



Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

Kapitel 12: Netzsicherheit - Schicht 2: WLAN

Inhalt

- WLAN: Eine kurze Einführung
- WLAN-Sicherheitsanforderungen und Mechanismen
- Wired Equivalent Privacy (WEP)
 - Authentisierung
 - Vertraulichkeit
 - Integrität
 - Autorisierung
 - Schwächen und Angriffe
- WiFi Protected Access (WPA)
 - Authentisierung mit 802.1X oder Preshared Keys (PSK)
 - Vertraulichkeit (TKIP)
 - TKIP-Schlüsselhierarchie
 - WPA- und TKIP-Sicherheit
- WPA 2
- WPA 3



Wireless Local Area Network (WLAN)

- WLAN standardisiert in IEEE 802.11x:

Standard	Frequenz [GHz]	maximaler Durchsatz [Mbit/s]
802.11	2,4	2
802.11a	5	54
802.11b	2,4	11
802.11g	2,4	54
802.11n	2,4 / 5	600
802.11ac	5	1,69 Gbit/s (6,77 Gbit/s)
802.11ax (WiFi 6, WiFi 6e)	2,4 / 5 / 6	2,5 Gbit/s (9,6 Gbit/s)

- Alle Geräte teilen sich die Bandbreite
- Maximaler Durchsatz praktisch nicht erreichbar (netto wird i.d.R. weniger als die Hälfte erreicht, z.B. 200-300 Mbit/s bei 802.11n)

Beispiel MWN

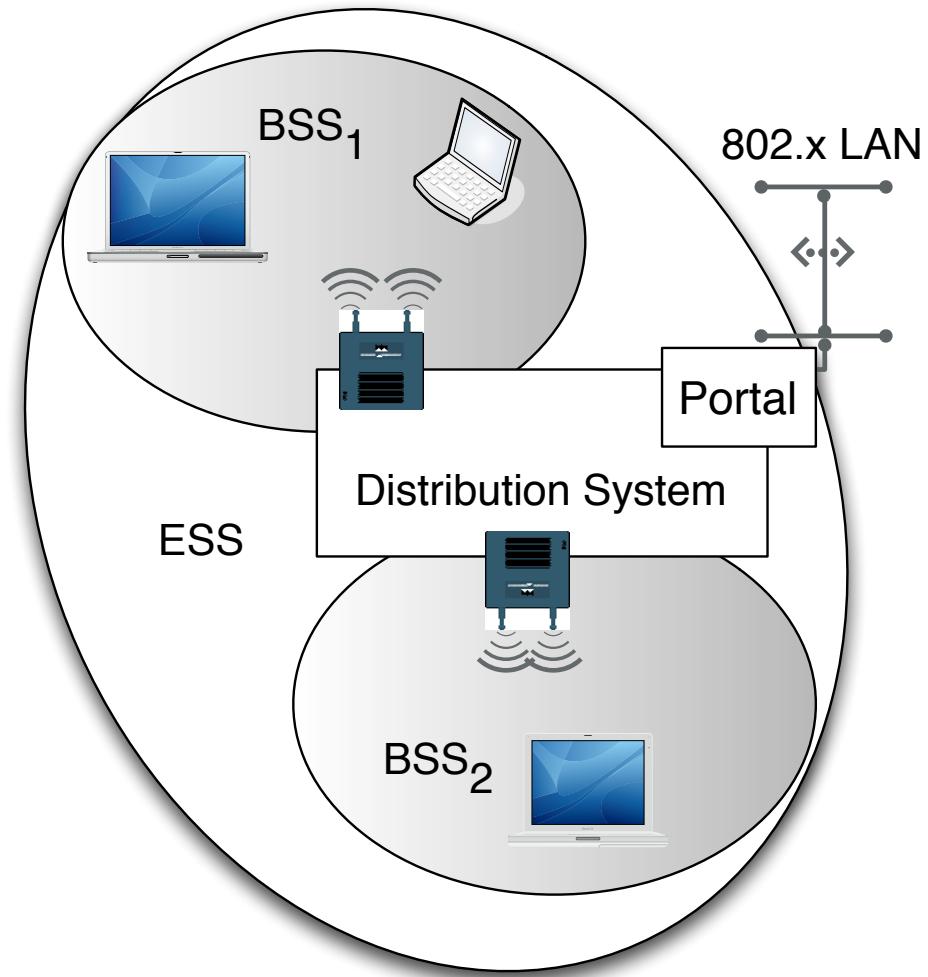
- Derzeit leistungsfähigste Geräte im MWN: Aruba AP-555
- Dualband-AP, d.h. 2,4 GHz- und 5 GHz-Frequenzband
- Multiuser MIMO
- Durchsatz bei opt. Bedingungen 6 Gbit/s (Marketing bzw. theoretischer Wert)
- Controller basierte Lösung



- Nutzungsstatistik installierter Access Points: <http://wlan.lrz.de/apstat/>
 - Gebäude: <http://wlan.lrz.de/apstat/filter/Unterbezirk/gs/>
 - einzelner AP: <http://wlan.lrz.de/apstat/apa10-0gs/>

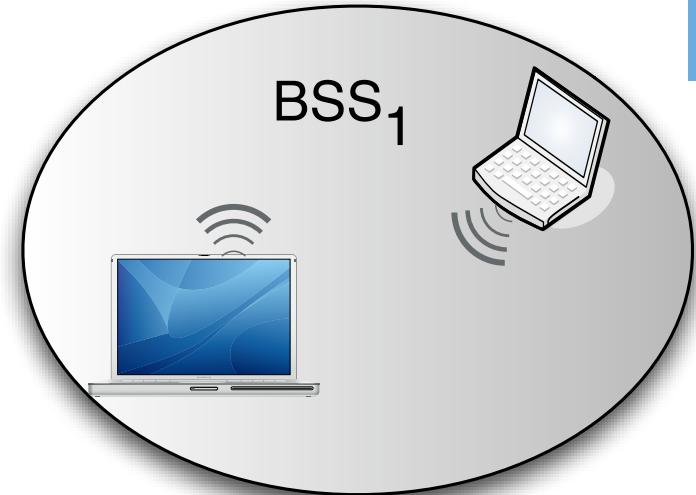
Infrastruktur-Modus

- Access Point (AP): Zugangsknoten zum WLAN
- Station (STA)
 - Gerät mit WLAN-Ausstattung
 - (Intelligenter) Client
- Basic Service Set (BSS)
 - Gruppe von STAs, die selbe Frequenz nutzen
- Extended Service Set (ESS)
 - logisches Netz aus mehreren BSS
 - wird gebildet durch Verbindungsnetz (Distribution System (DSS))
 - ESS wird durch SSID identifiziert
- Portal: Verbindung zu anderen Netzen



