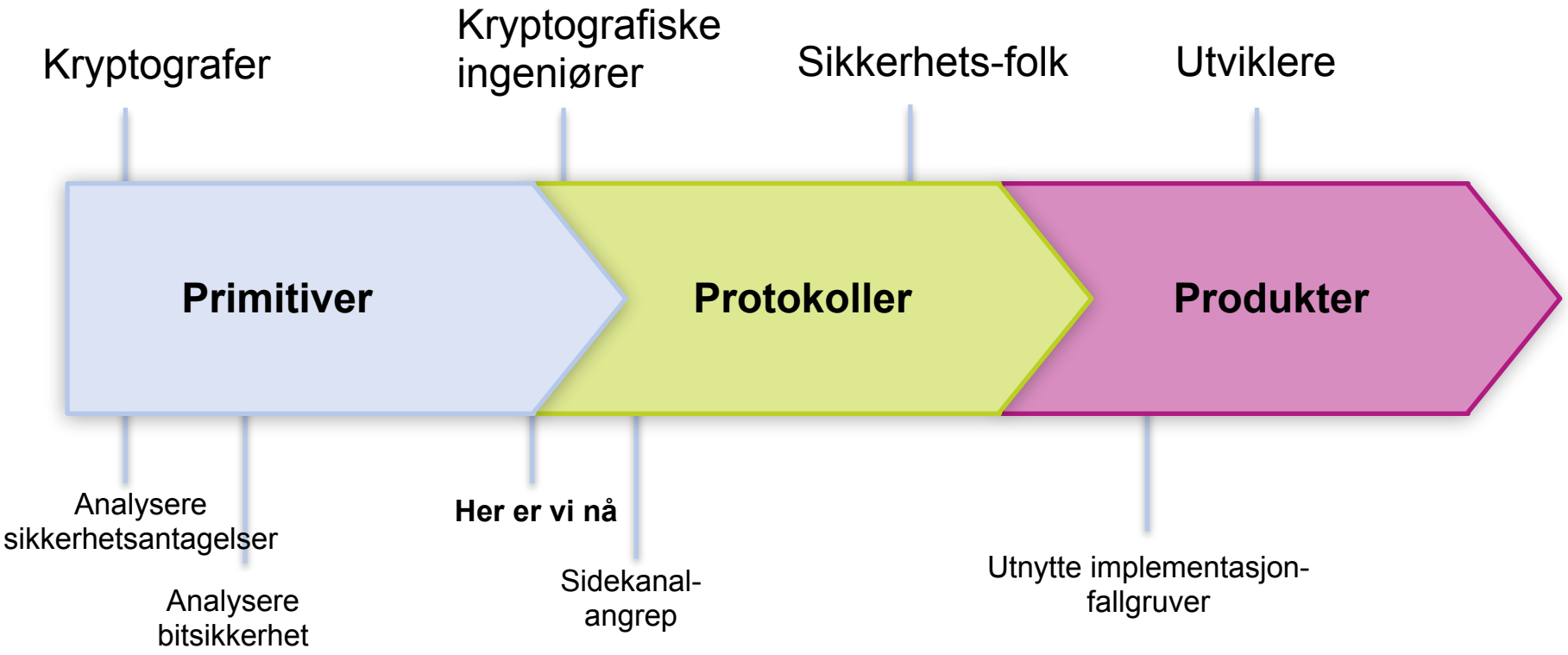
NTNU | Kunnskap for en bedre verden

Kvantesikker Kryptografi: Starten på slutten?

