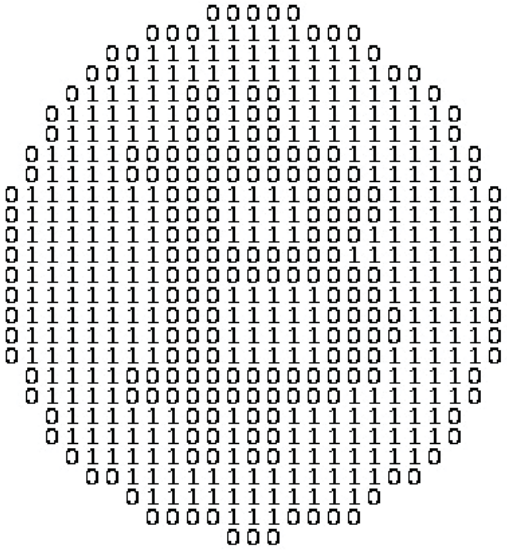
Cryptografische beveiliging op het Internet



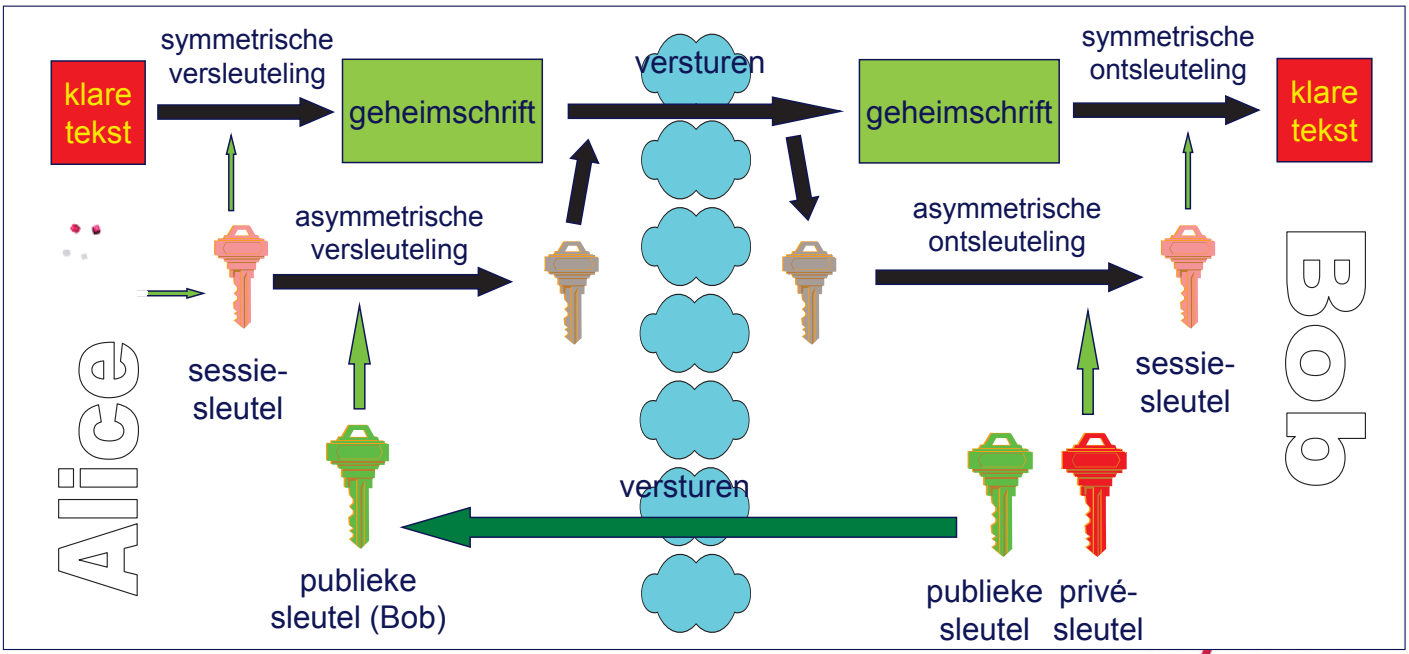
Benne de Weger
b.m.m.d.weger@tue.nl

augustus 2018

TU/e Technische Universiteit Eindhoven University of Technology

Where innovation starts

hybride cryptografie



TU/e Technische Universiteit Eindhoven University of Technology

TLS-protocol

wat gebeurt er als je naar een beveiligde website gaat

beveiligd = https:// in plaats van http://

handenschud-protocol, doelen:

