept **PACT**
- CEFIPRA **NFPPC**
- ANR **VERITAS**

Projets

Porteur ou coordinateur :

- ERC Starting Grant **OBELiSC** (2024—2029)
- PEPR Cybersécurité **SecureCompute** (2022—2028)
- **(Nouveau)** Amazon Research Award **PCTC** (2026—)

Terminés :

- *ANR JCJC **SCENE** (2021—2024)*
- *DIM RFSI **LICENCED** (2022—2023)*

Dépôts comme porteur ou coordinateur :

- ERC Proof of Concept **PACT**
- CEFIPRA **NFPPC**
- ANR **VERITAS**

ERC OBELISC

But :

Permettre la construction d'un réseau à grande échelle où nos données restent *privées par défaut* même lorsqu'elles sont *utilisées dans des calculs*

Projets

Porteur ou coordinateur :

- ERC Starting Grant **OBELiSC** (2024—2029)
- PEPR Cybersécurité **SecureCompute** (2022—2028)
- **(Nouveau)** Amazon Research Award **PCTC** (2026—)

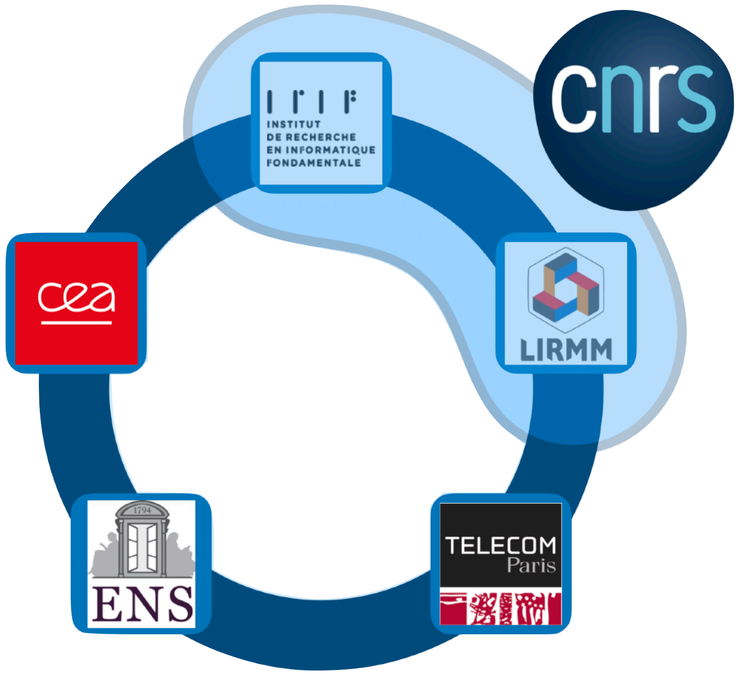
Terminés :

- *ANR JCJC **SCENE** (2021—2024)*
- *DIM RFSI **LICENCED** (2022—2023)*

Dépôts comme porteur ou coordinateur :

- ERC Proof of Concept **PACT**
- CEFIPRA **NFPPC**
- ANR **VERITAS**

PEPR SecureCompute



- Responsable partie CNRS
- Responsable d'un des axes

Projets

Porteur ou coordinateur :

- ERC Starting Grant **OBELiSC** (2024—2029)
- PEPR Cybersécurité **SecureCompute** (2022—2028)
- **(Nouveau)** Amazon Research Award **PCTC** (2026—)

Terminés :

- *ANR JCJC **SCENE** (2021—2024)*
- *DIM RFSI **LICENCED** (2022—2023)*

Dépôts comme porteur ou coordinateur :

- ERC Proof of Concept **PACT**
- CEFIPRA **NFPPC**
- ANR **VERITAS**

ARA PCTC

But : Implémentation (open source) et standardisation d'algorithmes pour la cryptographie à seuil

Projets

Porteur ou coordinateur :

- ERC Starting Grant **OBELiSC** (2024—2029)
- PEPR Cybersécurité **SecureCompute** (2022—2028)
- **(Nouveau)** Amazon Research Award **PCTC** (2026—)

Terminés :

- *ANR JCJC **SCENE** (2021—2024)*
- *DIM RFSI **LICENCED** (2022—2023)*

Dépôts comme porteur ou coordinateur :

- ERC Proof of Concept **PACT**
- CEFIPRA **NFPPC**
- ANR **VERITAS**

	Postdocs	Doctorant·es	Visiteur·se·s
FUTUR (Juin 2026)			
PRÉSENT			
PASSÉ (2021—2025)			

	Postdocs	Doctorant·es	Visiteur·se·s
FUTUR (Juin 2026)			
PRÉSENT			
PASSÉ (2021—2025)			

	Postdocs	Doctorant·es	Visiteur·se·s
FUTUR (Juin 2026)			
PRÉSENT			
PASSÉ (2021—2025)	Sven  Alex  Balthazar 		

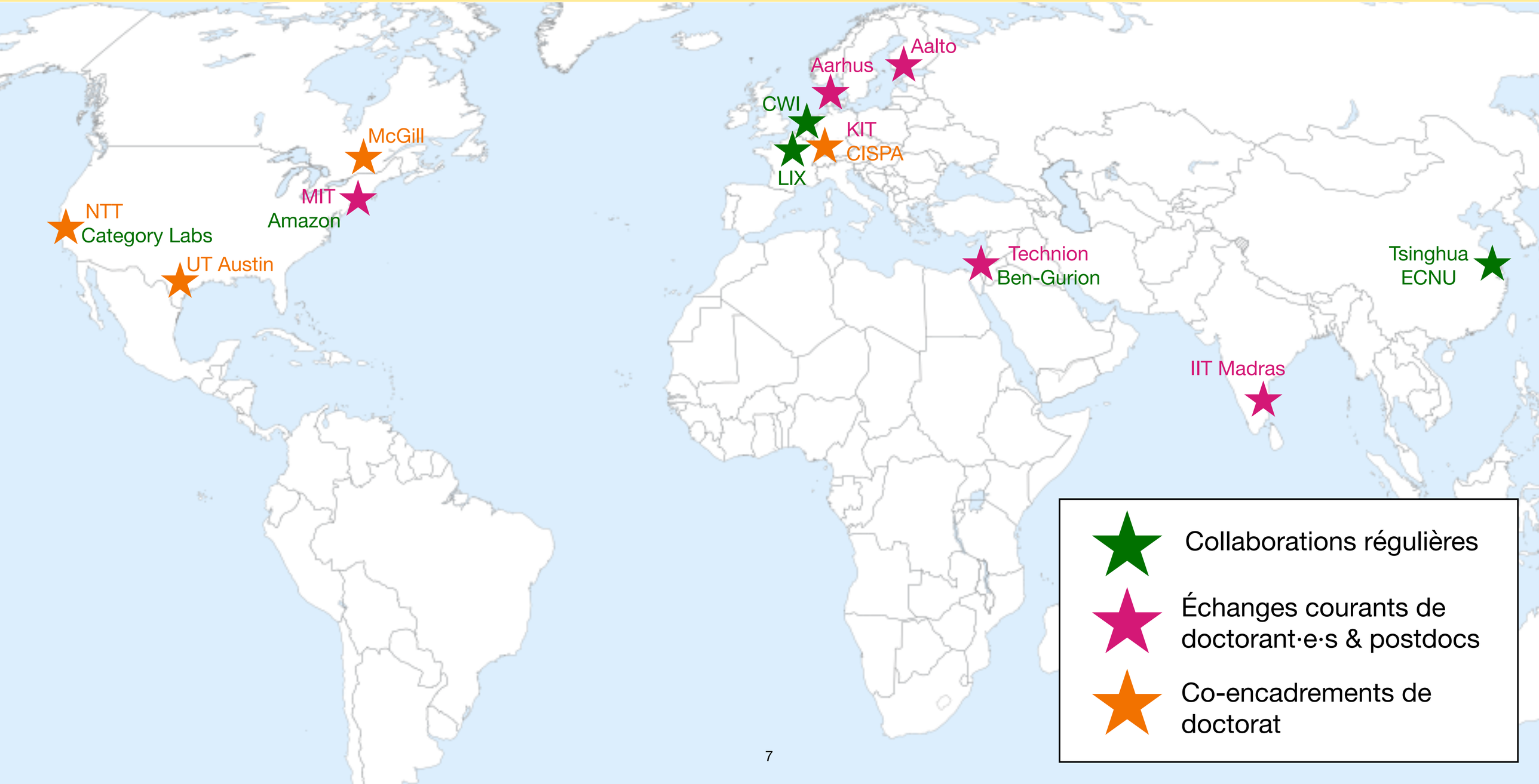
	Postdocs	Doctorant·es	Visiteur·se·s
FUTUR (Juin 2026)			
PRÉSENT			
PASSÉ (2021—2025)			

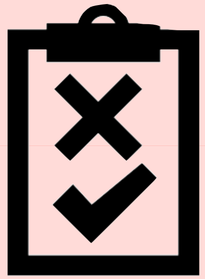
Postes permanents

	Postdocs	Doctorant·es	Visiteur·se·s
FUTUR (Juin 2026)			 Thejas 
PRÉSENT			
PASSÉ (2021—2025)	 Sven Alex Balthazar		 Xiaxi

Postes permanents

Échanges et collaborations





Dissémination, enseignement

- Livre : *An Introduction to Silent Secure Computation* (Springer, 2026)
- ~80 h/an d'enseignements (MPRI, ENS Lyon, Télécom, UPCité…)
- Création et animation d’un groupe de travail national (contact tracing)
- Séminaire au Collège de France (cours de Xavier Leroy, décembre 2025)

Prises de Responsabilités

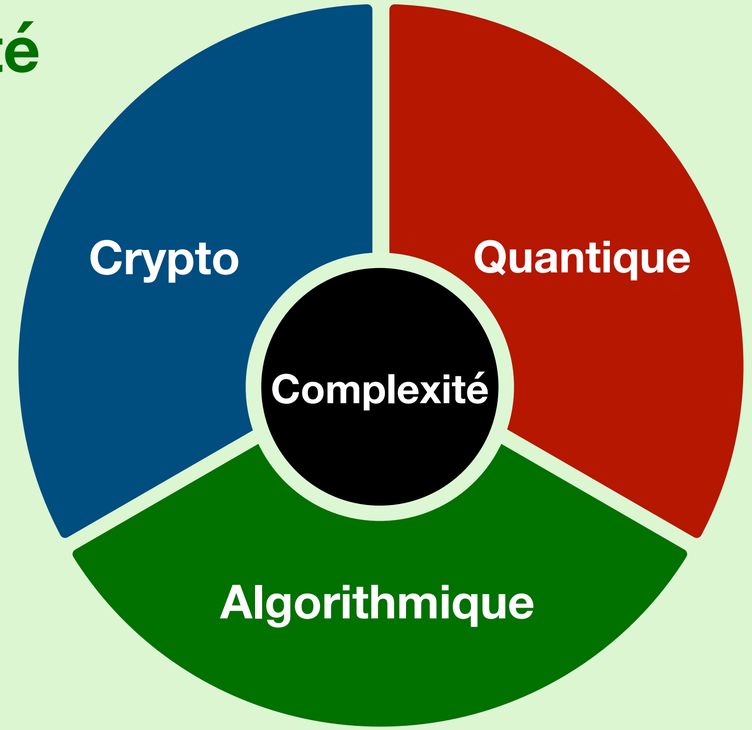
Équipe Algorithmes et Complexité

Responsable d'équipe (Janvier 26)

