Post Quantum Security : Present & Future Directions

Dr Appala Naidu Tentu
Associate Professor

22-01-2025

CR Rao Advanced Institute of Mathematics, Statistics and Computer Science
University of Hyderabad Campus,
Prof. C.R.Rao Road, Gachibowli, Hyderabad - 500046

Outline

- Introduction
- Symmetric Key Cryptography
- Public Key Cryptography
- Quantum Computing
- Quantum vs Post-Quantum
- Post-Quantum Cryptography
- Quantum Cryptography- QKD, QRNG
- NIST's Post-Quantum Cryptography Standards Competition
  - KEM
  - Signatures
- Lattice, Code, Hash, Multivariate PQC
- (Hybrid) Quantum Security Applications

Cyber Security

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

- **Network security**
  - ✓ securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security**
  - ✓ keeping software and devices free of threats.
- **Information security**
  - ✓ protects the integrity and privacy of data, both in storage and in transit.
- **Operational security**
  - ✓ processes and decisions for handling and protecting data assets.
  - ✓ permissions to users in accessing network, data.
- **Disaster recovery and business continuity**
  - ✓ responds to a cyber-security incident-loss of operations or data.
- **Disaster recovery policies**
  - ✓ Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- **End-user education**
  - ✓ most unpredictable cyber-security factor: people.
- **Trainings and awareness**

CyberSecurity

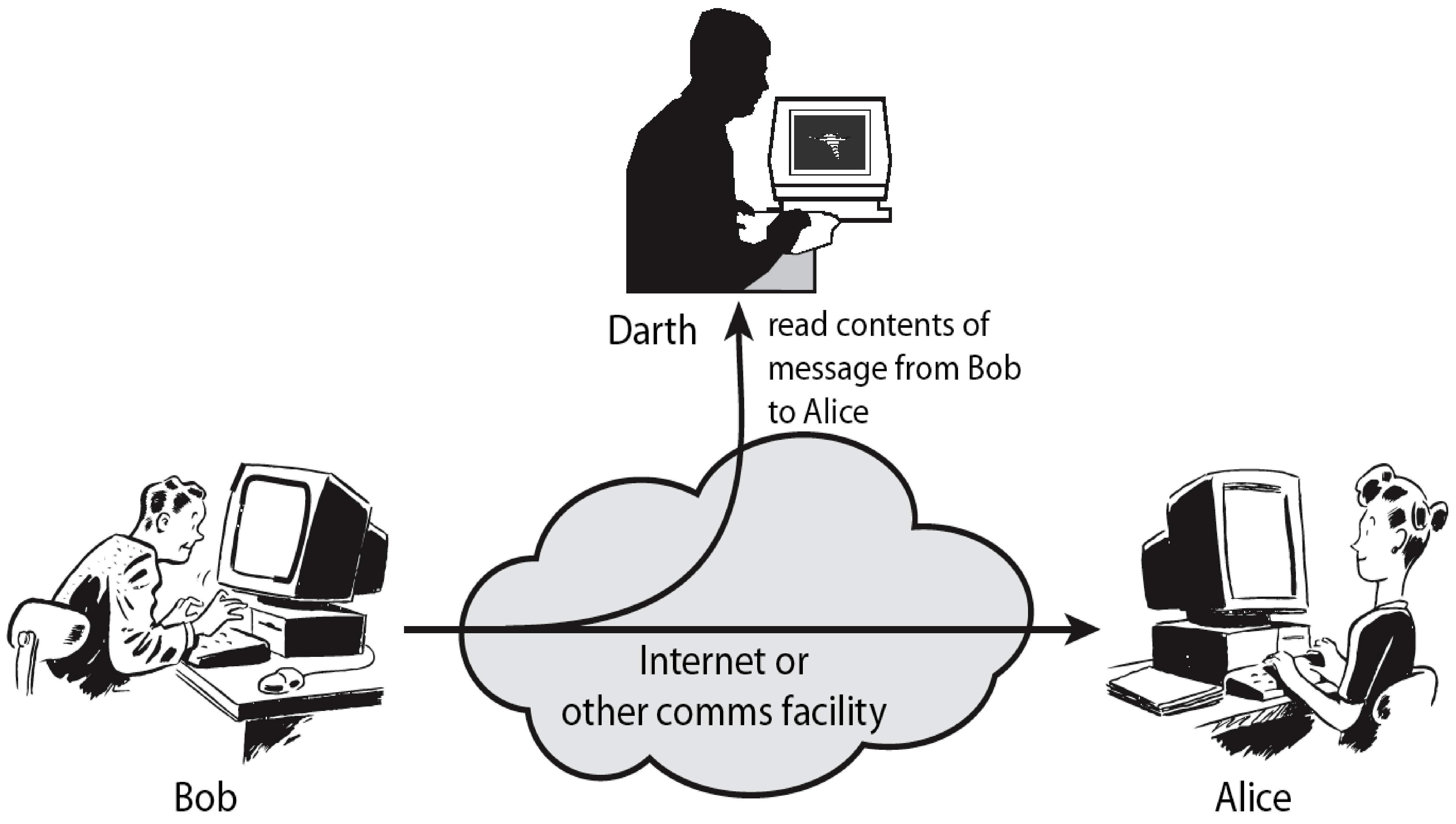
- **Well established needs for secure communication**
  - ✓ Network Security
  - ✓ Communication Security
  - ✓ War time communication
  - ✓ Business transactions, Social Media etc.

- **Requirements of secure communication**
  - ✓ **Confidentiality(Secrecy)**
    - Only intended receiver understands the message
  - ✓ **Authentication**
    - Sender and receiver need to confirm each others identity
  - ✓ **Message Integrity**
    - Ensure that their communication has not been altered, either maliciously or by accident during transmission

Cryptography is the science of secret, or hidden writing.

Cryptology

- **Cryptography:** process of making and using codes to secure transmission of information
  - **Encryption:** converting original message into a form unreadable
  - **Decryption:** Decrypting unreadable message into a readable form.
- **Cryptanalysis:** process of obtaining original message from encrypted message without knowing key.
- **Cryptology:** combines cryptography and cryptanalysis



Goals of Crypto

- Confidentiality is the concealment of information or resources.
  - E.g., only sender, intended receiver should "understand" message contents
- Authenticity is the identification and assurance of the origin of information.
- Integrity refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes.
- Availability refers to the ability to use the information or resource desired.

Security Mechanisms

- Specific security mechanisms:
  - Encipherment
  - Digital signatures
  - Access controls
  - Data integrity
  - Authentication exchange

General idea of traditional cipher

- Cipher is a method for encrypting messages

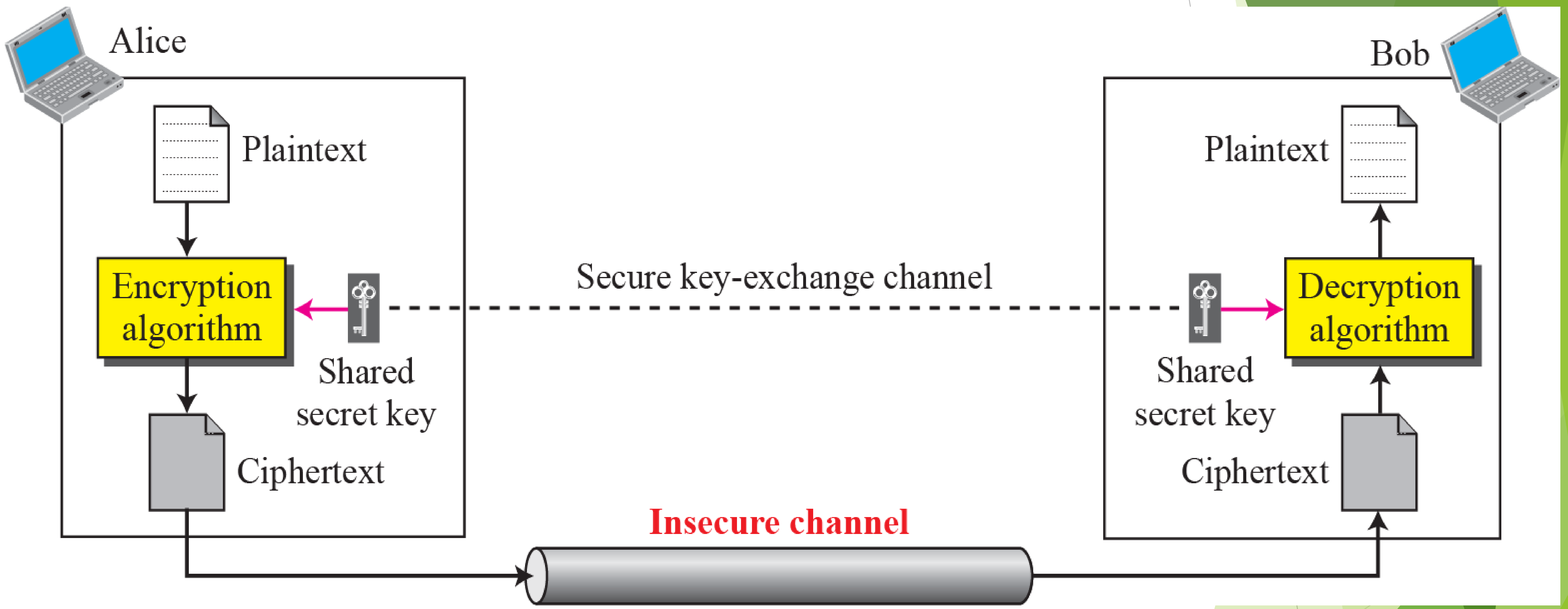
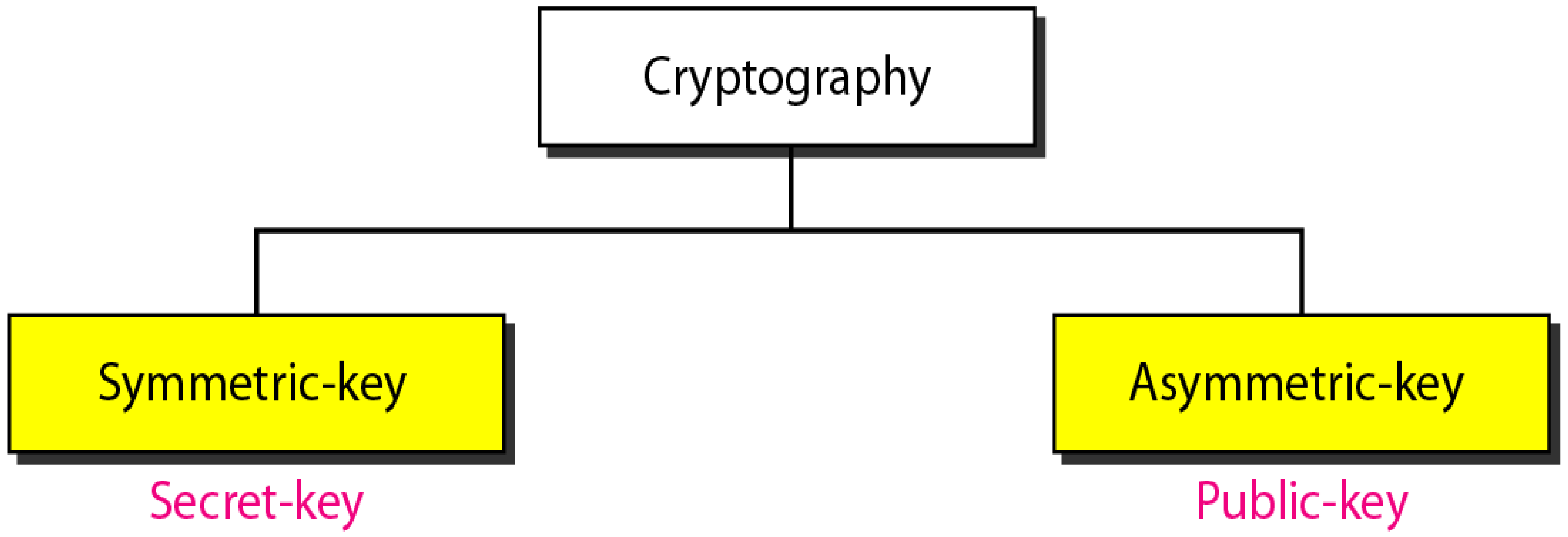


Fig: Enc-Dec Process

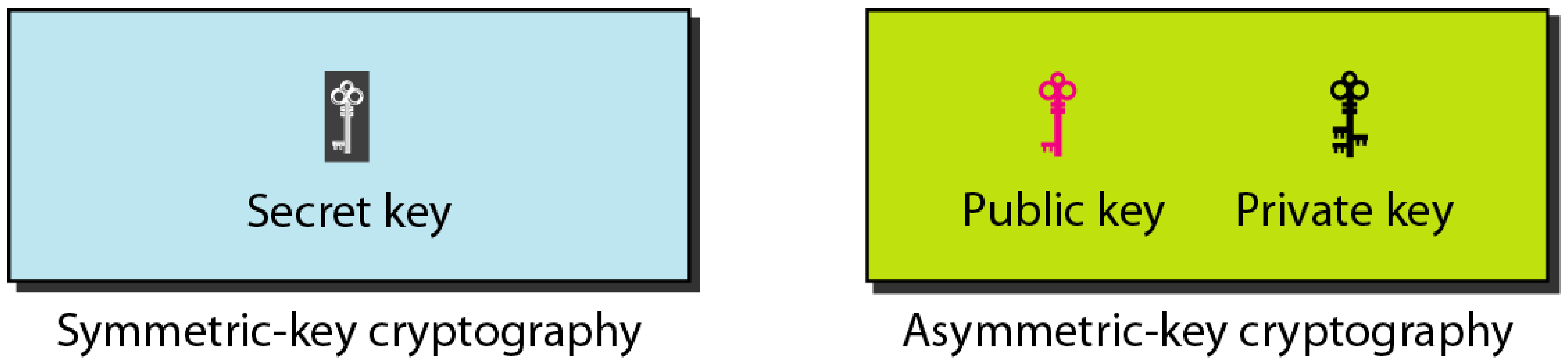
- Encryption algorithms are standardized & published
- The key which is an input to the algorithm is secret
  - Key is a string of numbers or characters
  - If same key is used for encryption & decryption the algorithm is called symmetric
  - If different keys are used for encryption & decryption the algorithm is called asymmetric.

Cryptography components

Types

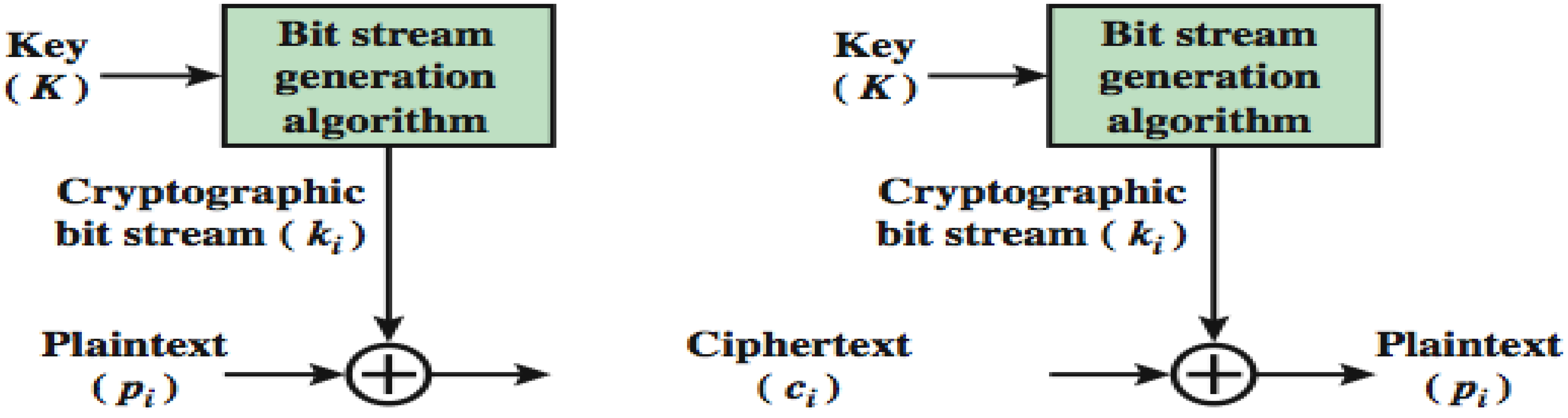


Keys used in cryptography

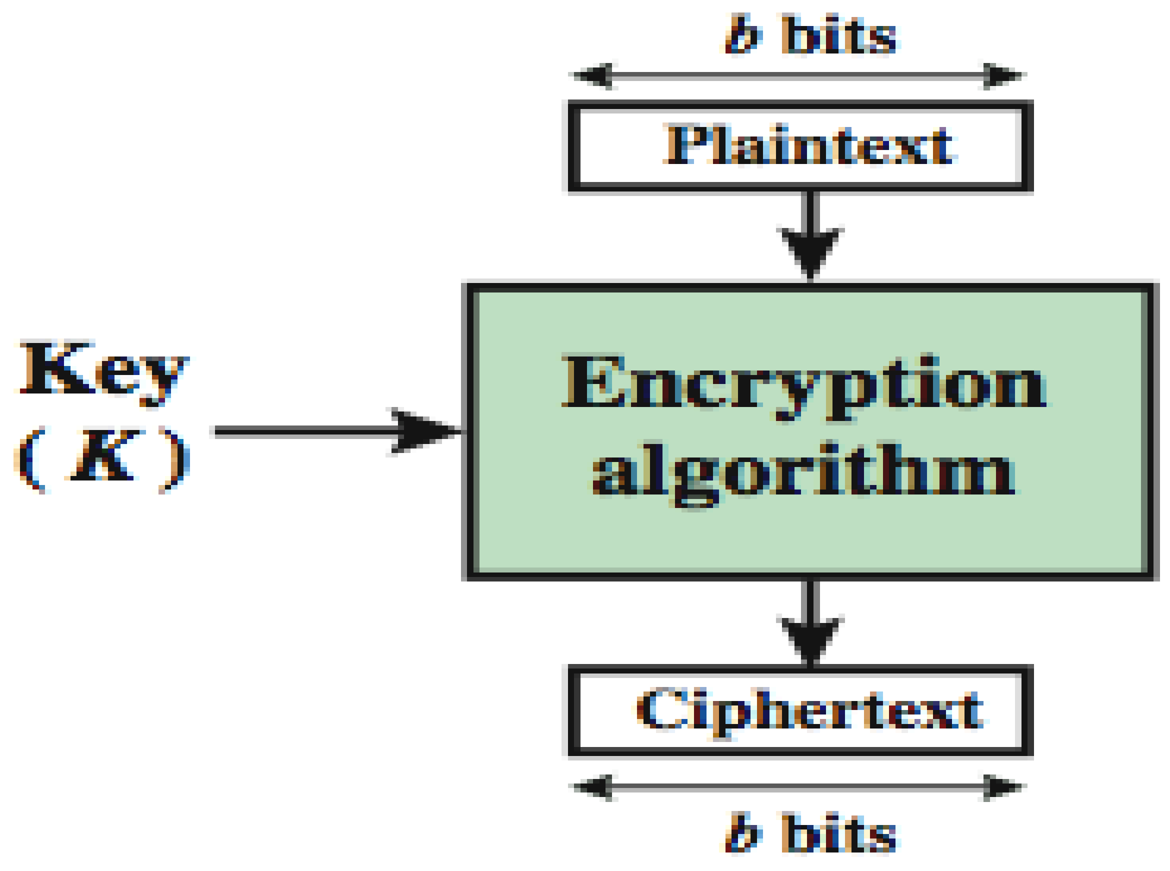


Symmetric key ciphers and Applications

Process of Symmetric key ciphers



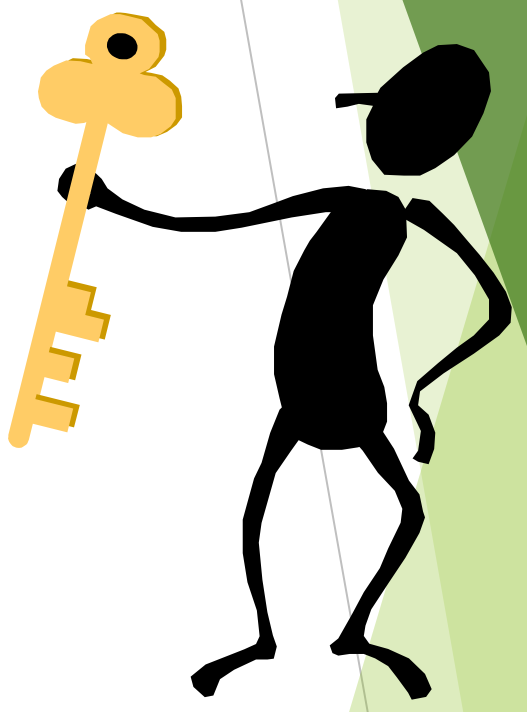
(a) Stream Cipher Using Algorithmic Bit Stream Generator



(b) Block Cipher

Wireless communication- GSM

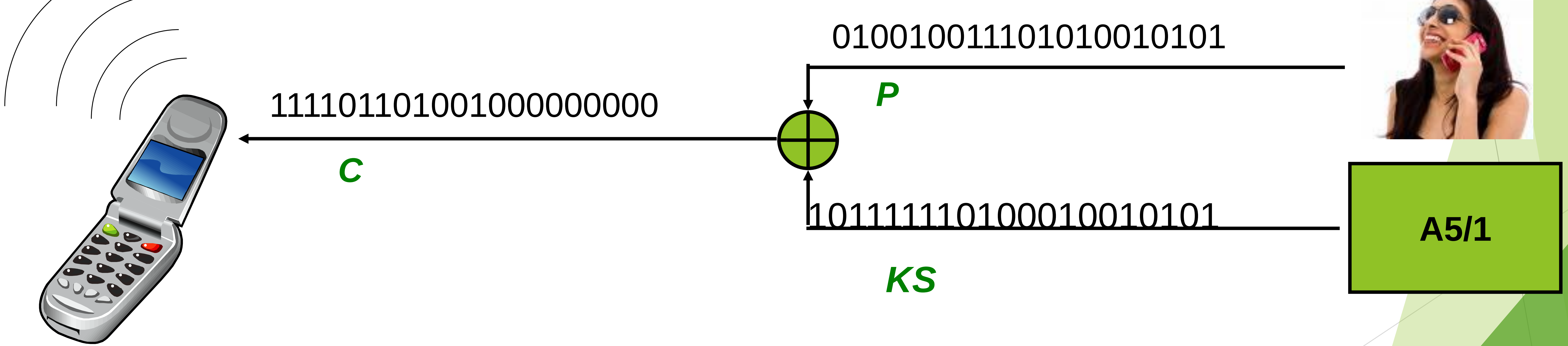
- Mutual Authentication with Replay Protection
- Protection of signalling data
  - Secure negotiation of protection algorithms
  - Integrity protection and origin authentication
  - Confidentiality
- Protection of user data payload
  - Confidentiality
- “Open” algorithms (block-ciphers) basis for security
  - AES for authentication and key agreement
  - Kasumi for confidentiality/integrity
- Security level (key sizes): 128 bits
- Protection further into the network



