2019-10565 Implémentation de primitives pour la cryptographie sur courbes elliptiques définies sur GF(p)

Informations générales

Statut	Diffusée
Entité de rattachement	SSSEC
Description de l'unité	Le Leti, institut de recherche technologique de Cea Tech, a pour mission d'innover et de transférer les innovations à l'industrie. Son cœur de métier réside dans les technologies de la microélectronique, de miniaturisation des composants, d'intégration système, et d'architecture de circuits intégrés, à la base de l'internet des objets, de l'intelligence artificielle, de la réalité augmentée, de la santé connectée. Le Leti façonne des solutions différenciantes, sécurisées et fiables visant à augmenter la compétitivité de ses partenaires industriels par l'innovation technologique. L'institut est localisé à Grenoble avec deux bureaux aux USA et au Japon, et compte 1800 chercheurs.
Délai de traitement	2 mois

Description du poste

Site	Grenoble
Pays	France
Lieu	17 avenue des martyrs 38000 Grenoble
Possibilité de poursuite en thèse	Oui
Domaine	Technologies micro et nano
Contrat	Stage
Intitulé de l'offre	Implémentation de primitives pour la cryptographie sur courbes elliptiques définies sur GF(p)
Sujet de stage	Implémentation de primitives pour la cryptographie sur courbes elliptiques définies sur GF(p)
Durée du contrat (en mois)	6
Description de l'offre	Le LSOSP, Laboratoire sécurité des objets et des systèmes physiques, mène des activités de R&D dans le domaine des technologies de sécurité et de protection de la vie privée. Il analyse et caractérise les risques auxquels sont soumis les systèmes électroniques et les composants; il conçoit des contre-mesures s'appuyant notamment sur des techniques cryptographiques mais aussi sur des modifications dans l'architecture des systèmes pour intégrer les technologies nécessaires (composants, codes embarqués, interfaces ou protocoles de communications...). Il caractérise l'efficacité des contremesures intégrées dans des composants, des objets (communicants) et des systèmes cyberphysiques afin de résister aux attaques au niveau de leur structure, de leurs fonctions ou de leur utilisation. La cryptographie sur courbes elliptiques est largement déployée dans l'industrie. Malgré tout, en faire une implémentation logicielle efficace et optimisée est un challenge. Ceci est dû aux différents paramètres d'entrée et au choix adéquate d'algorithmes. Ces paramètres sont la taille des données d'entrées, le modèle de courbes elliptiques et l'architecture sur laquelle est faite l'implémentation. L'objectif de ce stage est d'implémenter les différentes primitives nécessaires pour construire la cryptographie sur courbes elliptiques (ECC). Nous nous concentrerons sur les courbes définies sur les corps finis en grandes caractéristiques. De plus nous nous appuierons sur les standards FIPS 186-4 et RFC 7748. L'une des clefs d'une implémentation performante des ECC est l'opération de multiplication de multiprécision d'éléments de GF(p). Le stagiaire devrait faire un état de l'art des différents algorithmes de multiplication des grands nombres et en faire une implémentation. Un travail de caractérisation des performances des différents algorithmes implémentés devrait être fait par la suite. Des mesures détaillées devront être faites en fonction de l'architecture, de la taille des nombres à multiplier et des méthodes de multiplications. Des contraintes fortes de sécurité physiques devront être suivies : implémentation en temps constant, aucune « fausse instruction », éviter au maximum les déplacements des données, utiliser des adresses mémoires fixes, un espace mémoire statique...

	Par la suite, cette étude de performance servira à sélectionner le meilleur algorithme de multiplication pour différents cas d'usage correspondant à différentes tailles de courbes elliptiques et différentes architectures. Si le temps le permet la même étude peut être menée sur différents algorithmes lourd en calcul : la réduction modulaire et l'inversion. La finalité du stage est d'ajouter ces différentes implémentations à la bibliothèque cryptographique sur les courbes elliptiques du laboratoire. Dans le but d'obtenir une cryptographie sur courbes elliptiques efficaces.
Profil du candidat	Une bonne connaissance de la cryptographie sur courbes elliptiques est requise.

Critères candidat

Diplôme préparé	Bac+5 - Master 2
Formation recommandée	Cryptographie
Possibilité de poursuite en thèse	Oui

Programme

Segment CEA	Technologies de l'information

Demandeur

Direction du Demandeur	DRT
Nom Manager	Fournier
Prénom Manager	Jacques
E-mail Manager	jacques.fournier@cea.fr
E-mail du tuteur / Responsable	antoine.loiseau@cea.fr
Disponibilité du poste	01/02/2020

Suivi RH

Suivie par	Antoine LOISEAU
Alertes email	Toutes les candidatures
Récepteurs des alertes	Antoine LOISEAU
Date de mise à jour automatique	Non