

Proposition de stage de M2R Recherche

Laboratoire : IRISA – équipe CAIRN (Lannion)

Titre : *opérateurs arithmétiques pour cryptoprocasseur ECC résistant aux attaques en faute*

Mots clés : arithmétique des ordinateurs, cryptographie sur courbe elliptique, attaque par injection de faute, attaque par perturbation, contre-mesure matérielle, sécurité numérique, algorithme arithmétique, système de représentation des nombres, implantation FPGA

Contact : Arnaud Tisserand (arnaud.tisserand@irisa.fr) et Stanislaw Piestrak (stanislaw.piestrak@irisa.fr)

Description du projet

La sécurisation de cryptoprocasseurs vis à vis d'attaques par observation (mesure de la consommation d'énergie, du temps d'exécution ou du rayonnement électromagnétique) ou bien d'attaques par perturbation (ou attaques par injection de faute), est un enjeu important pour bon nombre d'applications en sécurité numérique. En effet, même si un protocole cryptographique est considéré comme mathématiquement robuste, son implantation dans un cryptoprocasseur risque d'être attaquée physiquement si on ne prend pas de précaution ou sans intégration de dispositifs de protection appelés contre-mesures.

Les attaques par injection de faute représentent un risque particulier pour des applications embarquées (genre carte à puces ou dispositifs portables). Un attaquant peut assez facilement faire varier des paramètres de l'environnement du circuit afin de provoquer des fautes internes qui conduiront potentiellement à des informations sur les valeurs secrètes manipulées par le circuit (comme des bouts des clés secrètes ou bien des messages en clair). Des variations ou injections de pics de courant sur les alimentations, variations sur les signaux d'horloge du circuit, variations de la température ou un bombardement laser ou rayon X, par exemple, peuvent provoquer des fautes internes (collage ou inversion de bit(s), forçage de test, ...). Il existe aujourd'hui toute une batterie d'attaques permettant de « remonter » à des informations sensibles à partir de quelques fautes.

Dans la cryptographie sur les courbes elliptiques (ECC), l'arithmétique joue un rôle important dans la mise en place de cryptosystèmes à la fois efficaces et sûrs. En particulier, l'arithmétique des corps finis doit être très rapide étant donnée la quantité de calculs effectués en nécessitant des ressources limitées (surface de circuit, taille mémoire, consommation d'énergie) mais aussi tout en offrant un bon niveau de robustesse vis à vis des attaques physiques. Les types de calculs nécessaires sont des additions, multiplications (de deux variables ou d'une variable par une ou des constantes), divisions, inversions et exponentiations. Ces opérations, qui peuvent paraître assez simples sur des petits entiers ou approximation de nombres réels, sont assez complexes sur des corps finis ($GF(p)$ ou $GF(2^m)$) avec des tailles de nombres de quelques centaines de bits (160 à 600 bits pour ECC).

Afin de proposer des opérateurs arithmétiques efficaces pour de telles tailles, il faut non seulement travailler sur l'algorithmique et la représentation des nombres, mais aussi sur les détails d'implantation (les constantes cachées dans les analyses classiques de complexité). Dans notre travail, nous ajoutons à ces contraintes celle de la robustesse vis à vis de certaines attaques physiques par injection de faute. C'est à dire que les opérateurs arithmétiques permettront de déterminer (directement ou par quelques calculs supplémentaires) si une faute à été injectée ou pas lors d'un calcul.

Objectifs généraux du stage et résultats attendus

L'objectif de ce stage de M2R est d'étudier, comparer, implanter sur FPGA des opérateurs arithmétiques pour ECC robustes d'un point de vue de la sécurité contre les attaques par perturbation. Il s'agira d'étudier les liens entre les algorithmes et les représentations des nombres en prenant en compte non seulement les performances classiques (vitesse, débit et surface de silicium) mais aussi la consommation d'énergie et la sécurité vis à vis de certaines attaques en faute. Une phase de bibliographie sur les attaques et les contre-mesures classiques permettra de fixer les limites de l'étude (type d'attaques à prendre en compte et estimation de la robustesse d'une portion de circuit). Ensuite, le travail portera sur l'étude et la mise en œuvre sur circuits FPGA d'opérateurs arithmétiques résistants aux attaques par perturbation fixées. Différentes méthodes de protection comme les techniques de redondance par duplication, codes de parité et des autres techniques de codage pourront être comparées. En particulier, nous pensons qu'il est possible d'intégrer efficacement des techniques issues du domaine des codes détecteurs et/ou correcteurs d'erreurs au plus bas niveau lors des calculs pour éviter le coût important de la duplication ou même triplification. Le taux de couverture de fautes atteignable sera fonction de nombreux paramètres. Il s'agira d'étudier les compromis possibles entre robustesse, performance en vitesse et le coût du cryptosystème (surface de silicium et/ou consommation d'énergie). Les résultats attendus sont une description théorique et un prototype pratique sur circuits FPGA d'opérateurs robustes. Une évaluation de leur robustesse sera proposée.

Remarques : Une indemnité de stage sera possible au tarif fixé par l'IRISA. Une poursuite en thèse dans notre équipe sur ce thème pourra être envisagée selon les résultats obtenus et les possibilités d'allocation.

Liens : <http://www.irisa.fr/cairn>

Références bibliographiques

- [1] D. Hankerson, A. Menezes, S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag
- [2] J.-P. Deschamps, J. L. Imana, G. D. Sutter. *Hardware Implementations of Finite-Field Arithmetic*. Mc Graw Hill
- [3] F. Koeune, F.-X. Standaert. *A Tutorial on Physical Security and Side-Channel Attacks*. 5th International School on Foundations of Security Analysis and Design FOSAD, pp 78-108, LNCS vol 3655. 2005
- [4] C. H. Kim, S. Kwon, C. P. Hong. *FPGA implementation of high performance elliptic curve cryptographic processor over $GF(2^{163})$* . Journal of Systems Architecture, vol. 54, n. 10, pp 893-900, 2009
- [5] S. Ghosh, M. Alam, D. R. Chowdhury, I. S. Gupta, *Parallel crypto-devices for $GF(p)$ elliptic curve multiplication resistant against side channel attacks*, Computers & Electrical Engineering, vol. 35, n. 2, pp 329-338, 2009
- [6] K. Markantonakis, M. Tunstall, G. Hancke, I. Askoxylakis, K. Mayes, *Attacking smart card systems: Theory and practice*, Information Security Technical Report, vol. 14, n. 2, pp 46-56, 2009