Communication System Security

Professor Guang Gong

Department of Electrical and Computer Engineering
University of Waterloo
CANADA
<http://comsec.uwaterloo.ca/~ggong>

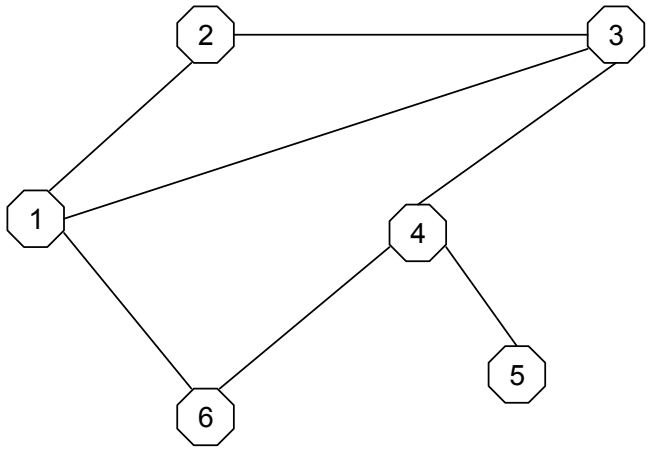
Communication System Security

1. **Topic 1**: Introduction
   - Security **Architecture**
   - Evolution of **Communication** Systems
   - **Historical** Developments of Secure Communications and Cryptographic Primitives
2. **Topic 2**. Basics of Protected Communication
   - Basic Information Security Concepts and **Protection** Mechanisms
   - **Trust** Model and Threat Model
   - Security Components
3. **Topic 3**: Case Study - Security in 4G-LTE Cellular System
   - Protection Wireless Link
   - **UMTS/4G-LTE** AKA and Air Link Protection
   - Some **forgery** Attacks on 4G-LTE Authentication Protection

Topic 1. Introduction

1. Secure Architecture

- A communication system can be described as a set of **nodes** connected with **links**.
- Information can be processed and stored inside a node and transmitted from one node to another through the links.

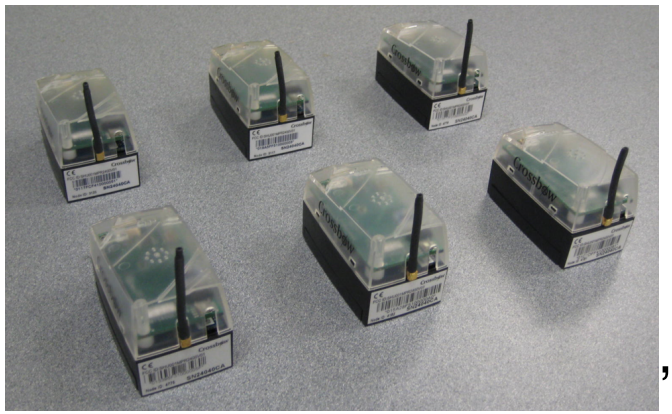


An abstract of a communication system

Security architecture defines **trust** relationships among the nodes and protection mechanisms for the information processed, stored, and transmitted.

Nodes, links and layers

Nodes: A node may consist of **hardware**, system software, and application software. It has capability of information storage, procession, and transmissions.

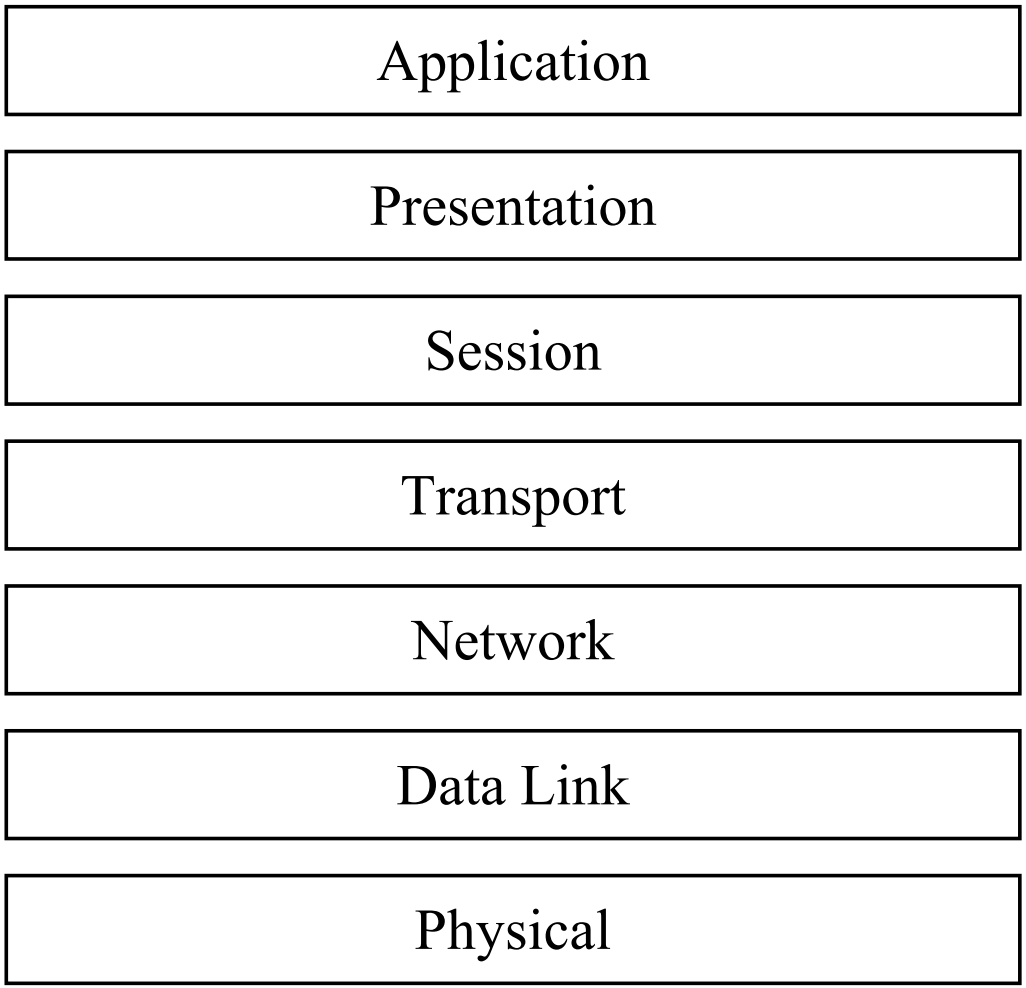


Links

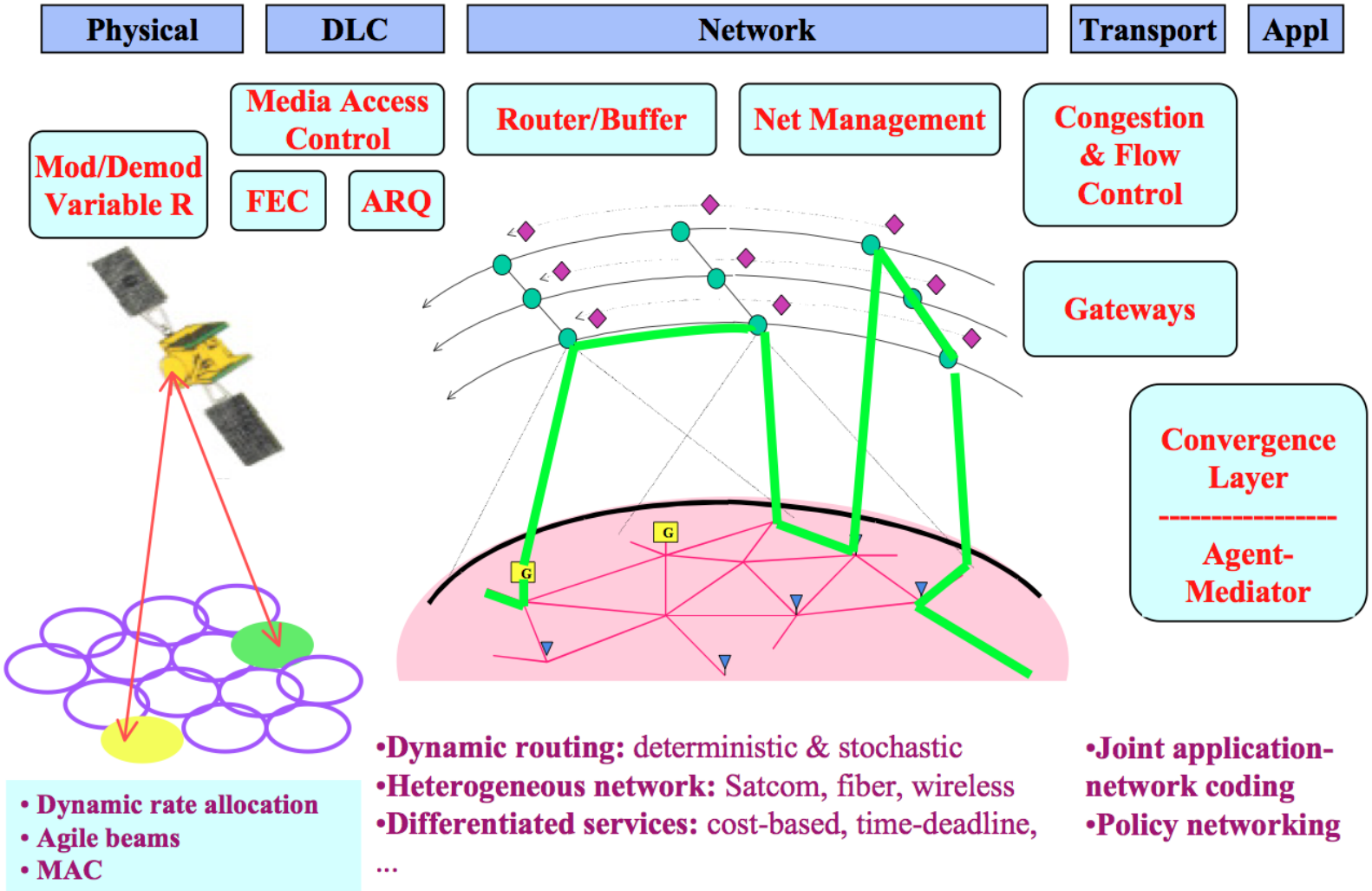
- A link connects two nodes where information is transmitted from one node to another.
- The transmission is conducted through a certain media, like radio, or physical materials, like copper wires to deliver the information from one node to another.
- In most of the cases, security protection has to be applied together with an actual communication protocol, for example, Internet Protocol (IP).

The information is often represented and processed through different protocols. The different protocols can be described through a layered architecture.

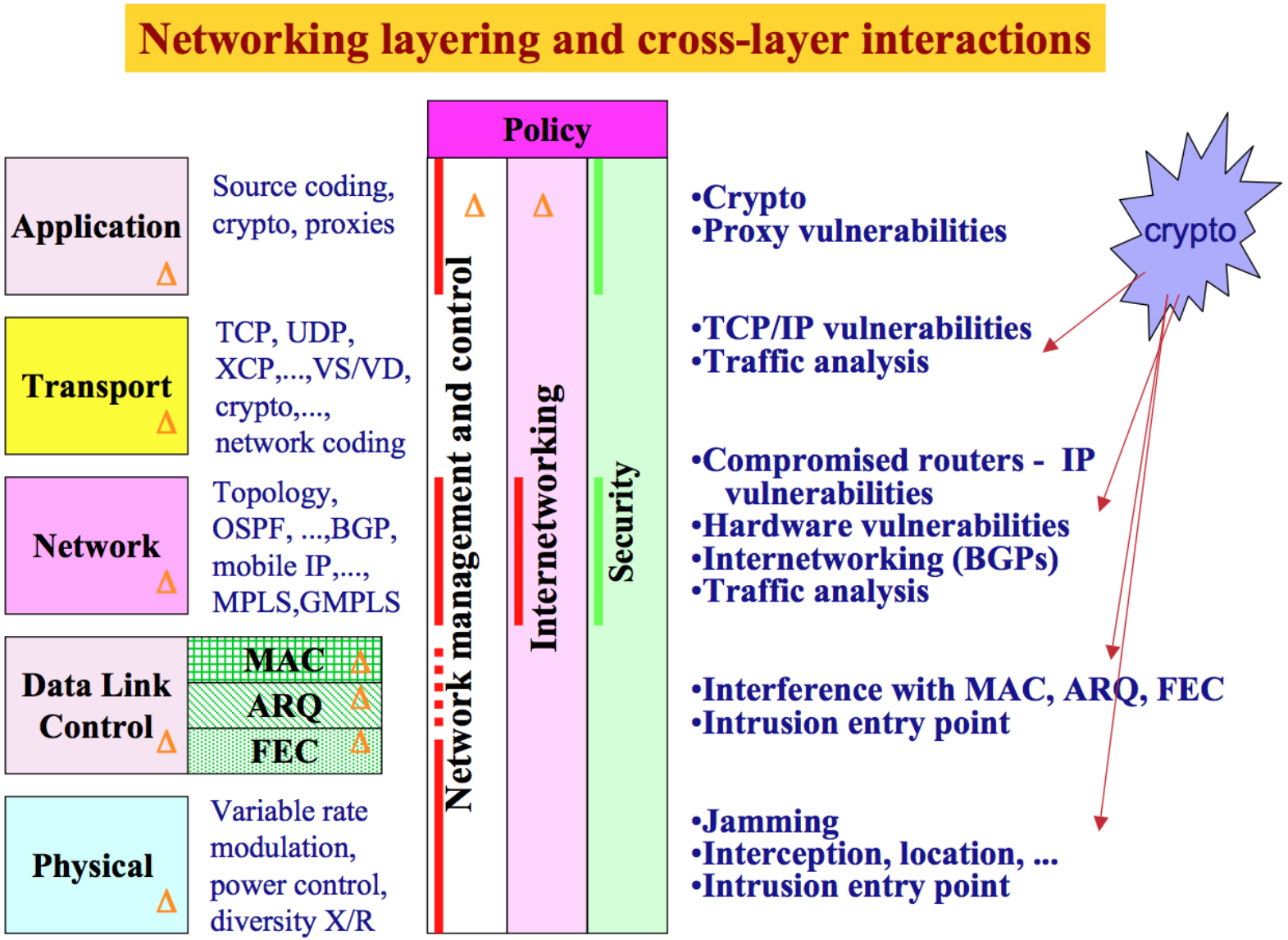
Layered Architecture in OSI Model



Dynamic Communication Network



Security Aspects in Network Layering



2. Evolution of Mobile Communication Systems

Generation	1G	2G	2.5G	3G	4/5G beyond
Time Frame	1980s	1990s	Late 1990s	2000s (2010 full deployment)	2010s
Signal Type	Analog	Digital	Digital	Digital	Digital
Multiple Access	FDMA/FDD, TDMA/FDD	CDMA/FDD	EDGE, GPRS	CDMA, W-CDMA, TD-SCDMA	MC-CDMA, OFDM
Frequency spectrum		824-894 MHz, 890-960 MHz, 1850-1990 MHz (PCS)		1800-2400 MHz (varies country to country)	Higher-frequency bands 2-8 GHz
Bandwidth				5-20 MHz	$\geq$ 100 MHz
Antenna				Optimized antenna, multi-band adapter	Smarter antenna, Multiband and wide-band support
FEC				Convolutional rate, 1/2, 1/3	Concatenated coding scheme
Media type	Voice	Mostly voice Low-speed data services via modem (10-70 kbps)	Mostly voice Higher-speed data (10-384 kbps)	Voice High-speed data (144kbps-2Mbps)	Converged voice data multimedia over IP; Ultra-high-speed data (2-100 Mbps)
Network type	Celluar	Celluar	Celluar	WWAN Cell based	Integrated WWAN, WMAN, WLAN (Wi-Fi, Bluetooth) and WPAN (Bluetooth)

Evolution of Mobile Communications Systems (cont.)

