



Laboratoire Wi-Fi

Sécurité sans fil, vulnérabilités majeures et expérimentations

Projet de Mastère Spécialisé Cybersécurité
Télécom SudParis

Auteurs : Tanguy HUE
Clément LEPRETTRE

Encadrant : Olivier PAUL

6 janvier 2026

Résumé

Ce rapport présente un état de l'art complet de la sécurité des réseaux Wi-Fi contemporains, une analyse détaillée des vulnérabilités majeures encore exploitables ainsi qu'une mise en pratique expérimentale basée sur un environnement virtualisé.

Mots-clés : Wi-Fi, WPA / WPA2, WPA3, cybersécurité, attaques réseau

Table des matières

1	Introduction	5
2	Objectifs du projet	6
2.1	Objectif général	6
2.2	Objectifs spécifiques	6
3	Fonctionnement des Protocoles Wi-Fi	7
3.1	Principe général du Wi-Fi	7
3.2	Sécurité Wi-Fi	10
3.2.1	WEP : Wired Equivalent Privacy	10
3.2.2	WPA : Wi-Fi Protected Access	12
3.2.3	WPA2 : AES-CCMP et le 4-Way Handshake	14
3.2.4	Dérivation des clés	14
3.2.5	WPA3 : SAE, Dragonfly, GCMP et PMF	15
3.3	Mécanismes cryptographiques avancés	16
3.3.1	AES-CCMP	16
3.3.2	GCMP (AES-GCM)	17
3.3.3	SAE / Dragonfly	17
3.4	Synthèse comparative approfondie	18
4	État de l'art sur la sécurité Wi-Fi	19
4.1	Évolution historique des attaques contre les réseaux Wi-Fi	19
5	Méthodologie	20
5.1	Environnement expérimental	20
6	Attaques Wi-Fi étudiées et reproduites	21
7	Conclusion	22
Références		23
A	Captures Wireshark	24
B	Scripts utilisés	24

Table des figures

1	Illustration des notions AP, STA, SSID et BSSID dans un réseau Wi-Fi	7
2	Mode Infrastructure : STA → AP central → Internet	8
3	Mode Ad hoc : communication directe sans AP	9
4	Mode Pont : extension réseau filaire via APs	9
5	Mode Répéteur : extension portée (débit /2, +latence)	9
6	Principe du chiffrement WEP	10
7	Format d'une trame WEP	10
8	Phase 3 WPA/TKIP : utilisation de la PTK (TK et MIC Key) pour le chiffrement par trame	13
9	4-Way Handshake WPA/WPA2	14
10	Dérivation cryptographique PMK → PTK → GTK	15
11	Structure d'une trame CCMP	15
12	Handshake SAE (WPA3)	16
13	Structure d'une trame GCMP (WPA3)	17

Liste des acronymes

AP Access Point. 3, 6–10, 13, 14

BSSID Basic Service set identifier. 3, 7

FAI Fournisseurs d'accès à Internet. 8

GTK Group Temporal Key. 8

ICV Integrity Check Value. 10, 11

IV Initialization Vector. 10

MIC Message Integrity Code. 12

PBKDF2 Password-Based Key Derivation Function 2. 12

PMK Pairwise Master Key. 8, 12

PSK Pre-Shared Key. 13

PTK Pairwise Transient Key. 8, 12

RC4 Rivest Cipher 4. 10

SSID Service set identifier. 3, 7, 8

STA Station. 3, 7, 8, 13, 14

TKIP Temporal Key Integrity Protocol. 12

TSC TKIP Sequence Counter. 12

WEP Wired Equivalent Privacy. 5, 7, 10

Wi-Fi Wireless Fidelity. 5, 6

WPA Wi-Fi Protected Access. 5, 12

WPA2 Wi-Fi Protected Access 2. 5

WPA3 Wi-Fi Protected Access 3. 5, 7

Glossaire

ANonce Authenticator Nonce : nombre aléatoire de 32 octets généré par le point d'accès lors du 4-Way Handshake pour créer la PTK. 12–14

concentrateur Équipement réseau de niveau 2, utilisé pour faire de la redirection de trame. 8

handshake Échange de messages pour authentifier et établir les clés de chiffrement. 8, 12

SNonce Supplicant Nonce : nombre aléatoire de 32 octets généré par la station lors du 4-Way Handshake pour créer la PTK. 12–14

trame Unité de données de la couche 2 transportant informations de gestion, contrôle ou données utilisateur. 7, 10

1 Introduction

Les réseaux Wireless Fidelity (Wi-Fi) sont devenus un élément incontournable des infrastructures numériques modernes. Que ce soit dans les environnements personnels, professionnels ou industriels, ils assurent une connectivité flexible, mais exposent également les systèmes à des risques spécifiques liés à la nature même des communications sans fil. Contrairement aux réseaux filaires, un réseau Wi-Fi dépasse toujours les limites physiques du bâtiment ou de l'organisation qui l'utilise, ce qui permet à un attaquant de s'y connecter ou de l'observer sans jamais avoir à pénétrer physiquement dans les locaux. Cette caractéristique en fait une cible privilégiée et un vecteur d'attaque largement exploité.