A5/1 Cipher

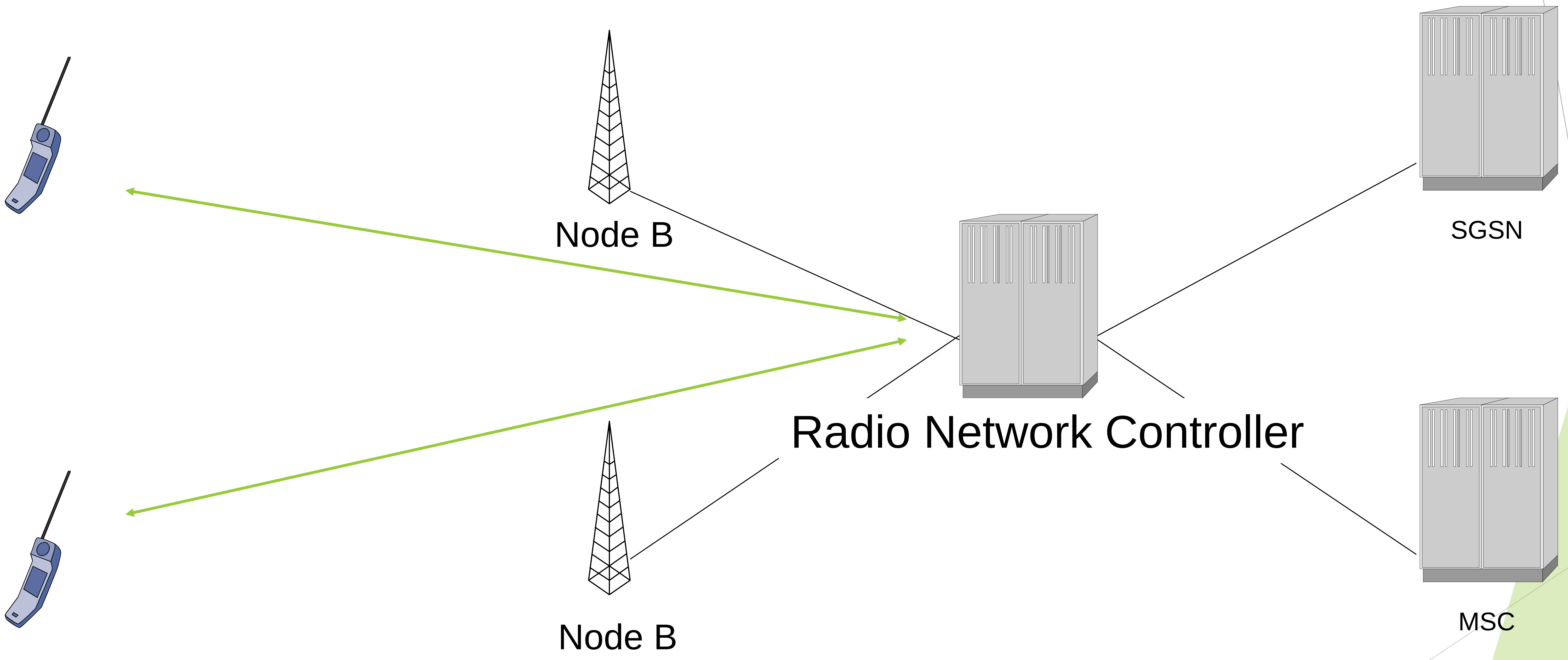
- Encrypts GSM communication
  - GSM communication organized in frames
  - 1 frame = 114 bits in each direction
- Stream cipher
  - produces the keystream ***KS*** being xored with the plaintext ***P*** to form ciphertext ***C***

$C = P \oplus KS$



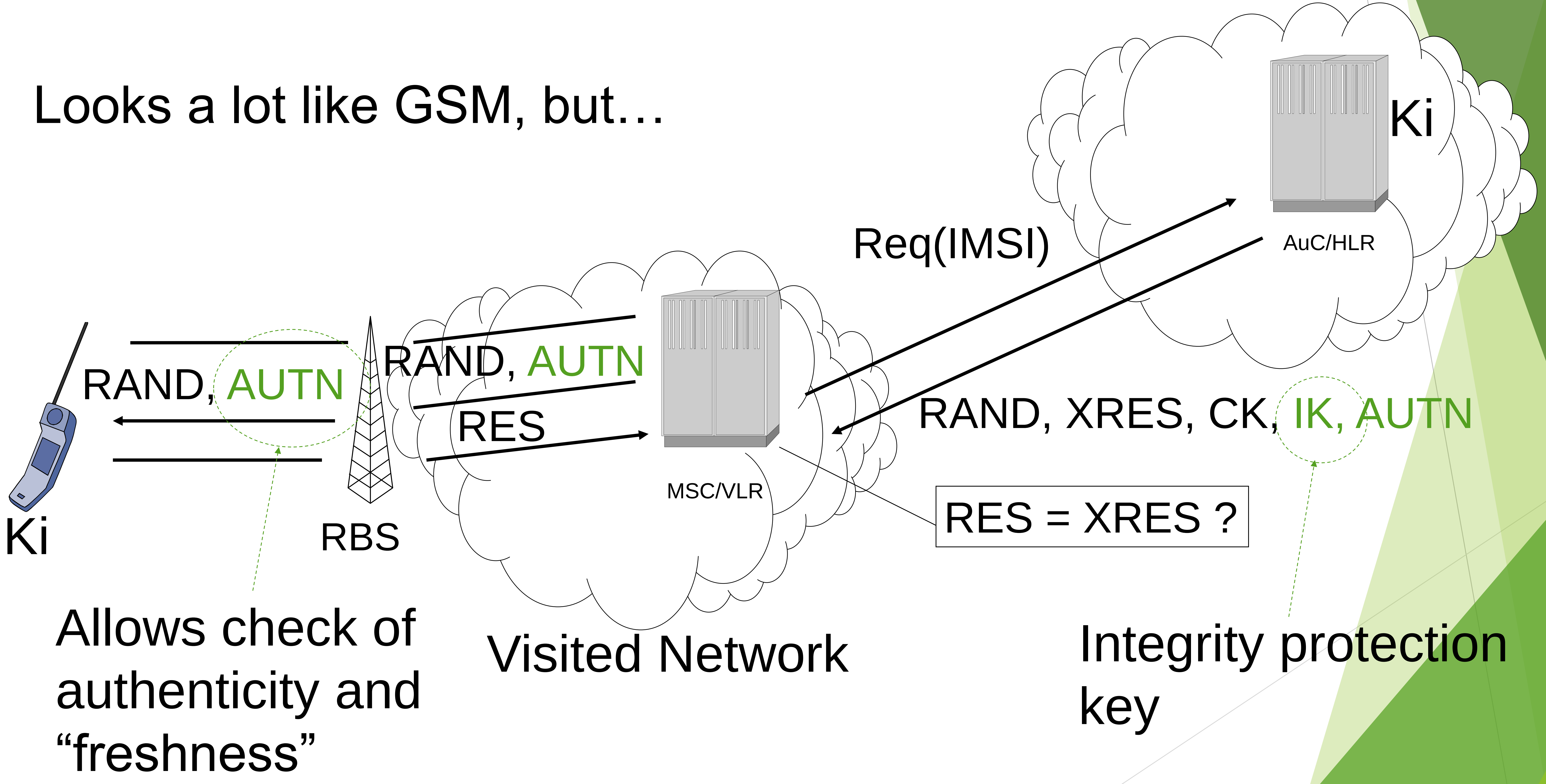
UMTS – Security

Integrity & Confidentiality
UIA & UEA algorithms (based on KASUMI)

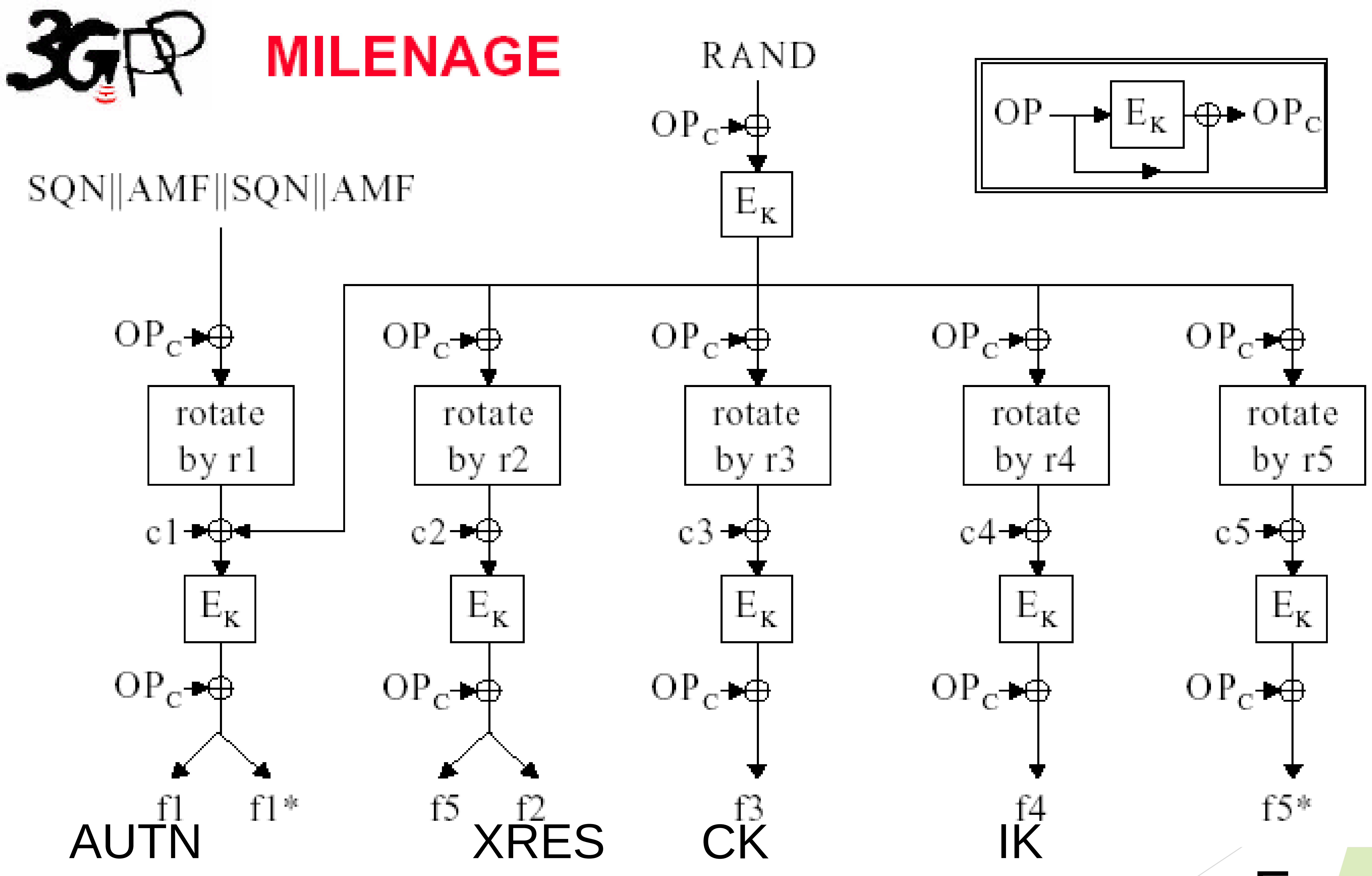


UMTS – Authentication and Key Agreement *AKA*

Looks a lot like GSM, but…



UMTS AKA Algorithms



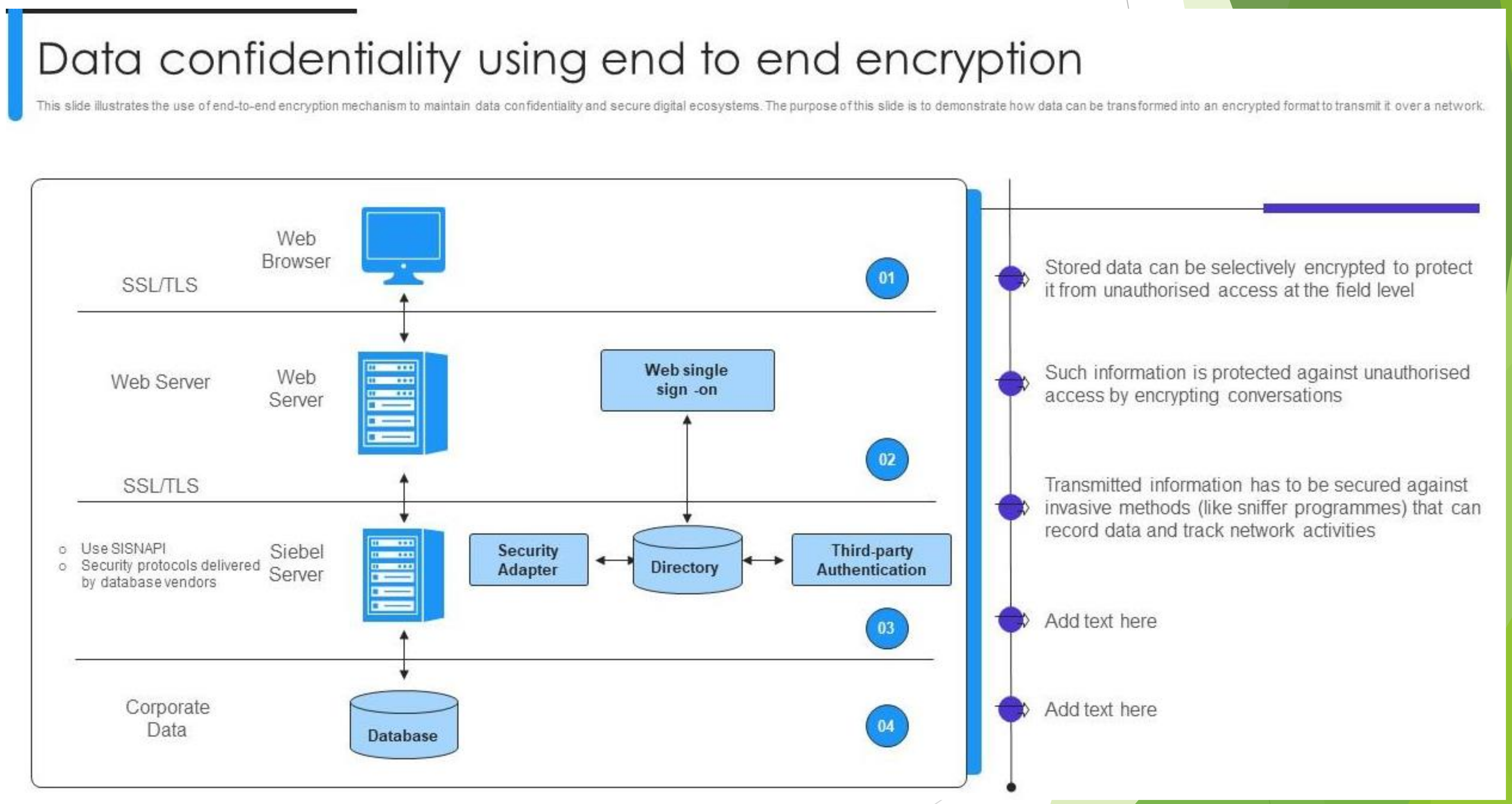
E_k = AES

Comparison of Security Mechanisms

	GSM		GPRS		WCDMA
Confidentiality					
- Algorithm	A5/1 & A5/2	A5/3	GEA1 & GEA2	GEA3	UEA (f8)
- Key length	64 (54)	64 (128)	64 (40)	64 (128)	128
- Public review	No	"Yes"	No	No	Yes
- Signalling	Yes	Yes	Yes	Yes	Yes
- User data	Yes	Yes	Yes	Yes	Yes
- Deployed	Yes	No	Yes	No	ongoing
Integrity					
- Algorithm	-	-	-	-	UIA (f9)
- Key length	-	-	-	-	128
- Tag length					32
- Public review	-	-	-	-	Yes
- Signalling	-	-	-	-	Yes
- User data	-	-	-	-	No
- Deployed	-	-	-	-	ongoing

Secure Sockets Layer Transport Layer Security

- Transport Layer Security defined in RFC 2246
- SSL general-purpose service
  - Set of protocols that rely on TCP
- Two implementation options
  - Part of underlying protocol suite
    - Transparent to applications
  - Embedded in specific packages
    - E.g. Netscape and Microsoft Explorer and most Web servers
- Minor differences between SSLv3 and TLS



SSL Architecture

- SSL uses TCP to provide reliable end-to-end secure service
- SSL two layers of protocols
- Record Protocol provides basic security services to various higher-layer protocols
  - In particular, HTTP can operate on top of SSL
- Three higher-layer protocols
  - Handshake Protocol
  - Change Cipher Spec Protocol
  - Alert Protocol
  - Used in management of SSL exchanges (see later)

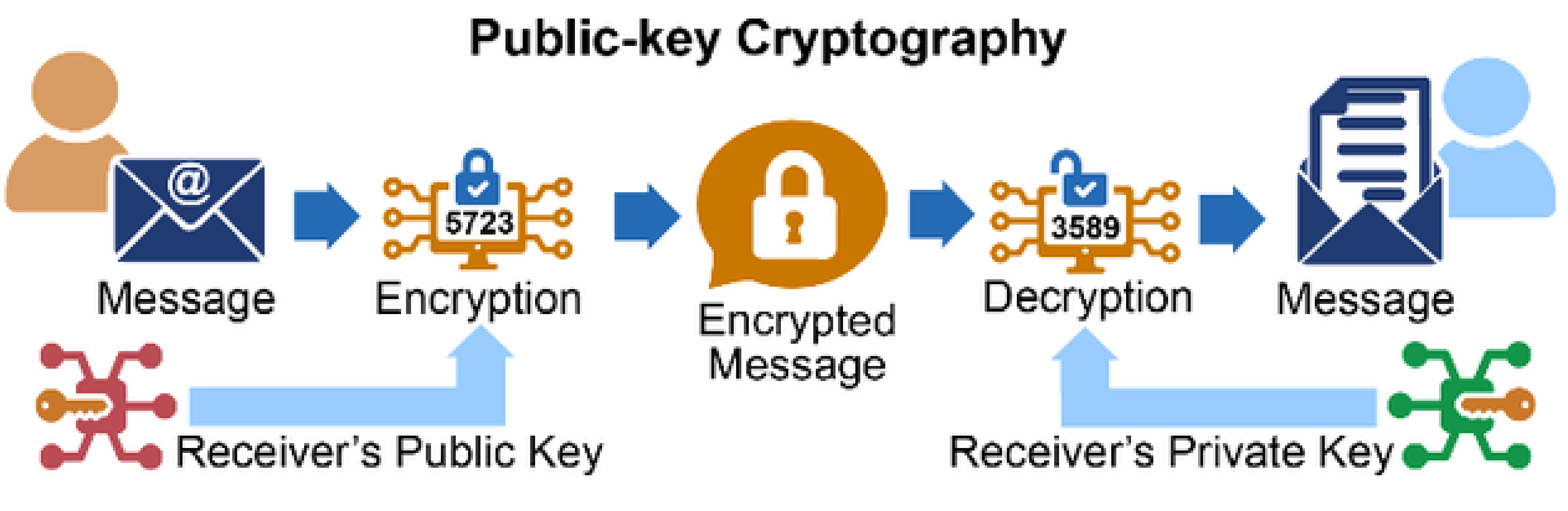
Protocols for Secure Communications

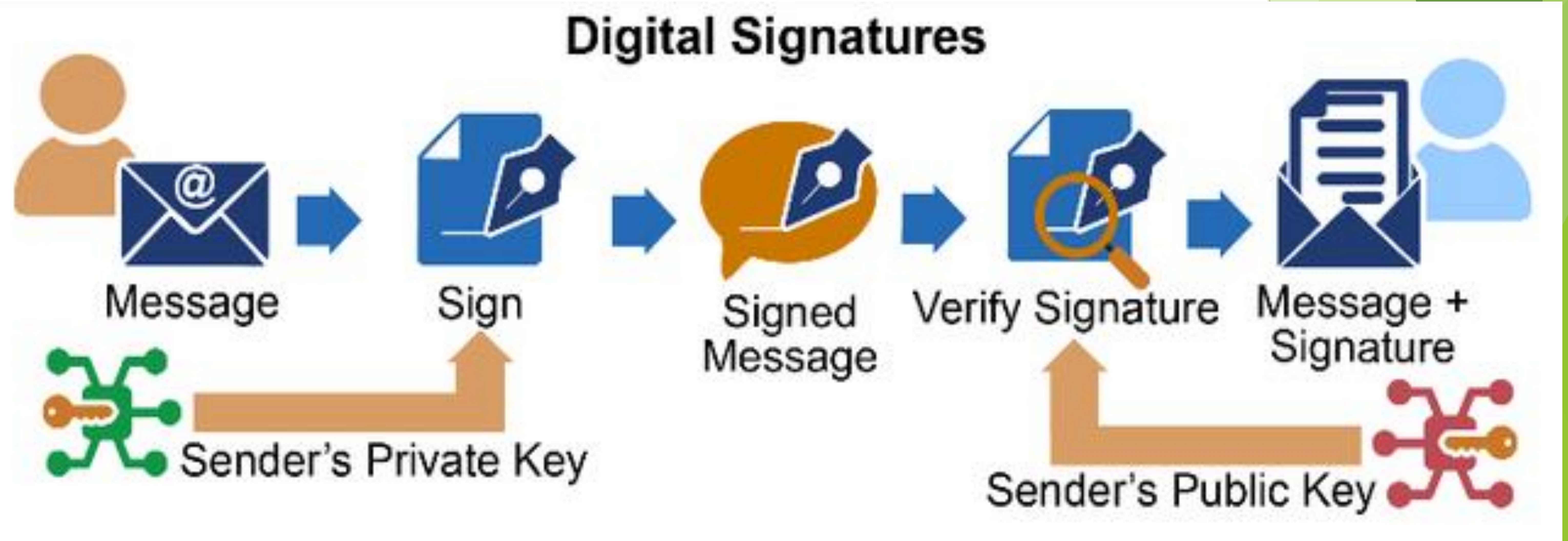
- Securing TCP/IP with IPSec
  - Internet Protocol Security (IPSec): open-source protocol to secure communications across any IP-based network
  - IPSec designed to protect data integrity, user confidentiality, and authenticity at IP packet level

- IPSec combines several different cryptosystems: Diffie-Hellman; public key cryptography; bulk encryption algorithms; digital certificates, AES, 3-DES.

