Elliptisk kurve kryptografi

Bacheloroppgave, Dataingeniør 2016
NTNU

Oversikt

- Oppgavestiller: Atmel Norway AS
- Oppgavebeskrivelse
- Hvorfor ble denne oppgaven valgt?
- Hvordan ble problemet løst?
- Resultater / Demo
- Videre arbeid

Oppgavestiller: Atmel Norway AS

- Atmel Norway ligger plassert oppe på Vestre Rosten, Tiller.
- Hovedkontor i San Jose, USA.
- Grunnlagt i 1984.
- Omtrent 5000 ansatte på verdensbasis.
- Verdensledende innen design og produksjon av mikrokontrollere, kapasitive berøringsløsninger, avansert logikk, osv.

Oppgavebeskrivelse

- Studer elliptisk kurve kryptografi.
- Studer kjente side-channel angrepsmetoder.
- Studer eksisterende arbeid på elliptisk kurve kryptografi.
- Implementere ECC krypterings- og dekrypteringsalgoritmer i C.
- Implementere side-channel beskyttelsesmekansimer mot timing- og power-analyser.
- Diskuter effektiviteten av de foreslåtte mekanismene, vurder effekten av de ulike implementasjonene som kan velges av en kompilator. List angrepsflater som ikke lett kan dekkes på C-nivå.

Hvorfor ble denne oppgaven valgt?

- Interesser for internettsikkerhet og datasikkerhet.
- Arbeide med noe nytt og nyskapende.
- Studere løsninger for et økende problem.
- Forberedelser på videre studier og arbeid.
- Utfordre meg selv på nye felt.

Hvordan ble problemet løst?

- Studier av litteratur innen ECC og side-channel angrep:
  - «Understanding Cryptography: A Textbook for Students and Practitioners»
  - «Hardware Security: Design, Threats, and Safeguards»
  - «Applied Cryptography: Protocols, Algorithms, and Source Code in C»
- Lesing i forskjellige artikler og forskningsrapporter på nett.
- Studier av relevant materiale på forskjellige nettsider.
- Egen utvikling og testing av løsninger.

Resultater / Demo

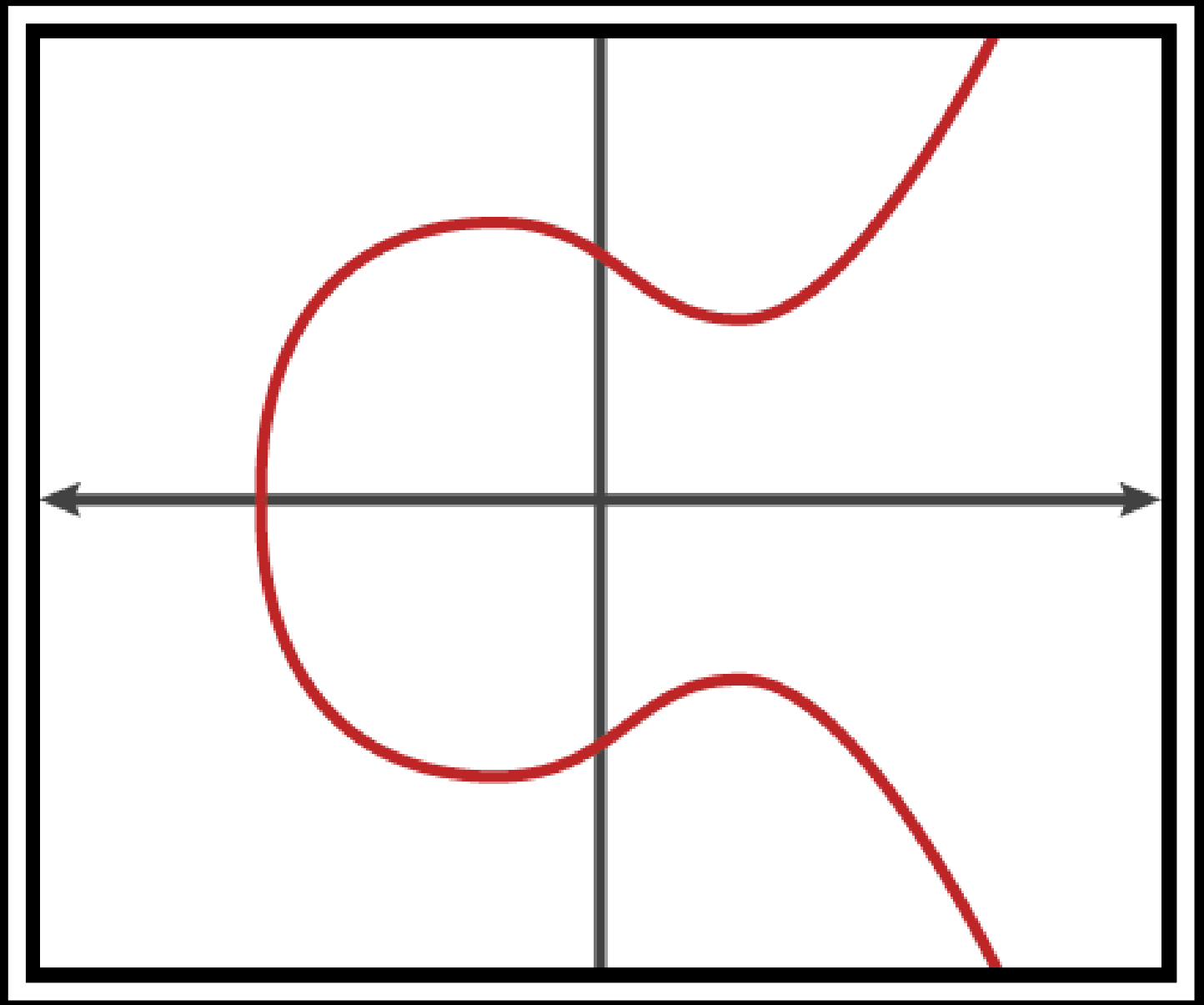
- Bacheloroppgaven (programkode+dokumentasjon):
  - https://bitbucket.org/fredrik_bakken/bachelor/src
  - www.fredrikbakken.no/bacheloroppgave.zip
- Dokumentasjonen:
  - https://bitbucket.org/fredrik_bakken/bachelor/src/02334e3bd8a984ddb53458be66ab5f96c019c765/Documentation/thesis/?at=master
  - www.fredrikbakken.no/dokumentasjon.zip
- Programkoden:
  - https://bitbucket.org/fredrik_bakken/bachelor/src/02334e3bd8a9/Code/?at=master
  - www.fredrikbakken.no/programkode.zip

Videre arbeid

- Videreutvikle selvutviklet versjon til å takle flere ord, setninger, filer, osv.
- Gjennomføre tester mot side-channel angrep.
- Gjøre validering av de beskyttelsesmekanismer som er utvikling (og videreutvikle disse).
- Utvikle bedre behandling av feilhåndering.
- PS: Dette gjelder selvutviklet kryptoløsning. Denne programløsningen bør ALDRI benyttes i andre programmer og løsninger.

Kilder

- http://www.atmel.com/About/corporate/factsheet.aspx
- http://www.atmel.com/about/corporate/default.aspx
- Atmel Norway bilde, http://www.hent.no/portfolio-item/atmel/
- Kryptografi bilde, http://www.txedo.me/blog/category/cryptography/



Presentert av

Fredrik Bakken