Les mécanismes de sécurité Wi-Fi ont pourtant beaucoup évolué au fil des années. Après les faiblesses majeures de WEP et les limites de WPA, WPA2 a longtemps été considéré comme un standard robuste, jusqu'à l'apparition d'attaques protocolaires comme KRACK. Plus récemment, WPA3 a introduit de nouveaux mécanismes destinés à renforcer l'authentification et la confidentialité, mais même cette version moderne a connu ses premières vulnérabilités dès sa diffusion. Cette succession d'avancées et de contournements montre que la sécurité Wi-Fi est un domaine en évolution constante, dans lequel chaque amélioration technique entraîne l'apparition de nouvelles attaques ciblées.

Malgré les améliorations successives des protocoles et l'apparition de WPA3, les réseaux Wi-Fi restent vulnérables. Beaucoup d'équipements utilisent encore des standards anciens ou sont configurés avec des options de rétrocompatibilité qui affaiblissent la sécurité. Les implémentations varient d'un constructeur à l'autre, certaines protections dépendent du comportement du client, et les attaques théoriques se révèlent parfois très simples à reproduire en pratique. La problématique centrale de ce travail est donc de comprendre quelles attaques restent réellement efficaces aujourd'hui, comment elles peuvent être mises en œuvre dans un environnement réaliste, et quelles implications elles ont sur la sécurité globale d'un réseau Wi-Fi.

Dans ce contexte, ce projet s'intéresse à la compréhension des principales failles affectant les réseaux Wi-Fi actuels et à l'analyse des attaques réellement exploitables sur le terrain. Il s'agit d'étudier comment un attaquant peut contourner les protections en place, quelles conditions pratiques rendent ces attaques possibles, et quelles sont leurs conséquences concrètes sur la confidentialité, l'intégrité et la disponibilité des communications. L'objectif n'est pas uniquement théorique : il s'agit de reproduire ces attaques dans un environnement maîtrisé afin d'observer leur fonctionnement, d'en comprendre les mécanismes internes et d'évaluer leur pertinence vis-à-vis des architectures modernes.

2 Objectifs du projet

2.1 Objectif général

Étudier, analyser et reproduire des attaques Wi-Fi représentatives de la menace actuelle.

2.2 Objectifs spécifiques

- Mettre en place un laboratoire Wi-Fi complet (Kali + AP + VM Windows).
- Reproduire des attaques Wi-Fi.
- Capturer, analyser et expliquer les traces réseau.
- Évaluer les conséquences et proposer des contre-mesures.

3 Fonctionnement des Protocoles Wi-Fi

La sécurité des réseaux Wi-Fi repose sur une succession de mécanismes cryptographiques introduits progressivement pour corriger les vulnérabilités de leurs prédecesseurs. Depuis WEP en 1997 jusqu'à WPA3 en 2018, chaque protocole a apporté des évolutions majeures : nouveaux algorithmes, nouvelles principes cryptographiques, mécanismes d'intégrité plus robustes, protection des trames de gestion, et résistance aux attaques hors ligne. Cette section propose une analyse approfondie de ces mécanismes, de leur logique interne, de leurs limites, ainsi que des structures de trames qu'ils manipulent.

3.1 Principe général du Wi-Fi

Le Wi-Fi, ou norme IEEE 802.11, désigne un ensemble de standards pour les réseaux locaux sans fil (WLAN) permettant la transmission de données numériques par ondes radio (principalement 2,4 GHz, 5 GHz et 6 GHz). Développé à partir des années 1990 par le comité IEEE 802.11 pour répondre à la demande croissante de connectivité mobile sans câblage Ethernet, le premier standard a été publié en 1997, révolutionnant l'accès aux données en éliminant les contraintes physiques des réseaux filaires.

Aujourd'hui, le Wi-Fi est omniprésent : hotspots publics (cafés, aéroports, transports), entreprises, foyers. Avec Wi-Fi 7 (802.11be, 2024) et au-delà, il supporte des débits >46 Gbit/s.

Définitions générales Wi-Fi

Avant d'aborder en détail le fonctionnement des différents protocoles de sécurité, il est utile de préciser brièvement certains termes fondamentaux du Wi-Fi. Le **Service set identifier (SSID)** correspond au nom d'un réseau et permet aux dispositifs de l'identifier lors de la phase de découverte. Le **Basic Service set identifier (BSSID)**, quant à lui, désigne l'adresse MAC unique du point d'accès assurant la diffusion du réseau. Le terme **Access Point (AP)** désigne ce même point d'accès, tandis que la **Station (STA)** représente tout client Wi-Fi, qu'il s'agisse d'un ordinateur, d'un smartphone ou d'un objet connecté.

