NTNU | Norwegian University of Science and Technology

Sikker autentisering i en kvanteverden

Tjerand Silde – 21. September, 2022

Hvor lang tid tar det å knekke?

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years

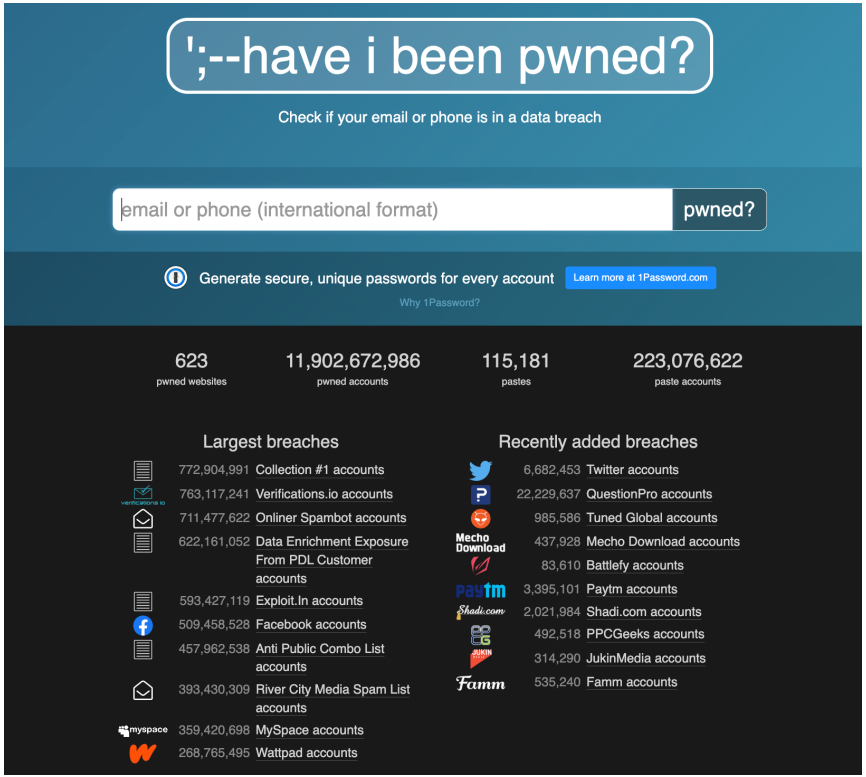
Hvor lang tid tar det å knekke?

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

De mest populære passordene...

RANK	PASSWORD	TIME TO CRACK IT
1	**123456**	< 1 Second
2	**123456789**	< 1 Second
3	**12345**	< 1 Second
4	**qwerty**	< 1 Second
5	**password**	< 1 Second
6	**12345678**	< 1 Second
7	**111111**	< 1 Second
8	123123	< 1 Second

Store passord-databaser på nett



NSM sine anbefalinger

NSMs anbefaling for virksomheter:

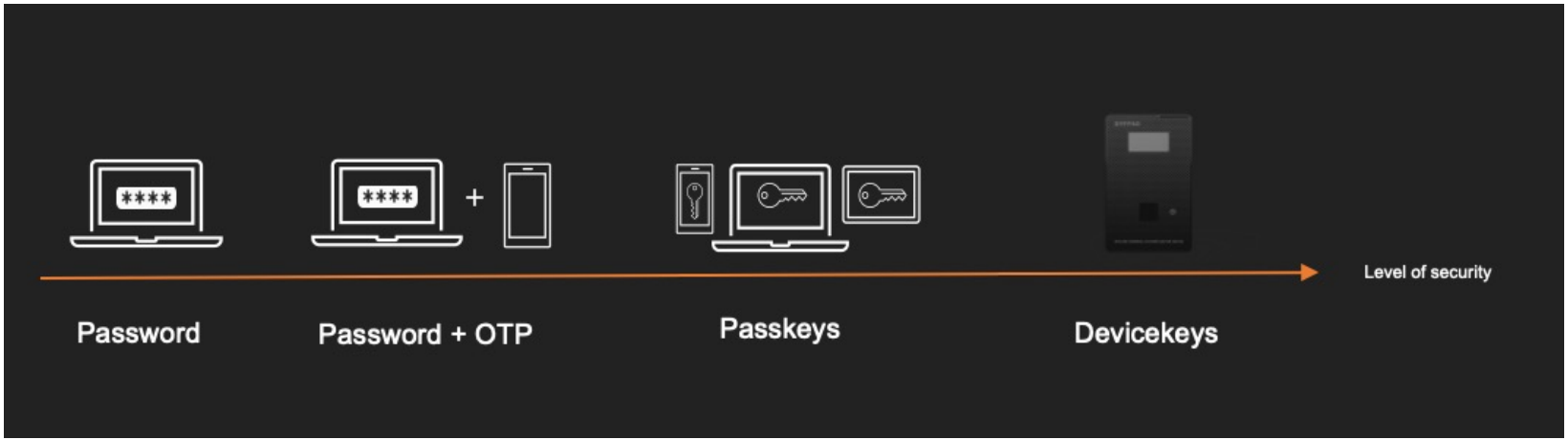
- Innfør to-faktor autentisering
- Unngå at passord lagres i klartekst
- Innfør rutiner for å kontrollere nye passord mot mye brukte og kompromitterte passord
- Innfør rutiner for å bytte standardpassord på nytt utstyr
- Gi brukere som trenger administratorrettigheter to kontoer

Det finnes også tjenester som https://haveibeenpwned.com/ der domeneeiere og IT-administratorer kan få varsler dersom en epost-adresse i domenet dukker opp i en lekkasje.

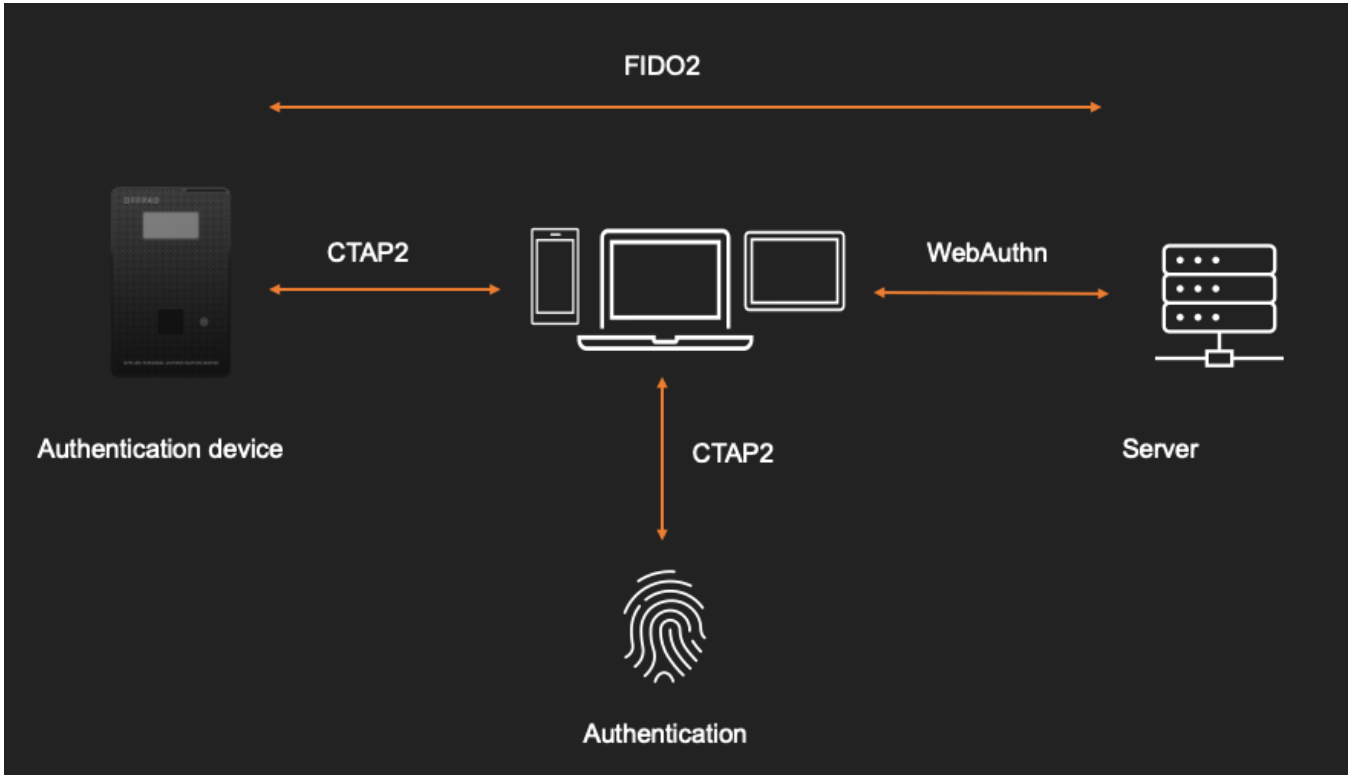
NSMs anbefaling for enkeltindivider:

- Bruk to-faktor autentisering der det tilbys
- Bruk unike passord
- Bruk passordhåndteringsprogrammer
- Privat kan du også lage en passordliste med penn og papir, men beskytt dokumentet som et verdipapir
- Alltid bytt standardpassord på produktene du kjøper

Sikker autentisering

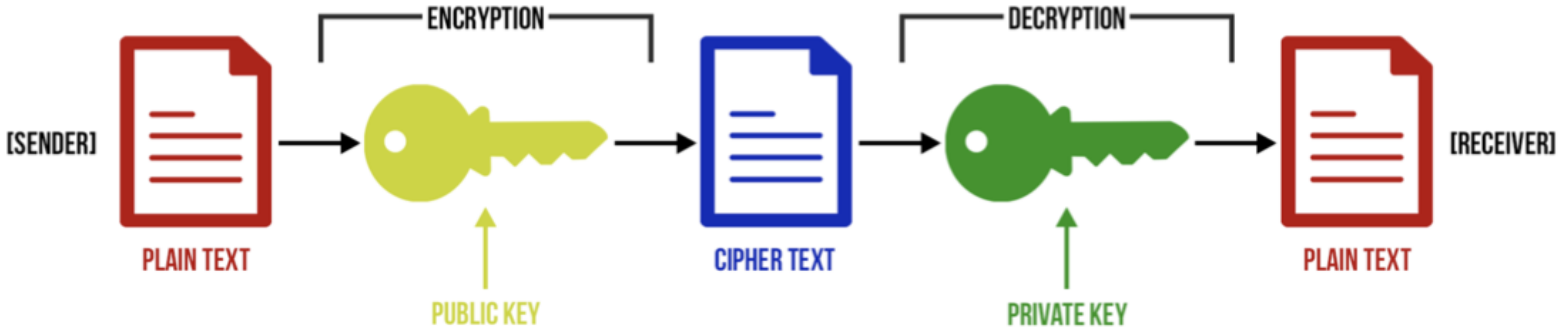