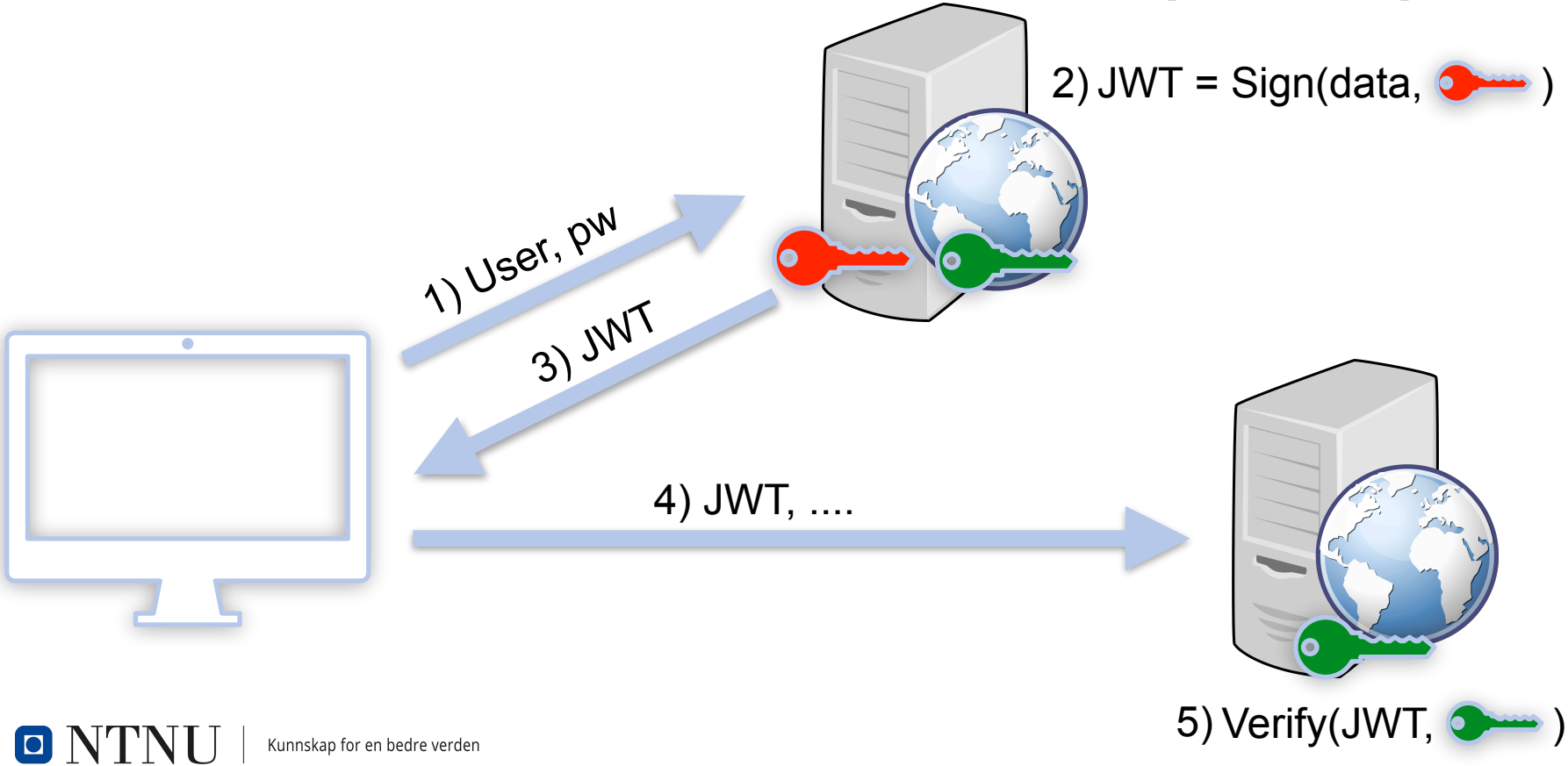
Jonathan Komada Eriksen - IIK, NTNU

Kryptografi i virkeligheten

FRA PRIMITIVER TIL PRODUKT


Kryptografer
Kryptografiske ingeniører
Sikkerhets-folk
Utviklere
Primitiver
Protokoller
Produkter
Analysere sikkerhetsantagelser
Analysere bitsikkerhet
Her er vi nå
Sidekanal-angrep
Utnytte implementasjon-fallgruver

"Enkelt": JSON Web Tokens (JWTs)



JWTs - Hva må være nytt?

- **JWT standarden -** implementere kvantesikre signaturer.
  - Drop in replacement - eller?
    - Størrelsen på signaturen kan bli et problem.
- **Produktledere -** Når skal man bytte til PQ signaturer?
- **Utviklere -** Må kunne sette det opp riktig.

Utfordrende: TLS

TLS - utfordringer

- Påvirker **all sikker trafikk** på internett.
- Trengs **bred enighet** om **standarder**.
- **Enkelt-bedrifter -** Lite å tenke på?
  - Fortsatt mye usikkerhet hvordan bedrifter vil påvirkes.
  - Prøveprosjekter er alt i gang.

Vanskelig: Signal, Bitcoin, e-voting, ...

- Krever ting **utenfor primitivene** som er standardisert.
- **Eks: Signal - Krever Non-Interactive Key Exchange**
  - Tvilsomt om PQ alternativer er praktiske
- Bedrifter **må ta stilling** til **hvor og hvordan** de bruker **kryptografi**
  - I værste fall finnes det ingen PQ alternativ.

