



NTNU | Kunnskap for en bedre verden

Kryptografi - Fortid, Nåtid og en Kvantesikker Fremtid

Jonathan Komada Eriksen - IIK, NTNU

Det enkle er ofte det beste?

KRYPTOGRAFI - FORTID

Historisk: Bok-Chiffer

Melding: Angrip imorgen

Historisk: Bok-Chiffer

Melding: Angrip imorgen

Hemmelig nøkkel:

The screenshot shows the top navigation bar of the NRK website. It features the NRK logo, links for TV, Radio, and other services like NRK Dagsrevyen and P3. Below the main menu, there's a secondary navigation bar with links for Nyheter, Sport, Kultur, Humor, Distrikt, and Mer. A "Logg på" button is also present. At the bottom of the page, there's a horizontal menu with links for Norge, Siste nytt, Dokumentar, Klima, and NRK Ytring.

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

«Elkjøp» reklamerte med råbillige vannkokere på Facebook.
Bak annonsen sto utenlandske kriminelle.

🇳🇴 Elkjøp gir bort de gjenværende
vannkokerne fra Smeg for kun 18k... Se mer



✉ Snorre Tønset
Journalist



Historisk: Bok-Chiffer

Melding: **Angrip imorgen**

Chiffertekst: 2/8



The screenshot shows the top navigation bar of the NRK website. It features the NRK logo on the left, followed by links for TV, Radio, and other services like NRK Dagsrevyen and NRK Nyhetskanalen. Below the main menu, there's a secondary navigation bar with links for Nyheter, Sport, Kultur, Humor, Distrikt, and Mer. On the right side, there are links for logging in, a search bar, and a language selection dropdown set to 'Norge'.

Nettsvindel øker kraftig: Advarer mot å trykke på slike **annonser**

«Elkjøp» reklamerte med råbillige vannkokere på Facebook.
Bak annonsen sto utenlandske kriminelle.

 Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... [Se mer](#)



[✉ Snorre Tønset](#)
Journalist



Historisk: Bok-Chiffer

Melding: Angrip imorgen

Chiffertekst: 2/8, 1/1

The screenshot shows the top navigation bar of the NRK website. It includes links for NRK TV, NRK RADIO, NRK DOK, and NRK Ytring. Below the bar, there's a menu with categories: Nyheter, Sport, Kultur, Humor, Distrikt, and Mer. On the right, there are links for 'Logg på' (Log in) and a search bar. At the bottom of the screenshot, the news headline is visible: 'Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser'.

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

«Elkjøp» reklamerte med råbillige vannkokere på Facebook.
Bak annonsen sto utenlandske kriminelle.

Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... Se mer



[Snorre Tønset](#)
Journalist



Historisk: Bok-Chiffer

Melding: An~~grip~~ imorgen

Chiffertekst: 2/8, 1/1, 1/22

The screenshot shows the top navigation bar of the NRK website. It includes links for NRK TV, NRK RADIO, NRK DOK, and NRK Ytring. Below the bar, there's a menu with categories: Nyheter, Sport, Kultur, Humor, Distrikt, and Mer. On the right, there are links for 'Logg på' (Log in) and a search bar. The main content area features a large headline in bold black text: 'Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser'. Below the headline, a subtext reads: '«Elkjøp» reklamerte med råbillige vannkokere på Facebook. Bak annonsen sto utenlandske kriminelle.' A snippet of the news article is shown, starting with 'Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... Se mer'. To the right of the snippet is a profile picture of Snorre Tønset, a journalist.

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

«Elkjøp» reklamerte med råbillige vannkokere på Facebook.
Bak annonsen sto utenlandske kriminelle.

Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... [Se mer](#)



[✉ Snorre Tønset](#)
Journalist

Historisk: Bok-Chiffer

Melding: Angr**ip** imorgen

Chiffertekst: 2/8, 1/1, 1/22, 3/7

The screenshot shows the top navigation bar of the NRK website. It includes links for NRK TV, NRK RADIO, NRK DOK, NRK KIDS, and NRK Ytring. Below the bar, there's a menu with categories: Nyheter, Sport, Kultur, Humor, Distrikt, and Mer. On the right, there are links for 'Logg på' (Log in) and a search bar. At the bottom of the bar, there are links for Norge, Siste nytt, Dokumentar, Klima, and NRK Ytring.

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

«Elkjøp» **reklamerte** med råbillige vannkokere på Facebook.
Bak annonsen sto utenlandske kriminelle.

Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... Se mer



[✉ Snorre Tønset](#)
Journalist



Historisk: Bok-Chiffer

Melding: Angrip imorgen

Chiffertekst: 2/8, 1/1, 1/22, 3/7, ...

The screenshot shows the top navigation bar of the NRK website. It includes links for NRK TV, NRK RADIO, NRK DOK, and NRK Ytring. Below the bar, there's a menu with categories: Nyheter, Sport, Kultur, Humor, Distrikt, and Mer. On the right, there are links for 'Logg på' (Log in) and a search bar. At the bottom of the bar, there are links for Norge, Siste nytt, Dokumentar, Klima, and NRK Ytring.

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

«Elkjøp» reklamerte med råbillige vannkokere på Facebook.
Bak annonsen sto utenlandske kriminelle.

Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... [Se mer](#)



[✉ Snorre Tønset](#)
Journalist



Historisk: Bok-Chiffer

Melding: Angrip imorgen

Chiffertekst: 2/8, 1/1, 1/22, 3/7, ...