39 membres : 14 permanents, 25 non-permanents

Axe crypto :

- Premier permanent à temps plein
- 13 membres, 3 permanents, 10 non-permanents
- Attractif : candidatures MCF/CR, +1 CR et +1 Professeure



Dans le laboratoire

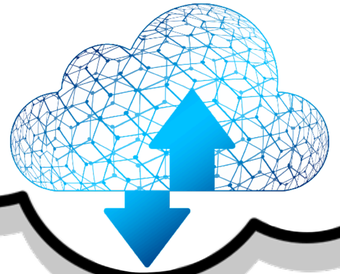
- Responsable commission IRIF & Environnement (2022—)
- Conseil de laboratoire (2022—)
- Conseil scientifique de l'UFR (2020—2025)
- Commission mentorat (2025—)

Calcul Sécurisé Efficace à Grande Échelle

Notre usage des réseaux a évolué : dès que l'on…

… utilise un appli de rencontre,

… cherche dans notre Cloud,



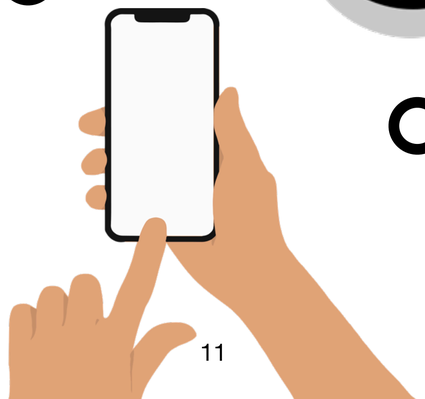
… voit une publicité ciblé,

… va sur un réseau social,

… reçoit une recommandation d'une plate-forme de streaming,

… utilise une appli de santé,

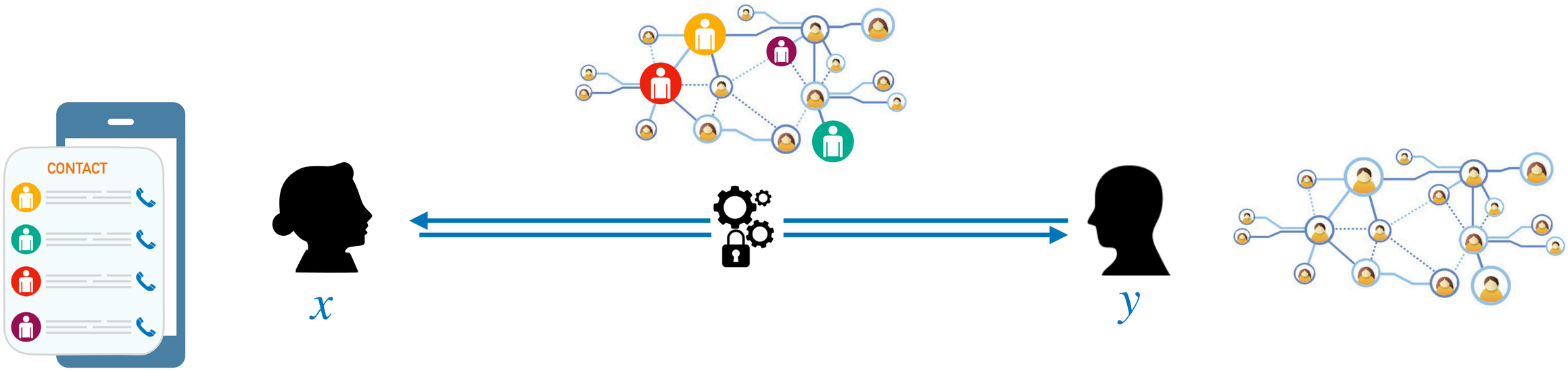
…



nos données privées sont **utilisées dans des calculs**

Calcul Sécurisé

- **Objectif.** *Calculer* une fonction **publique** sur des entrées privées
- **Modèle.** n joueurs, chacun avec une entrée privée

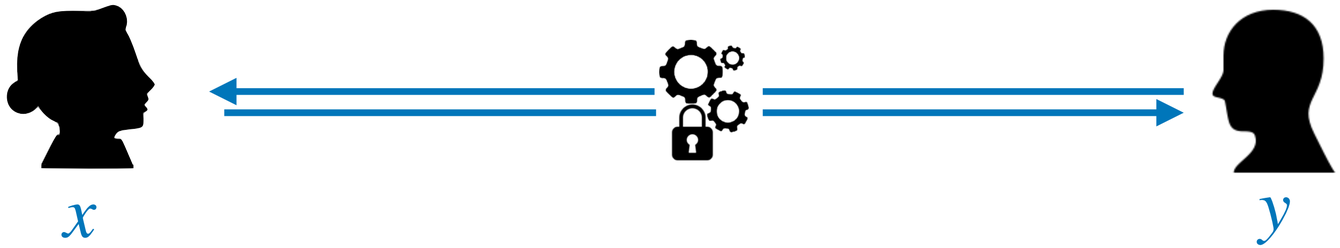


- **Résultat :** Alice apprend qui de ses contacts est déjà sur le réseau
- **Sécurité :** Alice et Bob n'apprennent rien de plus

Calcul Sécurisé

- **Objectif.** *Calculer* une fonction **publique** sur des entrées privées
- **Modèle.** n joueurs, chacun avec une entrée privée

$$f : (x, y) \mapsto (z_A, z_B)$$



- **Résultat :** Alice reçoit z_A et Bob reçoit z_B
- **Sécurité :** Alice et Bob n'apprennent rien de plus

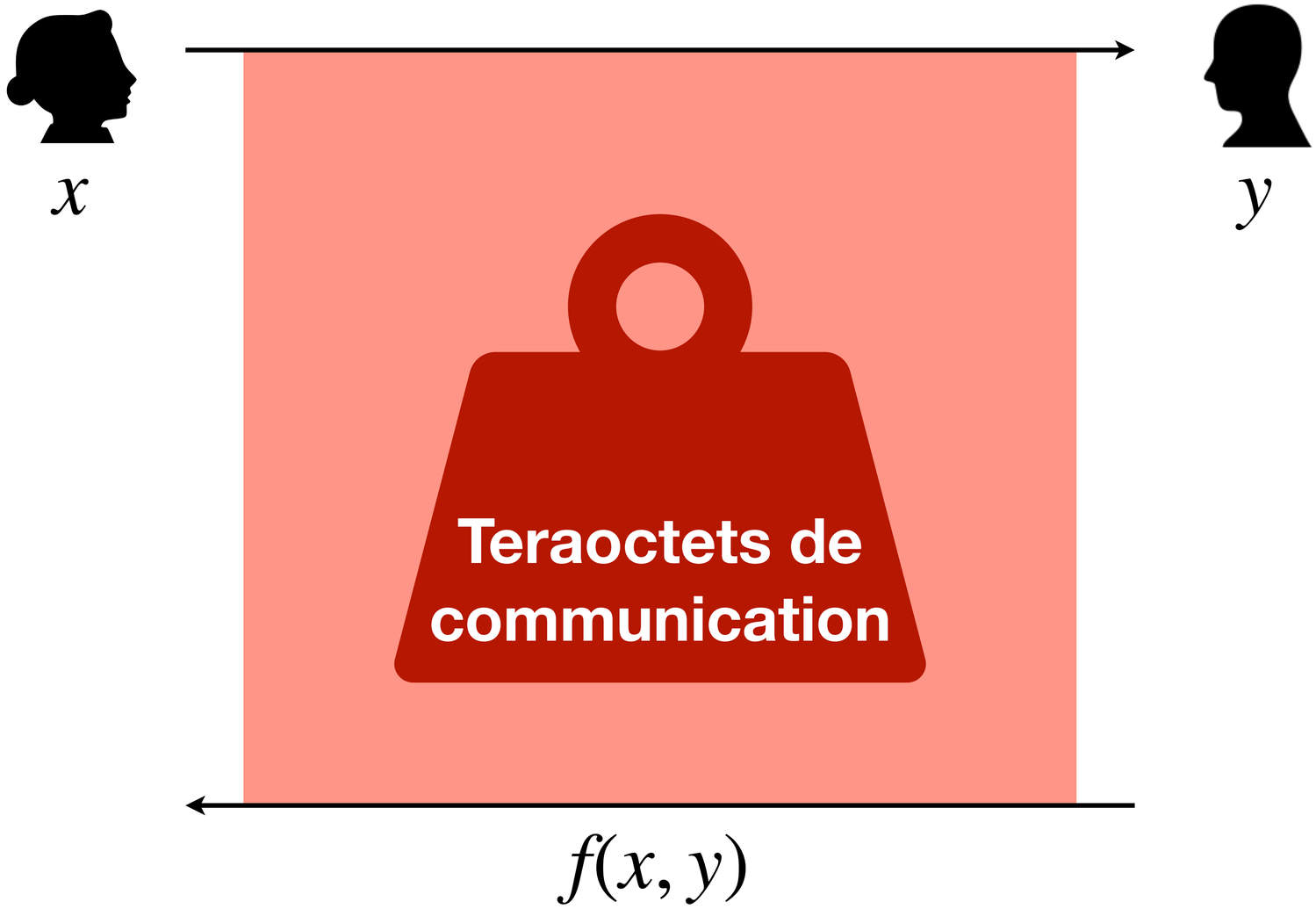
Un Nouveau Paradigme :
le Calcul Sécurisé Silencieux

