NTNU

Norwegian University of Science and Technology

Sikkerhet i en post-kvante verden

Sikkerhetsfestivalen 2019, Lillehammer

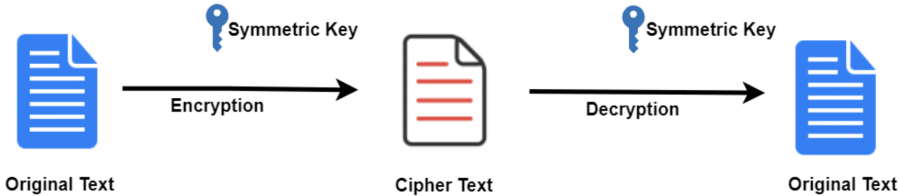
Tjerand Silde

Institutt for matematiske fag,
NTNU Trondheim

NTNU

Dagens kryptografi

Symmetrisk Kryptografi I



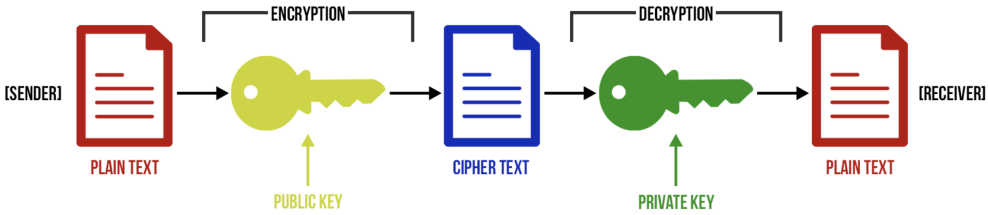
NTNU

Symmetrisk Kryptografi II

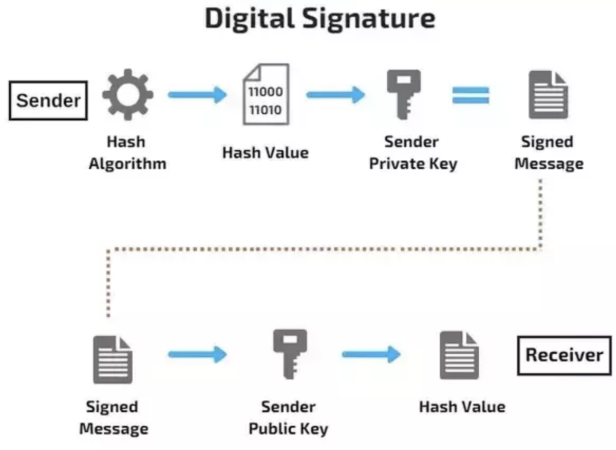
Egenskaper ved symmetrisk kryptografi:

- Begge parter må vite nøkkelen på forhånd
- Vanligvis er nøkler og blokker av størrelse 128 eller 256 bits
- Veldig raskt (bruker bare XOR, AND, vektorer osv.)
- Lengden av chiffertekst $\approx$ Lengden til meldingen
- Beste måten å knekke systemet er å gjette nøkkelen

Asymmetrisk Kryptografi I



Asymmetrisk Kryptografi II



NTNU

Asymmetrisk Kryptografi III

Egenskaper ved asymmetrisk kryptografi:

- En person kjenner den hemmelige nøkkelen, alle kjenner den offentlige
- Vanligvis er nøkler og chiffertekster av størrelse 256 til 4096 bits
- Ganske tregt (mange multiplikasjoner og eksponensieringer)
- Sikkerhet er basert på diskrete logratimer eller faktorisering

Asymmetrisk Kryptografi IV

RSA kryptografi:

- Velg to primtall p og q, og la $n = p \cdot q$
- Velg et tall e og finn et annet tall d avhengig av p og q
- Den offentlige nøkkelen er (e, n)
- Den private nøkkelen er (d, n)

Asymmetrisk Kryptografi V

RSA kryptering:

- Kryptering av en melding m: $\texttt{Enc}((e, n), m) = m^e \mod n = c$
- Dekryptering av en chiffertekst c: $\texttt{Dec}((d, n), c) = c^d \mod n = m$

NTNU

Asymmetrisk Kryptografi VI

RSA signaturer:

— Signere en melding m: $\texttt{Sign}((d, n), m) = (\texttt{H}(m))^d \mod n = \sigma$

