# Referat: Bluetooth, Wlan und NFC

Inhalt

[Referat: Bluetooth, Wlan und NFC 1](#_Toc530587852)

[WLAN 2](#_Toc530587853)

[Allgemeines 2](#_Toc530587854)

[IEEE-Norm 2](#_Toc530587855)

[Bitübertragungsverfahren 2](#_Toc530587856)

[Frequency Hopping Spread Spectrum(FHSS) 2](#_Toc530587857)

[Sicherheit 6](#_Toc530587858)

[WEP (Wired Equivalent Privacy) 6](#_Toc530587859)

[WPA (Wi-Fi Protected Access) 7](#_Toc530587860)

[WPA2 (Wi-Fi Protected Access 2) 7](#_Toc530587861)

[TKIP und CCMP – Was steckt dahinter 8](#_Toc530587862)

[TKIP (Temporal Key Integrity Protocol) 8](#_Toc530587863)

[CCMP (Counter-Mode/CBC-MAC Protocol) 8](#_Toc530587864)

[Welche WLAN Verschlüsselung ist die sicherste Wahl? 8](#_Toc530587865)

[Bluetooth 9](#_Toc530587866)

[NFC 9](#_Toc530587867)

# WLAN

## Allgemeines

WLAN steht für „Wireless Local Area Network“ und wurde 1963 durch die Verbindung zwischen American Institute of Electronical Engineers (AIEE) und Institute of Radio Engineers (IRE) erfunden. Dadurch wurde der Zusammenschluss zwischen Elektrotechnikern und Informatikern garantiert. 1980 wurden die IEEE 802 Normen gegründet und 1999 die Wireless Ethernet Compatibility Alliance. Später wurde sie in WIFI-Alliance umbenannt und zertifiziert Wi-Fi Produkte, um gewisse Standards einzuhalten. Nicht jedes IEEE 802.11 konforme Gerät ist automatisch Wi-Fi Aliance konform.

## IEEE-Norm

Begonnen wurde mit der Erstellung von der IEEE-Norm 802.11. Herausgeber ist das [Institute of Electrical and Electronics Engineers](https://de.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers). Die Definition der [IEEE-802-Normen](https://de.wikipedia.org/wiki/IEEE_802), die zunächst ganz allgemein den Netzwerkzugriff beschreiben, begann im Februar 1980, daher wurde die Bezeichnung 802 gewählt.

Die heute verwendeten Normen sind: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac. Die neueste Norm ist 802.11ay die 2019 herauskommen wird.

* 802.11 ursprünglicher Standard, 1997 verabschiedet
  + Datenrate: 1 oder 2 Mbit/s brutto
  + Frequenzband 2,400 –2,485 GHz
  + Lizenzfreies ISM-Band (Frequenzbereiche, die durch Hochfrequenzgeräte in Industrie, Wissenschaft, Medizin, in häuslichen und ähnlichen Bereichen lizenzfrei und meist genehmigungsfrei genutzt werden können)
  + Vielfachzugriffe mit CSMA/CA (Träger- und Kollisionserkennung) (Kapitel …)

Der heute meist verwendete Standard ist 802.11b der mit einer Übertragungsrate von 11 Mbits/s im 2,4 GHz Frequenzbereich operiert und das DSSS-Verfahren verwendet(kapitel).

