PKI vs. QC – Halbzeitstand 1:0

Spiel läuft noch

15. Security Forum der TH Brandenburg

Holger von Rhein

Asymmetrische Kryptographische Verfahren

Öffentlicher Schlüssel

Privater Schlüssel

Verschlüsseln

Entschlüsseln

Signatur überprüfen

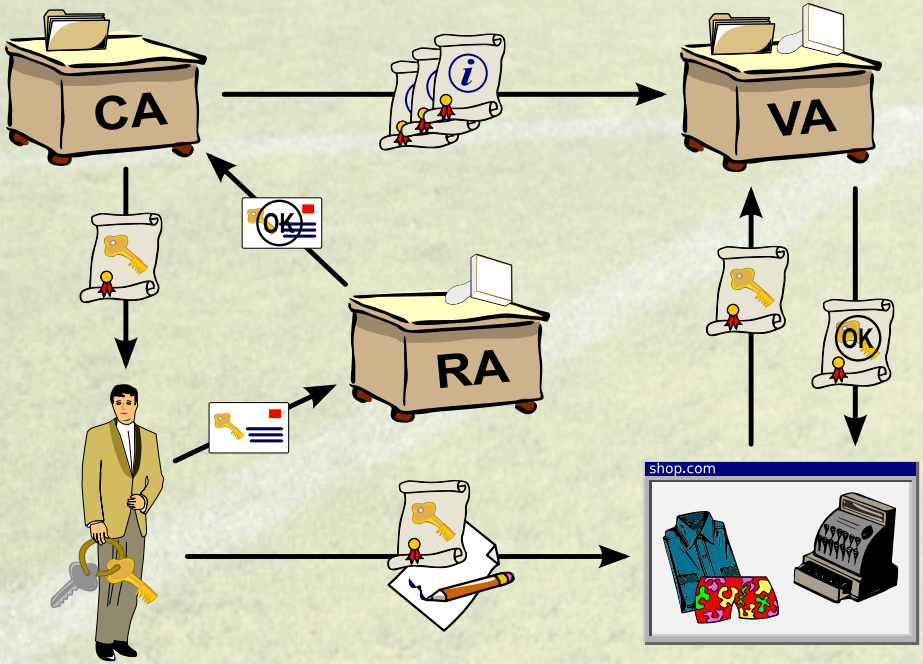
Signieren

Digitales Zertifikat

- Krypto-Material
  - öffentlicher Schlüssel
  - Signatur
- Infrastruktur Informationen
  - OCSP/CRL-URL
  - Policy-URL
- Metadaten
  - Inhaber Bezeichner (Subject)
  - Aussteller Bezeichner (Issuer)
  - Verwendungsweck: KeyUsage, Extended KeyUsage

Zertifikate-Aussage:
„Ich (Aussteller) bestätige die Korrektheit der hier enthaltenen Informationen.“

Public-Key-Infrastructure (PKI)