- **authenticatie van de website**
- **klaarzetten van sleutels**

daarna wordt al het verkeer met de website

- **symmetrisch versleuteld**
- **symmetrisch geauthenticeerd (hash met sleutel)**

het TLS-protocol

publieke sleutel van de webserver

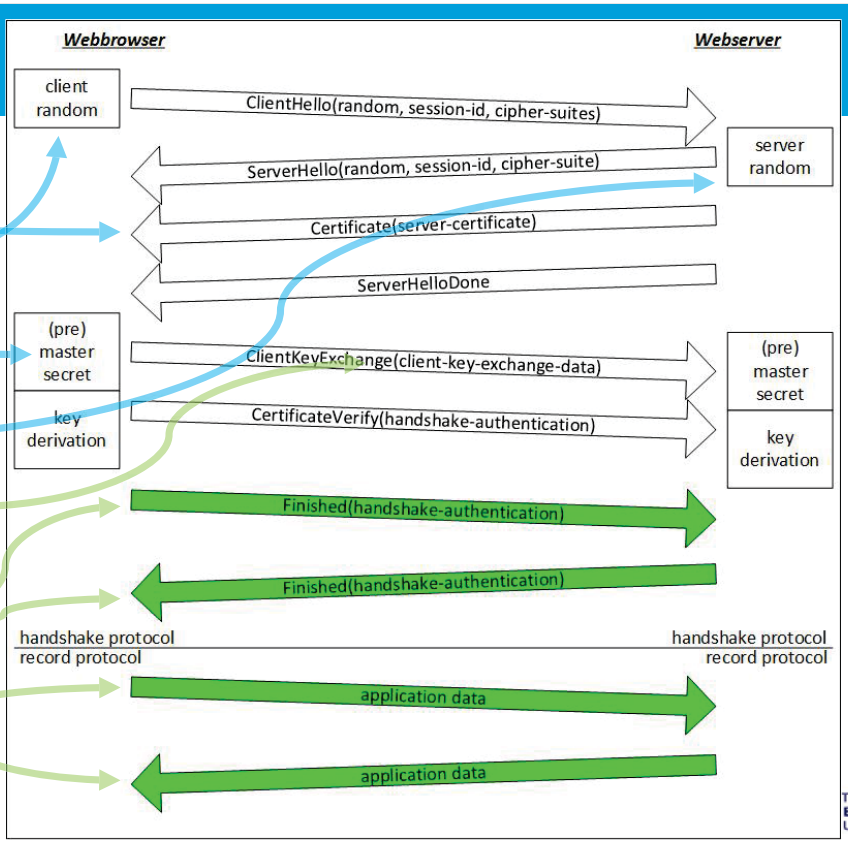
randomness van de webbrowser

randomness van de webserver