NIST on-ramp signatures.

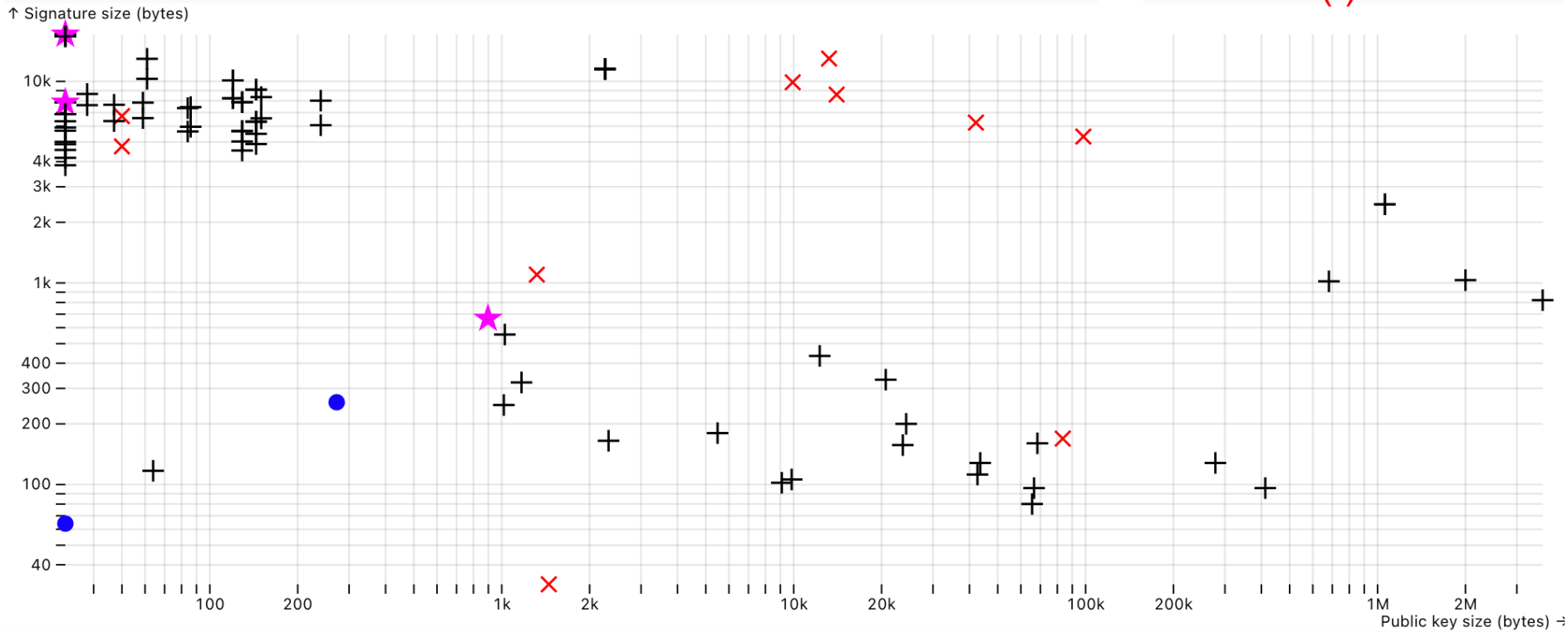
FLERE STANDARDER?