Ad-Hoc Modus

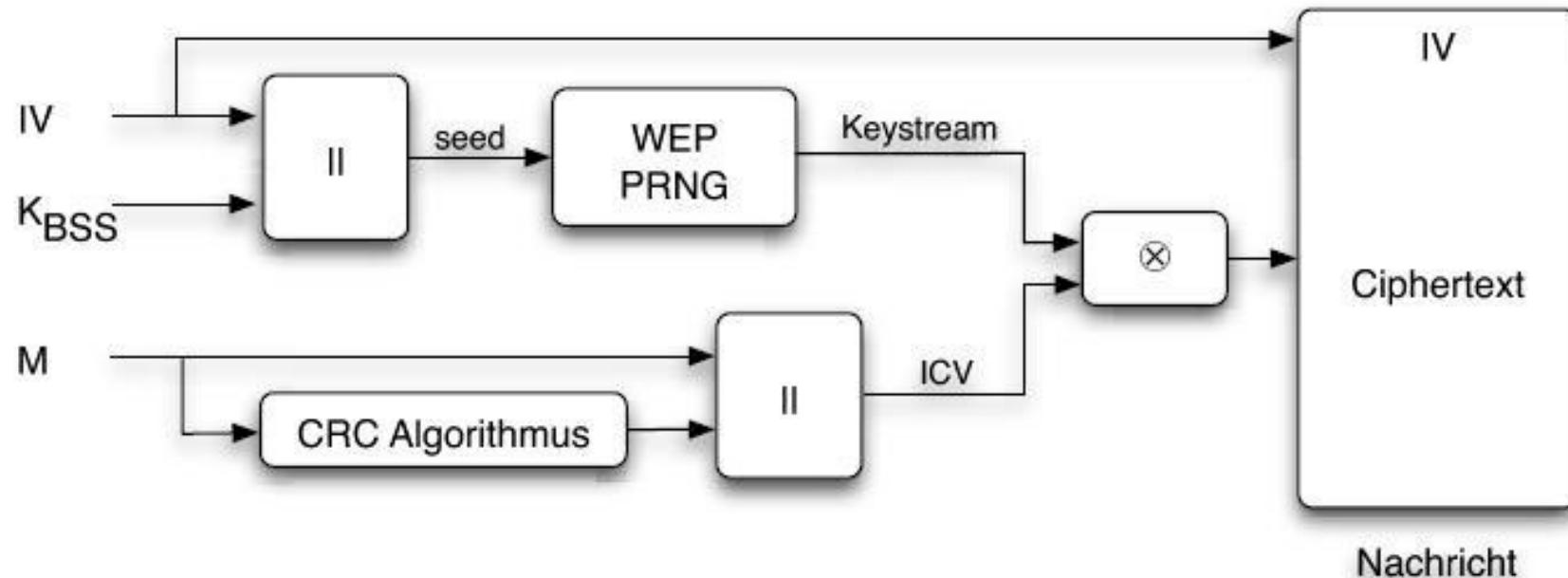
- Kein Access Point (AP) erforderlich
- Alle Stationen sind gleichberechtigt
- Basic Service Set (BSS)
 - Gruppe von STAs, die dieselbe Frequenz nutzen
 - Keine Kommunikation zwischen BSS möglich



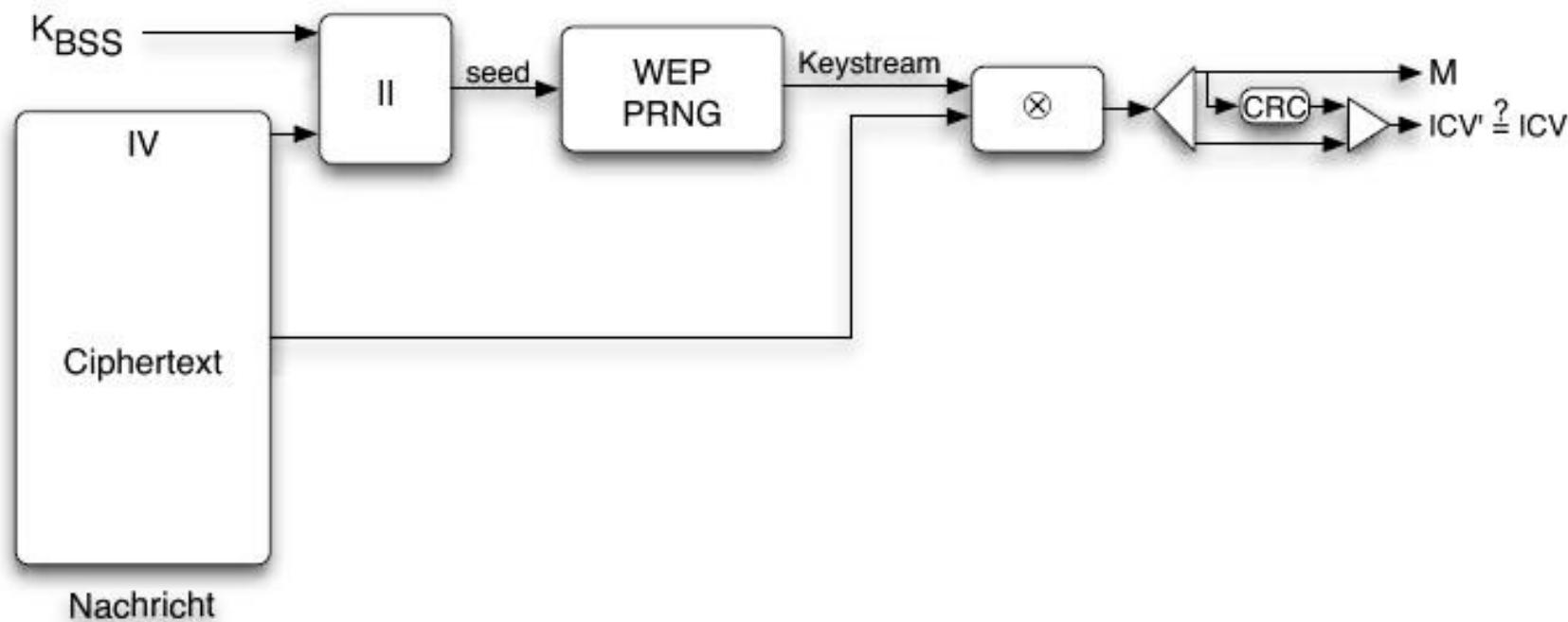
- Mallet und Eve haben es im WLAN (wg. Funk) noch einfacher als in kabelgebundenen Netzen
- Sicherheitsanforderungen
 - ❑ Authentisierung der Teilnehmer
 - ❑ Zugangskontrolle zum Netz (Autorsierung)
 - ❑ Vertraulichkeit der Daten
 - ❑ Integrität der Daten
- Sicherheitsmechanismen
 - ❑ Wired Equivalent Privacy (WEP)
 - ❑ WiFi Protected Access (WPA)
 - ❑ WiFi Protected Access 2 (WPA2)
 - ❑ IEEE 802.11i
 - ❑ WiFi Protected Access 3 (WPA3) (2018)

Wired Equivalent Privacy (WEP)

- Klartext wird mit Bitstrom XOR-verknüpft
- Bitstrom wird mit RC4 als Pseudozufallszahlengenerator (WEP PRNG) erzeugt
 - Für jede Nachricht 24-bit Initialisierungsvektor (IV) konkateniert mit 40-bit WEP-Schlüssel als 64-bit Seed für PRNG
 - Nachricht konkateniert mit CRC wird mit dem Bitstrom XOR-verknüpft



- IV wird im Klartext mit jedem Chiffretext übertragen
 - Jeder, der K_{BSS} kennt, kann Keystream erzeugen und Nachricht entschlüsseln
 - Selbstsynchronisierung von WEP
- Entschlüsselung ist inverser Vorgang zur Verschlüsselung