Generation	1G	2G	2.5G	3G	4/5G beyond
Structure	Infras.	Infras.	Infras.	Infras. based network	Hybrid of Infrastructure based and ad hoc network
Switching	Circuit switched	Circuit switched	Circuit switched	Circuit switched And packet switched	Packet switched
IP support	N/A	N/A		N/A Use several air link protocols, including IP5.0	All IP based (IP6.0)
New applications				Emails, maps, directions, News, shopping, e-commerce, interactive gaming, etc.	Ubiquitous computing with location intelligence
Ex system	AMPS, NMT, TACS	GSM, DCS1900, IS-95,CdmaOne	GPRS, EDGE	UMTS, IMT200, CDMA2000, WCDMA	
Security	M-sequences for voice enc	A5, m-sequences, auth	A5, m-seq. auth.	Stream cipher, block cipher, symmetric key auth	Public key crypto

Wireless Mobile Network

Security of a mobile device (i.e. smart phone or tablet) should have the same strength as a laptop computer.

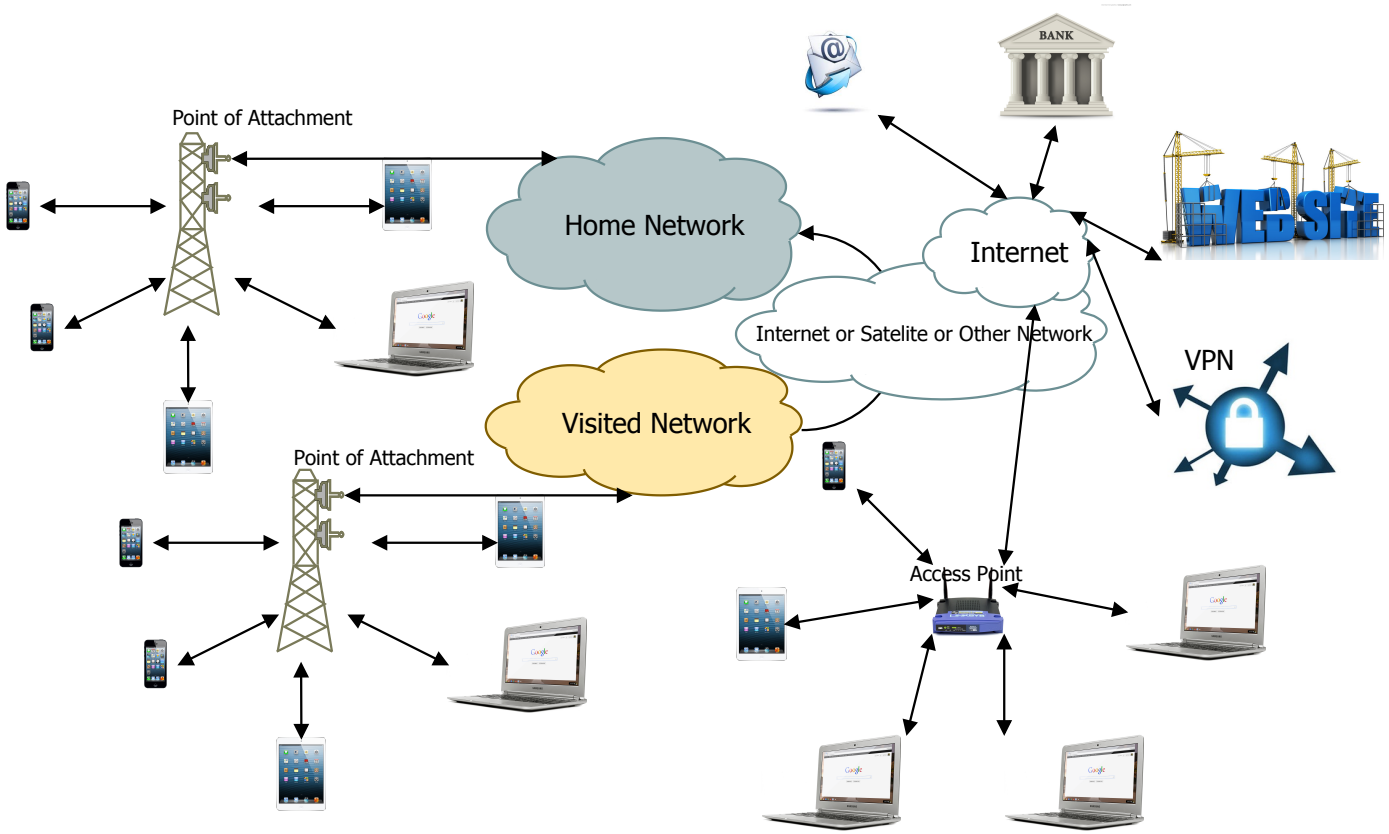


Figure : A Model of Wireless Mobile Network

Cellular Overview

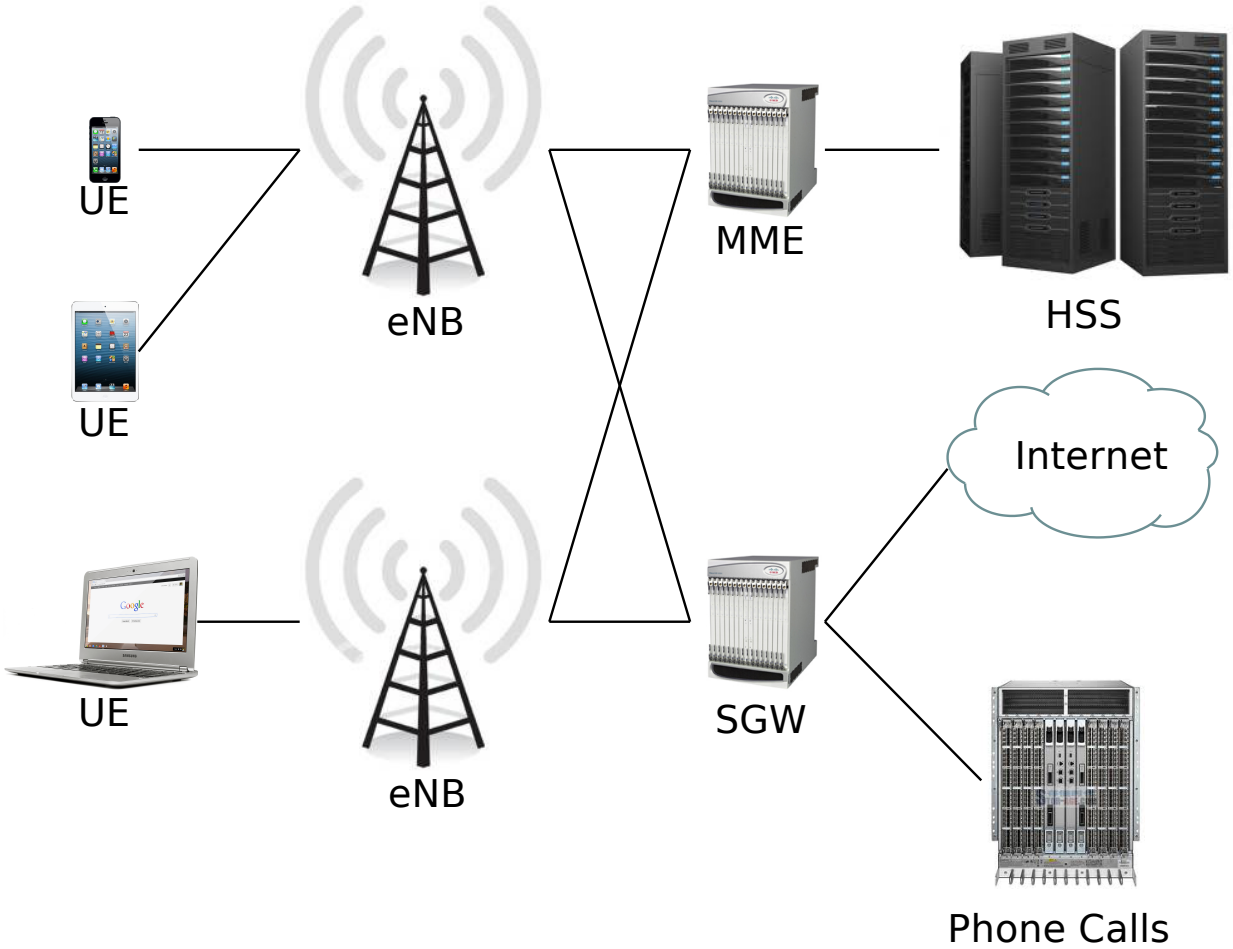


Figure : The Cellular System

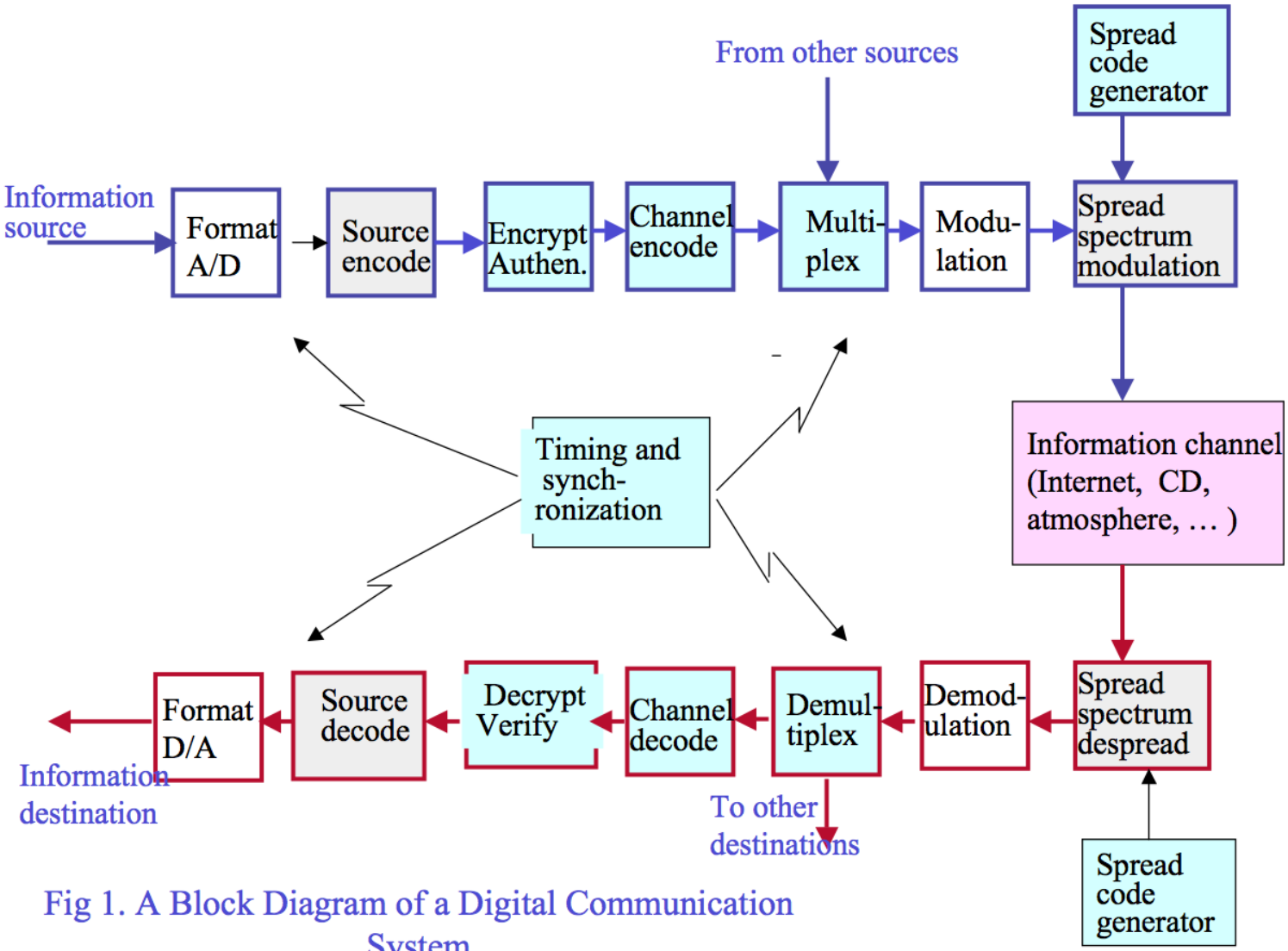


Fig 1. A Block Diagram of a Digital Communication System

3. Historic Developments

- Secure communication
- Cryptographic primitives for security services

Vernam Cipher in WWI

- The Vernam **telegraph** encryption method is the **first stream cipher** model.
- Vernam used Baudot 5-bit code to encode plaintext. He mixed two Baudot-coded punched paper tapes

  hole being a “+," no hole a “-"

  one tape contained the plaintext message and the other the “key".
- These **tapes** were added “modulo 2" (“exclusive or") in a **mechanical tape** reader producing output cipher signal.
- At the receiving end, the incoming cipher is added (modulo 2) with a **local copy** of the identical key producing the plain text.
- If the key is **unpredictable** (i.e., probability of a “$+$" equals that of “$-$" $= 1/2$), then the cipher text is “unbreakable" (impervious to cryptanalysis).

The Vernam logic:

Plaintext	Modulo 2 ($\cdot$)	Key	$=$	Ciphertext
$+$	$\cdot$	$-$	=	$+$
$-$	$\cdot$	$+$	=	$+$
$+$	$\cdot$	$+$	=	$-$
$-$	$\cdot$	$-$	=	$-$

(In current computer binary digits, $+ \leftrightarrow 1$ and $- \leftrightarrow 0$.)

Example Encrypt Hello for telegraph.

