CentraleSupélec

2e année
F. Popineau

2016 – 2017

# Sujet de projet de développement logiciel

## Cryptographie et arbres de Merkle

Les arbres de Merkle sont utilisés pour authentifier des transactions dans systèmes aussi divers que ceux des Bitcoin ou de Git.

L'objet de votre projet consistera à mettre en oeuvre un schéma de signature de données utilisant un arbre de Merkle. Votre document de référence sera celui-ci : Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis - 2008 - Becker

Vous commencerez par implanter un schéma de signature de Lamport pour signer à la demande un document. Ensuite, vous implanterez un schéma de signature basé sur un arbre de Merkle. Un système de signature à la demande requiert une clé publique longue et complexe à transmettre à chaque signature. Les arbres de Merkel ont pour propriété de permettre d'économiser le nombre de clés publiques nécessaires.

Votre démonstrateur comprendra un client et un serveur qui mettront en oeuvre la signature et la transmission de la donnée. Le client devra vérifier que la donnée est correctement signée.