The screenshot shows the NRK website interface. At the top, there's a dark header bar with the NRK logo, followed by links for NRK TV, NRK RADIO, NRK DOK, and NRK JR. Below the header is a navigation bar with links for Nyheter, Sport, Kultur, Humor, Distrikt, Mer, Logg på, and a search bar. A sub-navigation bar below the main menu includes Norge, Siste nytt, Dokumentar, Klima, and NRK Ytring. The main content area features a large red headline: "Fryktelig Kronglete". Below it is a black headline: "Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser". A subtext below the headline reads: "«Elkjøp» reklamerte med råbillige vannkokere på Facebook. Bak annonsen sto utenlandske kriminelle." At the bottom left, there's a snippet of another article: "Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... Se mer". On the right side, there's a profile picture of Snorre Tønset, a journalist, with his name and title below it.

Fryktelig Kronglete

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

«Elkjøp» reklamerte med råbillige vannkokere på Facebook. Bak annonsen sto utenlandske kriminelle.

Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... Se mer

✉ Snorre Tønset
Journalist

Historisk: Bok-Chiffer

Melding: Angrip imorgen

Chiffertekst: 2/8, 1/1, 1/22, 3/7, ...

The screenshot shows the NRK website interface. At the top, there are links for NRK TV, NRK RADIO, NRK DOK, and NRK Ytring. Below the navigation bar, there are links for Nyheter, Sport, Kultur, Humor, Distrikt, and Mer. A search bar with a magnifying glass icon and a 'Logg på' button are also present. The main headline is 'Fryktelig Kronglete' in large red text. Below it, the article title is 'Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser'. A subtext states: '«Elkjøp» reklamerte med råbillige vannkokere på Facebook. Bak annonsen sto utenlandske kriminelle.' To the right, there is a large red text overlay: 'Store, vanskelig å distribuere, nøkler'. Below the article, there is a snippet with a small Norwegian flag icon and the text: 'Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... Se mer'. On the right side, there is a profile picture of Snorre Tønset, a journalist, with the text 'Snorre Tønset Journalist'.

Fryktelig Kronglete

Nettsvindel øker kraftig: Advarer mot å trykke på slike annonser

«Elkjøp» reklamerte med råbillige vannkokere på Facebook. Bak annonsen sto utenlandske kriminelle.

Elkjøp gir bort de gjenværende vannkokerne fra Smeg for kun 18k... Se mer

✉ Snorre Tønset
Journalist

Symmetrisk Kryptografi



~1940

Symmetrisk Kryptografi



Enkel å bruke,
Små nøkler

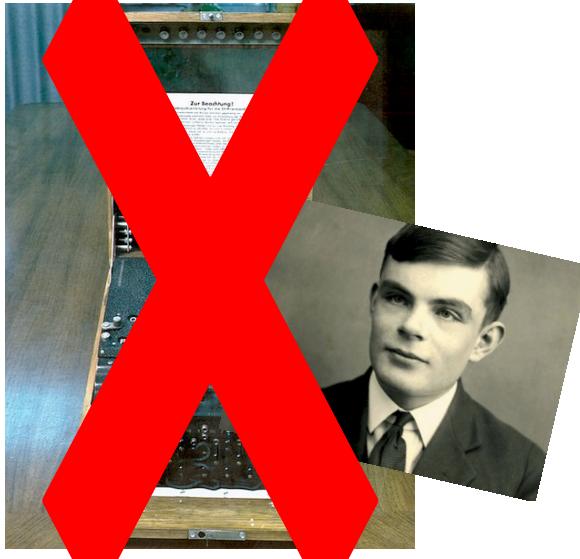
~1940

Symmetrisk Kryptografi



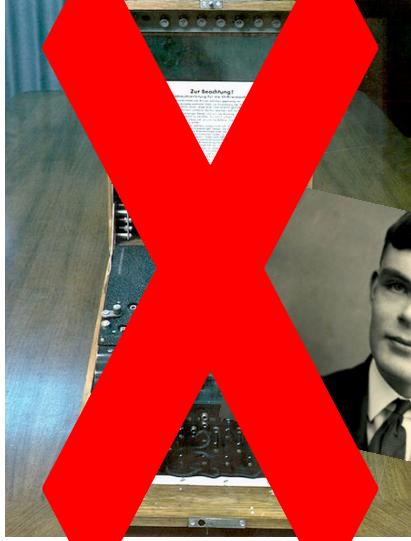
~1940

Symmetrisk Kryptografi



~1940

Symmetrisk Kryptografi



~1940



Kalde krigen

Symmetrisk Kryptografi



~1940



Kalde krigen



Made in

Symmetrisk Kryptografi



~1940

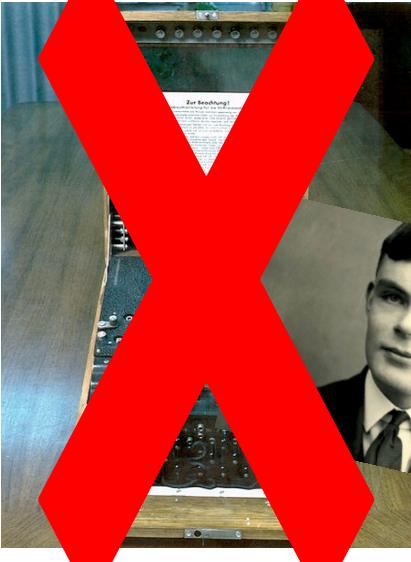


Kalde krigen



2001

Symmetrisk Kryptografi



~1940



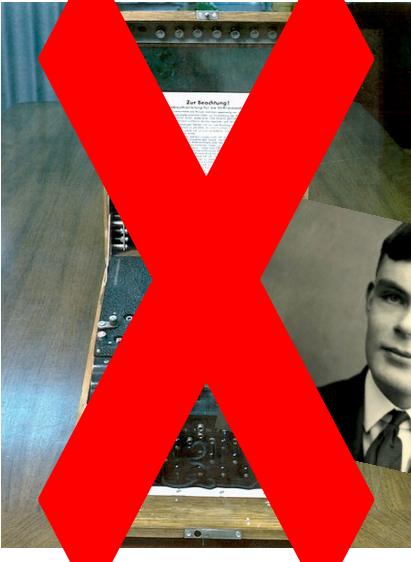
Kalde krigen

Små, forhånds-distribuerte nøkler



2001

Symmetrisk Kryptografi



~1940



Kalde krigen

Små, forhånds-distribuerte nøkler



2001

Sikker digital kommunikasjon muliggjort av matematikk!

