Promo SCCI 2010

Vanessa Terrade

Université Joseph Fourier

September 12, 2011

Parcours universitaire

- 2008 - Lincence SENA - UJF Valence
- 2009 - Master 1 Informatique - UJF Grenoble
- 2010 - Master SCCI - UJF Grenoble

- Verimag
- Pascal Lafourcade
- Implémentation et vérification de protocoles de paiement en ligne
  - SET
  - 3D Secure
- Etude de propriétés de vente aux enchères en ligne en pi-calcul
- Comparison of Cryptographic Verification Tools Dealing with Algebraic Properties *Pascal Lafourcade, Vanessa Terrade and Sylvain Vigier*

- Ingenico Valence
- 6 mois
- Mise en oeuvre d'un générateur de nombres aléatoires

Utilisé

- dans la création des clés de chiffrement 3DES
- pour la proctection contre les attaques DPA

Aprés le diplome...

De novembre 2010 à décembre 2010 :

- Philippe Elbaz-Vincent
- Implémentation et test de générateurs de nombres aléatoires :
  - le générateur du viaC7
  - Quantis
  - basé sur la suite de Fibonacci
  - basé sur le théorème des restes chinois

Aprés le diplome...

De janvier 2011 à juillet 2011 :

- Philippe Elbaz-Vincent
- Projet SHIVA
- Librairie MpHell
- Post-Processing sur les générateurs de nombres aléatoires

- Comparaison des performances
  - sur différentes machines
  - avec Miracl
  - sur l'arithmétique de base et l'arithmétique des courbes
- Réduction du NIST
- Courbes de Weierstrass :
  - Génération de courbes pseudo-aléatoires
  - Addition de points
- Multiplication rapide
  - Multiplication naïve intelligente
  - Karastuba

Et maintenant ?

Questions ?