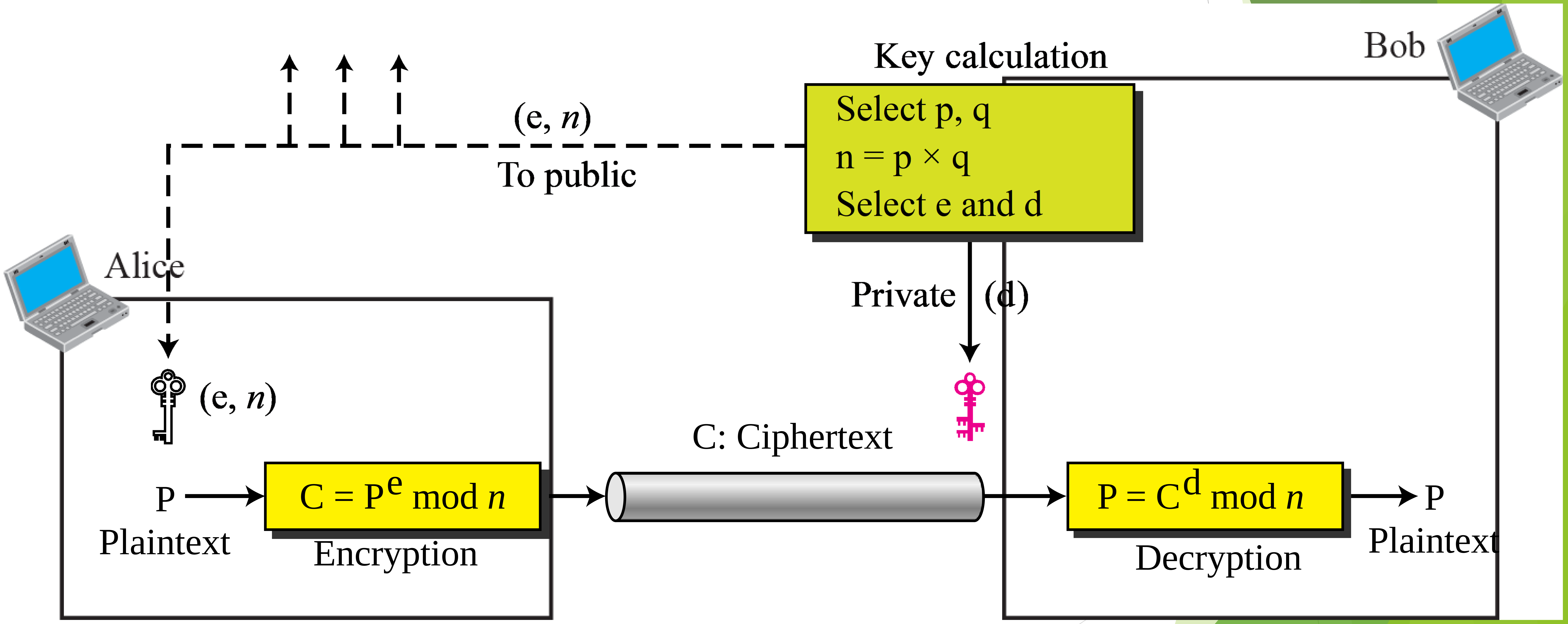
Public key Cryptography

Public Key Cryptography





Public Key Cryptography



RSA Key pair

(including Algorithm identifier)

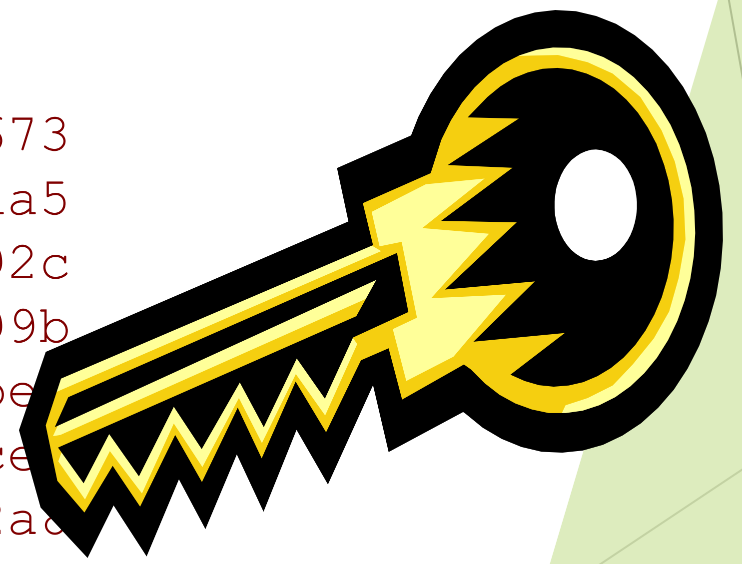
[2048 bit]

Private Key

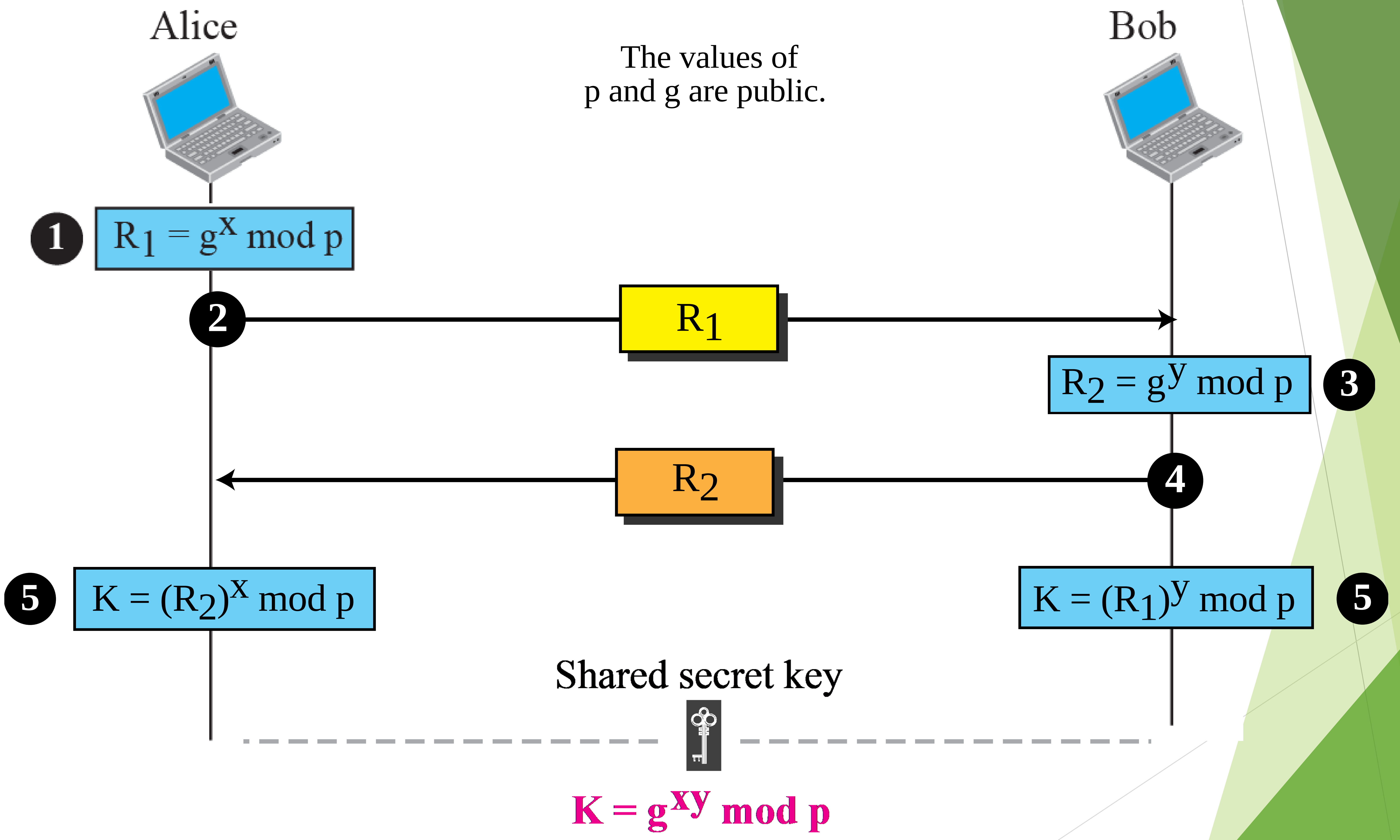
3082 010a 0282 0101 00b1 d311 e079 5543 0708 4ccb 0542 00e2 0d83 463d e493 bab6 06d3
0d59 bd3e c1ce 4367 018a 21a8 efbc ccd0 a2cc b055 9653 8466 0500 da44 4980 d854 0aa5
2586 94ed 6356 ff70 6ca3 a119 d278 be68 2a44 5e2f cfcc 185e 47bc 3ab1 463d 1ef0 b92c
345f 8c7c 4c08 299d 4055 eb3c 7d83 deb5 f0f7 8a83 0ea1 4cb4 3aa5 b35f 5a22 97ec 199b
c105 68fd e6b7 a991 942c e478 4824 1a25 193a eb95 9c39 0a8a cf42 b2f0 1cd5 5ffb 6bed
6856 7b39 2c72 38b0 ee93 a9d3 7b77 3ceb 7103 a938 4a16 6c89 2aca da33 1379 c255 8ced
9cbb f2cb 5b10 f82e 6135 c629 4c2a d02a 63d1 6559 b4f8 cdf9 f400 84b6 5742 859d 32a8
f92a 54fb ff78 41bc bd71 28f4 bb90 bcff 9634 04e3 459e a146 2840 8102 0301 0001

Public Key

3082 01e4 f267 0142 0f61 dd12 e089 5547 0f08 4ccb 0542 00e2 0d83 463d e493 bab6 0673
0d59 bf3e c1ce 4367 012a 11a8 efbc ccd0 a2cc b055 9653 8466 0500 da44 4980 d8b4 0aa5
2586 94ed 6356 ff70 6ca3 a119 d278 be68 2a44 5e2f cfcc 185e 47bc 3ab1 463d 1df0 b92c
345f 8c7c 4c08 299d 4055 eb3c 7d83 deb5 f0f7 8a83 0ea1 4cb4 3aa5 b35f 5a22 97ec 199b
c105 68fd e6b7 a991 942c e478 4824 1a25 193a eb95 9c39 0a8a cf42 b250 1cd5 5ffb 6be
6856 7b39 2c72 38b0 ee93 a9d3 7b77 3ceb 7103 a938 4a16 6c89 2aca da33 1379 c255 8ce
9cbb f2cb 5b10 f82e 6135 c629 4c2a d02a 63d1 6559 b4f8 cdf9 f400 84b6 5742 859d 32a
f92a 54fb ff78 41bc bd71 28f4 bb90 bcff 9634 04de 45de af46 2240 8410 02f1 0001



Key Exchange: Diffie-Helman



ENCRYPTION

Message 1

Central to the growth of e-commerce and e-governance is the issue of trust in electronic environment.

Encrypted Message 1

9a468 4335be49f0b9cab28d755aaa9cd9857 1b275bbb 405e6931e856ca3e5e569edd 135285482

Same Key

SYMMETRIC

Message 2

The Internet knows no ge has redefined time and space. Advances in computer and telecommunication technologies have led to the explosive growth of the Internet. This in turn is affecting the methods of communication, work, study, education, interaction, leisure, health, governance, trade and commerce.

Encrypted Message 2

a5 cb61a770f947ca856cd675463f1c95a 9a2 71f80830c87f5715f5f5933497 d7e97 39868 7

Different Keys

[Keys of a pair – Public and Private]

ASYMMETRIC

[PKI]

DECRYPTION

Encrypted Message 1

9a46894335be49f0b9cab28d755aaa9cd98571b2 75bbb0adb405e6931e856ca3e5e569edd1352854 82

Message 1

Central to the growth of e-commerce and e-governance is the issue of trust in electronic environment.

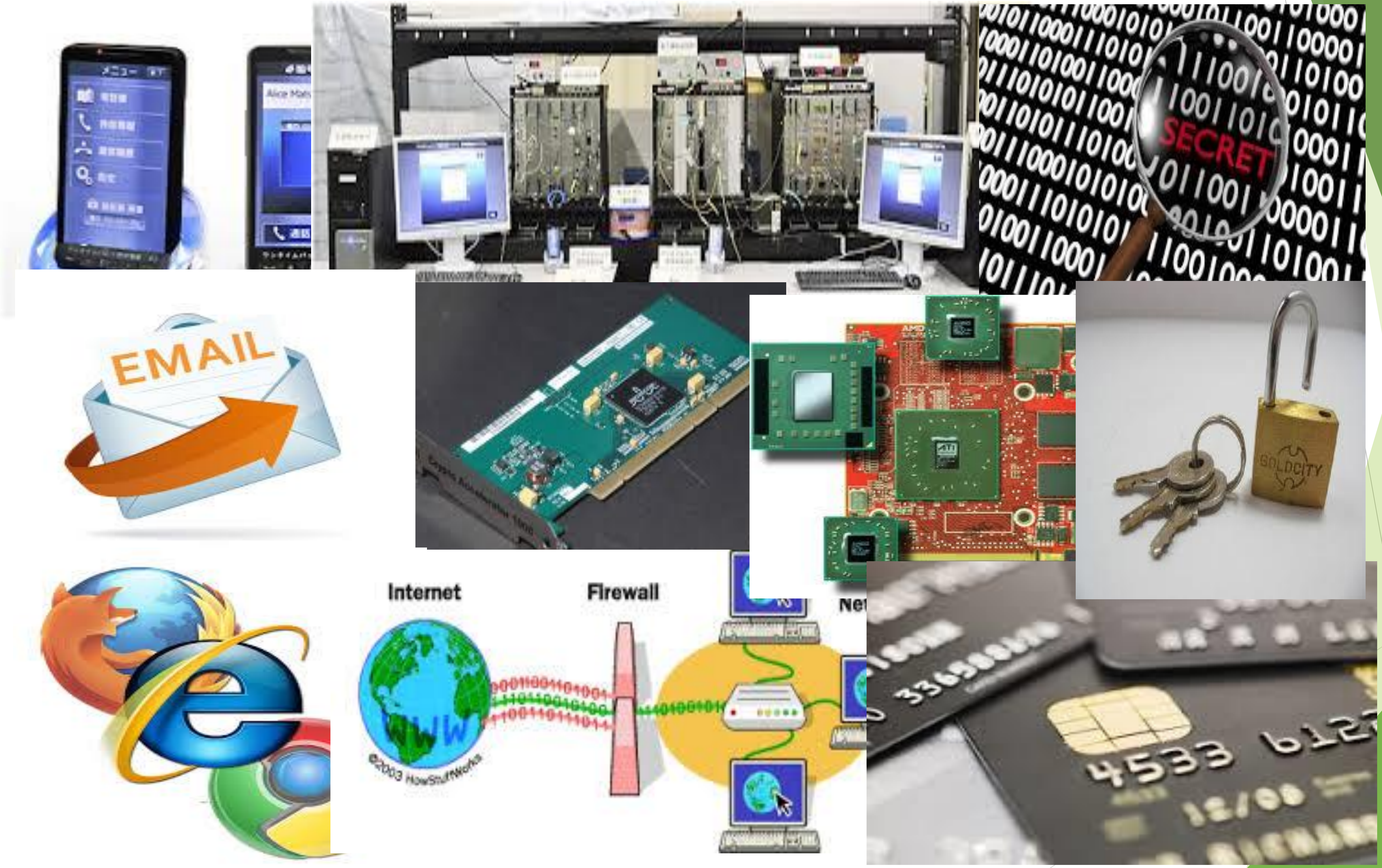
Encrypted Message 2

a520eecb61a770f947ca856cd675463f1c95a9a2b8 d4e6a71f80830c87f5715f5f59334978dd7e97da07 07b48a1138d77ced56feba2b467c398683c7dbeb8 6b854f120606a7ae1ed934f5703672adab0d7be66 dccde1a763c736cb9001d0731d541106f50bb7e54 240c40ba780b7a553bea570b99c9ab3df13d75f8cc fdddeaaf3a749fd1411

Message 2

The Internet knows no geographical boundaries. It has redefined time and space. Advances in computer and telecommunication technologies have led to the explosive growth of the Internet. This in turn is affecting the methods of communication, work, study, education, interaction, leisure, health, governance, trade and commerce.

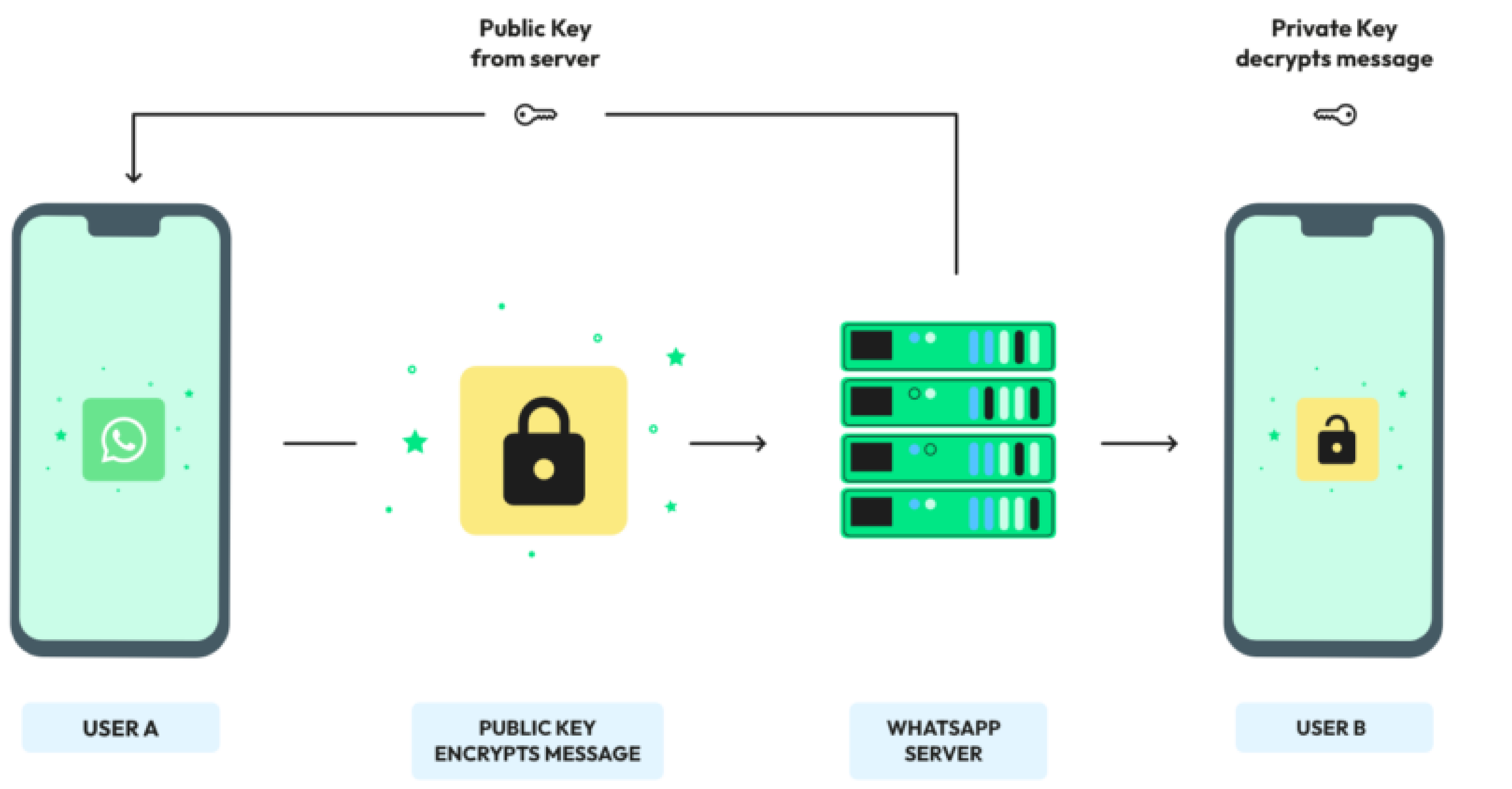
Crypto in Real World



WhatsApp Security

- **Encryption Standard:** WhatsApp uses **Signal Protocol**, a cryptographic protocol developed by Open Systems Whispers.

- Signal Protocol is based on well-established cryptographic primitives and is widely regarded as one of the most secure messaging protocols available.



How WhatsApp encryptions works

Elliptic Curve Diffie-Hellman (ECDH):

•**ECDH** is used for **key exchange**.