Un Nouveau Paradigme pour le Calcul Sécurisé

Goldreich, Micali, Wigderson, 1987

Beaver, 1995

Boyle, **Couteau**, Gilboa, Ishai 2018



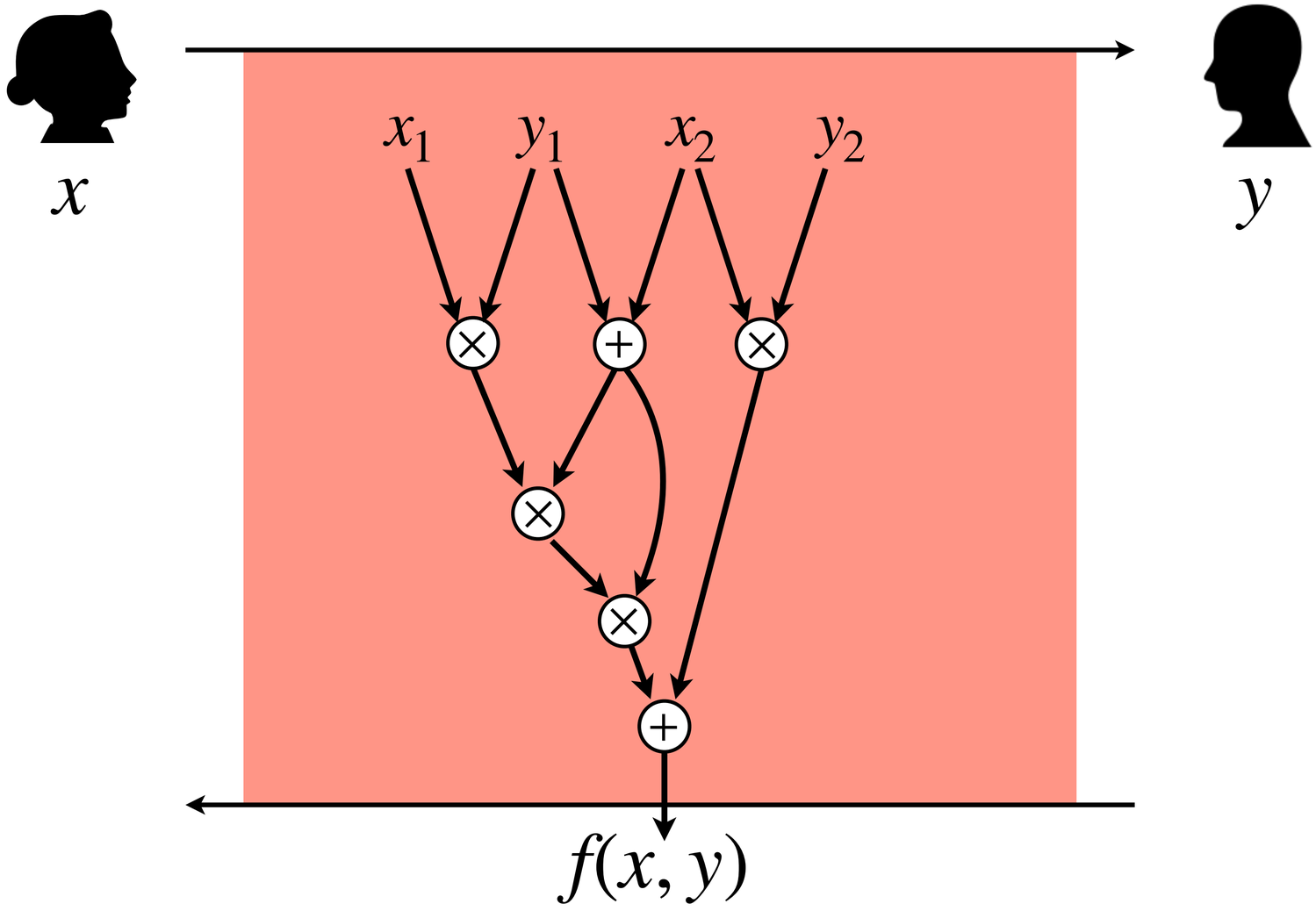
Exclusivement d'intérêt théorique

Un Nouveau Paradigme pour le Calcul Sécurisé

Goldreich, Micali, Wigderson, 1987

Beaver, 1995

Boyle, **Couteau**, Gilboa, Ishai 2018



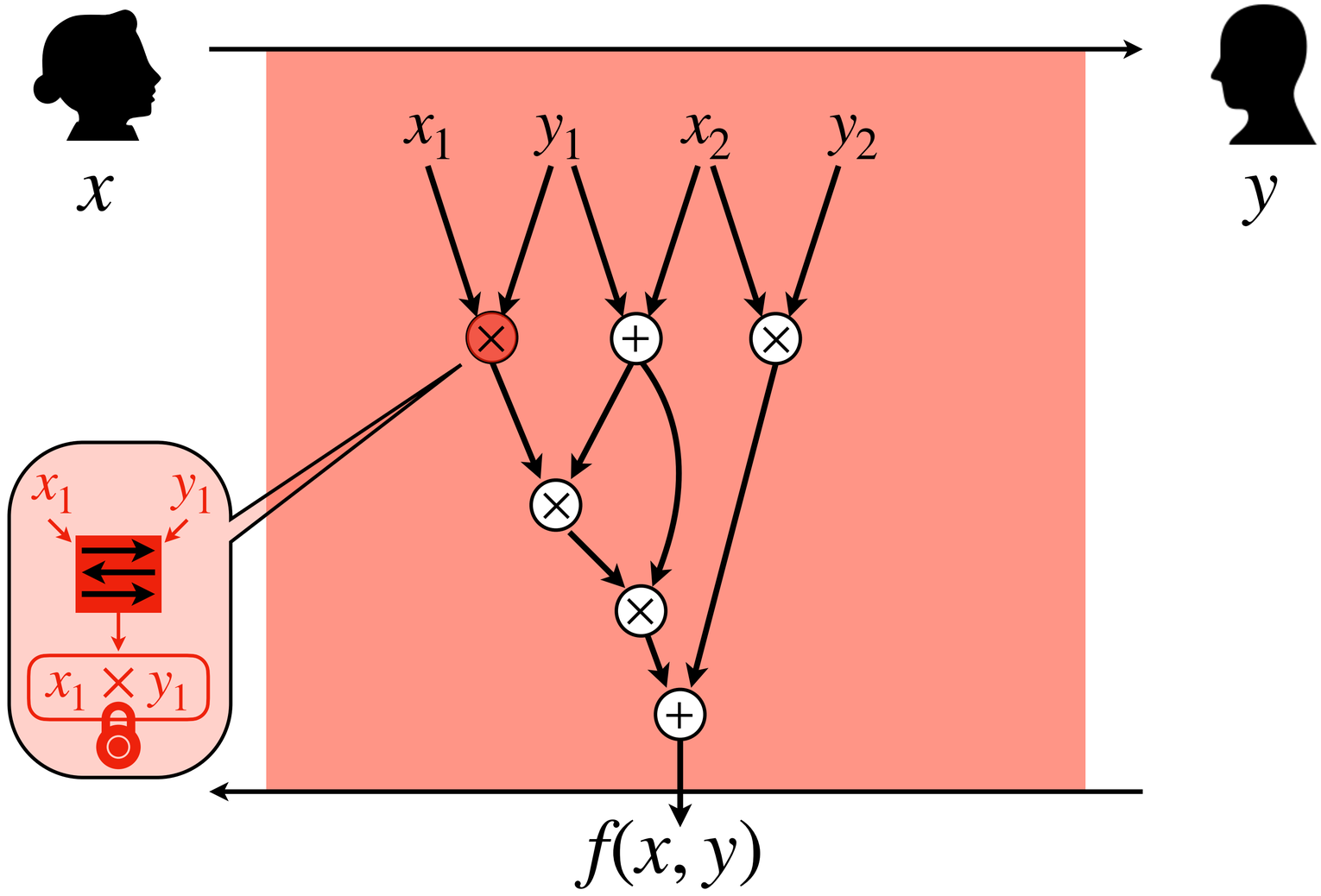
Exclusivement d'intérêt théorique

Un Nouveau Paradigme pour le Calcul Sécurisé

Goldreich, Micali, Wigderson, 1987

Beaver, 1995

Boyle, **Couteau**, Gilboa, Ishai 2018



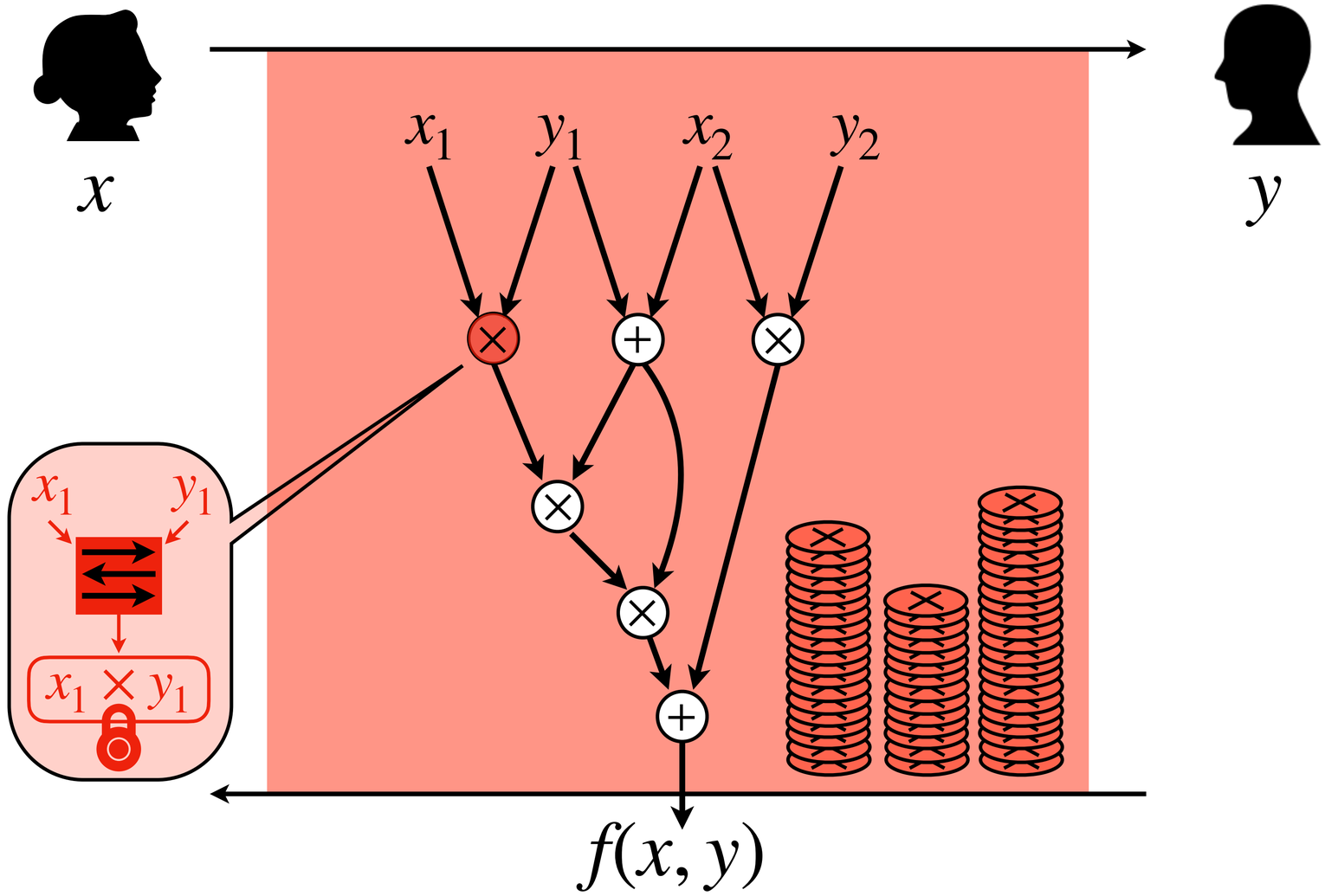
Exclusivement d'intérêt théorique

Un Nouveau Paradigme pour le Calcul Sécurisé

