Wi-Fi™ REFERENCE SERIES

XIRRUS®

Wi-Fi ENCRYPTION DEMYSTIFIED

STANDARDS

Wireless LAN security standards are defined by the IEEE within the 802.11 family. The commercial implementations are specified and certified by the Wi-Fi Alliance.

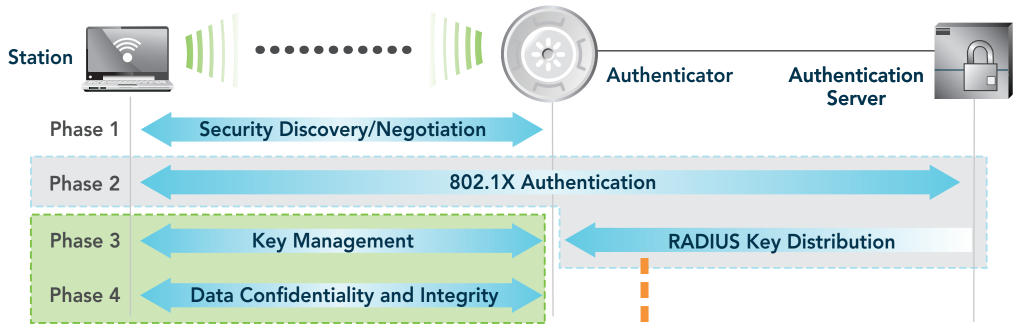
Wi-Fi Alliance				IEEE				
Certification	First Certified	Encryption Protocol	Authentication	Standard	Ratified	Clause	Encryption Protocol	Authentication
WPA2 Enterprise	2004	CCMP or TKIP	802.1X w/ EAP	802.11i	2004	8.3.3	CCMP	802.1X w/ EAP
WPA2 Personal	2004	CCMP or TKIP	Pre-shared Key					Pre-shared Key
WPA Enterprise	2003	TKIP or CCMP	802.1X w/ EAP			8.3.2	TKIP	802.1X w/ EAP
WPA Personal	2003	TKIP or CCMP	Pre-shared Key					Pre-shared Key
802.11a/b/g with WEP	2000	WEP	Shared Key	802.11	1997	8.2	WEP	Shared Key
			Open System					Open System

ENCRYPTION PROTOCOLS

Encryption Protocol	Encryption Algorithm	Key Management	Master Key	Initialization Vector	Encryption Key	Data Integrity Key	Data Integrity	Relative Security Strength (1-10 scale)
CCMP	AES	Yes	256 bits (PMK)	48 bits	128 bits (TK)	128 bits (TK)	CBC-MAC, including header	10
TKIP	RC4	Yes	256 bits (PMK)	48 bits	128 bits (TK)	64 bits (TMK)	Michael, including header	9
WEP	RC4	No	40 bits (WEP-40)	24 bits	64 bits	None	CRC32, no header	2
	RC4	No	104 bits (WEP-104)	24 bits	128 bits	None	CRC32, no header	2

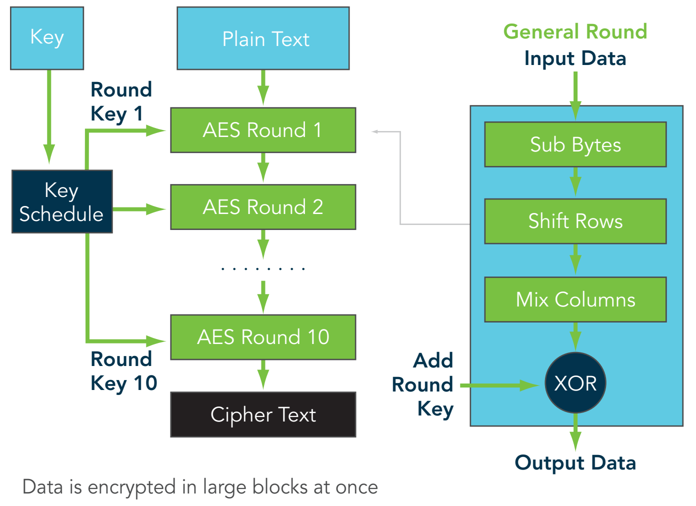
802.11i

802.11i is the official security standard for 802.11 wireless LANs as ratified by the IEEE in 2004. Its operation consists of 4 primary phases to establish secure communications. Phase 4 and a portion of Phase 3 are addressed in this poster; Phase 2 and portion of Phase 3 are addressed in the companion Wi-Fi Authentication poster.



