NTNU

Kunnskap for en bedre verden

Kryptografi ved NTNU

Kristian Gjøsteen
Institutt for matematiske fag
Norsk kryptoseminar, januar 2020

NTNU

Oversikt

Hvem?

Hva?

Hvorfor?

Og så . . .

NTNU

Hvem driver med krypto på NTNU?

Institutt for matematiske fag (IMF):

- Kristian Gjøsteen (internettvalg, Dual-EC-DRBG)
- Jiaxin Pan (offentlig-nøkkel-kryptografi)

Institutt for informasjonssikkerhet og kommunikasjonsteknologi (IIK):

- Colin Boyd (skrev boken om nøkkelutveksling)
- Danilo Gligoroski (konstruerer primitiver)
- Stig Frode Mjølsnes (smartkort-protokoller)

Alle i Trondheim.

NTNU

PhD-studenter og post.doc.

IMF:

- 8 PhD-studenter
- 2 post.doc.er

IIK:

- 3? post.doc.er
- 8? PhD-studenter

Vi utdanner 5-10 høyt utdannede kryptologer med norsk statsborgerskap innen 2023, og enda flere som er sikkerhetsklarerbare.

NTNU

Masterstudenter

IMF:

- Ca. 5 studenter i året.

IIK:

- Ca. 10 studenter i året.

NTNU

Samarbeid

Internasjonalt:

- Tyskland, Luxembourg, UK, Canada, osv.

Nasjonalt:

- Simula@UiB

NTNU

Kurs

Masternivå:

- **Kryptografi** Matematisk kryptografi, algoritmer for å knekke kryptografi.
- **Master-seminar i kryptografi**
- **Informasjonssikkerhet** Kryptografi sett fra et TLS-perspektiv.
- **Trådløssikkerhet** Sikkerhet i trådløse nettverk.
- **Blockchain**

PhD-nivå:

- **Videregående kryptografi** Flerpartsberegninger
- **Kryptografiske protokoller**
- **Identitetsbasert kryptografi**

Videreutdanning:

- ???

NTNU

Nyutdannede

3 fra IMF, 2 fra IIK siste 5 år.

- Anders S. Lund, *Internettvalg*
  Arbeider med sikkerhet i et nystartet konsulentselskap
- Håkon Jacobsen, *Sikkerhet i TLS*
  Thales
- Britta Hale, *Nøkkelutveksling og sikre kanaler*
  Tenure-track i USA
- Martin Strand, *Internettvalg og homomorfisk kryptering*
  FFI
- Herman Galteland (mars i år), *Ondsinnede anvendelser av kryptografi*
  ???

NTNU

Prosjekter: Malicious cryptology (NSM)

Finansiert av NSM.

Herman Galteland (PhD-student)

2015–2020

- cMix analyse
- Skjule skadevare
- Knekke Tor (pågående)
- Subliminale kanaler i kvante-sikre signatursystemer (pågående)
- Post-quantum offline assisted key exchange (pågående)

NTNU

Prosjekter: Cloud cryptography (NFR)

Samarbeid med Simula@UiB.

Gareth Davies (post.doc.) frem til 2018 og Yao Jiang (PhD-student)

2016–2020

- Security Notions for Cloud Storage
- Offline Assisted Key Exchange
- Post-quantum Offline Assisted Key Exchange
- Zero knowledge for FHE
- Updatable encryption (ongoing)
- Tight reductions for multi-user digital signatures and key exchange
- Post-quantum offline assisted key exchange

NTNU

Prosjekter: Cryptographic Voting Systems (NFR)

Samarbeid med Luxembourg.

2 x post.doc. og 1 x PhD-student (+ det samme i Luxembourg). I tillegg 1 x PhD-student finansiert av NTNU.

Startet høsten 2018

- Skal arbeide med alle aspekter av kryptografiske valgsystemer, fra brukervennlighet til hvordan vi beviser sikkerhet.
- 5-10 artikler så langt.

NTNU

Prosjekter: Quantum-Safe IoT (NFR)

Samarbeid med Simula@UiB.

1 x PhD-student (+ 1 x PhD-student og 1 x post.doc. ved Simula@UiB)

Startet høsten 2018

- Skal arbeide med post-quantum krypto for IoT-systemer, deriblant primitiver (Simula@UiB) og protokoller (NTNU).
- Kunnskapsløse bevis for stokking (pågående)
- Nøkkelutveksling i IoT (pågående).

NTNU

Prosjekter: Post-quantum Cryptography (Regjeringen)

En slags moralsk oppfølger til en NFR-søknad fra 2016.

3 x PhD-student

Startet høsten 2018

- Ny isogeny-basert nøkkelutvekslingsalgoritme.
- Lattice-basert nøkkelutveksling (pågående)
- Kunnskapsløse bevis for stokking (pågående).

NTNU

Prosjekter: Digital Transformation, blockchain (NTNU)

Internt tverrfaglig NTNU-prosjekt med 6 x PhD-studenter.

1 x PhD-student

Startet høsten 2018

- Teoretiske kryptologiske egenskaper.
- Samspill med nettverksteknologi.
- Anvendelser innen identitetshåndtering, medisin, økonomi og samfunnsvitenskap.
- Analysere blockchain-baserte protokoller med Tamarin (pågående).

Prosjekter: Cryptography for Blockchain Services (NTNU)

Internt NTNU-prosjekt.

1 x PhD-student

Startet vinter 2019

- Skal arbeide med kryptografi for blockchain.

NTNU

Prosjekter: Lightweight Cryptography

NFR-finansiert.

3 x PhD-student/post.doc.

Starter høsten 2019

— Lettvekts-kryptografi i forskjellige former.

NTNU

Hva kan vi?

Dette er vi gode på:

- Kryptoprotokoller.
- Nøkkelutveksling.
- Kryptografiske valgsystemer.
- Asymmetriske kryptoprimitiver.

Dette vil vi bli gode på i løpet av 2020:

- Kvante-sikker krypto.
- Blockchain.

Hva vi ikke skal drive med (hovedsaklig):

- Symmetrisk kryptografi (Bergen).

NTNU

Hvorfor?

- NTNU skal ha kryptomiljøer som er gode på forskning.
- NTNU skal utdanne brukbare kandidater.
- NTNU skal kunne bidra med kompetanse. F.eks. E-valg 2011.

NTNU

Mer samarbeid...

Regjeringen vil at vi skal snakke med relevante miljøer.

Mitt mål er at vi skal bry oss om relevante kryptoproblemer, bistå der vi kan og utdanne riktige kandidater.

NTNU

Senter for Fremragende Forskning?

Vi arbeider i disse dager med å sette sammen en søknad om et Senter for Fremragende Forskning innen kryptografi, i samarbeid med Simula UiB.

Vi ønsker kort fortalt at alle som driver med kryptografi i Norge på en eller annen måte skal være med i denne konstruksjonen.

- Enten direkte gjennom å bidra med penger, kompetanse og arbeidskraft: eller
- gjennom løsere samarbeidskonstellasjoner.

NTNU

Eurocrypt 2021

Siste uke i april 2021 i

Trondheim!

Vi trenger noen sponsorer.