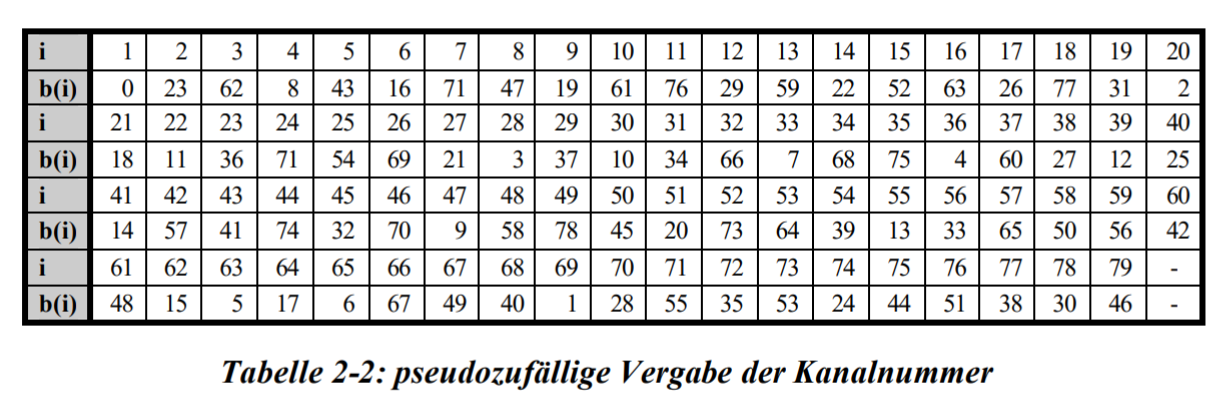
Um der ständigen Nachfrage nach Bandbreite gerecht zu werden, ist der IEEE 802.11a Standard entwickelt worden, um Geschwindigkeiten von bis zu 54 Mbits/s erreichen zu können. Realisiert wird dies in dem ebenfalls lizenzfreien 5,2 GHz Band mit dem OFDM Verfahren (Kapitel). Die Verwendung eines höheren Frequenzbandes hat zwei Nachteile: einerseits werden höhere Frequenzen stärker gedämpft, andererseits ist dieses Spektrum in Europa nicht vollständig zugelassen. Die Ursache liegt in der Überlappung des Frequenzbandes mit RADAR und anderen Funkdiensten. Hier muss eine weitere Entwicklung noch abgewartet werden.

## Bitübertragungsverfahren

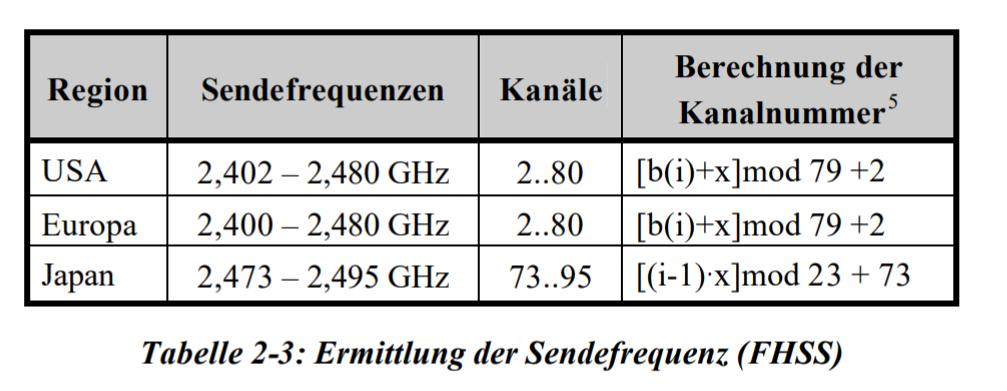
Die Störanfälligkeit der Bitübertragung muss hingegen der Drahtgebundenheit durch notwendige Verfahren kompensiert werden. Die ersten proprietären Übertragungen fanden schmalbandig statt, sind aber in der nächsten Generation durch Spreizspektrumtechniken abgelöst worden. Infrarot spielt in den IEEE 802.11 Standard nur eine optionale Rolle, die nicht weiter kommerziell genutzt wird.

### Frequency Hopping Spread Spectrum(FHSS)

In dem FHSS Standard sind nach IEEE 802.11 bis zu 79 nichtüberlappende Frequenzbereiche mit einer Bandbreite von jeweils 1 MHz vorgesehen, wobei 3 Gruppen mit je 26 Mustern zusammengefasst werden. Die Abfolge der Frequenzen wird an Hand einer Basisfolge b(i) berechnet, die einer Pseudozufallskette im Intervall von 0 bis 79 entspricht.