Integritätssicherung mit CRC-32

- Cyclic Redundancy Check (CRC) ist ein Fehlererkennungcode
- Entwickelt, um Übertragungsfehler u.a. in Ethernet zu erkennen
- Mathematische Grundlagen:
 - Bit-String wird als Polynom mit Koeffizienten 0 und 1 aufgefasst
 - Nachricht M wird interpretiert als Polynom $M(x)$
 - Berechnungen modulo 2; d.h. Addition und Subtraktion identisch mit XOR
- Berechnung des CRC-Werts von $M(x)$ zur Integritätssicherung:
 - Einigung auf Generatorpolynom $G(x)$ (i.d.R. standardisiert)
 - Sei n der Grad von $G(x)$, dann ist $n+1$ die Länge des Bit-Strings von $G(x)$
 - $M(x)$ wird durch $G(x)$ geteilt
 - Teilungsrest $M(x) \bmod G(x)$ ist CRC-Wert und wird an M angehängt
 - Empfänger berechnet: Gesamtnachricht $(M(x) | \text{CRC}) \bmod G(x)$
 - = 0; Nachricht wurde bei der Übertragung nicht verändert (außer Änderung ist Vielfaches von $G(x)$)
 - ≠ 0; Nachricht wurde verändert

- Bei Open System Authentication ohne Verschlüsselung kann jeder senden
- Falls WEP aktiviert ist, kann nur senden, wer KBSS kennt
- Keine individuelle Benutzeroauthentifizierung mittels WEP möglich
- Viele APs bieten zusätzlich MAC-adressbasierte Access Control Listen (ACLs)
 - Nur bekannte/freigeschaltete MAC Adressen dürfen senden, aber
 - MAC kann einfach mitgelesen werden
 - MAC kann einfach gefälscht werden

- WEP erfüllt **KEINE** der Sicherheitsanforderungen:
- Vertraulichkeit:
 - Schlüsselmanagement und Schlüssel sind ein Problem
 - WEP ist einfach zu brechen
 - Jeder der KBSS kennt, kann alle damit verschlüsselten Nachrichten mitlesen
- Integrität
 - CRC ist kein geeignetes Verfahren zur Integritätssicherung bei absichtlicher Manipulation
- Authentisierung
 - basiert auf WEP
- Zugriffskontrolle
 - Keine individuelle Authentifizierung, somit generell nur rudimentäre Zugriffskontrolle möglich

- RC4 ist Stromchiffre, d.h. der selbe Seed sollte nicht wiederverwendet werden
 - IV soll dies verhindern
 - IV wird aber im Klartext mit übertragen
 - 24 Bit für den IV sind deutlich zu kurz
- Wiederverwendung des Keystream (bei gleichem IV)
 - Zwei Klartextnachrichten M_1 und M_2 mit Plaintext $P_i = (M_i | CRC_i)$
 - Mit Ciphertext $C_1 = P_1 \oplus RC4(IV_1, K_{BSS})$
 - und $C_2 = P_2 \oplus RC4(IV_1, K_{BSS})$ gilt:
 - $C_1 \oplus C_2 = (P_1 \oplus RC4(IV_1, K_{BSS})) \oplus (P_2 \oplus RC4(IV_1, K_{BSS})) = P_1 \oplus P_2$
 - d.h. falls Angreifer M_1 und C_1 kennt, kann er P_2 (somit M_2) aus dem mitgehörten C_2 berechnen, ohne K_{BSS} zu kennen
(Known-Plaintext Angriff)
 - Known-Plaintext ist einfach zu erzeugen (Daten von außen schicken)

Traffic Injection

- Known-Plaintext Angriff: Mallet kennt M und C :
$$C = \text{RC4}(\text{IV}, K_{\text{BSS}}) \oplus (M, \text{CRC}(M))$$
- Damit kann Mallet den Key Stream berechnen:
$$\text{RC4}(\text{IV}, K_{\text{BSS}}) = C \oplus (M, \text{CRC}(M))$$
- Absichtliche Wiederverwendung alter IVs möglich:
Mallet berechnet
$$C' = \text{RC4}(\text{IV}, K_{\text{BSS}}) \oplus (M', \text{CRC}(M'))$$

und schickt (IV, C') an Bob
- Bob hält dies für ein gültiges Paket

- Wissen über verwendete höherliegende Protokolle erleichtert auch einen rein passiven Known-Plaintext Angriff:
 - Protokoll-Header, Adressen, Protokollprimitive sind Teile von M , meist an festen und bekannten Positionen

Integritätssicherung

- CRC und RC4 sind linear
- Mallet fängt Nachricht von Alice an Bob ab: (IV, C) mit
 $C = RC4(IV, K_{BSS}) \oplus (M, CRC(M))$
- Mallet verfälscht die Nachricht M zu Nachricht X :
 - Mallet wählt beliebige Nachricht M' mit derselben Länge
 - Mallet sendet Ciphertext $C' = C \oplus (M', CRC(M')) =$
 $RC4(IV, K_{BSS}) \oplus (M, CRC(M)) \oplus (M', CRC(M')) =$
 $RC4(IV, K_{BSS}) \oplus (M \oplus M', CRC(M) \oplus CRC(M')) =$
 $RC4(IV, K_{BSS}) \oplus (M \oplus M', CRC(M \oplus M')) =$
 $RC4(IV, K_{BSS}) \oplus (X, CRC(X))$
- Mallet kennt Inhalt von X nicht, da er M nicht kennt
- Aber: Eine „1“ an Position n in M' führt zu gekipptem Bit an Position n in X ; Mallet kann kontrollierte Änderungen in M durchführen. Beispiel: Zieladresse von IP-Paketen ändern

Breaking 104-bit WEP in less than 60 seconds

- Artikel von Tews, Weinmann, Pyshkin, TU Darmstadt, 2007
- Aktiver Angriff
- Nutzt ARP-Request- und ARP-Reply-Pakete
 - Feste Länge der Pakete
 - Über Länge der Frames sind die verschlüsselten ARP Pakete erkennbar
 - Die ersten 16 Byte des ARP Paketes sind vorhersagbar
 - 8 Byte LLC Header (AAAA 03 00 00 00 08 06) gefolgt von
 - 8 Byte ARP Header:
 - 00 01 08 00 06 04 00 01 für ARP Request
 - 00 01 08 00 06 04 00 02 für ARP Response
 - XOR Verknüpfung abgehörter Pakete mit dieser Bytefolge liefert die ersten 16 Byte des Keystream
 - Wiedereinspielen abgehörter ARP Requests beschleunigt den Angriff
 - Erfolgsrate bei nur 40.000 Frames schon > 50 %
 - Erfolgsrate bei 85.000 Frames rund 95 %

- WEP ist **NICHT** sicher
- WEP **NICHT** verwenden

WiFi Protected Access (WPA)

