OCAM

Opérateurs Cryptographiques et Arithmétique Matérielle

INRIA / LIP / LIRMM

Coordinateur : Nicolas Sendrier

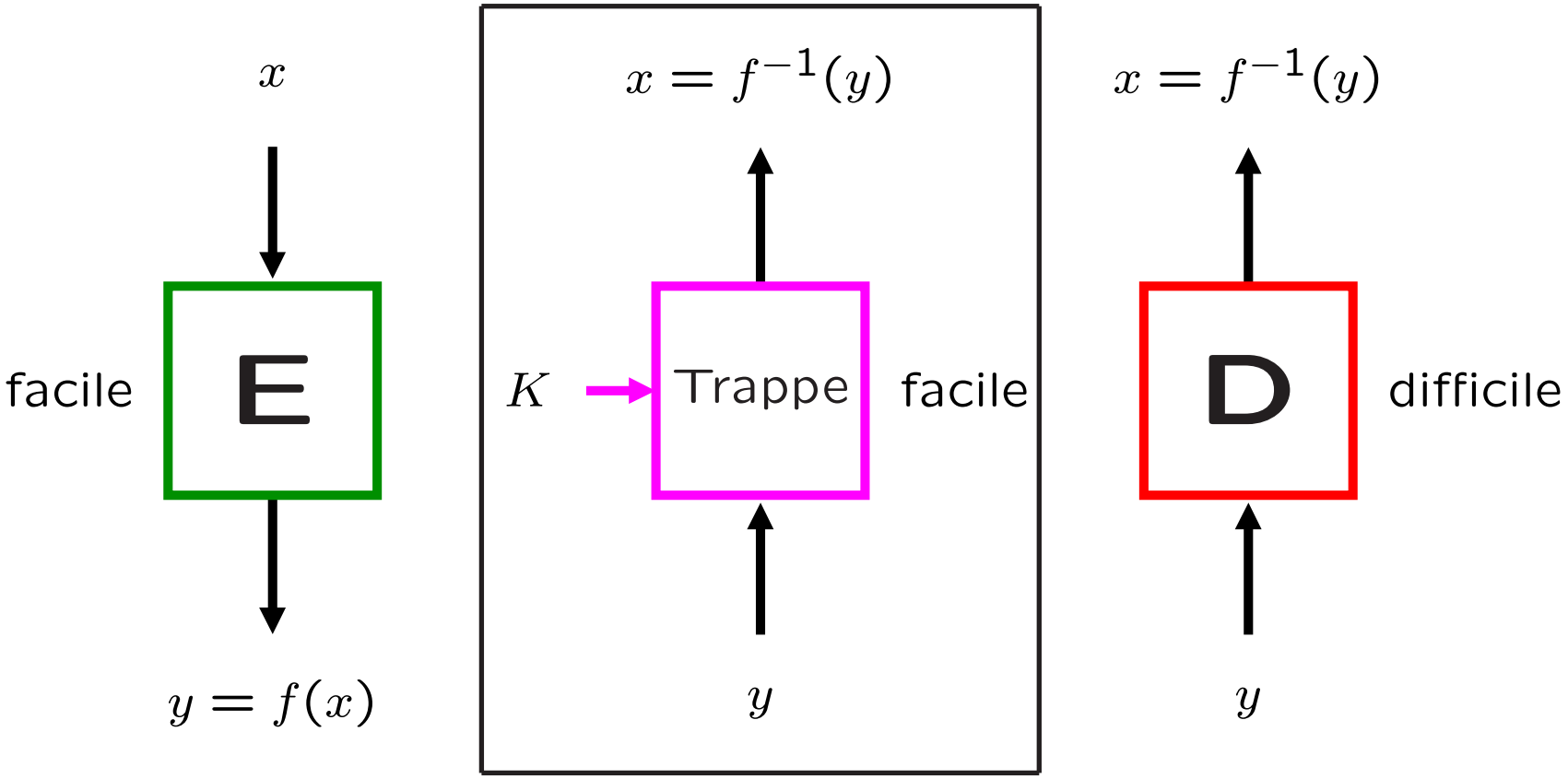
- Implémentation matérielle de cryptosystèmes
- Cryptologie basée sur les codes correcteurs d'erreurs
- Algorithmique des corps finis