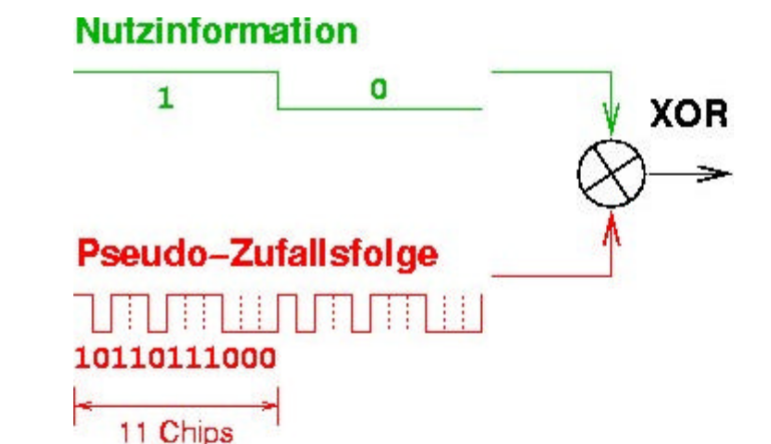
Wenn beim Modulationsverfahren ein Fehler beim Übertragen auf (Kollision, Störung…), kann das gleiche Paket auf einer anderen Frequenz versendet werden. Ein Abhören der Informationen ist nur möglich, wenn die Sendefrequenz bekannt ist. Diese Frequenz wird vor jeder Kommunikation von Sender und Empfänger vor Beginn nach folgender Tabelle pseudozufällig festgelegt.



Nur wenige Distributoren halten noch am FHSS Verfahren fest, denn mit einer Übertragungsgeschwindigkeit von 2 Mbit/s wird diese Technologie den heutigen Ansprüchen nicht mehr gerecht.

### Direct Sequence Spread Spectrum (DSSS)

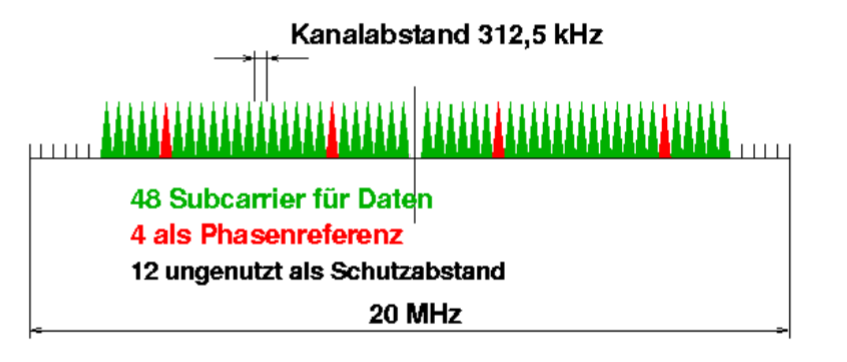
Beim DSSS-Verfahren stellt ein konstante Anzahl an Kanälen der Breite von 22 MHu zur Verfügung. Bei einem empfohlenen Kanalabstand von 25 MHz sind drei überlappungsfreie Kombinationen möglich. Jedes zu übertragende Bit wird mittels einer 11 Bit langen zufälligen Bitfolge kodiert und auf 13 MHz Bandbreite aufgespreizt gesendet. Dieses Signal ist somit ein weites Breitbandsignal, welches im Hintergrundrauschen verschwindet (militärische Anwendungen). Der Demodulationsprozess kann beim Empfänger nur durch Verwendung der richtigen Chip-Sequenz wieder rekonstruiert werden.



Aufgrund der technischen Notwendigkeit nach Bandbreitenmaximierung, hat sich das DSSS Verfahren mit bis zu 11 Mbit/s durchgesetzt und ist somit die augenblicklich von der Industrie favorisierte Technik.

