# Conception d'un meta-modèle (ontologie) d'architectures cryptographiques pour la vérification du respect des bonnes pratiques

Gurvan Le Guernic

29 janvier 2020

## 1 Sujet

L'utilisation correcte de la cryptographie est complexe (voir par exemple la présentation "Bad Cryptography" [6]). Une mauvaise utilisation aboutie à des failles de sécurité dans les systèmes. Afin de remédier à ce problème, des organismes nationaux et internationaux (NIST et ANSSI par exemple) publient des guides ou recommandations de bonnes pratiques de l'usage de la cryptographie [1] ; et des certifications spécifiques (FIPS-140/CMVP ou Common Criteria par exemple) vérifient l'usage correcte de la cryptographie dans certains produits. Cependant, pour de nombreux concepteurs de produits ou systèmes s'assurer qu'ils respectent les bonnes pratiques de l'usage de la cryptographie est une tâche complexe. Le but du projet IDM4AC est d'aboutir à la spécification du coeur (structure de données et algorithmes principaux) d'un outil d'Ingénierie Dirigée par les Modèles (IDM) pour valider l'application des recommandations de bon usage de la cryptographie lors de la conception de produits ou de systèmes de sécurité.

Il n'est pas question ici d'étudier des implémentation ou spécification d'algorithmes cryptographiques, mais de participer à la conception d'un outil facilitant la validation du respect des recommandations et bonnes pratiques (exprimées dans des documents publiques) concernant l'*usage* de mécanismes cryptographiques, et ce potentiellement dés la phase de conception alors qu'aucune implémentation n'existe. Ce type de validation se rapproche (sans être identique) de ce qui est fait à partir des documents de type "FIPS 140-2 Security Policy" qui sont à fournir pour des certifications CMVP (`https://www.google.com/search?q=FIPS+140-2+Security+Policy`).

Le projet de stage proposé consiste à (potentiellement partiellement en parallèle) :

1. Analyser des documents publiés par des organismes nationaux et internationaux (NIST principalement) décrivant des réglementations et bonnes pratiques concernant l'utilisation de la cryptographie (certains documents sont identifiés, mais la base documentaire pourrait être élargie) pour en extraire les règles vérifiables et les informations sur lesquelles se baseraient ces vérifications ;
2. Concevoir un meta-modèle (ontologie) embarquant les informations nécessaires à la vérification d'un sous-ensemble significatif des règles identifiées dans le point 1 ;
3. Formaliser ce meta-modèle (point 2) et les propriétés extraites (point 1) à l'aide de l'outil USE [2] (ou tout autre outils proposé par le stagiaire et validé par l'encadrement) ;
4. Valider, toujours à l'aide de l'outil USE ou équivalent, le travail de formalisation (point 4) via la modélisation d'architecture cryptographique de différents systèmes tels que : AWS [2, 3], WanaCry [1], SanSec's HSM [4].

Ce projet (qui pourra être "ingrat" par moments) requière :
— la volonté d'effectuer un important travail bibliographique (lire beaucoup et en anglais) ;
— ainsi que de bonnes capacités d'abstraction et de conceptualisation.

1. Le document NIST SP 800-175B [5] est un bon point de départ pour se familiariser avec ce type de recommandations.
2. `http://useocl.sourceforge.net/w/index.php/Main_Page`

## 2 Encadrement

Ce stage sera réalisé au sein de l'équipe DiverSE (`https://www.diverse-team.fr/`) de l'IRISA (`https://www.irisa.fr/`, unité mixte de recherche impliquant le CNRS, l'Université de Rennes 1, Inria et l'INSA Rennes) à Rennes (Bretagne).

Le stage sera encadré par :

**Gurvan LE GUERNIC** (Ph.D. Kansas State University et Université de Rennes 1)
- Expert technique de DGA MI [3]
- Collaborateur extérieur de l'équipe DiverSE
- Membre du Conseil Scientifique de l'Accord Général de Partenariat (AGP) associé au Pôle d'Excellence Cyber (`https://www.pole-excellence-cyber.org/`)
- `Gurvan.Le_Guernic@inria.fr`

**Olivier BARAIS** (Ph.D. Université de Lille)
- Professeur de l'Université de Rennes 1
- `http://olivier.barais.fr/`

## Références

[1] Maxat Akbanov, Vassilios G. Vassilakis, and Michael D. Logothetis. WannaCry Ransomware : Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms. *Journal of Telecommunications and Information Technology*, January 2019. `https://doi.org/10.26636/jtit.2019.130218`.

[2] Amazon. AWS Key Management Service : Cryptographic Details. Technical report, Amazon Web Services, Inc., August 2018. `https://d0.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf`.

[3] Amazon. AWS Key Management Service HSM. FIPS 140-2 Non-Proprietary Security Policy, Amazon Web Services, Inc., September 2018. `https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3139.pdf`.

[4] atsec information security corporation. Sansec HSM Cryptographic Module version SecHSM-V2. FIPS 140-2 Non-Proprietary Security Policy, Beijing Sansec Technology Development Co., December 2018. Version 1.2. `https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3350.pdf`.

[5] Elaine Barker. Guideline for Using Cryptographic Standards in the Federal Government : Cryptographic Mechanisms. NIST Special Publication 800-175B, National Institute of Standards and Technology, August 2016. `http://dx.doi.org/10.6028/NIST.SP.800-175B`.

[6] Bruce Barnett. Bad Cryptography. Talk at the Annual New York State Cyber Security Conference, June 2015. `https://its.ny.gov/sites/default/files/documents/2bruce_barnett.pptx.pdf`.

3. `https://www.defense.gouv.fr/dga/la-dga2/expertise-et-essais/les-centres-d-expertise-et-d-essais-de-la-dga/dga-maitrise-de-l-information`