Post-Quanten-Signaturen

an einem (hoffentlich niemals) praktischen Beispiel

Christian Amsüss <chrysn@fsfe.org>

PrivacyWeek 2021

2064

Ein historischer Abriss

2020er Quellen-Telekommunikationsüberwachung für große Anbieter

2030 Quellen-TKÜ für endanwenderfertige Geräte vorgeschrieben

2038 Verbot unautorisierter asymmetrischer Verschlüsselung sowie von asymmetrischem Schlüsselaustausch

Ein historischer Abriss

2020er Quellen-Telekommunikationsüberwachung für große Anbieter

2030 Quellen-TKÜ für endanwenderfertige Geräte vorgeschrieben

2038 Verbot unautorisierter asymmetrischer Verschlüsselung sowie von asymmetrischem Schlüsselaustausch

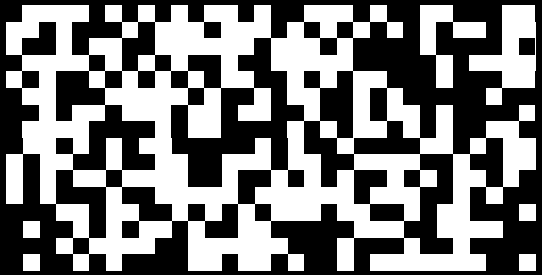
2052 erste Quantencomputer im kQbit-Bereich

Ende von RSA, Diffie-Hellman und Elliptic Curves

Ein Abseitstor – zwei Filmvarianten?

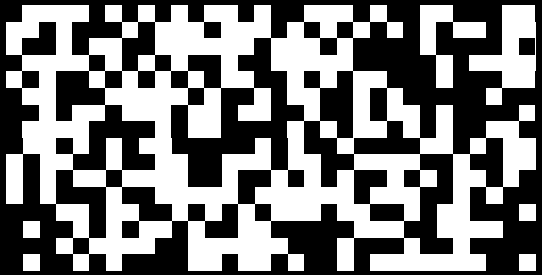
Auslosung zur Fußballeuropameisterschaft 2064

Deko oder Nachricht?



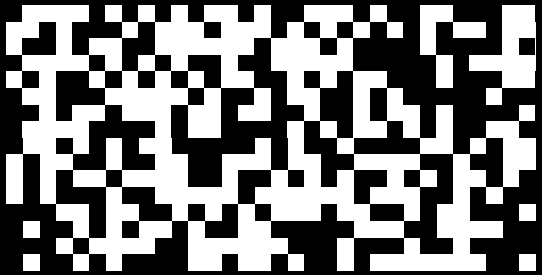
- Text?

Deko oder Nachricht?



- Text?
- Verschlüsselter Text?

Deko oder Nachricht?

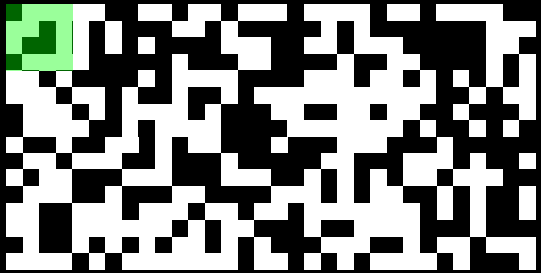


- Text?
- Verschlüsselter Text?
- Prüfsumme – Hashwert – Signatur?

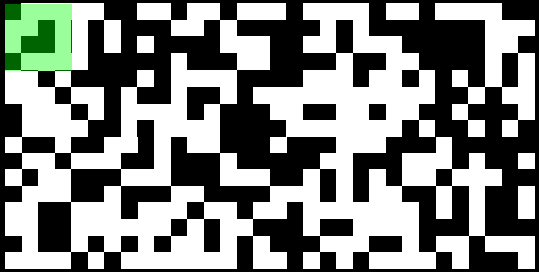
Eine erste Spur?

„Das Muster: Ein Statement?“

„Jenes Tor von Team 4 in der 65ten Minute war kein Abseits.“



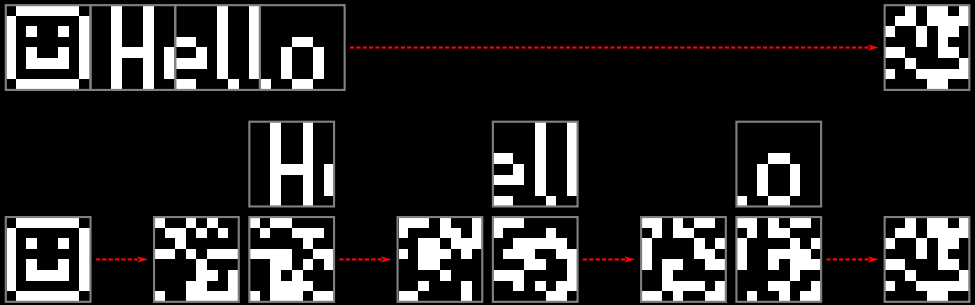
Aber welche Nachricht?