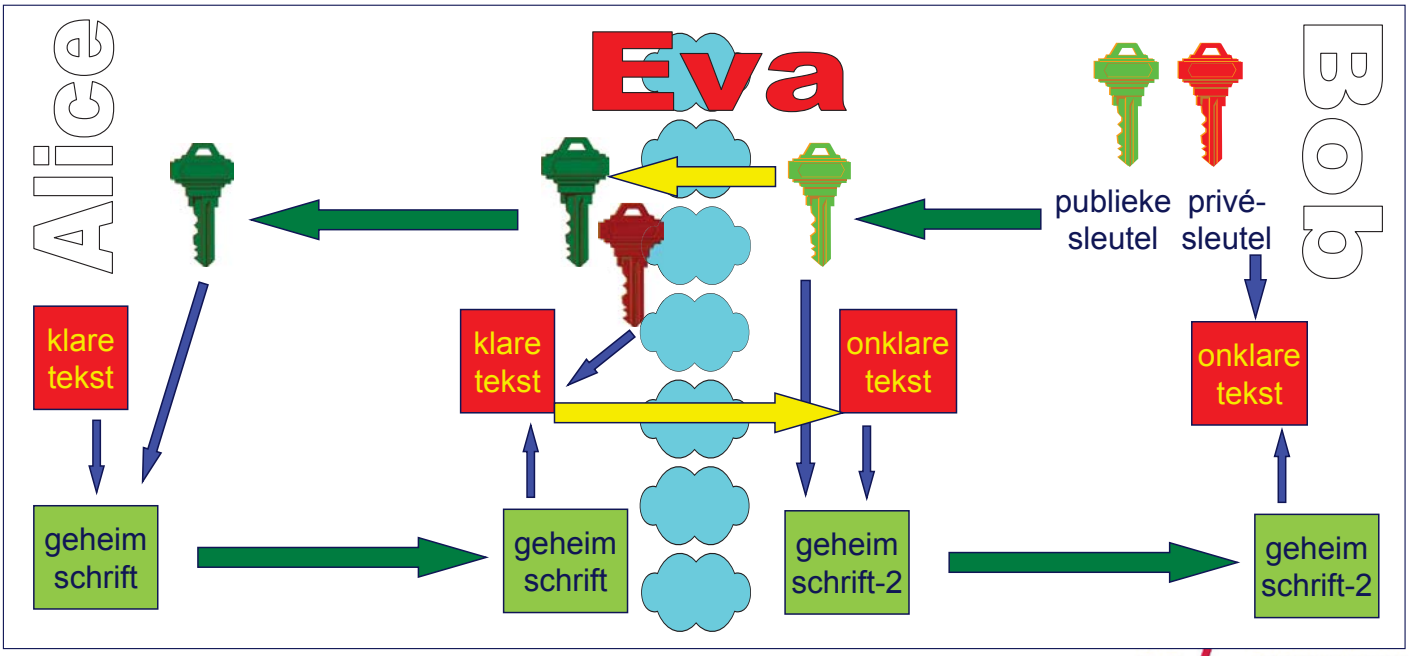
asymmetrisch versleuteld

handtekening over alle berichten, symmetrisch versleuteld

symmetrisch versleuteld en geauthenticeerd



de "mens in het midden"



PKI - Public Key Infrastructure

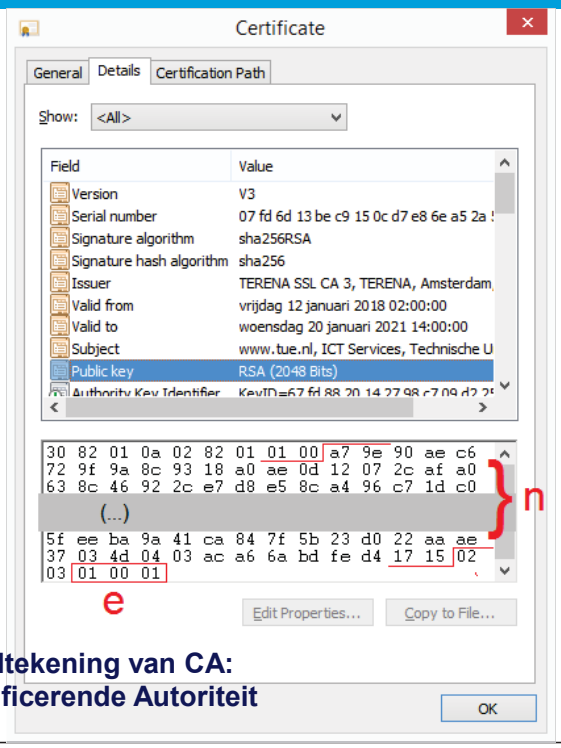
hoe weet Alice zeker dat de publieke sleutel die ze krijgt wel van Bob is?