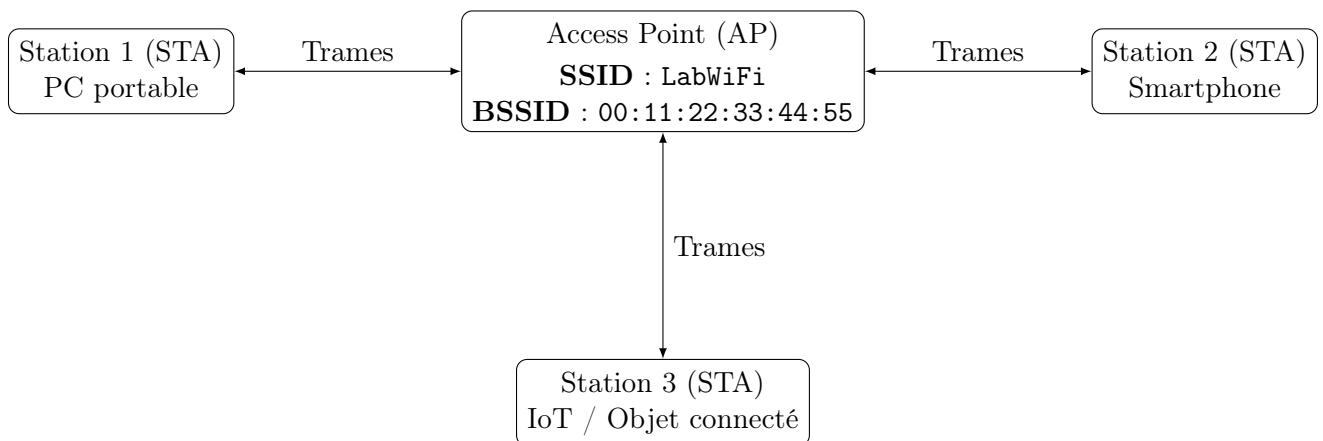


FIGURE 1 – Illustration des notions AP, STA, SSID et BSSID dans un réseau Wi-Fi

Les communications Wi-Fi reposent sur des trames qui circulent au niveau de la couche MAC du modèle 802.11. On distingue notamment les trames de *gestion*, essentielles pour l'association, l'authentification ou la déconnexion ; les trames de *contrôle*, destinées à réguler l'accès au médium ;

et les trames de *données*, qui transportent l'information utilisateur ou les paquets réseau encapsulés. La plupart des attaques Wi-Fi tirent parti de la possibilité d'observer, d'injecter ou de manipuler ces différentes catégories de trames.

Enfin, plusieurs notions cryptographiques apparaissent régulièrement dans ce chapitre. La **Pairwise Master Key (PMK)** constitue le secret partagé à partir duquel toutes les clés de session sont dérivées, tandis que la **Pairwise Transient Key (PTK)** correspond à la clé spécifique à la connexion entre un client et un point d'accès. La **Group Temporal Key (GTK)** est utilisée pour chiffrer le trafic multicast ou broadcast adressé à plusieurs stations. Ces clés sont produites ou échangées dans le cadre de mécanismes tel que le 4-Way Handshake, qui sera détaillé dans les sections suivantes.

Ces notions constituent le socle indispensable à la compréhension des protocoles de sécurisation Wi-Fi et des vulnérabilités qu'ils cherchent à prévenir.

Modes de mise en réseau [1]

Le Wi-Fi supporte plusieurs modes de mise en réseau, adaptés à des usages variés.

Mode Infrastructure Ce mode connecte les stations (STA) via un ou plusieurs points d'accès (AP) qui agissent comme des concentrateurs. Initialement utilisé en entreprise pour poser des bornes à intervalles réguliers, il nécessite un SSID commun pour la communication. L'avantage principal est le contrôle centralisé des accès : passage obligatoire par l'AP. Aujourd'hui, les routeurs fournis par les FAI aux particuliers fonctionnent en mode infrastructure, faciles à configurer.

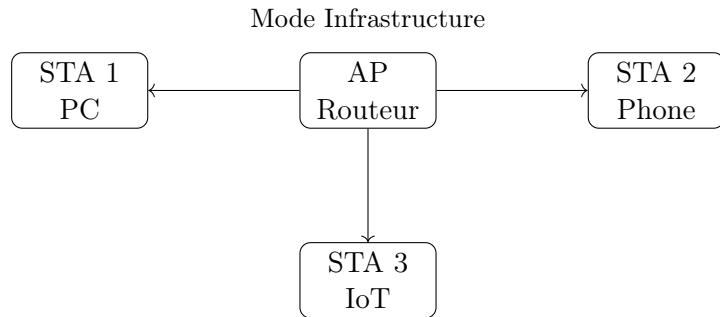


FIGURE 2 – Mode Infrastructure : STA → AP central → Internet

Mode Ad hoc Ce mode permet une connexion directe entre stations sans point d'accès intermédiaire. Idéal pour des échanges rapides (fichiers entre portables dans un train ou un café), il repose sur un SSID, un canal et une clé de chiffrement communs. Des protocoles de routage dynamique étendent la portée en mode maillé, où chaque noeud route pour les autres.

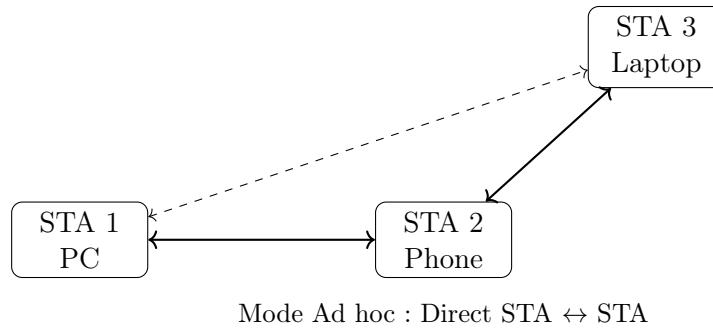


FIGURE 3 – Mode Ad hoc : communication directe sans AP

Mode Pont (Bridge) Un AP en mode pont relie d’autres AP pour étendre un réseau filaire (ex. : entre bâtiments) au niveau couche 2 OSI. Un AP racine distribue l’accès Internet, les autres se connectent en mode bridge et peuvent accueillir des clients comme en infrastructure.