#### Orthogonal Frequency Division Multiplexing (OFDM)

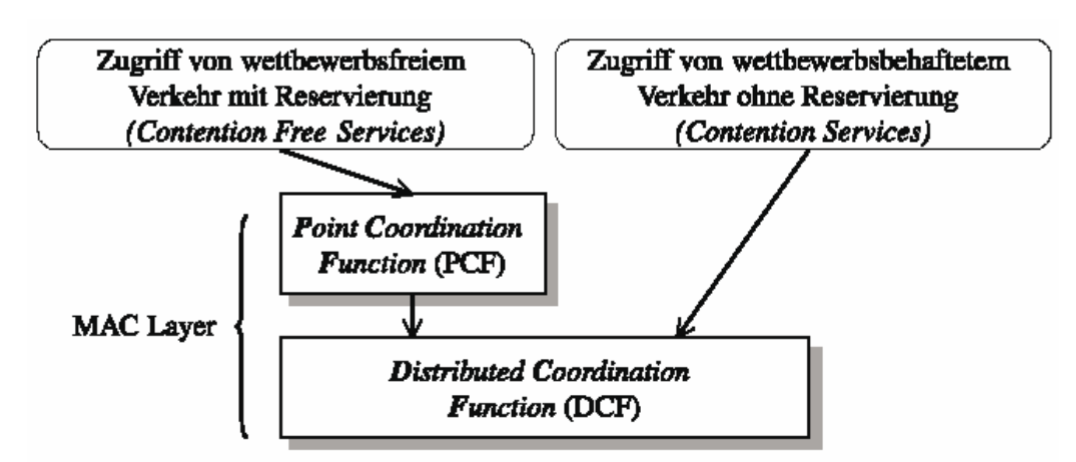
Dieses Verfahren ist im Gegensatz zum DSSS kein Spreizspektrumverfahren. Nach IEEE 802.11a wird das Spektrum in 11 nicht überlappende Kanäle aufgeteilt. Hierbei wird eine Information parallel über mehrere Frequenzen, den Unterfrequenzen (Subc arrier), gesendet.



Durch die Aufspaltung in mehrere Sub-Kanäle wird erreicht, dass weniger Bits fehlerhaft übertagen werden, die mit einem Korrektionsalgorithmus behoben werden können. Außerdem lässt sich jede Unterfrequenz optimal an die Eigenschaft des Übertragungskanals anpassen. Die herkömmlichen Frequenzmultiplexverfahren haben relativ große Abstände zwischen den Unterfrequenzen und somit das komplette Spektrum inneffizient ausnutzten. Als Modulationsverfahren wird die Phasenmodulation oder eine Kombination aus Amplituden und Phasenmodulation verwendet.

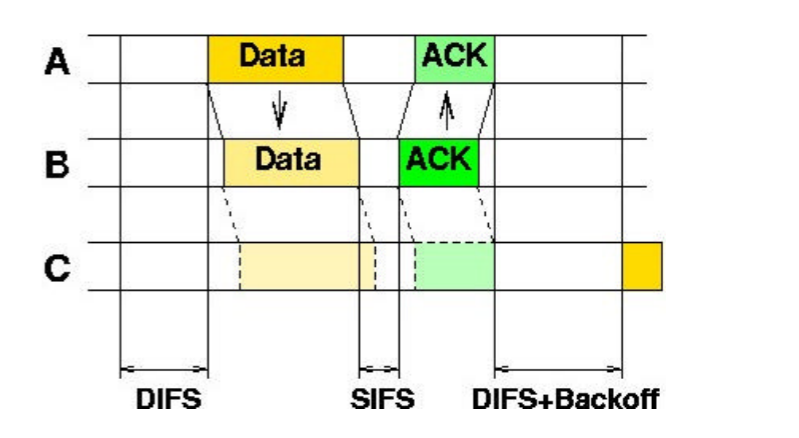
### Kanalzugriff

Bei Datentransporte über Funk können Kollisionen vermieden werden indem eine Reihenfolge der Sender festgestellt wird. Dies ist beim WLAN leider unmöglich, allerdings werden die Zeitspannen, in denen Kollisionen auftreten können, durch geschickte Algorithmen vermieden (CA). Der Zugriff erfolgt mit zwei unterschiedlichen Mechanismen, der Point Coordination Fuction (PCF) und der Distributed Coordination Function (DCF).