KRYPTOGRAFI - NÅTID

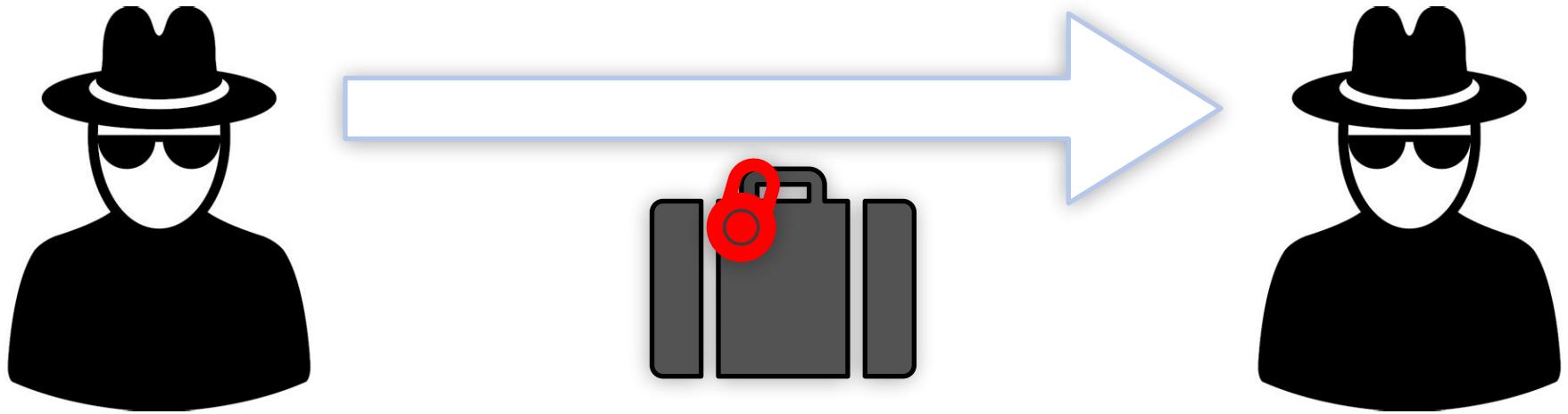
Asymmetrisk Kryptografi



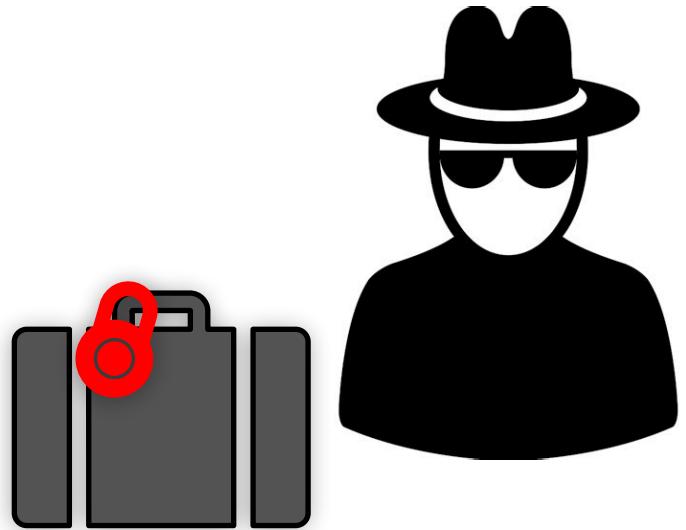
Asymmetrisk Kryptografi



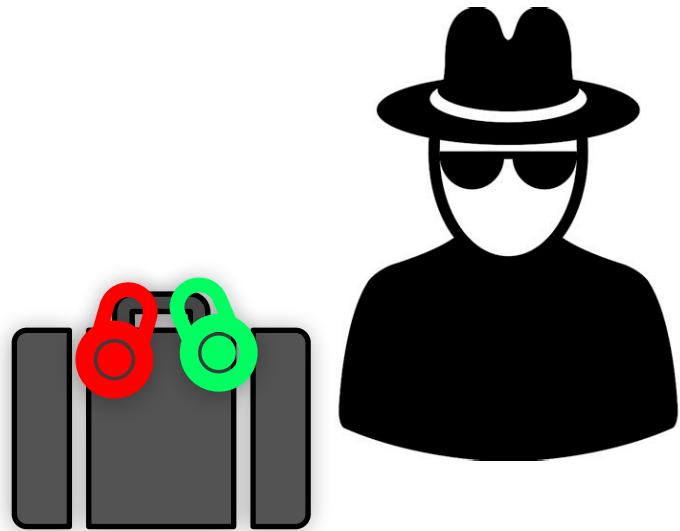
Asymmetrisk Kryptografi



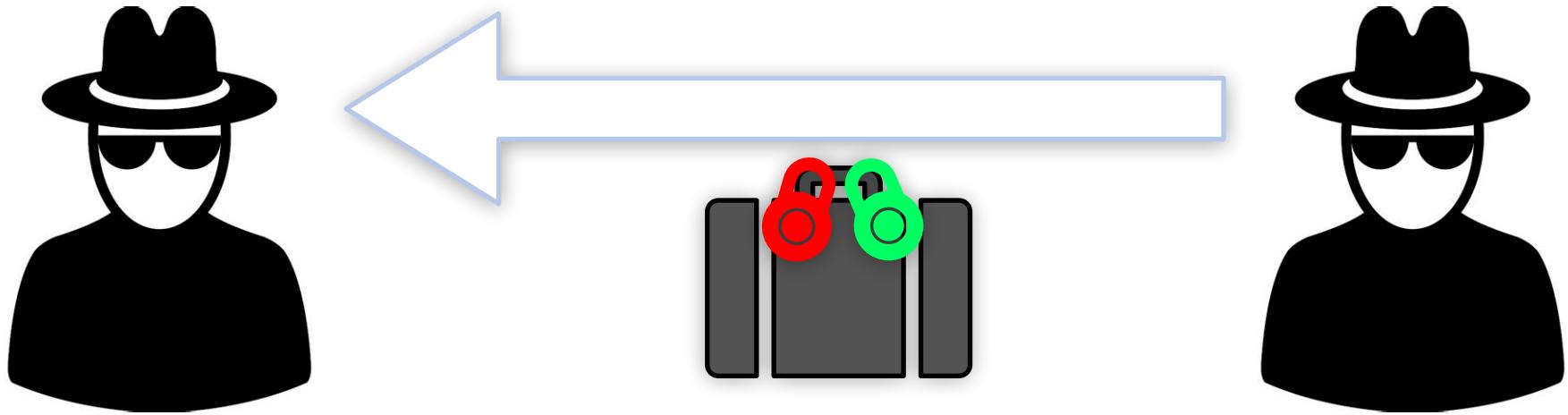
Asymmetrisk Kryptografi



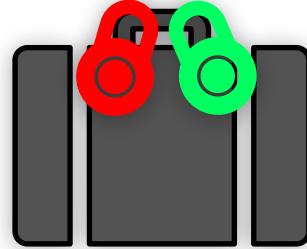
Asymmetrisk Kryptografi



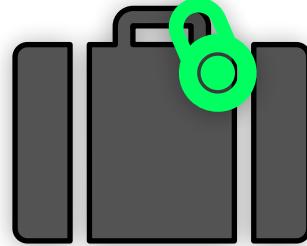
Asymmetrisk Kryptografi



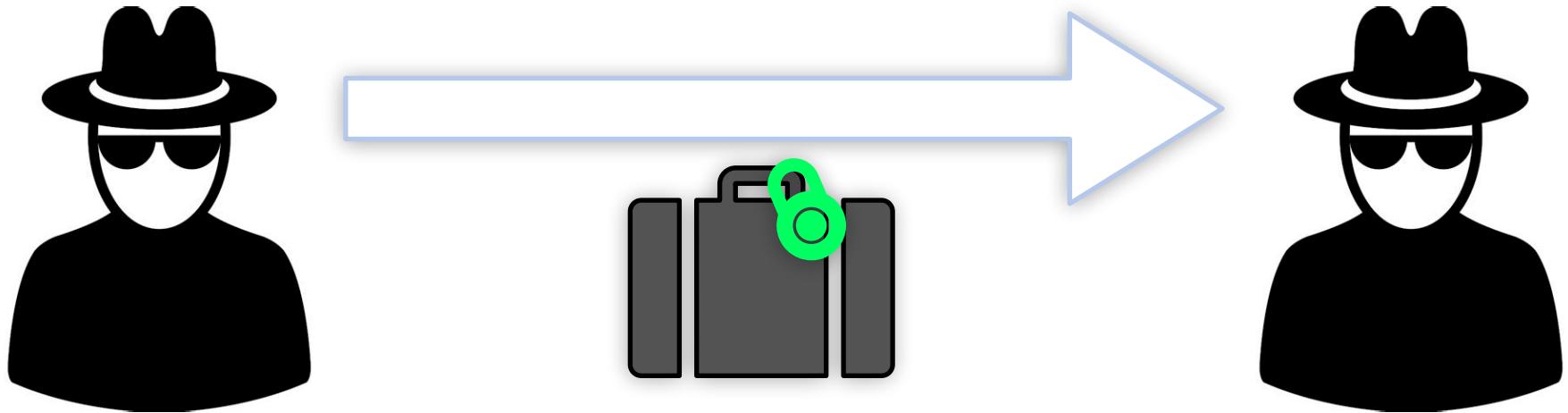
Asymmetrisk Kryptografi



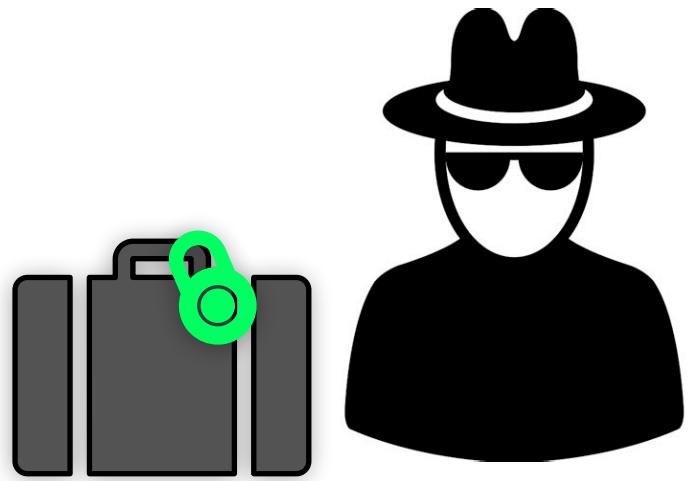
Asymmetrisk Kryptografi



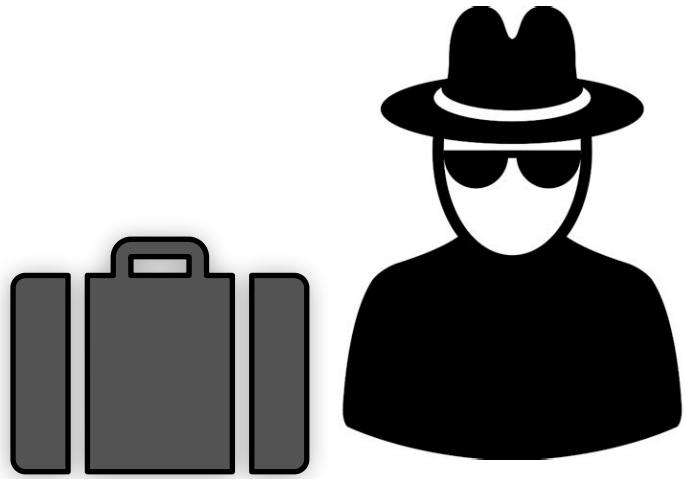
Asymmetrisk Kryptografi



Asymmetrisk Kryptografi



Asymmetrisk Kryptografi



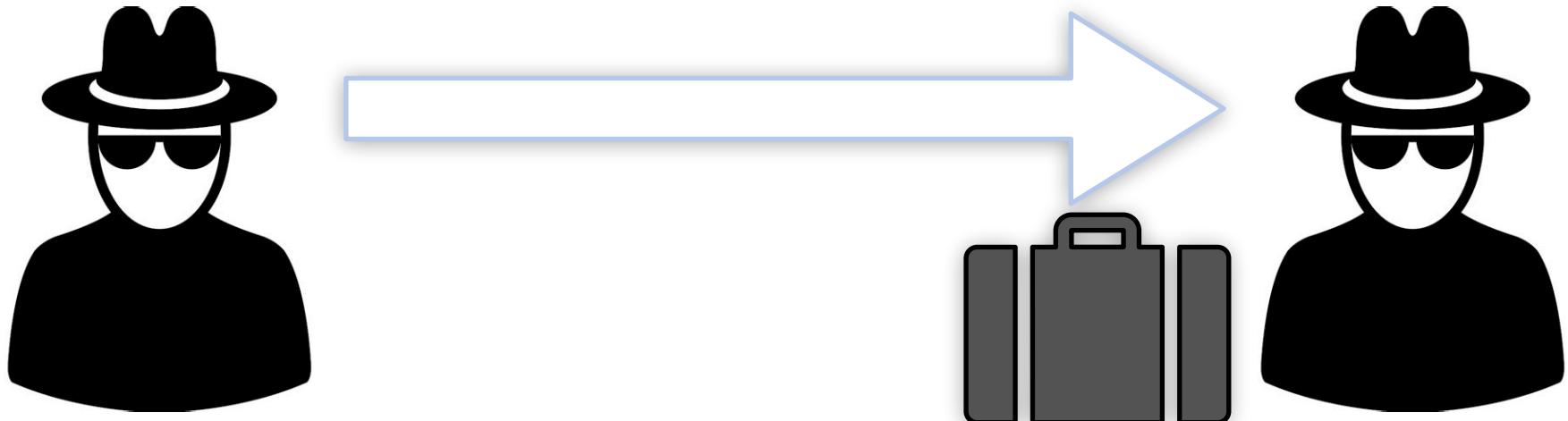
Asymmetrisk Kryptografi i virkeligheten



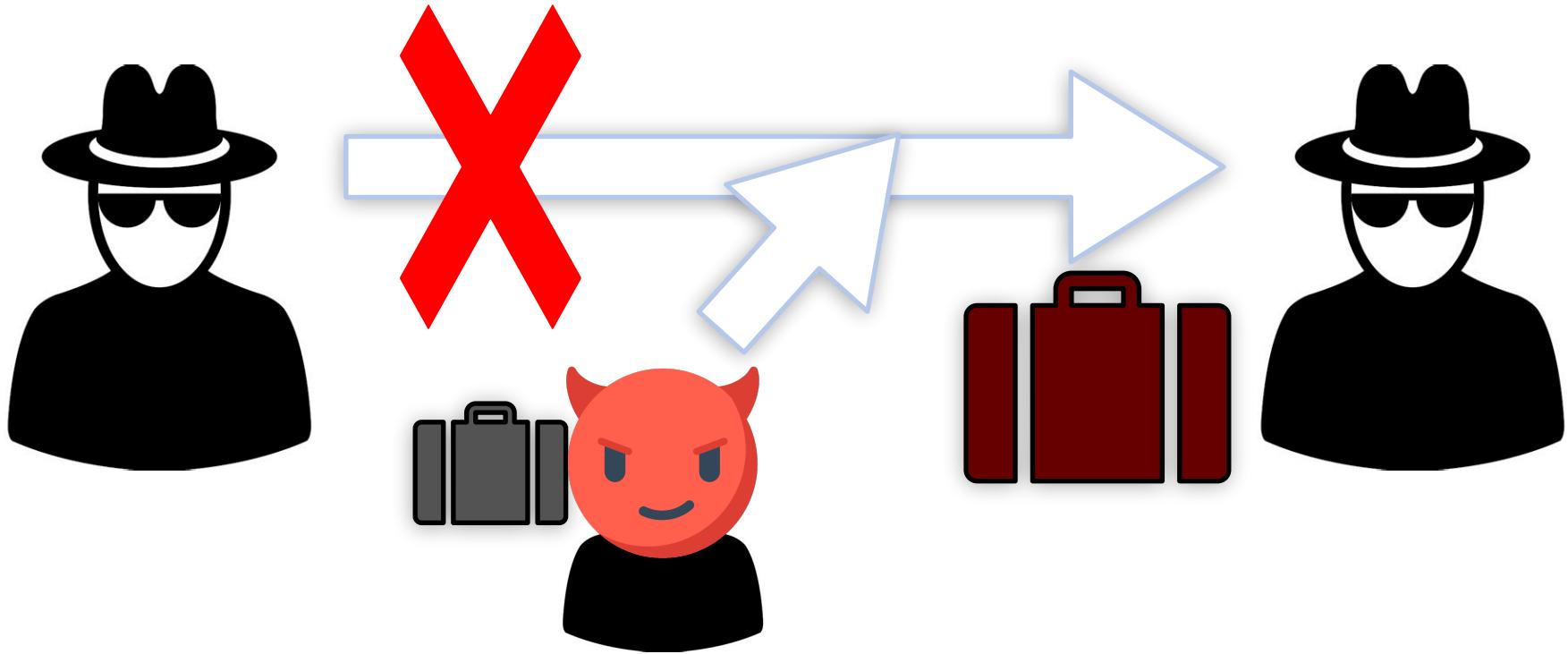
= 1 av 2 matematiske problemer

- **1. Faktorisering:**
 - **Lett:** $193 \cdot 337 = ???$
 - **Vanskelig:** $??? \cdot ??? = 65207$
- **(2. Diskret logaritmer)**

Digitale Signaturer og Meldinger



Digitale Signaturer og Meldinger



Helt essensiell del av internett

A screenshot of the NSM (Norwegian Security Museum) website. The URL `https://nsm.no/` is highlighted with a large red arrow pointing to it from the top left. The page features a dark blue header with the NSM logo and navigation links for ENGLISH, AKTUELT, and