RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Inria

cea

université de BORDEAUX

Analyse automatisée d'une bibliothèque crypographique

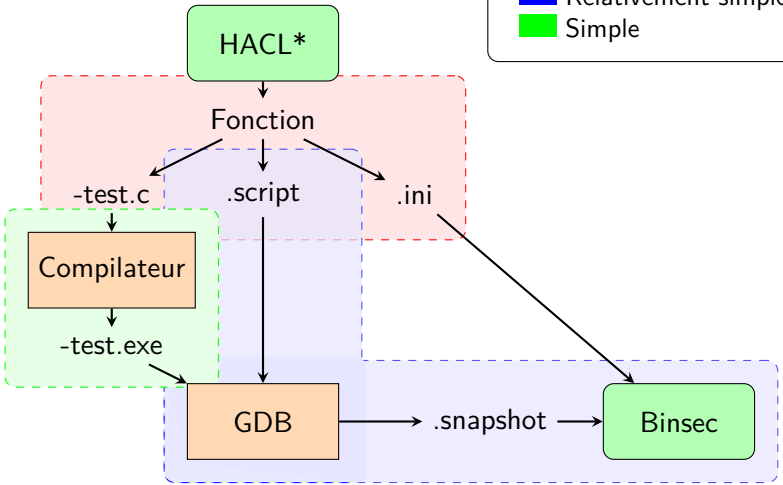
Détection de failles par canal auxiliaire par analyse statique et symbolique

Duzés Florian

Master Cryptologie et Sécurité Informatique

28 août 2025

Conception générale



Spécifications architecturales

graphes

Constructions en modules

graphes

Andhrímnir

Besoins

Conception générale

graphes

Premières passes

graphes

Analyses

graphes

Conclusion

Références

[Alm+13] José Bacelar Almeida et al. *Formal Verification of Side-Channel Countermeasures Using Self-Composition*. 2013.

[Ant+17] Thomas Antonopoulos et al. *Decomposition Instead of Self-Composition for Proving the Absence of Timing Channels*. 2017.

[Bar+14] Gilles Barthe et al. *System-level non-interference for constant-time cryptography*. 2014.

[Bar+16] Gilles Barthe et al. *Computer-Aided Verification for Mechanism Design*. 2016.

[BPT17] Sandrine Blazy, David Pichardie et André Trieu. *Verifying Constant-Time Implementations by Abstract Interpretation*. 2017.

[Bre+18] Thomas Brennan et al. *Symbolic Path Cost Analysis for Side-Channel Detection*. 2018.

[Cau+19] Srinath Cauligi et al. *FaCT : A DSL for timing-sensitive computation*. 2019.

[CFD17] Jie Chen, Yu Feng et Isil Dillig. *Precise detection of side-channel vulnerabilities using quantitative cartesian hoare logic*. 2017.

[DBR19] Lesly-Ann Daniel, Sébastien Bardin et Tamara Rezk. *Binsec/Rel : Efficient Relational Symbolic Execution for Constant-Time at Binary-Level*. 2019. arXiv : 1912.08788. URL : http://arxiv.org/abs/1912.08788.

[Dis20] Craig Disselkoen. *haybale-pitchfork*. https://github.com/PLSysSec/haybale-pitchfork