QC-SYND : Implémentation d'un cryptosystème sur FPGA

Mickaël Dardaillon, Philippe Gaborit, Cédric Lauradoux et Tanguy Risset
Laboratoire CITI, INSA Lyon, XLIM, Université de Limoges, INRIA
Journées SEmba 2011

Problématique

Utilisation de la cryptographie basée sur les codes :

- Grande vitesse d'exécution.
- Non adapté à l'embarqué.
- Solution : QC-SYND.

QC-SYND :

- Matrice quasi-cyclique pour réduire l'empreinte matérielle.
- Implémentation par décalage circulaire toute taille.
- Évaluation sur une plateforme matérielle embarquée.

Pré-requis : SYND

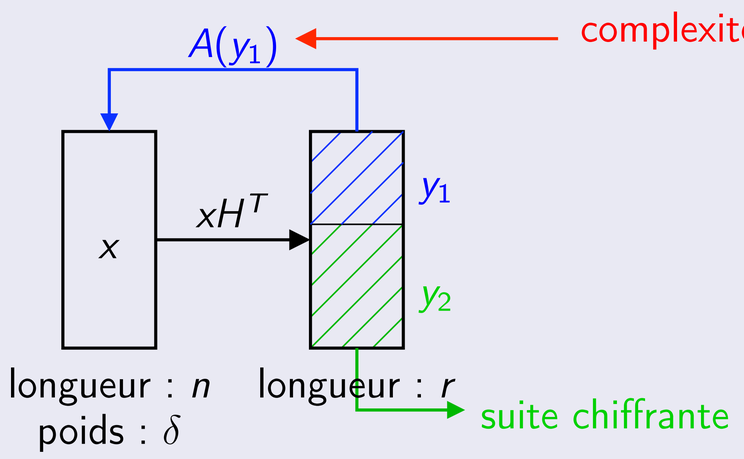
Problème du *syndrome decoding* :

Supposant une matrice binaire H de taille $r \times n$, un syndrome binaire S de longueur r et un entier w, ce problème consiste à trouver une erreur e de poids $\leq w$ tel que :

$$He = S$$

Problème difficile de théorie des codes :
Fischer et Stern, 1996 ; SYND, 2007

Fischer et Stern, ancêtre de SYND :



Apports de SYND :

Mot régulier : Utilisé à la place de la fonction $A()$.
Mot découpé en δ blocs, dont chacun définit la position d'un poids de Hamming.

$$x = (\underbrace{x_0, \cdots, x_\ell}_{i_0}, \cdots, \underbrace{x_{n-\ell}, \cdots, x_{n-1}}_{i_{(n/\delta)-1}})$$

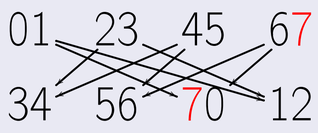
Matrice Quasi-Cyclique : Réduction empreinte mémoire.
Une colonne décrit toute la matrice (décalage circulaire successif).

$$\begin{bmatrix} h_0 & h_1 & h_2 \dots \\ h_1 & h_2 & h_3 \dots \\ \vdots & \vdots & \vdots \dots \\ h_{n-2} & h_{n-1} & h_0 \dots \\ h_{n-1} & h_0 & h_1 \dots \end{bmatrix}$$

Contribution : Décalage circulaire par blocs

La méthode classique possède deux contraintes :

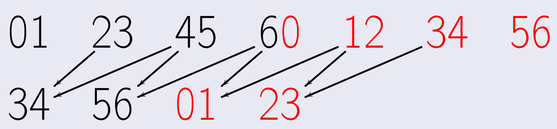
- $bloc_{sortie} = rol(bloc_{entrée\ 1}, bloc_{entrée\ 2}, shift)$
- Taille des données 2^x



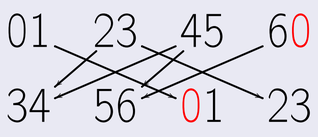
La taille de la colonne est contrainte pour des raisons de sécurité. Elle doit être égale à un nombre premier r et 2 doit être une racine primitive de $\mathbb{Z}/r\mathbb{Z}$ (par exemple $r = 509$ ou $r = 1019$).

La méthode classique n'est pas adaptée à ce problème (la donnée 7 supprimée vient s'immiscer dans le résultat). Nous proposons deux nouvelles méthodes :

- Méthode 1 : Agrandissement de la mémoire.



- Méthode 2 : Nouvelle gestion de l'adressage.