LEC. Below the header, there are three main service sections: "Digital sikkerhet" (Cybersecurity), "Personellsikkerhet" (Employee security), and "Fysisk sikkerhet" (Physical security). Each section has a circular icon and a brief description.

Getting Started | Limericks | Times | List of LaTeX mathe... | IACR Calendar of Ev... | Matematiske perler | EveryonePrint - Login | Blogs | CTF writeups | P

ENGLISH AKTUELT LEC

Digital sikkerhet

Cybersikkerhet, hendelseshåndtering, kryptosikkerhet, kommunikasjonssikkerhet, NCSC, Kryptologi og forskning, informasjonssikkerhet

Personellsikkerhet

Sikkerhetsklarering, autorisasjon, adgangsklarering, personkontroll

Fysisk sikkerhet

Objektsikkerhet, luftbårne sensorsystemer, sikringstiltak

Helt essensiell del av internett

The screenshot shows a web browser window displaying the "Page Info" for the URL <https://nsm.no/>. The browser interface includes a back/forward button, a search/address bar, and a menu bar with options like "Getting Started" and "Limericks". The main content area is a modal dialog titled "Page Info — https://nsm.no/" with tabs for General, Media, Permissions, and Security.

Website Identity

- Website: nsm.no
- Owner: This website does not supply ownership information.
- Verified by: Google Trust Services LLC [View Certificate](#)

Privacy & History