Goldreich, Micali, Wigderson, 1987

Beaver, 1995

Boyle, **Couteau**, Gilboa, Ishai 2018



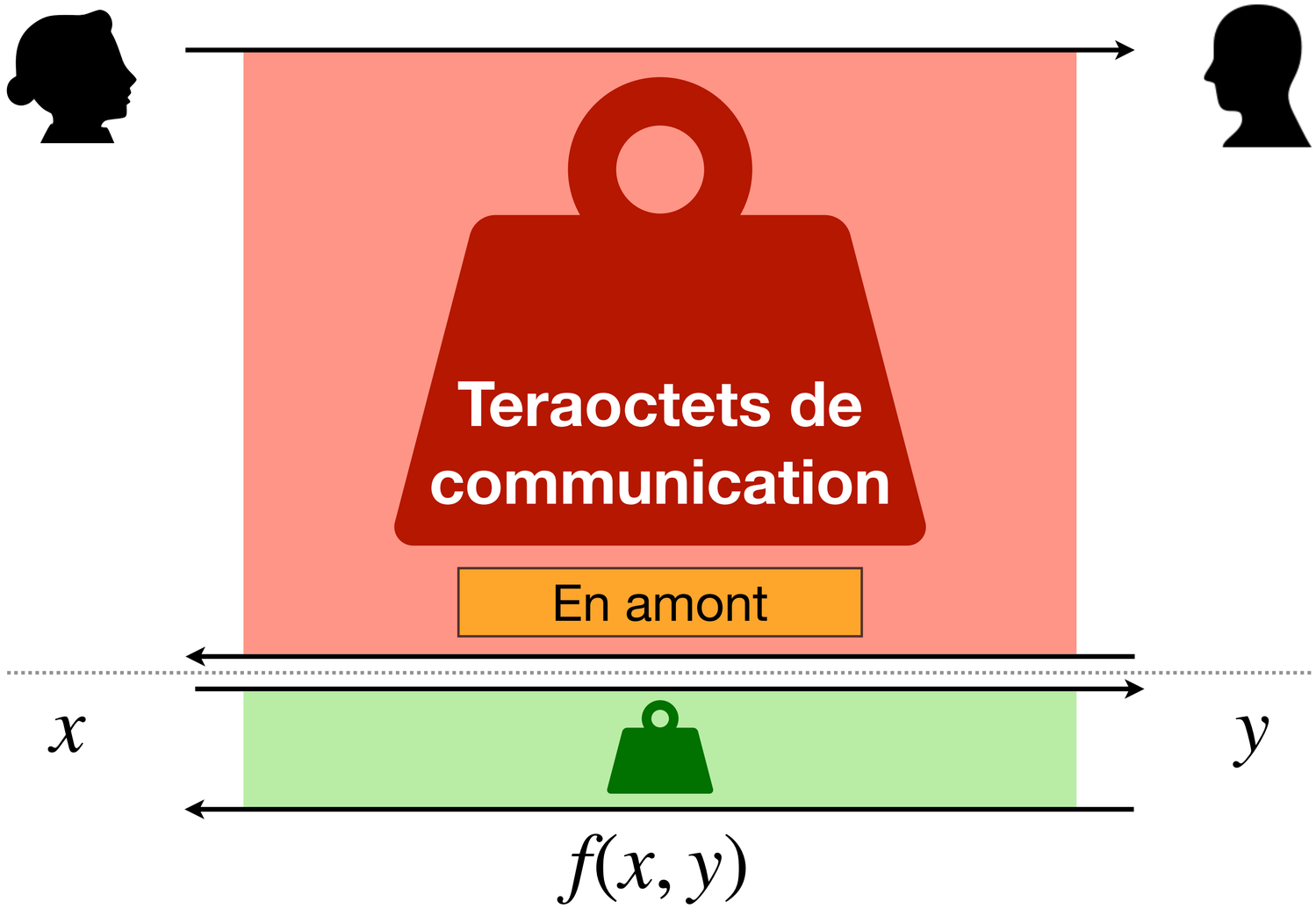
Exclusivement d'intérêt théorique

Un Nouveau Paradigme pour le Calcul Sécurisé

Goldreich, Micali, Wigderson, 1987

Beaver, 1995

Boyle, **Couteau**, Gilboa, Ishai 2018



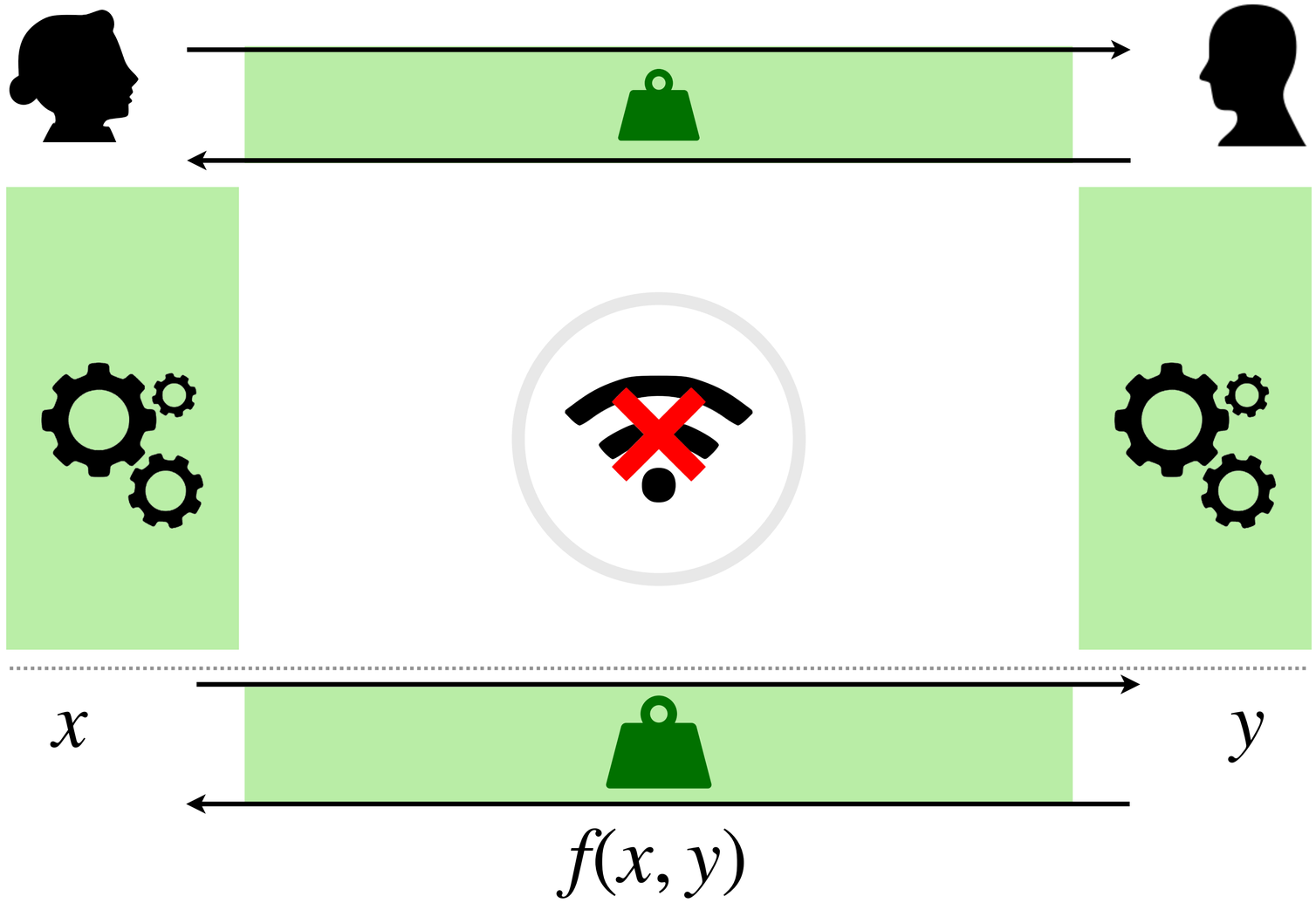
Inutilisable à grande échelle

Un Nouveau Paradigme pour le Calcul Sécurisé

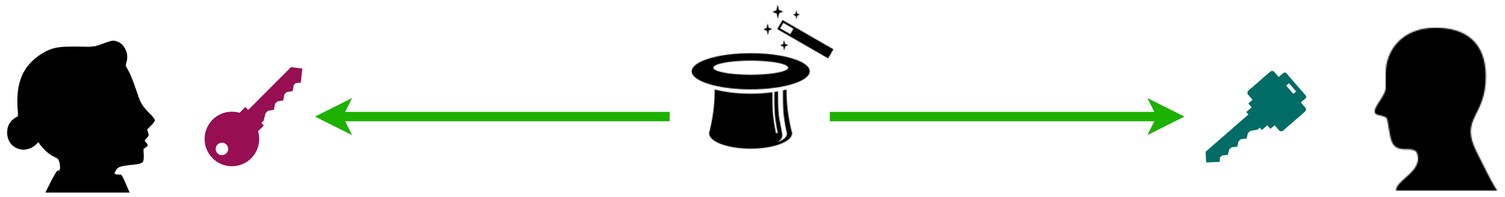
Goldreich, Micali, Wigderson, 1987

Beaver, 1995

Boyle, **Couteau**, Gilboa, Ishai 2018



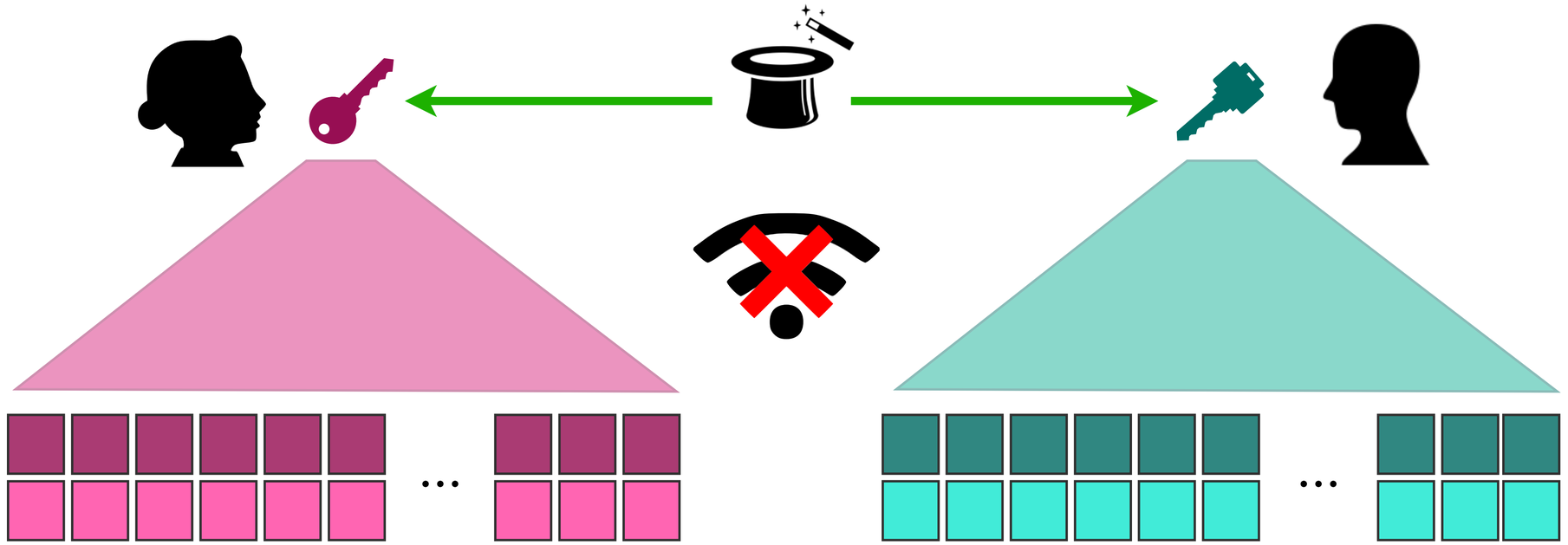
Générateurs de Corrélations Pseudoaléatoires [1,2]