Baudot code: $+ - + - - - - - - + + - - + - + - - + - + + - - -$

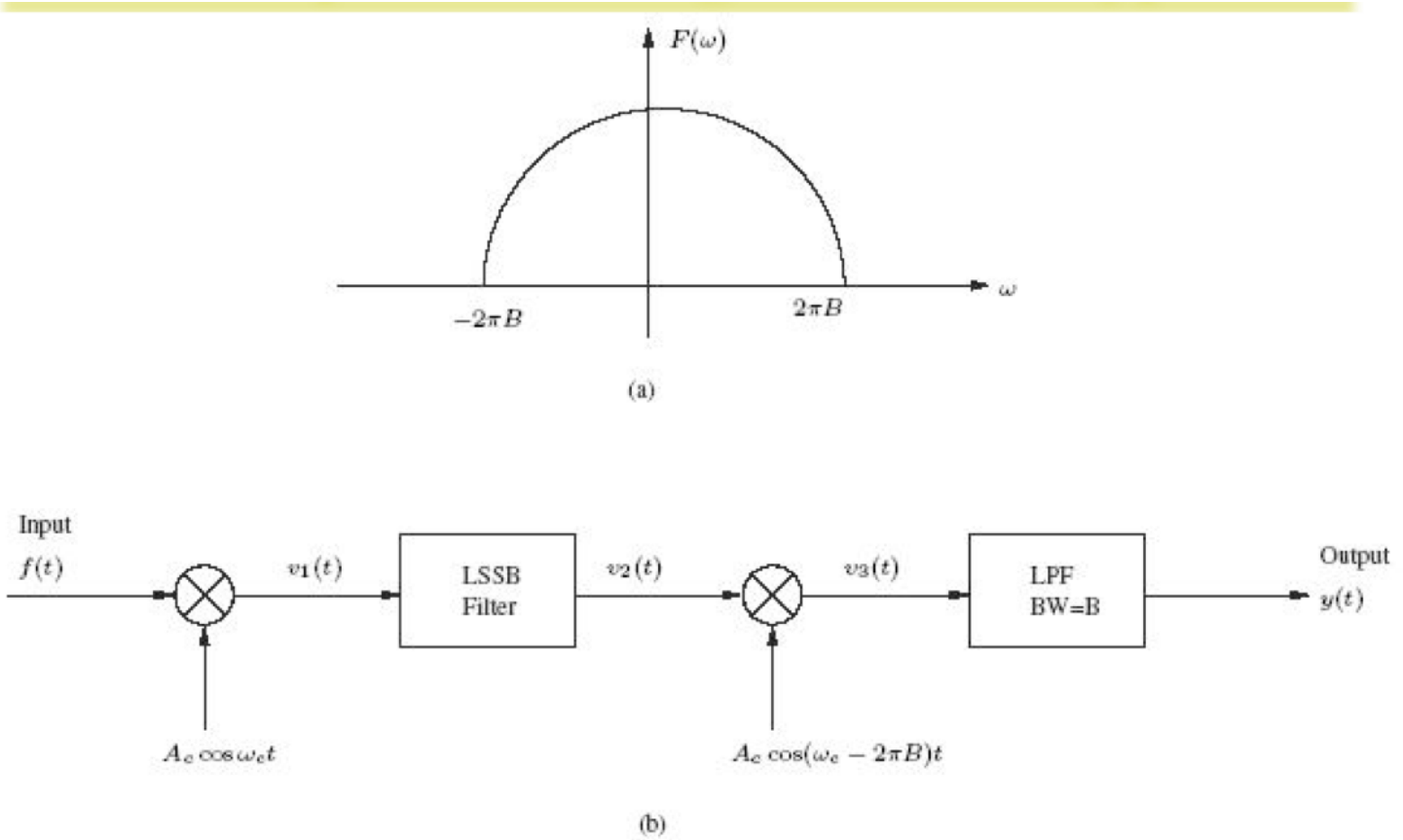
Key: $+ - - - + - - + + - + - + + + + + + - + + - + - -$

Ciphertext : $- - + - + - - + + + - - + - + - + + + + - + + - -$

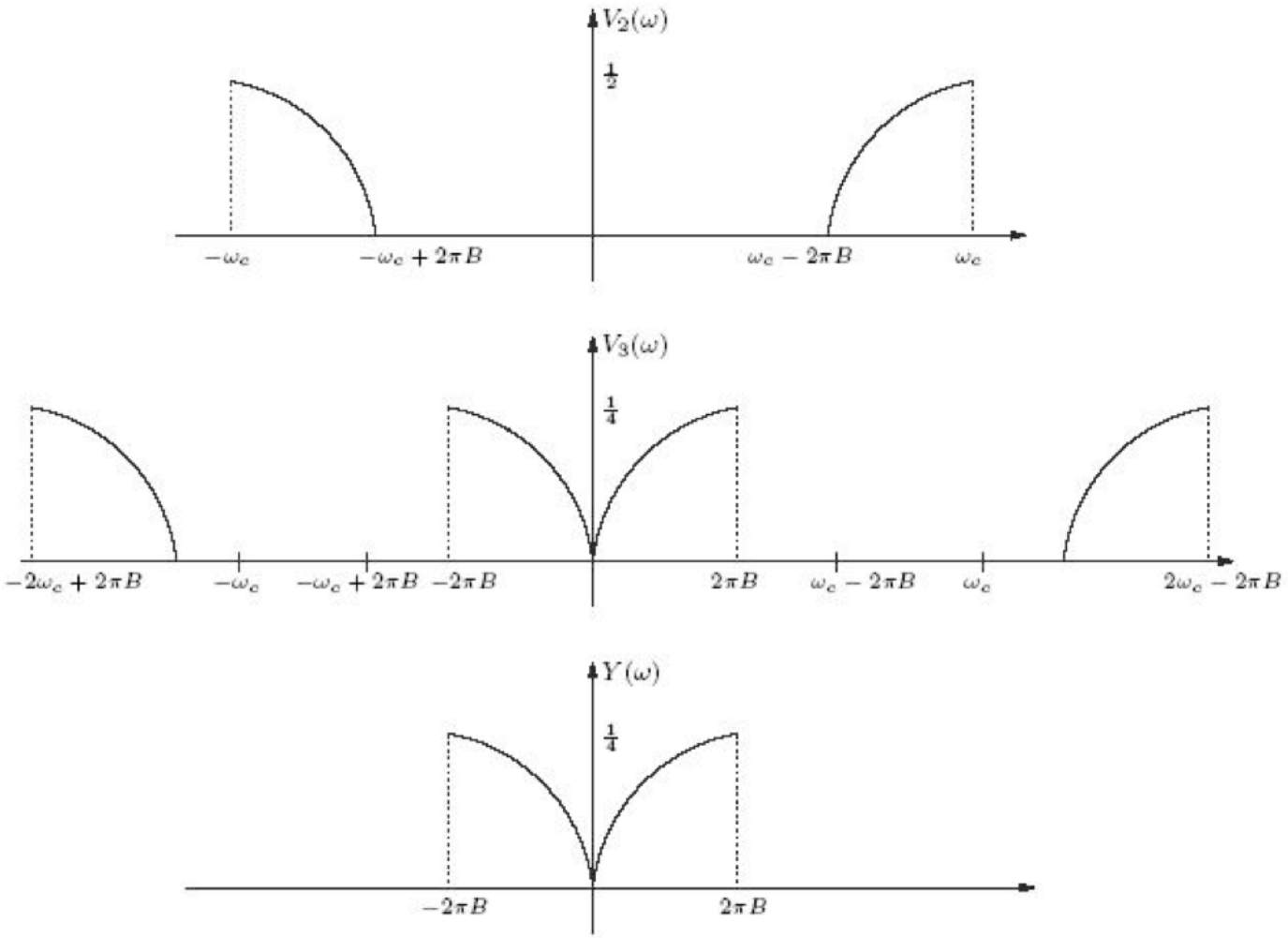
- G. S. Vernam, **Cipher printing telegraph** systems for secret wire and radio telegraphic communications, *Journal of the American Institute of Electrical Engineers*, vol. 45, pp. 109- 115, Feb. 1926.

Analog Voice Encryption

An **analog signal** $f(t)$ and its Fourier spectral density is given by $F(\omega)$, given in (a). The diagram of the encryption process is shown in (b) where the output is a scrambled signal.



Frequency Spectra of Encrypted Voice Signal



Enc and Dec

The encryption system and decryption system are the same, which used an analog amplitude modulation, called lower single sideband (LSSB) suppressed carrier amplitude modulation.

Security assumption:

The system is kept as secrecy. Or equivalently, the carrier frequency is served as a key.

How do you attack the system

Security services

Provided by upper layer crypto algorithms

- Confidentiality (privacy)
- Integrity check and authentication
- Digital signature
- Non-repudiation
- Access control

Provided by physical layer approaches

- Key distribution
- Confidentiality (privacy)
- Integrity check and authentication
- Anti-jamming attacks

Symmetric Crypto Algorithms in Practice

Stream cipher

- LFSR based
- A5/1 for GSM
- RC 4 for web security
- E0 in Bluetooth standard
- Grain, Trivium, WG in EStream
- Kasumi, Snow and ZUC for 3G
- AES in counter mode, Snow 3G and ZUC for 4G-LTE

Hash and MAC

- MD5, Rivest 1990
- SHA-1, SHA-2, NIST, 1995
- SHA-3 (NIST Dec 2010): BLAKE, Grostl, JH, Keccak, Skein.
- SHA-3, Keccak (2014)
- Authenticated Encryption (CAESAR,. March 2014)

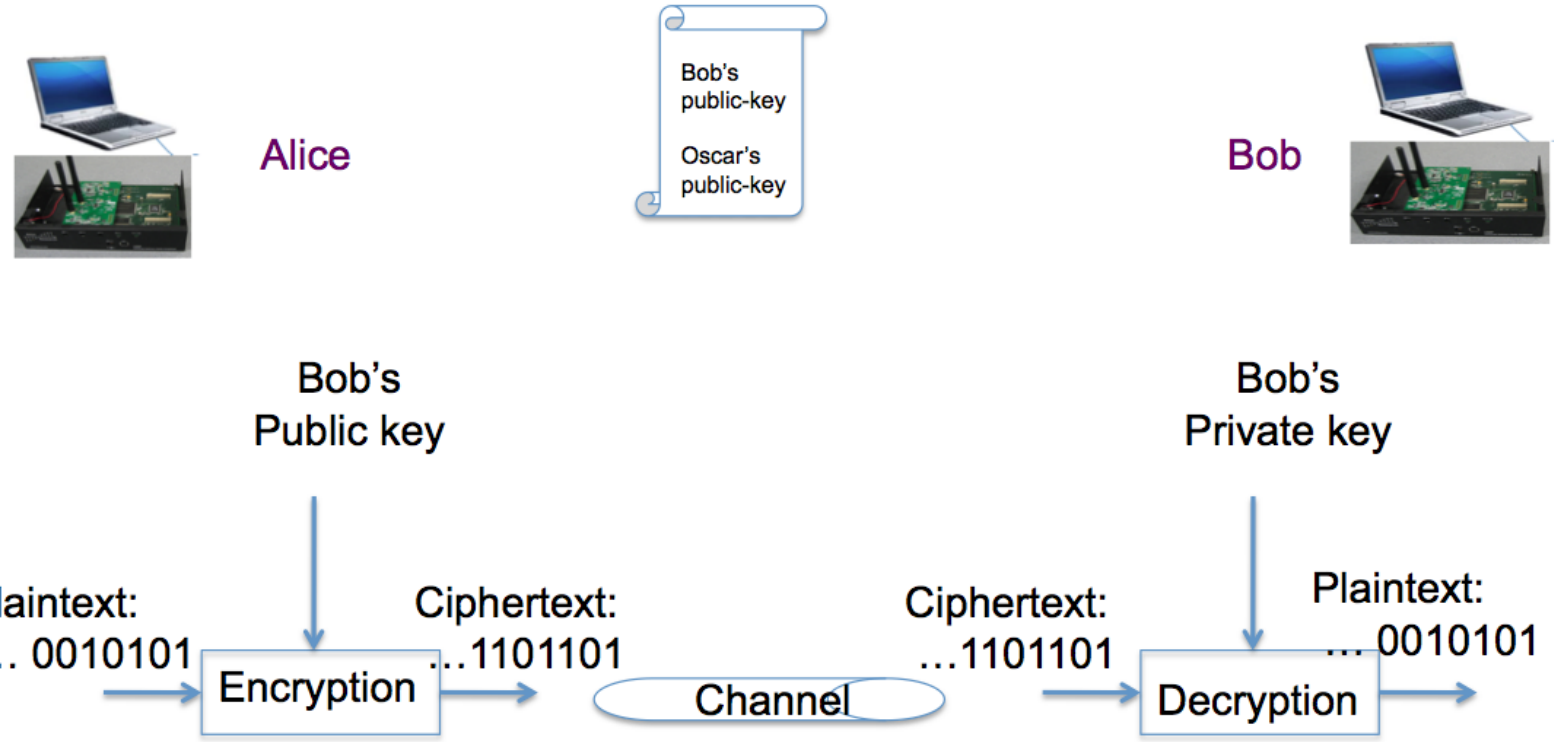
Block cipher

- DES (Data Encryption Standard, NIST, 1976)
- AES (Advanced Encryption Standard, RIJDAEL, NIST, 2000)

Secret sharing (or threshold crypto)

- Shamir, 1985, Blakley, 1985. Application sto decentralized key distribution and access control.

Simplified Model of Public-key Encryption

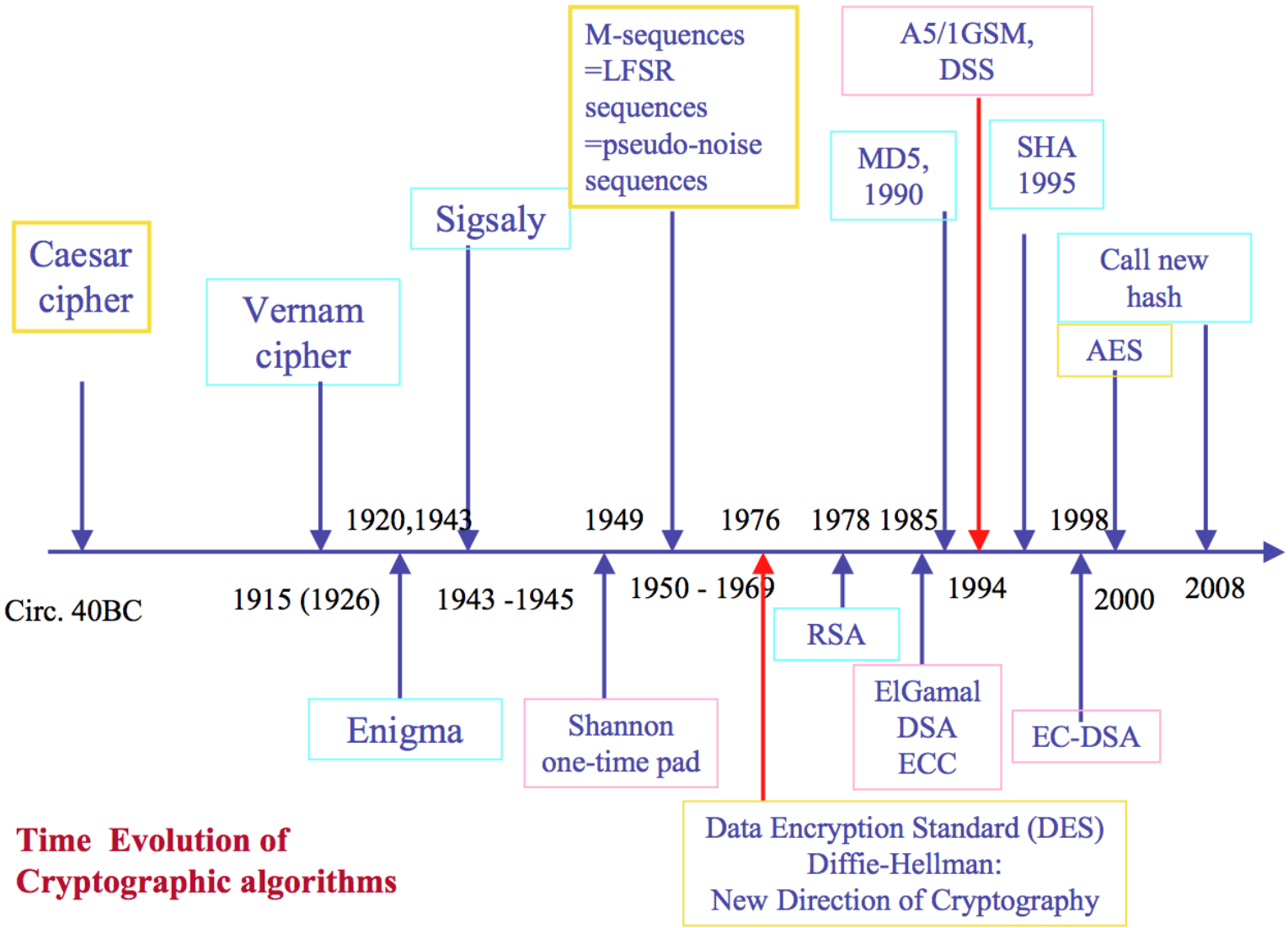


Simplified Model of Public-Key Encryption

Public-Key Cryptographic Algorithms

- DH (Diffie-Hellman) key exchange, New Direction of Cryptography,1976
- RSA, 1978
- ElGamal Digital Signature Algorithm (1985), DSS (Digital Signature Standard) NIST 1994, (a variant of ElGamal digital signature scheme, 1985)
- ECC (Elliptic Curve Cryptography), Koblitz 1987, Miller 1985, Menezes and Vanstone 1990, NIST 1998
- NTRU, 1998
- GH-PKS, Gong and Harn, 1999, XTR, 2000
- Identity-based cryptography (Shamir, 1985, Boneh and Franklin 02)
- FHE (Gentry 2008)

