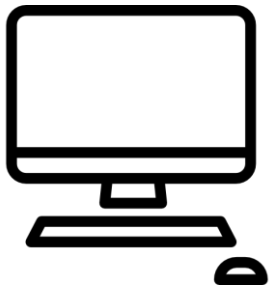
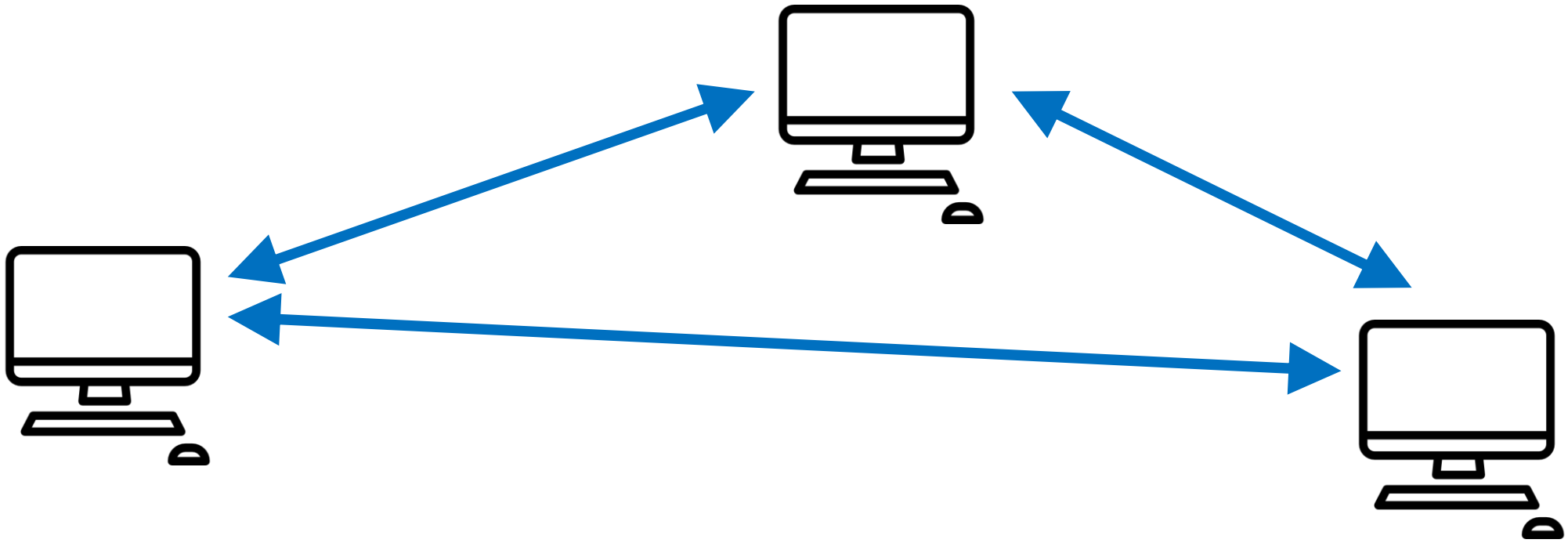
CUDA, Crackstation und Quantencomputer - sind unsere Passwörter noch sicher?

