Masterproef industriële ingenieurswetenschappen

Cryptografische blokken genereren in Lava

Nicky Hannosset

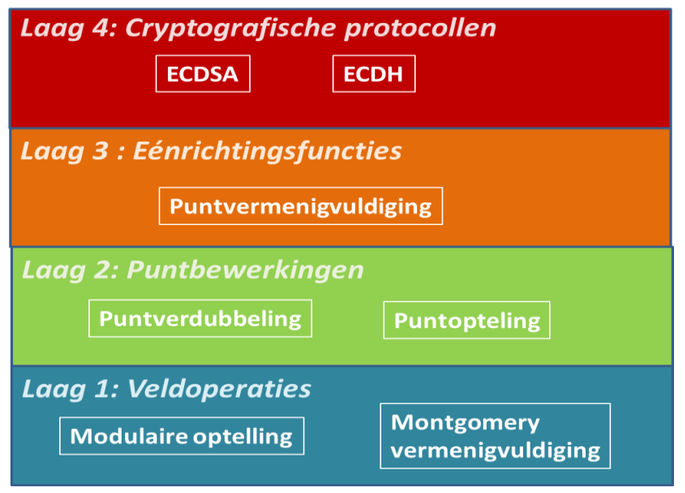
Academiejaar: 2013-2014

Introductie

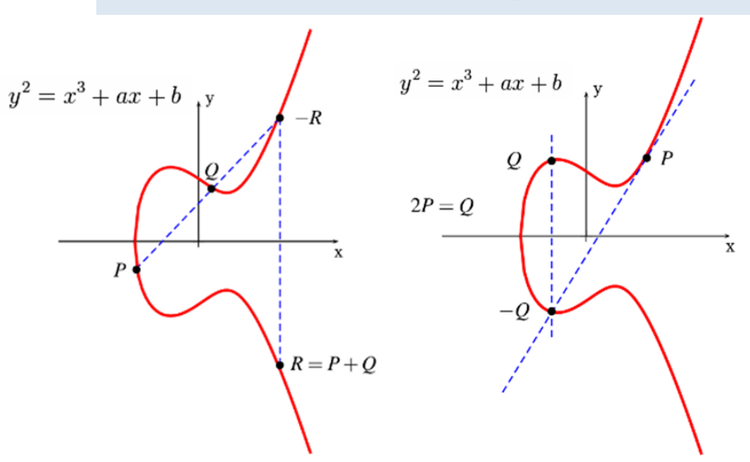
- De onderzoeksgroep ES&S (**E**mbedded **S**ystems and **S**ecurity) werkt aan een tool om cryptografische hardware automatisch te genereren.
- Kenmerken van EDA-DSE (Electronic Design Automation – Design Space Exploration) tool zijn:
  - Declaratieve beschrijving van zeer complexe Finite State Machine.
    = een model waarin een programma of sequentieel circuit wordt beschreven in verschillende fases.
  - Exploratie van verschillende hardware-mogelijkheden
  - Gebruikte programmeertalen: Lava en VHDL.

Doelstelling

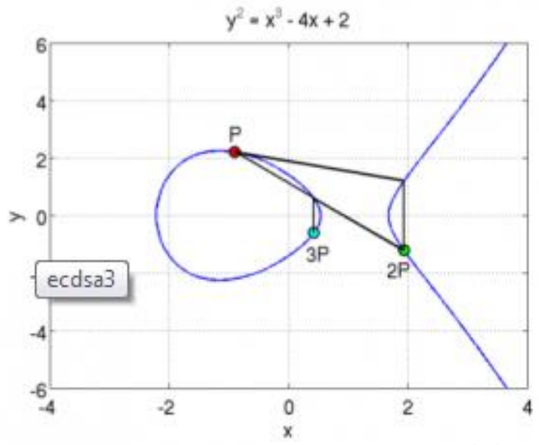
- Automatisch gegenereerde beveiliging bij communicatie tussen ≠ partijen.
- Generatie van cryptografische blokken volgens het ECC-algoritme (**E**lliptical **C**urve **C**ryptography).
- Implementatie van de puntbewerkingen van de 2e en 3e laag van het ECC. *(Zie figuur 1)*
- Na deze MP kunnen deze bewerkingen gebruikt worden in de cryptografische protocollen van laag 4.



Figuur 1: ECC algoritme



Figuur 2: Puntverdubbeling en -optelling



Figuur 3: Puntvermenigvuldiging

Plan van aanpak

1. Bestuderen van documentatie en code rond York Lava, de EDA-DSE -tool en het ECC-algoritme.
2. Werking van de bestaande tool beter begrijpen en documenteren d.m.v. uitvoeren van testen.
3. Integratie van puntverdubbeling en puntoptelling (2e laag). *(Zie figuur 2)*
4. Integratie van puntvermenigvuldiging (3e laag) in EDA-DSE. *(Zie figuur 3)*
5. Simulatie en testen in Lava en VHDL.

Resultaat

- Montgomery van 1e laag en puntverdubbeling van 2e laag aangepast omwille van fouten bij testen.
- Puntoptelling en –vermenigvuldiging geïmplementeerd.
- Testen geven het te verwachten resultaat.
- Getallen met grotere aantal bits (vb. 256 bits) geven nog errors.
- VHDL conversie werkt nog niet. (Lava kan bepaalde structuren niet omzetten)

Conclusie

De tool biedt voldoende kansen om uitbreidingen toe te voegen, maar kent een steile leercurve. Grootste nadeel van de huidige aanpak is dat het debuggen moeilijk verloopt en dat het zwaar is om inzicht te krijgen hoe de VHDL gegenereerd wordt, waardoor dat probleem niet opgelost kon worden.

De simulatie toont wel aan dat de 2e en 3e laag correct geïmplementeerd zijn. Tegelijk is de kwaliteit van de documentatie verhoogd zodat men in vervolgprojecten gemakkelijker en sneller kan voortbouwen op de resultaten.

Promotoren / Copromotoren: Prof. Dr. Kris Aerts, Prof. Dr. Ir. Nele Mentens

KU LEUVEN | universiteit hasselt