- WPA zur Verbesserung der Sicherheit eingeführt
- WEP-Hardware sollte weiter benutzbar bleiben
- Vertraulichkeit:
 - Temporal Key Integrity Protocol (TKIP)
 - Rekeying-Mechanismus zum automatischen Wechseln der Schlüssel
 - Hierarchie von Schlüsseln
- Integritätssicherung
 - TKIP Message Integrity Code - MIC (genannt „Michael“);
zur Unterscheidung von MAC (Media Access Control)
 - Mit Schlüssel parametrisierte kryptographische Hash-Funktion
 - Verbessert ungeeigneten CRC-Mechanismus von WEP
- Authentisierung
 - Nach wie vor Möglichkeit für Pre-Shared Key (PSK)
 - Bietet aber auch 802.1X (insb. in großen IT-Infrastrukturen genutzt)

Temporal Key Integrity Protocol (TKIP)

- TKIP verwendet Schlüsselhierarchie, um kurzlebige Schlüssel zu erzeugen
- Drei Hierarchiestufen (von unten nach oben):
 1. Temporäre Schlüssel (Temporal Key, TK)
 - In jede Richtung (AP zu STA, STA zu AP) eigene Schlüssel:
 - zur Verschlüsselung (128 Bit)
 - zur Integritätssicherung (64 Bit)
 - Erneuerung des Schlüsselmaterials durch `rekey key` Nachricht
 - `rekey key` Nachricht enthält Material, damit STA und AP neue Sitzungsschlüssel ableiten können; Nachricht verschlüsselt mit
 2. Pairwise Transient Key (PTK)
 - Sichern die Übertragung temporärer Schlüssel
 - 1 Schlüssel zur Sicherung des Schlüsselmaterials
 - 1 Schlüssel zur Sicherung der `rekey key` Nachricht

3. Pairwise Master Key (PMK)

- Höchster Schlüssel innerhalb der Hierarchie
- Erzeugt vom 802.1X Authentication Server und vom AP an STA weitergereicht
- Individuell pro Endgerät (AP)
- Falls 802.1X Setup „zu komplex“; Preshared Keys möglich (d.h. in der Praxis: Passwörter)
- Master Key wird zur Sicherung der key-encryption Keys genutzt
- Damit Aufbau einer Sitzungsstruktur möglich; von der Authentisierung über 802.1X bis
 - Widerruf des Schlüssels
 - Ablauf des Schlüssels
 - STA verliert Kontakt zum AP
- Achtung: Kompromittierung des Master Key führt zur Kompromittierung der gesamten Hierarchie!

TKIP Schlüsselhierarchie Zusammenfassung

- Aus IEEE 802.11i-2004 (geht über reines TKIP hinaus)
- hier Verwendung von 802.1X

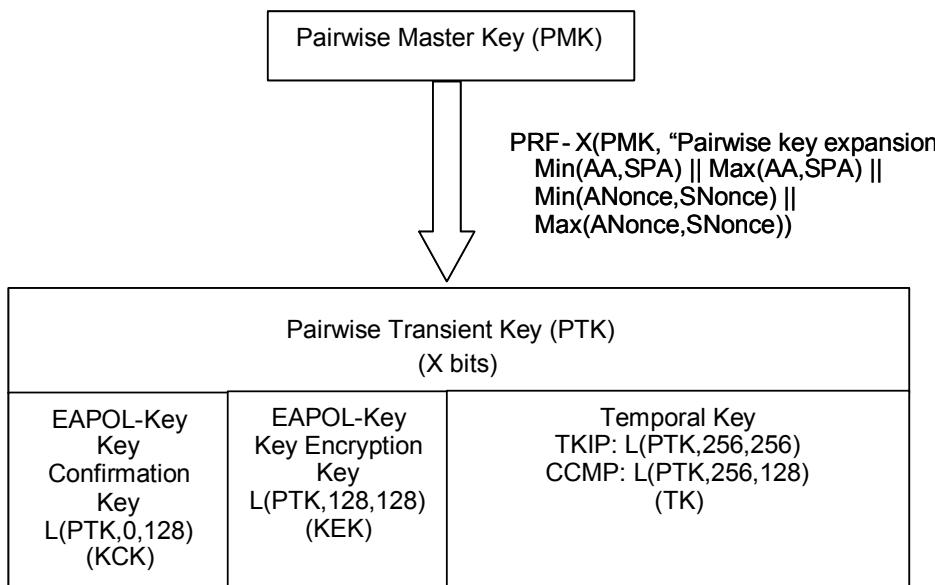


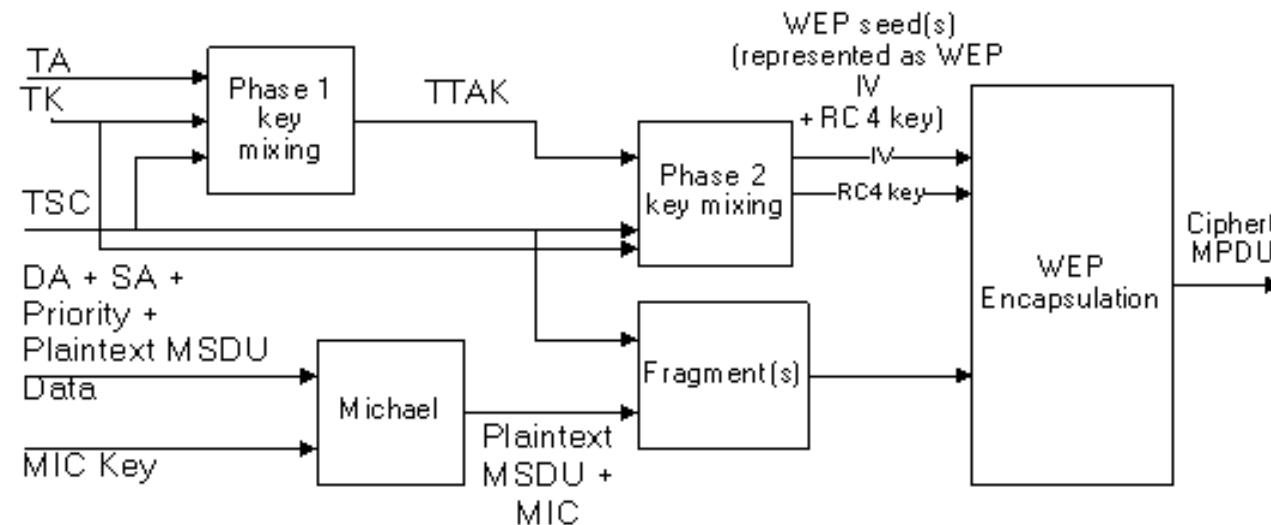
Figure 43s—Pairwise key hierarchy

- **PRF** Pseudo Random Function
- **AA** Authenticator Address
- **SPA** Supplicant Address
- **EAPOL** EAP over LAN
- **KCK** Key Confirmation Key (Integritätssicherung)
- **KEK** Key Encryption Key
- **L(x,0,128)** Teilstring ab Bit 0 mit Länge von 128
- **X(x) = L(x,0,512)** bei TKIP; **L(x,0,384)** bei CCMP

- CCMP ist Bestandteil von WPA2 (später)
- PRF: Pseudo Random Function zur Schlüsselableitung (vgl. PKCS#5 oder RFC2898)

