Présentation des candidats CAESAR

Brice Minaud

ANSSI, 17 octobre 2014

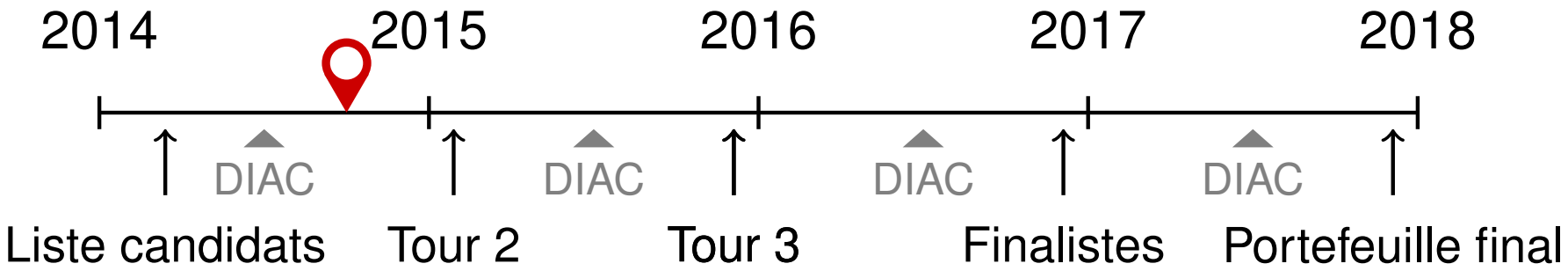
Plan

La Compétition CAESAR

- « Suite » d'AES, eSTREAM, SHA-3...
- Chiffrements authentifiés.
- Motivation :
  - AES-GCM a une sécurité imparfaite (réutilisation du nonce, limite de données...)
  - OCB est breveté (aux US ; sauf GPL).
- Principe : pas de critères absolus.
  $\Rightarrow$ Portefeuille d'algorithmes choisis.
- *Sponsorisée* par le NIST, organisée par Dan Bernstein.

La Compétition CAESAR

Déroulement prévu :



Jury :

Steve Babbage
Anne Canteaut
Christophe De Cannière
Tetsu Iwata
David McGrew
Bart Preneel
Phillip Rogaway
Hongjun Wu
Daniel J. Bernstein
Carlos Cid
Orr Dunkelman
Lars R. Knudsen
Willi Meier
Vincent Rijmen
Greg Rose
Alex Biryukov
Joan Daemen
Henri Gilbert ←
Stefan Lucks
Kaisa Nyberg
Matt Robshaw
Serge Vaudenay

Informations

- Le site principal, de Dan Bernstein (notamment, les candidats) :
  competitions.cr.yp.to/
- La mailing list (notamment, les attaques) :
  groups.google.com/d/forum/crypto-competitions
- Le zoo (pas complètement à jour) :
  aezoo.compute.dtu.dk

Les Candidats au Premier Tour

- 57 candidats.
- Mais, 8 cassés rapidement, 3 dans les limbes (en attente de corrections depuis des mois), 2 camisoles, 3 très suspects (problèmes de spéfication etc)
  $\Rightarrow$ environ 40 candidats réellement éligibles pour le second tour.
- Environ 30% sont de purs modes ($\approx$ une quinzaine).