AES (Advanced Encryption Standard):

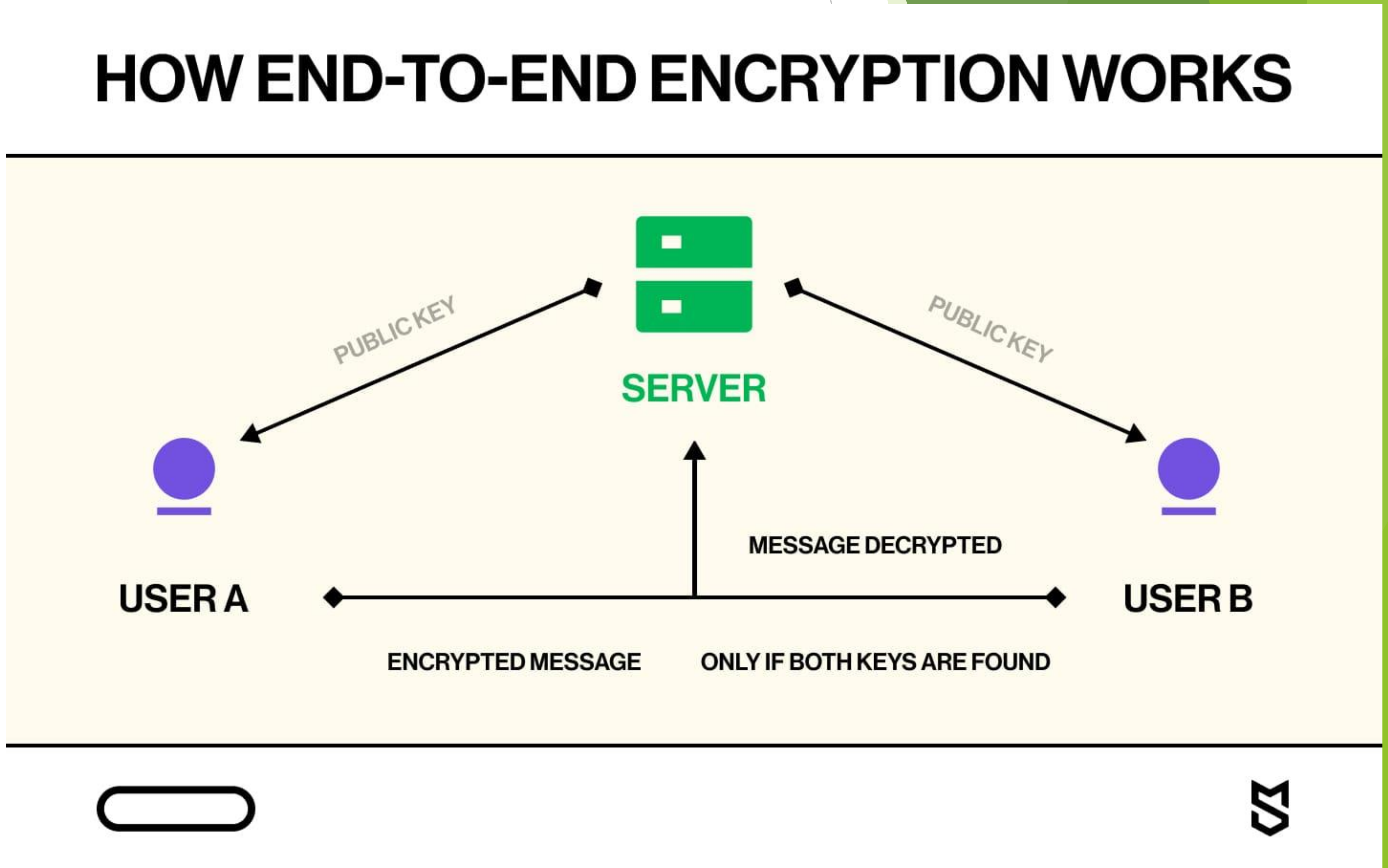
•WhatsApp uses **AES-256** in **Galois/Counter Mode (GCM)** for **symmetric encryption** of the message content.

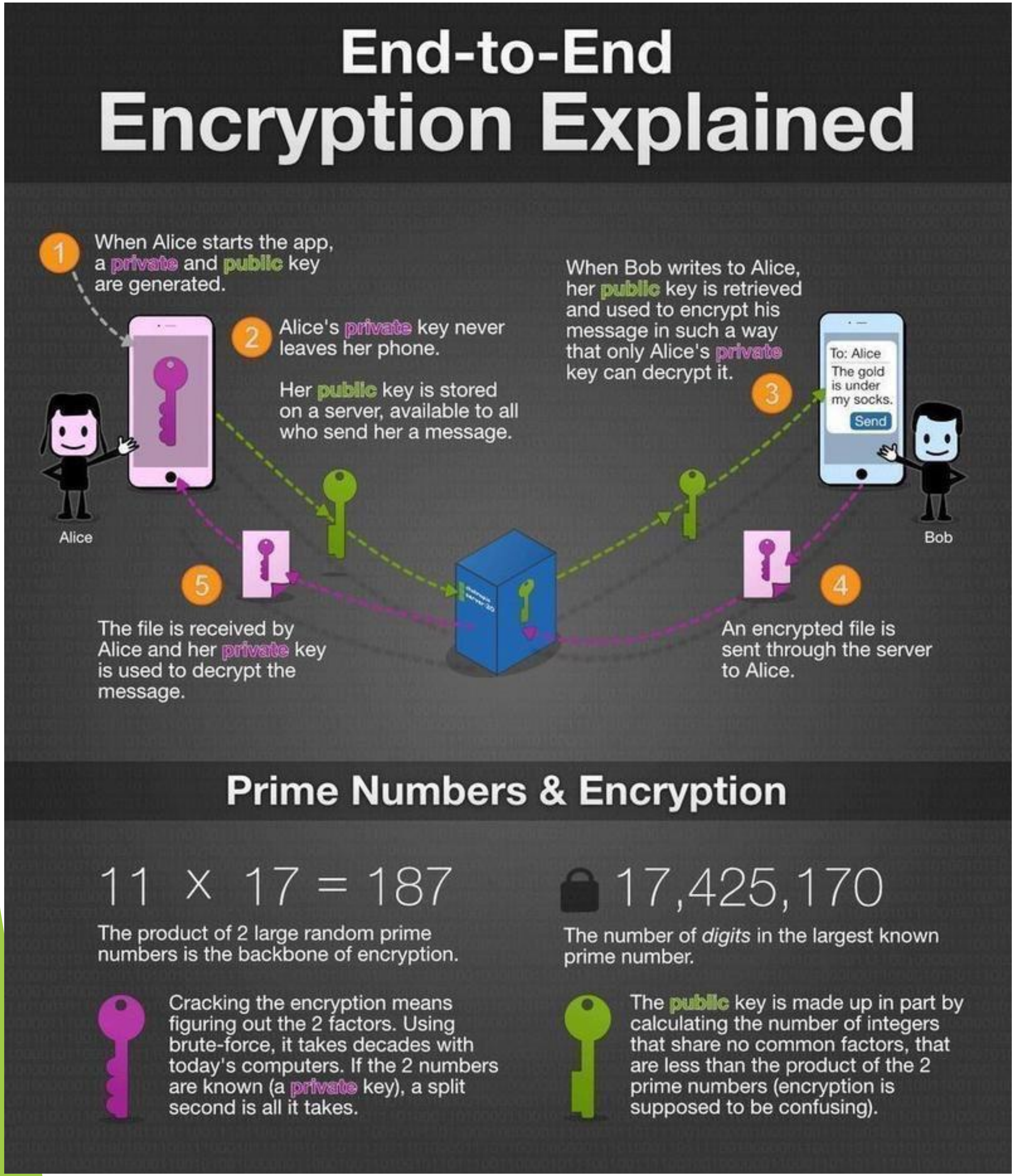
HMAC (Hash-Based Message Authentication Code):

•**HMAC-SHA256** is used for **message integrity and authenticity**. It ensures that messages have not been tampered with during transmission.

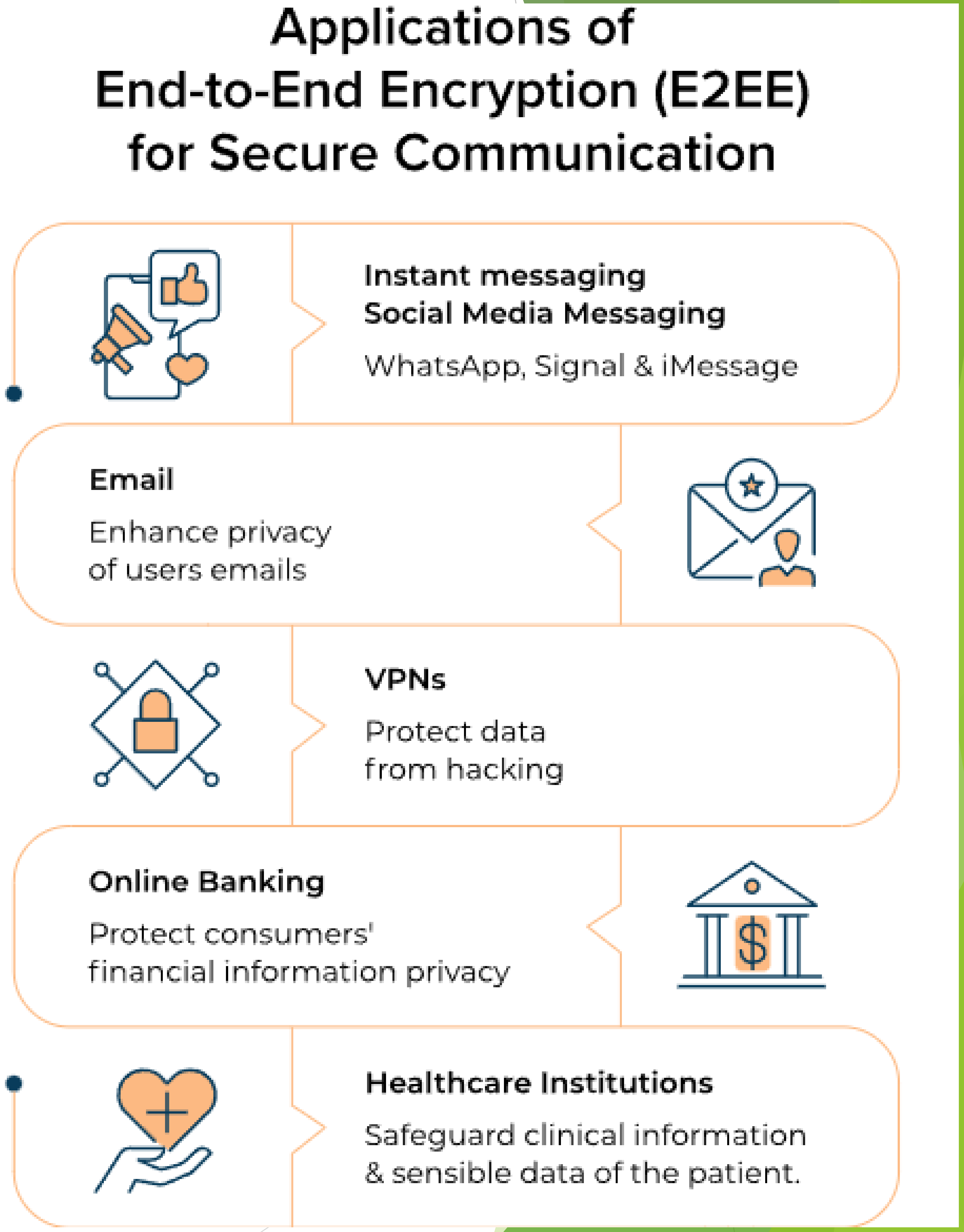
EdDSA (Edwards-Curve Digital Signature Algorithm):

•**EdDSA** is used to sign messages and verify the authenticity of public keys.





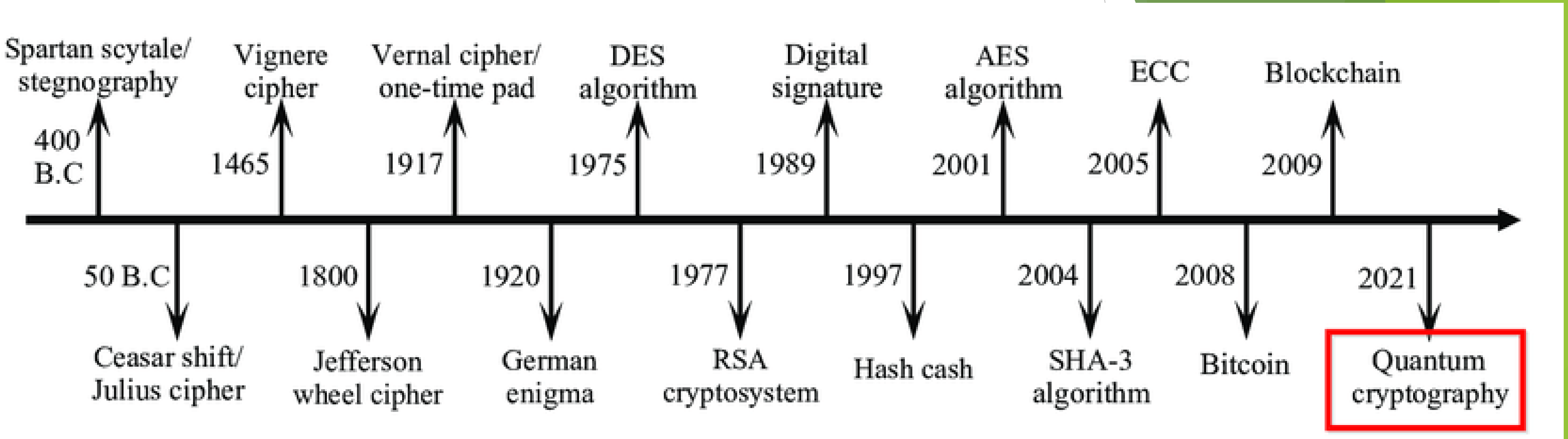
End-to-End
Encryption Explained
1
When Alice starts the app, a private and public key are generated.
2
Alice's private key never leaves her phone.
Her public key is stored on a server, available to all who send her a message.
When Bob writes to Alice, her public key is retrieved and used to encrypt his message in such a way that only Alice's private key can decrypt it.
3
To: Alice
The gold is under my socks.
Send
Alice
Bob
5
4
The file is received by Alice and her private key is used to decrypt the message.
An encrypted file is sent through the server to Alice.
Prime Numbers & Encryption
11 X 17 = 187
The product of 2 large random prime numbers is the backbone of encryption.
17,425,170
The number of digits in the largest known prime number.
Cracking the encryption means figuring out the 2 factors. Using brute-force, it takes decades with today's computers. If the 2 numbers are known (a private key), a split second is all it takes.
The public key is made up in part by calculating the number of integers that share no common factors, that are less than the product of the 2 prime numbers (encryption is supposed to be confusing).



Applications of
End-to-End Encryption (E2EE)
for Secure Communication
Instant messaging
Social Media Messaging
WhatsApp, Signal & iMessage
Email
Enhance privacy of users emails
VPNs
Protect data from hacking
Online Banking
Protect consumers' financial information privacy
Healthcare Institutions
Safeguard clinical information & sensible data of the patient.

Cryptography : History - Timelines

Fig: Milestones



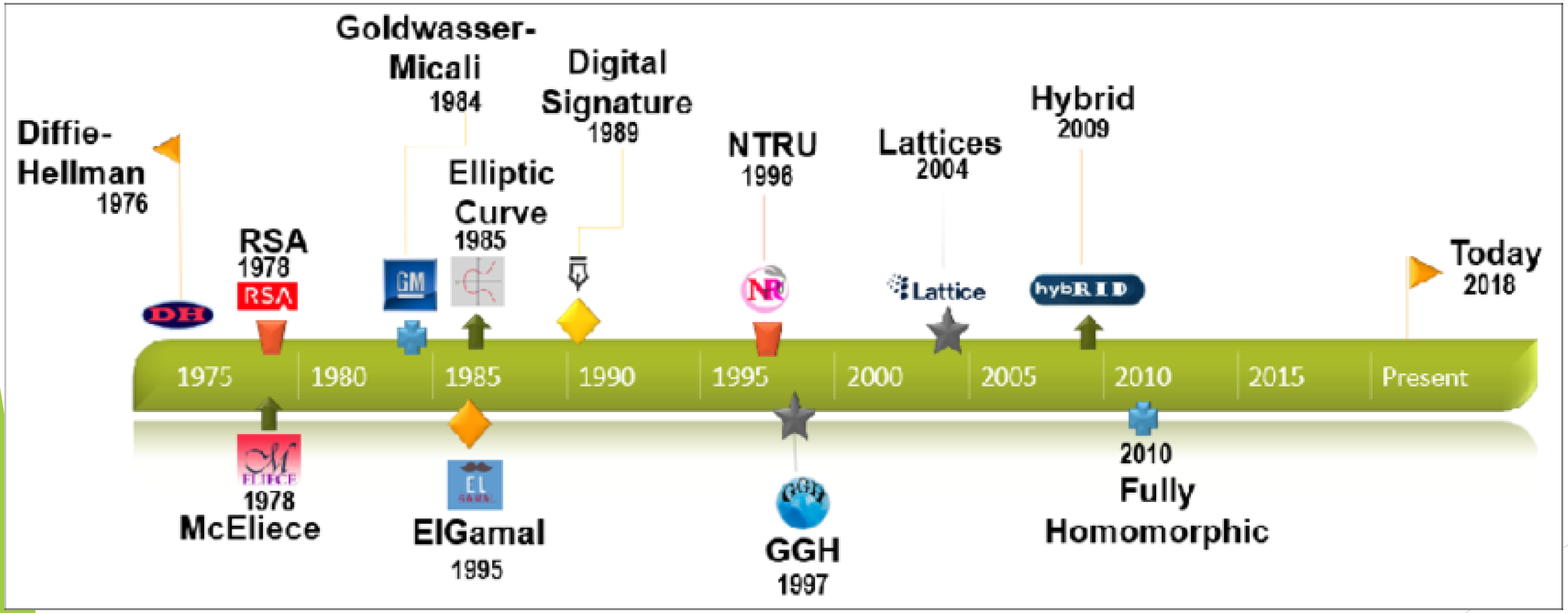


Fig : PKC

Quantum and Post Quantum

Quantum computer threat

- Quantum computing is an area of computer science that leverages the principles of quantum mechanics to perform computations that would be infeasible for classical computers.

- **Key Concept**: Unlike classical computers, which use binary bits (0 or 1), quantum computers use quantum bits or **qubits.**

Classical vs. Quantum Computing

- Classical Computing:
  - Uses bits (0 or 1).
  - Works with deterministic algorithms.
  - Performs computations sequentially.

- **Quantum Computing:**
  - Uses qubits (superposition of states).
  - Leverages quantum algorithms (e.g., Shor's, Grover’s).
  - Can perform parallel computations using quantum states.

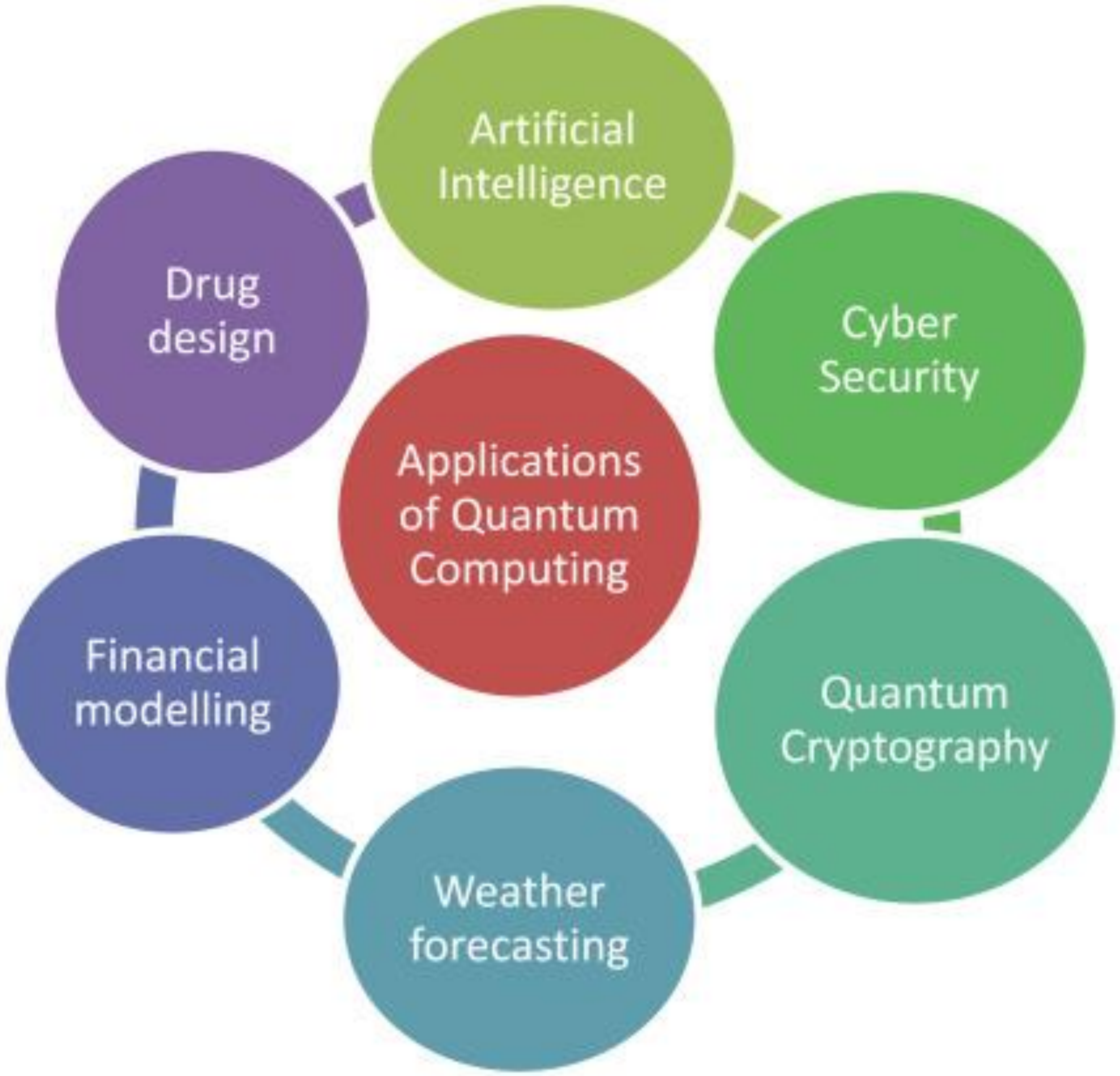
Applications of Quantum Computing

- **Cryptography:** Breaking traditional encryption schemes (e.g., RSA) and developing quantum-resistant algorithms.

- **Optimization Problems:** Solving complex optimization problems in logistics, finance, and manufacturing.

- **Simulating Quantum Systems:** Modeling molecules and materials for chemistry and physics.

- **Artificial Intelligence:** Enhancing machine learning algorithms through quantum speedup.



Quantum computer threat

- Present asymmetric cryptosystems are mostly based on two hard problems:
  - The discrete logarithm problem
  - The integer factorization problem
- Classical attacks are atleast sub-sequential.
- The Shor's quantum algorithm (Shor, 1997) proposes a theoretical attack which is of polynomial time.
- Threat by Emergence of quantum computers.