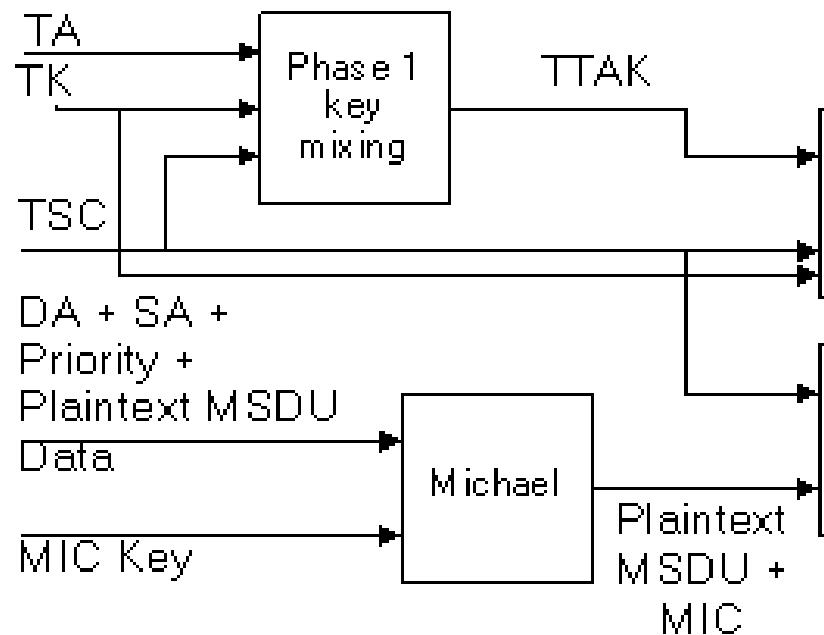
TKIP Verschlüsselung: Blockdiagramm

- Aus IEEE 802.1i-2004



- | | | | |
|-------|-----------------------|--------|----------------------------|
| ■ TA | Transmitter Address | ■ MSDU | MAC Service Data Unit |
| ■ TK | Temporal Key | ■ MPDU | Message Protocol Data Unit |
| ■ TSC | TKIP Sequence Counter | ■ TTAK | TKIP Mixed Address and Key |
| ■ DA | Destination Address | ■ MIC | Message Integrity Code |
| ■ SA | Source Address | | |

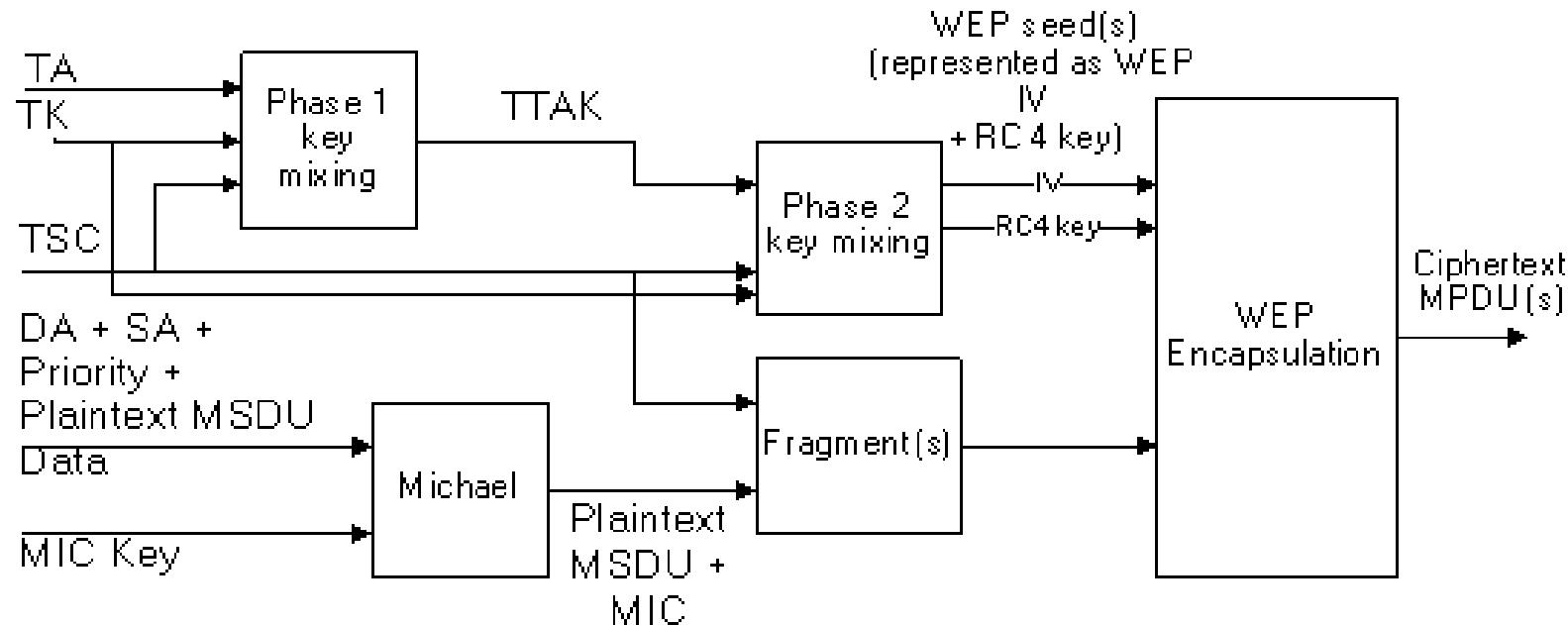
TKIP Verschlüsselung



- **TTAK** TKIP Mixed Address and Key
- **TK** Temporal Key
- **TSC** TKIP Sequence Counter

- **Phase 2 Key Mixing**
 - TTAK = Phase1(TA, TK, TSC)
 - Phase2(TTAK, TK, TSC)
 - Phase2 ist Feistel-Chiffre:
 - Einfache Operationen für „schwache“ AP-Hardware
 - XOR, UND, ODER, >>
 - S-Box
 - Erzeugt 128 Bit WEP-Schlüssel
 - 24 Bit Initialisierungsvektor
 - 104 Bit RC4-Schlüssel