Bildquelle: Wikipedia

„System“, zum …

… ausstellen von digitalen Zertifikaten

… verteilen von digitalen Zertifikaten

… prüfen von digitalen Zertifikaten

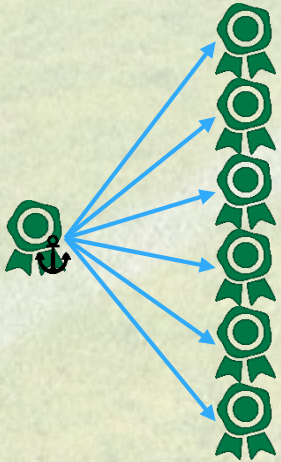
Zertifikats-Hierarchien

No-Hierarchy

Self-Signed

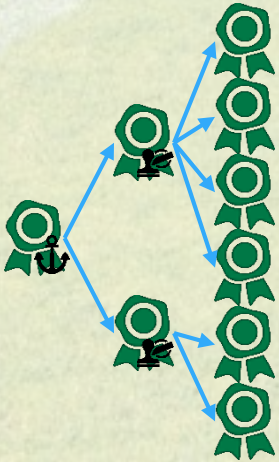
1-Layer-Hierarchy

Root-CA



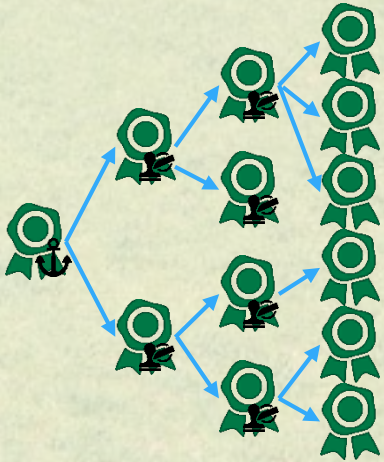
2-Layer-Hierarchy

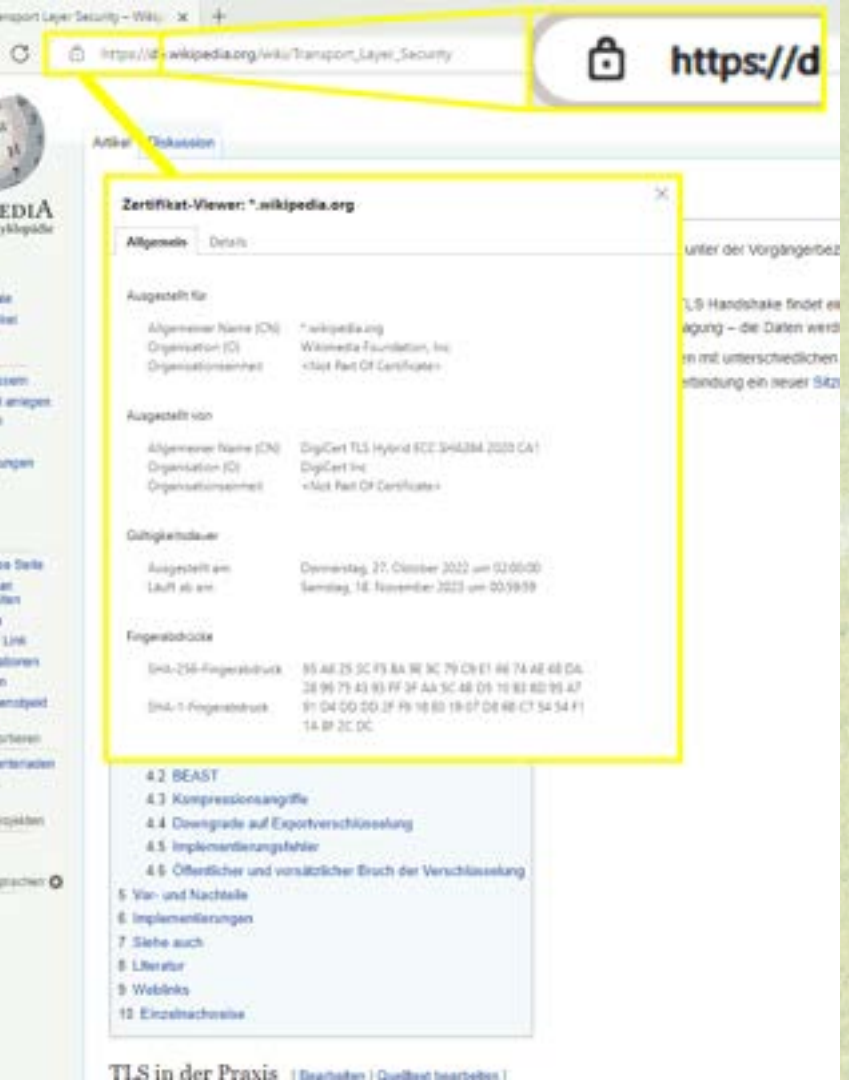
Root-CA, Issuing-CA



3-Layer-Hierarchy