UPDATES

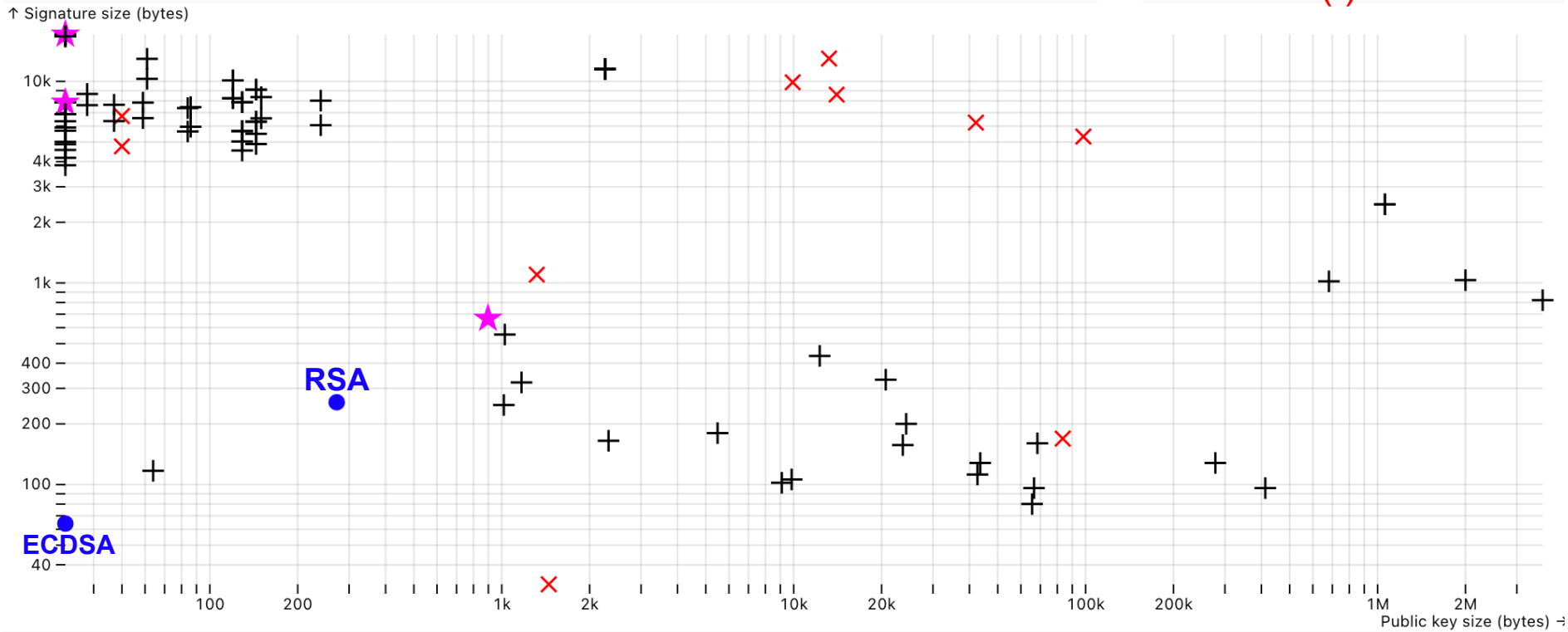
NIST Announces Additional Digital Signature Candidates for the PQC Standardization Process

NIST has completed the reviews for all the "onramp" digital signature submissions received by the deadline.