Algorithmes de signature

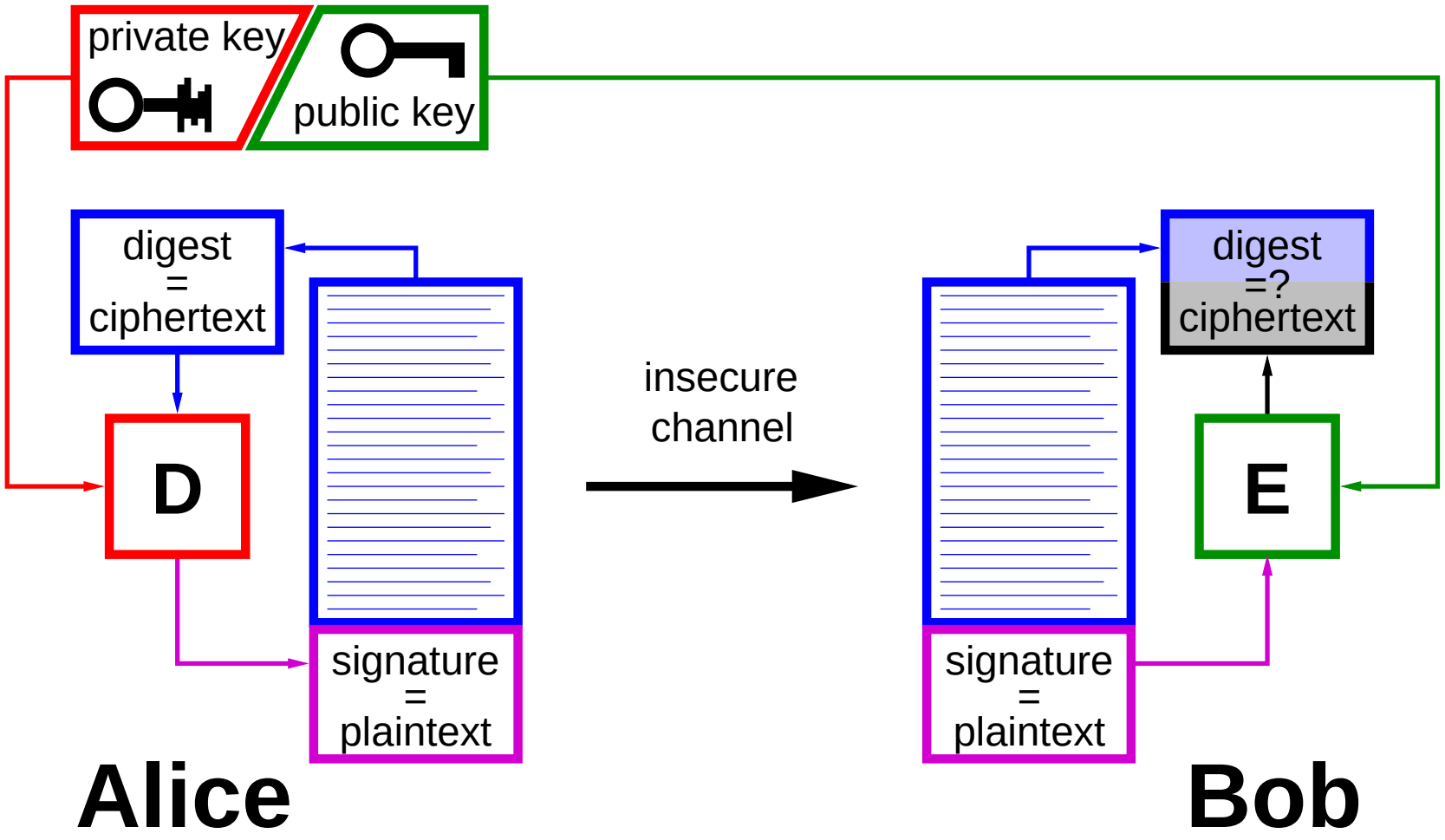
- **Classiques** : sécurité éprouvée
  - RSA, longueur 1024 bits
  - Courbes elliptiques, 320 bits
- **Récents** : sécurité à prouver
  - Couplage de Weil, 160 bits
  - HFE (SFLASH), 128 bits

- **Nouveau** : réduction *prouvée* de sécurité
  - Asiacrypt 2001 [Courtois, Finiasz, S.], 80 bits
    basé sur les codes correcteurs d'erreurs (Niederreiter)

Fonction à sens unique à trappe



Signature à partir du chiffrement



Signer avec un code $\Leftrightarrow$ Décodage complet

Avec le système de chiffrement de McEliece (ou de Niederreiter) le condensé (*digest*) n'est pas un cryptogramme en général, à moins de pouvoir effectuer un décodage complet.

Problème : trouver un code (des paramètres) tel que
- Le décodage complet soit trop difficile sans la trappe
- Le décodage complet soit possible avec la trappe

Solution : un code de grande longueur corrigeant peu d'erreurs

Un schéma de signature utilisant les codes

Schéma de Niederreiter avec un code de Goppa
de longueur $n = 2^{16}$ correcteur de $t = 9$ erreurs

	$n = 2^m$	$m = 16,\ t = 9$	
Longueur	$(t-1)m + log_2(t)$	132 bits	81 bits
Coût d'une signature	$O(t!t^2m^3)$	≈ 2 mn	
Coût d'une vérification	$O(t^2m)$	$\approx 1\ \mu$s	≈ 1 mn
Taille de la clé publique	$tm(2^m - tm)$	≈ 1.1 Mo	
Attaque par décodage	$2^{tm/2(1+o(1))}$	2^{80}	
Attaque par structure	$2^{tm(1+o(1))}$	2^{119}	

Comment rendre le système (plus) praticable ?

– En réduisant la taille de la clé publique
– En accélérant le calcul de la signature

Avec un code de Goppa t-correcteur de longueur 2^m ($t = 9$, $m = 16$)

Chaque signature nécessite en moyenne $t! \simeq 360\,000$ décodages dans le code de Goppa.

Chaque décodage nécessite
– un calcul de syndrome (algèbre linéaire), coût $O(m^2t^2)$
– un algorithme d'Euclide dans $\mathbf{F}_{2^m}$, coût $O(m^2t^2)$
– un test de divisibilité dans $\mathbf{F}_{2^m}[z]$, coût $O(m^3t^2)$

La composition du projet OCAM

- **LIRMM** Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier
  Équipe Arithmétique Informatique
  Laurent Imbert, Jean-Claude Bajard
- **LIP** Laboratoire de l'Informatique du Parallélisme
  Projet Arénaire
  Arnaud Tisserand, Jean-Luc Beuchat, Gilles Villard
- **INRIA** Rocquencourt
  Projet Codes
  Nicolas Sendrier, Matthieu Finiasz, Pierre Loidreau

Les objectifs initiaux du projet OCAM

- Implantation matérielle de l'algorithme de signature
- Étude d'autres algorithmes cryptographiques algébriques en vue de leur implantation matérielle
- Arithmétique des extensions de $\mathbf{F}_2$ et applications en cryptologie