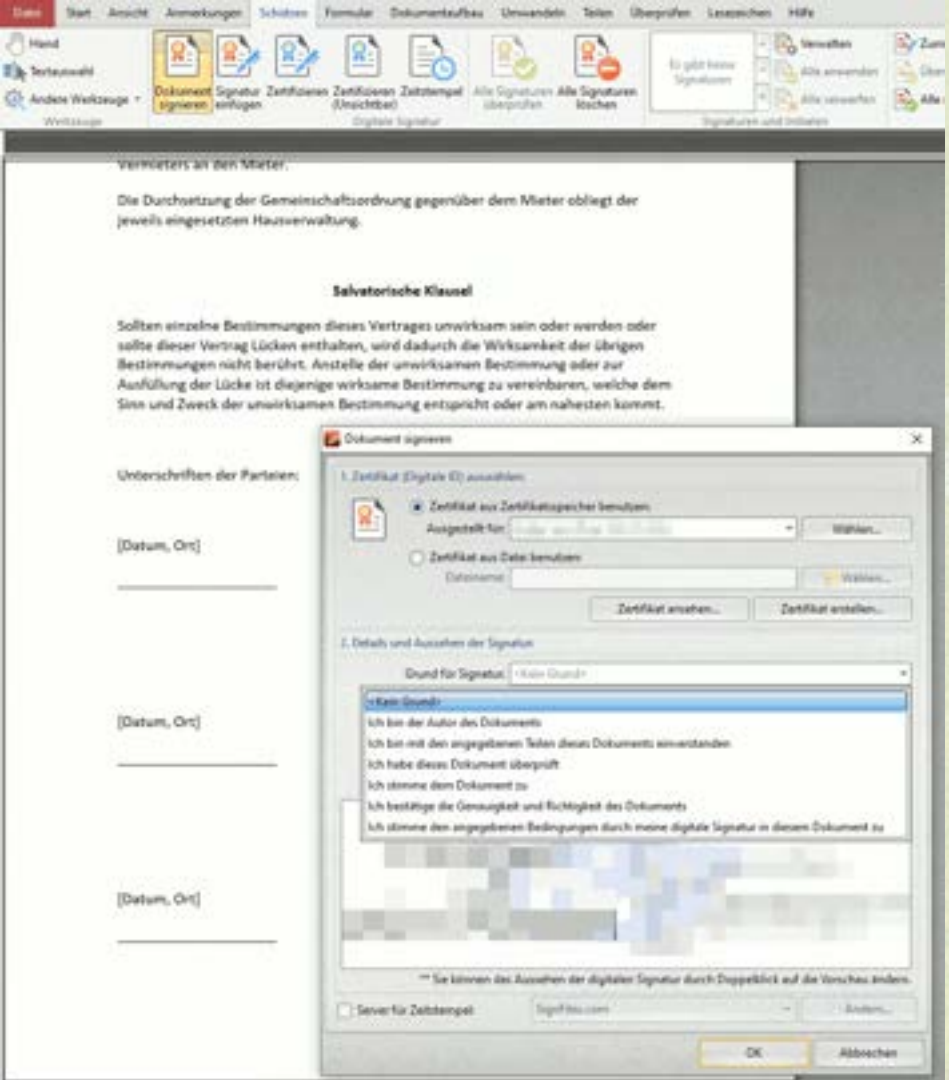
Root-CA, Intermediate-CA, Issuing-CA





Sichere Kommunikation

Zweck Zertifikat:
Identitätsnachweis Server



Dokumentensignatur

Zweck Zertifikat:
Identitätsnachweis Unterzeichner

Zu erwartende Aufwände für Primfaktorzerlegung einer RSA-Zahl

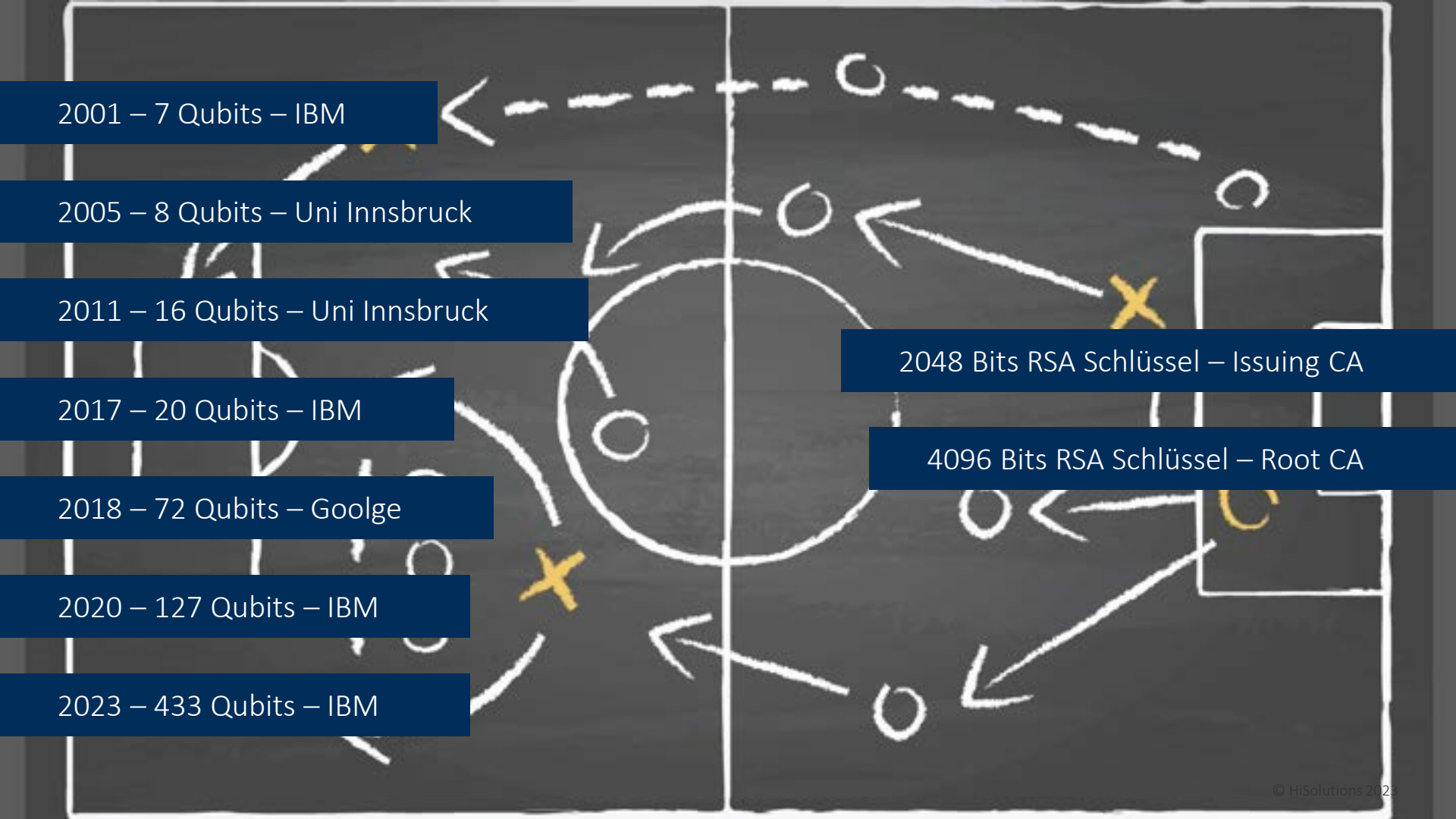
n: Bit-Größe der RSA-Zahl

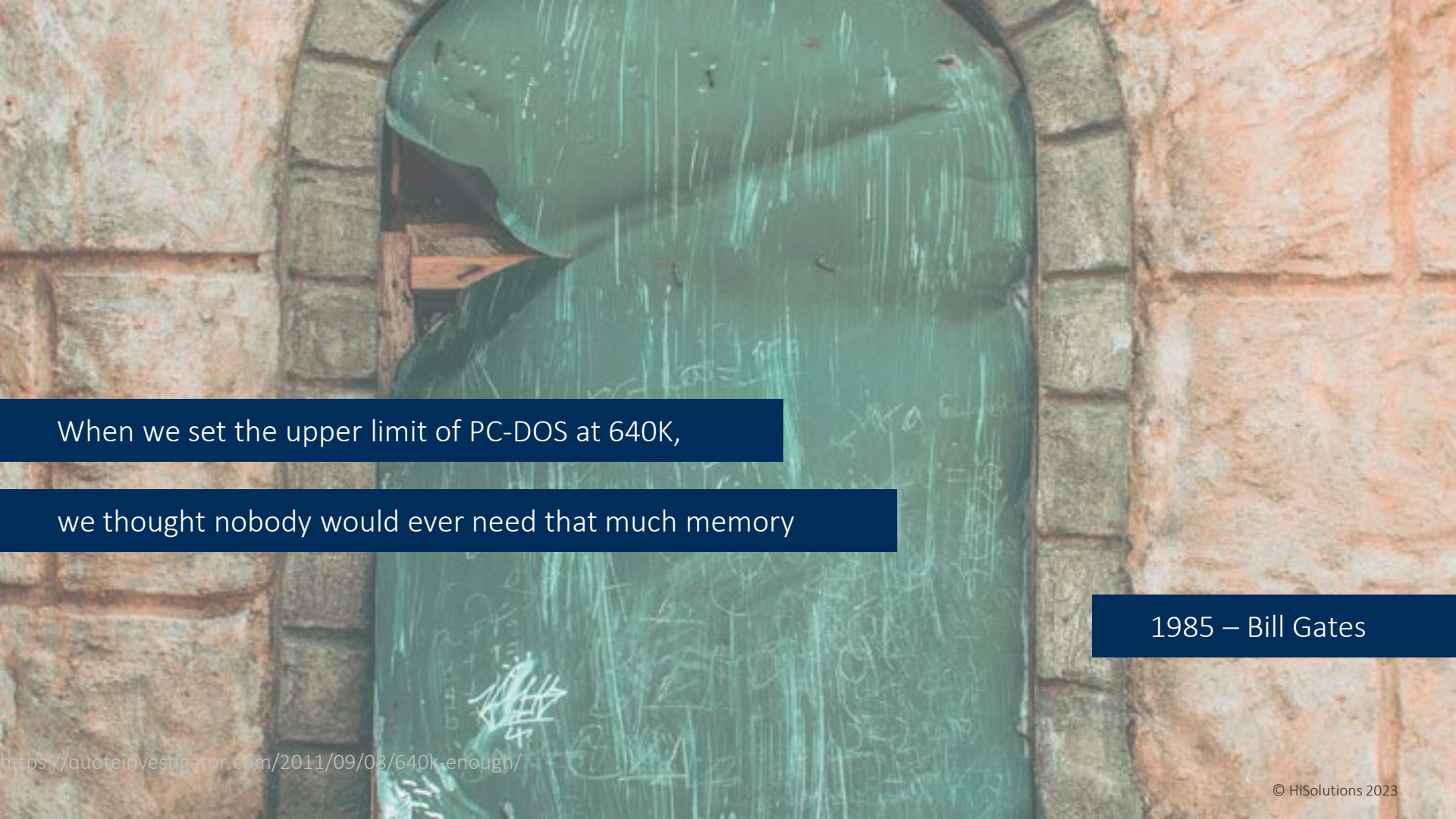
MD: Rechen-Tiefe

T: Fehlerkorrektur