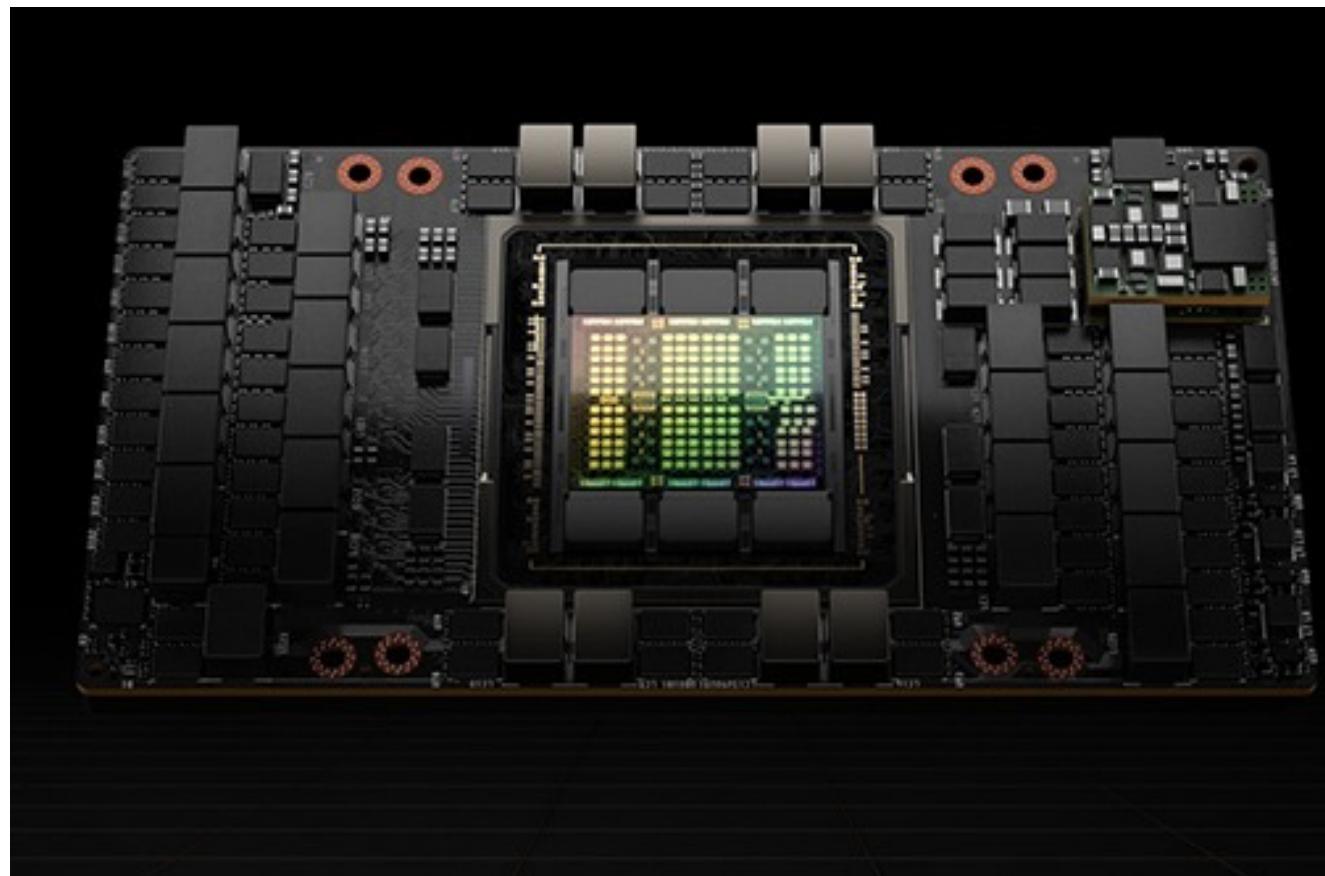
TKIP Verschlüsselung: Zusammenfassung



- Für jedes Frame (MSDU) wird eigener Schlüssel generiert
- Hardware-Abwärtskompatibilität; d.h. Verwendung von RC4 nach wie vor problematisch

- Bei Verwendung von Pre Shared Keys (PSK) hängt die Sicherheit stark von der Stärke des Passworts ab
- Angriff mit Rainbow-Tables (seit 2004)
- Angriff auf PRF Funktion der Schlüsselverteilung (August 2008)
 - nutzt GPUs (Graphics Processing Units) anstatt CPUs
 - Entwickelt auf NVIDIA-CUDA (Compute Unified Device Architecture)
 - Compiler und Entwicklungsumgebung
 - nativer Zugriff auf GPUs auf Grafikkarten
 - dadurch massive Parallelisierung möglich
 - damit Speedup von Faktor 30 und mehr möglich
 - Zeit für „Raten“ eines Passwortes reduziert sich auf 2-3 Tage

- 2022 announcement,
Codename Hopper
- 7296 Cores
- 134 TFlops (10^{12})
(Single Precision, FP32)
68 TFlops (Double
Precision, FP64)
- 2 x 350-400 W



NVIDIA DGX H100

- 8 x H100 GPU
- 640 GB GPU-Speicher
- 4 x NVIDIA NVSwitches
 - 7,2 TB/s zwischen GPUs
 - Netzinterface mit 400 Gb/s
- Dual x86 CPU mit 2 TB Speicher
- 30 TB NVMe-SSD
- 10,2 kW (ohne Kühlung)



Top 500 - Liste der 500 schnellsten Rechner weltweit

2	Aurora - HPE Cray EX - Intel Exascale Compute Blade, Xeon CPU Max 9470 52C 2.4GHz, Intel Data Center GPU Max, Slingshot-11, Intel DOE/SC/Argonne National Laboratory United States	4,742,808	585.34	1,059.33	24,687		
3	Eagle - Microsoft NDv5, Xeon Platinum 8480C 48C 2GHz, NVIDIA H100, NVIDIA Infiniband NDR, Microsoft Microsoft Azure United States	1,123,200	561.20	846.84			
9	Eos NVIDIA DGX SuperPOD - NVIDIA DGX H100, Xeon Platinum 8480C 56C 3.8GHz, NVIDIA H100, Infiniband NDR400, Nvidia NVIDIA Corporation United States	485,888	121.40	188.65			

Top 500 - Abschätzung Energieverbrauch Platz 3 und 9

- Annahmen:
 - NVIDIA H100 SXM-Modul: Betrieb im 700 W Modus und 67 TFlop/s Leistung
 - Theoretical Peak (Rpeak) - ausschließlich aus den H100-GPUs
- **Eagle (Platz 3)**
 - 847 PFlops/s Leistung entspricht 12.640 H100 SXM Module
 - entspricht 1.580 DGX H100
 - DGX H100 benötigt 10,2 kW
 - Stromaufnahme **16.116 kW** (ohne Kühlung)
- **Eos NVIDIA (Platz 9)**
 - 187 PFlop/s entspricht 2.792 H100 SXM Module
 - entspricht 349 DGX H100
 - Stromaufnahme **3.560 kW** (ohne Kühlung)

NVIDIA DGX SuperPod





Energieeffizienz im Rechenzentrum: Maßzahlen

- Power Usage Effectiveness (PUE)

$$PUE = \frac{\text{Gesamtenergieverbrauch}}{\text{Energieverbrauch IT}}$$

$$PUE > = 1,0$$

PUE je näher an 1,0 umso besser

- typische PUE-Werte
 - RZ mit Luftkühlung (1,5 bis 2,x)
 - RZ mit Wasserkühlung (< 1,5)
- Grenzen des PUE
 - Geographische Lage (Nordfinnland im Vergleich zu Spanien)
 - Steigender Stromverbrauch der IT führt zu sinkendem PUE
- ABER:
 - PUE gut als Maßzahl für die Bewertung von Maßnahmen in einem RZ
 - Vergleich der Größenordnung des PUE verschiedener RZ

Eagle - Stromverbrauch und Kosten

- Stromaufnahme 16.116 kW (ohne Kühlung)
- Kühlungsaufschlag: PUE 1,65 - 1,89
 - ca. 30 % Lüfter, 30 % Kältekompressionsmaschinen
- Stromaufnahme im Normalbetrieb ~ 60% - 70% der Spitzenlast, d.h. 10.500 kW
- Stromaufnahme inkl. Kühlung bei 8.400 Betriebsstunden pro Jahr
 - $10.500 \text{ kW} * 1,65 * 8.400 \text{ h/a} = 145.530.000 \text{ kWh/a}$
 - **146 GWh**
- Zum Vergleich:
 - durchschnittlicher Stromverbrauch pro Person 1.500 kWh/a
 - Tesla Model Y (LR) ~ 18,5 kWh/100 km
- Eagle verbraucht pro Jahr so viel Strom wie
 - 97.000 Personen (Erlangen: 117.000, Bamberg 80.000)
 - 786 Mrd. Tesla Kilometer
 - 38.400 Tesla Model Y mit einer Jahreslaufleistung von 20.000 km/a

Stellenanzeige Microsoft vom Oktober 2023

Principal Program Manager Nuclear Technology | Microsoft Careers

01.10.23, 13:11

Job you selected

Principal Program Manager Nuclear Technology

5 days ago

Multiple Locations, United States

Up to 100% work from home

"The next major wave of computing is being born, as the Microsoft Cloud turns the world's most advanced AI models into a new computing platform," said Satya Nadella, chairman and chief executive officer of Microsoft. "We are committed to helping our customers ..."