AES ENCRYPTION

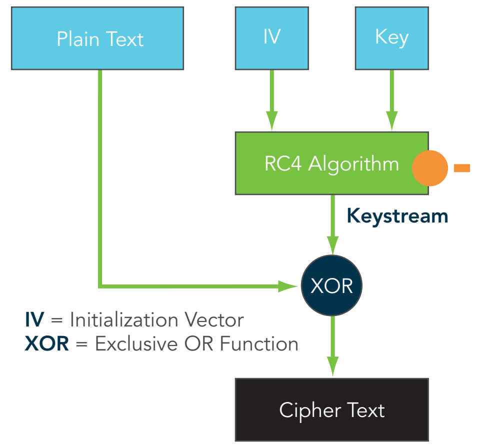
AES (Advanced Encryption Standard) is a block cipher encryption standard defined by Federal Information Processing Standards (FIPS) PUB 197. The encryption process is shown below—the decryption process is largely symmetric.



- Data is encrypted in large blocks at once
- A fixed, unvarying transformation is used for encryption
- Multiple rounds operate on 4×4 byte arrays of data. Each round consists of:
  – Sub Bytes — each byte is replaced with another per a lookup table
  – Shift Rows — each row is shifted cyclically a certain number of steps
  – Mix Columns — combines each column using a transformation
  – Add Round Key — each byte is XORed with a subkey

RC4 ENCRYPTION

RC4 (Rivest Cipher 4) is a stream cipher developed by RSA Security. The encryption process is shown below—the decryption process is largely symmetric.



IV = Initialization Vector
XOR = Exclusive OR Function

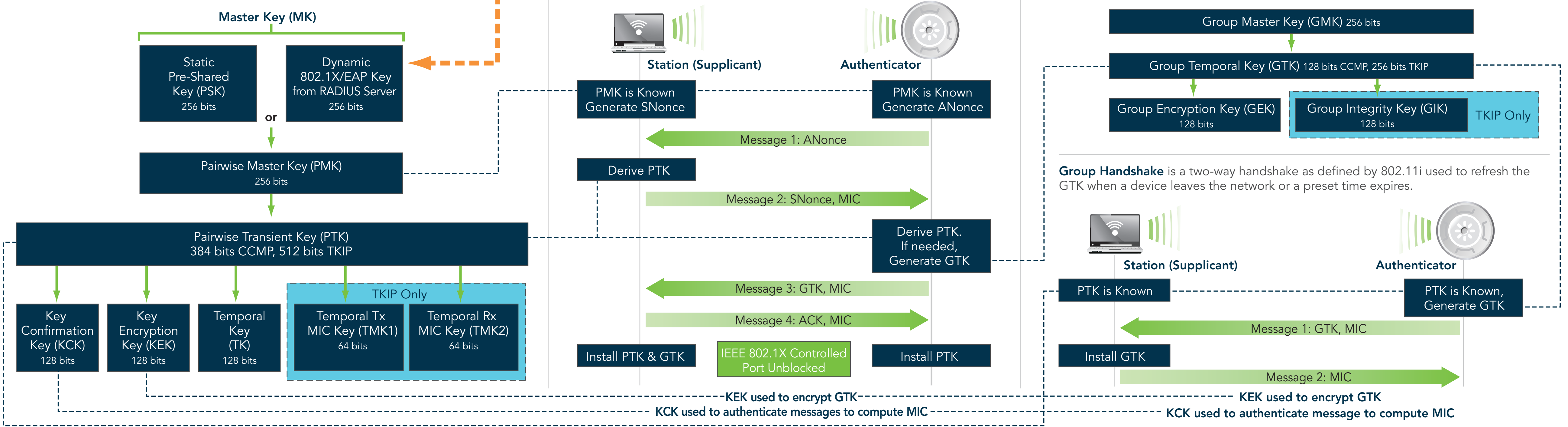
- Bytes are encrypted sequentially, one at a time
- Encryption keystream varies one byte to the next
- Key is used to create a 256-bit state table
- RC4 algorithm generates pseudo-random keystream
- Key stream XORed into data stream to encrypt the data