[1] Compressing Vector OLE, **CCS 2018**
Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai

[2] Efficient Pseudorandom Correlation Generators: Silent OT Extension and More, **CRYPTO 2019**
Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl

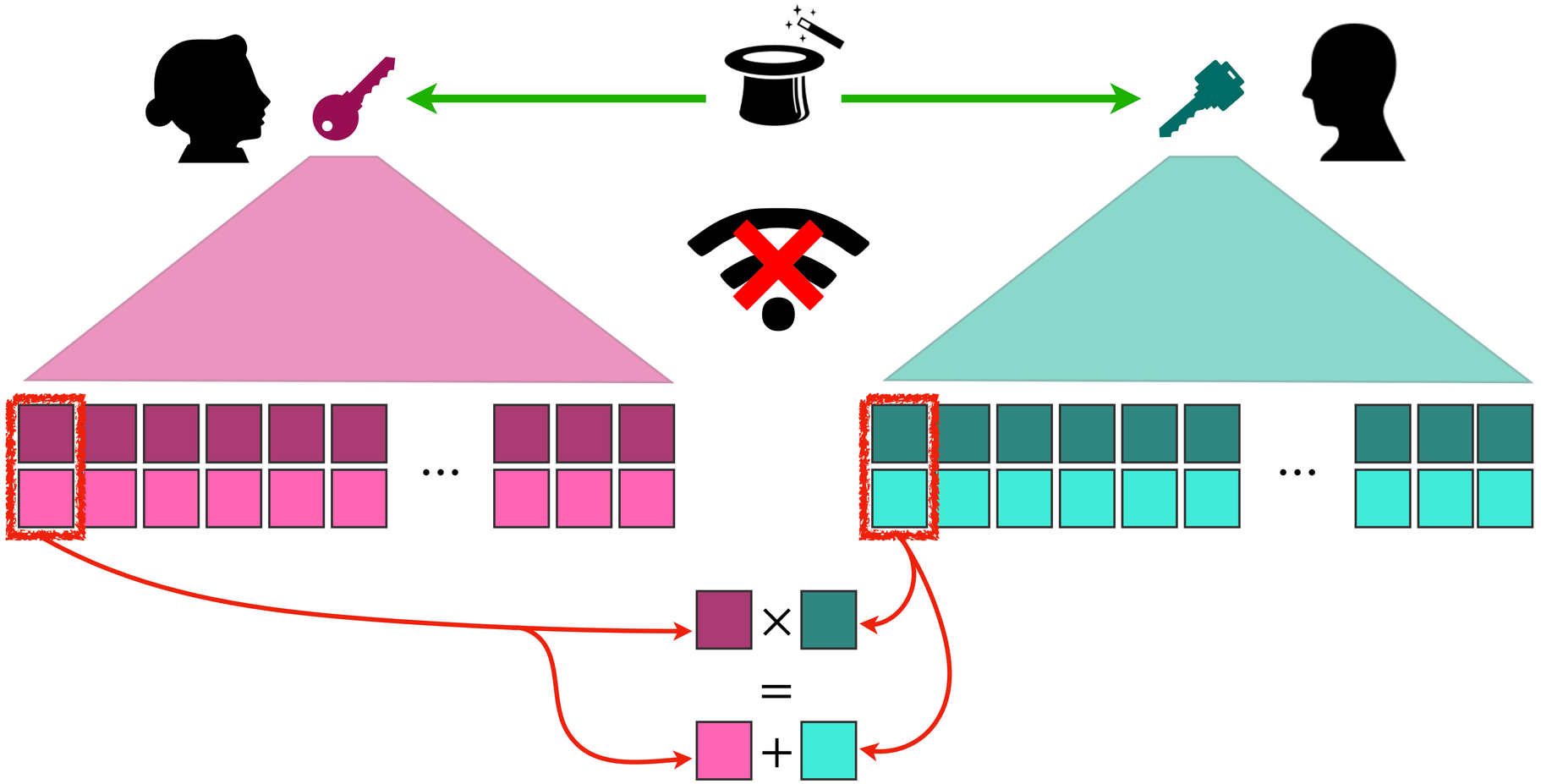
Générateurs de Corrélations Pseudoaléatoires [1,2]



[1] Compressing Vector OLE, **CCS 2018**
Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai

[2] Efficient Pseudorandom Correlation Generators: Silent OT Extension and More, **CRYPTO 2019**
Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl

Générateurs de Corrélations Pseudoaléatoires [1,2]



[1] Compressing Vector OLE, **CCS 2018**
Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai

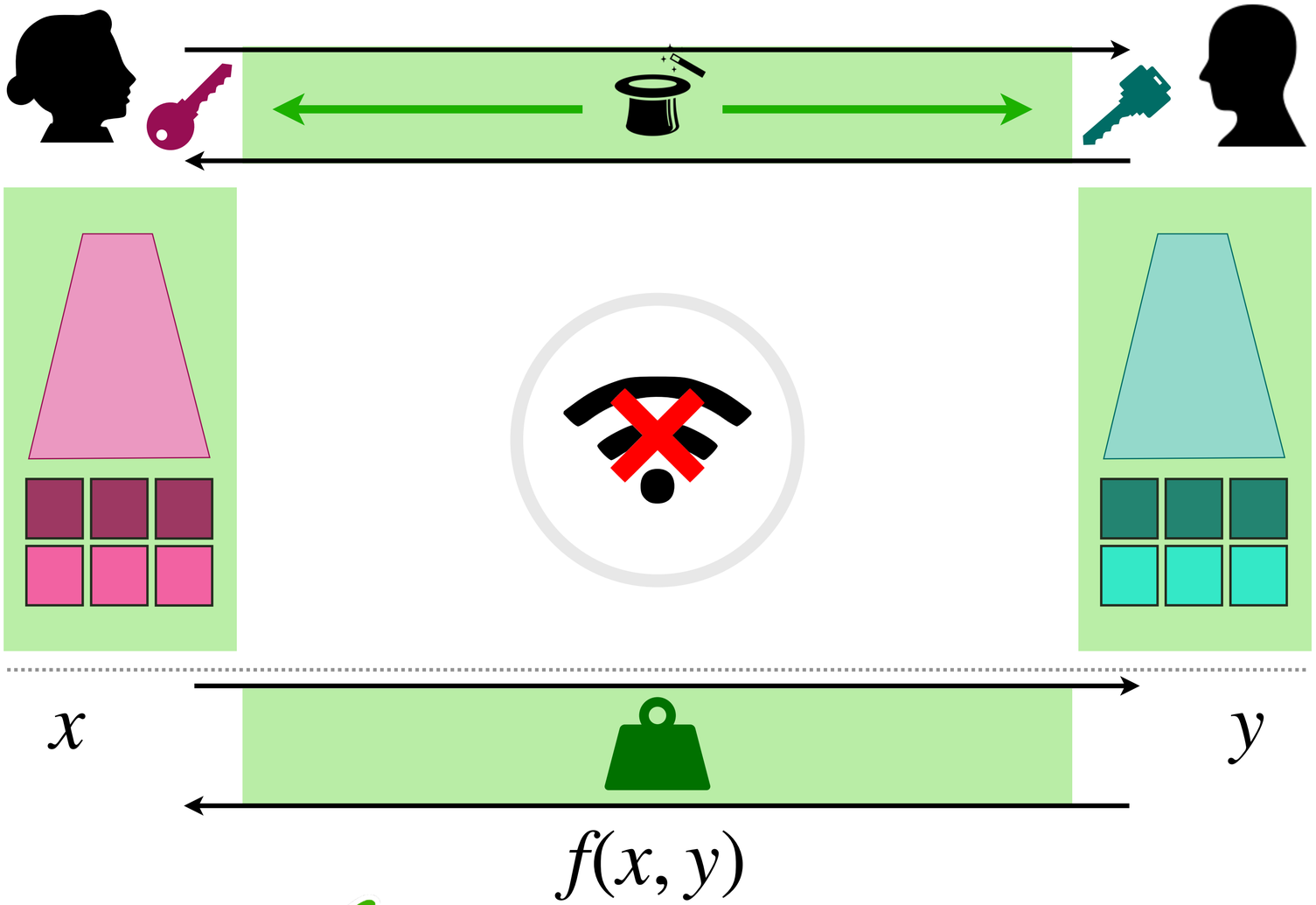
[2] Efficient Pseudorandom Correlation Generators: Silent OT Extension and More, **CRYPTO 2019**
Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl