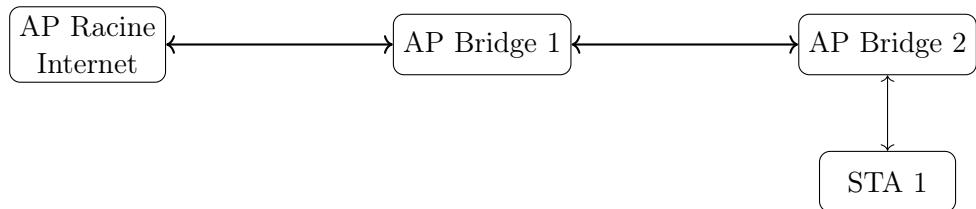


FIGURE 4 – Mode Pont : extension réseau filaire via APs

Mode Répéteur (Range-extender) Ce mode étend la couverture en répétant le signal (ex. : fond de couloir). L’interface Ethernet reste inactive, mais chaque saut augmente la latence et divise le débit par deux (réception + retransmission sur la même antenne).



FIGURE 5 – Mode Répéteur : extension portée (débit /2, +latence)

Mode	Lien principal	Ethernet	Usage
Infrastructure	STA → AP	✓	Internet
Ad hoc	STA ↔ STA	✗	Échange direct
Pont	AP ↔ AP (câble)	✓	Relier bâtiments
Répéteur	WiFi répété	✗	Étendre portée

TABLE 1 – Modes Wi-Fi : synthèse

Ces modes fondamentaux conditionnent les mécanismes de sécurité analysés dans la suite, particulièrement en mode infrastructure dominant.

3.2 Sécurité Wi-Fi

3.2.1 WEP : Wired Equivalent Privacy

WEP (1997) constitue la première tentative de sécuriser les communications Wi-Fi. Il a été conçu à une époque où la cryptographie grand public était encore émergente, et souffre aujourd’hui de nombreuses limitations. Son objectif était de fournir une confidentialité comparable à celle d’un réseau filaire, mais son fonctionnement s’est révélée profondément vulnérable.

Fonctionnement interne

WEP repose sur l’algorithme de chiffrement par flot RC4. Le mécanisme de chiffrement est simple :

- une clé secrète partagée statique, nommée SharedKey (40 ou 104 bits) ;
- un Initialization Vector (IV) de 24 bits, envoyé en clair ;
- concaténation $IV \parallel \text{clé}$ comme entrée de RC4 ;
- un Integrity Check Value (ICV) calculé via CRC-32, ajouté au plaintext (*texte en clair*) avant chiffrement.

Le chiffrement d’un paquet se fait ainsi :

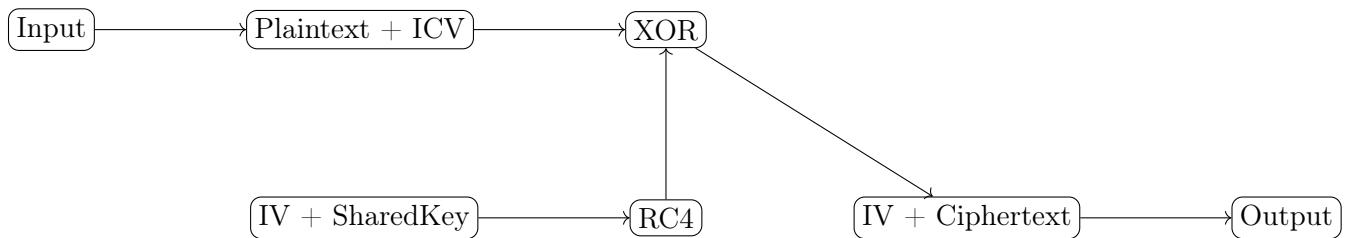


FIGURE 6 – Principe du chiffrement WEP

Format d’une trame WEP

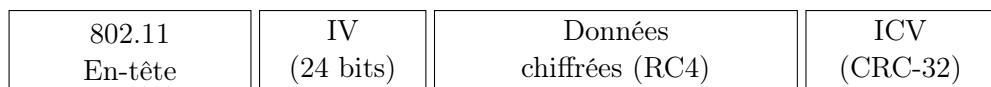


FIGURE 7 – Format d’une trame WEP

Faiblesses cryptographiques majeures Le protocole WEP présente des faiblesses structurelles fondamentales :

- **IV de 24 bits (16 777 216 valeurs possibles)** : chaque trame WEP transmet son vecteur d’initialisation en clair. Avec un trafic normal, les collisions d’IV surviennent en quelques minutes (souvent moins de 5 minutes pour un AP actif). Un attaquant peut alors combiner deux trames avec le même IV+clé pour annuler le keystream par XOR.
- **Aucun renouvellement de clé** : la clé secrète reste statique pendant des semaines/mois. Un IV réutilisé expose la même clé RC4 pendant toute la durée de vie de la clé, permettant une attaque par collecte massive de trames.
- **ICV trop faible** : L’ICV s’appuie sur un algorithme peu robuste, il est possible de modifier des trames chiffrées sans connaître la clé, en recalculant un ICV valide.

Pour mieux comprendre le problème majeur de la taille de l'IV, nous allons prendre comme exemple : un IV est utilisé 2 fois IV_0 , et deux messages combinés (données | ICV) M_1 et M_2 .