KEY MANAGEMENT

Pairwise Key Hierarchy describes the temporal keys derived from a master by the 4-Way Handshake protocol. These keys are used in unicast communications by CCMP and TKIP as defined by 802.11i. This key set is unique per station.

4-Way Handshake is used to generate, exchange, and refresh keys for encryption and integrity as defined by 802.11i.

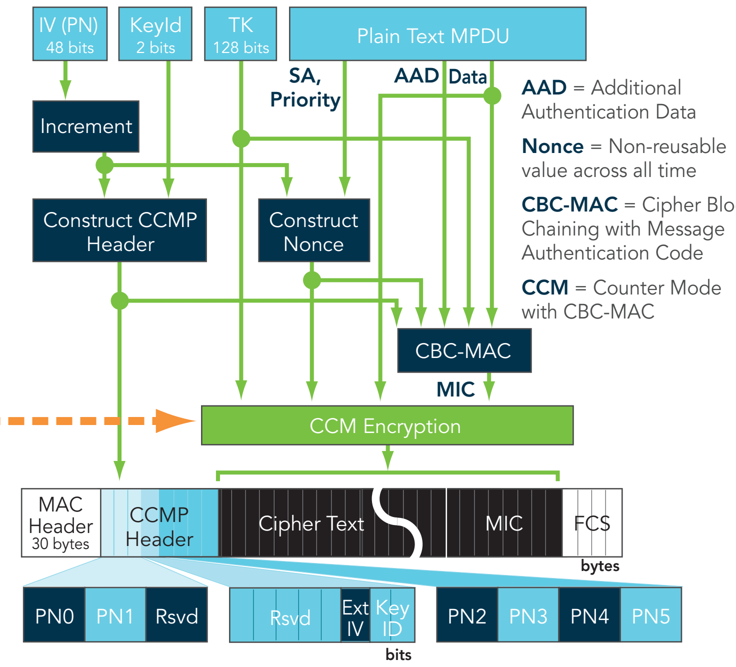
Group Key Hierarchy describes the temporal keys derived from a randomly generated master (GMK) for use in multicast communications with CCMP and TKIP as defined by 802.11i. This key set is unique per group of users in a multicast group per BSSID.


Master Key (MK)
Static Pre-Shared Key (PSK) 256 bits
or
Dynamic 802.1X/EAP Key from RADIUS Server 256 bits
Pairwise Master Key (PMK) 256 bits
Pairwise Transient Key (PTK) 384 bits CCMP, 512 bits TKIP
Key Confirmation Key (KCK) 128 bits
Key Encryption Key (KEK) 128 bits
Temporal Key (TK) 128 bits
TKIP Only
Temporal Tx MIC Key (TMK1) 64 bits
Temporal Rx MIC Key (TMK2) 64 bits
Station (Supplicant)
Authenticator
PMK is Known Generate SNonce
PMK is Known Generate ANonce
Message 1: ANonce
Derive PTK
Message 2: SNonce, MIC
Derive PTK. If needed, Generate GTK
Message 3: GTK, MIC
Message 4: ACK, MIC
Install PTK & GTK
IEEE 802.1X Controlled Port Unblocked
Install PTK
KEK used to encrypt GTK
KCK used to authenticate messages to compute MIC
Group Master Key (GMK) 256 bits
Group Temporal Key (GTK) 128 bits CCMP, 256 bits TKIP
Group Encryption Key (GEK) 128 bits
Group Integrity Key (GIK) 128 bits
TKIP Only
Station (Supplicant)
Authenticator
PTK is Known
PTK is Known, Generate GTK
Message 1: GTK, MIC
Install GTK
Message 2: MIC
KEK used to encrypt GTK
KCK used to authenticate message to compute MIC

Group Handshake is a two-way handshake as defined by 802.11i used to refresh the GTK when a device leaves the network or a preset time expires.