wat nodig is, is *authenticatie van publieke sleutels*

PKI verzorgt dat

belangrijkste concept: *certificaat*

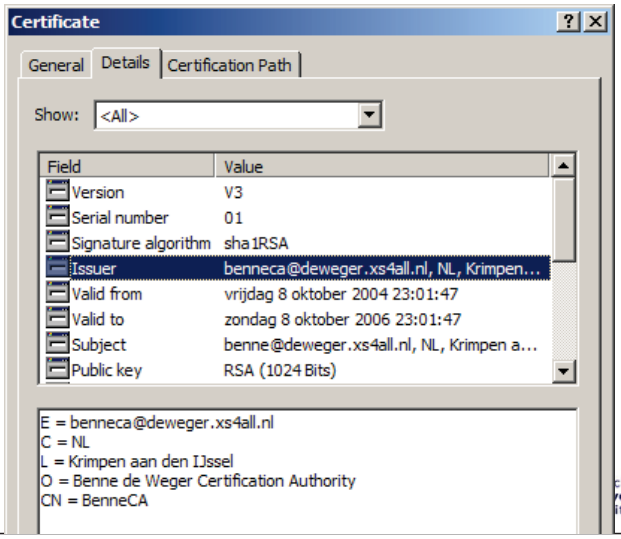
certificaat van www.tue.nl



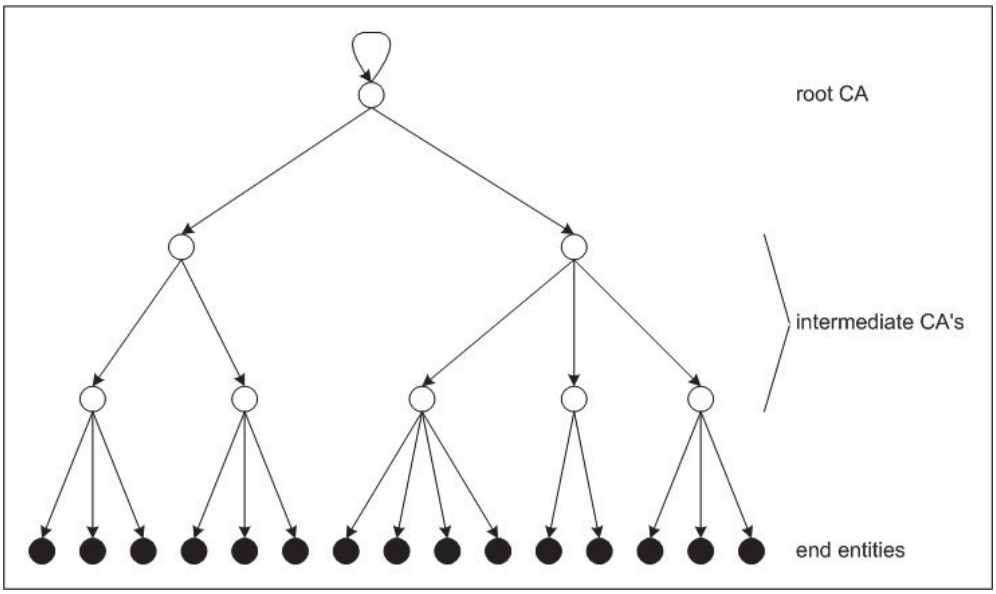
handtekening van CA:
Certificerende Autoriteit