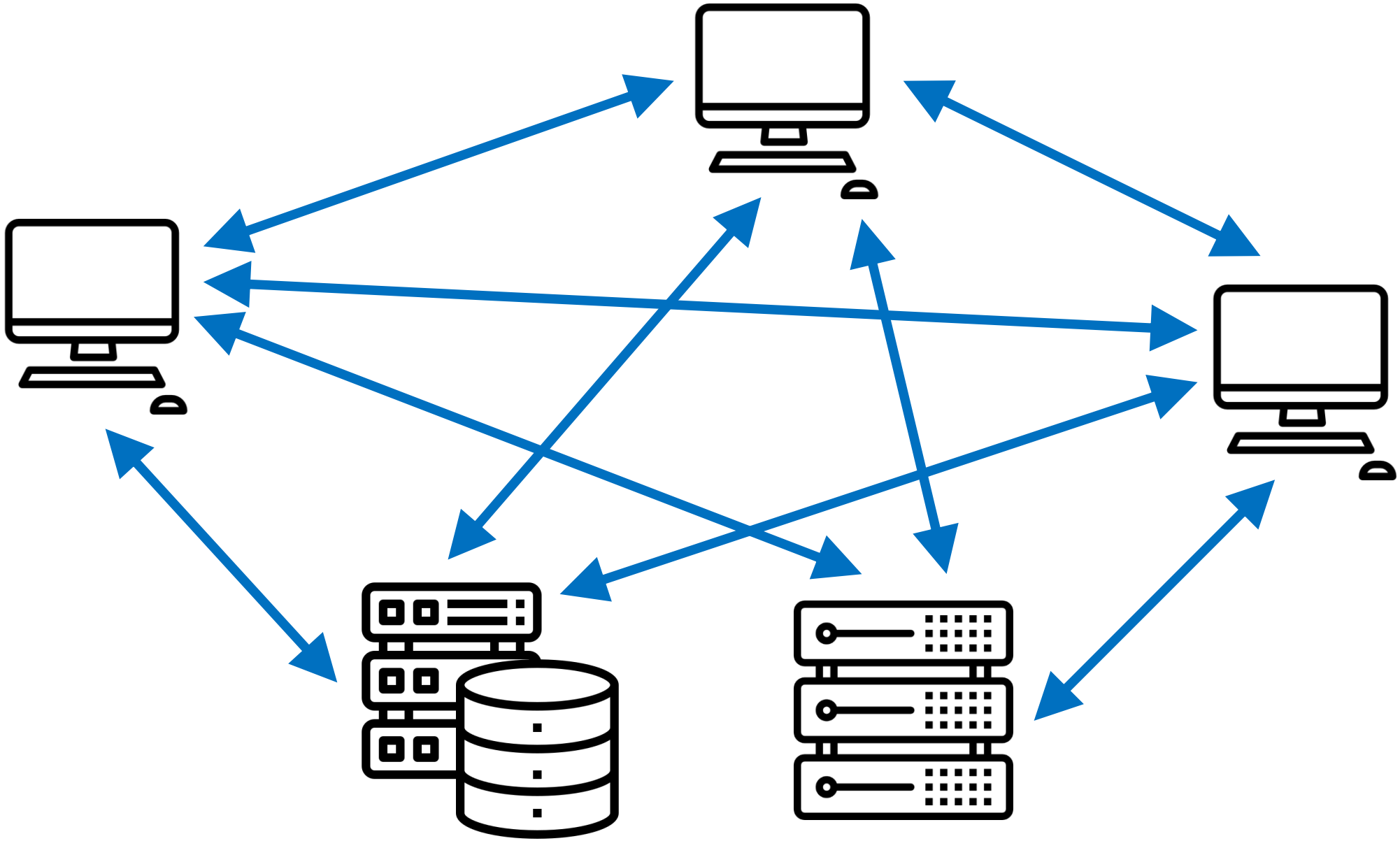
KNF-Kongress 2020

Roland Wagner

roland@datevnet.de







- peter:secret
- johnny:geheim
- fritz:unbekannt
- max:kenntmannicht
- jochen:strenggeheim
- harald:qwerasdf
- carolin:KNF2020

Bildrechte: Shuichi Seki im Auftrag von ZDF und ORF

- „KNF2020“ → Abbildung → 9a08644b9e3405f322ddf54fbbf8090db0b67036

- „KNF2020“ → Abbildung → 9a08644b9e3405f322ddf54fbbf8090db0b67036
- Bedingungen für Abbildungsfunktion

1. Einwegfunktion: Rückweg nicht möglich. Es gibt keine Möglichkeit um aus (9a08644b9e3405f322ddf54fbbf8090db0b67036) das Passwort „KNF2020“ zu ermitteln
2. Kollisionsresistenz: Unmöglich, zwei verschiedene Eingabewerte (Passwörter) zu finden, die den gleichen Ausgabewert ergeben (Kollision)

Kryptologische Hash-Funktion

- „KNF2020“ → Abbildung → 9a08644b9e3405f322ddf54fbbf8090db0b67036
- Bedingungen für Abbildungsfunktion

1. Einwegfunktion: Rückweg nicht möglich. Es gibt keine Möglichkeit um aus (9a08644b9e3405f322ddf54fbbf8090db0b67036) das Passwort „KNF2020“ zu ermitteln
2. Kollisionsresistenz: Unmöglich, zwei verschiedene Eingabewerte (Passwörter) zu finden, die den gleichen Ausgabewert ergeben (Kollision)
3. Bsp: MD4, MD5, SHA-1, SHA-256 (Whirlpool, BLAKE), SHA-3

- peter:e5e9fa1ba31ecd1ae84f75caaa474f3a663f05f4
- johnny:906072001efddf3e11e6d2b5782f4777fe038739
- fritz:a4967ca039748e9759b9f54732cf2a4806de4d31
- max:7f63f64b754f13fb8a8f351bea2cf9838cd78491
- jochen:b8b4f289613500eeaece0133491b6b9f91597377
- harald:67866a7772ab749f833dc52d82ac7853df866bf5
- carolin:9a08644b9e3405f322ddf54fbbf8090db0b67036

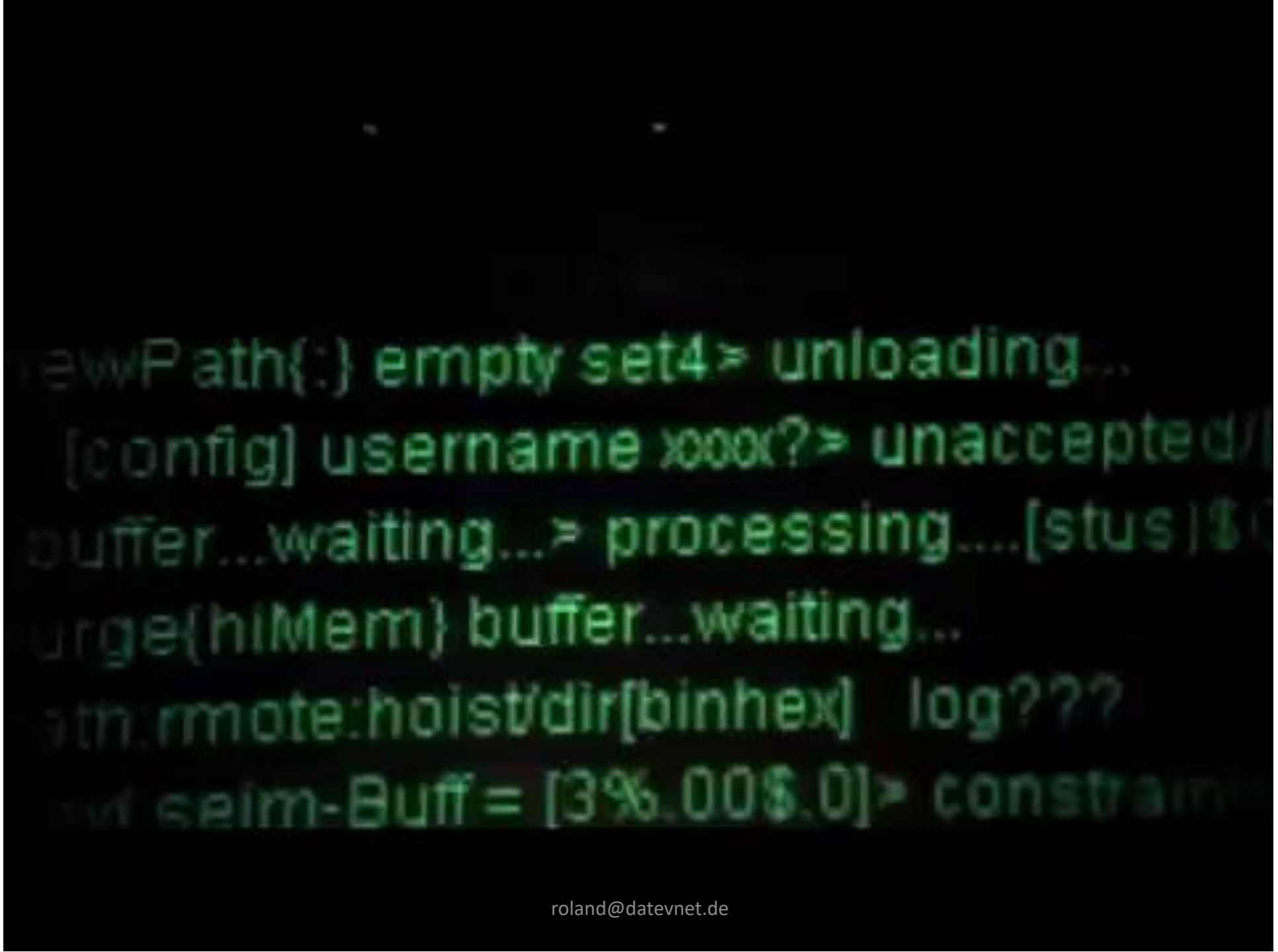
- Wie geht das PW hacken eigentlich?

