







Analyse automatisée d'une bibliothèque crypographique

Détection de failles par canal auxiliaire par analyse statique et symbolique

Duzés Florian



1996: Paul C. Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems

Une mesure précise du temps requis par des opérations sur les clés secrètes permettrait à un attaquant de casser le cryptosystème.



1996: Paul C. Kocher, *Timing Attacks on Implementations of Diffie-Hellman. RSA. DSS. and Other Systems*

Une mesure précise du temps requis par des opérations sur les clés secrètes permettrait à un attaquant de casser le cryptosystème.

2003: Brumley et Boneh Remote Timing Attacks Are Practical



1996: Paul C. Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems

Une mesure précise du temps requis par des opérations sur les clés secrètes permettrait à un attaquant de casser le cryptosystème.

2003: Brumley et Boneh Remote Timing Attacks Are Practical

2011: Brumley et Tuveri Remote Timing Attacks are Still Practical

Innia -28/08/2025 2 / 15

HACL*

"High Assurance Cryptography Library" a est une bibliothèque cryptographique, écrite en F* ("F star"), implémentant tous les algorithmes de cryptographie modernes et est prouvée mathématiquement sûre.

HACL* est notamment utilisé dans plusieurs systèmes de production tels que Mozilla Firefox, le noyau Linux, le VPN WireGuard...

a. https://hacl-star.github.io/

28/08/2025 *Enría* Investit (1960) (28/08/2025 (1960) (28/08/200) (28/08) (28/08/200) (28/08/200) (28/08/200

- QR1 Est-il possible de propager les garanties de sécurité pendant la compilation?
- QR2 Est-il possible d'automatiser la détection de ces failles sur des fichiers compilés ?
- **QR3** Est-il possible d'appliquer ces mécanismes pour assurer la vérification d'une bibliothèque cryptographique?

28/08/2025 *(nría* whitesité heightein 4 / 15

Sommaire

- 1. Méthodes de protection et limitations
- 2. Outils de vérifications
- 3. Automatismes
- 4. Érysichthon
 - 1. Conception générale
 - 2. Andhrímnir





Usages de compilateurs spécialisés

- Constantine
- Raccoon
- CompCert
- Jasmine



Usages de compilateurs spécialisés

- Constantine
- Raccoon
- CompCert
- Jasmine

Information exterieur

- Entretien avec Maria Mishtaq
- Réunion Mercredi 2 juillet 15h30

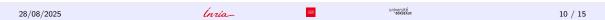
Bonnes pratiques de programmations



03 Outils de vérifications



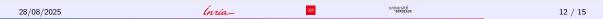




04 Automatismes







05 Érysichthon