Evolution of Crypto Primitives



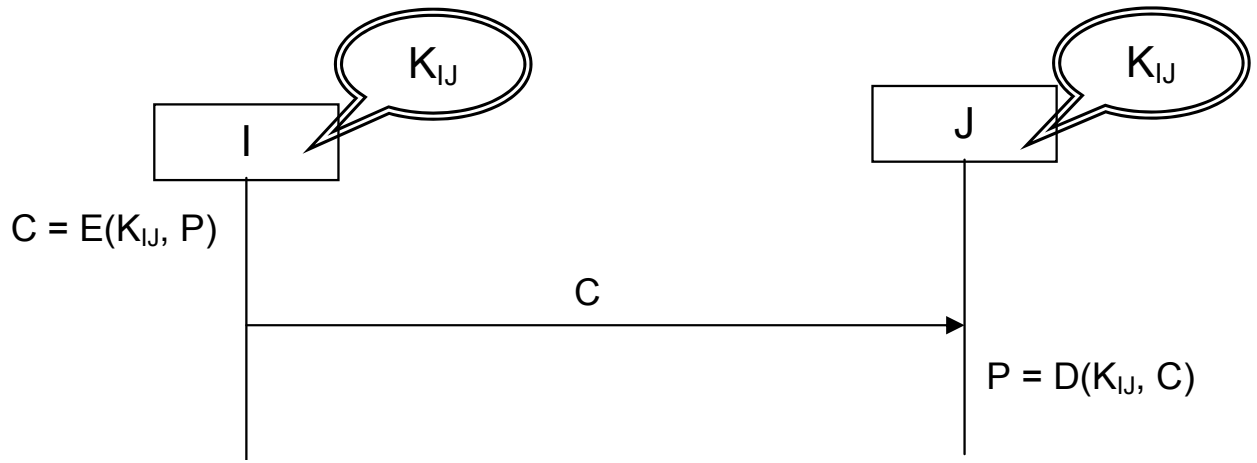
Time Evolution of Cryptographic algorithms

Topic 2. Basics of Protected Communications

1. Basic Information Security Concepts and **Protection** Mechanisms
2. **Trust** Model and Threat Model
3. Security Components

1. Basic Information Security Concepts and Protection Mechanisms

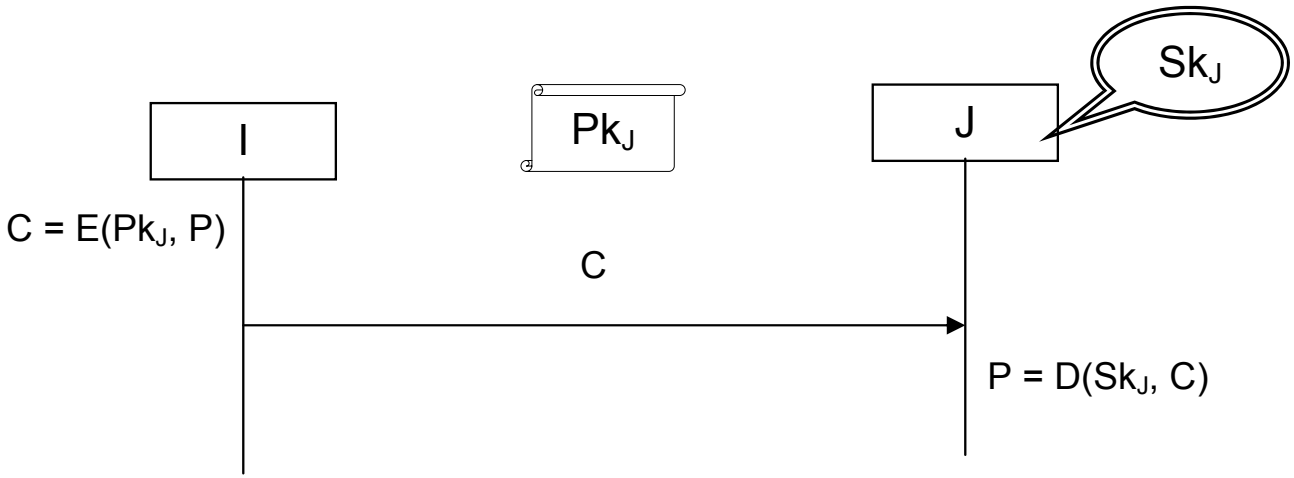
- Confidentiality: to protect information from accessing by non-eligible parties, provided encryption.
- P: plaintext and C: ciphertext.



Symmetric key based encryption: preshare the key K_{ij}

Confidentiality (cont.)

(Sk_j, Pk_j): a private key and public-key pair of entity j.



Asymmetric key based encryption

Integrity and Authentication

- Integrity and authenticity are two inseparable features in communication.
- Integrity is to guarantee that the information received is the same as it is sent.
- Authenticity is to guarantee that the originator appears to the receiver is its actual originator.
- In other words, integrity is to prevent from altering the message content, while authenticity is to prevent from altering the message source.

Two methods to provide integrity and authentication:

MAC (symmetric approach) and digital signature (public-key approaches)

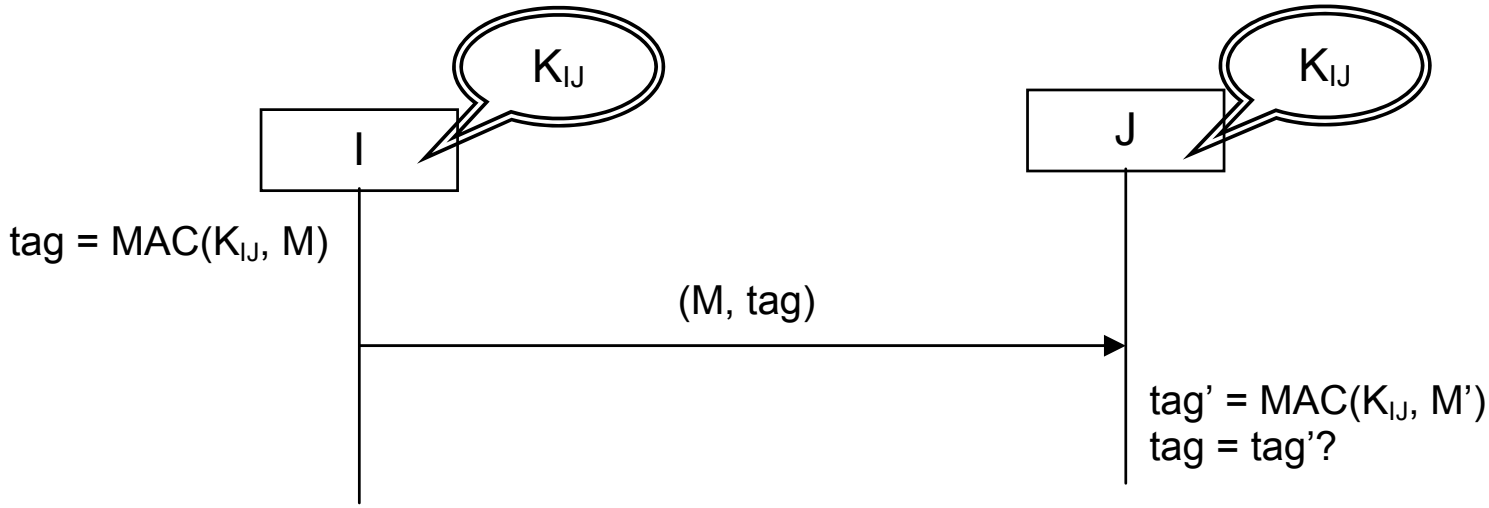


Figure : **MAC based scheme**

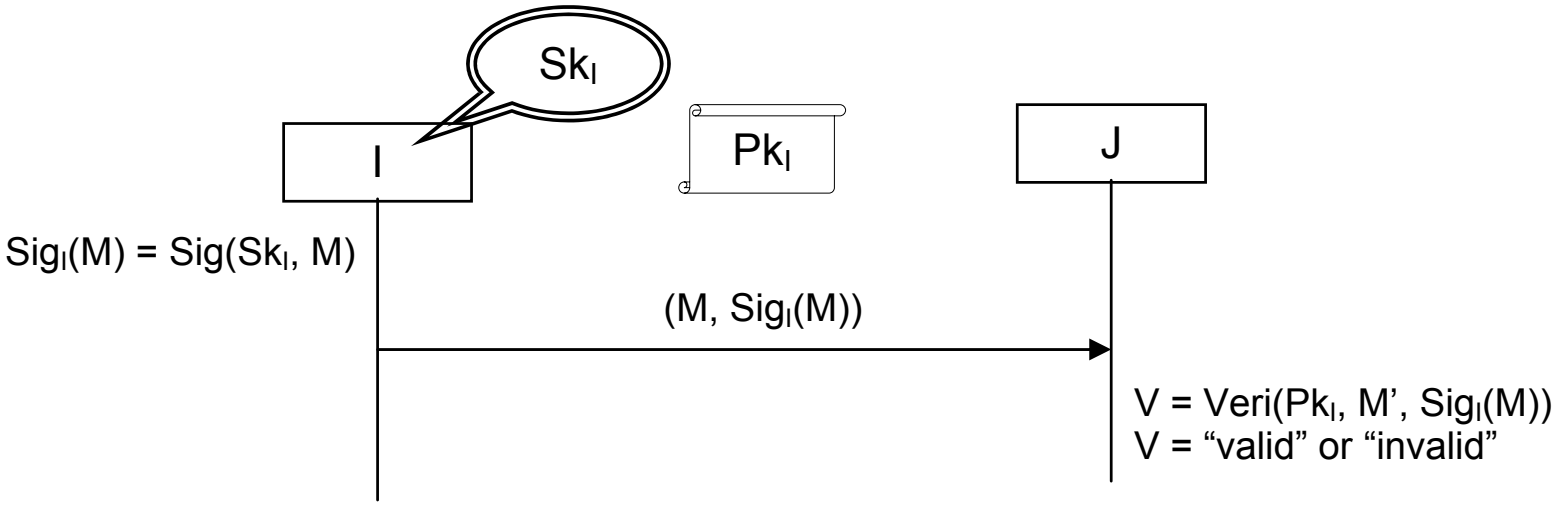
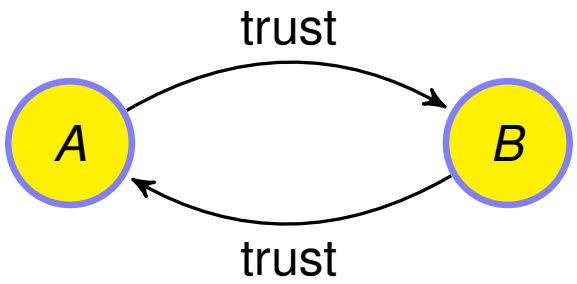


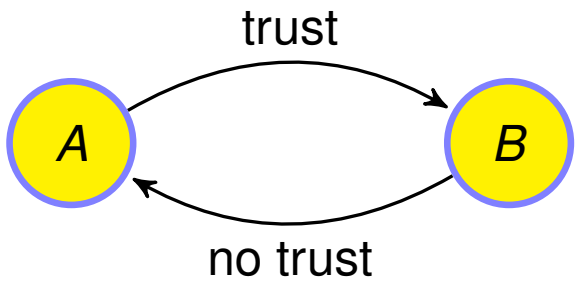
Figure : **Digital signature based scheme**

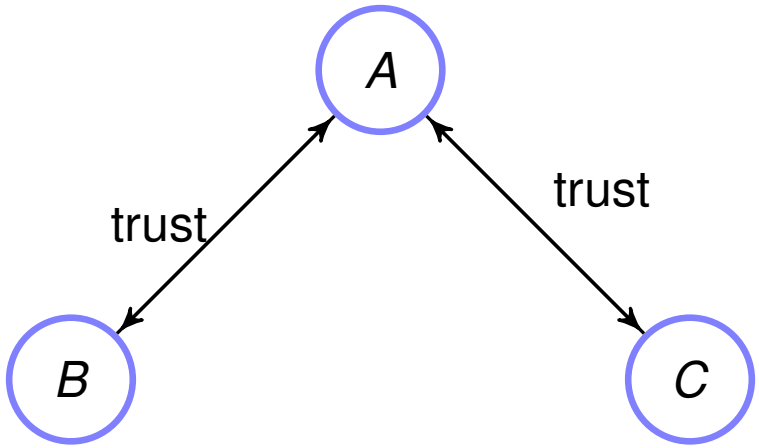
2. Trust Model and Threat Model

Trust Model

- A trust model is to define trust relations among different parties.
- The trust relations could be established by 1) assumptions for the security mechanisms, or 2) through applying security mechanisms.
- Two party trust or hierarchical trust for multiple parties.







Trust model and Infrastructure

- A trust model shall include security infrastructure support to the system.
- Informally, infrastructure support is to provide certain service to establish trust relation for other parties.
  - For a public key based cryptographic, it is very important to trust the binding between a public key and its owner.
  - Certificate authority: will be trusted by the other parties to bind a public key with its owner.

What else should we trust?

- Determined by business relations:
  - E.g., a cellular service provider may play a role of trusted party for its subscribers in the sense that the service provider can hold cryptographic keys for authenticating subscribers.
- The physical environment:
  - E.g: we may trust a server located in a company's building more than a wireless access point installed in a rest area of highway.

Threat Model

(a) Threat from the processing and communicating capacity of an attacker for breaking algorithms and protocols.

(b) The physical threat: Depends how easy it can break in a node without destroying it. For example, one can access the communication devices, can induce errors in processing, and can measure power consume. These result in what are called side-channel attacks, such as power analysis attack, fault analysis and timing attacks.

(c) The capability or possibility for an attacker to access the communications to conduct a man-in-the middle attack.

(d) Threat from wireless transmission: a wireless link is much easier to intercept or jam than a wired link (we will do it in more details). For example, use cell phones to jam civilian Globe Position System (GPS) signals. Also, using SDR to jam police and emergency frequencies are possible, which raises public safety concerns.