- Have I visited this website prior to today? Yes, 8 times
- Is this website storing information on my computer? Yes, cookies [Clear Cookies and Site Data](#)
- Have I saved any passwords for this website? No [View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

A question mark icon is located at the bottom right of the modal dialog.

In the background, the NTNU website is visible with sections like "Digital sikkerhet", "Cybersikkerhet", "Fysisk sikkerhet", and "Kunnskap for en bedre verden". The NTNU logo is at the bottom left.

Helt essensiell del av internett

The screenshot shows a web browser window with the URL <https://nsm.no/>. The browser interface includes a back/forward button, a search/address bar, and a menu bar with options like 'Getting Started' and 'Limericks'. Below the address bar is a navigation bar with three colored dots (red, yellow, green). The main content area displays 'Page Info — https://nsm.no/' with tabs for General, Media, Permissions, and Security. The Security tab is active, showing the following details:

Website Identity

- Website: nsm.no
- Owner: This website does not supply ownership information.
- Verified by: Google Trust Services LLC

Privacy & History

- Have I visited this website prior to today? Yes, 8 times
- Is this website storing information on my computer? Yes, cookies
- Have I saved any passwords for this website? No

Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Digital sikk

Cybersikke
hendelseshånd

kryptosikke

kommunikasjonssik

Kryptologi og fo
informasjonss

Fysisk sikkerhet

Objektsikkerhet, luftbårne
ensorsystemer, sikringstiltak

Helt essensiell del av internett

Page Info — <https://nsm.no/>

General Media Permissions Security

Website Identity

Website: nsm.no
Owner: This website does not supply ownership information.
Verified by: Google Trust Services LLC [View Certificate](#)

Privacy & History

Have I visited this website prior to today? Yes, 8 times
Is this website storing information on my computer? Yes, cookies [Clear Cookies and Site Data](#)
Have I saved any passwords for this website? No [View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Helt essensiell del av internett

Subject Alt Names

DNS Name	nsm.no
DNS Name	*.nsm.no

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	BD:5C:29:E9:05:AE:0A:F2:4C:C5:8B:76:36:01:B5:1D:C6:84:C4:F0:E0:5E:0...

Helt essensiell del av internett

Subject Alt Names

DNS Name	nsm.no
DNS Name	*.nsm.no

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	BD:5C:29:E9:05:AE:0A:F2:4C:C5:8B:76:36:01:B5:1D:C6:84:C4:F0:E0:5E:0...

Kan du faktorisere dette tallet kan du
utgi deg for å være *.nsm.no



De underliggende problemene....