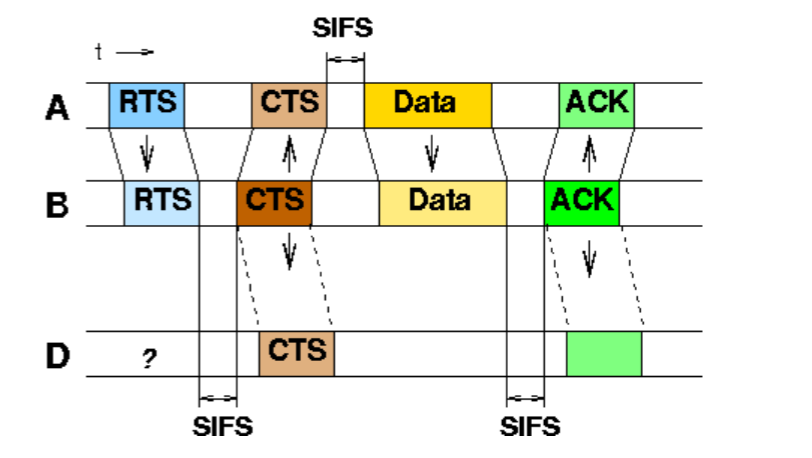


#### Distributed Coordination Function (DCF)

Bevor eine Übertragung stattfinden kann, muss das Medium abgehört werden (Carrier Sense). Zwei Fälle sind möglich. Ist das Medium nicht belegt, kann nach einer Abhörzeit (DIFS) das Senden auf diesem Kanal beginnen (Station A sendet an B) Die Versendung der Quittung (ACK) erfolgt nach einer weiteren Wartezeit (SIFS). Diese Wartezeiten haben eine konstante Länge, so dass alle Stationen in einem gleichen „Takt“ arbeiten. Die Verständigung wird über Broadcasting aller relevanten Stations- und Kanalinformationen erreicht. Ist das Medium belegt, wird die Übertragung in einen Wartezyklus (Backoff) gesetzt. Nach Ablauf der Wartezeit wird das Medium erneut kontrolliert.

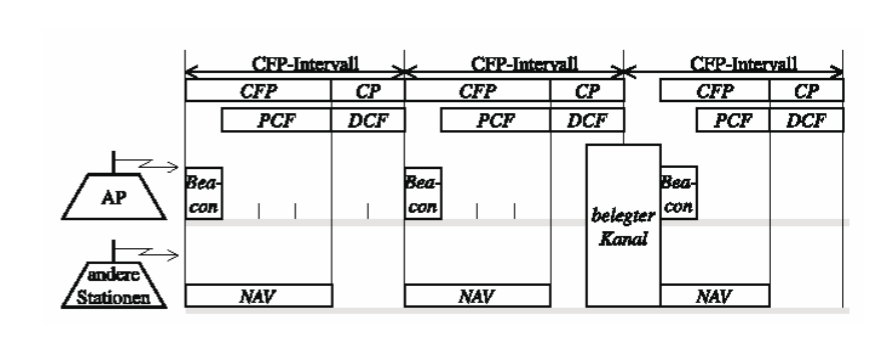


Das Verfahren funktioniert zuverlässig, wenn alle Stationen direkt miteinander kommunizieren. Normalerweise gefährden Hindernisse (hidden nodes) einen direkten Kontakt, so dass ein weiterer Zugriffsmechanismus (RTS/CTS) verwendet wird. Folgende Abbildung zeigt den gemeinsamen Kanalzugriff der Stationen A und B unter der Nebenbedingung, dass kein Informationskontakt zwischen der Station A zu der Station D besteht.



Ein RTS-Frame wird an alle sendewilligen Stationen gesendet. Dieser Rahmen enthält Informationen über die Dauer der Datenübertragung. Der adressierte Sender quittiert den Erhalt mit einem CTS-Frame ebenfalls an alle vorhandenen Stationen, die übrigen Empfänger schalten für die angegebene Zeit in einen unabhängig vom Backoff-Prozess vorgegebenen Wartemodus- Die Verwendung der SIFS-Zeit sichert der CTS-Anwort eine höhere Priorität gegenüber der normalen Übertragung. Schlägt die Sendung eines CTS-Frames fehl, erfolgt ein erneutes Senden des RTS-Frames nach Ablauf des Backoff-Zyklus.