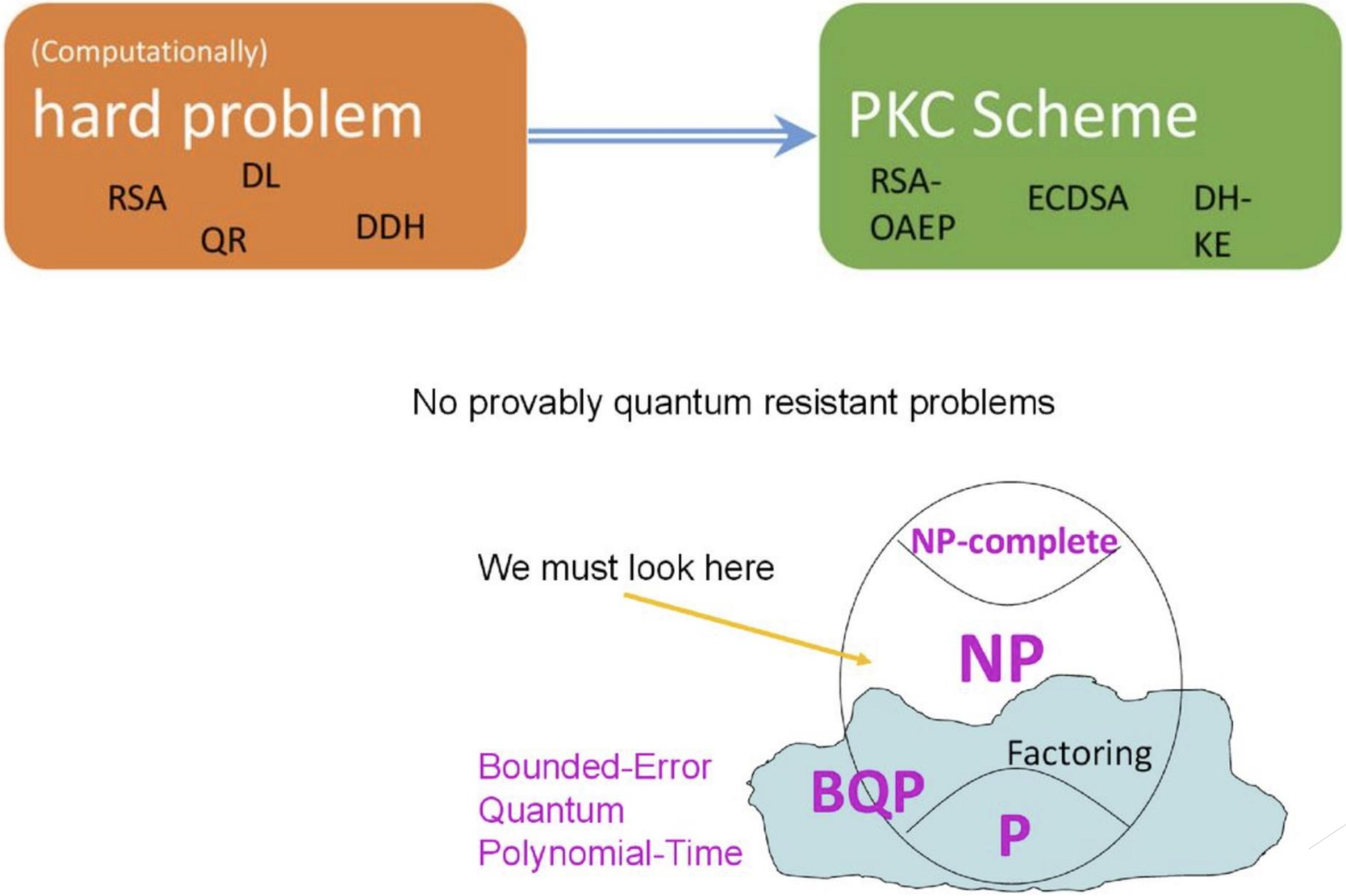
In Q2B-2020, Zapata computing.

Quantum computer threat

n-bit target		Classical	Quantum
Factorization		$\exp(n^{1/3} \log^{2/3} n)^{1.923}$	n^3
DLP	Finite field	$\exp(n^{1/3} \log^{2/3} n)^{1.923}$	n^3
	Elliptic curve	$2^{n/2}$	
Unstructured search		2^n	$2^{n/2}$

While the quantum Grover's algorithm does speed up attacks against symmetric ciphers, doubling the key size can effectively block these attacks

How to build PKC



Credits: Buchmann, Bindel 2015

- The threat today

"Post-quantum cryptography" (classical crypto, quantum-secure)

What must be done?

1. Identify assumptions that are not quantum-broken (e.g., lattice-based crypto, not RSA)
2. Build cryptosystems based on those
3. Prove security

Needs quantum know-how/ techniques

Possible without "quantum literacy"?

Quantum Cryptography

Definition:

- Use of quantum mechanics principles to perform cryptographic tasks.

Key Principles:

- Quantum key distribution (QKD)
- Quantum entanglement

Advantages:

- Unbreakable encryption
- Detection of eavesdropping

Quantum Protocols

Use quantum communication to make impossible tasks feasible

- Best known example:
  Unconditionally secure key distribution

- Possible today!

(No quantum computer needed.)

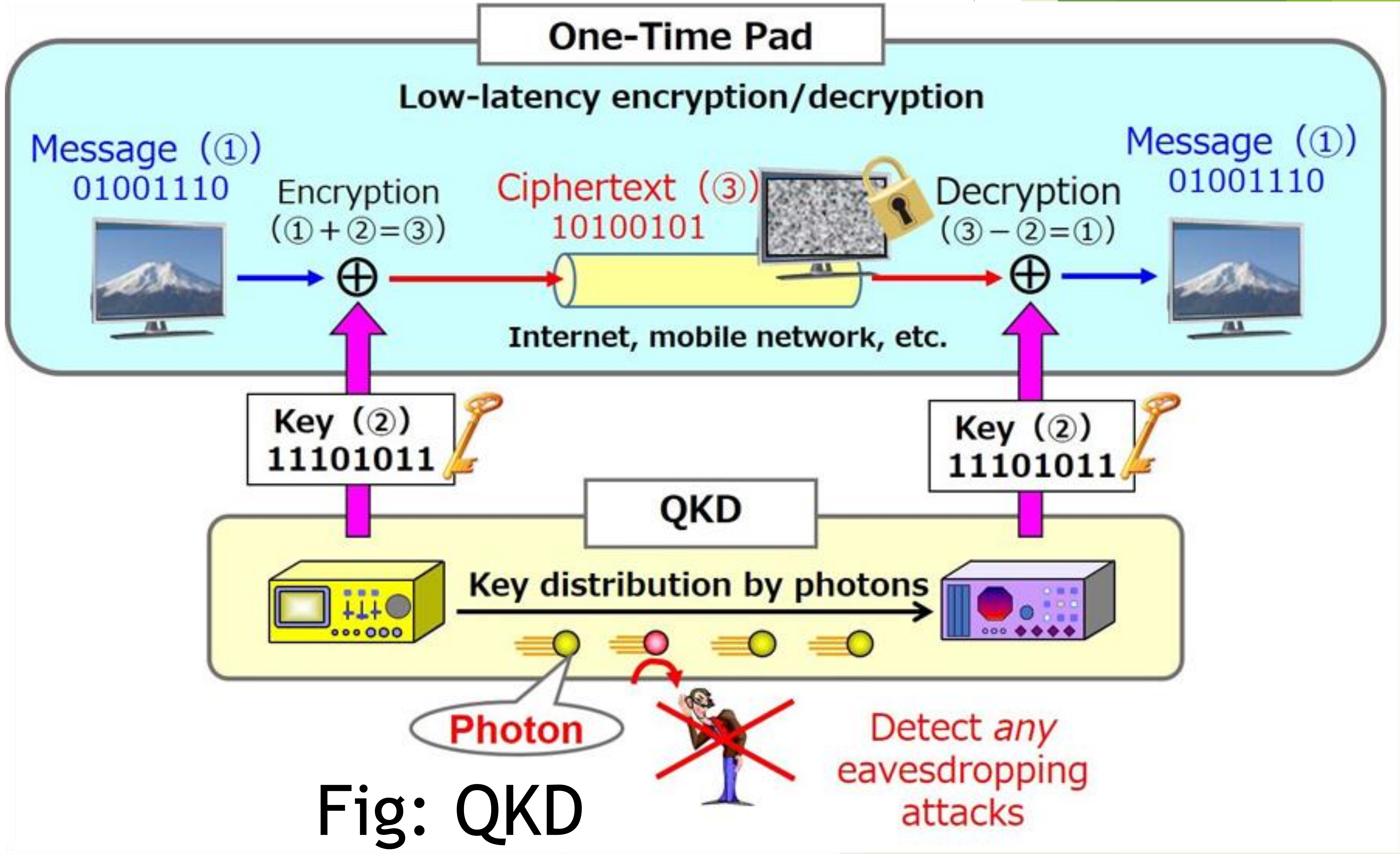


Fig: QKD

Random Number Generators

- Randomness phenomenon is important for variety of information processing applications.
- The types of random number generators (RNGs) can be divided in relation to e.g., the type of the generation process:

(i) Software RNGs (based on the deterministic software)

(ii) Hardware RNGs (based on the physical phenomenon i.e., classical or Quantum).

Random Number Generators

- PRNGs is a software-based algorithm which generates random numbers from deterministic source seed.
- TRNGs uses hardware-based inputs to create random values. The inputs are generally physical processes like thermal noise or atmospheric noise.
- QRNGs are devices that use quantum mechanical effects to produce the highest level of randomness possible.

- Statistical tests offer a common approach to randomness testing. Widely used test suites like NIST, Diehard, testU01.

- Mersenne Twister algorithm, Bell-Test (like inequalities) can serve as a device independent test for randomness.

QRNGs- Nature

	PRNG	TRNG
Efficiency	Very efficient	Generally efficient
Determinism	Deterministic	Non deterministic
Periodicity	Periodic	Non periodic

Classical RNGs	Quantum RNGs
Software based PRNG that use algorithms are limited by the original seed numbers	Not limited by any seed numbers
Physical RNGs achieve either high entropy or high throughput, never both	Achieve both high entropy and high throughput
Vulnerable to quantum computers	Impregnable to quantum computers

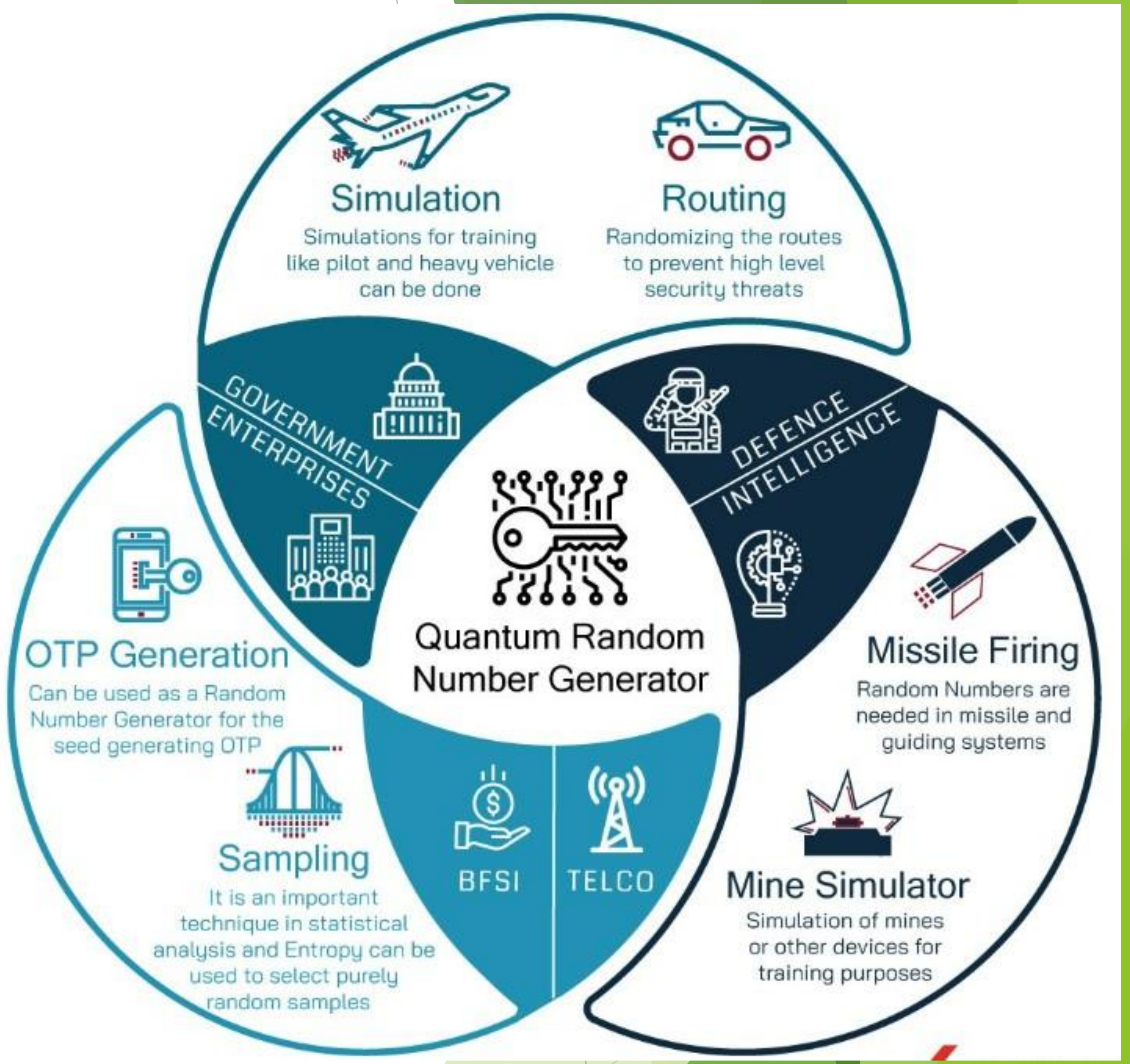


Fig: RNG: Applications

Post-Quantum Cryptography

Definition:

- Cryptographic algorithms that are secure against quantum computer attacks

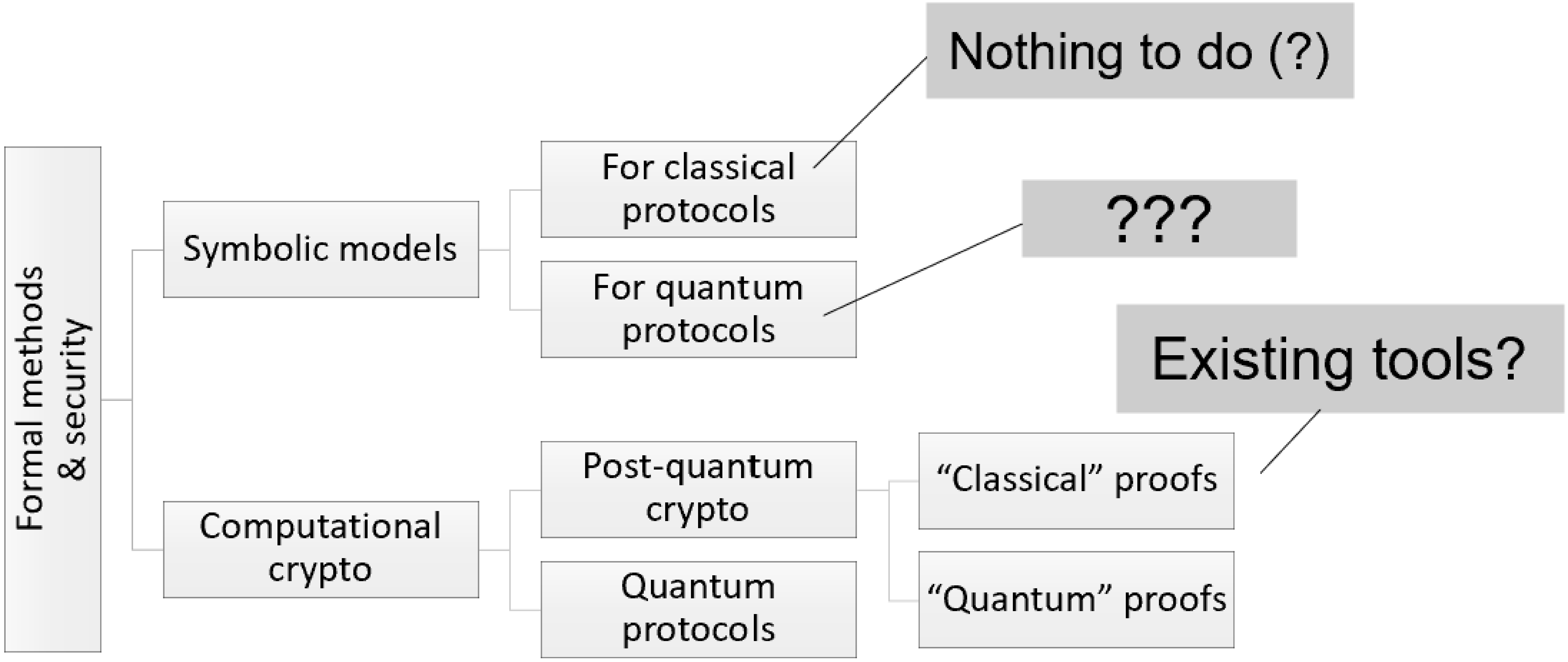
Key Principles:

- Based on mathematical problems that are hard for quantum computers to solve (e.g., lattice-based cryptography, hash-based cryptography).

Advantages:

- Compatibility with existing infrastructure
- No need for quantum hardware

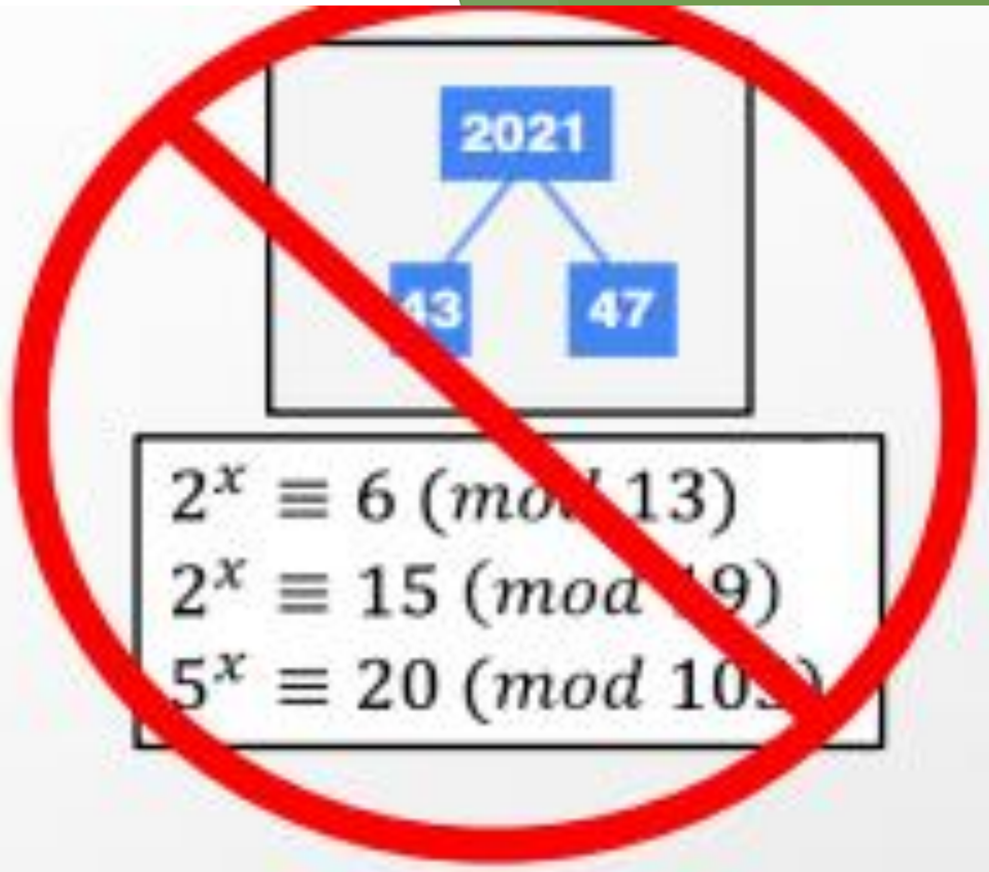
- Quantum Crypto & Verification

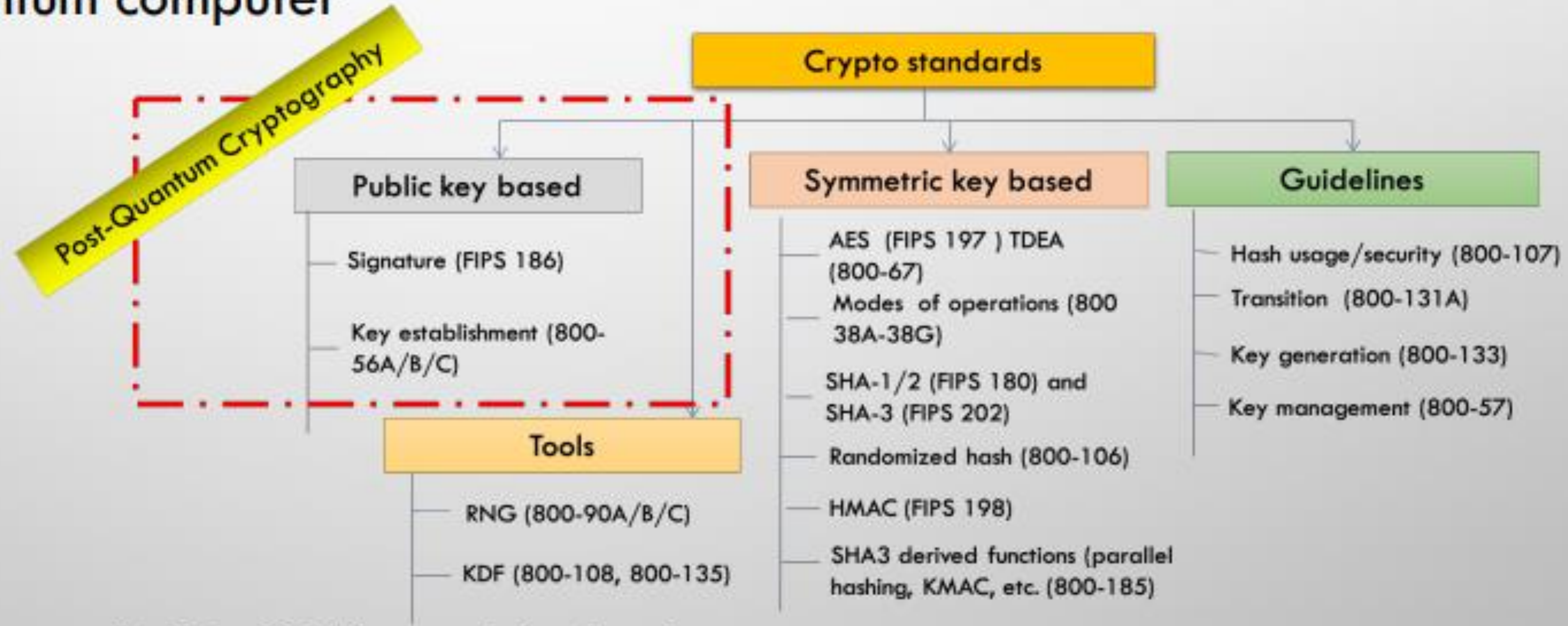


- NIST public-key crypto standards
  - **SP 800-56A**: Diffie-Hellman, ECDH
  - **SP 800-56B**: RSA encryption
  - **FIPS 186**: RSA, DSA, and ECDSA signatures

all vulnerable to attacks from

a (large-scale) quantum computer





- Symmetric-key crypto (AES, SHA) would also be affected, but less dramatically

Public-Key Crypto: Post-Quantum Scenario

- But, that's not the end of PKC. Fortunately, there are at least four types of public-key cryptosystems.
  - Code-based cryptography: McEliece encryption scheme, 1978
  - Hash-based cryptography: Merkle's hash-tree signature system, 1979
  - Lattice-based cryptography: NTRU encryption scheme, 1996
  - Multivariate-quadratic-equations: HFE signature scheme, 1996