FIDO Økosystemet

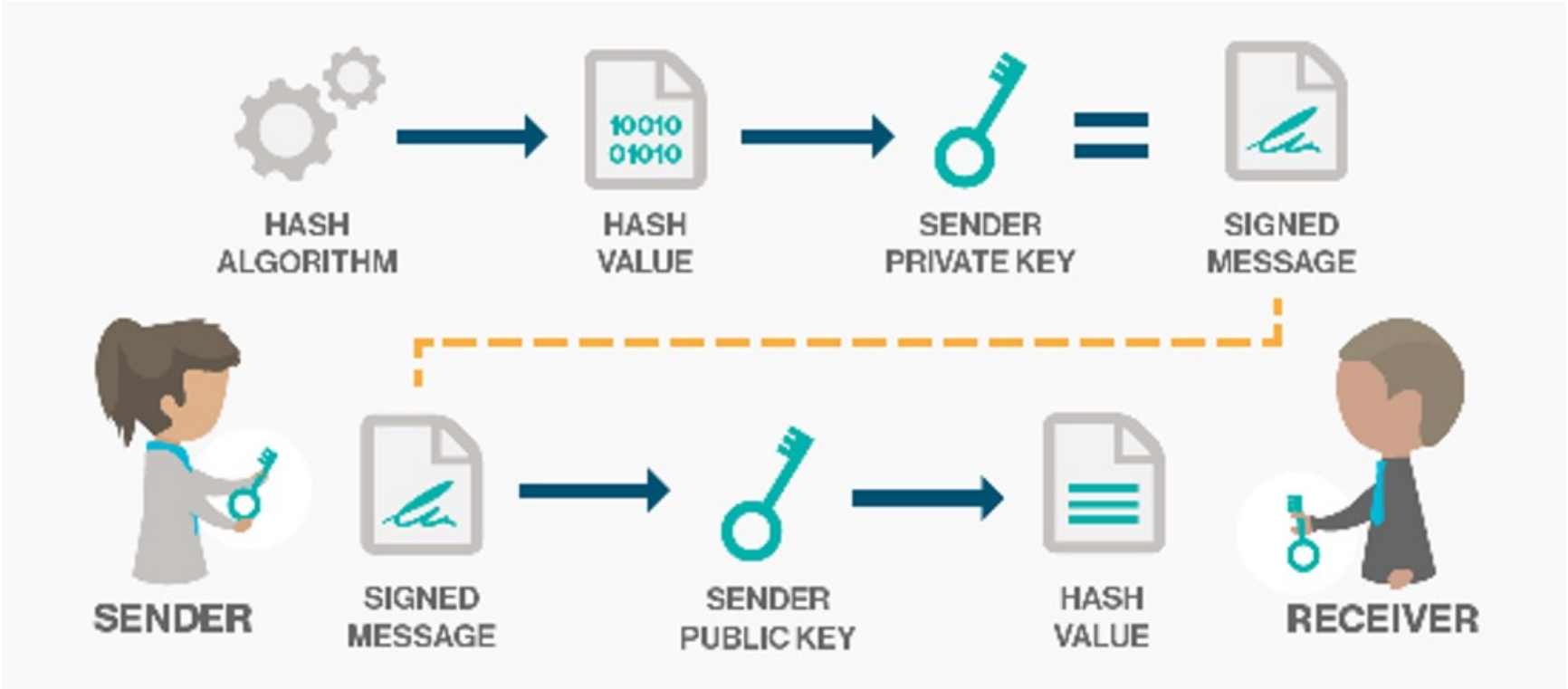


Symmetrisk-nøkkel kryptering

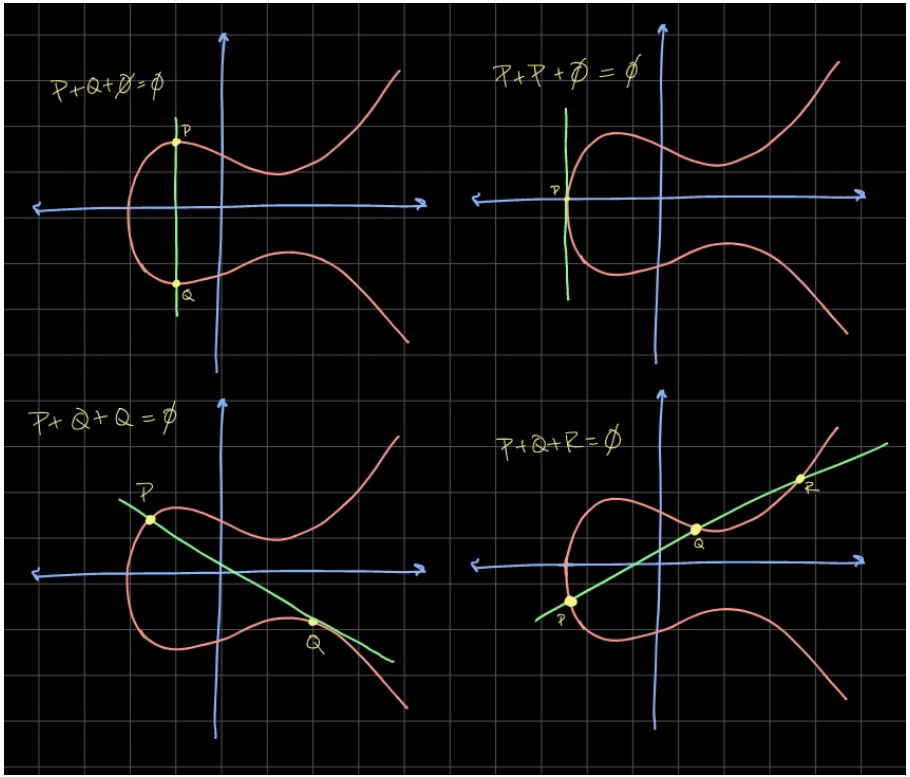
Offentlig-nøkkel kryptering