	Abstract Qubits	Measurement Depth	Toffoli+T/2 Count
Factoring RSA integers		Asymptotic	
Vedral et al. 1996 [87]	$7n + 1$	$80n^3 + O(n^2)$	$80n^3 + O(n^2)$
Zalka 1998 (basic) [90]	$3n + O(1)$	$12n^3 + O(n)$	$12n^3 + O(n^2)$
Zalka 1998 (log add) [90]	$5n + O(1)$	$600n^2 + O(n)$	$52n^3 + O(n^2)$
Zalka 1998 (fft mult) [90]	$\approx 96n$	$\approx 2^{17} n^{1.2}$	$\approx 2^{17} n^2$
Beauregard 2002 [6]	$2n + 3$	$144n^3 \lg n + O(n^2 \lg n)$	$576n^3 \lg^2 n + O(n^3 \lg n)$
Fowler et al. 2012 [28]	$3n + O(1)$	$40n^3 + O(n^2)$	$40n^3 + O(n^2)$
Häner et al. 2016 [42]	$2n + 2$	$52n^3 + O(n^2)$	$64n^3 \lg n + O(n^3)$
(ours) 2019	$\mathbf{3n + 0.002n \lg n}$	$\mathbf{500n^2 + n^2 \lg n}$	$\mathbf{0.3n^3 + 0.0005n^3 \lg n}$
Solving elliptic curve DLPs		Asymptotic	
Roetteler et al. 2017 [74]	$9n + O(\lg n)$	$448n^3 \lg n + 4090n^3$	$448n^3 \lg n + 4090n^3$

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits – Craig Gidney and Martin Ekera





