Masterproef industriële ingenieurswetenschappen

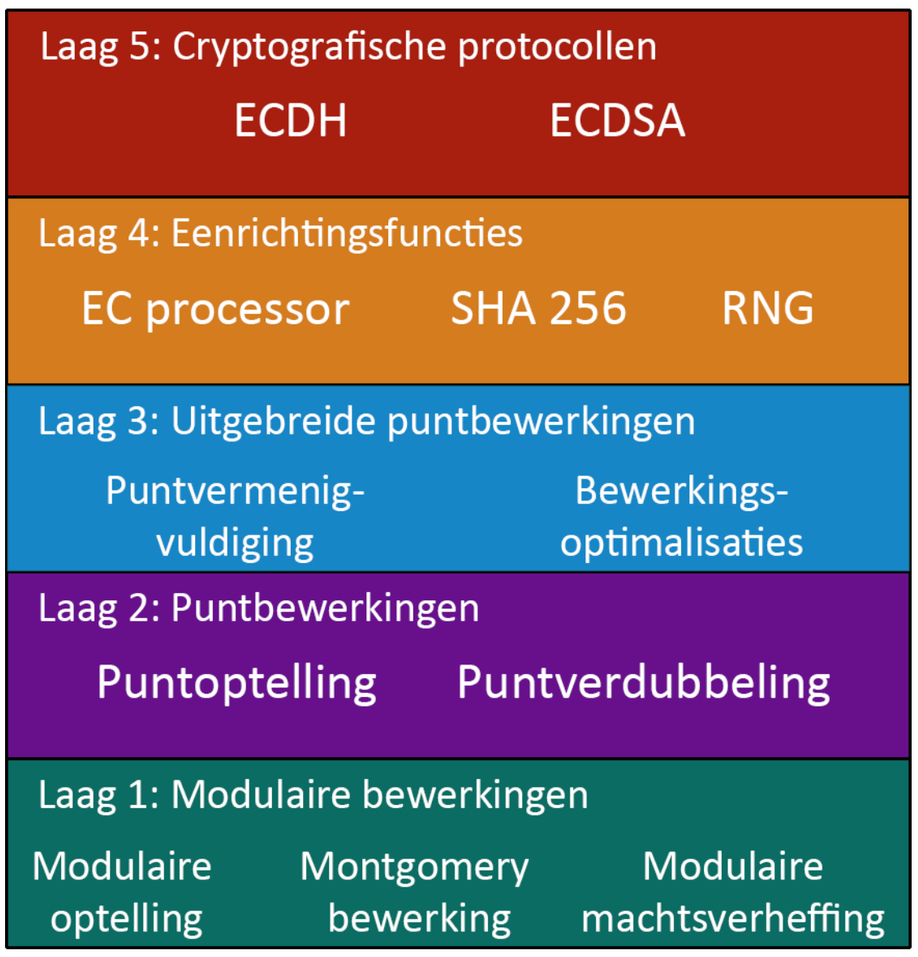
Een bibliotheek van cryptografische operaties met Lava

Bartel Sielski

Academiejaar: 2014-2015

Probleemstelling:

Goede cryptografie ontwikkelen is complex en tijdrovend.
Om kwaliteit te garanderen werd de implementatie van cryptografische hardware vereenvoudigd.



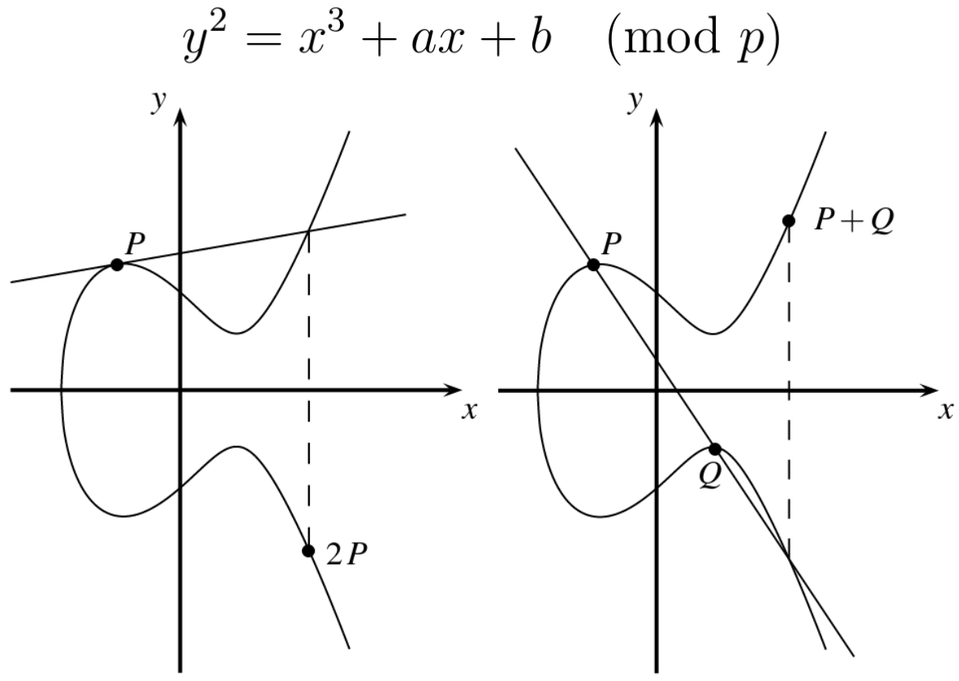
Figuur 2: opbouw van de ECDH/ECDSA module

Eindresultaat:

Werkende EDCH/ECDSA module

Moet nog uitgebreid worden met:

- Random nummer generator (RNG)
- Omzetting naar VHDL
- Bescherming tegen *side-channel attacks*



Figuur 1: EC puntoptelling en -verdubbeling

Doelstelling:

Bibliotheek ontwikkelen en toegankelijk stellen, met focus op Elliptische Kromme Cryptografie (of ECC).
Garandeert dezelfde veiligheid als andere algoritmes met kortere sleutels (zie tabel 1).

Manier van werken:

- Gebruik maken van York Lava en EDA-DSE tool van ES&S.
- Verder bouwen op bestaande modulaire bewerkingen en de bewerkingsoptimalisaties.

Algoritme familie	Cryptosysteem	Veiligheidsniveau (bit)			
		80	128	192	256
Ontbinden in priemfactoren	RSA	1024	3072	7680	15360
Discrete logaritme probleem	DH, DSA, Elgamal	1024	3072	7680	15360
Elliptische krommen	ECDH, ECDSA	160	256	384	512
Symmetrische encryptie	AES, 3DES	80	128	192	256

Tabel 1: sleutel lengtes van algoritmes

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

KU LEUVEN | universiteit hasselt