- quantum resistance of popular symmetric cryptosystem, a big relief

NIST, 2022 Standards

NIST Competition & Standardization

NIST Competition

Post-Quantum Cryptography | CSRC (nist.gov)

- On 5th July 2022, NIST has completed the third round of the PQC standardization process, which selects public-key cryptographic algorithms to protect information through the advent of quantum computers.
- A total of four candidate algorithms have been selected for standardization, and four additional algorithms will continue into the fourth round.
  - Public-Key Encryption/KEMs: CRYSTALS-KYBER
  - Digital Signatures: CRYSTALS-Dilithium, FALCON, SPHINCS+

Short URL: https://www.nist.gov/pqcrypto

THE FIRST THREE ROUND

ROUND 1 (DEC '17 – JAN '18)

- 69 CANDIDATES AND 278 DISTINCT SUBMITTERS
- SUBMITTERS FROM >25 COUNTRIES, 6 CONTINENTS
- APR 2018, 1ST NIST PQC CONFERENCE
- ALMOST 25 SCHEMES BROKEN/ATTACKED
- NISTIR 8240, NIST REPORT ON THE 1 ST ROUND

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-v	[illegible]	[illegible]	[illegible]
Symme	[illegible]	[illegible]	[illegible]
Other	[illegible]	[illegible]	[illegible]
Total	[illegible]	[illegible]	[illegible]

ROUND 2 (JAN '18 – JUL '20)

- 26 CANDIDATES
- AUG 2019 – 2ND NIST PQC CONFERENCE
- 7 SCHEMES BROKEN/ATTACKED
- NISTIR 8309, NIST REPORT ON THE 2 ND ROUND

	Signatures	KEMs/Encryption	Total
Lattice-based	3	9	12
Code-based	0	7	7
Multi	[illegible]	[illegible]	[illegible]
Symm	[illegible]	[illegible]	[illegible]
Othe	[illegible]	[illegible]	[illegible]
Total	[illegible]	[illegible]	[illegible]

ROUND 3 (JUL '20 – JUL '22)

- 7 FINALISTS AND 8 ALTERNATES
- JUNE 2021 – 3RD NIST PQC CONFERENCE
- NISTIR 8413, NIST REPORT ON THE 3RD ROUND

	Signatures	KEMs/Encryption	Total
Lattice-based	2	5	7
Code-based	0	3	3
Multi-variate	2	0	2
Symmetric-based	2	0	2
Other	0	1	1
Total	6	9	15

THE FIRST THREE ROUND

Table 3: Third-Round Finalists

Public-Key Encryption/KEMs	Digital Signatures
Classic McEliece	CRYSTALS-DILITHIUM
CRYSTALS-KYBER	FALCON
NTRU	Rainbow
SABER	

Table 4: Alternate Candidates

Public-Key Encryption/KEMs	Digital Signatures
BIKE	GeMSS
FrodoKEM	Picnic
HQC	SPHINCS+
NTRU Prime	
SIKE	

ROUND-3 RESULTS

3rd round selection (KEM)	3rd round selection (Signatures)
CRYSTALS-Kyber	**CRYSTALS-Dilithium, Falcon, SPHINCS+**

See NISTIR 8413, *Status Report on the 3rd Round of the NIST PQC Standardization Process*, for the rationale on the selections

4th round candidates (all KEMs) evaluated for 18-24 months

- ClassicMcEliece
- BIKE
- HQC
- SIKE

On-ramp signatures

- NIST issued a new call for additional signatures – preferably for signatures based on non-lattice problems

THE KEMS IN THE 4th ROUND

- Classic McEliece
  - NIST is confident in the security
  - Smallest ciphertexts, but largest public keys
  - We'd like feedback on specific use cases for Classic McEliece
- BIKE
  - Most competitive performance of 4th round candidates
  - We encourage vetting of IND-CCA security
- HQC
  - Offers strong security assurances and mature decryption failure rate analysis
  - Larger public keys and ciphertext sizes than BIKE
- SIKE
  - The SIKE team acknowledges that SIKE (and SIDH) are insecure and should not be used

ROUND 4

PQC Candidates – Code based

Code-based Crypto

One of the most promising PQ-candidates

- An alternative offered by algebraic coding theory which has a firm, well developed mathematical background
- Code-based cryptosystems rely on some of the hard problems related to some specific linear codes, such as
  - General Decoding Problem
  - Syndrome Decoding Problem
  - Goppa Code Distinguishing
- The basic essential properties of a prospective code:
  - To be from a sufficiently large family
  - To have efficient decoding algorithms

Classical McEliece

1. Algorithm
   - KEM consists of Key generation, Encapsulation and Decapsulation
   - Key generation ()
     parameter set $= P_k$ and S_k
     $P_K = mt \times (n - mt)$
     S_k = s, L, Goppa poly
   - Encapsulation ()
     $Enc_{P_k}(e) = (K, \psi_0)$
   - Decapsulation ()
     $Dec_{S_k}(\psi_0) = (K, e)$

1. Hard Problem
   - Hardness is decoding a general linear code
   - GDP: Given an [n,k] code $\mathbb{C}$ over $\mathbb{F}_q$, an integer t_0 and a vector $c \in \mathbb{F}_q^n$, find a codeword $x \in \mathbb{C}$ with $d(x, c) \leq t_0$

Classical McEliece
Implementations

1. Software
   - Implementation in ARM Cortex-M4, with 256 KiB RAM and 2 MiB flash memory
   - Clock speed 168 Mhz, OS type-FreeRTOS v10.0.1
   - 482,594 cycles for encapsulation and 2,291,003 cycles for decapsulation and 1,589,600,267 for Key generation.

1. Hardware
   - Implementation in Xlilinx Artix 7 FPGA
   - most time consuming operation of Classic McEliece is the systemization of the public key matrix during key generation.
   - key generation in 5.2 ms to 20 ms, encapsulation in 0.1 ms to 0.5 ms, and decapsulation in 0.7 ms to 1.5 ms for all security levels on an Xlilinx Artix 7 FPGA

Security Parameter Sizes

- mceliece-6960119 parameter set: 1047319 (1MB) bytes for public key. 13908(13KB) bytes for secret key.
- mceliece-8192128 parameter set: 1357824 bytes for public key. 14080 bytes for secret key
- mceliece-6688128 parameter set: 1044992 bytes for public key. 13892 bytes for secret key.
- mceliece-460896 parameter set: 524,160 bytes for public key. 13,568 bytes for secret key.
- mceliece-348864 parameter set: 261120 bytes for public key. 6452 bytes for secret key.
- **Constant time software (measured on Haswell, larger parameters): 295932 cycles for enc, 355152 cycles for dec (decoding, hashing, etc.)**

PQC Candidates – Lattice based

Lattices-Intro

- Lattice-based Cryptography is the recent innovation in the fundamentals of cyber-security, laying foundations to strengthen the weak cryptographic policies & the unstructured security protocols.
- It uses high-dimensional geometric structures to hide information, creating problems that are considered impossible to solve without the key even by universal fault-tolerant quantum computers. Hence termed as quantum resistant cryptosystems.
- Some lattice-based cryptosystems namely GGH, Piekert's Ring -Learning with Errors(Ring LWE) Key Exchange, NTRUEncrypt, The Micciancio Cryptosystem and few others whose construction is based on the presumed hardness of the lattice problems.
- Among those NTRUEncrypt is still considered secure since its inception by Jeffrey Hoffstein, Jill Piper and J Sulliven in 1998.

Lattices Hard problems

- Some general Lattice problems used in cryptographic primitives are:
  - Shortest-Vector Problem (SVP)
  - Approximate Shortest Vector Problem (α-SVP)
  - Shortest In-dependent Vector Problem (SIVP)
  - Closest Vector Problem (CVP)
  - Approximate Closest Vector Problem (α-CVP)
  - Bounded Distance Decoding (BDD)
  - Shortest Integer Solution problem(SIS)

LWE

- The LWE (or Learning With Error), in the first instance, is a generalization of the problem Learning from parity with error.
- This problem is equivalent, to the SIVP or Shortest Independent Vector Problem of a lattice, in terms of difficulty.
- MLWE - Learning With Error other Module Lattices is considered as lattices between those used in the LWE problem definitions and those used for the Ring-LWE problem.
- The Module-LWE offers a compromise between the two extremes of the LWE and the Ring-LWE.

The LWE problem:

- Given uniform $\mathbf{A} \in \mathbb{Z}^{k \times l}$
- Given "noise distribution" χ
- Given samples $\mathbf{As+e}$, with $\mathbf{e} \leftarrow \chi$
- Search version: find $\mathbf{s}$
- Decision version: distinguish from uniform random

Hard problem?

- Find the secret vector s, to given point t, in a given random lattice A.
- In short, a Closest Vector Problem(CVP), where given a target point in a lattice, find the closest vector.

Parameters

The three paramter sets for Kyber variants Kyber-512, Kyber-768 and Kyber-1024.

variant	n	k	q	δ	quantum bits of security
Kyber 512	256	2	3329	2^{-178}	100
Kyber 786	256	3	3329	2^{-164}	164
Kyber 1024	256	4	3329	2^{-174}	230

Where n=degree of the polynomial,k= size of polynomials, q= modulc ($q \equiv 1 \bmod 2n$), δ= decryption failure.

- Kyber comes in three security levels. The size vs. security tradeoff are showed below with RSA as a pre-quantum comparison:

Variant	Security level	Private-key size (Bytes)	Public-key size (Bytes)	Ciphertext size (Bytes)
Kyber 512	AES-128	1632	800	768
Kyber 786	AES-192	2400	1184	1088
Kyber 1024	AES-256	3168	1568	1568

While AES keys are still smaller, Kyber key sizes are in the same magnitude wherein the case of Classic McEliece which is even in the megabyte range.

CRYSTALS-Dilithium

- CRYSTALS-Dilithium (digital signatures) was selected for its strong security and excellent performance, and NIST expects them to work well in most applications(July 05, 2022). In addition, the signature schemes FALCON and SPHINCS+ will also be standardized.
- CRYSTALS-Dilithium is a lattice-based digital signature scheme whose security is based on the hardness of finding short vectors in lattices.
- It is based on the" Fiat-Shamir with Aborts" technique of Lyubashevsky which uses rejection sampling to make lattice-based Fiat-Shamir schemes compact and secure.
- It has the smallest public key + signature size of any lattice-based signature scheme that only uses uniform sampling (avoids all uses of discrete Gaussian sampling).
- The strength of a CRYSTALS-Dilithium key is represented by the size of its matrix of polynomials. For example, CRYSTALS-Dilithium (6,5) has a matrix size of 6x5. The larger the matrix size, the stronger the key

	5x4 matrices	6x5 matrices
Public key	1.5kb	1.8kb
Signature	2.7kb	3.4kb

(Hybrid) Quantum Security Applications

PQC Applications

- Create a plan to replace the vulnerable algorithms with post-quantum algorithms as they become available.
- Prioritize those systems that store or transfer your most sensitive data.
- This will probably mean updating your old operating systems, and maybe even your old hardware.
  - RSA, DSA, ECC, DH – the actual vulnerable algorithms
  - TLS, SSH, S/MIME, PGP, IPSEC – protocols that depend on these vulnerable algorithms
  - VPNs, Kerberos – protocols that may depend on these vulnerable algorithms
  - Browsers, encrypted messaging, disk encryption, authentication schemes – applications that (potentially) use these protocols and vulnerable algorithms.

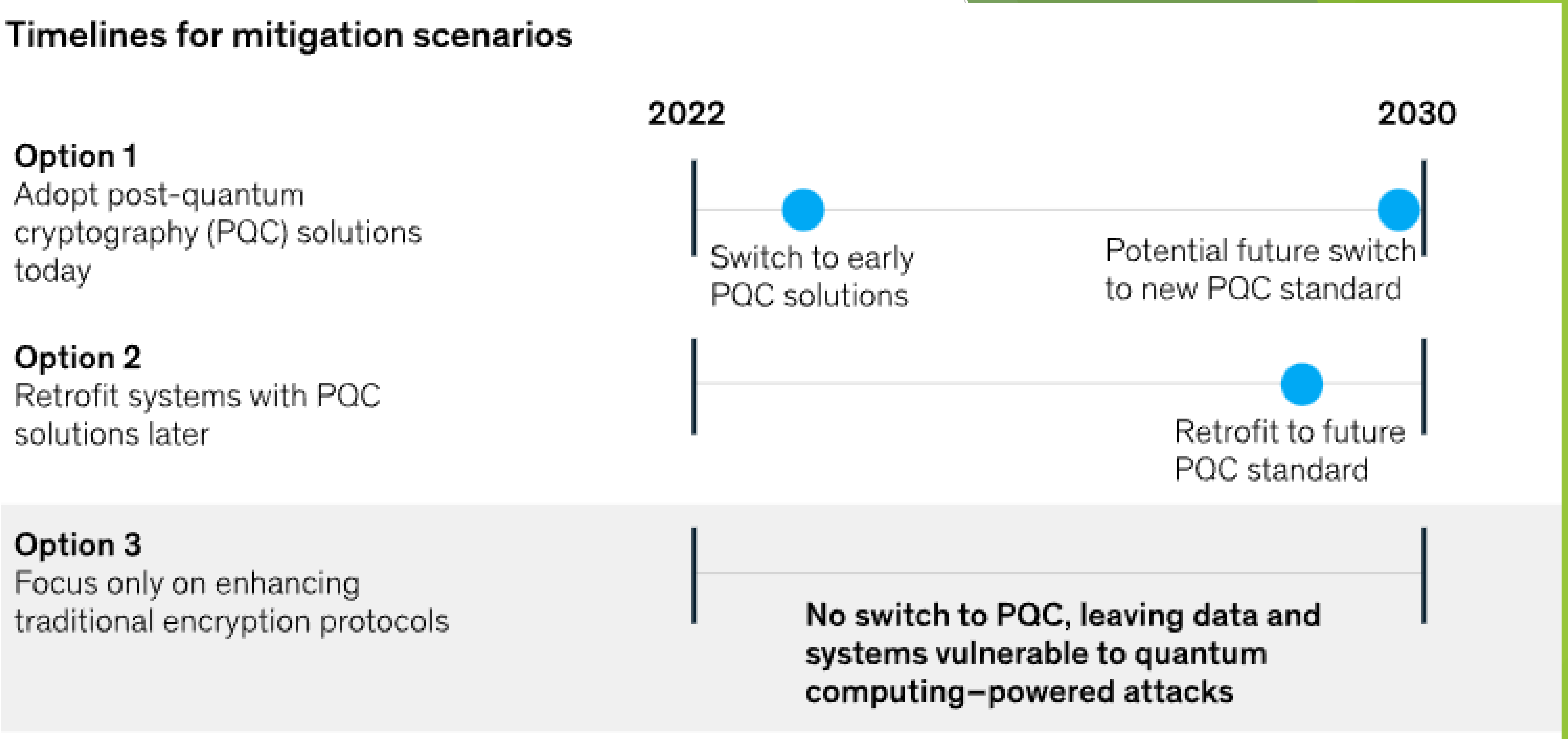
When to act

- Decision makers have three options to mitigating PQC threats.

Option 1: Adopt post-quantum cryptography solutions today

Option 2: Retrofit systems with post-quantum cryptography solutions later

Option 3: Focus only on enhancing traditional encryption protocols



QUANTUM CRYPTOGRAPHY

Quantum Cryptography has Numerous Applications

Banking & Finance
Core Banking Database

Critical Infrastructure
Authentication Records

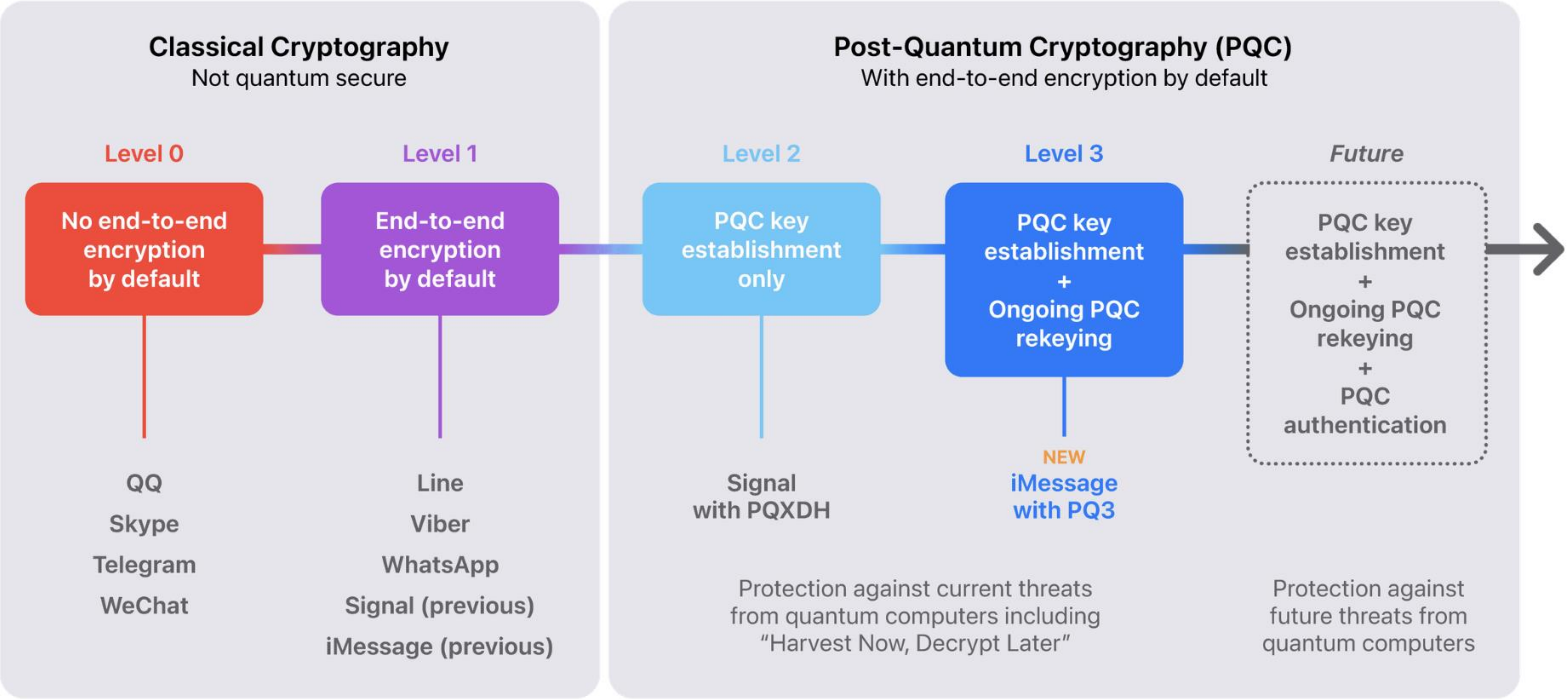
IP Protection
Research & Development Documents

Government
Citizens Unique Identifier Database, Classified Data

Defense
Voice and Data Communication

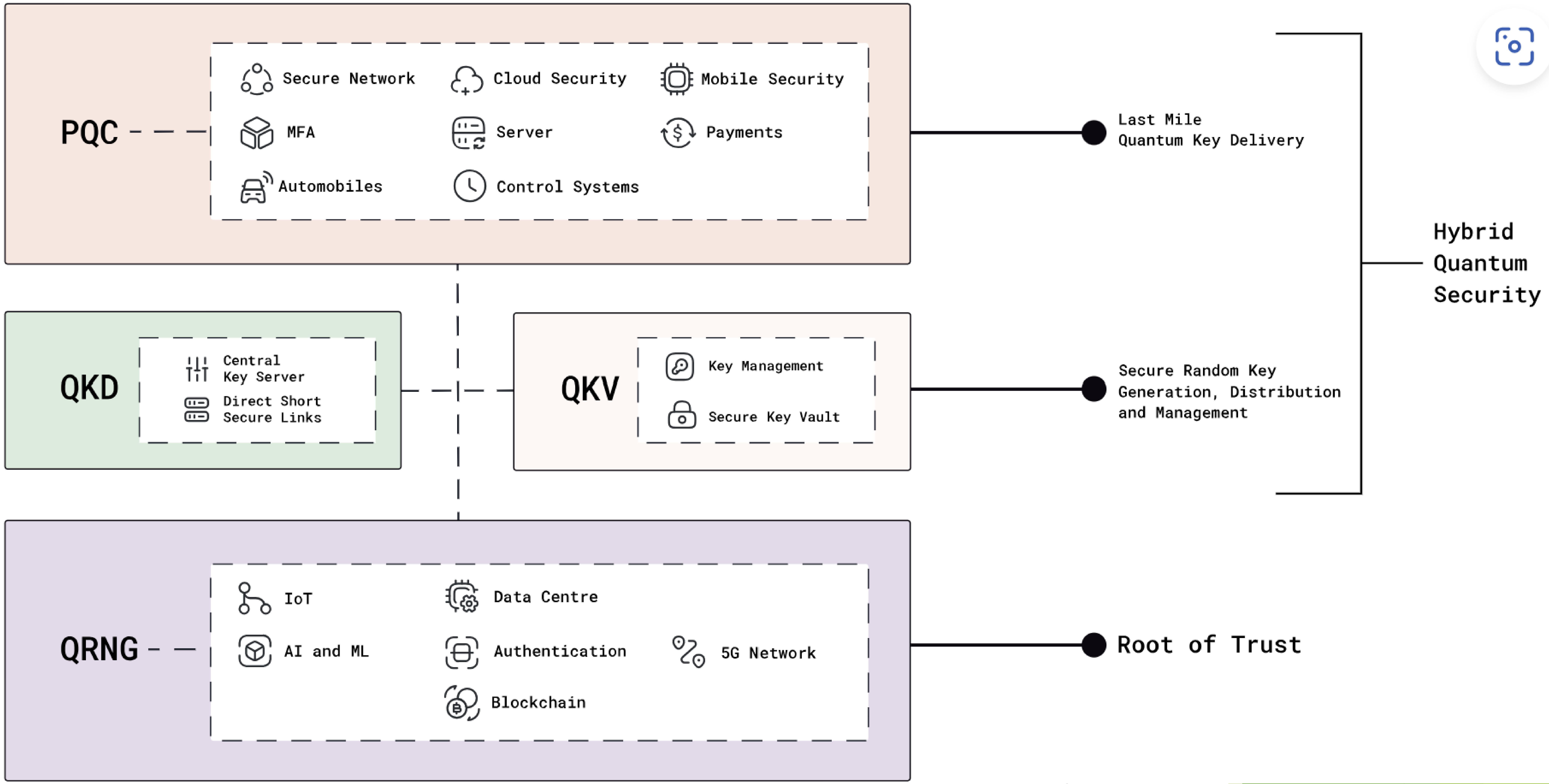
Healthcare
Health Records

Quantum-Secure Cryptography in Messaging Apps



Note: This comparison evaluates only the cryptographic aspect of messaging security, and therefore focuses on end-to-end encryption and quantum security. Such a comparison doesn't include automatic key verification, which we believe is a critical protection for modern messaging apps. As of the time of this writing, only iMessage and WhatsApp provide automatic key verification. The iMessage implementation, called Contact Key Verification, is the state of the art – it provides the broadest automatic protections and applies across all of a user's devices.