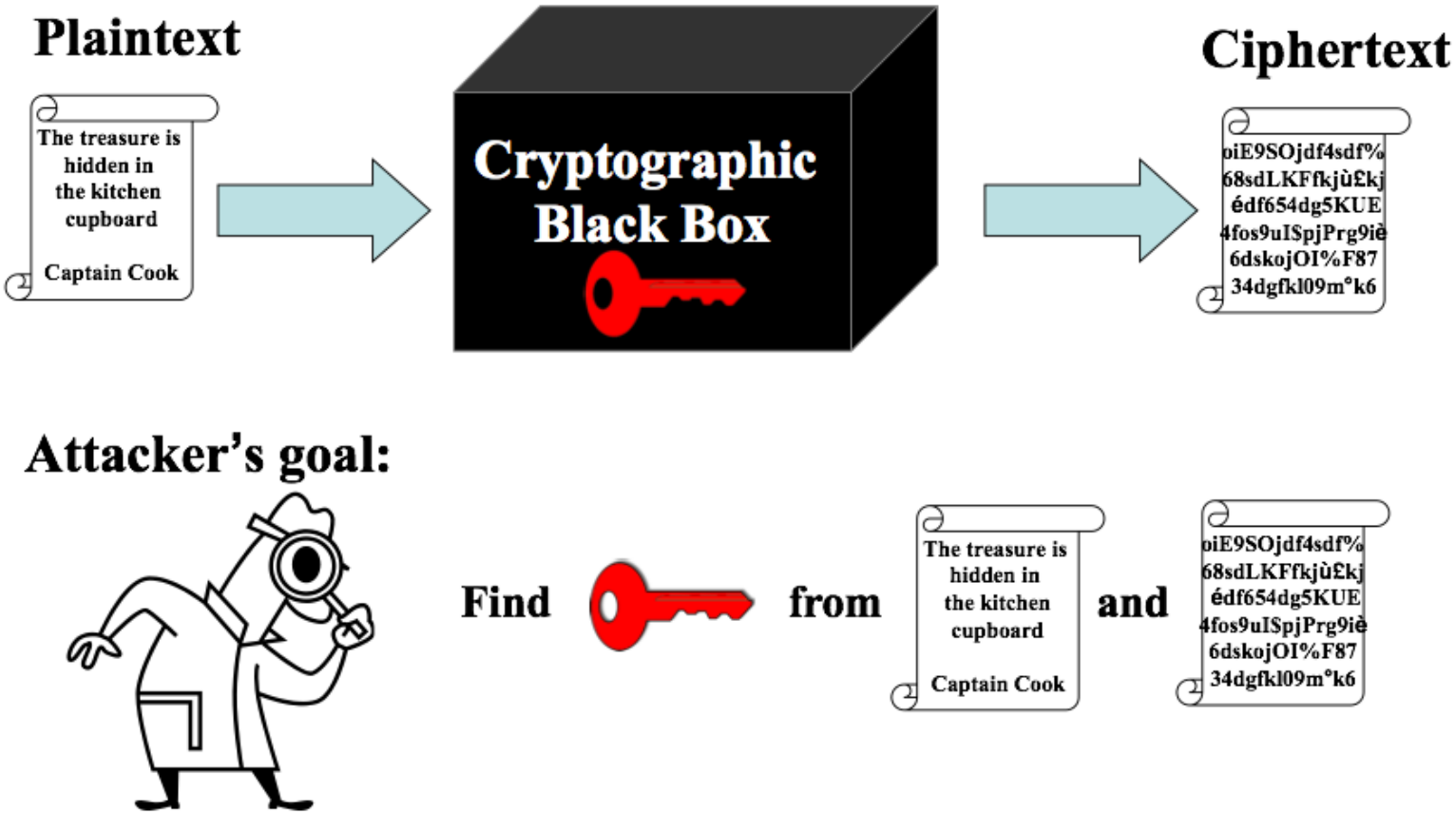


Figure : (a) Cryptographic attacks

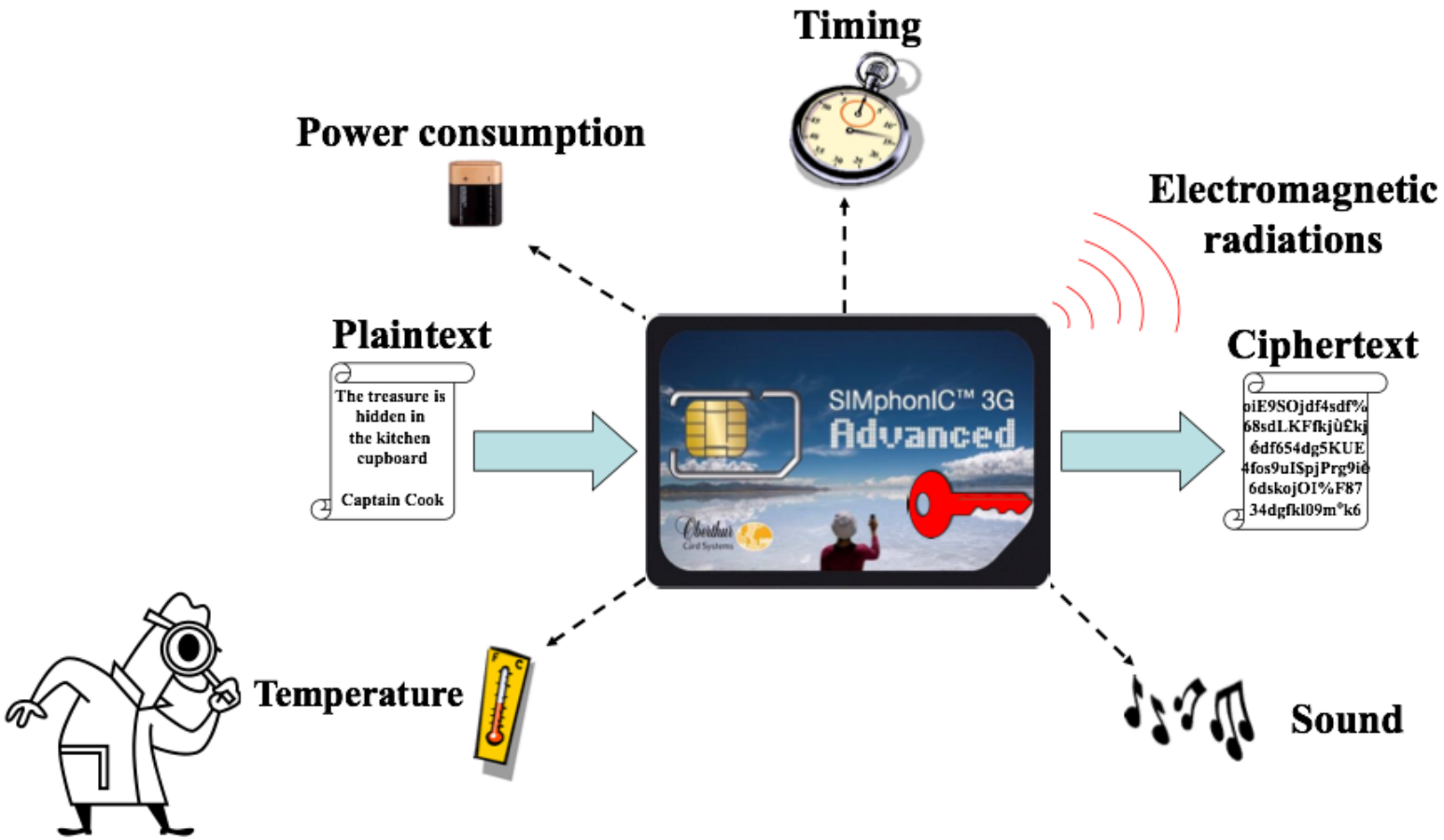


Figure : (b) Side-channel attacks

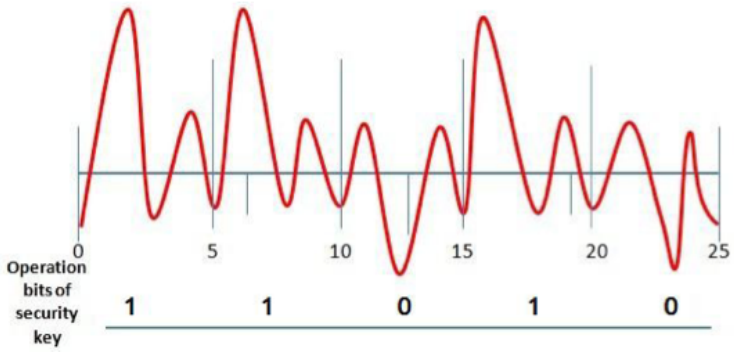


Figure : Power analysis for getting keys

The Man-in-the-Middle Attack: Case 1

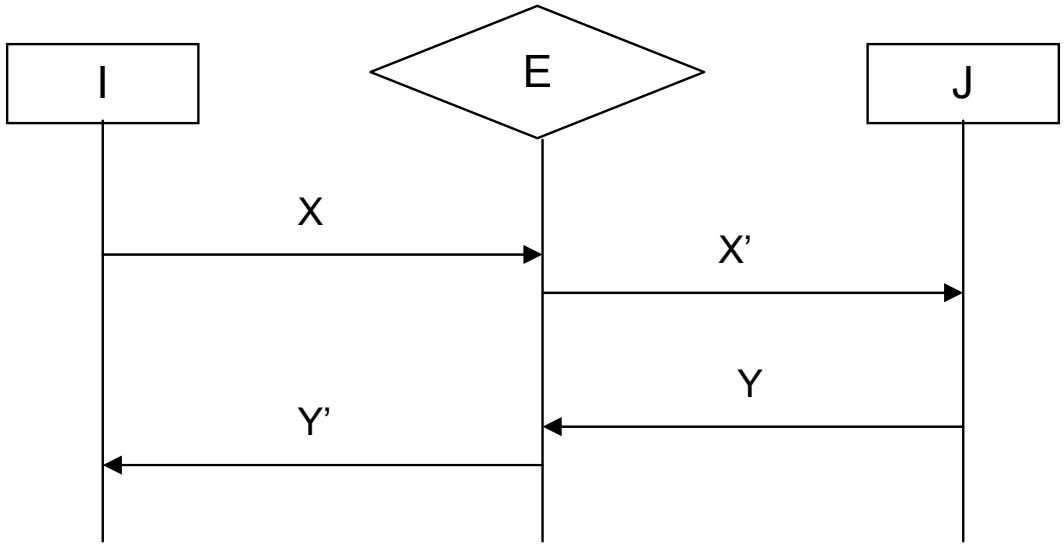
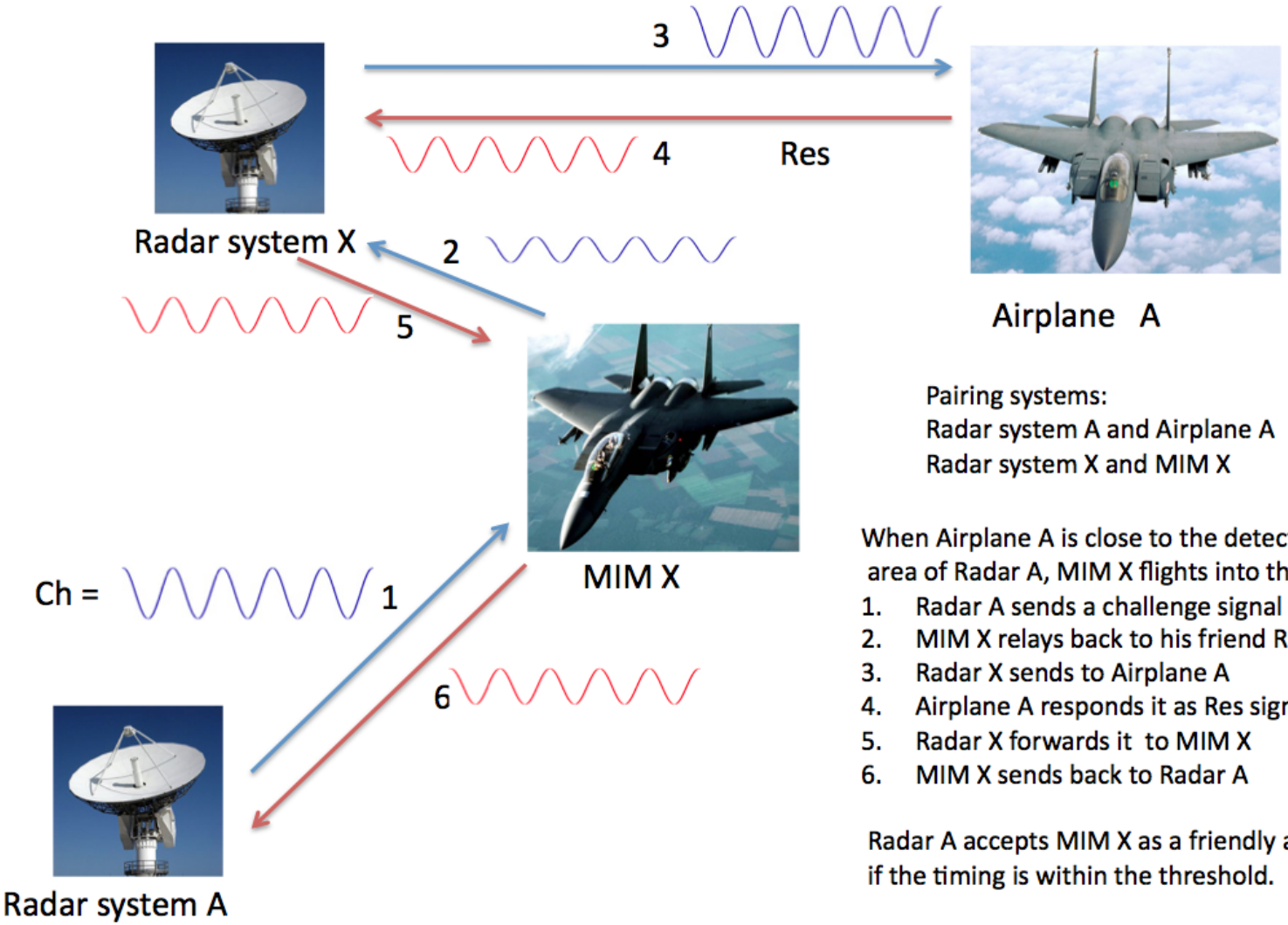


Figure : (c) Active man-in-the-middle attack

The Man-in-the-Middle Attack: Case 1 (cont.)

- The middle man E can actively intercept the message X and modify it to X before forwarding to its destination.
- It can do the same on another direction, that is, intercept the message Y and modify it to Y before forwarding, then the middle man E can manipulate the protocol between I and J and cheat either of them or both.
- Whether the man-in-the-middle can conduct a successful attack depends on different factors and attackers' intentions.
- Authenticated case: Forge is hard: messages X and Y are authenticated, then the middle man, in order to conceive any of them, must have the capability to forge a message authentication codes or valid digital signatures in real time, which is unlikely without knowing the key.
- Disrupt the protocol is easy, then fail of the verification.

The Man-in-the-Middle Attack: Case 2



Pairing systems:
Radar system A and Airplane A
Radar system X and MIM X

When Airplane A is close to the detection area of Radar A, MIM X flights into this area.