1. $IV_0 \rightarrow RC4(IV_0 || SharedKey) \oplus M_1 = C_1$
2. $IV_0 \rightarrow RC4(IV_0 || SharedKey) \oplus M_2 = C_2$
3. $C_1 \oplus C_2 = M_1 \oplus M_2$
4. En-têtes IP (IP/TCP standardisé) connus de $M_1 \rightarrow M_2$ instantané

En pratique, avec Aircrack NG, William Arbaugh note qu'il existe 50 % de risque de collision après 4 823 paquets. [2] La documentation conseille elle 250,000 IVs pour des clés de 64 bit et 1,500,000 IVs pour des clés de 128 bit. [3]

3.2.2 WPA : Wi-Fi Protected Access

Face à la crise WEP, la Wi-Fi Alliance introduit en 2003 WPA comme correctif transitoire, visant à remplacer les composants vulnérables tout en conservant le matériel existant (compatibilité ascendante).

Fonctionnement interne

WPA introduit plusieurs mécanismes :

- un mélange de clés élaboré (phase 1 et phase 2) ;
- un TKIP Sequence Counter (TSC) pour de l'anti-replay ;
- un Message Integrity Code (MIC) pour de l'intégrité ;
- une rotation des clés fréquente.

Phases de WPA

Le protocole de WPA est divisé en 3 phases.

- **Phase 1 (PBKDF2 4096 itérations)** : passphrase → PMK résistante dictionnaire (impossible bruteforce hors ligne contrairement à WEP).
- **Phase 2 (4-Way Handshake)** : PMK → PTK échangée sans jamais transmettre la clé (ANonce/SNonce + MIC protègent). Clés éphémères.
- **Phase 3 (TKIP par trame)** :
 - TSC 48 bits (vs IV 24b WEP)
 - MIC (Michael) → intégrité (vs CRC-32 faible)
 - RC4 + TSC → keystream unique par trame

Fonctionnement interne (3 phases)

WPA corrige WEP par 3 étapes distinctes :

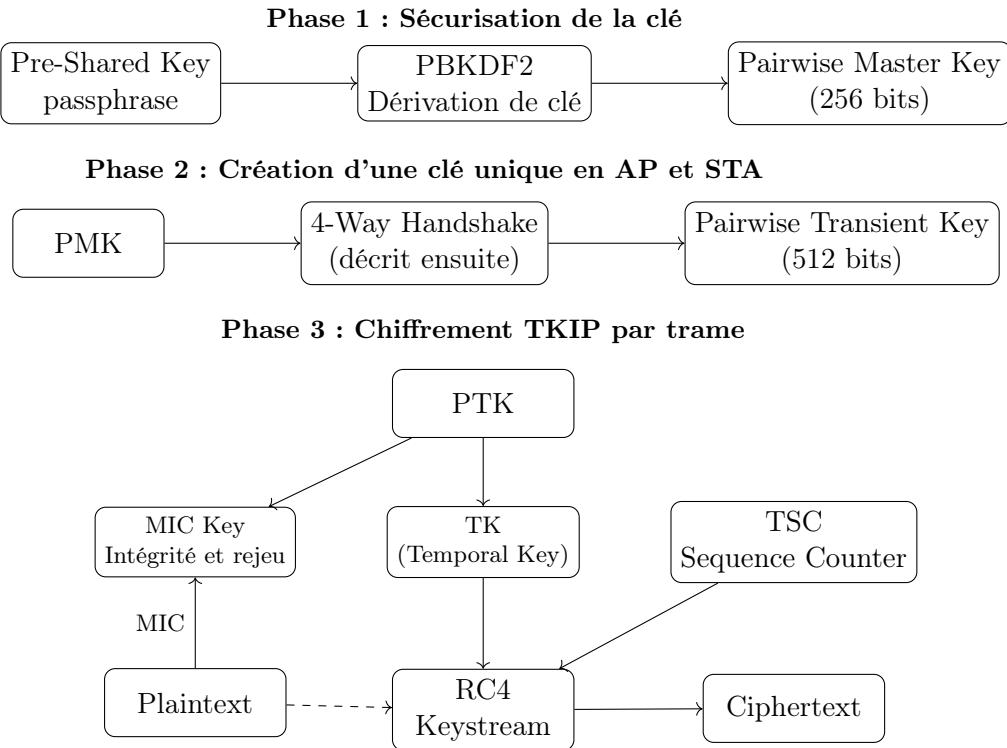


FIGURE 8 – Phase 3 WPA/TKIP : utilisation de la PTK (TK et MIC Key) pour le chiffrement par trame

Bien que RC4 soit toujours utilisé, WPA réduit significativement les risques d'attaque sans néanmoins les éliminer.

Le 4-Way Handshake

Le **4-Way Handshake** assure 3 objectifs critiques :

- **Preuve mutuelle PMK** : STA et AP prouvent qu'ils connaissent la même PMK sans jamais la transmettre.
- **PTK (Pairwise Transient Key, 512 bits)** : clé unique unicast STA ↔ AP, dérivée de : $PTK = PRF(PMK, SSID, \min(ANonce, SNonce) || \max(ANonce, SNonce))$.
- **GTK (Group Temporal Key)** : clé broadcast/multicast partagée par TOUS les clients du réseau (trafic groupe). L'AP l'envoie chiffrée avec la PTK du client.