— Verifisere en signatur σ: $\texttt{Verify}((e, n), \sigma, m) = \sigma^e \mod n \stackrel{?}{=} \texttt{H}(m)$

NTNU

Kvantedatamaskiner og algoritmer

Kvantedatamaskiner og algoritmer I

Quantum Physics

A fast quantum mechanical algorithm for database search

Lov K. Grover (Bell Labs, Murray Hill NJ)

(Submitted on 29 May 1996 (v1), last revised 19 Nov 1996 (this version, v3))

Kvantedatamaskiner og algoritmer III

AES-128 security, revisited

Quantum	#	Classical	#
depth:	2^{40}	depth:	2^{35} AES ops
circuits:	2^{82}	processors:	2^{93}
qubits/circuit:	2,953		
gates/circuit:	2^{46}	gates/processor:	2^{50}
Total gates:	2^{128}	Total gates:	2^{143}

- The 2^{93} classical processors used for error correction could be repurposed to perform exhaustive key search in time 2^{35} AES operations.
- It isn't clear then that Grover's search is more effective than classical exhaustive search in breaking AES-128.

Figure: Alfred Menezes - NutMiC 2019

Quantum Physics

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer

Peter W. Shor (AT&T Research)

(Submitted on 30 Aug 1995 (v1), last revised 25 Jan 1996 (this version, v2))

Quantum Physics

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney, Martin Ekerå

(Submitted on 23 May 2019)

Kvantedatamaskiner og algoritmer VI

Figure: www.qubitcounter.com

NTNU

Hva betyr dette for oss idag?

Levetiden til et kryptosystem

Levetiden til et kryptosystem

Kilde: Kvanteresistent Krypto, NSM A03 - G:17/173.

NTNU

Utfordringer I

- Meldinger som sendes idag kan dekrypteres i fremtiden...
- Det tar tid å finne nye algoritmer som er post-kvante sikre
- Det tar lang tid å implementere nye algoritmer på en sikker måte
- Det tar lang tid å optimalisere nye algoritmer til å bli raske nok
- Det tar lang tid å få systemer til å bytte over til nye algoritmer
- Mye informasjon som sendes i dag må holdes hemmelig i lang tid

Utfordringer II

Eksempler:

- DES, MD-5, SHA-1, “eksport”-DH brukes fremdeles idag...
- RSA ble foreslått i 1977, men ble først standardisert i 1993
- ECC ble foreslått i 1985, men ble først tatt i bruk de siste 10 årene
- Nye algoritmer må inkluderes i populære protokoller som TLS og SSH

NTNU

NIST Standardisering

NIST Standardisering I

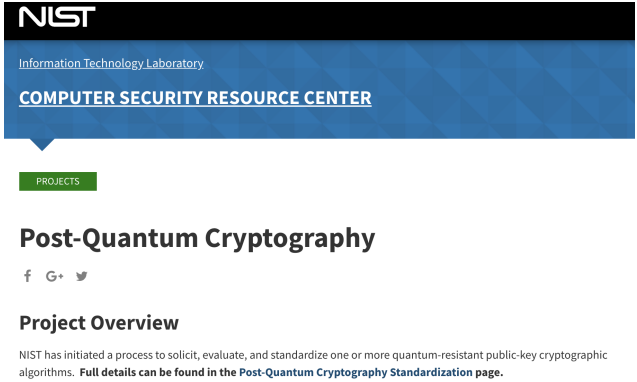


Figure: csrc.nist.gov/Projects/Post-Quantum-Cryptography

NIST Standardisering II

Målsetting:

- Oppfordre til forskning innen post-kvante kryptografi
- Plukke ut en håndfull nye anbefalte algoritmer
- Ikke standardisere kun en algoritme slik som ved AES og SHA-3

NIST Standardisering III

Første runde:

- Frist for å sende inn forslag var november 2017
- Asymmetrisk kryptering og digitale signaturer
- 82 forslag til ny standard ble sendt inn
  - 69 forslag ble akseptert til prosessen
  - 5 forslag trakk seg tidlig

NIST Standardisering IV

The 1st Round Candidates

- 82 submissions received.
- 69 accepted as “complete and proper” (5 withdrew)

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Symmetric-based	3		3
Other	2	5	7
Total	**19**	**45**	**64**

Figure: csrc.nist.gov/Events/2019/Second-PQC-Standardization-Conference

NIST Standardisering V

Andre runde:

- Ble annonsert i januar 2019
- 26 kandidater gikk videre
  - 17 krypteringsalgoritmer
  - 9 digitale signaturer

NIST Standardisering VI

Hva skjer fremover?