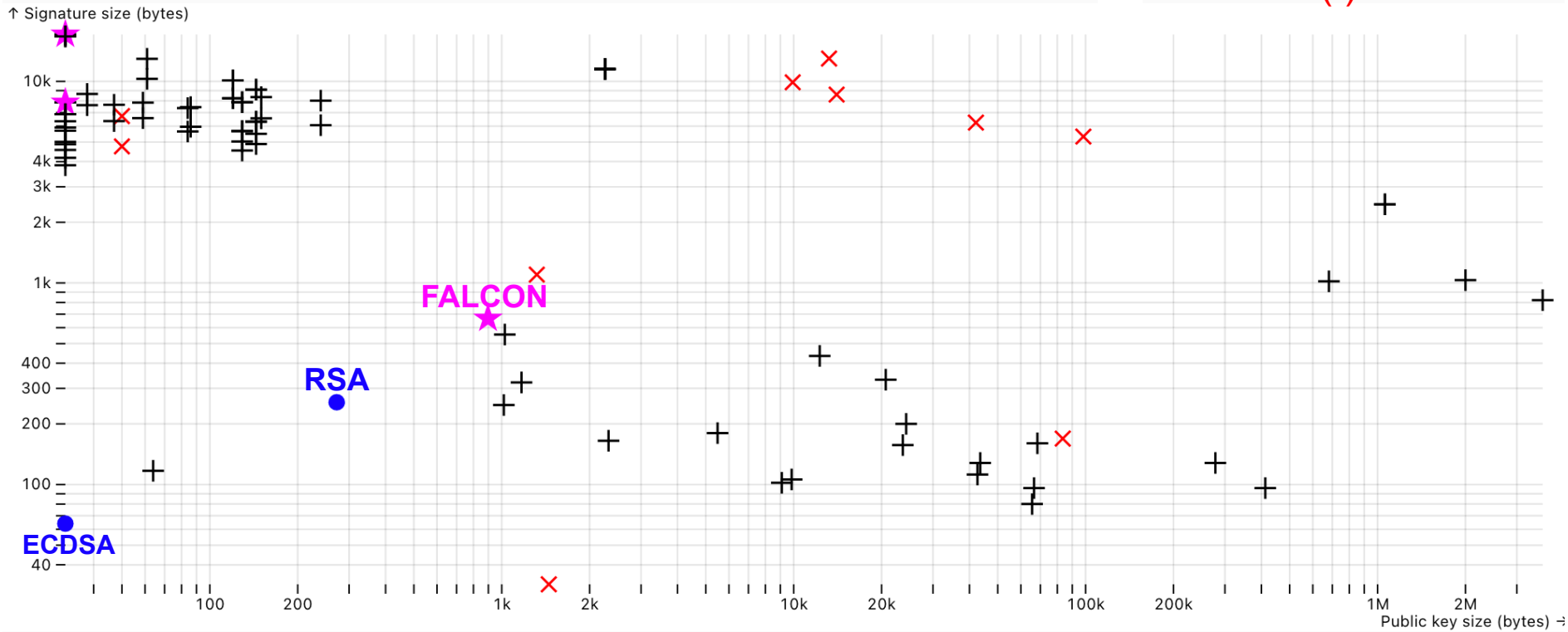
July 17, 2023



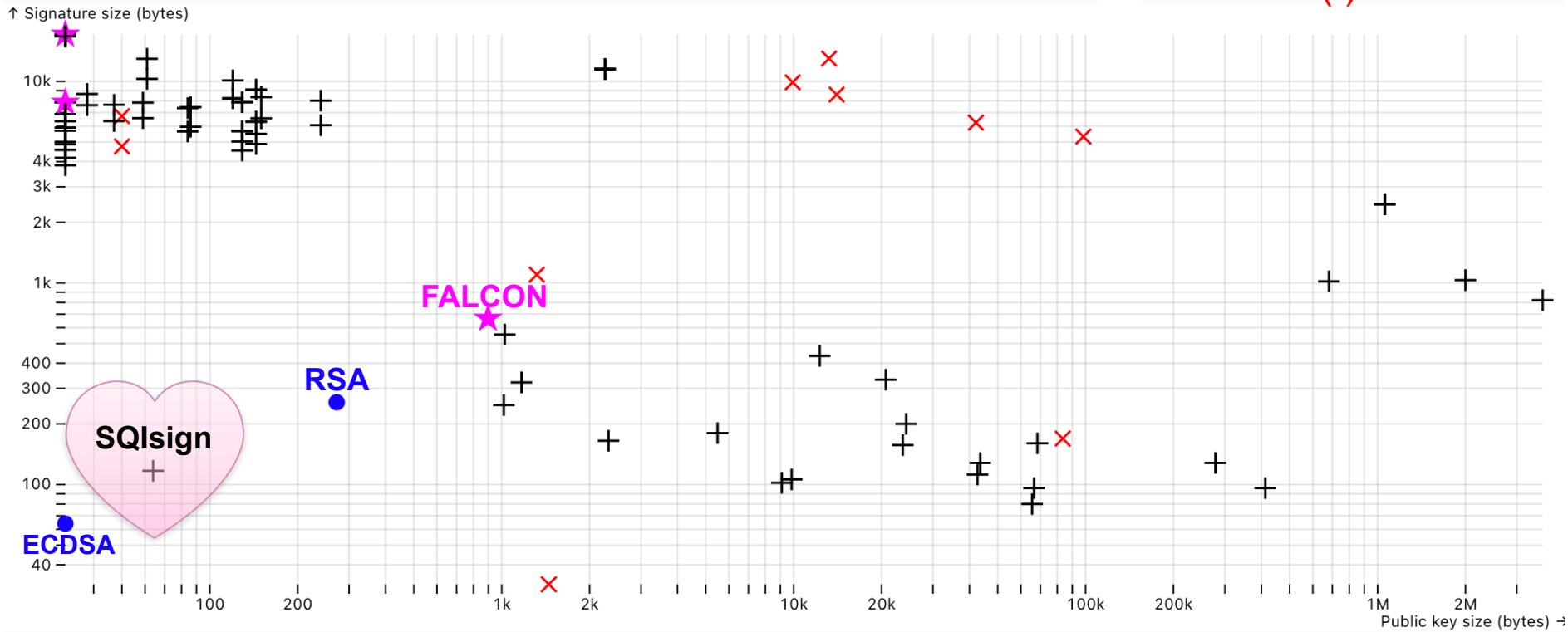
https://pqshield.github.io/nist-sigs-zoo/wide