When we set the upper limit of PC-DOS at 640K,

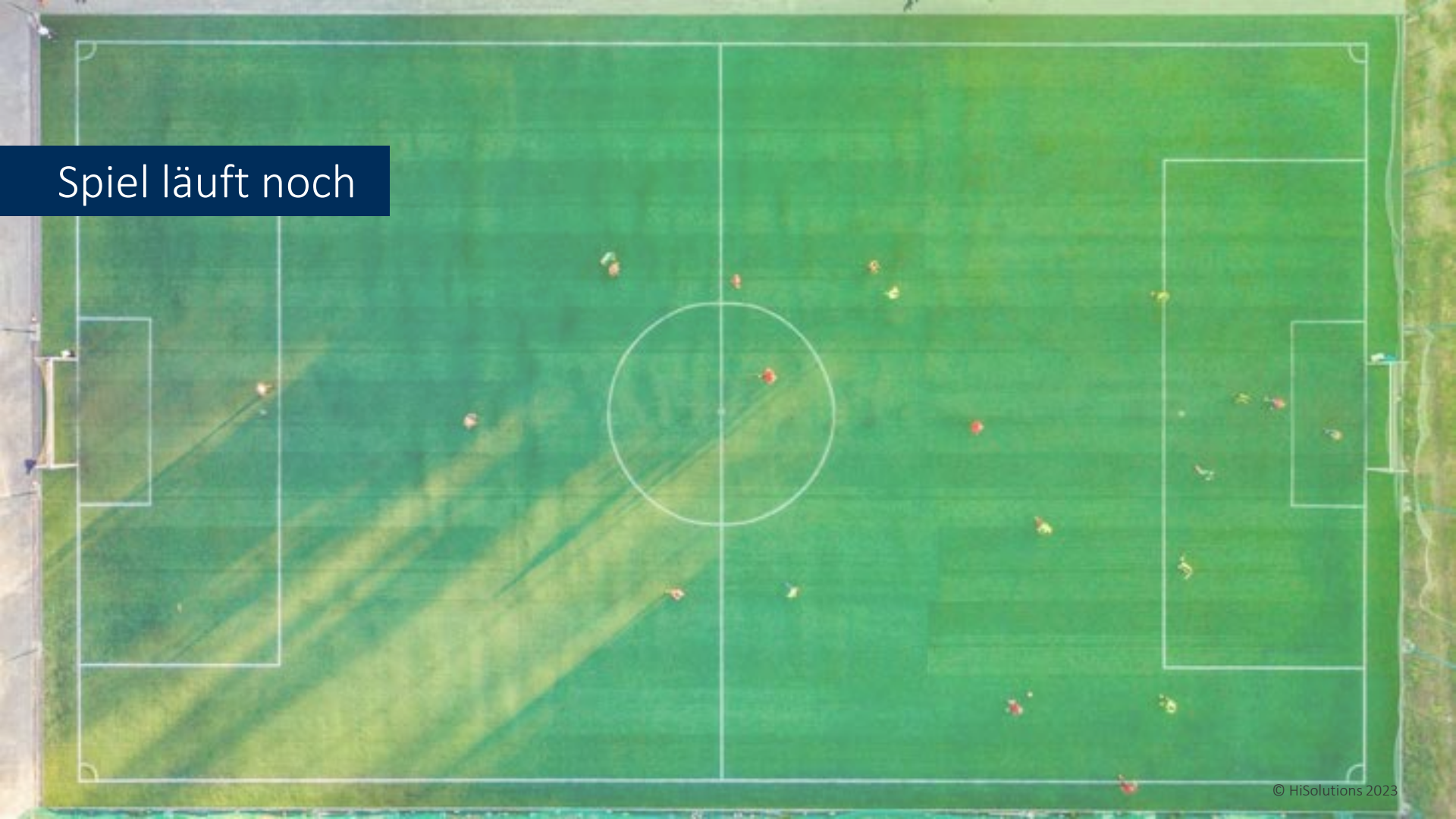
we thought nobody would ever need that much memory