Un Nouveau Paradigme pour le Calcul Sécurisé

Goldreich, Micali, Wigderson, 1987

Beaver, 1995

Boyle, **Couteau**, Gilboa, Ishai 2018



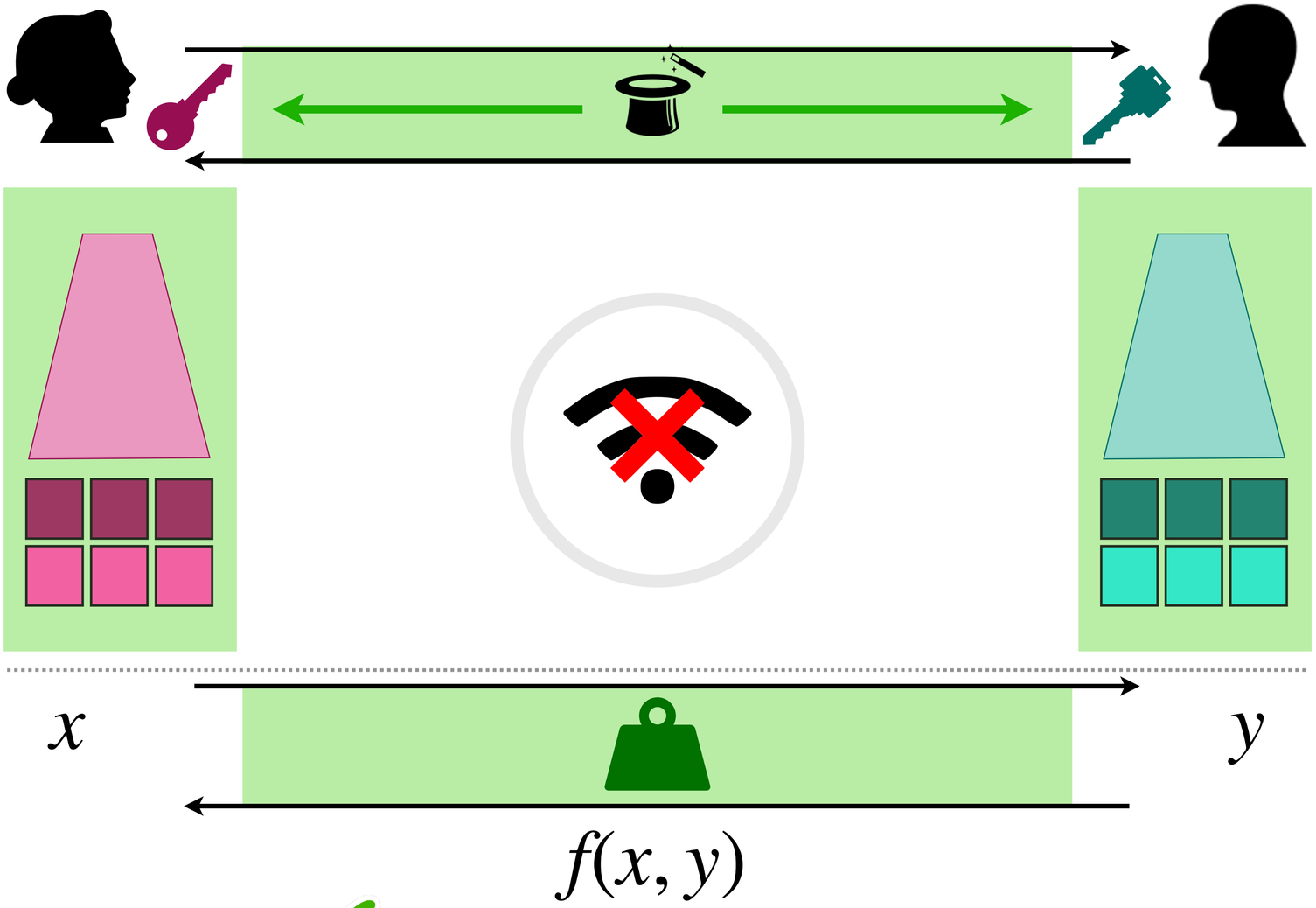
✓ Utilisable à grande échelle

Un Nouveau Paradigme pour le Calcul Sécurisé

Goldreich, Micali, Wigderson, 1987

Beaver, 1995

Boyle, **Couteau**, Gilboa, Ishai 2018



✓ Utilisable à grande échelle

… Dans certains cas

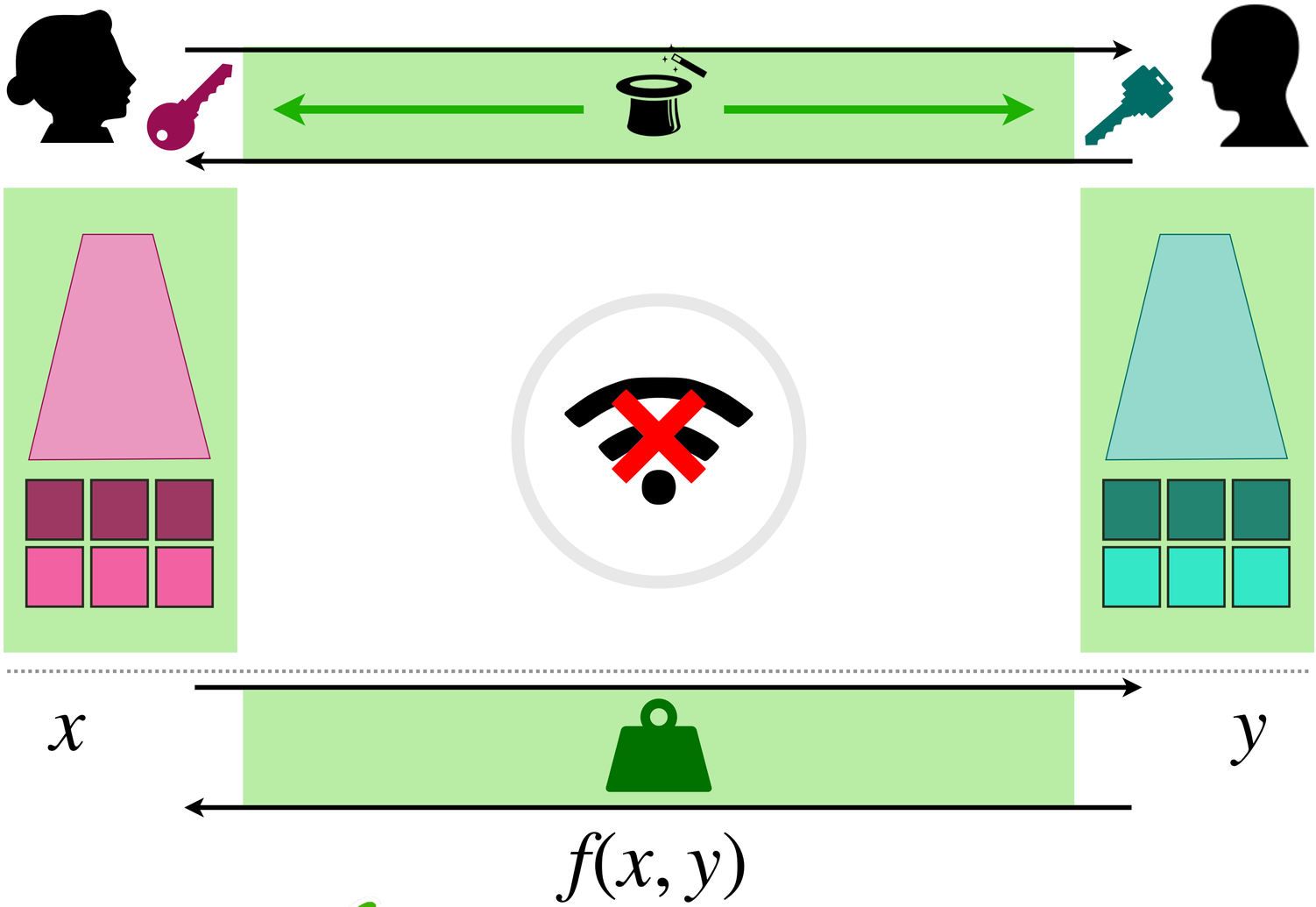
Un Nouveau Paradigme pour le Calcul Sécurisé

Goldreich, Micali, Wigderson, 1987

Beaver, 1995

Boyle, **Couteau**, Gilboa, Ishai 2018

- Fonctions restreintes
- Uniquement 2 joueurs
- Quantité d'aléa bornée
- Hypothèses nouvelles



Utilisable à grande échelle

… Dans certains cas

Une Sélection de Mes Travaux en Calcul Sécurisé Silencieux

CCS 2018

Générateur de correlations pseudo-aléatoires

+ faisabilité

- quatre verrous

Crypto 2019
CCS 2019

+ tous les circuits

Crypto 2020

+ n participants

- circuits sur corps larges

FOCS 2020

+ Calcul sécurisé silencieux sans limites

Crypto 2021
Crypto 2022

+ amélioration de la vitesse d'exécution

Crypto 2023
Asiacrypt 2024

+ n participants
+ tous les circuits

Eurocrypt 2024
Asiacrypt 2024

+ distribution des clés sans interaction

Asiacrypt 2025

+ hypothèse standard

Fonctions restreintes | 2 joueurs | Quantité d'aléa bornée | Hypothèses nouvelles

Une Sélection de Mes Travaux en Calcul Sécurisé Silencieux

CCS 2018

Générateur de correlations pseudo-aléatoires

+ faisabilité

- quatre verrous

Crypto 2019
CCS 2019

+ tous les circuits

Crypto 2020

+ n participants

- circuits sur corps larges

FOCS 2020

+ Calcul sécurisé silencieux sans limites

Crypto 2021
Crypto 2022

+ amélioration de la vitesse d'exécution

Crypto 2023
Asiacrypt 2024

+ n participants
+ tous les circuits

Eurocrypt 2024
Asiacrypt 2024

+ distribution des clés sans interaction

Asiacrypt 2025

+ hypothèse standard

Fonctions restreintes | 2 joueurs | Quantité d'aléa bornée | Hypothèses nouvelles

Une Sélection de Mes Travaux en Calcul Sécurisé Silencieux

CCS 2018

Générateur de correlations pseudo-aléatoires

+ faisabilité

- quatre verrous

Crypto 2019
CCS 2019

+ tous les circuits

Crypto 2020

+ n participants

- circuits sur corps larges

FOCS 2020

+ Calcul sécurisé silencieux sans limites

Crypto 2021
Crypto 2022

+ amélioration de la vitesse d'exécution

Crypto 2023
Asiacrypt 2024

+ n participants
+ tous les circuits

Eurocrypt 2024
Asiacrypt 2024

+ distribution des clés sans interaction

Asiacrypt 2025

+ hypothèse standard

Fonctions restreintes | 2 joueurs | Quantité d'aléa bornée | Hypothèses nouvelles

Une Sélection de Mes Travaux en Calcul Sécurisé Silencieux

CCS 2018

Générateur de correlations pseudo-aléatoires

+ faisabilité

- quatre verrous

Crypto 2019
CCS 2019

+ tous les circuits

Crypto 2020

+ n participants

- circuits sur corps larges

FOCS 2020

+ Calcul sécurisé silencieux sans limites

Crypto 2021
Crypto 2022

+ amélioration de la vitesse d'exécution

Crypto 2023
Asiacrypt 2024

+ n participants
+ tous les circuits

Eurocrypt 2024
Asiacrypt 2024

+ distribution des clés sans interaction

Asiacrypt 2025

+ hypothèse standard

Fonctions restreintes | 2 joueurs | Quantité d'aléa bornée | Hypothèses nouvelles

Une Sélection de Mes Travaux en Calcul Sécurisé Silencieux

CCS 2018

Générateur de correlations pseudo-aléatoires

+ faisabilité

- quatre verrous

Crypto 2019
CCS 2019

+ tous les circuits

Crypto 2020

+ n participants

- circuits sur corps larges

FOCS 2020

+ Calcul sécurisé silencieux sans limites

Crypto 2021
Crypto 2022

+ amélioration de la vitesse d'exécution

Crypto 2023
Asiacrypt 2024

+ n participants
+ tous les circuits

Eurocrypt 2024
Asiacrypt 2024

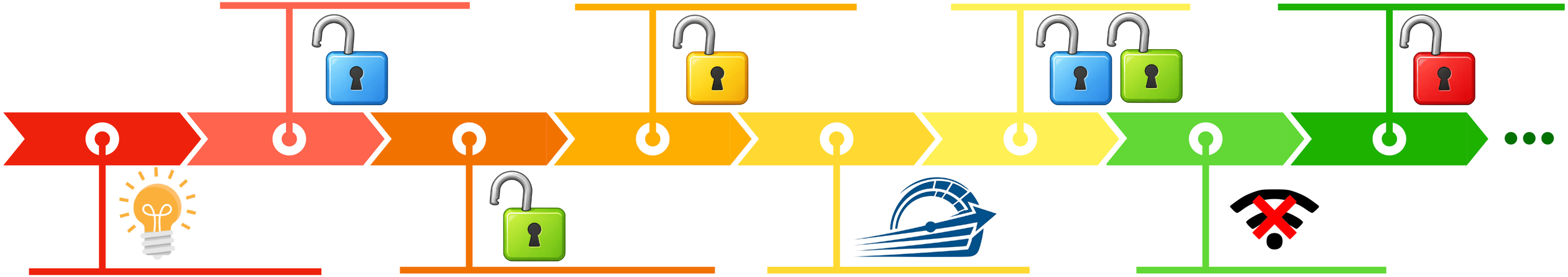
+ distribution des clés sans interaction

Asiacrypt 2025

+ hypothèse standard

Fonctions restreintes | 2 joueurs | Quantité d'aléa bornée | Hypothèses nouvelles