https://pqshield.github.io/nist-sigs-zoo/wide



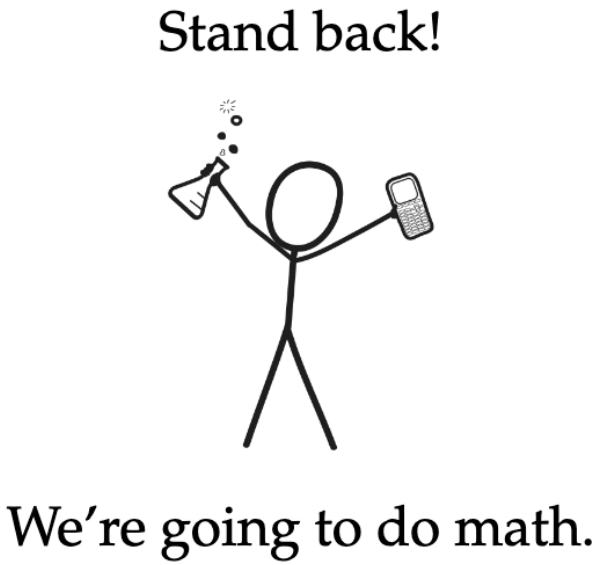
https://pqshield.github.io/nist-sigs-zoo/wide



https://pqshield.github.io/nist-sigs-zoo/wide

Hvordan beviser man at en protokoll ikke kan knekkes?

- Man kan ikke! Det beste vi kan håpe på, er **reduksjoner** til andre problemer man tror er vanskelige.



Eksempel: Et tidlig kryptosystem

- **Antagelse:** Gitt $N = pq$ er det vanskelig å finne p og q

Eksempel: Et tidlig kryptosystem

- **Antagelse:** Gitt $N = pq$ er det vanskelig å finne p og q
- **Knekke kryptografien:** Finn tall m større enn 1, og mindre enn $N - 1$ slik at $m^2 - 1 = kN$ for en k

Eksempel: Et tidlig kryptosystem

- **Antagelse:** Gitt $N = pq$ er det vanskelig å finne p og q
- **Knekke kryptografien:** Finn tall m større enn 1, og mindre enn $N - 1$ slik at $m^2 - 1 = kN$ for en k
- **Teorem:** Gitt **antagelsen**, så er **kryptosystemet sikkert**

Eksempel: Et tidlig kryptosystem

- **Antagelse:** Gitt $N = pq$ er det vanskelig å finne p og q
- **Knekke kryptografien:** Finn tall m større enn 1, og mindre enn $N - 1$ slik at $m^2 - 1 = kN$ for en k
- **Teorem:** Gitt **antagelsen**, så er **kryptosystemet sikkert**
- **Reduksjon:** $m^2 - 1 = (m-1)(m+1) = kpq$
  - Observer at p og q kan ikke begge dele samme faktor
  - Kan finne p eller q som største felles divisor av $m + 1$ og N
  - Q.E.D.

Sikkerhetsantagelsene er ikke vanntette!

Quantamagazine | Physics | Mathematics | Biology | Computer Science | Topics | Archive

CRYPTOGRAPHY

‘Post-Quantum’ Cryptography Scheme Is Cracked on a Laptop

Two researchers have broken an encryption protocol that many saw as a promising defense against the power of quantum computing.

https://www.quantamagazine.org/post-quantum-cryptography-scheme-is-cracked-on-a-laptop-20220824/

Reduksjonene er feil!

- **Merkle-Hellman Knapsack Cryptosystem.**
  - Basert på det **NP-komplette** knapsack problemet.
- "Forgjengeren" til **Lattice-basert** kryptografi.
- **Fullstending knukket**
  - Knapsack er selvsagt ikke løst, men selve reduksjonen var feil.

https://en.wikipedia.org/wiki/Merkle-Hellman_knapsack_cryptosystem

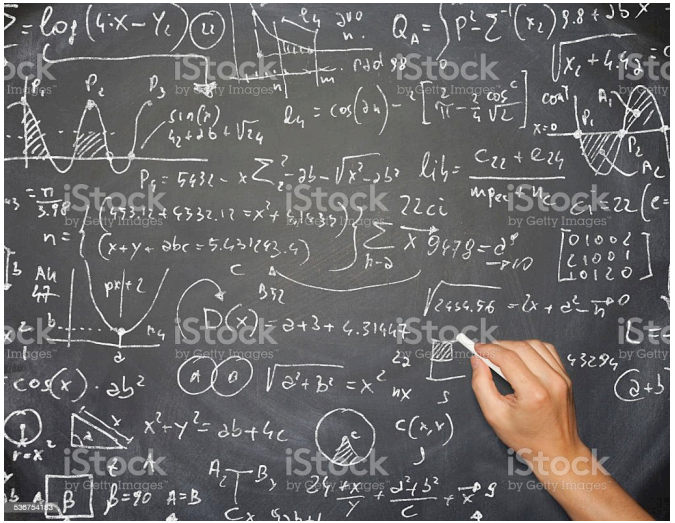
Hvordan knekkes kryptografi i praksis? Hva er konsekvensen av dette?

