Injection de faute sur RSA-CRT

Kévin Boyeldieu
Titouan Tanguy
TLS-SEC

Mars 2018

Procédure d'installation

Pour mettre en place le challenge, il faut avoir une carte FPGA Xilinx Nexys2, ainsi qu'un ordinateur sous Linux avec un port COM et un câble permettant la liaison entre notre FPGA et le port COM de l'ordinateur.
En premier lieu il faut programmer la carte FPGA avec *nexys2_rsa_crt.bit*. Le plus simple pour ce faire est de connecter le port micro-usb de la carte à un port USB de l'ordinateur et d'utiliser la commande :

```
djtgcfg -d Nexys2 prog -i 0 -f nexys2_rsa_crt.bit
```

Dans le cas où l'on voudrait que le programme reste sur la carte après avoir éteint cette dernière il faut utiliser le fichier *nexys2_rsa_crt.mcs* et la commande suivante :

```
djtgcfg -d Nexys2 prog -i 1 -f nexys2_rsa_crt.mcs
```

Ces deux commandes nécessitent l'installation de Digilent Adept software.

Une fois la carte prête, la **LED J14** devrait s'allumer. Il ne suffit plus alors qu'à lancer le programme python *uart_receiver.py* sur la machine Linux (cela peut nécessiter les droits administrateurs). Ce programme permet de récupérer les signatures calculées et envoyées par la carte.
Pour le reste du tutoriel, à savoir le calcul de la différence et du $PGCD$ nous ne fournissons pas de sources, mais une console python par exemple fonctionnera très bien. L'utilisateur donnera sa réponse en exécutant le programme *chall.py* se trouvant dans *src/rsa_crt*.