Une Sélection de Mes Travaux en Calcul Sécurisé Silencieux



CCS 2018

Générateur de correlations pseudo-aléatoires

\+ faisabilité

\- quatre verrous

Crypto 2019
CCS 2019

\+ tous les circuits

Crypto 2020

\+ n participants

\- circuits sur corps larges

FOCS 2020

\+ Calcul sécurisé silencieux sans limites

Crypto 2021
Crypto 2022

\+ amélioration de la vitesse d'exécution

Crypto 2023
Asiacrypt 2024

\+ n participants
\+ tous les circuits

Eurocrypt 2024
Asiacrypt 2024

\+ distribution des clés sans interaction

Asiacrypt 2025

\+ hypothèse standard

Fonctions restreintes | 2 joueurs | Quantité d'aléa bornée | Hypothèses nouvelles

Une Sélection de Mes Travaux en Calcul Sécurisé Silencieux

CCS 2018

Générateur de correlations pseudo-aléatoires

+ faisabilité

- quatre verrous

Crypto 2019
CCS 2019

+ tous les circuits

Crypto 2020

+ n participants

- circuits sur corps larges

FOCS 2020

+ Calcul sécurisé silencieux sans limites

Crypto 2021
Crypto 2022

+ amélioration de la vitesse d'exécution

Crypto 2023
Asiacrypt 2024

+ n participants
+ tous les circuits

Eurocrypt 2024
Asiacrypt 2024

+ distribution des clés sans interaction

Asiacrypt 2025

+ hypothèse standard

Fonctions restreintes | 2 joueurs | Quantité d'aléa bornée | Hypothèses nouvelles

Calcul Sécurisé Silencieux à n Joueurs, Bref Aperçu ([1,2])

[1] Correlated Pseudorandomness from the Hardness of Quasi-Abelian Decoding, **CRYPTO 2023**
Maxime Bombar, Geoffroy Couteau, Alain Couvreur, Clément Ducros

[2] FOLEAGE: F4-OLE-Based Multi-Party Computation for Boolean Circuits, **ASIACRYPT 2024**
Maxime Bombar, Dung Bui, Geoffroy Couteau, Alain Couvreur, Clément Ducros, Sacha Servan-Schreiber

Calcul Sécurisé Silencieux à n Joueurs, Bref Aperçu ([1,2])

Exemple. Soit $\mathscr{R} = \mathbb{F}[\mathbb{G}]$ une algèbre de groupe :

$$\mathscr{R} = \left\{ \sum_{x \in \mathbb{F}} x \cdot g_x \;\middle|\; g_x \in \mathbb{G} \right\} = \mathbb{F}_q[X_1, \ldots, X_d]/(X_1^{q-1} - 1, \ldots, X_d^{q-1} - 1)$$

Théorème : si $(a, a \cdot e + f) \approx$ aléatoire pour e, f « creux » et si $\mathscr{R}$ admet une transformée de Fourier rapide, $\exists$ un générateur de corrélation pseudoaléatoire efficace à n joueurs sur $\mathbb{F}$.

[1] Correlated Pseudorandomness from the Hardness of Quasi-Abelian Decoding, **CRYPTO 2023**
Maxime Bombar, Geoffroy Couteau, Alain Couvreur, Clément Ducros

[2] FOLEAGE: F4-OLE-Based Multi-Party Computation for Boolean Circuits, **ASIACRYPT 2024**
Maxime Bombar, Dung Bui, Geoffroy Couteau, Alain Couvreur, Clément Ducros, Sacha Servan-Schreiber

Calcul Sécurisé Silencieux à n Joueurs, Bref Aperçu ([1,2])

Exemple. Soit $\mathscr{R} = \mathbb{F}[\mathbb{G}]$ une algèbre de groupe :

$$\mathscr{R} = \left\{ \sum_{x \in \mathbb{F}} x \cdot g_x \;\middle|\; g_x \in \mathbb{G} \right\} = \mathbb{F}_q[X_1, \ldots, X_d]/(X_1^{q-1} - 1, \ldots, X_d^{q-1} - 1)$$

Théorème : si $(a, a \cdot e + f) \approx$ aléatoire pour e, f « creux » et si $\mathscr{R}$ admet une transformée de Fourier rapide, $\exists$ un générateur de corrélation pseudoaléatoire efficace à n joueurs sur $\mathbb{F}$.

Concevoir (et implémenter) une FFT optimisée sur des algèbres de groupe

« Distinguer $(a, a \cdot e + f)$ d'un aléa » $\Longleftrightarrow$ problème du décodage de codes quasi-abéliens, étudié en théorie des codes depuis les années 90

[1] Correlated Pseudorandomness from the Hardness of Quasi-Abelian Decoding, **CRYPTO 2023**
Maxime Bombar, Geoffroy Couteau, Alain Couvreur, Clément Ducros

[2] FOLEAGE: F4-OLE-Based Multi-Party Computation for Boolean Circuits, **ASIACRYPT 2024**
Maxime Bombar, Dung Bui, Geoffroy Couteau, Alain Couvreur, Clément Ducros, Sacha Servan-Schreiber

Des Implémentations et des Déploiements par des Entreprises

Collaborations

Category Labs

Chainlink

ZKPASS

VISA Research

ANT GROUP

Consultant

Fireblocks

Autres

J.P.Morgan

holonym

Google

aws

TA

primus

STEALTH SOFTWARE

Programme de Recherche

Programme de Recherche

Calcul sécurisé sur Internet

Défi 1 : le passage à l'échelle

Les protocoles deviennent inefficaces pour n grand (coût en $\mathcal{O}(n^2)$).
Comment passer à l'échelle de millions d'utilisateurs ?

Défi 2 : l'interactivité

Les protocoles nécessitent beaucoup d'allers-retours. Peut-on les rendre *non-interactifs* pour réduire la latence ?

Défi 3 : la communication

La communication grandit avec la taille de la fonction à calculer.
Peut-on communiquer moins que la taille du circuit ?

Défi 4 : fondements théoriques

Quelle cryptographie si P = NP ?
Quelles limites pour l'apprentissage machine ?

Programme de Recherche

Calcul sécurisé sur Internet

Défi 1 : le passage à l'échelle

Les protocoles deviennent inefficaces pour n grand (coût en $\mathcal{O}(n^2)$).
Comment passer à l'échelle de millions d'utilisateurs ?

Défi 2 : l'interactivité

Les protocoles nécessitent beaucoup d'allers-retours. Peut-on les rendre *non-interactifs* pour réduire la latence ?

Défi 3 : la communication

La communication grandit avec la taille de la fonction à calculer.
Peut-on communiquer moins que la taille du circuit ?

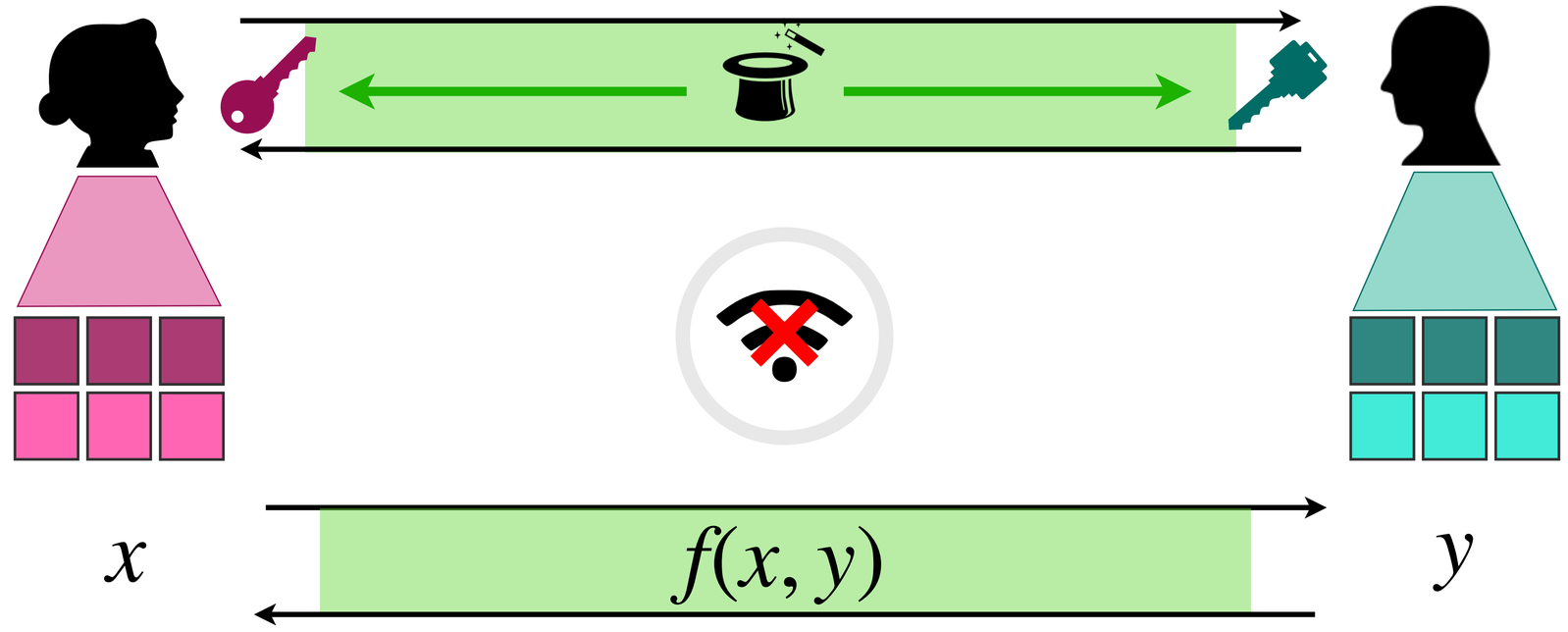
Défi 4 : fondements théoriques

Quelle cryptographie si P = NP ?
Quelles limites pour l'apprentissage machine ?