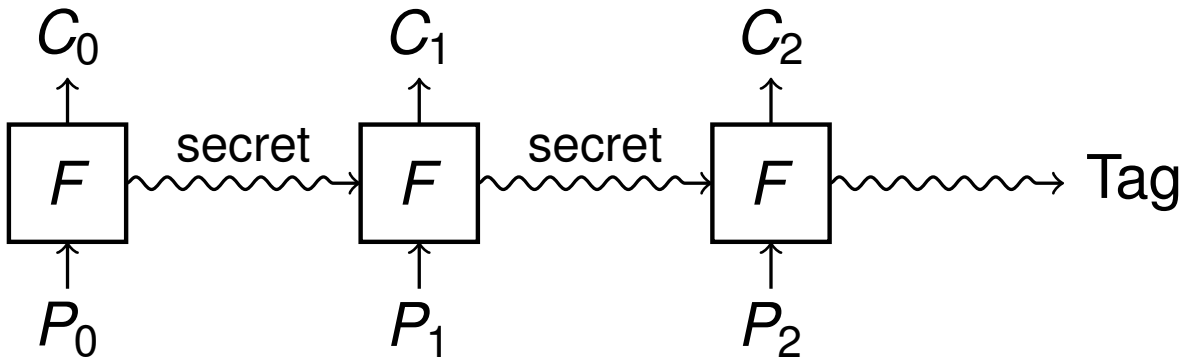
Quelques caractéristiques distinctives

- Nonce misuse.
  - 1 réutilisation donne la clef d'intégrité pour AES-GCM.
  - Dans tous les cas pour un chiffrement *online*, répétition de nonce $\Rightarrow$ information sur préfixes de messages égaux, et possibilité de deviner message bloc par bloc.
  - La « AE-nonce-misuse resistance » complète est très chère (cf infra). Nécessite résistance différentielle etc.
  - Suffit peut-être que nonce misuse n'implique pas fuite d'info sur clef ou possibilité de forge.
- Decryption misuse.
  - Inévitable pour schéma online. Implique nonce misuse.
  - Sous-traité (déchiffrement offline, tags intermédiaires...), pas de nomenclature établie.
  - Comme nonce misuse, évite en général au moins fuite d'info sur clef/forge. Mais pas dans le claim de sécurité.
- Poids (lightweight).
- Efficacité software/hardware. Notamment : optimisation par AES-NI ; ou surcoût de masquage diminué.

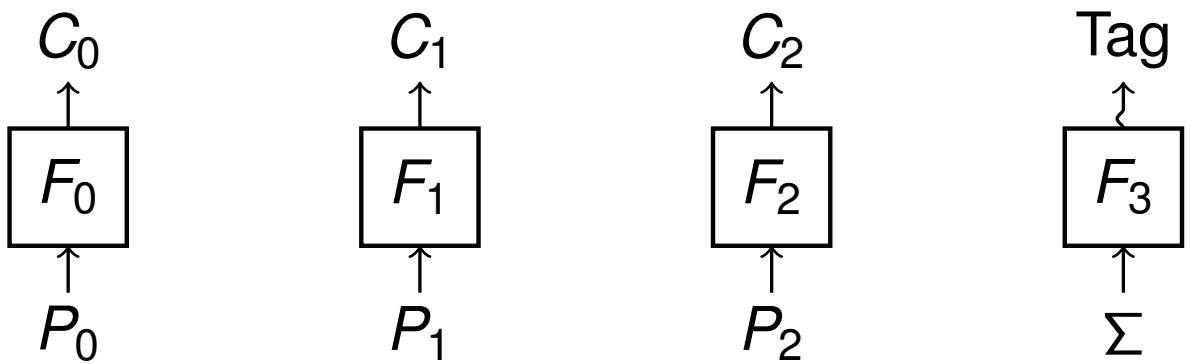
Candidats : quelques grandes familles

On met à part les modes.
Intégrité $\Rightarrow$ ordre des blocs est non malléable.

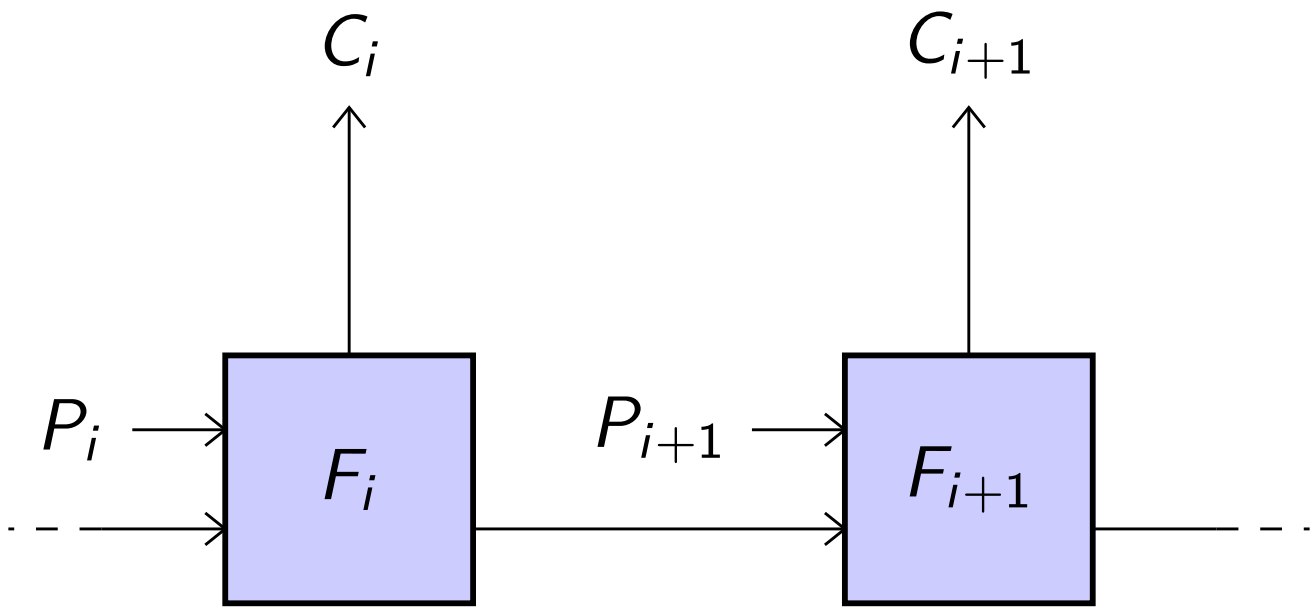
1. Un secret un transmis (modèle « leakage » : ALE, Fides, Duplex...).