#### Point Coordination Function (PCF)

Die PCF ist ein optionales Verfahren, zeitkritischen Diensten priorisierten Zugriff zu gewähren. Die PCF steuert die Übertragung der Rahmen während einer wettbewerbsfreien Zeit (CFP), die sich mit der durch die DCF gesteuerten Wettbewerbsperiode abwechselt (CP). Die CFP wird in regelmäßigen Zeitabständen mit der CFP-Rate wiederholt und startet mit der Übertragung eines Beacon-Rahmens, der die maximale Dauer der CFP enthält. 

## Netzwerkkonzepte

Der IEEE 802.11 Standard lässt verschiedene Kombinationen offen, wie ein drahtloses Netzwerk aufgebaut werden kann.

### Ad-Hoc

Das Ad-Hoc Netz ist eine direkte Verbindung von mobilen Stationen ohne Zugangspunkt. Somit ist die der einfachste Weg, eine drahtlose Kommunikation aufzubauen.

### Infrastruktur-Netz

Dies ist die Kombination aus drahtlosem und drahtgebundenem Netz. Notwendig für solch eine Anbindung ist ein Zugangspunkt (Access-Point). Der Access-Point koordiniert den gemeinsamen Datenverkehr. Er vermittelt zwischen LAN und WLAN sowie auch zwischen den mobilen Stationen.

### Roaming

Das aus dem Mobilfunk bekannte Verfahren des Roamings ermöglicht eine erweiterte, drahtlose Erreichbarkeit.

Voraussetzung hierfür ist, dass sich die Mobilstation im gleichen Sub-Netz befindet. Der WLAN Benutzer hat den Vorteil einer größeren Mobilität, ohne Veränderungen an seiner Konfiguration tätigen zu müssen.

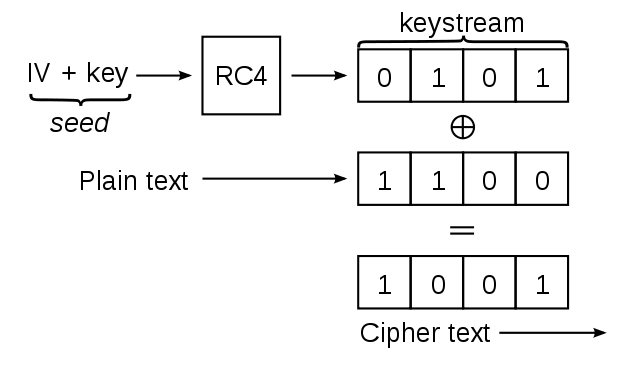
## Sicherheit

Am Anfang der IEEE-Standards war der Zugang zum Wlan offen und die Datenpakete nicht verschlüsselt.

### WEP (Wired Equivalent Privacy)

Die erste Form der WLAN Verschlüsselung war der Standard WEP. Er ist immer noch in vielen [aktuellen Routern](https://www.only4gamers.de/bester-wlan-router/) und Geräten implementiert, wobei seine Entwicklung auf das Jahr 1999 zurückgeht und die technischen Gegebenheiten dieser Ära wiederspiegelt. Damals schien sich dieses Protokoll als sicher zu erweisen, doch schon bald wurden viele Nutzer eines besseren belehrt. Seit dem Jahr 2001 gilt WEP als geknackt und die Routinen zur [Verschlüsselung](http://www.was-ist-malware.de/it-sicherheit/verschluesselung-definition-ziele-funktionsweise-und-verfahren/) sind inzwischen allgemein bekannt. Somit handelt es sich bei dieser WLAN Verschlüsselung um eine veraltete Technologie, die nicht mehr eingesetzt werden sollte.

Die Schwäche von WEP liegt vor allem in der Art des verwendeten Verschlüsslungs-Algorithmus. Dieser zeigte sehr schnell seine Lücken, denn die Anzahl der möglichen Code-Kombinationen beschränkt sich auf eine für Computer, durchaus überschaubare Zahl. Da nur 16.777.216 Möglichkeiten existieren, wiederholt sich der Schlüssel in heutigen Systemen relativ schnell. Ein Cracker kann also den WLAN-Verkehr mitsniffen und erhält mittels technischer Beschleunigungsverfahren innerhalb weniger Minuten den gesuchten WLAN-Code. Damit hat er Zugriff auf die übertragenen Daten und könnte sogar [Schadsoftware auf Ihren Computer](http://www.was-ist-malware.de/allgemein/schadsoftware/) installieren.