- https://www.youtube.com/watch?v=msX4oAXpvUE

„ncis hacking two keyboard“

“ncis 2 idiots 1 keyboard”


FOLSOM STATE PRISON


ewPath(:) empty set4> unloading...
[config] username xxxx?> unaccepted//
uffer...waiting...> processing....[stus]
rge(hiMem) buffer...waiting...
th:rmote:hoist/dir[binhex] log???
eim-Buff = [3%.00$.0]> constra

Wie funktioniert das wirklich?

Online

Offline

Offline

Wie kommt man an die Hashes?

- Zugriff vom Admin

Offline

Wie kommt man an die Hashes?

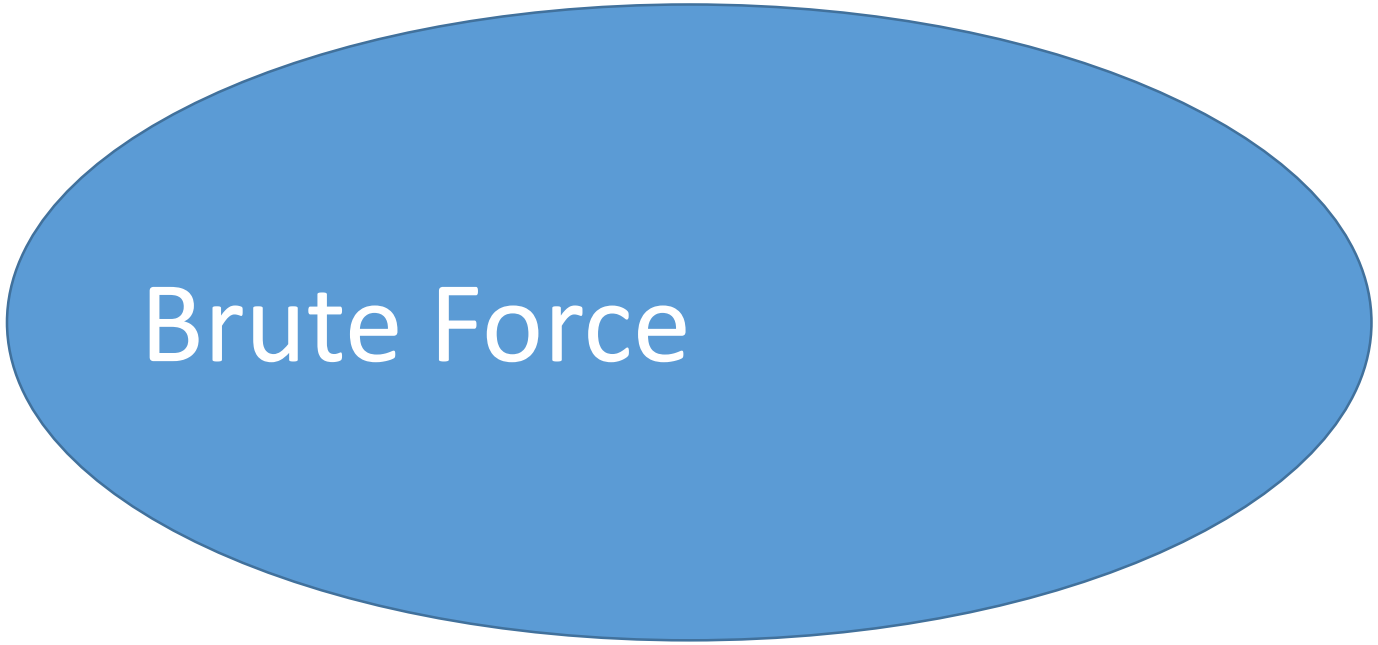
- Zugriff vom Admin
- Virus, Trojaner
- Leaken (Veröffentlichung gestohlener Passwörter)
- „Verkauf/Ankauf“ von Passwörtern