certificaten kun je in je browser makkelijk vinden

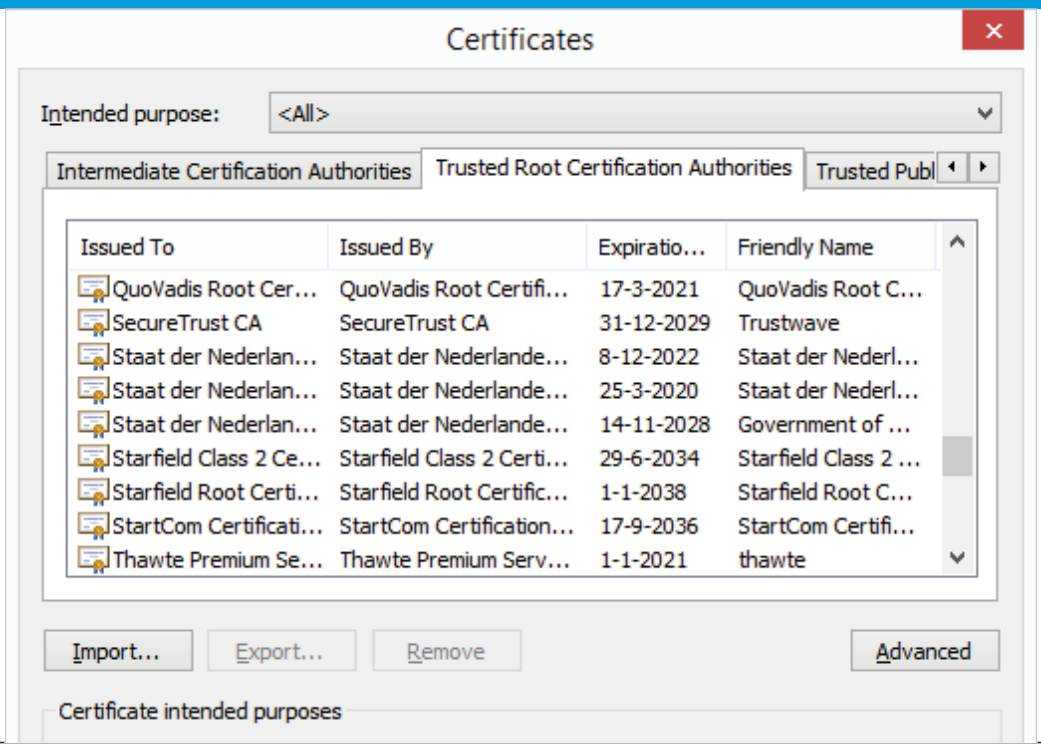
of zelf maken



X.509 hierarchie



waarom zou je die vertrouwen?



omdat Bill Gates dat zegt...

de DigiNotar-affaire

DigiNotar - Nederlandse Certification Authority

- **verzorgde certificaten voor de overheid**

gehackt in 2011

- **privé-sleutel niet gelekt**
- **maar was wel toegankelijk voor hackers**
- **nepcertificaten verspreid: *.google.com**

target was kennelijk Iran

DigiNotar binnen enkele weken failliet

HSM - hardware security module

de Rogue-CA-aanval

MD5 is een hashfunctie, veelgebruikt in certificaten

MD5 is niet meer botsingbestendig:

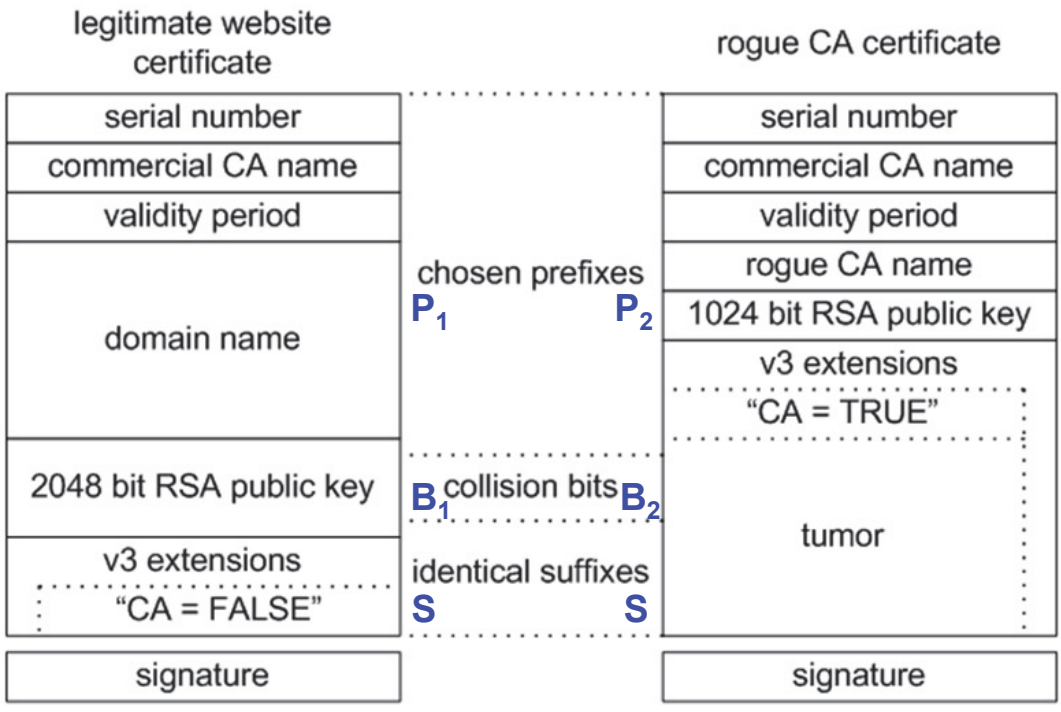
Wang (2004) - Stevens (2008)

- **mogelijk om botsingen te maken van de volgende vorm:**
- **kies zelf twee beginstukken P_1, P_2**
- **bereken botsingcodes B_1, B_2**
- **kies zelf eindstuk S**
- **dan MD5($P_1||B_1||S$) = MD5($P_2||B_2||S$)**

gebruikt om handtekening van echte CA te "stelen"