[See details](#)

< Show similar jobs

Principal Program Manager Nuclear Technology

Multiple Locations, United States

[Apply](#)

[Save](#)

[Share job](#)

* No longer accepting applications

Date posted **Sep 25, 2023**

Job number **1627555**

Work site **Up to 100% work from home**

Travel **0-25 %**

Role type **Individual Contributor**

Profession **Program Management**

Discipline **Technical Program Management**

Employment type **Full-Time**

Feedback

We're looking for a Principal Program Manager, Nuclear Technology, who will be responsible for maturing and implementing a global Small Modular Reactor (SMR) and microreactor energy strategy.

This senior position is tasked with leading the technical assessment for the integration of SMR and microreactors to power the datacenters that the Microsoft Cloud and AI reside on. They will maintain a clear and adaptable roadmap for the technology's integration, diligently select and manage technology partners and solutions, and constantly evaluate the business implications of progress and implementation.



NVIDIA DGX A100
8 GPUs pro DGX
16 GPUs pro Rack
Luftgekühlt
PUE: 1,65-1,80



MCML im Vergleich zu terrabyte



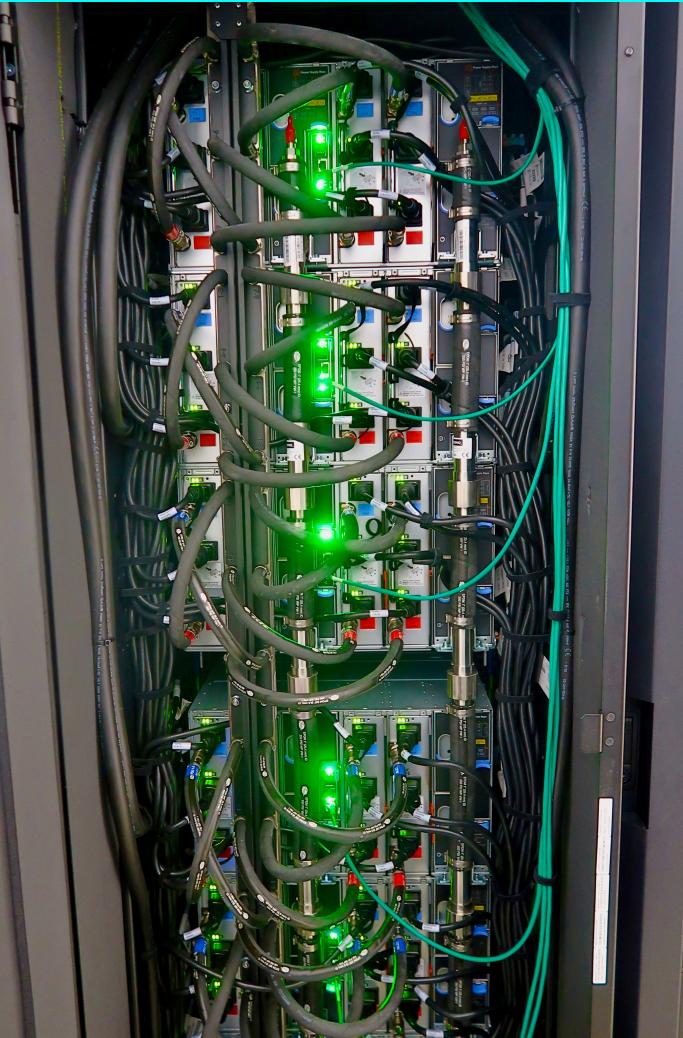
NVIDIA DGX A100
8 GPUs pro DGX
16 GPUs pro Rack
Luftgekühlt
PUE: 1,65-1,80

NVIDIA DGX A100
4 GPUs pro DGX
bis zu 144 GPUs pro Rack
Direkt Warmwassergekühlt
frei Kühlung das ganze Jahr
PUE: 1,03-1,05



terabyte

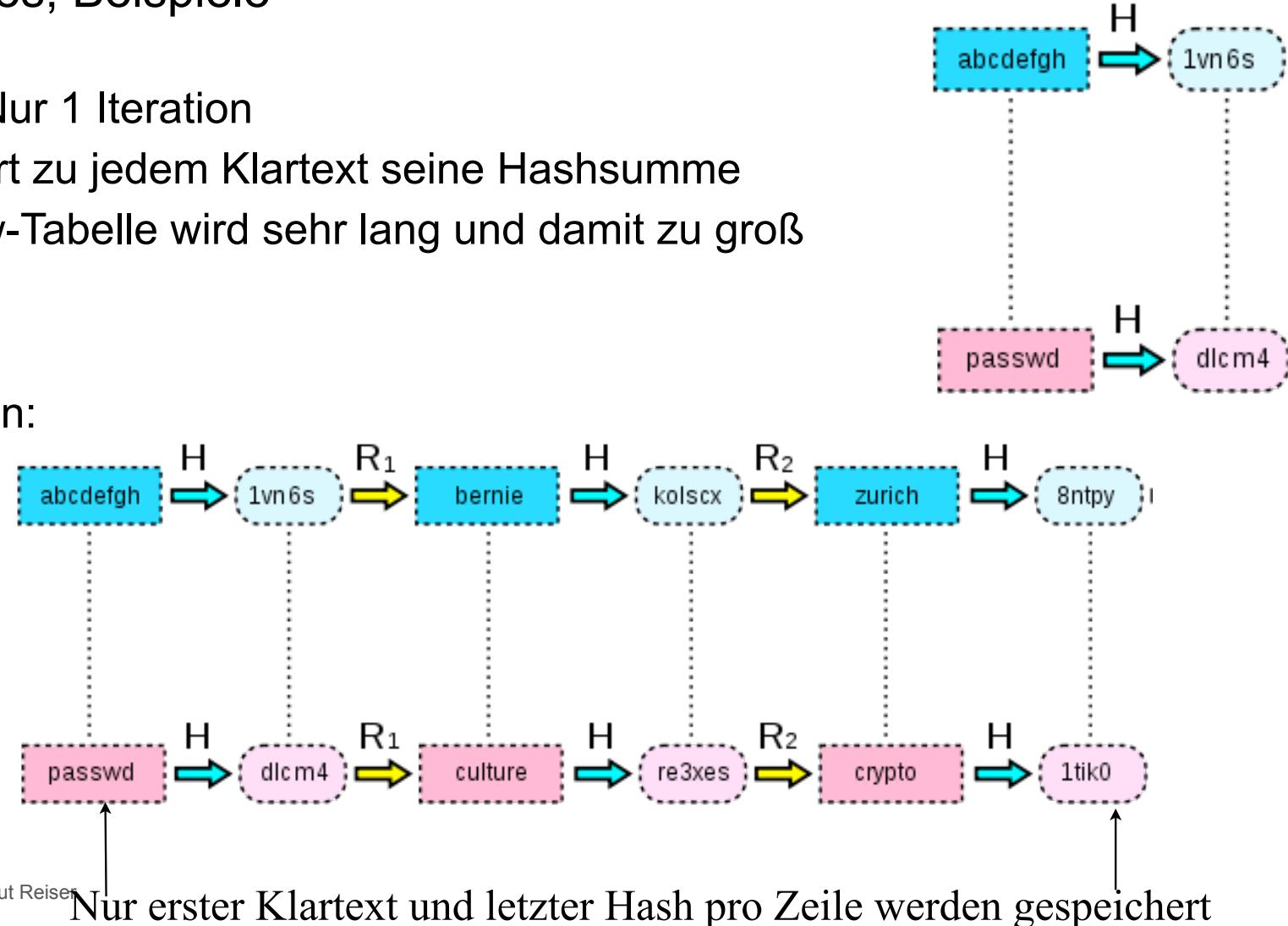
NVIDIA DGX A100
4 GPUs pro DGX
bis zu 144 GPUs pro Rack
Direkt Warmwassergekühlt
frei Kühlung das ganze Jahr
PUE: 1,03-1,05