1985 – Bill Gates

https://quoteinvestigator.com/2011/09/08/640k-enough/

https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

Spiel läuft noch



RFC5280 – X.509 Zertifikate

RFC3279 – Algorithmen und Identifier

Kein PQC-Algorithmen

IACR - Cryptology ePrint Archive
“The Viability of Post-Quantum X.509 Certificates”

meisten PQ-Schemas: Public Key und Signaturen sind um Faktoren größer

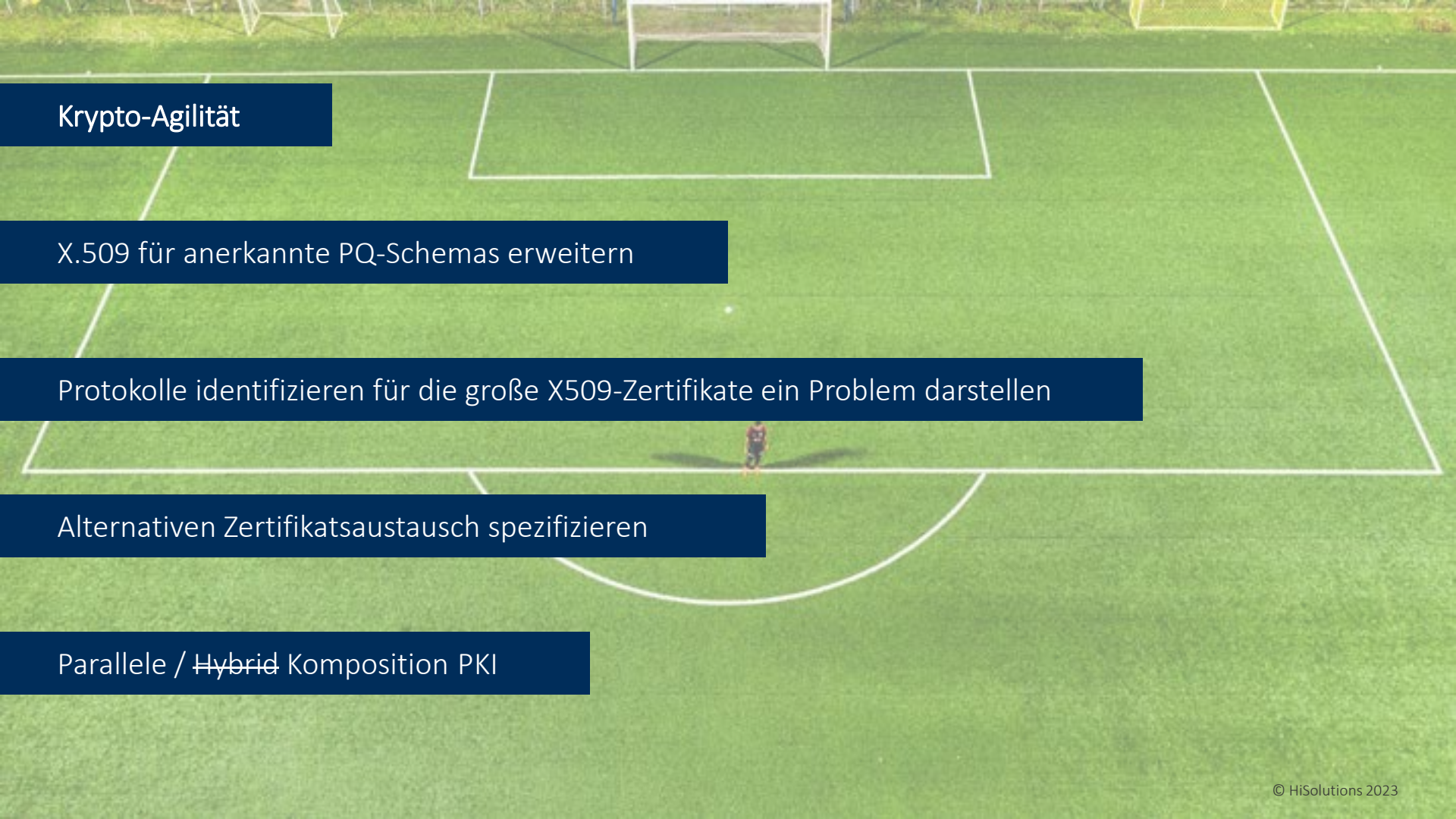
Aktuelle Verfahren: kleiner 520 Bytes

Bei Dokumenten/Code-Signaturen vermutlich kein Problem

Bei Kommunikationsverbindungen ein nicht zu verachtender Mehraufwand

Größe in Bytes (von NIST Submissions)

Algorithmus	Öffentlicher Schlüssel	Chiffretext / Signatur
RSA	256 bis 512	256 bis 512
Kyber	800 bis 1.568	786 bis 1.568
CRYSTALS-Dilithium	1.312 bis 2.592	2.420 bis 4.595
Falcon	897 bis 1.793	666 bis 1.280
Sphincs	32 bis 64	7.856 bis 49.856
Classic-McEliece	262.144 bis 1.048.576	128 bis 240



Krypto-Agilität

X.509 für anerkannte PQ-Schemas erweitern

Protokolle identifizieren für die große X509-Zertifikate ein Problem darstellen

Alternativen Zertifikatsaustausch spezifizieren

Parallele / ~~Hybrid~~ Komposition PKI

Fragen ?