KRYPTANALYSE

Hva knekker kryptografien?

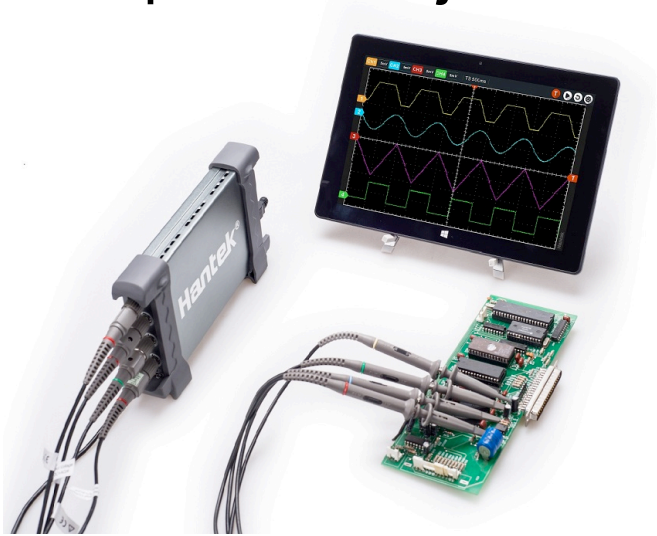
NIST-prosessen

- Reduksjoner og antagelser.



Virkeligheten

- Sidekanal angrep og implementasjonsfeil.



Sidekanal angrep

- Utnytter informasjonslekkasjer.
- Eksempler mot TLS:
  - Lucky Thirteen
  - POODLE
  - Etc...
- Forskning på kvantesikker kryptografi **i startfasen**:
  - **Satsningsområde på NTNU:**
    - Kjøpt inn **utstyr** (nesten 1 mill NOK) til å utføre slike angrep
    - **Masterprosjekter:** Se f.eks. Erlend Håkegård's oppgave

Det helt suverent vanligste...

- **Implementasjonsfeil.**
- Utviklere ≠ Kryptografer.
- "Åpenbare" feil blir **vanligere fremover.**
- Nye **subtile feil** kommer til å bli oppdaget.

Et utvalg av mine (enkleste) favoritter...