- Ny runde om ca. ett år
- Redusere antall kandidater ytterligere
- Endelig beslutning i ca. 2022
- NSA planlegger å ta i bruk fra ca. 2024
- ...

Fordeler og ulemper I

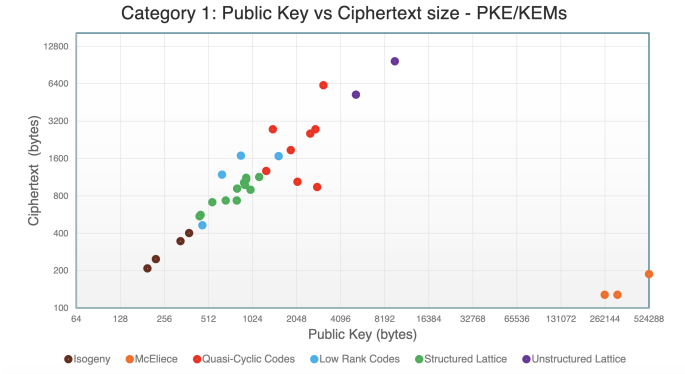


Figure: csrc.nist.gov/Events/2019/Second-PQC-Standardization-Conference

Fordeler og ulemper II

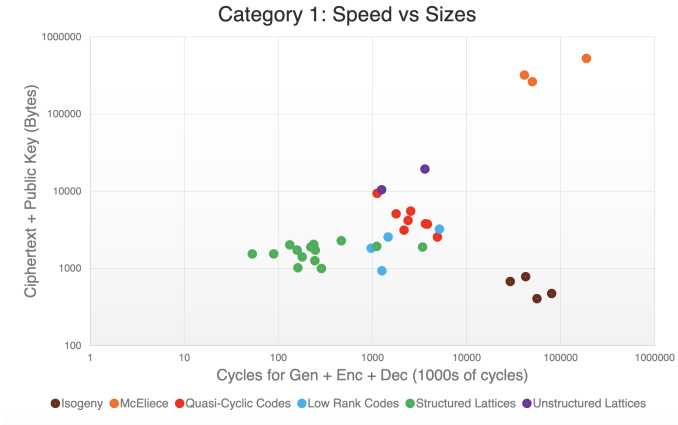


Figure: csrc.nist.gov/Events/2019/Second-PQC-Standardization-Conference

NTNU

Testing av PQC i TLS

NTNU

Google-test i 2016: X25519 + NewHope

Kombinerte vanlig kryptografi med post-kvante kryptografi:

- Vanlig elliptisk kurve kryptografi: X25519
- Ny lattice basert post-kvante kryptografi: NewHope
- NewHope har store nøkler, men er veldig rask
- Testet hvordan TLS 1.2 taklet større nøkler og nye algoritmer
- Bare benyttet når Chrome koblet seg til Google's servere
- TLS 1.2 forhandler om algoritme før nøkkel sendes
- Ingen tilkoblinger kræsjet, men tilkobling tok noen ms ekstra

Kilde: CECPQ1 results - Adam Langley.

NTNU

Google-test i 2018: dummy values

Sendte ekstra data for å teste tilkoblinger:

- Testet hvordan TLS 1.3 taklet større nøkler
- TLS 1.3 sender nøkkel før enighet om algoritme
- Testet med tre ulike størrelser: 400, 1100 og 3300 bytes
- Bare benyttet når Chrome koblet seg til Google's servere
- Dette gav ca. 4%, 10% og 100% overhead i tid
- Betraktet ikke beregningstid hos klient eller server

Kilde: Post-quantum confidentiality for TLS - Adam Langley.

NTNU

Google- og Cloudflare-test i 2019: X25519 + HRSS/SIKE I

Kombinerte vanlig kryptografi med post-kvante kryptografi (igjen):

- Vanlig elliptisk kurve kryptografi: X25519
- Ny elliptisk kurve basert post-kvante kryptografi: SIKE
- Ny lattice basert post-kvante kryptografi: HRSS
- SIKE er mindre men tregere enn HRSS
- Tester hvordan TLS 1.3 takler større nøkler og nye algoritmer
- Testes når Chrome kobles til Google's eller Cloudfare's servere

Kilde1: CECPQ2 - Adam Langley.
Kilde2: Towards Post-Quantum Cryptography in TLS - Kris Kwiatkowski.