CCMP (WPA2)

CCMP (CTR with CBC-MAC) is the preferred standard encryption protocol defined by 802.11i and certified by the Wi-Fi Alliance as part of WPA2.



AAD = Additional Authentication Data

Nonce = Non-reusable value across all time

CBC-MAC = Cipher Block Chaining with Message Authentication Code

CCM = Counter Mode with CBC-MAC

PN = Packet Number, the Initialization Vector (IV) for CCMP. The PN is monotonically incremented per packet. PN5 is the most significant octet.

Rsvd = reserved bits, set to 0

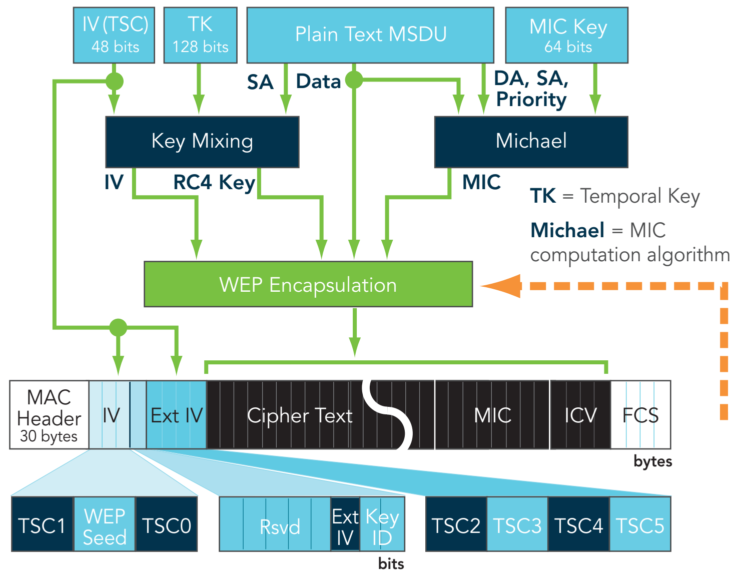
Ext IV (1 bit) = indicates 8 byte CCMP header, always set to 1

Key ID (2 bits) = index that identifies specific key value used

MIC = Message Integrity Code

TKIP (WPA)

TKIP (Temporal Key Integrity Protocol) is an encryption protocol defined by 802.11i and certified by the Wi-Fi Alliance as part of WPA. It was designed to allow existing hardware systems supporting WEP to be upgraded to improve security with larger keys, dynamic keys, and different encryption and integrity keys.



TK = Temporal Key

Michael = MIC computation algorithm

TSC = TKIP Sequence Counter, the Initialization Vector (IV) for TKIP. The TSC is monotonically incremented per packet. TSC5 is the most significant octet.

WEP Seed = (TSC1 | 0x20) & 0x7f

Rsvd (5 bits) = reserved bits, set to 0

Ext IV (1 bit) = 1 indicates 4 byte Extended IV follows, 0 not

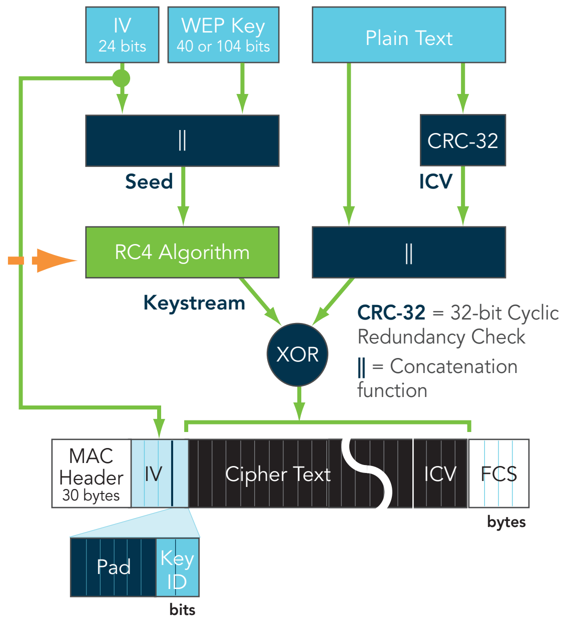
Key ID (2 bits) = index that identifies specific key value used