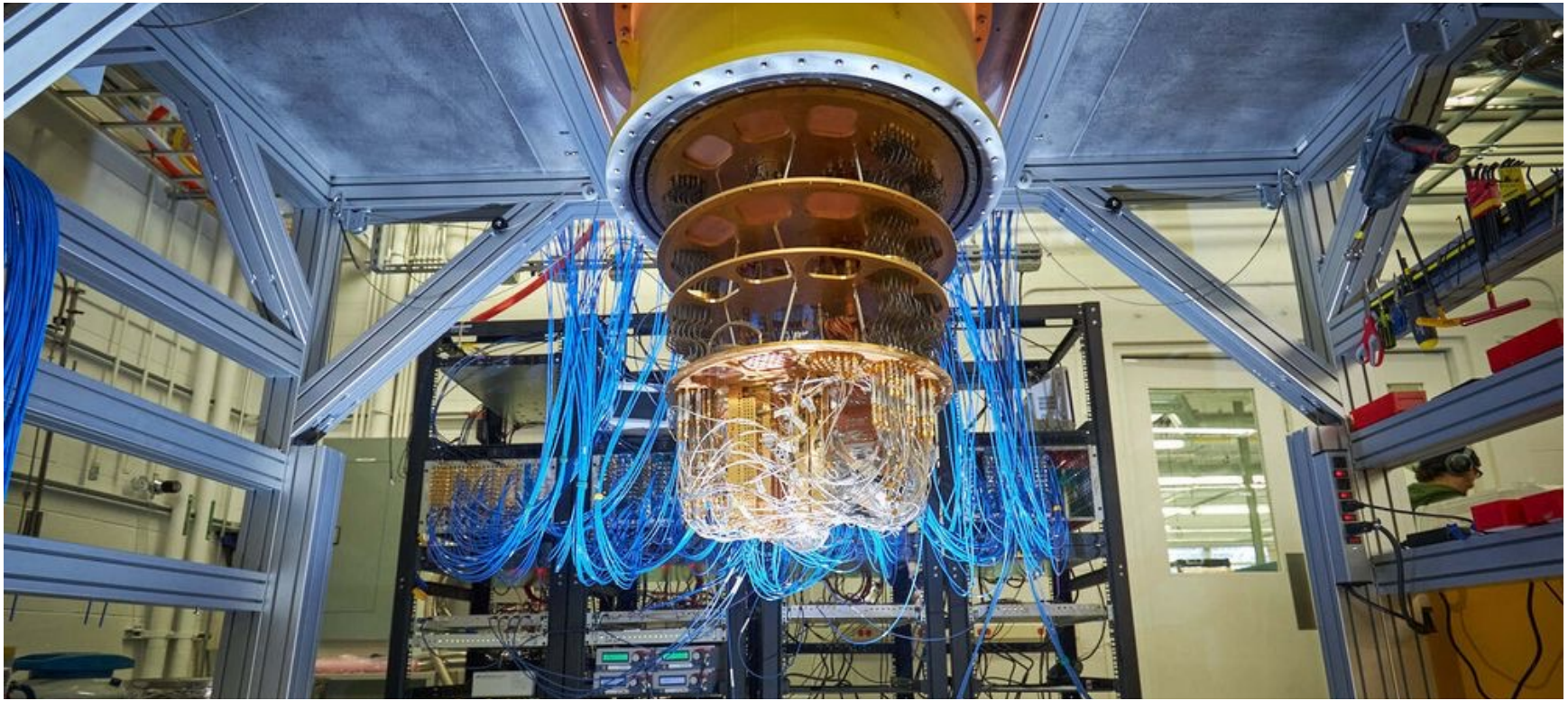
Digitale signaturer



I dag: Elliptiske kurver

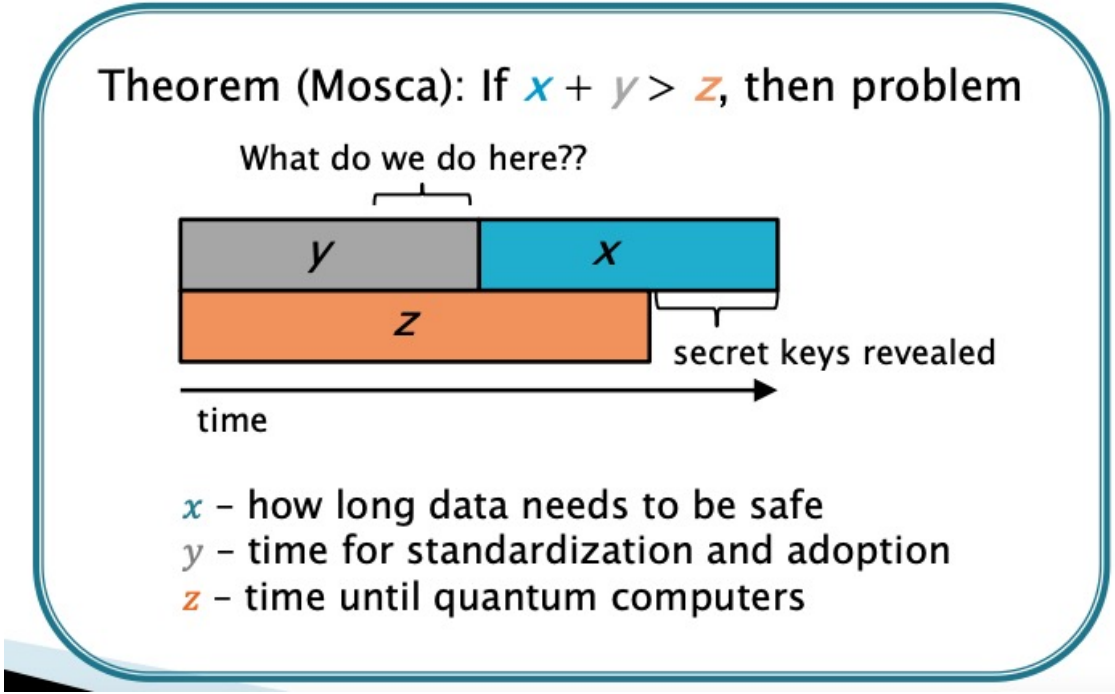


Kvantedatamaskinene er på vei!