Google- og Cloudflare-test i 2019: X25519 + HRSS/SIKE II

SERVER-SIDE RESULTS

Configuration	Additional latency over control group w/ 95% confidence intervals (ms)	
	CECPQ2	CECPQ2b
Android*, 25th	N/A	[51, 63]
Android*, Median	N/A	[47, 62]
Android*, 95th	[45, 537]	N/A
Windows, 25th	N/A	N/A
Windows, Median	[0.9, 3.1]	[16, 20]
Windows, 95th	[69, 100]	[48, 74]

Figure: csrc.nist.gov/Events/2019/Second-PQC-Standardization-Conference

Google- og Cloudflare-test i 2019: X25519 + HRSS/SIKE III

CLIENT-SIDE RESULTS

Chrome is measuring TLS handshake latency, not including TCP connection costs.

The metrics system calculates 95% confidence intervals for changes and a result is considered "significant" if no-change isn't inside that interval.

Configuration	Additional latency with 95% confidence	
	CECPQ2	CECPQ2b
Windows, 25th	N/A	[53%, 102%]
Windows, Median	N/A	[20%, 76%]
Windows, 99th	N/A	N/A
Android, 25th	N/A	[30%, 96%]
Android, Median	N/A	N/A
Android, 99th	[19%, 278%]	N/A

Figure: csrc.nist.gov/Events/2019/Second-PQC-Standardization-Conference

NTNU

Relevante Foredrag

47 - OLE KASPER OLSEN

Kvantedatamaskiner og kryptoløsninger

Ole Kasper Olsen, forsker NSM

OM FOREDRAGET

Det har i de senere år dannet seg konsensus om at kvantedatamaskiner vil kunne bygges i overskuelig fremtid. Bare muligheten for at dette kan skje vil medføre store konsekvenser for hvordan vi velger kryptografiske mekanismer i våre løsninger over de neste 10 år. Dette gjelder anvendelser med nasjonal sikkerhetsmessig betydning, men også i løsninger for næringslivet og for privatpersoner.

Foredraget vil søke å belyse problemstillingene kvantedatamaskiner reiser, og hvordan en kan forsøke å håndtere den store risikoen kvantedatamaskinene representerer for sikkerheten i all vår digitale kommunikasjon.

OM FOREDRAGSHOLDEREN

Ole Kasper Olsen arbeider som forsker i NSMs seksjon for kryptoutvikling, og har 12 års erfaring med evaluering og sertifisering av kryptosystemer for høygraderte anvendelser.

Figure: Kulturhuset Banken festsalen kl. 12:30 - 13:00

NTNU

66 - MADS HENRIKSVEEN

Beyond 2048 (bits RSA)

Mads Henriksveen, *Fagansvarlig CA & eID*, Buypass AS

OM FOREDRAGET

RSA er i dag den mest brukte algoritmen for asymmetrisk kryptografi og en nøkkellengde på 2048 bits er gjeldende beste praksis. Men det er ikke lenge før denne bør erstattes av sterkere kryptografi og hvilke alternativer har vi da?

Vi kan fortsette med RSA og øke nøkkellengden - eller vi kan skifte til mer «lettbente» kryptografiske algoritmer basert på elliptisk kurve kryptografi (ECC). I bakgrunnen truer kvantedatamaskiner som vil utgjøre en trussel mot all bruk av asymmetrisk kryptografi basert på både RSA og ECC. Hva gjør vi når dette er en realitet.

Buypass er en tilbyder av elektronisk identifikasjon og tillitstjenester som i stor grad baserer seg på bruk av asymmetrisk kryptografi. Foredraget vil gi et innsyn i hvordan Buypass tenker på dette området samt hvilke utfordringer de ser både i sin egen rolle som leverandør av tillitstjenester og for brukere og konsumenter av tjenestene.

Figure: Kinoen sal 1 kl. 15:00-15:30

NTNU

Takk! Spørsmål?

E-post: tjerand.silde@ntnu.no
Presentasjon: `www.tjerandsilde.no/talks`