Masterproef industriële ingenieurswetenschappen 2015-2016

Impact van publieke sleutel cryptografie op draadloze sensornetwerken

Ümit Gültekin

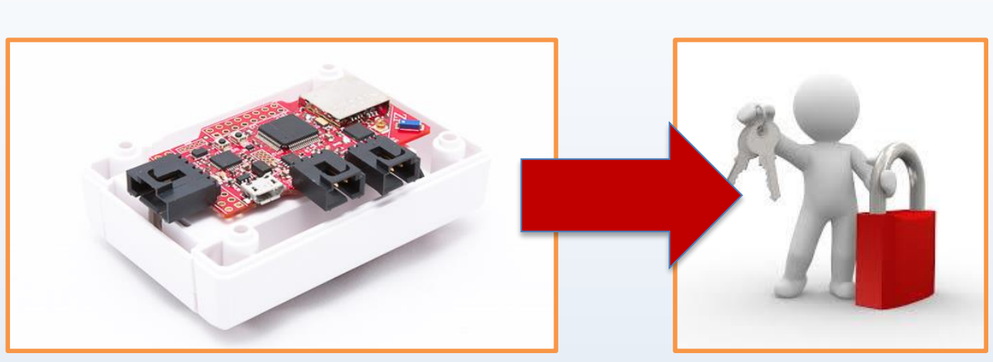
master IW elektronica-ICT

Probleemstelling

Draadloze sensornetwerken zijn voornamelijk *batterij-gevoed* en beschikken over *beperkte rekenkracht en geheugen*. Hierdoor wordt het *implementeren* van *publieke sleutelcryptografie* beveiliging *moeilijk en kostelijk*. Maar omdat de *sensor nodes* gaande weg *krachtiger worden* is het wel *nuttig* om te kijken wat de *huidige impact* is van publieke sleutelcryptografie.

Doelstelling

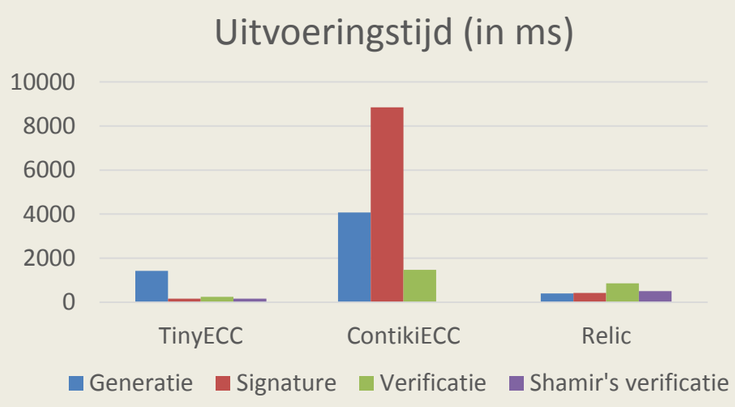
Het belangrijkste doel van deze thesis is de implementatie van publieke sleutelcryptografie op sensor nodes en de analyse van de impact op geheugen, energie en rekenkracht van de sensoren.

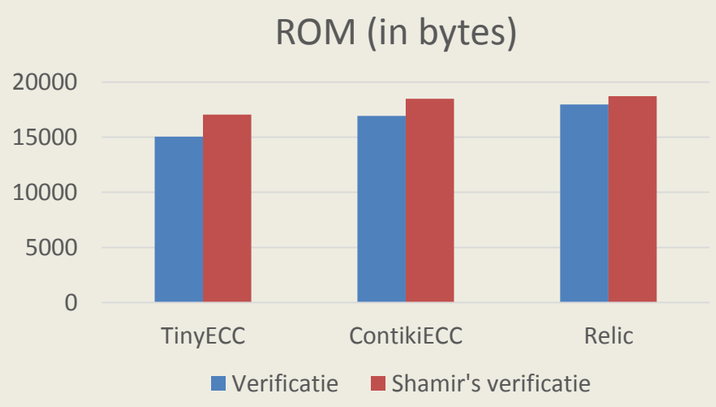


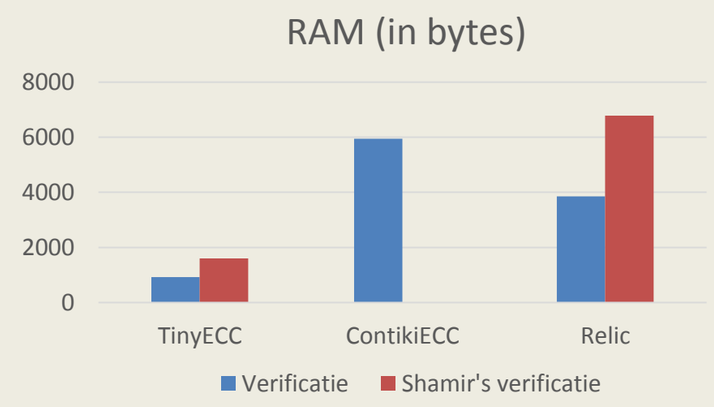
Manier van werken

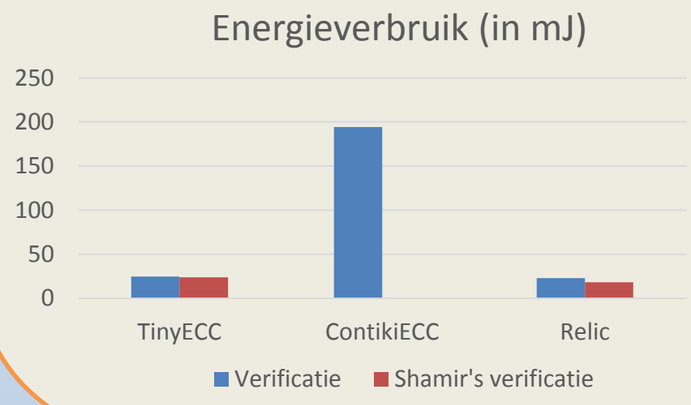
- Het bestuderen van publieke sleutelcryptografie om Elliptic Curve Cryptography (ECC) te kunnen situeren;
- Het begrijpen en analyseren van bestaande bibliotheken voor publieke sleutelcryptografie;
- Het uitvoeren van profiling op de verschillende onderdelen van de code om een grondige analyse te kunnen uitvoeren op de geïmplementeerde onderdelen;
- Het nagaan van de mogelijkheid tot uitbreiding van de implementatie.

Resultaten









Conclusie

Op sensor nodes is een hoog niveau van veiligheid met kleine sleutelgroottes toepasbaar; hierdoor is er verbetering in energieverbruik en timing prestaties, wat zorgt voor minder batterijverbruik.

Promotoren / Copromotoren: ing. Ruben Smeets
Prof. dr. ir. Nele Mentens

Embedded Systems & Security

KU LEUVEN | universiteit hasselt