Offline

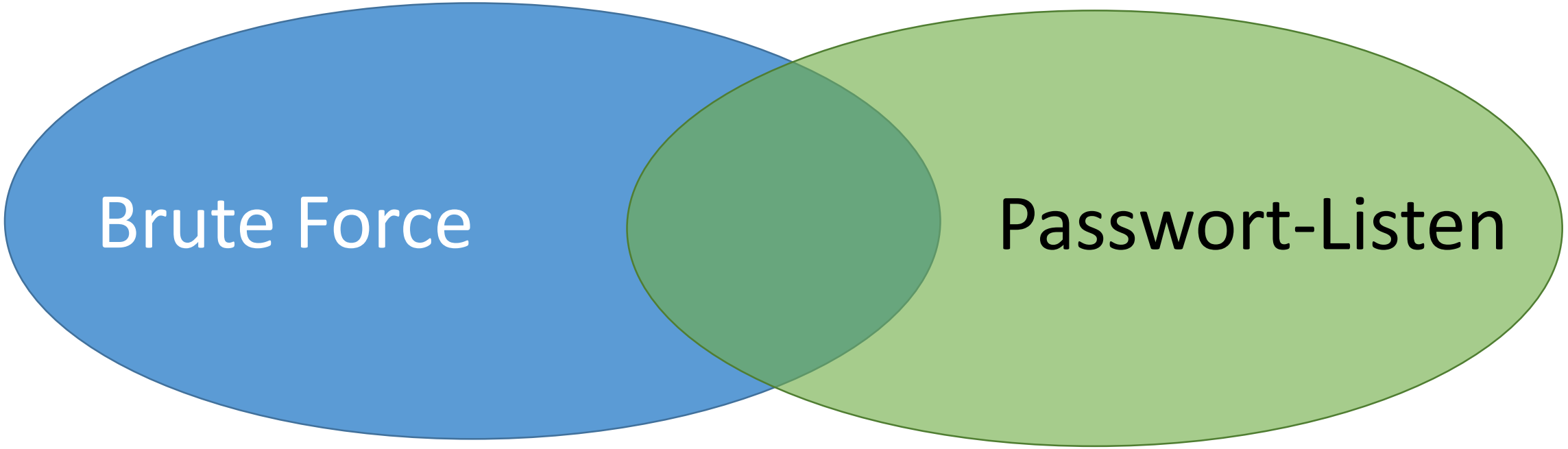
Wie kommt man an die Hashes?

- Zugriff vom Admin
- Virus, Trojaner
- Leaken (Veröffentlichung gestohlener Passwörter)
- „Verkauf/Ankauf“ von Passwörtern
- Unabsichtliche Veröffentlichung (Hilfe-Foren)
- Memory-Dump
- Software-Schwachstellen (.htpasswd über Webserver auslesbar)