2. Chiffrements indépendants, i.e. tweakable block cipher.

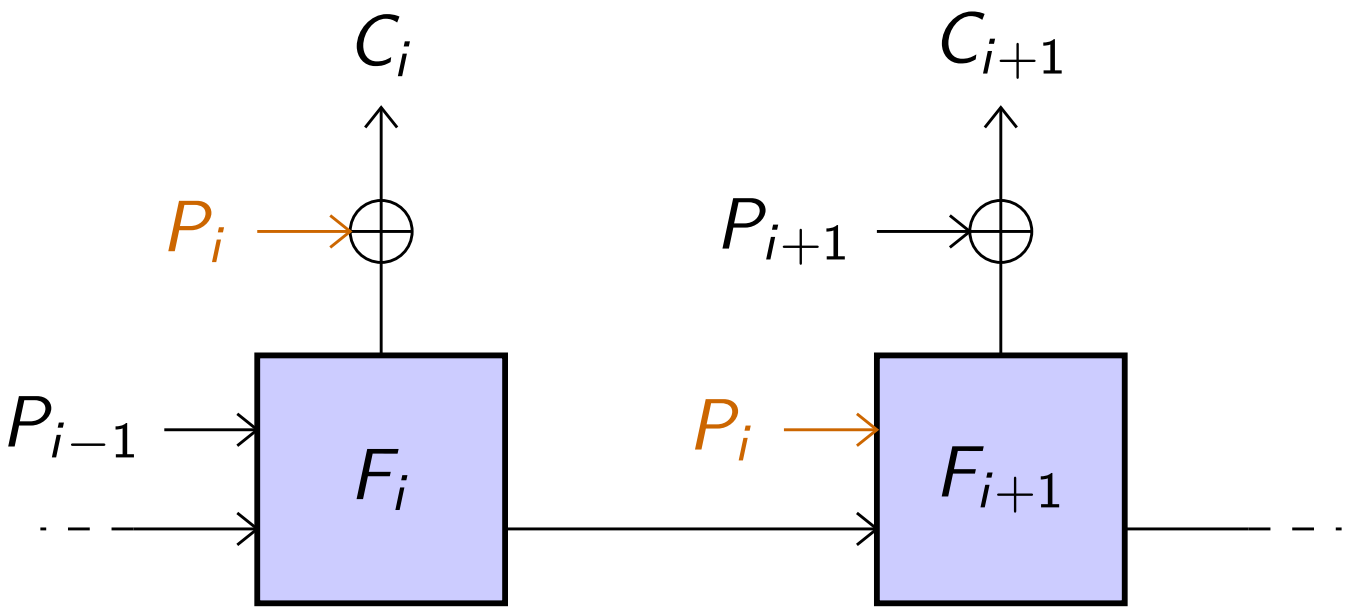


Famille « leakage »



Cela nécessite F_i^{-1} pour le déchiffrement.

Famille « leakage »



P_i est inséré dans l'état après la production de C_i.

Famille « leakage »

Deux grandes sous-familles :

1. Variantes de duplex.

   Artemia, Ascon ($\approx$ LS-design), CBEAM, ICEPOLE, Keyak & Ketje ($\approx$ mini-Keccak), PANDA, π-Cipher, 2/3 PRIMATEs (AES-like), STRIBOB ($\approx$ GOST)...

2. AEGIS-like.

   AEGIS, MORUS, PAES, Tiaoxin.

Famille « tweakable » 

- État moins grand ; seule chance de vrai lightweight ?
- Plus de fuite si un nonce est répété.

  Deoxys, Joltik, KIASU, SCREAM/iSCREAM.

Quelques candidats intéressants

- AEGIS.
  Hongjun Wu, Bart Preneel.
- Deoxys, Joltik, KIASU.
  Jérémy Jean, Ivica Nikolić, Thomas Peyrin.
- Keyak et Ketje.
  Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, Ronny Van Keer.
- MORUS.
  Hongjun Wu, Tao Huang.
- SCREAM/iSCREAM.
  Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici.
- ACORN, Ascon, ICEPOLE, Minalpher, NORX, PRIMATEs, Prøst, STRIBOB, Tiaoxin...