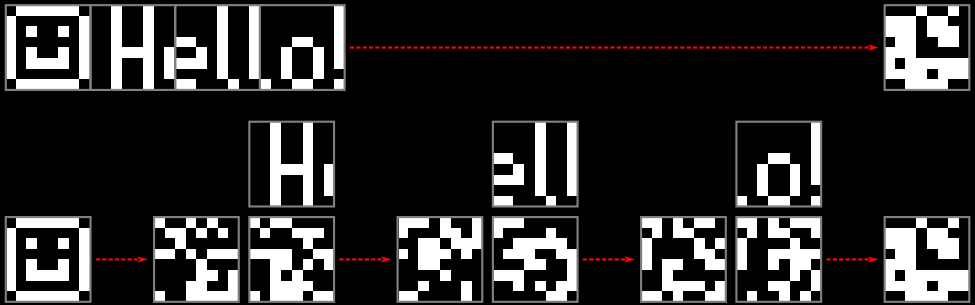
Aber welche Nachricht?

Was sind und was sollen die Hashfunktionen?

Was sind und was sollen die Hashfunktionen?

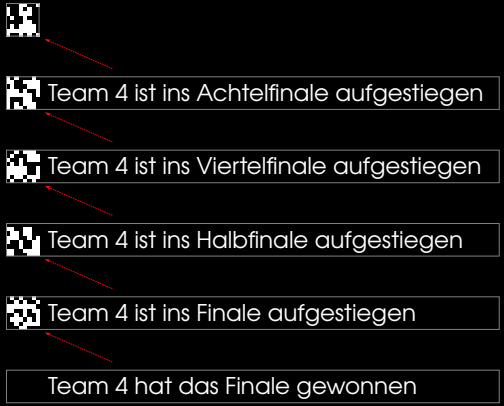


Was sind und was sollen die Hashfunktionen?



Eine Nachricht, die noch nicht fest steht?

„Deep Hash: Eine Nachricht in vielen Stufen?“



Eine andere Theorie

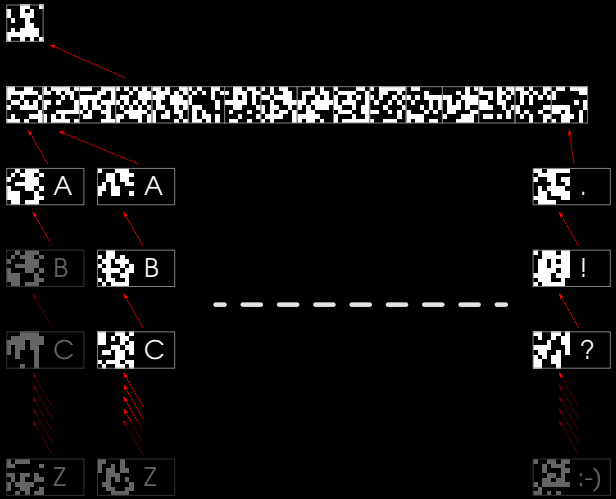
„Wide Hash“

Eine andere Theorie

„Wide Hash“

mit Nachträgen

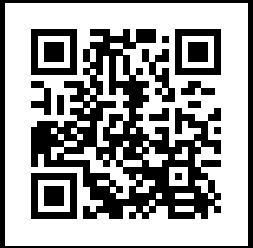
Es muss ja nicht immer Fußball sein...



Post-Quanten-Signaturen sind einfacher erklärt als klassische.
(Leider auch etwas größer. . .)

Zum Rest: Lassen wir es gar nicht so weit kommen!
(Außer bei den Quantencomputern. Die können nichts dafür.)

Folien mit Links auf `https://fahrplan.privacyweek.at/pw21/talk/JVRY9N/`



Christian Amsüss
<chrysn@fsfe.org>

Weiterführende Links

- Hashing Algorithms and Security – Computerphile
  `https://www.youtube.com/watch?v=b4b8ktEV4Bg`
- Visualisierung des SHA-3-Algorithmus
  `https://visualizekeccak.com/simulation`
- HSS/LMS in voller Ausführlichkeit
  `https://www.rfc-editor.org/rfc/rfc8708`

Bildquellen:

- Vectortoons, CC-BY-SA adaptiert von
  `https://commons.wikimedia.org/wiki/File:Cartoon_Woman_Doing_A_Business_Tallk.svg`
- Blog screenshots: Contrast, Relearn, Future Perfect
  `https://themes.gohugo.io/`