Augments Quantum Security Systems



Projects PoCs

Areas of Research

Cryptography and Cryptanalysis

Leading research group working in design of customized encryption algorithms, authentication algorithms, AI, cryptanalysis and key management in IoT.

- Design of Proprietary Block Ciphers and Stream Ciphers
- Development of Cryptanalysis tools for of Stream and Block ciphers
- Randomness and Test suites for Cryptanalysis
- Machine learning approaches for Cryptanalysis
- Design of Secret Sharing schemes
- SAT and SMT Solvers based Cryptanalysis
- High performance computing for Cryptanalysis
- Lightweight Cryptography
- Design and analysis of Image Encryption Methods
- Authenticated Encryption with Associated Data Schemes
- Key Management in IoT

Quantum & Post Quantum Cryptography

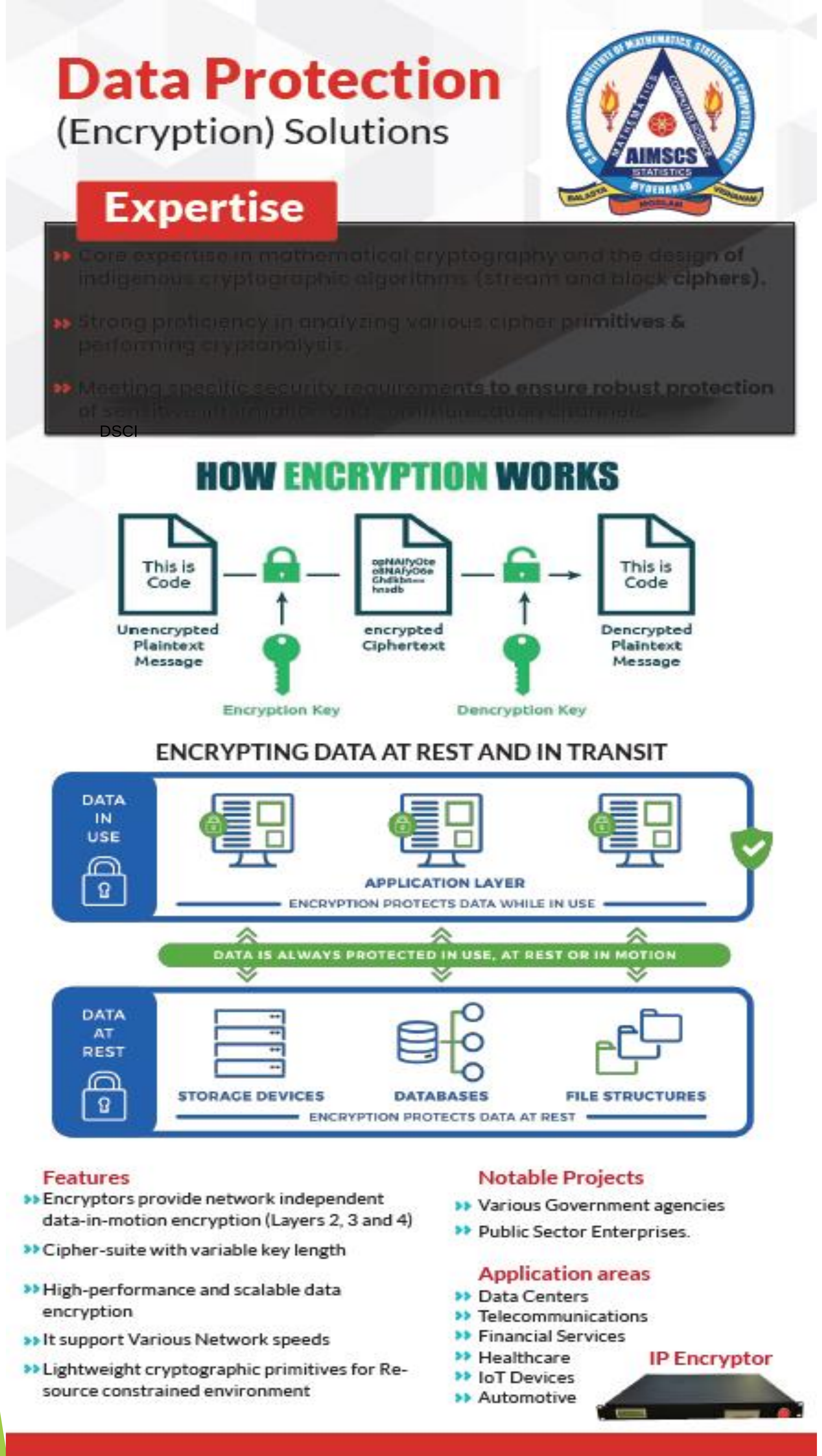
Research group working in code and lattice based cryptography, Post Quantum and Quantum cryptography.

Post Quantum Cryptology:

- Code based Cryptography and Cryptanalysis
- Lattice based Cryptography and Cryptanalysis

Quantum Cryptology:

- QKD
- QTRNG
- Quantum Cryptanalysis



Research Areas & Expertise Developed

The design of proprietary block ciphers and stream ciphers is a critical area of research and development in the field of cryptography, especially for specialized applications requiring customized encryption algorithms.

Research Topics:

- Design of Proprietary Block Ciphers and Stream Ciphers
- Development of Cryptanalysis tools for of Stream and Block ciphers
- Randomness and Test suites for Cryptanalysis
- Machine learning approaches for Cryptanalysis
- Design of Secret Sharing schemes
- SAT and SMT Solvers based Cryptanalysis
- High performance computing for Cryptanalysis
- Lightweight Cryptography
- Design and analysis of Image Encryption Methods
- Key Management in IoT
- Authenticated Encryption with Associated Data Schemes.

Software tools/PoCs:

- Developed Indigenous stream and block ciphers
- Developed various cryptanalysis tools.
- Developed a Tool kits

Publications: Journals 14, Conferences: 6

Users: SAG-DRDO, CAIR-DRDO

Crypto-Suite

Test the strength of Random sequence & Cipher

Purpose

Cryptanalysis Toolkit aims at making people understand network security threats and working of cryptology.

This Tool-kit allows users to self-validate their cryptographic systems and detect any vulnerabilities or weaknesses.

PRNG/QRNG

PRNGs: software based algorithm which generates random numbers from deterministic source seed.

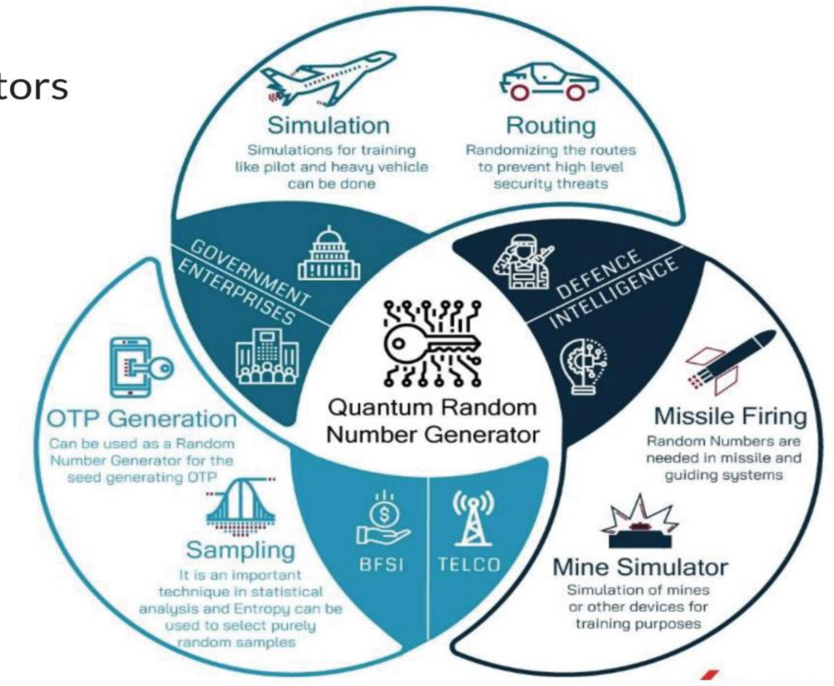
TRNGs: hardware based inputs to create random values. The inputs are generally physical processes like thermal noise or atmosphericnoise.

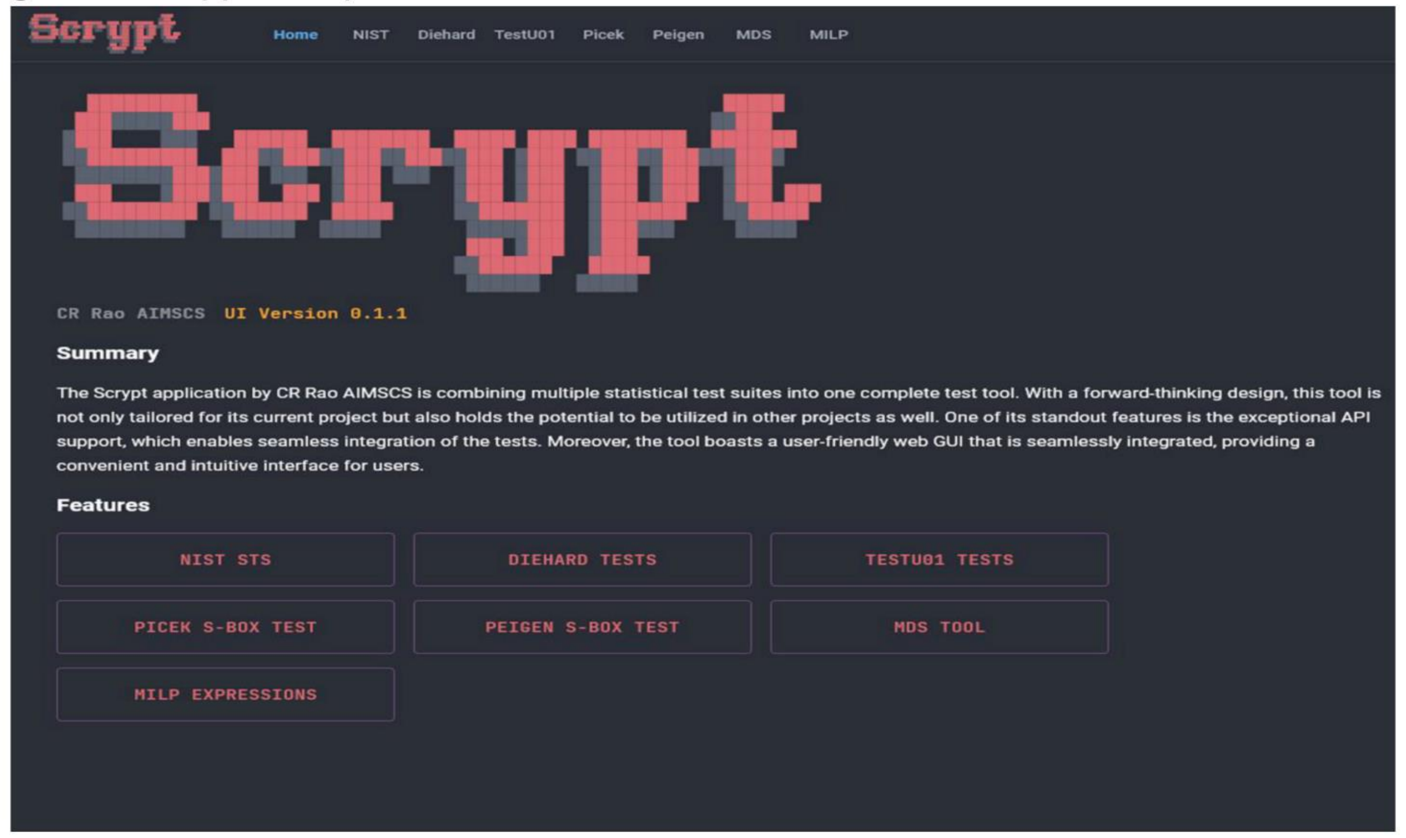
QRNGs: devices that use quantum mechanical effects to produce the highest level of randomness possible

Statistical tests offer a common approach to randomness testing..

Features

- Pseudo Random number generators
- NIST Test suite
- Diehard Test suite
- TestU01
- CRR Test suite
- Picek S-Box Test
- PEIGEN S-Box Test
- MDS Tool
- Mixed Integer Programming Expressions.
- Linear cryptanalysis
- Differential cryptanalysis
- Algebraic cryptanalysis





The automated suite provides various randem test suites & cryptanalysis methods

Research Areas & Expertise Developed:

- Testing the randomness of a sequence generated by classical/ Quantum generators
- Evaluation of strength of a cryptosystem and crypto primitives.
- Generation of Non-linear components of a cryptosystem.

Research Topics:

- Randomness-Testing (TRNG/PRNG/QRNG)
- S-Box Testing
- MDS Matrix generation and testing
- Linear/Differential/Algebraic Cryptanalysis
- MILP based cryptanalysis

Publications:

- Journals: 6
- Conferences: 4

Software tools/PoCs: Developed a Tool kit for

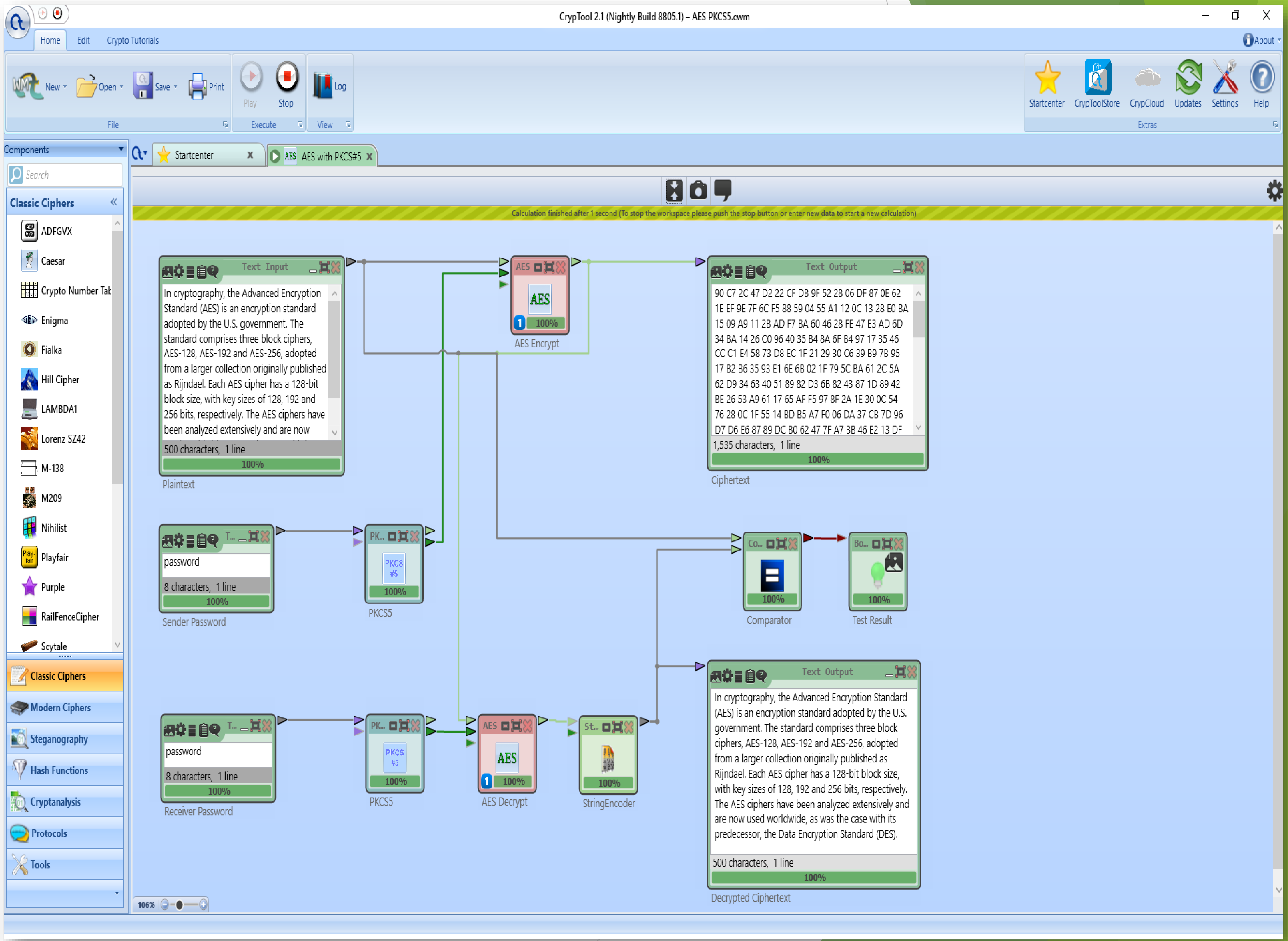
i. Checking the strength of a crypto primitives and randomness.

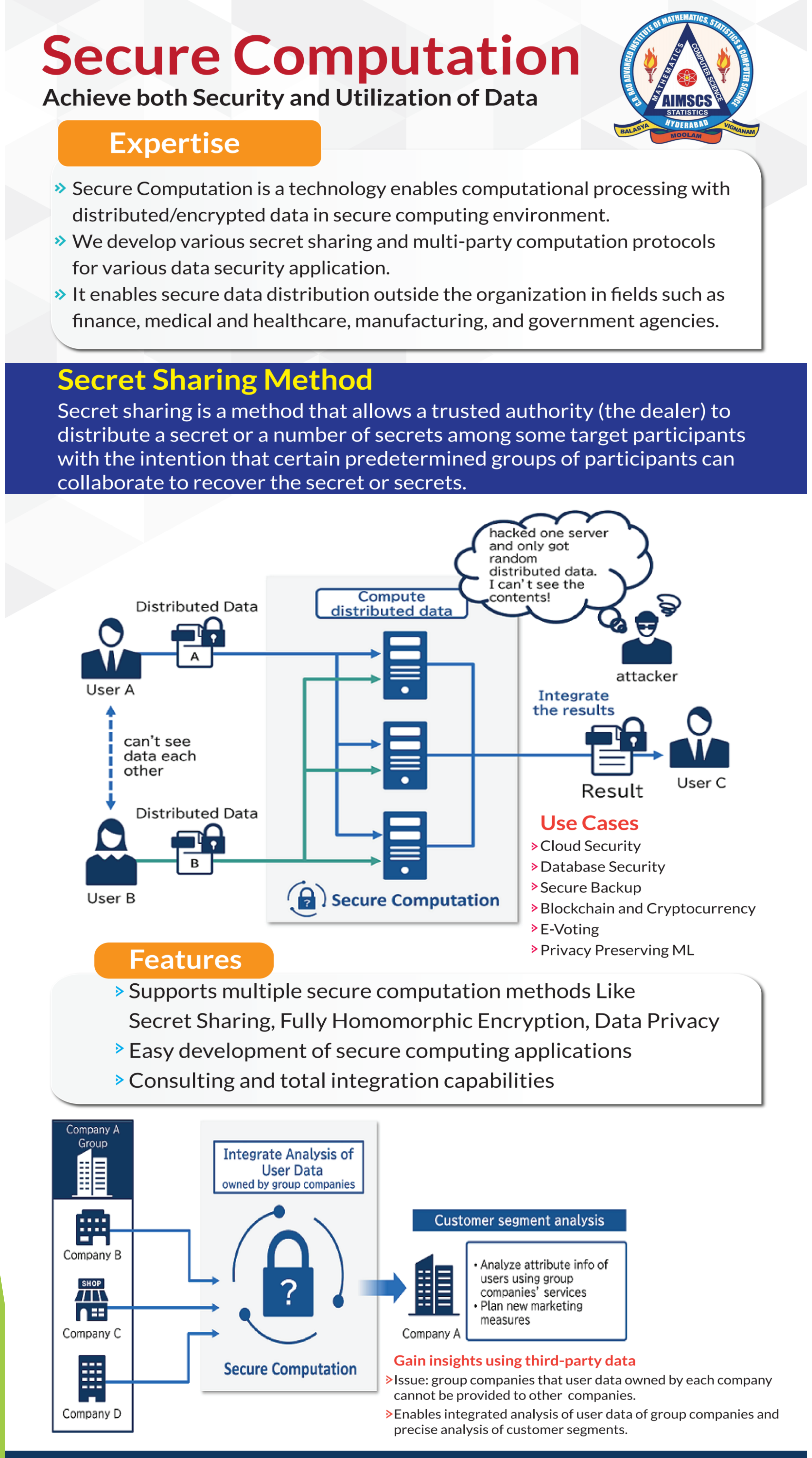
ii. Generation of efficient crypto primitives

Users: DRDO, NTRO, QuNu

Crypt-Tool

The proposed toolkit looks like





- **Research Areas & Expertise Developed**

  We developed various secret sharing and multi-party computation protocols for various data security application.