Focus sur le Défi 2 : Calcul Sécurisé Non-Interactif

Communiquer par Internet, aujourd'hui :

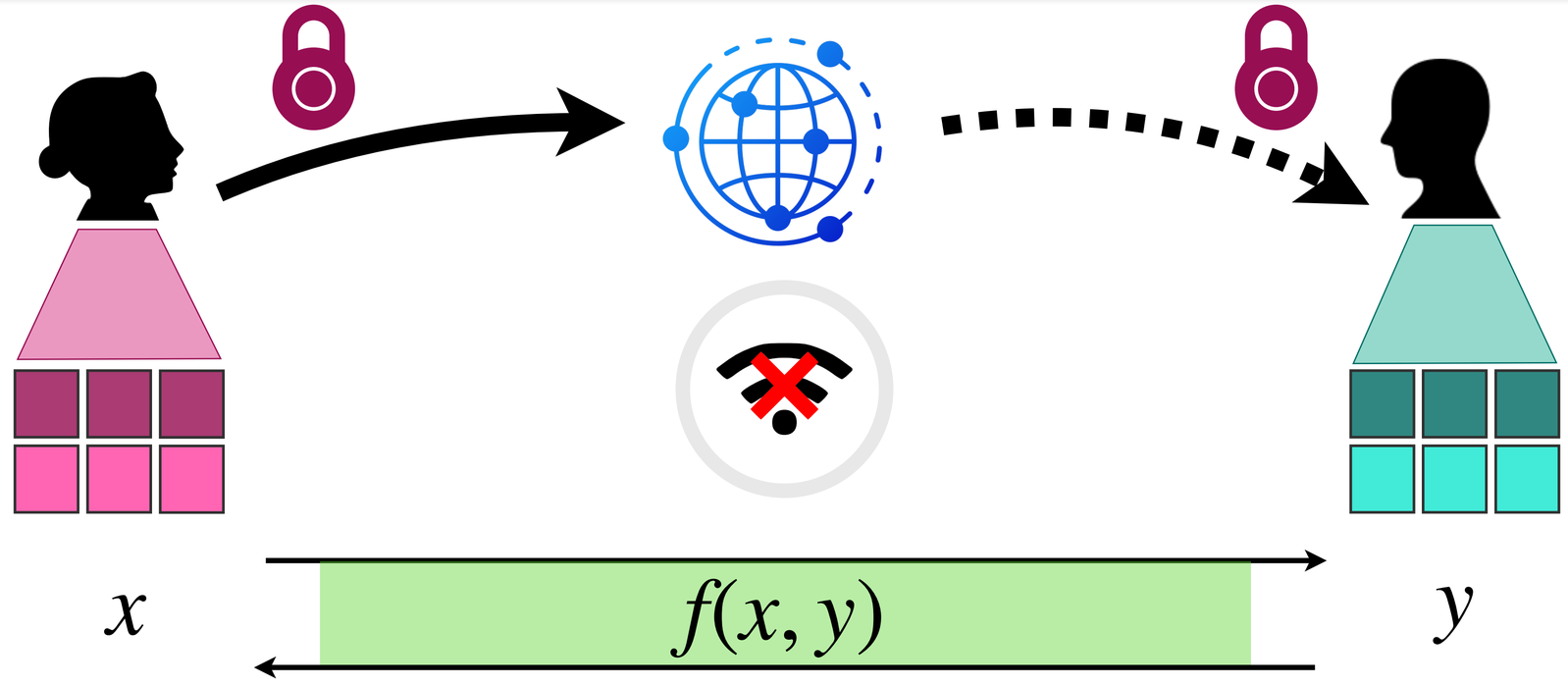
Calcul sécurisé silencieux :



Focus sur le Défi 2 : Calcul Sécurisé Non-Interactif

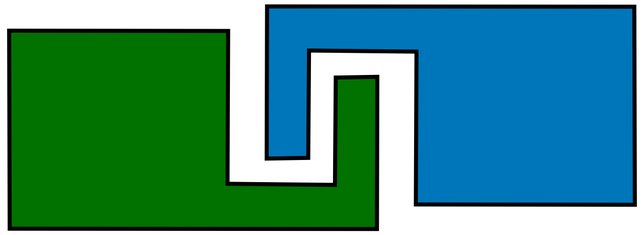
Communiquer par Internet, aujourd'hui :

Calcul sécurisé silencieux… Non-interactif ?



Focus sur le Défi 2 : Calcul Sécurisé Non-Interactif

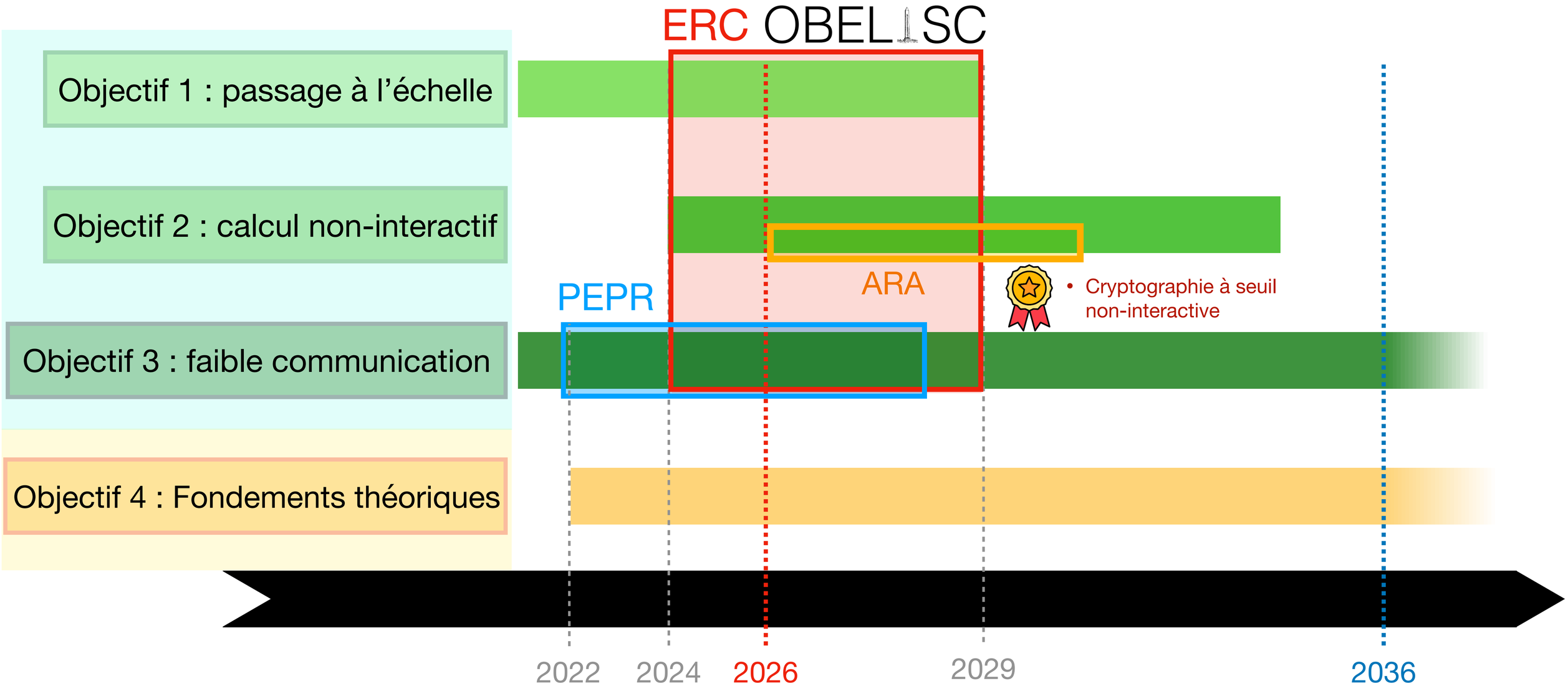
- Fondamentalement impossible dans le framework utilisé jusqu'alors
- On introduit dans [1] un paradigme radicalement différent



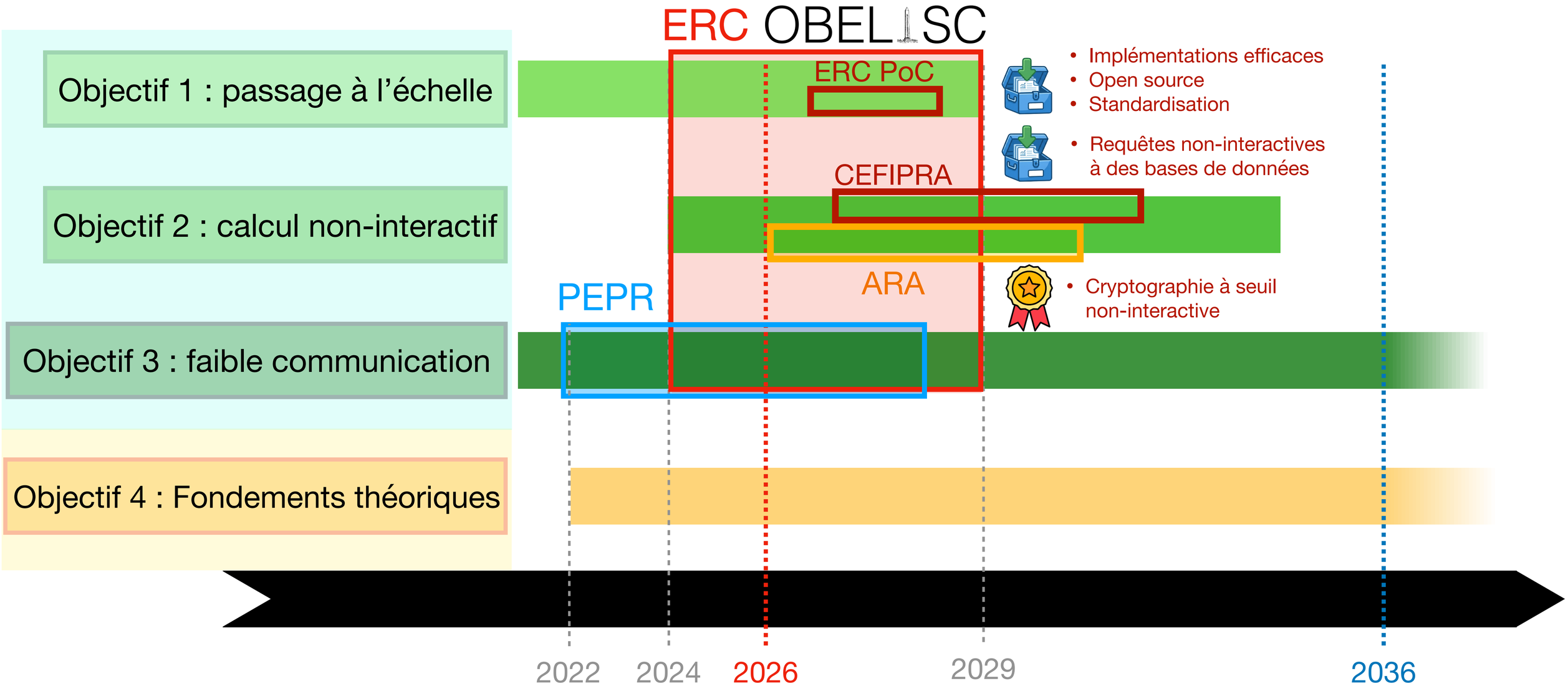
Il existe une unique construction de  … Et elle repose sur des hypothèses qu'un ordinateur quantique pourrait casser !

[1] Fast Public-Key Silent OT and More from Constrained Naor-Reingold, **EUROCRYPT 2024**
Dung Bui, Geoffroy Couteau, Pierre Meyer, Alain Passelègue, Mahshid Riahinia

Déroulement



Déroulement



Merci pour votre attention

Publications

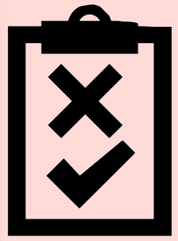
70 publications (+2 janvier)
- **47** : FOCS, Crypto, EC, AC, JoC, CCS, S&P
- **40** : avec étudiant·es/postdocs encadrés

Projets en cours

- ERC Starting Grant
- PEPR Cybersécurité
- **(Nouveau)** Amazon Research Award

Encadrement

- **8** doctorant·e·s (**5** soutenus)
- **13** postdocs (**6** en cours)
- **13** longues visites (> 2 mois)



Responsabilités

- Responsable d'équipe AlgoComp
- Responsable de commission

Programme de Recherche

Efficacité et passage à l'échelle du calcul sécurisé silencieux

Calcul sécurisé non-interactif

Calcul sécurisé avec faible communication

Fondations théoriques de la cryptographie