[](http://www.was-ist-malware.de/wp-content/uploads/2017/06/wlan-verschluesselung-wep.png)

### WPA (Wi-Fi Protected Access)

Als WEP im Jahre 2001 als absolut unsicher eingestuft wurde, sahen sich die Entwickler im Zugzwang. Eine neue Technik musste her, die nicht die Fehler der alten Methode wiederholte. So wurde WPA entwickelt und im Jahre 2003 mit der Zertifizierung begonnen.

Dabei unterscheidet sich die Funktionsweise von WPA nicht sonderlich von der des vormals verwendeten WEP. Es kommt auch bei diesem Standard immer noch die gleiche [RC4-Stromchiffre](https://www.kryptographiespielplatz.de/index.php?aG=5651c3bab8f2a5a60cc93b8e2a7e6a377eb26a34) zum Einsatz. Allerdings besitzt diese keinen festen 48-Bit Verschlüsselungs-Algorithmus mehr. Diese WLAN Verschlüsselung verwendet für jedes neue Datenpaket einen eigenen Key, sodass quasi jeder Block separat entschlüsselt werden muss. Diese Methode nennt sich Temporal Key Integrity Protocol – kurz TKIP (siehe weiter unten). Durch dieses Prinzip werden dynamische Keys erstellt, die ein Auslesen durch reines „Mithören“ unmöglich machen.

Allerdings bieten sich auch bei WPA Optionen, wie der Key herausgefunden werden kann. So können Brutforce-Angriffe durchaus zum Erfolg führen, denn hierbei werden alle möglichen Kombinationen ausprobiert, bis ein korrektes Passwort für den Router ermittelt werden konnte. Daher hängt es allein von der Komplexität des Passwortes ab, wie lange es dauert, bis WPA von einem Cracker umgangen wurde.

### WPA2 (Wi-Fi Protected Access 2)

Als die Schwachstellen von WPA bekannt wurden und somit das Sicherheitsrisiko wieder beim User lag – er musste ein komplexes Passwort wählen – wurde eine Weiterentwicklung in Angriff genommen. Aus diesem Prozess ging dann WPA2 hervor, welches im Jahre 2005 auf den Weg gebracht wurde.

WPA2 setzt ausschließlich auf [AES (Advanced Encryption Standard)](http://www.was-ist-malware.de/it-sicherheit/advanced-encryption-standard-aes/). So kann diese WLAN Verschlüsselung bis zu 256-Bit verwenden, um die eingegebene Passwort-Phrase zu verbergen. Zudem wird der verwendete Schlüssel asymmetrisch genutzt. Dies bedeutet, dass für die Verschlüsselung des Klartextes nicht immer der ganze Schlüssel zum Einsatz kommen muss, sondern auch nur Teile von diesem in unterschiedlichen Permutationen angewendet werden können. Ein Auslesen dieser Daten, ohne das dabei der Originalschlüssel bekannt ist, ist auch nach fast 17 Jahren immer noch nicht möglich.

Allerdings gibt es auch bei WPA2 Schwachstellen, die es zu berücksichtigen gilt. Zum einem kommt immer noch das schon im WEP verwendet TKIP-Verfahren zum Einsatz, was bei dieser WLAN Verschlüsselung wiederum ein Einfallstor für Cracker sein könnte. Allerdings soll dieser Umstand bald der Vergangenheit angehören, denn als neuer Standard ist langfristig CCMP (Counter-Mode/CBC-MAC Protocol) geplant.

Die hauptsächliche Schwachstelle von WPA2 ist aber darin zu sehen, dass die gesamte WLAN Verschlüsselung als eine nicht-lineare Gleichung verstanden werden kann, die sich im Grunde mit entsprechend hoch entwickelter Software auflösen lässt. Allerdings hat dieser Faktor für den alltäglichen Einsatz derzeit noch keine Bedeutung.