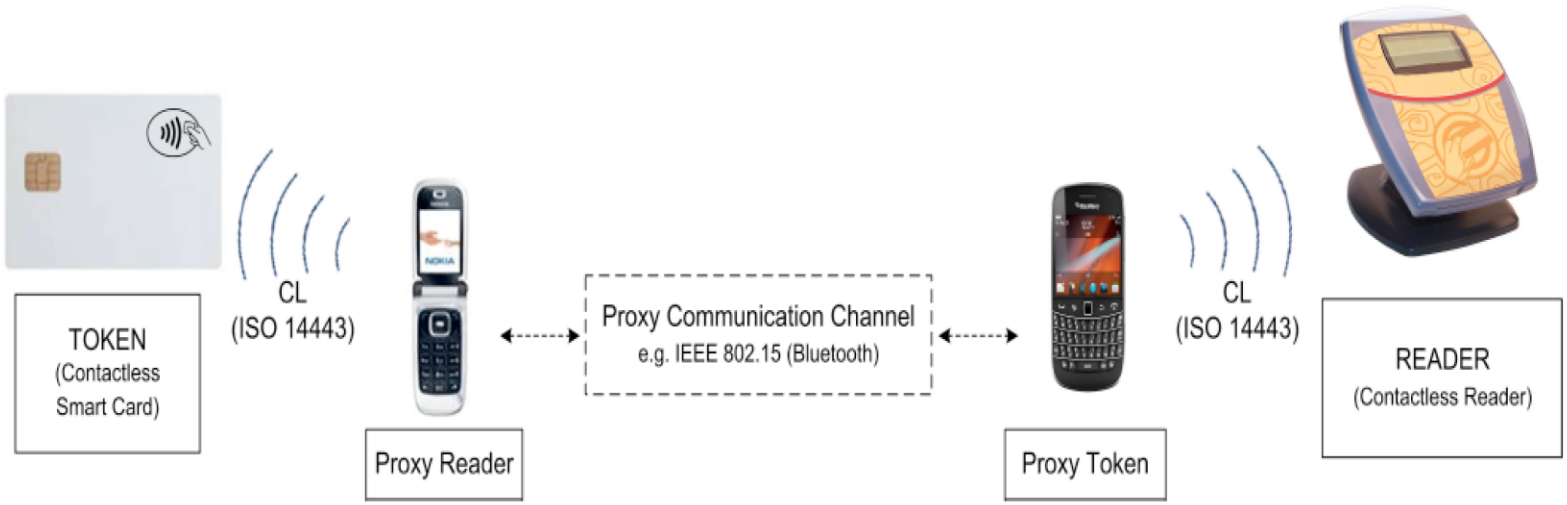
1. Radar A sends a challenge signal =ch
2. MIM X relays back to his friend Radar X
3. Radar X sends to Airplane A
4. Airplane A responds it as Res signal
5. Radar X forwards it to MIM X
6. MIM X sends back to Radar A

Radar A accepts MIM X as a friendly airplane if the timing is within the threshold.

The man-in-the-middle-attack: relay case

The Man-in-the-Middle Attack: Case 2 - Example

How your money can be stolen?



Relay Attack on on Contactless Transactions Using NFC Mobile Phone

(d) Jamming Attacks in Wireless Link

- The goal of a jammer is to deprive reliable communications from its adversary at a **minimum cost**.
- Even though it is impossible to make a communication system completely invulnerable to jamming attacks, the **goal of anti-jamming** design for a communication system is to make effective jamming attacks cost more than the attacker′s available resources.
- All modulation schemes without spreading processes in **physical layer** suffer the jamming attacks introduced in this section and the **spread-spectrum techniques** are the essential countermeasures.

Anti-Jamming Strategies

- For anti-jamming, a general principle for the design of countermeasures is to force a jammer to exhaust its resource (1) over a wide-frequency band, (2) for a maximum time, (3) from a diversity of locations.
- The most popular design options are to use the following techniques.
  (a) **Frequency diversity**, by use of spread-spectrum techniques,
  (b) **time diversity**, by use of time hopping,
  (c) **spatial discrimination**, by means of a narrow-beam antenna, which forces a jammer to enter the receiver through an antenna side-lobe or by use of new ultra wideband (UWB) technologies, and
  (d) combinations of the above three options, i.e., hybrid designs.

Note. UWB can be considered as spreading techniques, since it occupied very large bandwidth.

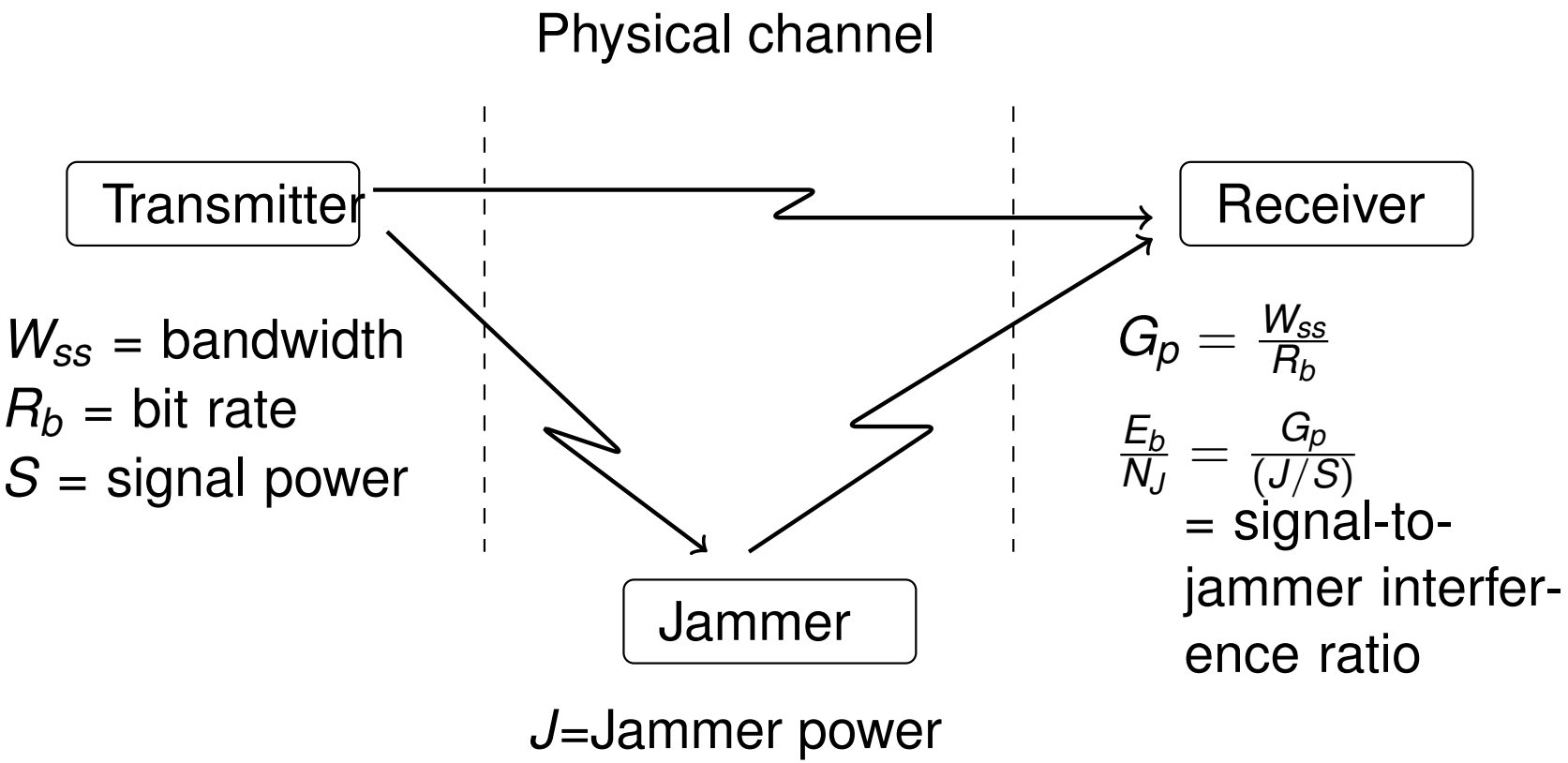
Spread spectrum techniques

1. **Direct sequence (DS)** spreading: each signal waveform is modulated with a PN (pseudo-noise) sequence generated waveform.
2. **Frequency hopping (FH)** spreading: each bit is transmitted using different frequency in its carrier signal.

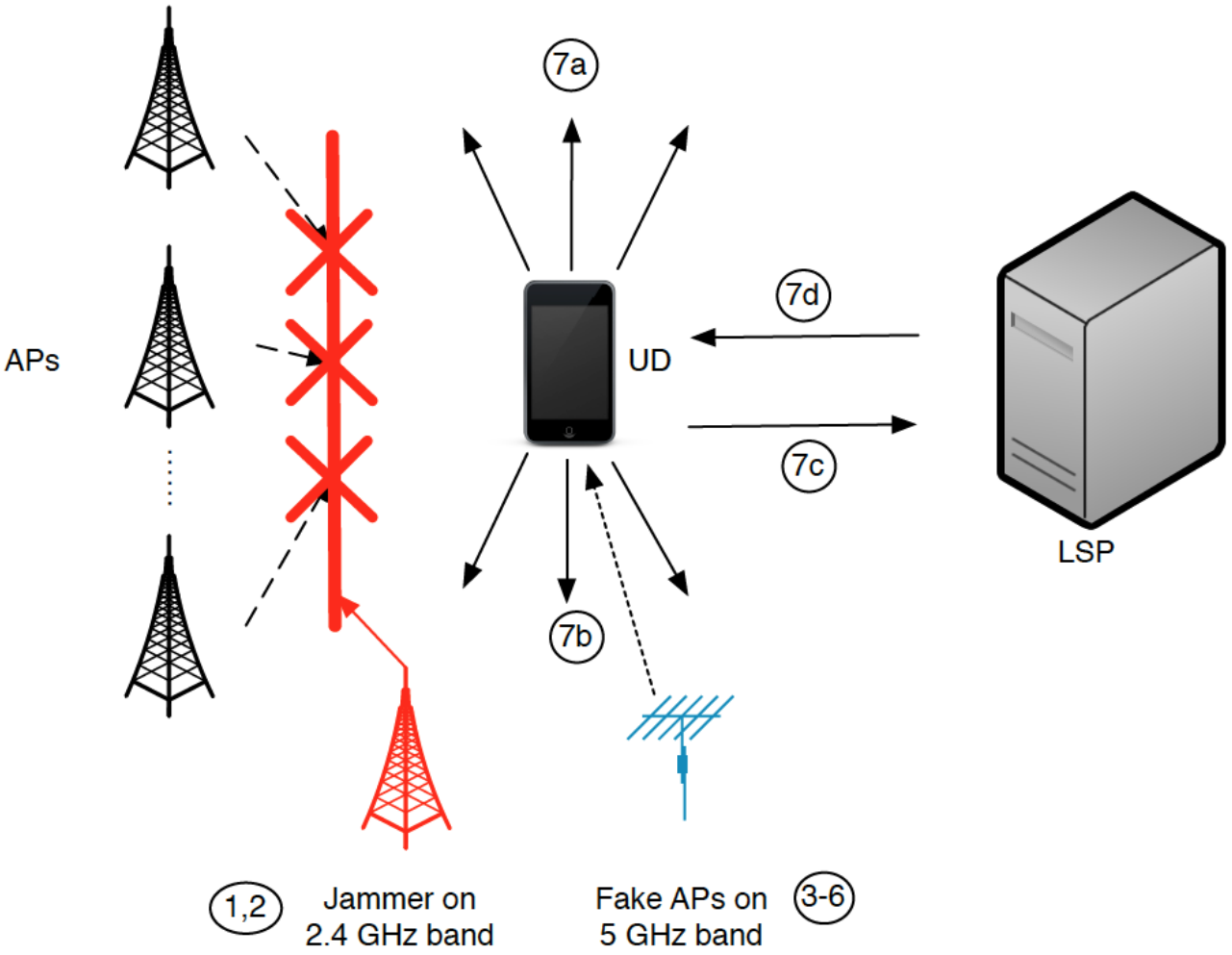
Assumptions and Definitions of a Jamming Game

1. The jammer has a **priori knowledge** of most system parameters, such as frequency bands, timing, traffic, etc..
2. The jammer does not know the **seed or key** used in the PN generator for generating spreading sequences or hopping sequences (may know PN generators but does not know the key which generates the sequence for each spreading process).

System model and assumptions for a jamming game



Example of jamming attacks



R. Feng and G. Gong

WiFi-based Location Services Attack on Dual-band Hardware, to be appeared at EMC 2014 (invited) , August 3-8, 2014, Raleigh, U.S.

Trusted Platform

- A platform should be understood as a generic term for a node. Logically, platform is a relative concept.
  - Examples: A personal computer, relative to operating system (OS) and system software, hardware processors and memories will form a platform.
  - For applications, the hardware and system software will be integrated to a platform.
- A trusted platform is a platform to operate as it is supposed to.
  - Cannot bypass an execution of encryption function before transmitting a message, if it is supposed to encrypt it.
  - Cannot issue an access to a file if the process is not entitled to.

Requirements of Trusted Platform

1). Robust hardware

- Capability to etect and response tamper or intrusion.
- To block leaking of physical characters during executions. Able to shelter physical characters of execution from observing. For example, it should hinder observations on power consumptions for cryptographic operations to prevent from obtaining useful information for the cryptanalysis.

2) Validated system software

- Operating system, includes mechanisms to execute security enhancements.
- All the security enhancements will function in the same way as they are supposed to. For example, access control may be executed by system software.
- Validated system software can assure that the access control policy is executed in the same way as it is specified.

3) Authenticated applications

- Applications should be authenticated before executed to prevent harmful applications, which either maliciously installed or poorly designed, from weakening the security.

What is in protected Communications?

- The protected communications are the communications with one or all the security properties: confidentiality, integrity, and authenticity.
- These security properties can be achieved through cryptographic algorithms.
- In order to apply cryptographic functions, the cryptographic keys need to be established between two nodes.

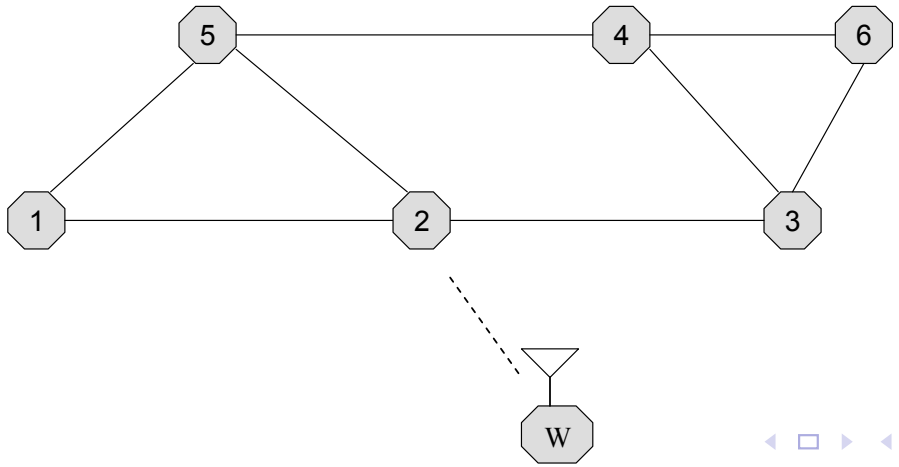
Some basic requirements to establish and conduct protected communications

- **Mutual authentication** - Each of the nodes must be insured with whom to communicate, i.e., the entity authentication, which can be understood as an insurance that the entity is actually the same as it is claimed to be.
- **Key establishment** - The key establishment must be authenticated so that each node will know with whom the keys are established. For each key, both nodes must agree on its usage, that is, for which cryptographic function and with which algorithm. They may also agree on the key life time so that the key shall not be used after it is expired.
- **Protected negotiation** - The two nodes need to negotiate which mechanisms will be applied to the communications, for example, encryption, authentication, etc. It will also negotiate that for each mechanism, which algorithms are used. The negotiation should be authenticated so that none of the nodes or an attacker can degrade the security level.
- **Failure detection** - Once the protected communication starts, each node shall be able to detect failures for the protection. That is, if one of the nodes is fail to apply the agreed protection, then the another node shall detect the failure and response properly.