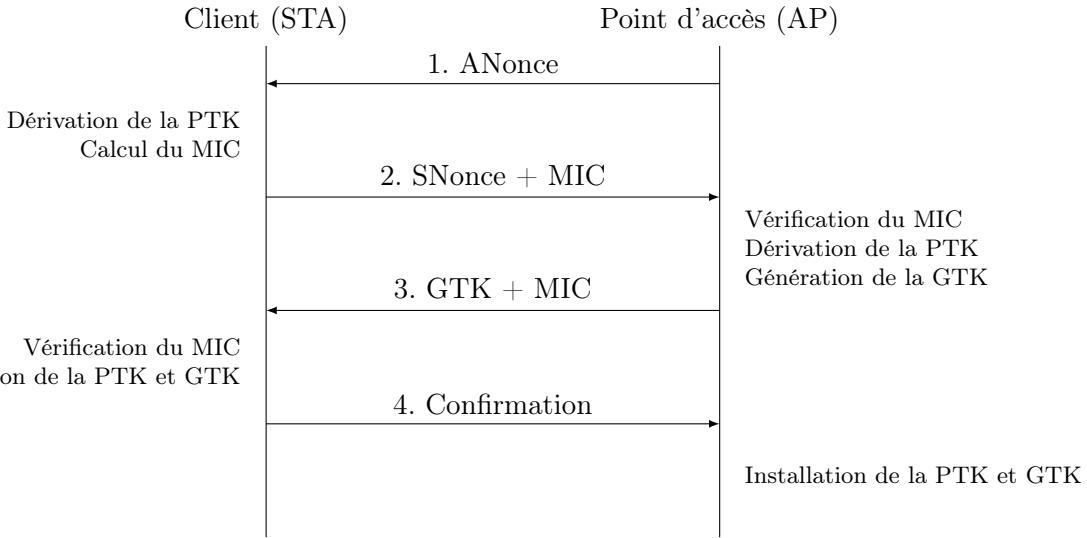


FIGURE 9 – 4-Way Handshake WPA/WPA2

3.2.3 WPA2 : AES-CCMP et le 4-Way Handshake

WPA2 apporte une amélioration profonde : l'abandon de RC4 au profit d'un chiffrement moderne AES-CCMP.

Modes d'authentification

- **WPA2-PSK** : la PMK (*Pairwise Master Key* : clé maîtresse) = PBKDF2(*Password-Based Key Derivation Function 2* : basée sur une passphrase et le SSID).
- **WPA2-Enterprise** : PMK fournie via un serveur RADIUS et une authentification EAP.

3.2.4 Dévolution des clés

Au-delà de l'échange de messages représenté dans la Figure 9, le 4-Way Handshake repose sur un mécanisme de dévolution de clés particulièrement structuré. L'ensemble du processus débute avec la PMK (Pairwise Master Key), qui constitue la base cryptographique partagée entre le client et le point d'accès. Dans le cas d'un réseau WPA2-PSK, cette PMK résulte directement de l'application d'une fonction de dévolution (PBKDF2) sur la passphrase et le SSID ; dans un environnement Enterprise, elle est fournie après l'authentification EAP par un serveur RADIUS. L'objectif du handshake n'est donc pas de négocier une nouvelle clé, mais de prouver que les deux entités possèdent bien cette PMK sans jamais la transmettre.

À partir de cette PMK, les deux parties vont dériver une clé plus large appelée PTK (Pairwise Transient Key). La construction de la PTK repose sur plusieurs éléments : l'adresse MAC du point d'accès, celle du client, ainsi que deux valeurs aléatoires appelées ANonce (envoyée par l'AP) et SNonce (envoyée par la station). Ces quatre paramètres garantissent que la PTK générée est unique pour chaque session, même si la PMK reste identique : une propriété essentielle pour éviter la réutilisation de clés et limiter les risques d'attaque par rejeu ou par corrélation.

La PTK n'est pas utilisée directement ; elle est découpée en trois sous-clés distinctes, chacune remplissant un rôle spécifique dans la sécurisation du lien. La première est la KCK (Key Confirmation Key), employée pour calculer les MIC (Message Integrity Code) des messages du handshake. Elle permet à chaque partie de vérifier que l'autre possède bien la PTK correcte, et donc implicitement

la PMK. La deuxième sous-clé est la KEK (Key Encryption Key), utilisée par l'AP pour chiffrer la GTK (Group Temporal Key) transmise dans le message 3. Cette clé assure que seul un client légitime peut recevoir ou mettre à jour la clé de diffusion. Enfin, la dernière composante est la TK (Temporal Key), qui servira au chiffrement effectif du trafic unicast échangé entre la station et l'AP après la fin du handshake.

Un autre élément important est la présence de la GTK, envoyée par le point d'accès lors du message 3 du 4-Way Handshake. Contrairement à la PTK, qui est propre à une paire client-AP, la GTK est partagée entre tous les clients d'un même réseau et sert au chiffrement des trames multicast et broadcast. Sa transmission protégée par la KEK garantit qu'un attaquant passif ne peut pas l'intercepter, tandis que son renouvellement régulier limite les risques de compromission en cas d'écoute prolongée.

Ainsi, le 4-Way Handshake ne se réduit pas à un simple échange de valeurs nonces, mais constitue un véritable protocole d'initialisation cryptographique. Il assure simultanément la preuve de possession du secret initial, la dérivation de clés fraîches, l'établissement d'un canal chiffré sécurisé et la synchronisation des compteurs de trames. L'ensemble du mécanisme repose sur des propriétés formelles destinées à garantir la confidentialité et l'intégrité des échanges, tout en minimisant les risques liés à la réutilisation ou à la dérivation incorrecte des clés.