  - Explore the potential applications of SS and the Threshold Signature model within the blockchain and distributed systems framework.
  - It facilitates secure data sharing across organizational boundaries in industries like finance, healthcare, manufacturing, and government.
  - Design of SS protocols that satisfy the conflicting demands of efficiency, scalability, verification transparency, and protection against unauthorized access presents a significant challenge.

Research Topics:

- Secret Sharing Schemes
- Multi-Party Computation
- Secure Data Distribution and Computation
- Fully Homomorphic Encryption
- Data Privacy

Software tools/PoCs:

- Developed application using Publicly verifiable secret sharing schemes and implemented in client server application for secure storage.

Publications: • Journals: 24, Conferences: 8

Users: NTRO

- **Research Areas & Expertise Developed**

  - Lightweight cryptography focuses on designing cryptographic algorithms and protocols that provide strong security guarantees while being efficient in terms of computational, memory, and power resources.

- We developed cryptographic algorithms tailored for resource-constrained environments such as IoT devices, mobile devices, and embedded systems.

Research Topics:

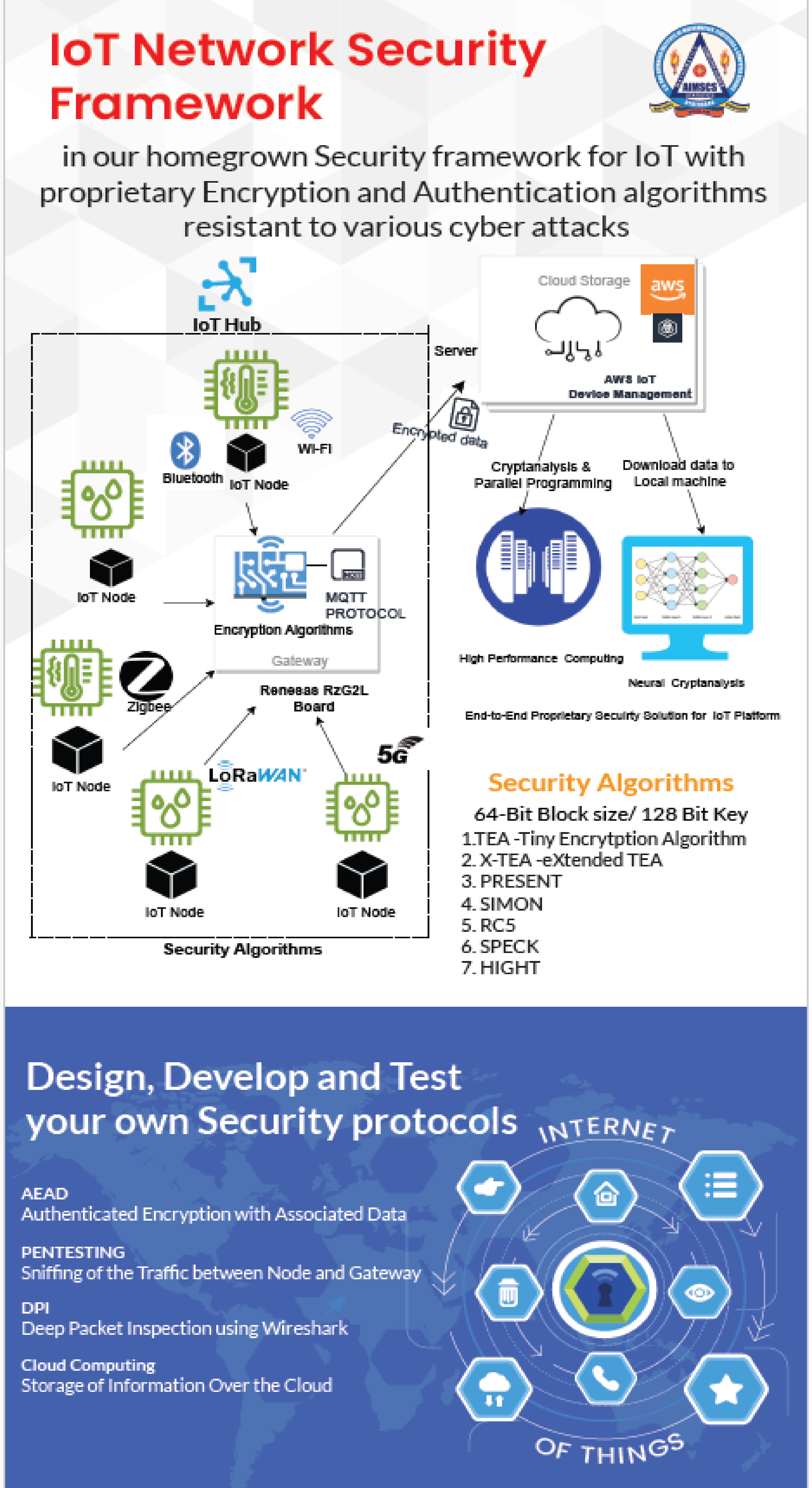
- Designing of efficient Lightweight block and stream ciphers
- Efficient authentication methods for embedded systems
- Lightweight adaptations of public-key schemes.
- Authentication and Key Exchange: Lightweight protocols for secure communication, such as key exchange and mutual authentication, are critical for constrained devices.
- Zero-Knowledge Proofs (ZKPs): Zero-knowledge proofs are often considered too computationally expensive, but researchers are working on lightweight versions to enable privacy-preserving protocols in constrained environments.

Software tools/PoCs:

- Cryptanalysis tools for lightweight block ciphers.

Publications: • Journals: 3, Conferences: 2

Users: DRDO, CAIR, DSCI



- **Research Areas & Expertise Developed**

An Internet of Things (IoT) system connects a device through various network interfaces to a cloud that houses the platform and applications that offer services that IoT service consumers employ.

- In order to ensure that security and identities are appropriately managed, configured, and monitored within the domain in accordance with policies, regulations, and agreements, domain management of security and identity functions within domains is used.
- High speed data generation using IoT device for Testing Encryption algorithm
- Design and develop lightweight encryption algorithms
- AEAD Schemes on IoT Devices
- Design IoT Security using Proprietary Algorithms
- AI/ML techniques in IoT

Research Topics:

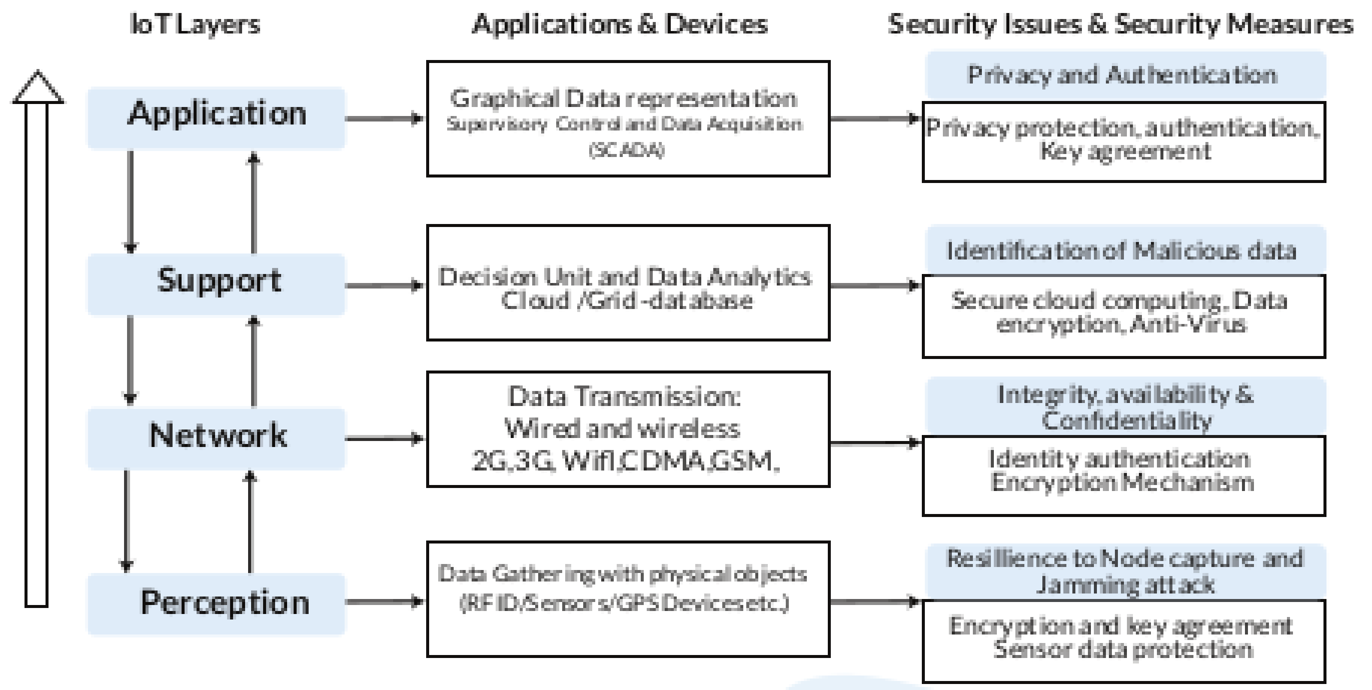
- Applying Lightweight encryption schemes to IoT devices
- Authenticated Encryption with Associated Data for keyless authentication
- ML/DL Soft Computing Techniques
- Design of LLMs for Encryption classification / Identification
- **Use cases**:
  - Medical IoT (IoMT), Applying Security frameworks for Internet of Medical Things (IoMT)

Lightweight Blockchain Based Authentication Scheme for IoT Security

A Lightweight Authenticated Key Management Protocol for Securing Industrial Control Systems: IoT as the Use Case

Key Components

- Robust, verifiable, authenticated lightweight group key management protocol frameworks, applicable to IoT environment
- Security analysis - Scyther & AVISPA (Automated Validation of Internet Security Protocols and Applications)

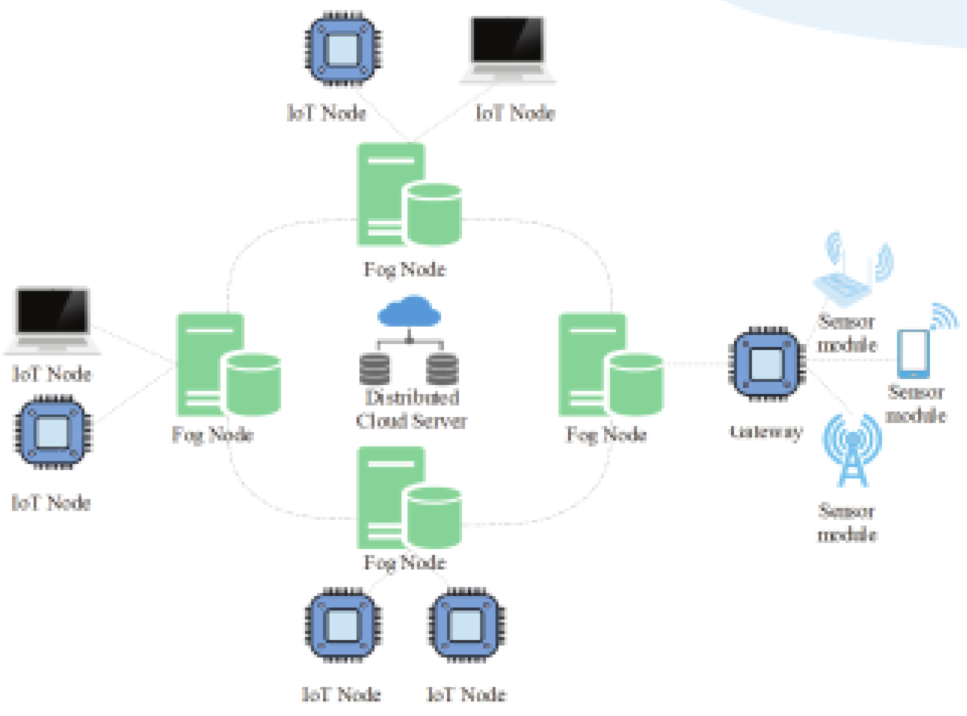


Blockchain based Lightweight Authentication Scheme for IoT Environment

- We set up a dev environment to build smart contract(s) for the authentication protocol using blockchain.
- Use Ethereum or Knuct

Use cases

- Secure boot for (battery operated) IoT devices
- Small size root of trust implementations
- Digital fingerprinting of messages
- RFID tag message counterfeiting protection
- Vehicle-to-Vehicle communication



- **Research Areas & Expertise Developed**

  Focusing on enhancing both the efficiency and security of authentication protocols tailored for resource-constrained IoT environments.

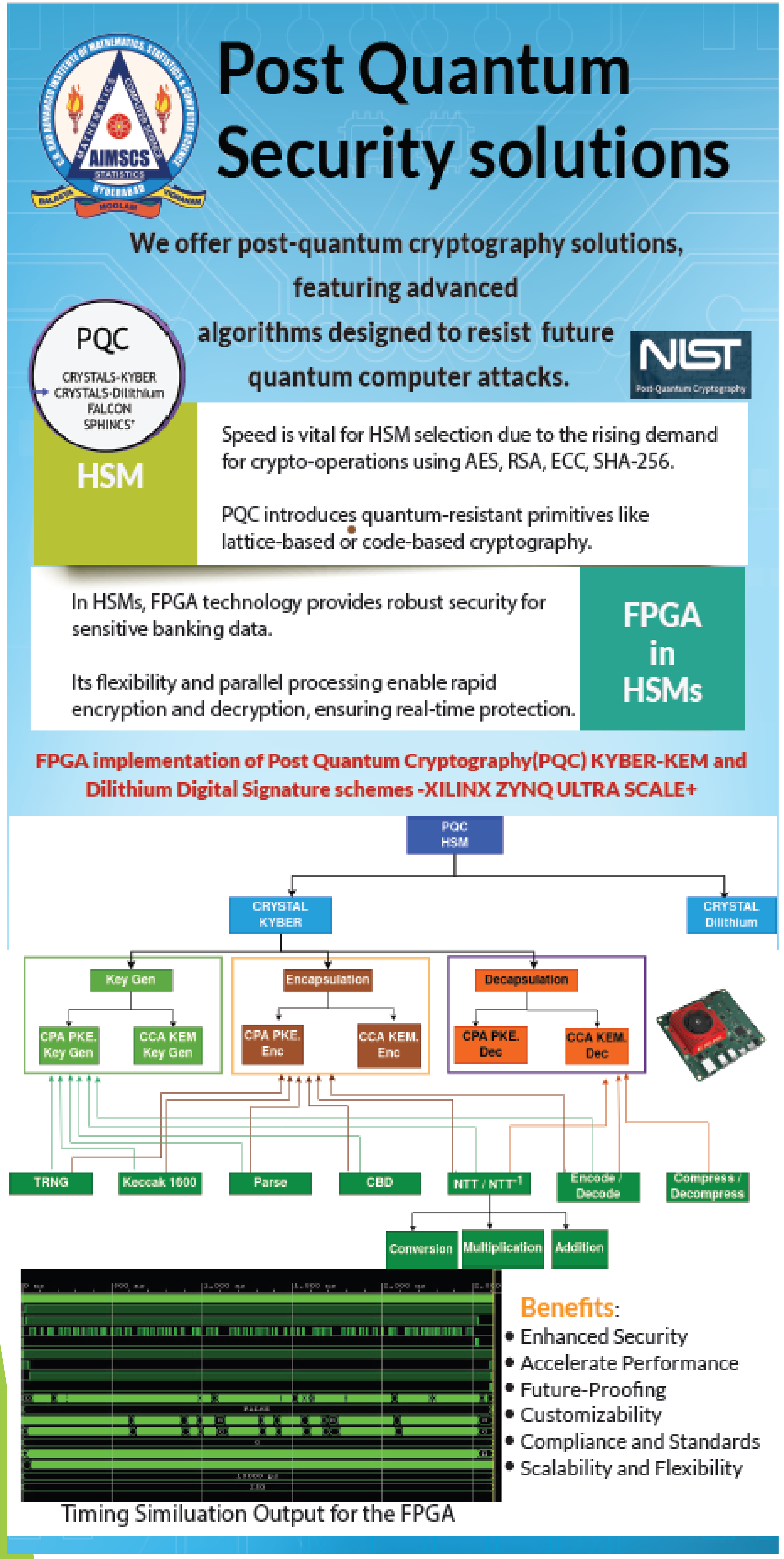
Research Topics:

- Exploring methods like homomorphic encryption and zero-knowledge proofs within blockchain
- Efficient Consensus Mechanisms in Resource-Constrained Environments.
- Lightweight blockchain-based authentication techniques for IoT (Internet of Things) security focus on utilizing the decentralized, tamper-resistant, and transparent nature of blockchain to secure IoT devices and their communications, while also addressing the resource constraints (limited processing power, memory, and energy) of IoT devices.
- Research in lightweight cryptography spans multiple areas, including algorithm design, hardware implementation, and application scenarios.

Software tools/PoCs:

- A lightweight authenticated protocol for securing industrial management systems: IoT as use case.

Publications: Journals: 4, Conferences: 2, Patents: 1



- **Research Areas & Expertise Developed**

  Design and analysis of lattice and code-based Post Quantum Secure Key Encapsulation Mechanisms, Encryption schemes and Digital Signatures.

Expertise Developed

Hardware implementation of NIST PQC Finalists CRYSTALS KYBER & CRYSTALS DILITHIUM.

Applications:

- Hardware Security Module (HSM)
- Industrial communication protocols like TLS 1.3/SSH/VPNs
- Software and firmware updates
- Secure emailing and messaging

Software tools/PoCs:

1. Design and analysis of lattice based PKE - DRDO(2011-2013)
2. Design and analysis of code-based PKE - DRDO(2013-2015)
3. Hardware implementation of NIST PQC Finalists KYBER -KEM and Dilithium on Xilinx FPGA- an industry project

- **Software tools/PoCs/APIs**

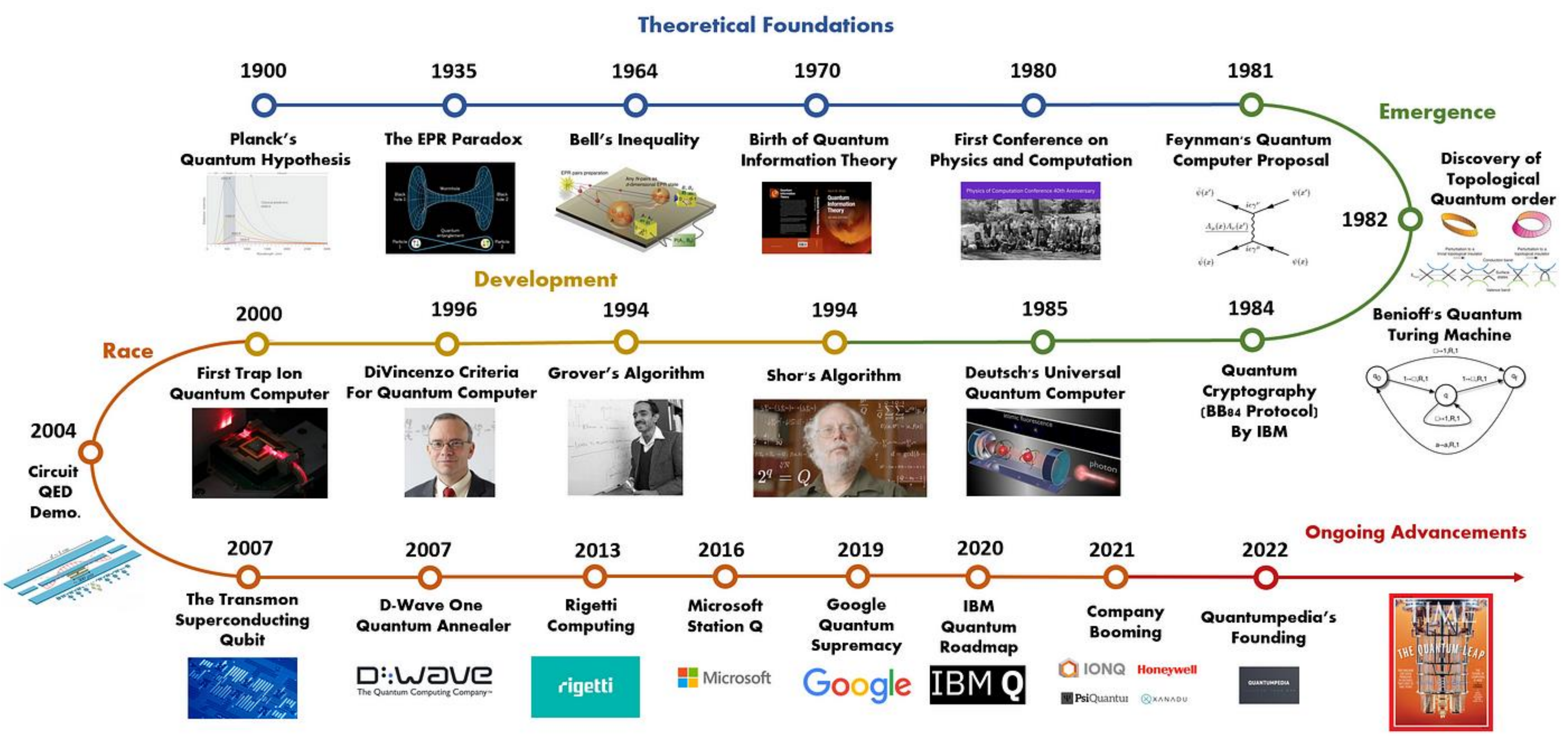
PoCs implemented- currently under progress

Users: Govt and Defence sectors , Cybersecurity Industry

THANK YOU

Contact me:
tanaidu@crraoaimscs.res.in
+91-8297852575

A Brief History of Quantum Computing (Copyright: Quantumpedia)



Roadmap


2016
Public call for candidate submissions
• 82 received
2017
Round 1 completed
• Whittled down to 69 algorithms
• 21 broken
2019
Round 2 completed
• 26 algorithms remain
• 8 suffered attacks
2021
Round 3 completed
• 7 finalists selected
• 1 suffered attack
2022
• 4 finalists expected to be announced in early 2022
• Call for public comments opens
2024
Standard finalized
2025–26
Commercial products using approved algorithms begin to hit the market
2034+
NIST warns 5–15 years will be needed after final standards are published for full transition to be completed