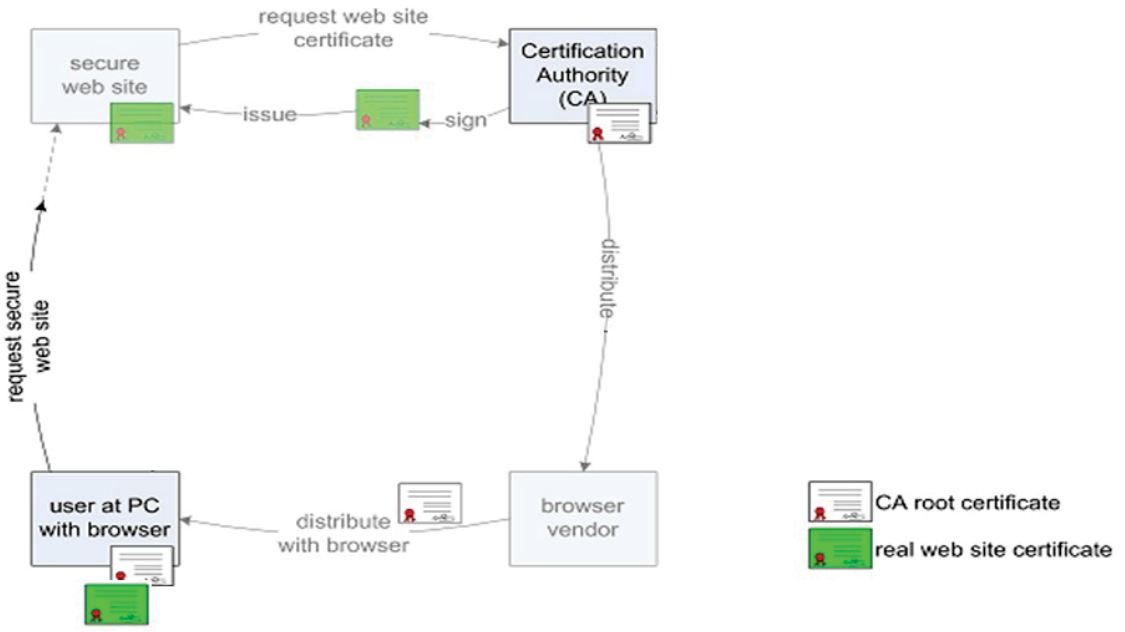
cluster van 200 PlayStations (EPFL Lausanne)