= 1 av 2 matematiske problemer

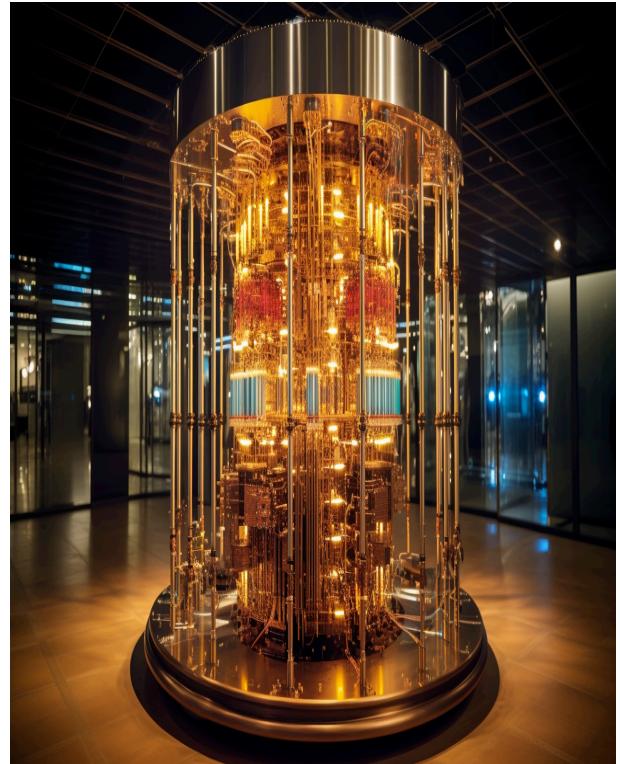
- 1. Faktorisering:
 - **Lett:** $193 \cdot 337 = ???$
 - **Vanskelig:** $??? \cdot ??? = 65207$
- (2. Diskret logaritmer)

De underliggende problemene....



= 1 av 2 matematiske problemer

- 1. Faktorisering:
 - **Lett:** $193 \cdot 337 = ???$
 - **Lett:** $??? \cdot ??? = 65207$
- (2. Diskret logaritmer) (**Lett**)



Kvantemaskiner???



Bits: 011101000101010000010111...

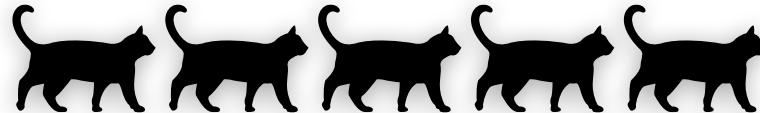
Kvantemaskiner???



Bits: 011101000101010000010111...



Qubits:



Kan kvantemaskiner bli realitet?



Physics Mathematics Biology Computer Science Topics



QUANTUM COMPUTING

New Algorithm Closes Quantum Supremacy Window

HARDWARE > QUANTUM | April 25, 2023 | updated 17 May 2023 8:36am

Investment in quantum technology hit a record \$2.35bn last year

Real quantum computers.
Right at your fingertips.

Kvantemaskiner store nok til å knekke dagens kryptografi er **5** år unna

Kan kvantemaskiner bli realitet?



Physics Mathematics Biology Computer Science Topics



IBM Quantum

QUANTUM COMPUTING

New Algorithm Closes Quantum Supremacy Window

HARDWARE > QUANTUM | April 25, 2023 | updated 17 May 2023 8:36am

Investment in quantum technology hit a record \$2.35bn last year

Real quantum computers.
Right at your fingertips.

Kvantemaskiner store nok til å knekke dagens kryptografi er **30** år unna

Kan kvantemaskiner bli realitet?



Physics Mathematics Biology Computer Science Topics



QUANTUM COMPUTING

New Algorithm Closes Quantum Supremacy Window

HARDWARE > QUANTUM | April 25, 2023 | updated 17 May 2023 8:36am

Investment in quantum technology hit a record \$2.35bn last year

Real quantum computers.
Right at your fingertips.

Kvantemaskiner store nok til å knekke dagens kryptografi er **0** år unna

Kan kvantemaskiner bli realitet?



Physics Mathematics Biology Computer Science Topics



QUANTUM COMPUTING

New Algorithm Closes Quantum Supremacy Window

HARDWARE > QUANTUM | April 25, 2023 | updated 17 May 2023 8:36am

Investment in quantum technology hit a record \$2.35bn last year

Real quantum computers.
Right at your fingertips.

Kvantemaskiner store nok til å knekke dagens kryptografi er ∞ år unna

Morgendagens kryptografi

EN KVANTESIKKER FREMTID

Kvantesikker Kryptografi



= nye matematiske problemer

- **Gitter (Latticer) ?**
- **Isogenier !?**
- **Feil-korrigende koder ?!**
- **Flervariabe ligninger ??**
-

Nye standarder på vei!



Kvantesikker Kryptografi



= nye matematiske problemer

- **Gitter (Latticer) ?**
- **Isogenier !?**
- **Feil-korrigende koder ?!**
- **Flervariabe ligninger ??**
-

Nye standarder på vei!



Not an International STandard

Kvantesikker Kryptografi



= nye matematiske problemer

- **Gitter (Latticer) ?**
- **Isogenier !?**
- **Feil-korrigende koder ?!**
- **Flervariabe ligninger ??**
-

Nye standarder på vei!



Not an International Standard



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



FakeIACR @FakeIACR · Jun 20



Når må man over på ny kryptografi?

- **X** = Antall år konfidensiell informasjon må holdes hemmelig

Når må man over på ny kryptografi?

