Conception d'outils d'audit de primitives cryptographiques

CryptAudit

anr agence nationale de la recherche

Appel : ANR-17-CE39-0003

Année : 2017

Instrument : JCJC

Contact : patrick.derbez@irisa.fr

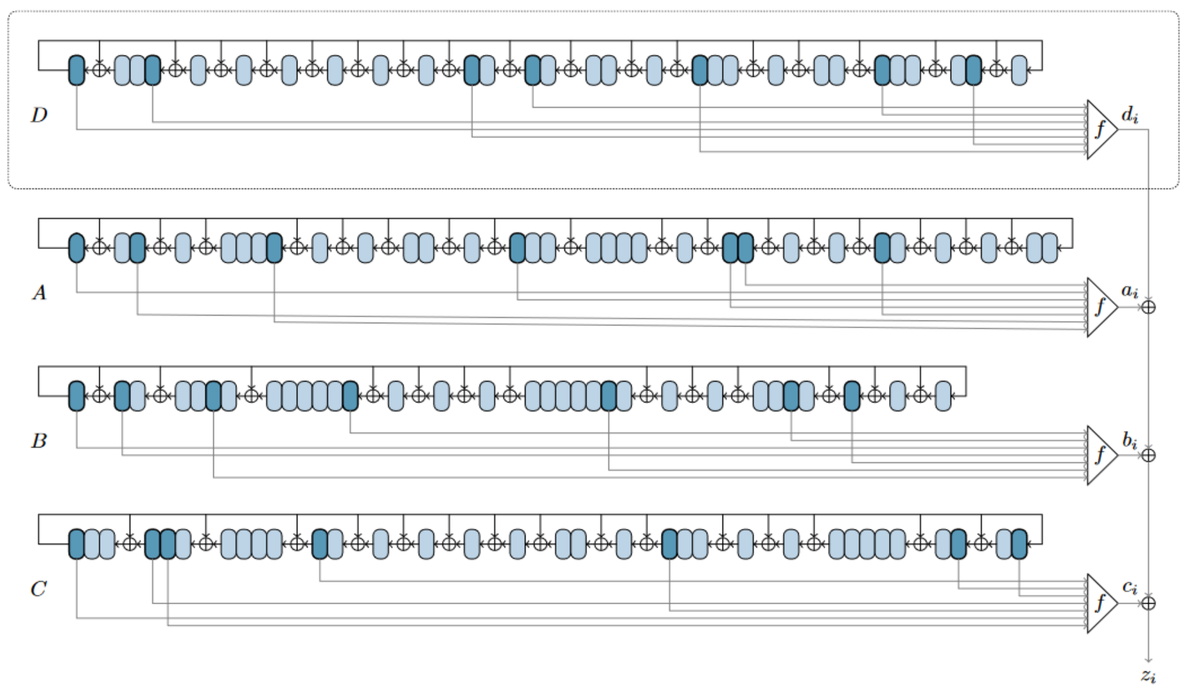
COORDINATEUR : Patrick DERBEZ

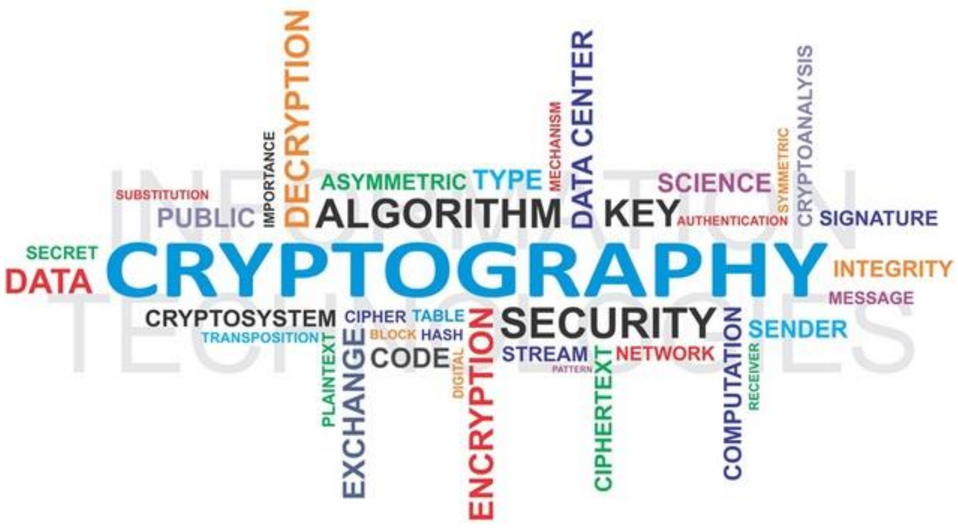
PARTENAIRE : Université Rennes 1

Objectif: Développer de nouvelles techniques de cryptanalyse ainsi qu'un ensemble d'outils open-sources dédiés à l'évaluation des primitives de la cryptographie symétrique.

Contexte

Les systèmes de chiffrement symétriques sont largement répandu car ils sont les seuls à proposer des fonctionnalités essentielles comme le chiffrement très rapide, le chiffrement à petit coût, l'authentification de messages en temps réel et le hachage efficace. Mais, contrairement aux algorithmes cryptographiques à clef publique, la sécurité de ces algorithmes est établie empiriquement par la non-découverte d'attaques ou faiblesses par les chercheurs en cryptographie.





Le Monde

Cryptologie : une curieuse faille sur les anciens téléphones mobiles

Une équipe internationale a démontré une faiblesse d'origine volontaire dans la sécurité de la transmission des données de téléphones 2G et 2.5G, utilisés essentiellement avant 2013. Des technologies encore ponctuellement employées.

Méthodologie

- Résoudre des problèmes algorithmiques
- Exploiter la structure des problèmes (ex: symétries) pour réduire l'espace de recherche
- Utiliser des solveurs MILP, CP et SAT

Résultats

- 9 papiers publiés dans les meilleurs journaux et conférences du domaine (dont 2 dans des conférences A*)
- 1 outil dédié à la recherche de distingueurs de type *integral*
- 1 outil dédié aux attaques Meet-In-The-Middle
- 1 outil pour attaquer les implémentations en boîte blanche de chiffrement similaire à AES
- Résolution d'un problème ouvert depuis 10 ans relatif à la conception des réseaux de Feistel
- Nouveaux algorithmes pour déterminer de bons algorithmes d'expansion de clés
- Correction d'une technique de cryptanalyse basée sur les *presque collisions*
- Attaques pratiques sur un candidat à la compétition lightweight du NIST
- Attaques pratiques sur les algorithmes GEA-1 et GEA-2 utilisés dans le protocole de télécommunication 2G+

Table 4: Overview of the phones and basebands supporting (●) GEA-X

Phone	Year	Baseband	GEA-1	GEA-2
Apple iPhone XR	2018	Intel XMM 7560	●	●
Apple iPhone 8	2017	Intel XMM 7480	●	●
Samsung Galaxy S9	2018	Samsung Exynos 9810	●	●
HMD Global Nokia 3.1	2018	Mediatek MT6750	●	●
Huawei P9 lite	2016	HiSilicon Kirin 650	●	●
OnePlus 6T	2018	Qualcomm Snapdragon 845	●	●

UNIVERSITÉ DE RENNES 1 — cnrs — UMR IRISA