de "botsende" certificaten

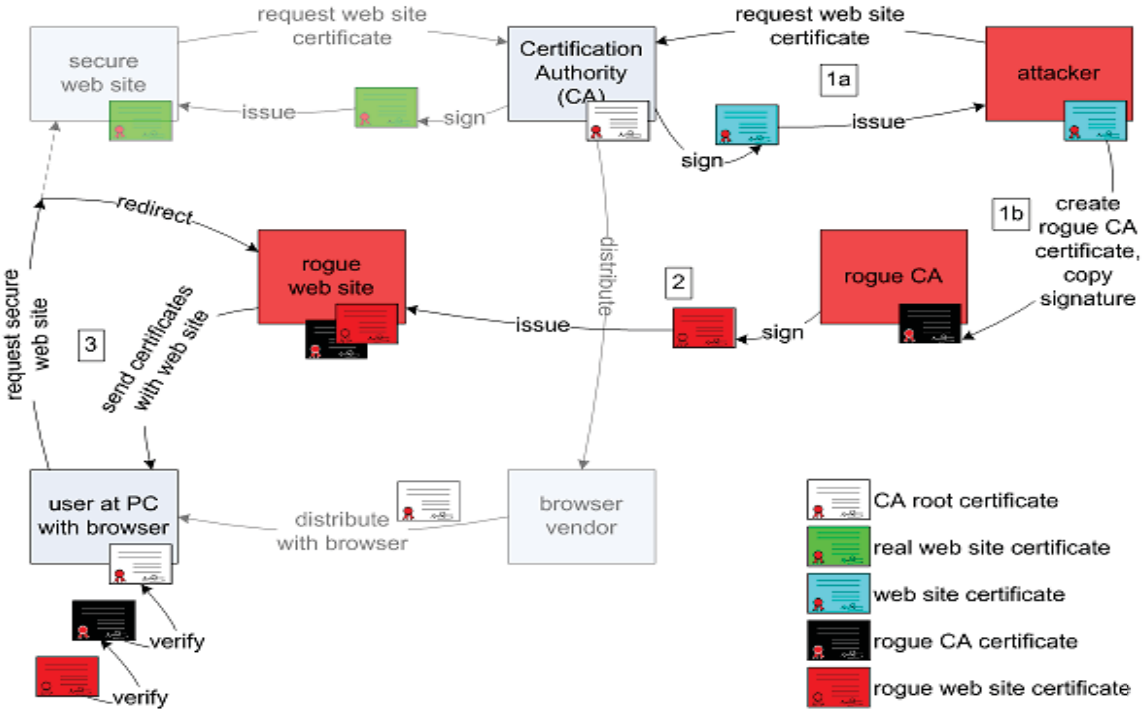


Technische Universiteit Eindhoven University of Technology

hoe het veilige Internet hoort:



hoe wij het veilige Internet in principe "ownden"



Quantum - de toekomst?

- instantaan parallel rekenen met qubits
  - n bits kunnen 2^n mogelijke toestanden hebben
  - klassieke bits: kunnen in slechts 1 toestand tegelijk zijn
  - quantum bits: kunnen in alle 2^n toestanden tegelijk zijn (superpositie)
- operaties op qubits: quantum-logica
  - slechts specifieke algoritmen zijn mogelijk
  - Shor's algoritme: ontbinden in priemfactoren, en ook discrete logaritmen, kunnen razend snel (polynomiaal i.p.v. exponentieel)
  - Grover's algoritme: zoeken in lijst van grootte n kan in tijd $n^{1/2}$

negatieve gevolgen

- symmetrische cryptografie (sleutellengte k bits):
  - brute kracht-aanval in tijd $2^{k/2}$
  - sleutellengtes dus verdubbelen (256 i.p.v. 128)
  - geen erg groot probleem
- asymmetrisch:
  - de meeste nu gebruikte systemen zijn totaal gebroken:
    - op ontbinden in factoren gebaseerd: RSA
    - op discrete logaritmen gebaseerd: Diffie-Hellman, DSA
    - op elliptische krommen gebaseerde systemen zijn nog veel kwetsbaarder door hun korte sleutellengtes
  - heel erg groot probleem

positieve gevolgen

- QKD: quantum key distribution
  - qubit = bit + codering
  - Alice kiest random bits en random coderingen
  - Alice stuurt Bob qubits maar niet de coderingen
  - Bob meet met behulp van random coderingen
  - Alice en Bob gebruiken klassiek kanaal om coderingen uit te wisselen, houden alleen de bits met gelijke codering
- quantum veiligheid
  - meten van een qubit (gecodeerd bit) verandert het
  - afluisteraar ziet foute qubits
  - mens in het midden: kan nog steeds!
    - klassieke kanaal is niet vertrouwelijk
      maar moet wel geauthenticeerd worden

QKD hype: “onbreekbare crypto”

- afluisteren wordt altijd ontdekt, maar:
  - klassieke authenticatie nog steeds nodig
  - kan alleen over directe optische kabel
    - lengte beperkt (150km)
- QKD lost dus niet de problemen op die quantum cryptanalyse veroorzaakt

Post-Quantum Cryptography

- klassieke cryptografie gebaseerd op moeilijke problemen die ook voor quantum computers moeilijk zijn
- vier richtingen worden nu intensief onderzocht
  - *op roosters gebaseerde* cryptografie (NTRU, NewHope)
  - *op codes gebaseerde* cryptografie (McEliece)
  - *op hashes gebaseerde* cryptografie (Merkle hash trees)
  - *multivariate* cryptografie (polynomiaal-vergelijkingen in veel variabelen)
- EU-gesubsidieerd PQCrypto-project
- Google is gestart met experimenten met NewHope (i.s.m. CWI en Radboud Uni.)
- NIST is gestart met standardisatie

roosters

- rooster: hoog-dimensionale verzameling van punten in een niet-rechthoekig grid
- privé-sleutel: geheim roosterpunt
- publieke sleutel: maak kleine verstoringen op coördinaten
  (tussen roosterpunten in)
- moeilijk probleem: vind rooster-punt dichtst bij publieke sleutel
  - beste algoritmen bekend zijn exponentieel in dimensie
  - practische dimensies: 200 – 1000
- geen quantum-aanvallen bekend
  - zeer aktief onderzoeksgebied