Topic 3: Case Study - Security in Wireless Communication Systems

1. Protect Wireless Links

- **Wireless network** serves as an access network to connect a communication node to a wired network through radio technologies such as cellular and IEEE 802.11, where the wireless link is the first hop or the last hop in a communication path.
- **A group** of nodes can also be connected to each other through wireless links without relying on wired network.
- But due to the limited transmission distance, a network with only wireless links is only used for communications within a small geographic area.



- **Theoretically**, the security mechanisms we have discussed before should be applicable to protect wireless links.
- Practically, the selection and implementation of the security mechanisms for wireless links must consider some special requirements.
- The requirements in applying security protection for wireless scenarios, i.e., assume that the wireless link we will consider is the link between a wireless terminal and a ***point of attachment (PoA)***, which is connected to a wired network.
- The protections are applied between a wireless terminal and a PoA.

Key Establishment for Wireless Link

- In order to protect communications between a wireless terminal and a PoA, the cryptographic keys and algorithms must be established.
- The **keys** may be established through an access authentication between the wireless terminal and an authentication server.
- Then the keys are **delivered** to the PoA through a wired link.
- **Example:** In the UMTS network, the cipher key *CK* and integrity key *IK* obtained from the authentication vector will be delivered to the Radio Network Controller (RNC) to apply the protections over the air link upon a successful authentication (see Chapter 10 in the text).
- On the other hand, **the PoA** may execute a local authentication with the wireless terminal using a local authentication key. The local authentication may also derive session keys to protect the communications.

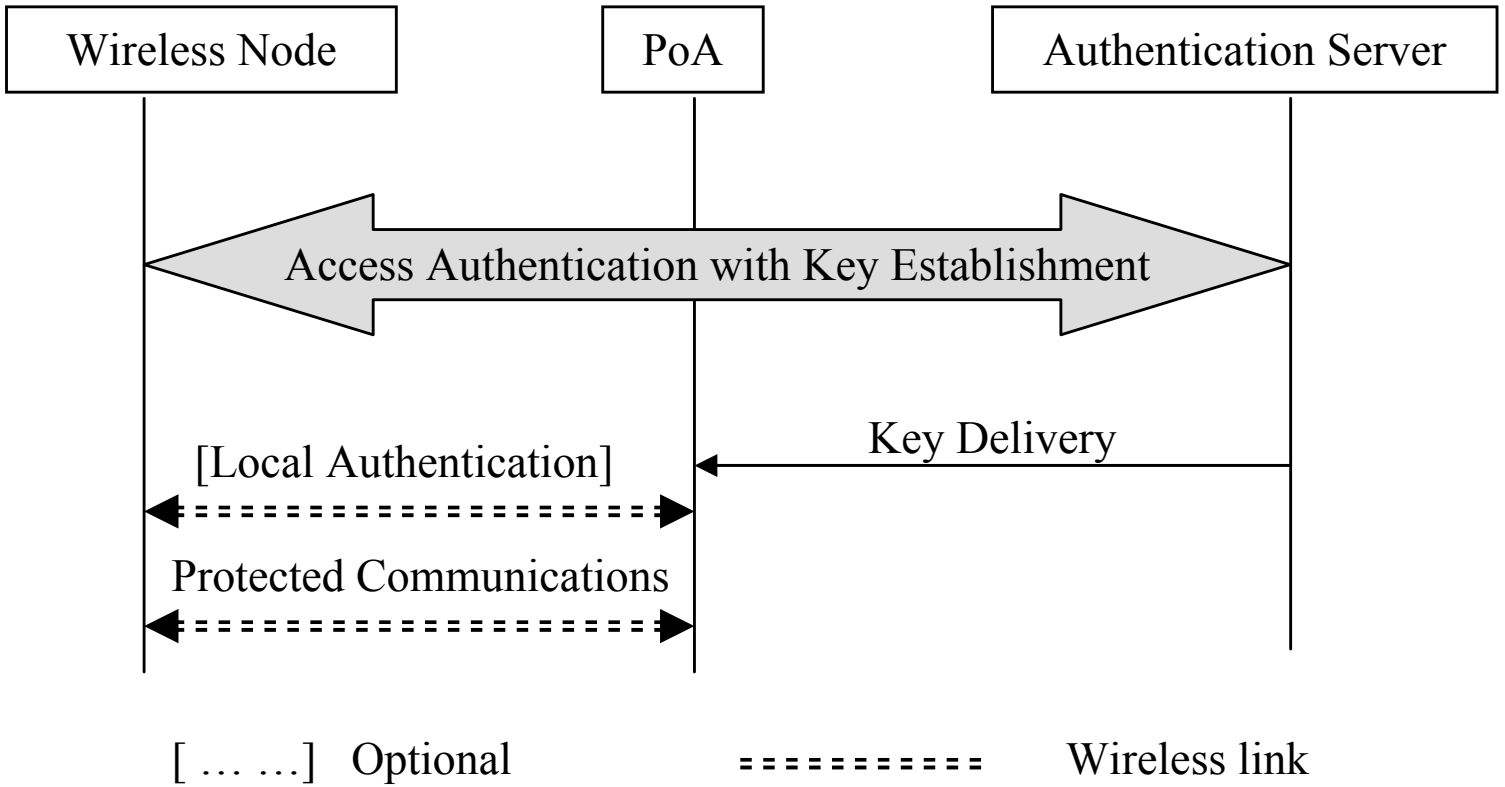


Figure : Key Establishment for Wireless Link

Challenges: Throughput and Processing Efficiency (1)

- For the **wireless** link, protections are applied at the lower layer, which will eliminate the possibility to distinguish the different application data.
- As a result, no matter which data the communication packet is carried, it must use the same mechanisms with the **maximum possible security** strength, since there is no way to make selection based on the carried data at the lower layer.
- Therefore, the performance of the security mechanisms used to protect the wireless link is crucial, considering the required **throughput** for all kinds of possible applications.
- In order to achieve the required throughput, **stream cipher** is often selected for the air link encryption due to their efficiency.
- In a stream cipher encryption, a key stream is generated independent to the plaintext string. As a result, the encryption (and decryption) will provide a pretty much **same throughput** as the original plaintext (and ciphertext) in transmission.

Challenges: Throughput and Processing Efficiency (2)

Concerns on PoA Protection

- In a wireless access network, a PoA may simultaneously conduct protected communications with a large number of wireless devices.
- The **protection** mechanisms are often implemented in hardware to avoid a bottleneck.
- The hardware implementations will **limit** the choice of the algorithms to a relatively small set, which in some way may reduce the burden for ciphersuite negotiation.
- On the other hand, if only one algorithm is supported, when the algorithm is compromised, then the hardware must be replaced.
- **Hardware** implementation makes the selection of the supported algorithms harder than the decision for software implementations.

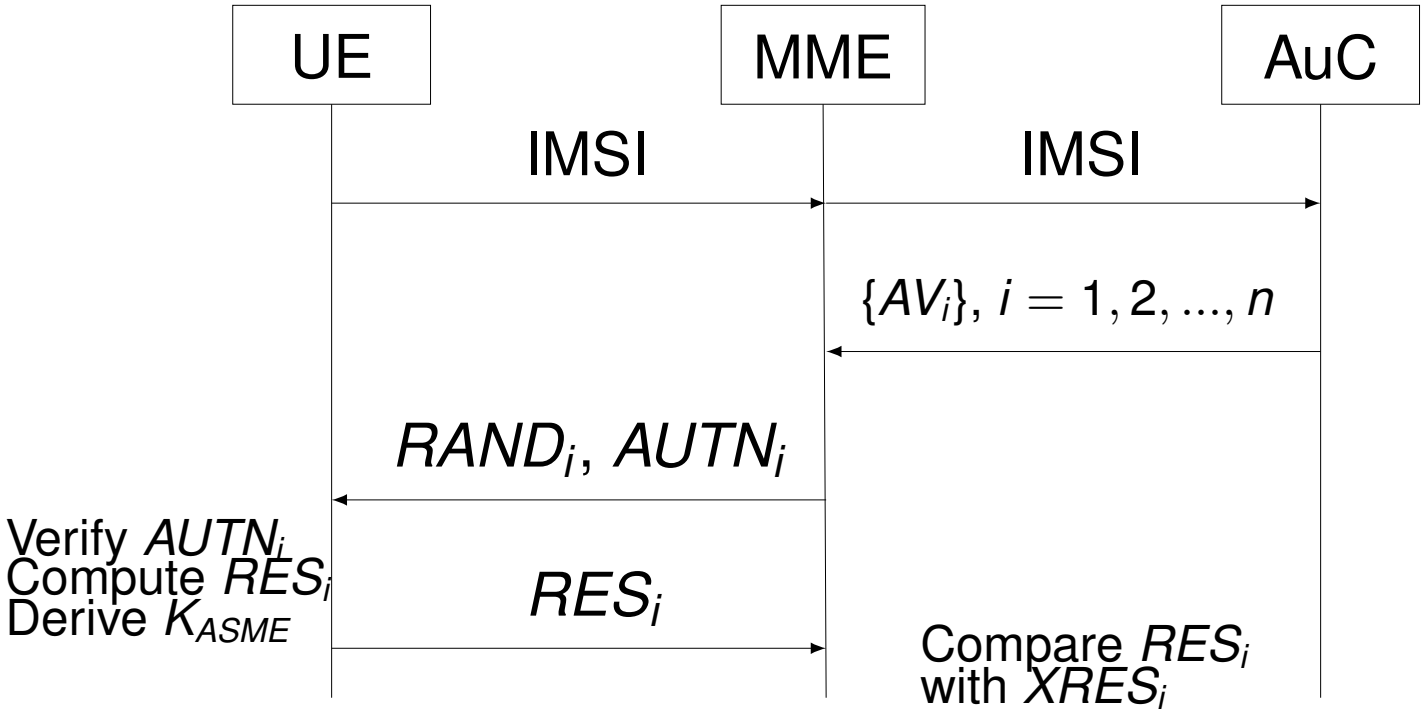
Vulnerabilities

- **Wireless signals** can be captured without physically accessing the equipments.
- For the same key, an attacker can easily obtain significant amount of ciphertexts in a short period of time to make successful **cryptanalysis**.
- When a stream cipher is used for encryption, if the plaintext includes certain redundancies, then it will not take very long to obtain a large amount of key streams. Therefore, the keys used for protecting the wireless link should be **updated frequently**.
- Wireless transmissions are easily to be **jammed**.

2. UMTS/4G-LTE AKA and Air Link Protections

- For UMTS/4G-LTE, the keys used for air link protections are established in an authentication and **key agreement (AKA)** protocol as specified in 3GPP 33.102.
- Upon a successful authentication, a cipher key (*CK*) and an integrity key (*IK*) are delivered to the **Radio Network Controller (RNC)**.
- At the **network** side, the protections are applied by RNC.
- At the **user equipment (UE)** side, even though AKA is implemented in a smart card called ***Universal Subscriber Identity Module (USIM)***, the protection mechanisms are applied in the “shell" of a UE.
- Upon a successful authentication, the USIM passes *CK* and *IK* to the UE to execute the protection mechanisms.

LTE Access Authentication Protocol - The Authentication and Key Agreement (AKA)



Detailed LTE Access Authentication Protocol (Single AV)

AKA

UE/USIM (K)	MME	AuC (K)
	$\xrightarrow{IMSI}$	$RAND, SQN \in_R Z$, compute $AV = (RAND, XRES, K_{ASME}, AUTN)$ $MAC = f_1(K, RAND, SQN, AMF)$ $XRES = f_2(K, RAND)$, $CK = f_3(K, RAND)$, $IK = f_4(K, RAND)$, $K_{ASME} = KDF(CK, IK, SN\ id)$, $AK = f_5(K, RAND)$ $AUTN = SQN \oplus AK \| \| AMF \| \| MAC$
	$\xleftarrow{AV}$	
	$\xleftarrow{(RAND, AUTN, KSI_{ASME})}$	
Compute AK Recover $SQN = (SQN \oplus AK) \oplus AK$ If $SQN > SQN_{store}$, verify MAC, compute $RES = f_2(K, RAND)$ CK, IK, K_{ASME} Otherwise, resyn.	$\xrightarrow{RES}$	Verify $RES = ?XRES$

Where does protection execute?

- **Integrity and authenticity** are only provided for control signals. Since RRC layer exists only for control signals, the integrity protection is applied in **RRC layer**.
- The **confidentiality** is provided for both user data and control signals, which is in either MAC layer or RLC layer, both are sublayers in the link layer.

Cipher Suites

Cipher suites in UMTS

- UEA1 and UIA1 are based on the **block cipher Kasumi**,
- UEA2 and UIA2 are based on the **stream cipher Snow 3G**, and
- UEA3 and UIA3 are based on the **stream cipher ZUC**, released July 2010.

The first two are currently license controlled and not freely available.

Cipher Suites in 4G-LTE

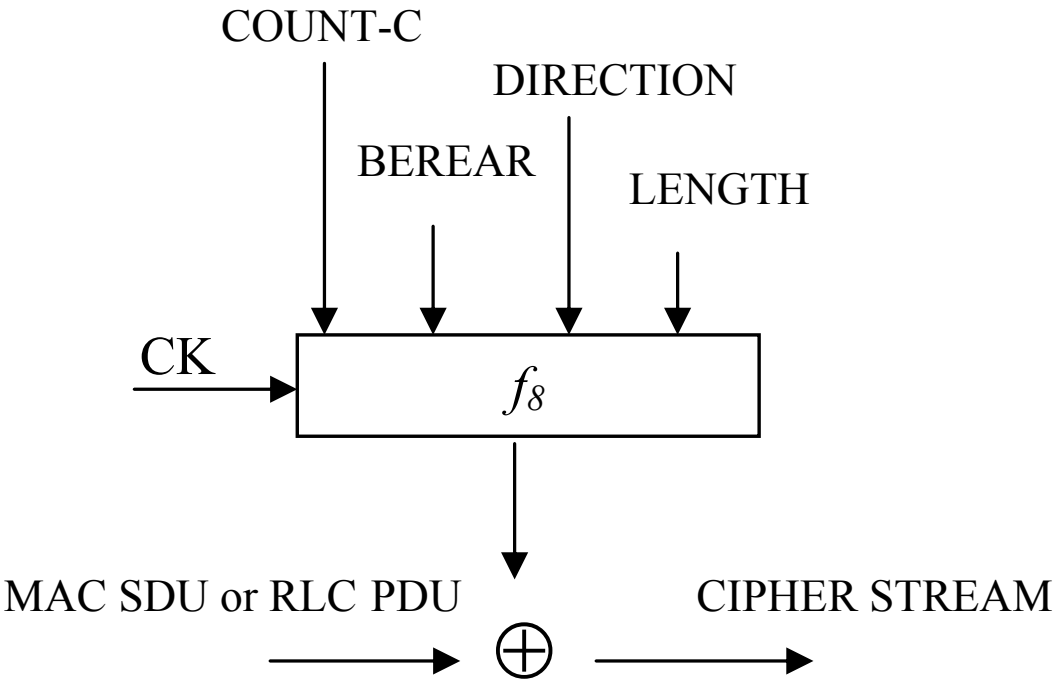
When it migrates to 4G-TLE, the block cipher Kasumi is replaced by AES, and the other two stream ciphers remain, however, it uses different terms.