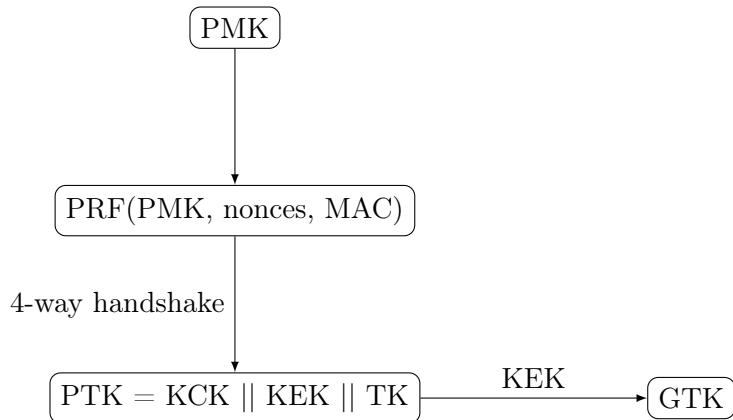


FIGURE 10 – Dérivation cryptographique PMK → PTK → GTK

Format d'une trame CCMP (WPA2)



FIGURE 11 – Structure d'une trame CCMP

3.2.5 WPA3 : SAE, Dragonfly, GCMP et PMF

WPA3 corrige des failles structurelles de WPA2, notamment KRACK, en introduisant SAE (Dragonfly), OWE, PMF obligatoire, et le support obligatoire de GCMP dans certaines suites.

Handshake SAE (Dragonfly)

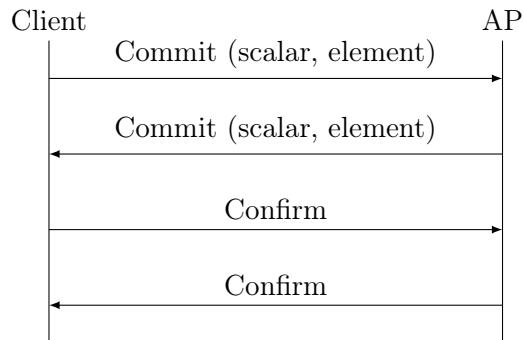


FIGURE 12 – Handshake SAE (WPA3)

3.3 Mécanismes cryptographiques avancés

Les protocoles de sécurité modernes du Wi-Fi reposent sur des mécanismes cryptographiques plus élaborés que ceux utilisés par les générations précédentes. Contrairement à WEP et TKIP, qui n’offraient qu’une protection minimale contre l’écoute, l’injection ou la manipulation des trames, WPA2 et surtout WPA3 reposent sur des constructions cryptographiques complètes, conçues pour fournir à la fois confidentialité, intégrité, résistance aux attaques par rejet et garanties formelles sur la sécurité de la session. Trois mécanismes occupent une place centrale : AES-CCMP, GCMP et SAE (aussi appelé Dragonfly). Ces primitives ne jouent pas le même rôle, mais constituent ensemble la base de la sécurité Wi-Fi contemporaine.

3.3.1 AES-CCMP

AES-CCMP est devenu la norme de chiffrement par défaut avec WPA2. Son objectif est d’aller bien au-delà du simple masquage des données transportées : il assure simultanément la confidentialité des informations, l’intégrité des trames et la protection contre les attaques par rejet.

Pour y parvenir, CCMP combine deux éléments complémentaires. D’une part, il utilise AES en mode compteur (CTR) pour le chiffrement. Ce mode transforme le bloc AES en générateur de flot chiffrant, permettant de chiffrer efficacement des paquets de taille variable sans introduire de structure exploitable. De l’autre, CCMP associe ce chiffrement à un code d’authentification basé sur CBC-MAC, un mécanisme cryptographique destiné à garantir que les données n’ont subi aucune altération. Cette combinaison forme une construction dite *AEAD* (Authenticated Encryption with Associated Data), dans laquelle confidentialité et intégrité sont assurées simultanément par une même clé, ce qui évite un grand nombre de vulnérabilités présentes dans les générations antérieures.

L’ensemble repose également sur un numéro de paquet (Packet Number, PN) utilisé comme nonce unique. Toute réutilisation est interdite, ce qui empêche un attaquant de rejouer ou de réinjecter des trames chiffrées. En pratique, AES-CCMP constitue encore aujourd’hui une référence en matière de chiffrement pour les réseaux Wi-Fi.

AES-CCMP combine :

- AES en mode CTR pour le chiffrement ;
- CBC-MAC pour l’intégrité (authentification).

C’est une construction AEAD robuste, largement testée.

3.3.2 GCMP (AES-GCM)

GCMP, introduit avec les standards 802.11ac et repris dans WPA3-Enterprise, reprend les principes d’AES-CCMP mais s’appuie cette fois sur AES-GCM. Cette construction fait partie des modes de chiffrement AEAD les plus étudiés et les plus robustes. AES-GCM associe un chiffrement en mode CTR à la fonction d’authentification GHASH, reposant sur des opérations arithmétiques dans un corps de Galois. Cette approche permet de calculer l’intégrité et le chiffrement de façon quasi parallèle, ce qui rend GCMP particulièrement performant sur les architectures modernes.