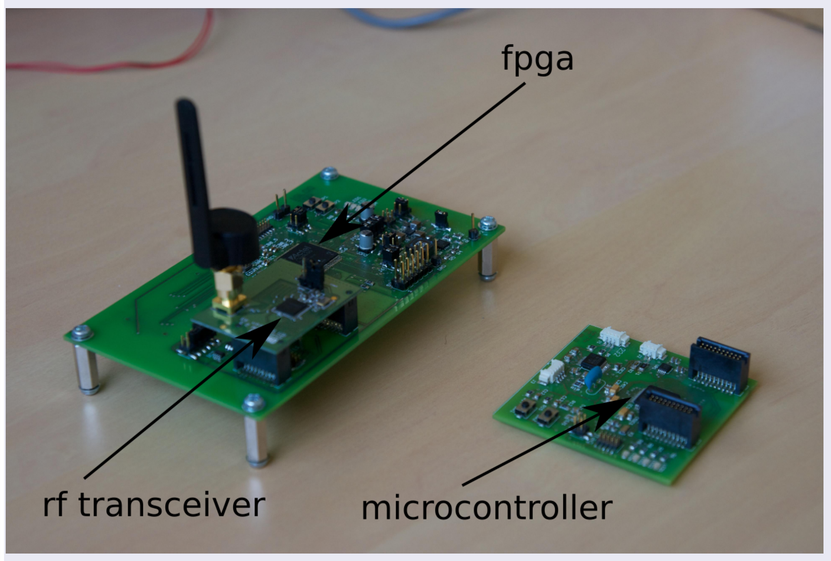
Contribution : Architecture matérielle

Architecture multicycle avec shifter partagé.

Une architecture alternative utilisant un double shifter est aussi évaluée.

Plateforme d'évaluation

PowWow.



FPGA Actel Igloo

RF transceiver TI CC2420

Microcontrôleur TI MSP430

Plateforme matérielle pour les réseaux de capteurs conçue par l'équipe INRIA CAIRN.
Développement d'un protocole d'authentification sur le FPGA.
Démonstrateur s'authentifiant à un noeud Senslab.

Résultats expérimentaux

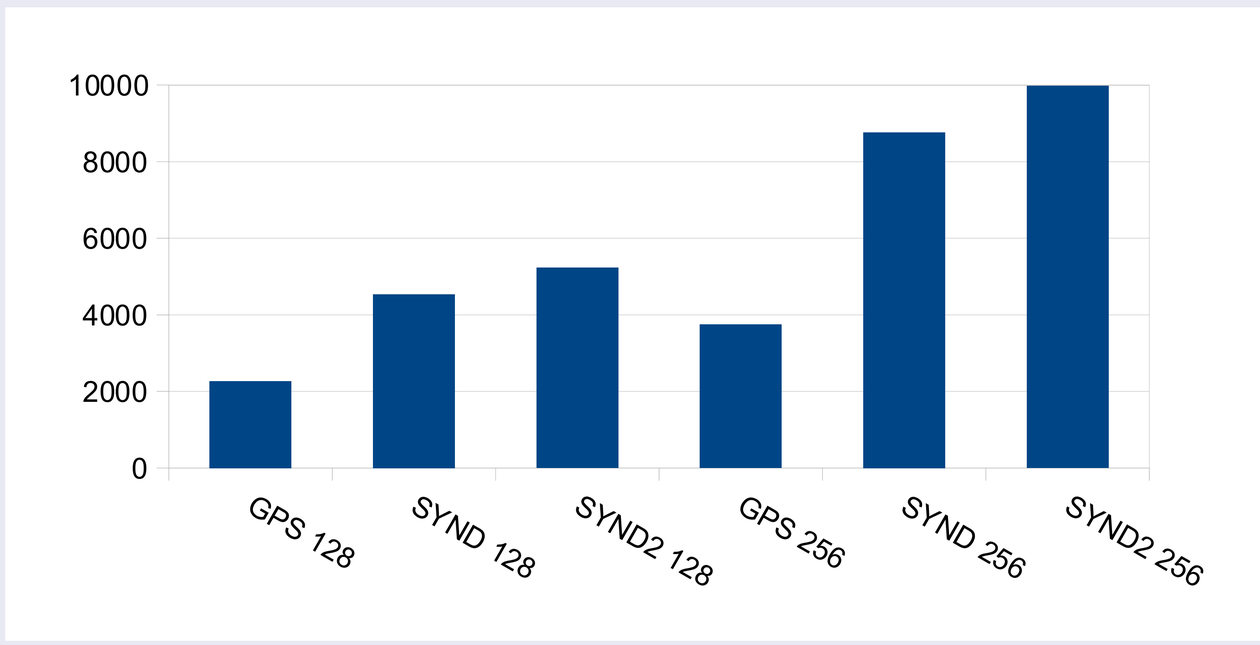
Coût du décalage circulaire par blocs.

Gain sur l'empreinte matérielle 13% avec le nouvel adressage.
Choix à réaliser en fonction du ratio coût mémoire/calcul.

Évaluation de l'empreinte matérielle.

GPS ≈ QC-SYND

QC-SYND est un crypto-système basé sur les codes adapté à l'embarqué.



Cellules logiques utilisées en fonction de l'architecture.

- SYND : shifter partagé
- SYND2 : double shifter