- Bei allen Krypto-Angriffen ist Rechenzeit- und Speicherplatzkomplexität zu betrachten
- Rainbow-Tables versuchen, optimalen time-memory tradeoff zu nutzen, um vollständigen Brute-Force-Angriff zu sparen
- Idee: Optimale Speicherung einer Klartext-zu-Hash Tabelle
- Kompakte Speicherung von sog. Chains (Ketten/PW-Sequenzen)
 - Kette startet mit initialem Klartext-Wort, dieses wird gehasht
 - resultierender Hash wird Reduktionsfunktion unterworfen
 - Reduktionsfunktion liefert weiteres potentielles Klartext-Wort
 - Dieser Vorgang wird n-mal wiederholt
 - relevant sind nur erstes Klartext-Wort und letzter Hash-Wert
 - Vorgang wird einmal für alle Wörter eines Wörterbuchs wiederholt
 - Kollisionen vermeiden: internes Klartext-Wort darf nicht Startwert einer anderen Kette sein

Rainbow Tables; Beispiele

- Trivialfall: Nur 1 Iteration
 - Speichert zu jedem Klartext seine Hashsumme
 - Rainbow-Tabelle wird sehr lang und damit zu groß
- 3 Iterationen:



Rainbow Tables: Anwendung

- Rainbow-Tabelle mit w Einträgen und Ketten der Länge n
- MD5 Hash: bca6a2aed3edc8e22f68ed65e39682c6 („IT-Sec“)
- Suche in Tabelle auf rechter Seite. Fallunterscheidung:
 1. Hash-Wert gefunden, steht z.B. in Zeile 17
 - Kette aus Zeile 17 komplett durchlaufen
 - $(n-1)$ te Anwendung der Reduktionsfunktion liefert den gesuchten Klartext
 2. Hash-Wert steht nicht in Rainbow-Table
 - Reduktion des Hashes (vereinfachtes Bsp. erste 6 Zeichen): bca6a2
 - MD5(bca6a2) liefert 3c41c8c8c5d27647d3f64937a801c90a
 - Suche diesen Hash in Tabelle
 - In der Praxis werden verschiedene Reduktionsfunktionen kombiniert
 - Ziel: Kollisionen / Wiederholungen vermeiden, um möglichst viele Klartexte abzudecken

Angriff auf TKIP Verschlüsselung

- Beck, TU Dresden, Tews, TU Darmstadt; publ. 08.11.2008
- Erstes Verfahren, das keine Pre Shared Keys voraussetzt
- Basiert auf chop-chop Angriff (bekannt seit 2005)
- Funktionsweise:
 - Angreifer schneidet Verkehr mit, bis er verschlüsseltes ARP-Paket findet (vgl. Folien „Breaking WEP in less than 60 seconds“)
 - letztes Byte wird entfernt
 - Annahme: Byte war 0; mit XOR-Verknüpfung mit bestimmten Wert wird versucht, eine gültige Checksumme zu erzeugen
 - Paket wird an STA gesendet:
 - Inkorrekt: Paket wird verworfen
 - Korrekt: Client erzeugt MIC Failure Report Frame; Angreifer muss dann vor nächstem Versuch 60 Sekunden warten, sonst erzwungener Verbindungsabbau
 - Worst Case: 256 Tests für 1 Byte erforderlich. Praktisch: In 12 Minuten mindestens 12 Byte entschlüsselbar.

- Sicherheitsmaßnahmen von WPA
 - Anti-chopchop: zwei falsche MICs in 1 Minute \Rightarrow Verbindungsabbau
 - TSC (Sequenznummer) verhindert Wiedereinspielen
- Gegenmaßnahmen:
 - 60 Sekunden warten (vgl. Folie vorher)
 - Replay nicht an verwendeten, sondern an anderen Sendekanal
- Entschlüsselung des ARP Pakets ermöglicht:
 - Schlüsselstrom vom AP zu STA und MIC Code können ermittelt werden
 - Eigene verschlüsselte Pakete können an STA gesendet werden; z.B. zum Manipulieren von ARP-Paketen
- Grenzen des Angriffs
 - Rekeying-Intervall muss ausreichend groß sein
 - QoS muss aktiviert sein, sonst stehen keine 8 Kanäle zur Verfügung
 - nur eine Richtung: AP zu STA

WPA-Schlüssel in der Cloud brechen (Jan. 2011)



- Angriff auf WPA-Schlüssel (Pre-Shared Keys) über die Elastic Compute Cloud (EC2) Infrastruktur von Amazon
- Prinzipiell nichts Neues, nutzt nun aber die Cluster GPU Instances
- Wörterbuch-Angriff mit 70 Millionen Wörtern; pro Amazon-Maschine rund 50.000 Wörter pro Sekunde
- Alternative z.B. www.wpacracker.com: \$17 für Wörterbuch-Angriff mit mehr als 250 Millionen Wörtern auf 400 „herkömmlichen“ Amazon CPU Instances

- WPA **NICHT** verwenden

- Empfehlung: Verwendung von WPA 2 anstelle von WPA
- Änderungen:
 - AES ersetzt verpflichtend RC4
 - CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) als Ersatz für TKIP
- Verfahren gilt derzeit als sicher
 - Verpflichtend für Geräte mit Wi-Fi Logo

- Im Juni 2018 als Ergänzung zu WPA 2 standardisiert
- Authentisierung mit Simultaneous Authentication of Equals (SAE) - Drageonfly Protokoll; für PreShared Key Netze
 - Sichere Generierung von Sitzungsschlüsseln
 - Schutz vor KRACK
 - Schutz in Mesh Netzen
- Schutz offener und Gast Netze
 - Oportunistic Wireless Encryption Methode (OWE, RFC 8110)
 - Individuelle Verschlüsselung pro Client
 - ohne individuelles Passwort
 - Diffie-Hellman Verfahren zur Erzeugung von PMKs