# Analyse d'applets JavaCard et réalisation d'automates

Romain Barrat
Simon Garrelou
Clément Jarrige
Marwen Sami

Encadrant : Jean-Louis Lanet

11 octobre 2016

## Introduction

JavaCard est une technologie permettant de faire tourner des applets Java sur des *smartcards*, des cartes à puce (comme par exemple des cartes bancaires ou des cartes SIM). Le but premier de JavaCard est la sécurité : il est très simple d'utiliser des algorithmes de chiffrement comme AES, Triple DES ou encore RSA.

Les applets JavaCard développés pour des *smartcards* sont un exemple concret du besoin de sécurité dans des projets informatiques. En effet, un applet mal sécurisé peut potentiellement être utilisé à des fins non prévues par le programmeur, ce qui peut avoir des effets néfastes, par exemple dans le cas d'un système de paiement. Notre projet a pour but de générer un automate représentant un applet JavaCard de manière automatique, pour ensuite le comparer à un automate de référence. Il sera donc possible de savoir les actions qui font passer un applet d'un état à un autre et de remarquer simplement les changements d'état non prévus.

## 1 État de l'art

### 1.1 JDart

JDart [1] est une bibliothèque Java permettant de faire de l'*exécution concolique*. Plus clairement, JDart est capable de détecter les valeurs de variables qui feront passer un programme dans des branchements différents. Cet outil est une extension de Java Pathfinder, un environnement développé par la NASA crée pour vérifier le bytecode de programmes Java.

1. `https://github.com/psycopaths/jdart`

### 1.2

## 2 Travail à réaliser

— Améliorer l'outil JaCaCoCo développé en Licence 3 pour lui permettre de générer un fichier XML comportant les entrées concrètes utilisées lors des tests.
— Corriger certains bugs dans JDart
— Créer un programme annotant automatiquement un code source Java afin que celui-ci soit utilisable avec JDart.
— Récupérer la sortie de JDart pour générer un automate sous forme graphique.
— Pouvoir comparer l'automate généré avec un automate de référence.