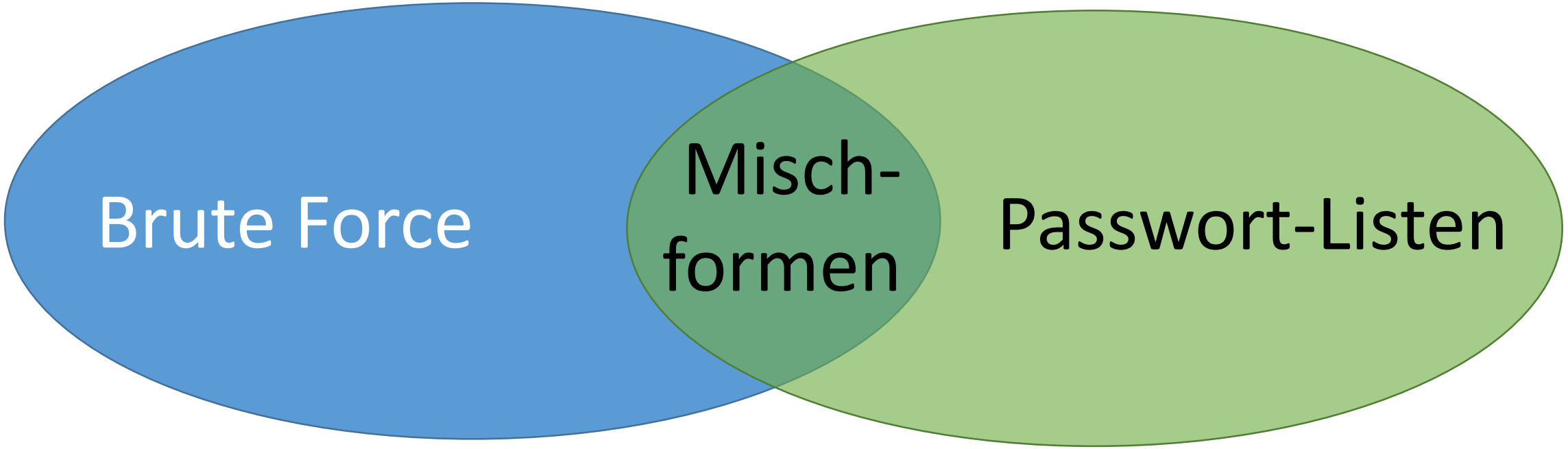
Methoden



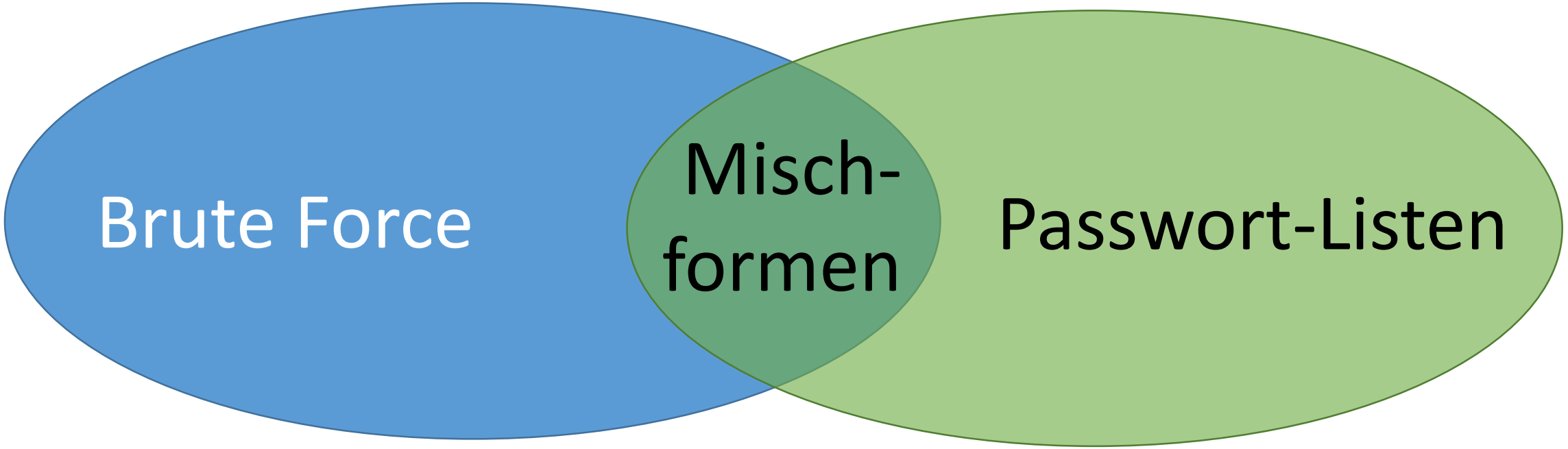
Methoden



Methoden



Methoden



Rainbow Tables → Saltet Hash

Gefahren I – Der Faktor Technik

- Einwegfunktion
- Zeitdauer abhängig von Länge, Komplexität
- Kleinbuchstaben, Großbuchstaben, Sonderzeichen, Zahlen ➔ Passwortstärke ➔ Entropie H=**Länge*log2(#Zeichen)**

Gefahren I – Der Faktor Technik

- Einwegfunktion
- Zeitdauer abhängig von Länge, Komplexität, Hardware
- Kleinbuchstaben, Großbuchstaben, Sonderzeichen, Zahlen ➔ Passwortstärke ➔ Entropie H=**Länge*log2(#Zeichen)**
- Offline: CPU

Jahr	Hardware	FLOPS
2005	Pentium 4, 3,2 GHz	6,4 GFLOP/S

Gefahren I – Der Faktor Technik

- Einwegfunktion
- Zeitdauer abhängig von Länge, Komplexität, Hardware
- Kleinbuchstaben, Großbuchstaben, Sonderzeichen, Zahlen ➔ Passwortstärke ➔ Entropie H=**Länge*log2(#Zeichen)**
- Offline: CPU

Jahr	Hardware	FLOPS
2005	Pentium 4, 3,2 GHz	6,4 GFLOP/S
2014	Intel i7-5960X, 8K/16T	375 GFLOP/S
2020	Intel Core i9-10900K	1696 GFLOPS
2020	NVIDIA GeForce RTX 3090	35580 GFLOP/S

Gefahren I – Der Faktor Technik

- Einwegfunktion
- Zeitdauer abhängig von Länge, Komplexität, Hardware
- Kleinbuchstaben, Großbuchstaben, Sonderzeichen, Zahlen ➔ Passwortstärke ➔ Entropie H=**Länge*log2(#Zeichen)**
- Offline: CPU

Jahr	Hardware	FLOPS
2005	Pentium 4, 3,2 GHz	6,4 GFLOP/S
2014	Intel i7-5960X, 8K/16T	375 GFLOP/S
2020	Intel Core i9-10900K	1696 GFLOPS
2020	NVIDIA GeForce RTX 3090	35580 GFLOP/S
2018	SuperMUC-NG	26700000 GFLOP/s

- **CUDA** (Compute Unified Device Architecture) -> Schnittstelle für Programmierung der massiv parallelen Recheneinheiten der GPU (Hashcat, John the Ripper, Hash Suite, …)

Gefahren I – Der Faktor Technik

- Einwegfunktion
- Zeitdauer abhängig von Länge, Komplexität, Hardware
- Kleinbuchstaben, Großbuchstaben, Sonderzeichen, Zahlen ➔ Passwortstärke ➔ Entropie H=**Länge*log2(#Zeichen)**
- Offline: CPU

Jahr	Hardware	FLOPS
2005	Pentium 4, 3,2 GHz	6,4 GFLOP/S
2014	Intel i7-5960X, 8K/16T	375 GFLOP/S
2020	Intel Core i9-10900K	1696 GFLOPS
2020	NVIDIA GeForce RTX 3090	35580 GFLOP/S
2018	SuperMUC-NG	26700000 GFLOP/s

- CUDA (Compute Unified Device Architecture) -> Schnittstelle für Programmierung der massiv parallelen Recheneinheiten der GPU (Hashcat, John the Ripper, Hash Suite, …)

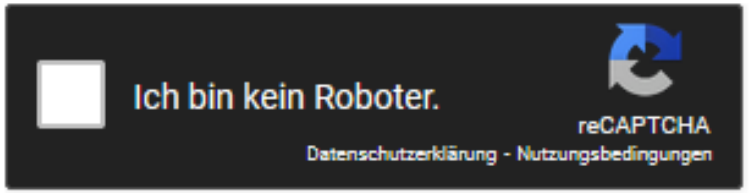
- Frei verfügbare Cracker (Crackstation)

https://crackstation.net/

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
a8901e3a9cf39f5c6aff9bc1e9663150edfabe1e
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
a8901e3a9cf39f5c6aff9bc1e9663150edfabe1e	sha1	Passwort321

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Gefahren I – Der Faktor Technik

- Einwegfunktion
- Zeitdauer abhängig von Länge, Komplexität, Hardware
- Kleinbuchstaben, Großbuchstaben, Sonderzeichen, Zahlen ➔ Passwortstärke ➔ Entropie H=**Länge*log2(#Zeichen)**
- Offline: CPU