(a) EEA1 and EIA1, based on stream cipher Snow 3G where EIA 1 is designed in a similar fashion as GCM;

(b) EEA2 and EIA2, based on block cipher AES counter mode for encryption and CBC - MAC for integrity; and

(c) EEA3 and EIA3, based on stream cipher ZUC.

Encryption for Air Link



UMTS/4G-LTE air link encryption where f_8 could be one of cipher in the cipher suites.

Galois Counter Mode (GCM) for Authenticated Encryption

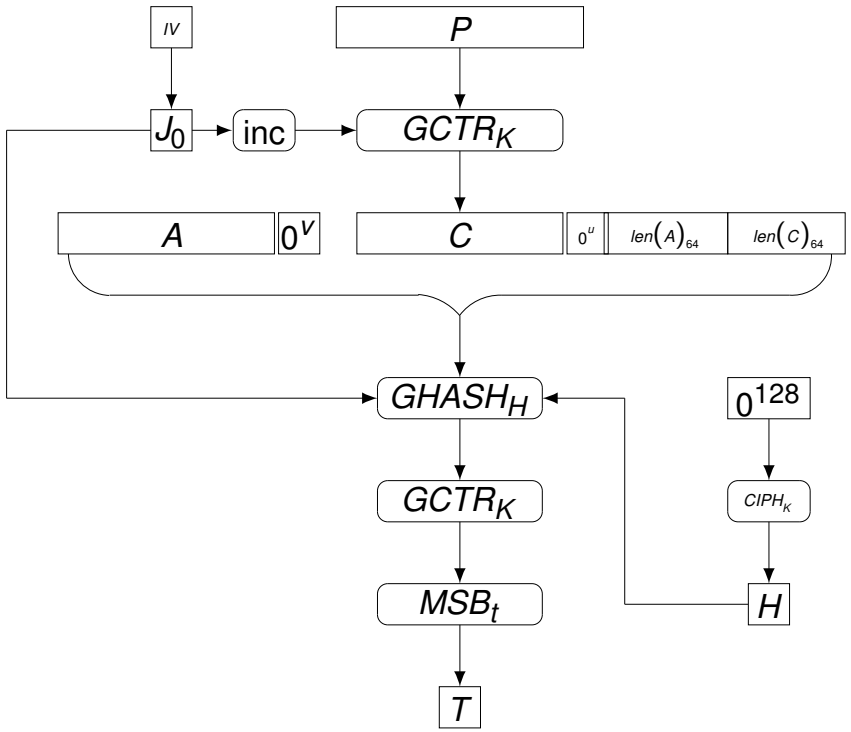


Figure : GCM (NIST Special Publication 800-38D)

GHASH in GCM

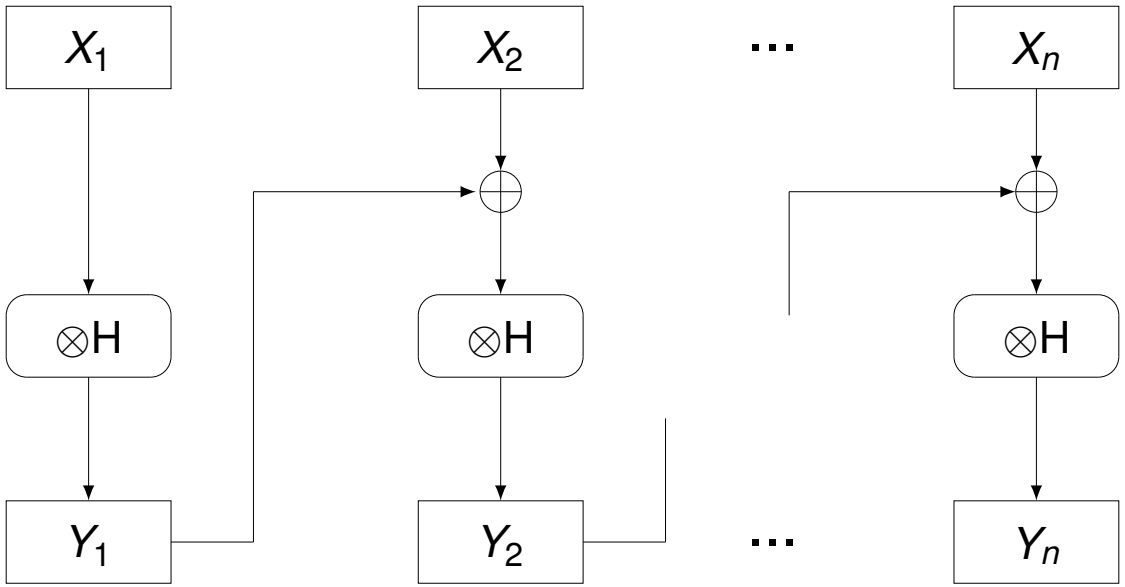


Figure : GHASH

Integrity Algorithm (EIA1)

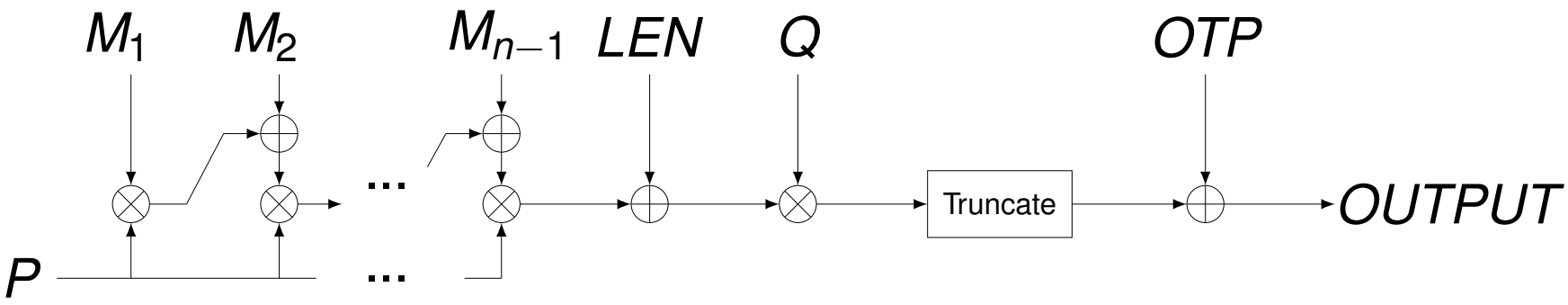


Figure : EIA1 where (P, Q, OPT) is 160-bits generated by SNOW 3G with a 128-bit key and a 128-bit IV where 128-bit IV is initialized by FRESH, a 32-bit random number F and a 32-bit COUNT-I, from the counter message. It uses a GHASH over the plaintext.

3. Some Forgery Attacks on 4G-LTE Authentication

Linear Forgery Attack

Linear Forgery Attack (Wu and Gong, 2013)

Let i be a either 1 or 2. For any $\lambda \in GF(2^{32})$

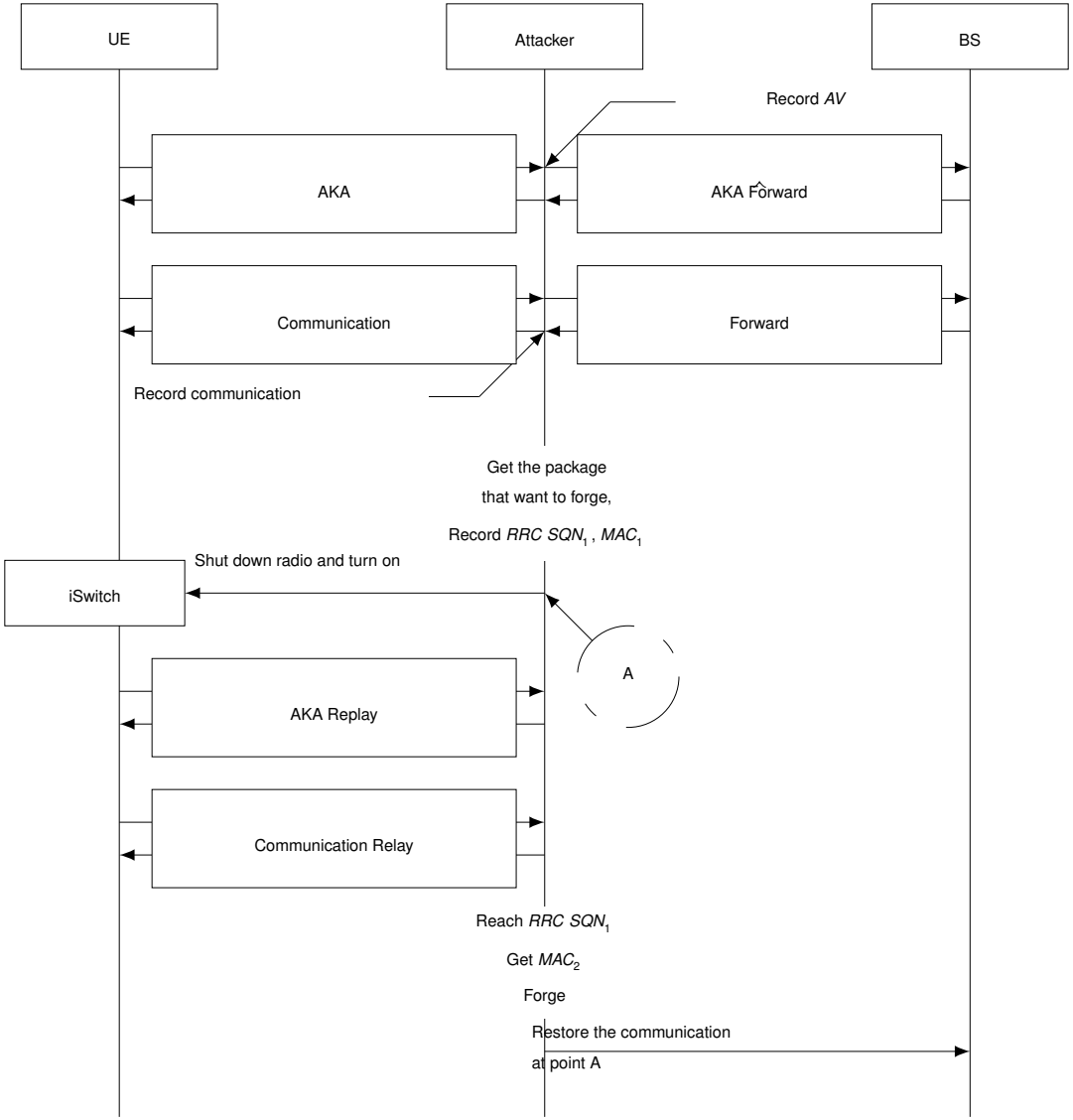
$$MAC(\mathbf{M}_{new}) = \lambda(MAC(\mathbf{M}_1) + MAC(\mathbf{M}_2)) + MAC(\mathbf{M}_i) \quad (1)$$

which is a valid MAC value of the message

$$\mathbf{M}_{new} = \lambda(\mathbf{M}_1 + \mathbf{M}_2) + \mathbf{M}_i.$$

Important Remark. EIA's MAC has 32 bits. Thus the probability of forging a valid tag by randomly picking 32-bit is $1/2^{32}$. However, if the attacker can make two queries for obtaining two valid MACs with the same IV, then he can forge 2^{32} messages with valid MACs.

Attack Scenario

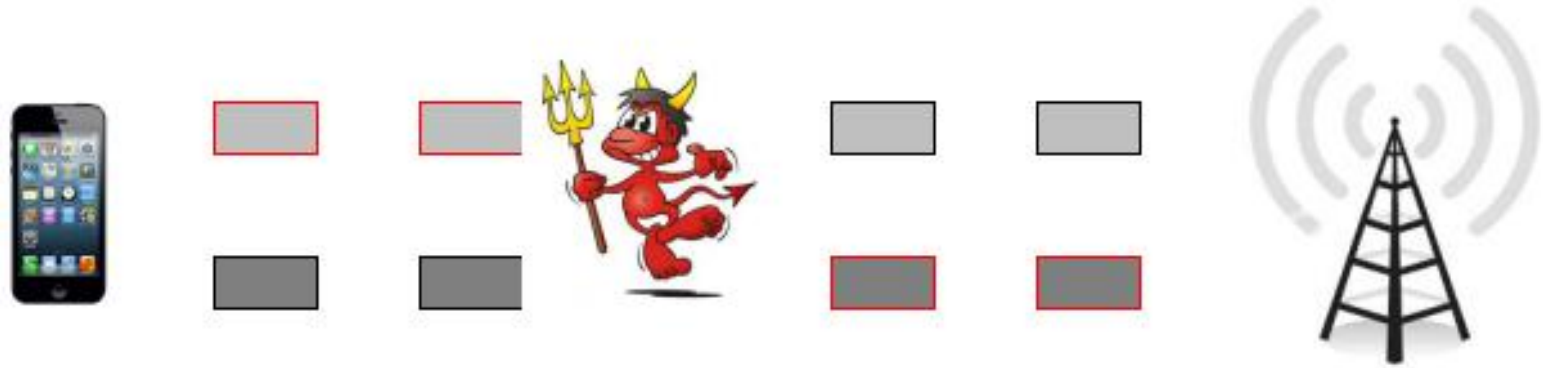


Forge the Counter Check Message

Message	Identity	UCounter	DCounter
$\mathbf{M}_1$	10 50	258 260	257 259
$\mathbf{M}_2$	10 50	259 261	258 260
$\mathbf{M}_3$	10 50	577 274	531 352

Table : Counter Check Messages

Harm of Forging the Counter Check Message



The red block could be like "<meta http-equiv="refresh" content="1;url=http://example.com">", which redirects to example.com. Or it could be a piece of advertisement.

Some Remarks

- The linear forgery attack on EIA1 can be realized through the man-in-the-middle attack (MITM).
- One can forge 2^{32} valid MACs from two queries. The probability of finding a meaningful message and corresponding MAC is increased dramatically due to the fact that the messages usually have some specific structures which may shrink the searching space.
- The forgery can be implemented because it takes
  1. the weakness of the implementation of sequence numbers used in the authentication of 4G-LTE;
  2. the fact that MAC only applied to the control data NOT user data!

Teng Wu and Guang Gong

The weakness of integrity protection for LTE. In Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks (WiSec '13). ACM, New York, NY, USA, 79-88.

How to prevent this attack?

- Change the linear structure of **GHASH**.
- Add detection machenisms for detecting fake basestation which launch MITM attack in the forgery.
- Implementation of **SQN structure** should be changed. How hard is it?
- Integrity and authentication protection should apply to user data as well. This causes the trade-off between efficiency and security of the cellular system. How can it be resolved?
- 4G-LTE should consider to perform **true mutual authentication** instead of the sequence based authentication in UE!
- . . .

Reference

If you intend to know more about communication system security, you may wish to read:

- L.D. Chen and G. Gong, **Communication System Security**, CRC 2012.