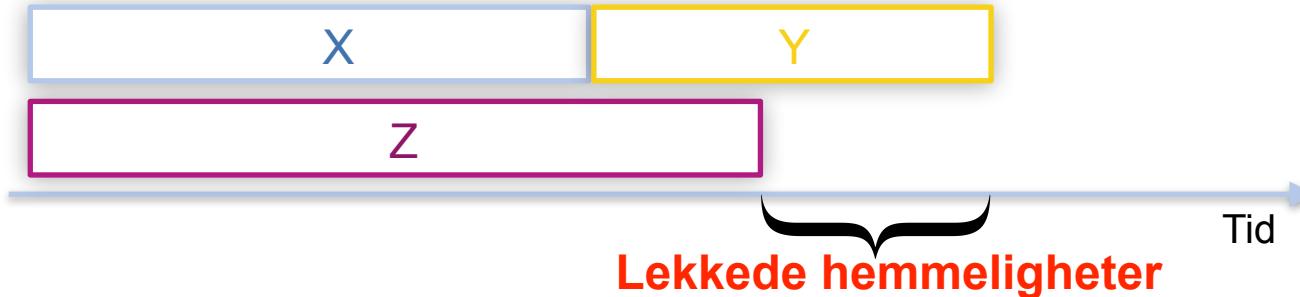
- **X** = Antall år konfidensiell informasjon må holdes hemmelig
- **Y** = Antall år før kvantesikker krypto kan integreres i systemet ditt

Når må man over på ny kryptografi?

- **X** = Antall år konfidensiell informasjon må holdes hemmelig
- **Y** = Antall år før kvantesikker krypto kan integreres i systemet ditt
- **Z** = Antall år før en fullskala kvantemaskin finnes

Når må man over på ny kryptografi?

- **X** = Antall år konfidensiell informasjon må holdes hemmelig
- **Y** = Antall år før kvantesikker krypto kan integreres i systemet ditt
- **Z** = Antall år før en fullskala kvantemaskin finnes
- **Teorem (Moscha):**
Hvis $X + Y > Z$ er det på tide å bli bekymret!



Hva om kvantemaskiner aldri kommer?



Physics Mathematics Biology Computer Science Topics



IBM Quantum

QUANTUM COMPUTING

New Algorithm Closes Quantum Supremacy Window

HARDWARE > QUANTUM | April 25, 2023 | updated 17 May 2023 8:36am

Investment in quantum technology hit a record \$2.35bn last year

Real quantum computers.
Right at your fingertips.

Kvantemaskiner store nok til å knekke dagens kryptografi er ∞ år unna

Hva om kvantemaskiner aldri kommer?



Physics Mathematics Biology Computer Science Topics



IBM Quantum

QUANTUM COMPUTING

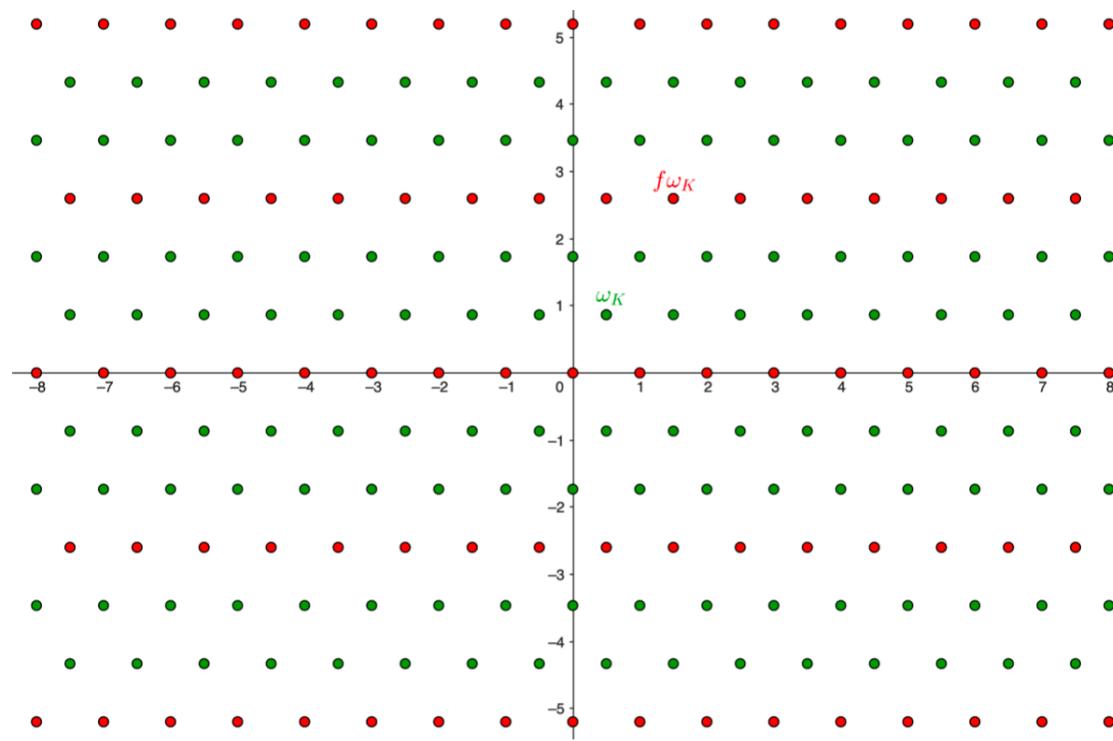
New Algorithm Closes Quantum Supremacy Window

HARDWARE > QUANTUM | April 25, 2023 | updated 17 May 2023 8:36am

Investment in quantum technology hit a record \$2.35bn last year

Real quantum computers.
Right at your fingertips.

Kvantemaskiner store nok til å knekke dagens kryptografi er ∞ år unna
Spiller ingen rolle, alle må over på nye standarder etterhvert



Tusen takk!

Epost: jonathan.k.eriksen@ntnu.no

Nettside: jonathke.github.io