Jahr	Hardware	FLOPS
2005	Pentium 4, 3,2 GHz	6,4 GFLOP/S
2014	Intel i7-5960X, 8K/16T	375 GFLOP/S
2020	Intel Core i9-10900K	1696 GFLOPS
2020	NVIDIA GeForce RTX 3090	35580 GFLOP/S
2018	SuperMUC-NG	26700000 GFLOP/s

- CUDA (Compute Unified Device Architecture) -> Schnittstelle für Programmierung der massiv parallelen Recheneinheiten der GPU (Hashcat, John the Ripper, …)

- Frei verfügbare Cracker (Crackstation)
- Fehlerhafte Software (Implementierungen) – bei Offline und Online

Gefahren II – Der Faktor Mensch

- Social Engineering (Fishing)
- Wiederverwendung von Passwörtern

Gefahren II – Der Faktor Mensch

- Social Engineering (Fishing)
- Wiederverwendung von Passwörtern
- Zwang zu strengen Passwörtern
  - Durchnummerierung
  - Sonderzeichen am Ende
- Sonderzeichen leicht erreichbar / vorhanden auf Tastatur (£, {, [, ~)

Gefahren II – Der Faktor Mensch

- Social Engineering (Fishing)
- Wiederverwendung von Passwörtern
- Zwang zu strengen Passwörtern
  - Durchnummerierung
  - Sonderzeichen am Ende
- Sonderzeichen leicht erreichbar / vorhanden auf Tastatur
- Passwortlisten generieren aus Twitter, Homepage, Facebook, etc.
  (twofi, Twitter Words of Interest; CUPP - Common User Passwords Profiler, …)
- Passwörter aus Filmen, Büchern, etc.

Gefahren III - Quantencomputer

- Basis: Quantenmechanische Zustände
- Qubits anstatt Bits

- Theoretische Arbeiten (Shor-Algorithmus)

Gefahren III - Quantencomputer

- Basis: Quantenmechanische Zustände
- Qubits anstatt Bits

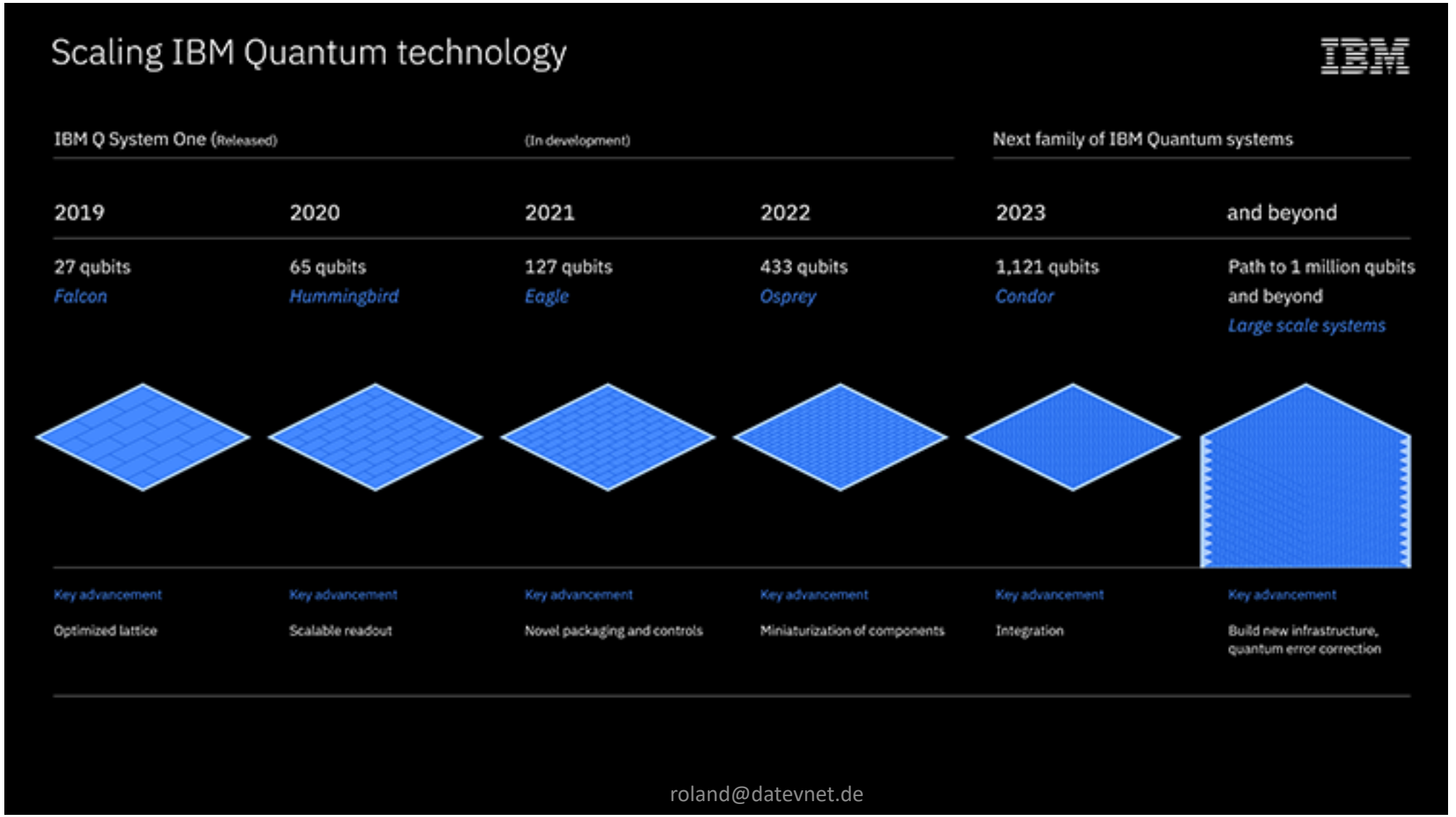
- Theoretische Arbeiten (Shor-Algorithmus)

- Microsoft (Theoretische Arbeiten, Simulator)
- Praktische Realisierung (Labor)