HISOLUTIONS

Ihr Ansprechpartner

Barbara Grützig

algorithmen extrem schnell und der Cipher-text ist der bisher kleinste aller NIST-Post-Quanten-Kryptografie-Kandidaten.

VERFAHREN DER ZUKUNFT

Auch das BSI hat bereits erste Empfehlungen ausgesprochen. Dazu zählen z. B. die Entwicklung von kryptoagilen Lösungen und die Verwendung von Post-Quanten-Kryptographie-Algorithmen in hybrider Form. Hybrid bedeutet die Kombination mit klassischen kryptografischen Algorithmen, da viele Verfahren noch sehr jung und wenig erforscht sind. Dies führt zu den nächsten Herausforderungen. Kryptografische Protokolle müssen weiterentwickelt werden und die Public-Key-Infrastruktur muss in der Lage sein, Zertifikate zu verarbeiten, die sowohl die längeren klassischen Schlüssel als auch die quantensicheren Schlüssel enthalten.

Auch wenn es bisher nur sehr wenige offizielle Lösungen gibt, die die asymmetrischen kryptografischen Verfahren ersetzen, kann man heute schon einiges tun:

- Sensibilisierung für das Thema
  - Vorbereitung auf die Migration
  - Verantwortlichkeiten finden
  - Identifizierung der Baustellen (wo werden in der Organisation kryptografische Produkte eingesetzt und welche?)
  - Migrationskonzept erstellen
- Umsetzung der Maßnahmen, die bereits veröffentlicht sind.
  - Migration auf größere Schlüssellängen (mind. 256 Bit bei symmetrischen Verfahren)
  - Flexible Gestaltung der kryptografischen Mechanismen um kommende Standards einbinden/schneller umsetzen zu können (Kryptoagilität)

IHR QUANTENSPRUNG MIT HISOLUTIONS

Unsere Experten von HiSolutions analysieren für Sie Ihre spezifischen Systeme, die kryptografische Verfahren verwenden. Danach werden die notwendigen Änderungen für die Migration zu Post-Quanten-Kryptografie-Lösungen unter Berücksichtigung spezifischer Anforderungen identifiziert. Dabei entwickeln wir für Sie geeignete Migrations- und Übergangslösungen. Ebenfalls möchten wir das Bewusstsein für die Problematik schärfen, die sich aus der Entwicklung der Quanteninformatik für Unternehmen ergibt.

Mehr Informationen zum Quantencomputer und den Gefährdungen wie Lösungsmöglichkeiten finden Sie in einem Dokument des BSI oder in unserem Beitrag im HiSolutions Research Blog.

VORGEHENSWEISE: MIGRATION ZUR POST-QUANTEN-KRYPTOGRAFIE

1. Entscheidung zur Migration
   a. Sensibilisierung
   b. Entscheidung zur Migration
2. Vorbereitung auf die Migration
   a. Festlegung der Verantwortlichkeit
   b. Identifizierung der Ressourcen
   c. Festlegung der Post-Quanten-Kryptografie-Verfahren
   d. Analyse der vorhandenen Public-Key-Infrastruktur
3. Planung der Migration
   a. Erstellung eines Umsetzungsplans
   b. Risikomanagement
   c. Planung von Ausfallzeiten
4. Durchführung der Krypto-Strukturanalyse
   a. Klassifikation von Informationen
   b. Durchführung der Krypto-Struktur-analyse
   c. Outsourcing Identifizierung der relevanten Dienstleister!
   d. Identifizierung der eingesetzten kryptografischen Verfahren
5. Durchführung der Migration
   a. Migration der Verfahren
   b. Reporting
6. Überprüfung der Migration
   a. Durchführung eines technischen Audits

Wir sind auch immer auf der Suche nach Werkstudenten

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com