ECDSA: (0,0) er en gyldig signatur på enhver melding

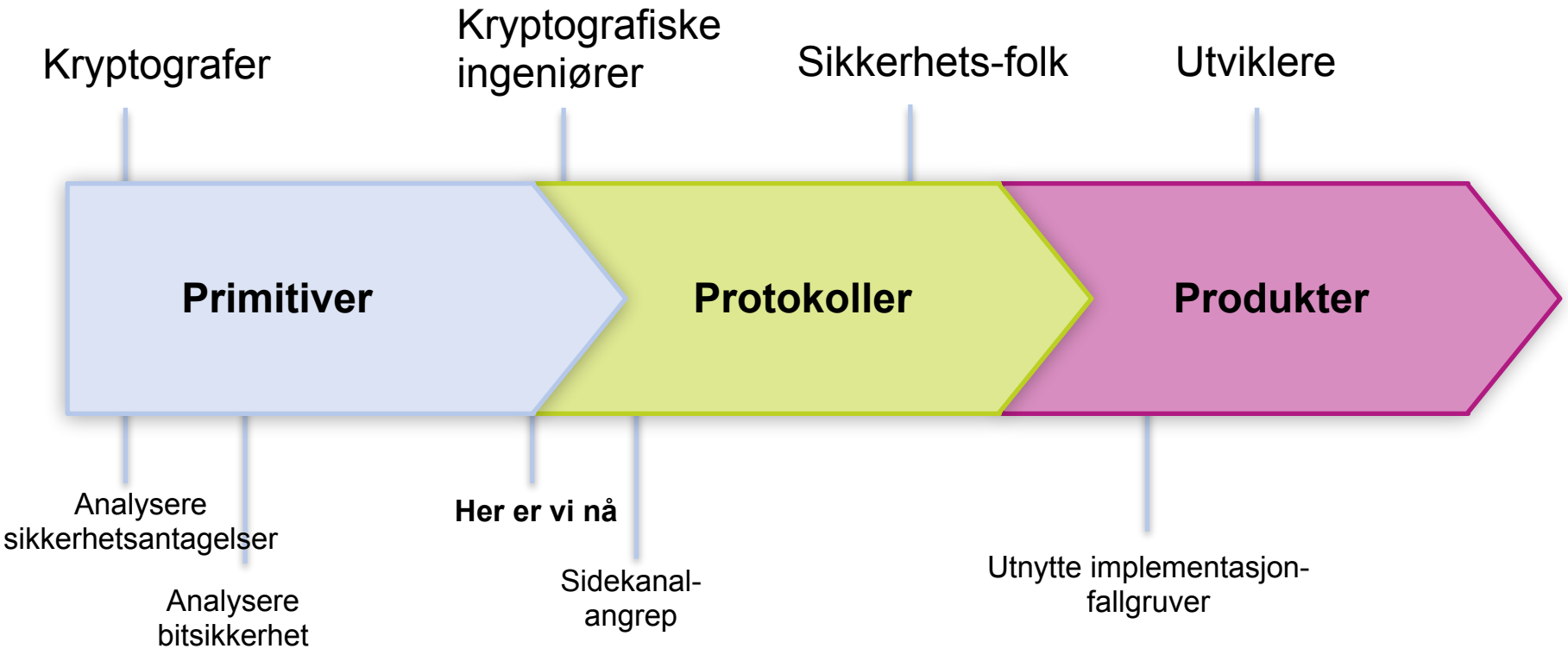
RSA: Dersom primtallene er generert på litt feil måte...

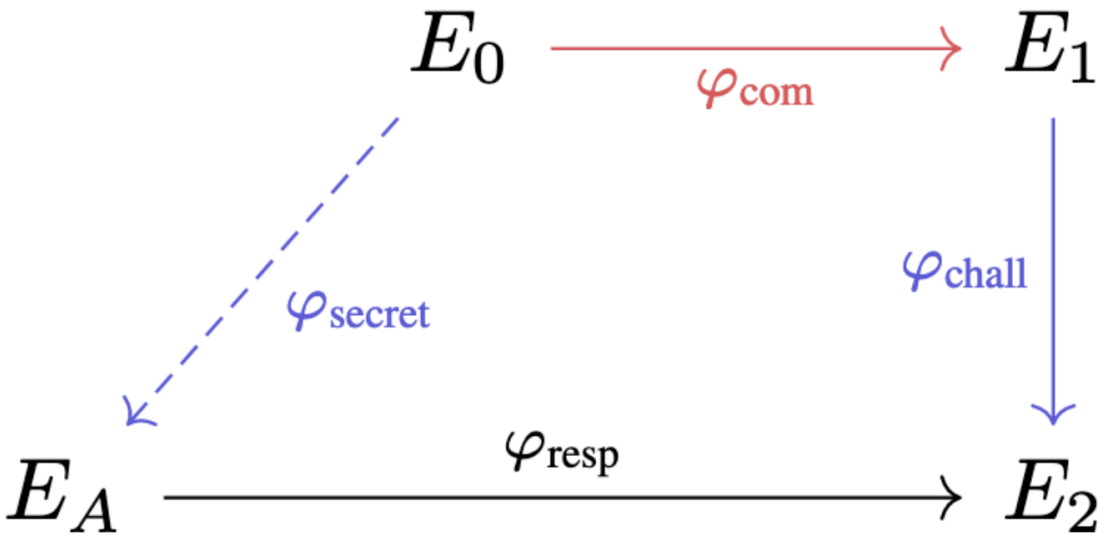
ECDSA: Dersom en tilfeldig verdi ikke er "tilfeldig nok"

Hva blir fremtidens varianter av disse type svakhetene?

Tidslinje av hvem som involveres hvor

OPPSUMMERING


Kryptografer
Kryptografiske ingeniører
Sikkerhets-folk
Utviklere
Primitiver
Protokoller
Produkter
Analysere sikkerhetsantagelser
Analysere bitsikkerhet
Her er vi nå
Sidekanal-angrep
Utnytte implementasjon-fallgruver



Tusen takk!

Epost: jonathan.k.eriksen@ntnu.no
Nettside: jonathke.github.io