Gefahren III – Quantencomputer Google

Sycamore von Google (53 Qubits)
200 Sekunden vs. 10000 Jahre

Gefahren III – Quantencomputer IBM



Gefahren III – Quantencomputer Rigetti

Rigetti right now

Aspen-8		Median Time Duration (µs)		Median Fidelity (per op.)	
Deployed	20.05.20	T1 Lifetime	29	Single-qubit gates	99.8%
Qubits	31	T2 Lifetime	19	Two-qubit gates (CZ)	94.7%
				Two-qubit gates (XY)	96.0%

Gefahren III - Quantencomputer

1. Aufwand: Supraleitung, Mikrowellen, Laserlicht
2. Fehlerrate -> Fehlerkorrektur
3. „Lebensdauer“ (Dekohärenz - Verlust der Superpositionseigenschaft)

Gefahren III - Quantencomputer

1. Aufwand: Supraleitung, Mikrowellen, Laserlicht
2. Fehlerrate -> Fehlerkorrektur
3. „Lebensdauer“ (Dekohärenz - Verlust der Superpositionseigenschaft)

„Post-Quantum Krypto-Algorithmen“

… und was jetzt …

- Faktor Technik:

Balance zwischen Aufwand und Datenschutz

- Faktor Mensch:

Awareness & Unterstützung durch Technik

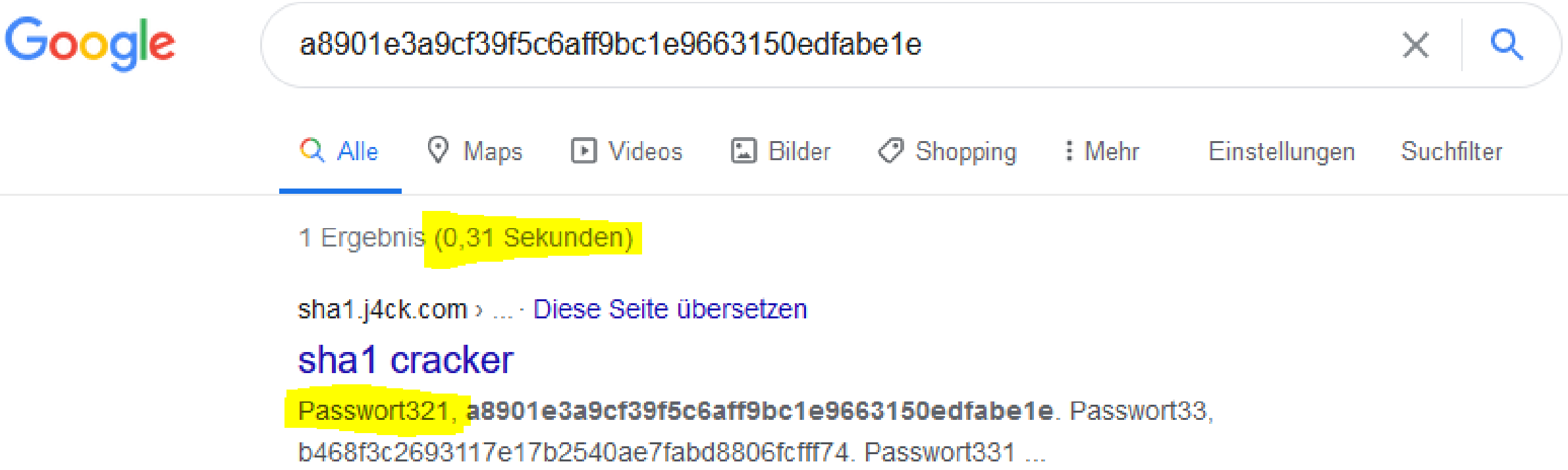
- Quantencomputer:

„Am Ball bleiben“


Any
Questions

Anhang I – Schnellster PW-Cracker ?

Anhang I – Schnellster PW-Cracker ?