## TKIP und CCMP – Was steckt dahinter

Bei einer WLAN Verschlüsslung ist immer wieder von den Begriffen TKIP und CCMP die Rede. Für den normalen Verbraucher handelt es – sofern nicht erweiterte technische Kenntnisse im Hintergrund stehen – dabei um kryptische Zeichenfolgen. Doch tatsächlich ist das Ganze einfacher erklärt, als es im ersten Moment erscheinen mag.

### TKIP (Temporal Key Integrity Protocol)

TKIP wurde eigentlich geschaffen, um bei der Umstellung von WEP auf WPA behilflich zu sein. Durch diesen Sicherheitsstandard musste die Hardware nicht vollständig ausgetauscht werden – die Methode konnte einfach in die bestehenden Router per Software-Update implementiert werden.

Das Protokoll stellt quasi den RC4-Algorithmus für die Codierung des WLAN-Keys zur Verfügung und verfügt gleichzeitig über eine 64-bit Hashkomponente welcher die Prüfsumme bereitstellt. Dabei wird jedem Datenpaket ein eigener Key zugewiesen, der auch noch die MAC-Adresse des jeweiligen Clients enthält. Am einfachsten ausgedrückt stellt TKIP die mathematische Basis, für die Verschlüsselung der Informationen dar.

### CCMP (Counter-Mode/CBC-MAC Protocol)

CCMP ist der nächste Schritt bei den Verschlüsselungsprotokollen. Dieser Algorithmus basiert nur noch auf AES und liefert einen 128-Bit langen Schlüssel, welcher jeweils über 48-Bit lange Initialisierungsvektoren verfügt. Dabei kommt eine Mischung aus verschiedenen Verschlüsselungen zum Einsatz, sodass der Key kaum noch auszulesen ist.

## Welche WLAN Verschlüsselung ist die sicherste Wahl?

Doch welche WLAN Verschlüsselung ist nun die sicherste Wahl für den Endkunden? Natürlich kann hier nur zu WPA2 AES mit CCMP geraten werden. Diese Methode ist so gut wie undurchdringbar und es wird vermutlich genauso lang wie bei WPA dauern, bis diese WLAN Verschlüsselung die ersten Schwachstellen preisgibt.

Allerdings kann auch noch auf WPA2 mit AES und TKIP gesetzt werden. Diese WLAN Verschlüsselung ist ebenfalls noch ungeknackt, selbst wenn sich im Laufe der Zeit einige Makel offenbart haben. Wer gegenwärtig diesen Standard verwendet, kann sich also als sicher betrachten.

Einzig WEP sollte als WLAN Verschlüsselung absolut gemieden werden. In den aktuellsten Geräten aus dem jetzigen Jahrgang ist diese Technik auch nicht mehr verfügbar, sie kann aber aufgrund von Kompatibilitäsproblemen durchaus noch nachinstalliert werden.http://vg01.met.vgwort.de/na/d8b801bf8ba74f62a20c962fb85c5910

# Bluetooth

Bluetooth dient zur schnellen Datenübertragung. Bluetooth sendet im 2,5 GHz Bereich und arbeitet mit Frequenzy-Hopping. Dies bedeutet, dass nach jedem gesendeten Paket das Modul in eine andere Frequenz wechselt. Dies dient dazu um Störungen vorzubeugen.

Bluetooth arbeitet mit zwei Verbindungstypen:

* Synchronous Connection Oriented (SCO), wird für Voice-Verkehr eingesetzt
* Asynchronous Connectionless (ACL), für Datenverkehr im symetrischen und asymetrischen Verkehr verwendet

Beide Verbindungstypen verwenden ein Zeitmultiplexverfahren für Duplex-Datenübertragung.

So ist es möglich mehrere Kanäle für eine Verbindung zu verwenden, indem jedem ein unterschiedlicher Zeitintervall (Slot) zugeteilt wird.

/ Bei synchronen Datenpackten können mehrere Slots reserviert werden, wobei ein Datenpacket bis  
/ zu fünf Slots beanspruchen kann

Bluetooth ist in der Lage ein Point-to-Point oder ein Point-to-Mulitpoint Netzwerk aufzubauen.

Die Geräte sind dabei in der selben Hopping-Frequenz synchronisiert, haben eine identische Implementation

# NFC