L’intérêt principal de GCMP réside donc dans sa rapidité : il offre un débit supérieur à CCMP, ce qui le rend bien adapté aux environnements à forte charge ou aux réseaux professionnels nécessitant des débits élevés. Il reste néanmoins sensible aux erreurs d’implémentation, comme l’ont montré certaines variantes des attaques Dragonblood qui ciblaient directement GCMP-128 lorsque les nonces n’étaient pas utilisés correctement. Malgré cela, GCMP demeure une brique cryptographique robuste lorsqu’il est correctement mis en œuvre.

3.3.3 SAE / Dragonfly

Contrairement à AES-CCMP et à GCMP, qui sont des mécanismes de chiffrement et d’intégrité utilisés *après* l’établissement de la connexion, SAE (Simultaneous Authentication of Equals) intervient au moment de l’authentification. SAE n’est pas un algorithme de chiffrement mais un protocole d’échange de clés sécurisé, faisant partie de la famille des PAKE (Password-Authenticated Key Exchange).

L’enjeu de SAE est de résoudre l’un des problèmes fondamentaux des versions antérieures : avec WPA2-PSK, un attaquant pouvait capturer un 4-Way Handshake puis tenter hors ligne de retrouver le mot de passe par dictionnaire. Dans SAE, ce type d’attaque est impossible. Le protocole s’appuie sur un échange Diffie–Hellman (sur groupes modp ou courbes elliptiques), dans lequel le mot de passe n’est jamais transmis ni dérivé sous forme exploitable. Chaque tentative d’authentification nécessite une interaction en temps réel avec le point d’accès, ce qui empêche les attaques hors ligne et limite naturellement la vitesse des tests possibles.

SAE offre également la propriété de *Forward Secrecy* : même si un mot de passe venait à être compromis ultérieurement, les sessions passées resteraient inexploitables, car la clé de session résulte d’un secret éphémère renouvelé à chaque connexion. Cette approche corrige l’une des failles conceptuelles les plus importantes de WPA2 et constitue la principale amélioration de WPA3-Personal.

Pour résumer, ses caractéristiques principales sont les suivantes :

- s’appuie sur Diffie–Hellman (modp ou ECC) ;
- offre Forward Secrecy ;
- empêche les attaques hors-ligne ;
- protège contre attaques dictionnaires massives.

Format d’une trame GCMP

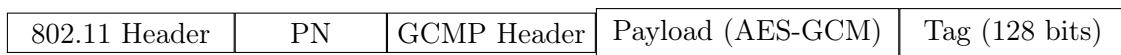


FIGURE 13 – Structure d’une trame GCMP (WPA3)

3.4 Synthèse comparative approfondie

Protocole	Crypto	Auth	Intégrité	Résistance
WEP	RC4	Clé statique	CRC-32	Nulle
WPA	RC4	PSK	MIC	Faible
WPA2	AES-CCMP	PSK/802.1X	CBC-MAC	Forte (hors KRACK)
WPA3	AES-CCMP/GCMP	SAE/802.1X	PMF	Très forte
OWE	Diffie-Hellman	Aucune	CCMP/GCMP	Élevée

TABLE 2 – Comparaison des protocoles de sécurité Wi-Fi

4 État de l'art sur la sécurité Wi-Fi

La surface d'attaque des réseaux Wi-Fi n'a cessé d'évoluer depuis 1997. Les vulnérabilités historiques et contemporaines exploitent indifféremment : les faiblesses cryptographiques intrinsèques, les défauts d'implémentation, les erreurs de configuration, et les mécanismes d'interaction entre utilisateurs et points d'accès. Cet état de l'art se concentre exclusivement sur les **attaques**, désormais que les protocoles ont été décrits dans la section précédente, et présente une analyse détaillée des vecteurs connus, de leur fonctionnement interne et de leur pertinence actuelle.

4.1 Évolution historique des attaques contre les réseaux Wi-Fi

L'évolution des attaques Wi-Fi suit logiquement celle des protocoles eux-mêmes. Chaque nouvelle protection a donné naissance à un nouveau type d'attaque : statistiques pour WEP, cryptanalytiques pour WPA, protocolaires pour WPA2 et side-channels pour WPA3.

5 Méthodologie

5.1 Environnement expérimental

- Hôte Windows + VirtualBox
- VM Kali Linux avec carte Wi-Fi compatible monitor/injection
- VM Lubuntu configurée en point d'accès Wi-Fi

6 Attaques Wi-Fi étudiées et reproduites

7 Conclusion

Références

- [1] C. aux projets Wikimedia, “Wi-fi — wikipédia,” 8 2003, [Online ; accessed 2026-01-06]. [Online]. Available : https://fr.wikipedia.org/wiki/Wi-Fi#Modes_de_mise_en_r%C3%A9seau
- [2] C. to Wikimedia projects, “Aircrack-ng - wikipedia,” 5 2006, [Online ; accessed 2026-01-06]. [Online]. Available : <https://en.wikipedia.org/wiki/Aircrack-ng#WEP>
- [3] A. N. darkAudax, “simple_wep_crack [aircrack-ng],” 3 2018, [Online ; accessed 2026-01-06]. [Online]. Available : https://www.aircrack-ng.org/doku.php?id=simple_wep_crack

Annexes

A Captures Wireshark

B Scripts utilisés