Anhang II – „Selftest“

HASH erzeugen

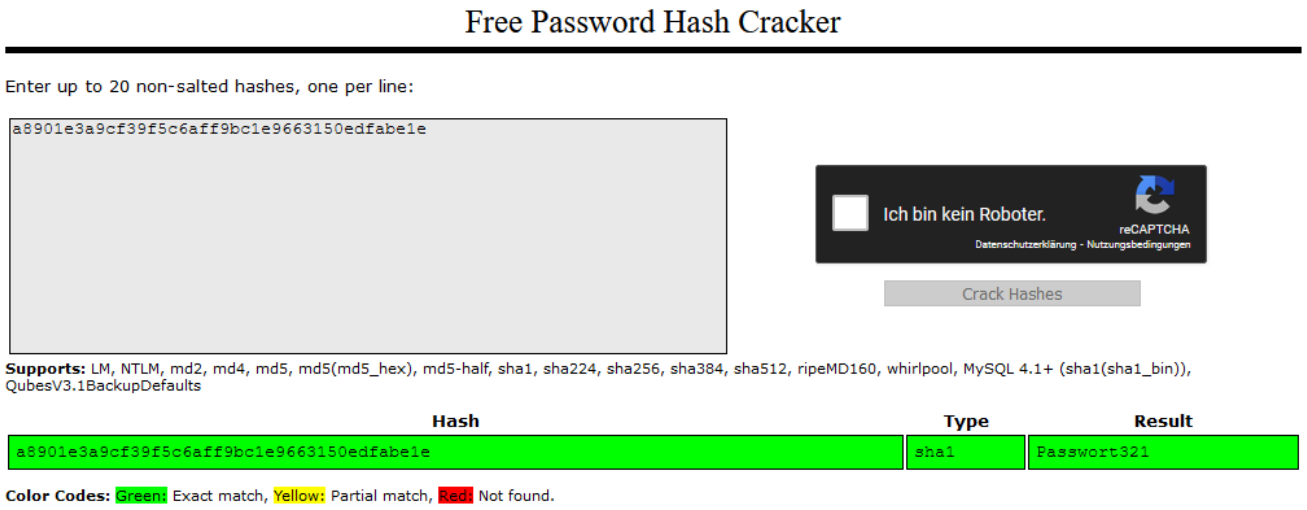
z.B. online

http://www.sha1-online.com/

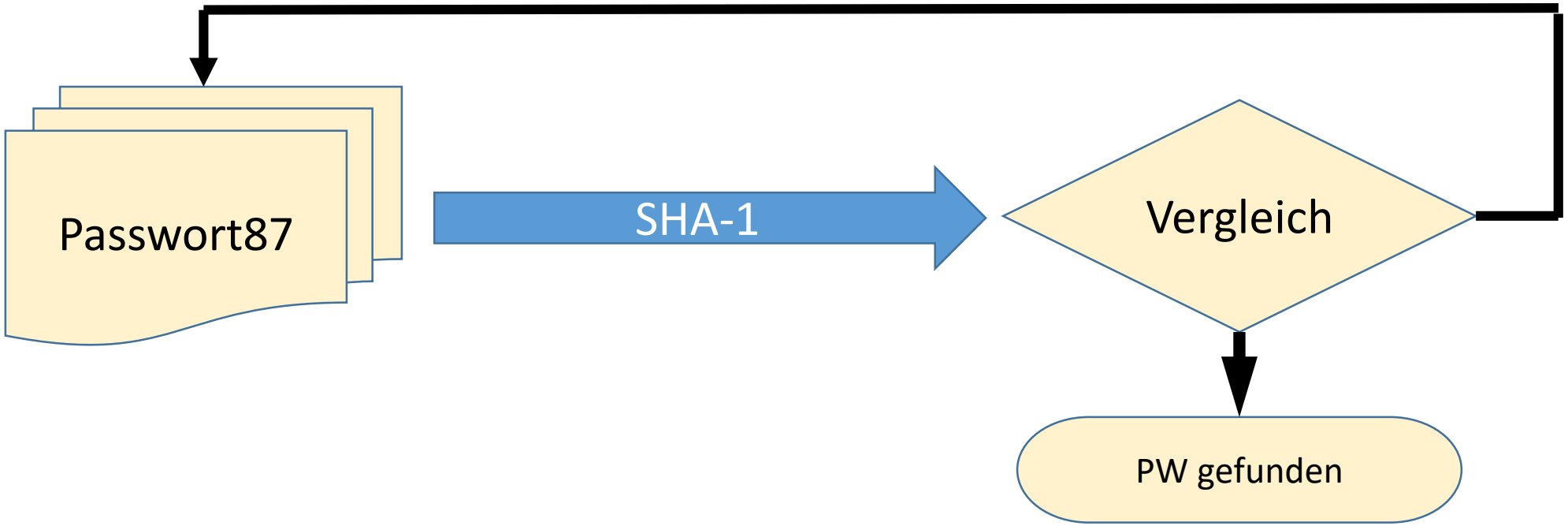
und Online (Crackstation)

https://crackstation.net/

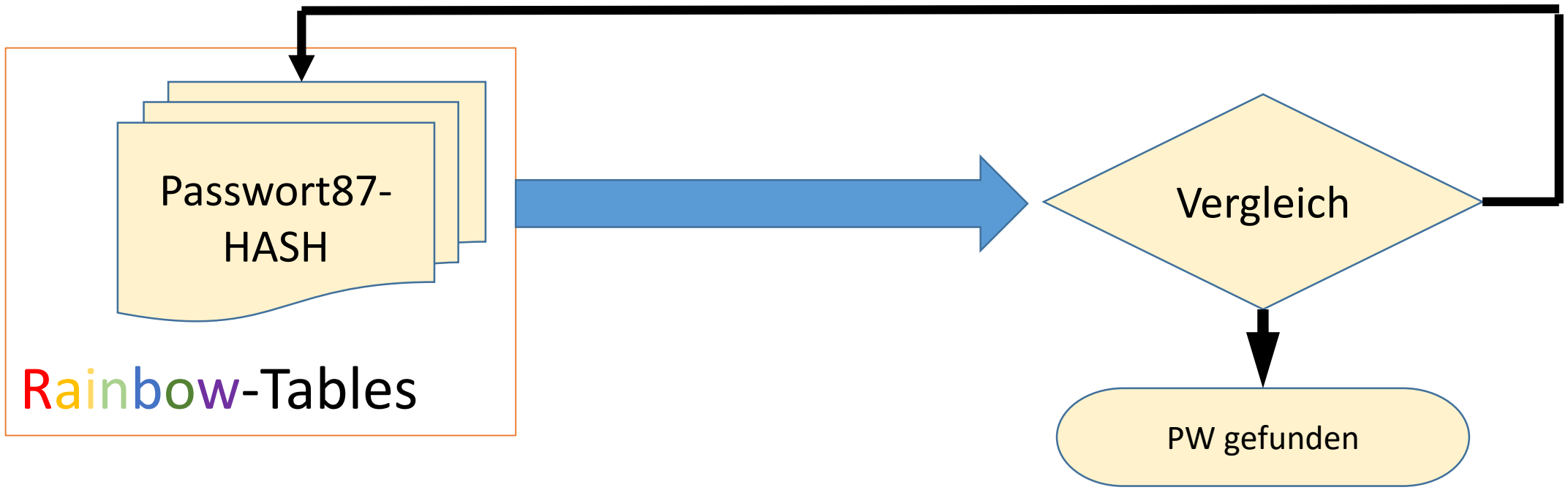
oder Offline (hashcat, Hash Suite) prüfen



Anhang III – Rainbow Tables & Saltet Hash



Anhang III – Rainbow Tables & Saltet Hash



Anhang III – Rainbow Tables & Saltet Hash

„salzen“