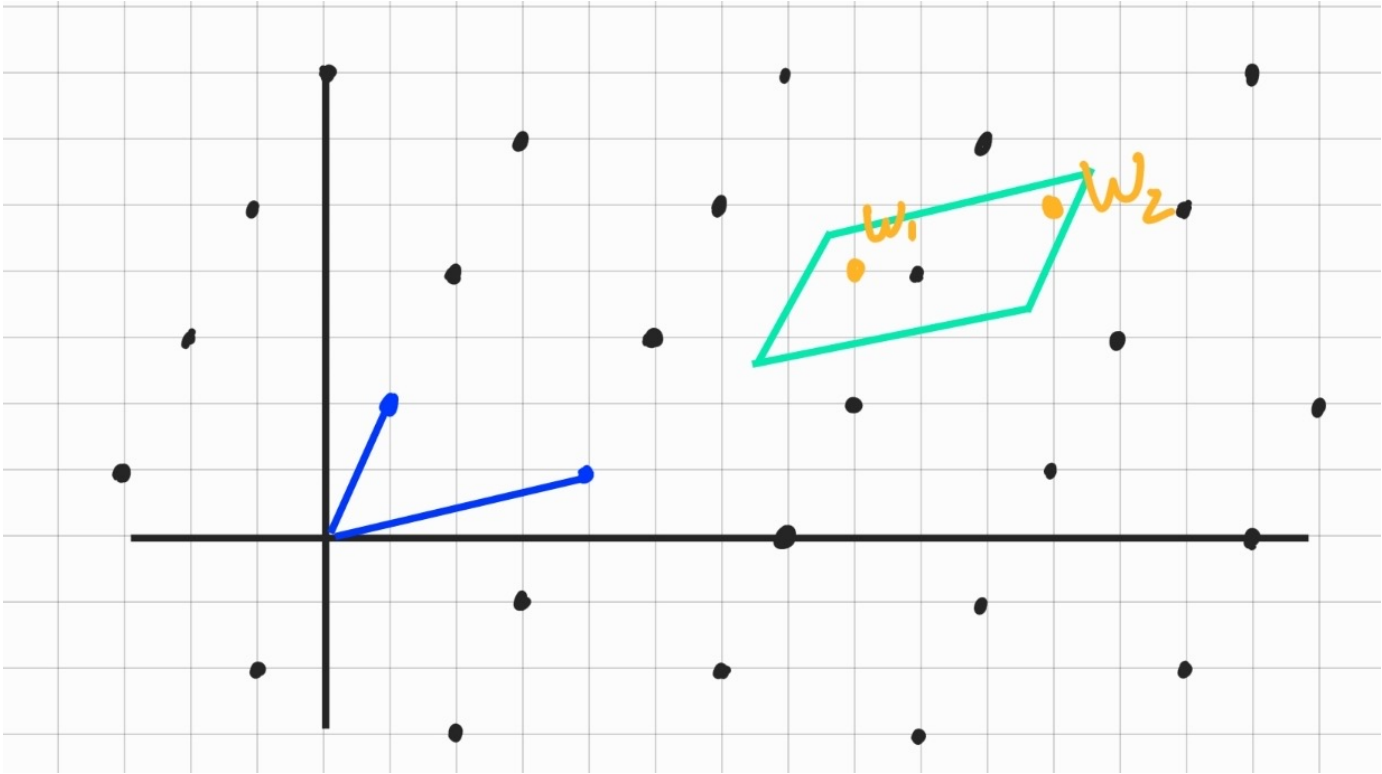
Krypterte kanaler på internett

Levetid for databeskyttelse



PQC standardisering

I morgen: gitter-basert kryptografi



Takk! Spørsmål?

Epost: tjerand.silde@ntnu.no
Web: tjerandsilde.no