Planning Masterproef 2008-2009
Implementations of pairings for cryptography in constrained environments

Anthony Van Herrewege

5 november 2008

Doelstellingen

Deze masterproef heeft tot doel het ontwerpen van een implementatie van pairings over elliptische krommen waarbij speciale aandacht zal besteed worden aan een compact ontwerp dat gebruikt kan worden in apparaten met beperkte rekenkracht (bv. bankkaarten en RFID tags).

Meer specifiek zal een Tate-pairing over elliptische krommen in karakteristiek 2 geïmplementeerd worden in GEZEL. Naast het zo compact mogelijk maken van deze implementatie zal rekening gehouden worden met het feit dat een aanvaardbare rekentijd behouden moet blijven.

Planning

oktober Literatuurstudie ECC en GEZEL, leren GEZEL. (100u)

november - december MALU implementatie GEZEL. Structuur thesistekst uitwerken. (150u)

januari - midden maart Pairing implementatie in GEZEL. (250u)

midden maart - midden april Debuggen, testen, optimalisaties, trade-offs. (100u)

midden april - mei Afwerken thesistekst en Engels artikel. (150u)

eind mei Indienen thesistekst en Engels artikel. Presentatie maken. (50u)