MIC = Message Integrity Code

ICV = Integrity Check Value

WEP

WEP (Wired Equivalent Privacy) is the wireless LAN security protocol defined by the IEEE with the original 802.11 standard in 1997. It has since been proven insecure and replaced with 802.11i (WPA2/WPA).



CRC-32 = 32-bit Cyclic Redundancy Check

|| = Concatenation function

IV = Initialization Vector, random generated

Pad = 6 bits, all zeros

Key ID = 2 bits, identifies 1 of 4 secret key values

ICV = Integrity Check Value

FCS = Frame Check Sequence

GLOSSARY

4-way handshake—a key management protocol defined by 802.11i and based on 802.1X. It operates between an AP (authenticator) and station (supplicant) to generate, exchange, and refresh encryption and data integrity keys.

802.1X—IEEE standard for authentication that uses the Extensible Authentication Protocol (EAP).

802.11i—IEEE standard ratified in 2004 that defines a security architecture for wireless LANs. It incorporates both authentication and encryption methods.

AES (Advanced Encryption Standard)—a block cipher encryption standard defined by Federal Information Processing Standards (FIPS) PUB 197.

CBC-MAC (Cipher Block Chaining with Message Authentication Code)—algorithm used by CCMP to calculate the MIC for data origin authenticity.

CCM (CTR with CBC-MAC)—encryption mechanism defined by RFC 3610 and used by 802.11i for data confidentiality using CTR and data integrity using CBC-MAC.

CCMP (CCM Protocol)—encryption protocol defined by IEEE 802.11i and certified by the Wi-Fi Alliance in WPA2.

CTR (Counter Mode)—the block cipher mode used in conjunction with AES in 802.11i to provide data confidentiality.

Group Handshake—a key management protocol defined by 802.11i and using the 802.1X protocol to refresh group (multicast) keys.

IV (Initialization Vector)—data combined with an encryption key to produce a unique keystream.

MIC (Message Integrity Code)—a value generated by cryptographic means and used to protect data from undetected alteration.

Michael—the algorithm used by TKIP to generate the MIC.

MPDU (MAC Protocol Data Unit)—single packet of data after fragmentation.

MSDU (MAC Service Data Unit)—single packet of data before fragmentation.

passphrase—a sequence of 8-63 characters shared between the AP and client to control access to a Wi-Fi network. It is used to derive the pre-shared key (PSK) in WPA/WPA2.

PSK (Pre-shared Key)—a static encryption key shared between and common to both the AP and client.

RC4 (Rivest Cipher 4)—a stream cipher developed by RSA Security.

Rijndael Algorithm—the encryption algorithm used by AES encryption.

RSN (Robust Security Network)—the architecture for secure wireless networks defined by 802.11i, including TKIP and CCMP but not WEP.

TKIP (Temporal Key Exchange Protocol)—an encryption protocol defined by IEEE 802.11i as an enhancement to WEP with larger keys, dynamic keys, and different encryption and integrity keys.

WEP (Wired Equivalency Protocol)—the original encryption protocol defined by IEEE 802.11 for wireless LANs.

WPA (Wireless Protected Access)—the Wi-Fi Alliance certification of 802.11i that uses TKIP encryption.

WPA2 (Wireless Protected Access 2)—the Wi-Fi Alliance certification of 802.11i that uses CCMP/AES encryption.

+805.262.1600 • 800.947.7871 • posters@xirrus.com • www.xirrus.com