Future Proof Security Algorithm: Quantum-Safe Encryption

By

Prashant Chugh
C-DOT, New Delhi

Agenda

- Background
  - Cryptography
  - Types of cryptography
  - Quantum Computing & algorithms
- Threat to current cryptographic systems
- International efforts in Standardization of PQC
- Quantum-safe techniques
- C-DOT's CEM (Compact Encryptor Module)
- A recall of M2M Architecture
- Quantum-safe encryption in M2M

Background Cryptography

- Cryptography is a tool that is used by security practitioners everywhere to protect anything that relies on electronic communication and data storage
- Cryptography is a foundational building block for secure banking, e-commerce and secure communications and is a prime area of National Security
- Cryptography uses computational hardness as a means to protect sensitive data. This is to say that there are cryptographic problems that are difficult or impossible to solve using conventional computing

Background Types of Cryptography

- **Secret Key Cryptography (SKC)**
  - – Also referred to as Symmetric encryption.
  - – Only one key is used for both encryption and decryption.
  - – much faster than asymmetric algorithms
- **Public Key Cryptography (PKC)**
  - – Also called Asymmetric encryption
  - – Two keys are used (public and private keys)
  - – Sender encrypts the information using the receiver's public key. The receiver decrypts the message using his/her private key
- **Hash Functions**
  - – No key / with key
  - – Also called one-way encryption
  - – mainly used to ensure that a file has remained unchanged.

Background Quantum Computing

- Quantum computing is a new branch of computing in which fundamental unit of storage is qubits rather than bits in the conventional computer. A qubit can store both 0 and 1 at the same time.
- Quantum computers can perform very rapid parallel computations as compared to classical computers.
- For certain classes of mathematical problems like integer factorization and discrete logarithms, quantum computers are able to perform much better than classical computers

Background Quantum Algorithms

- Algorithms that run on Quantum computers are called Quantum Algorithms
- Some cryptographic problems, which are difficult or impossible to solve using conventional computing, become fairly trivial to solve using quantum algorithms
- Two quantum algorithms- Shor’s algorithm and Grover's algorithm are a threat to many currently widely used cryptosystems
- A lot of further research is happening in the field of Quantum Computers and Quantum Algorithms
- A more than 50 qubit Quantum Computer is expected to be developed any time in next 10 years and this is likely to be more powerful than any of the supercomputers existing today.

Threat to Cryptographic Systems

- Breaking a cryptographic algorithm can have catastrophic repercussions for anyone using that algorithm who is ignorant of its compromise.
- There is a great advantage for anyone who can break adversary's cryptographic algorithm.
- Cryptographic Systems are increasingly vulnerable to quantum attacks as quantum computing matures and the state of the art in computation and algorithm design is redefined.

Threat to Cryptographic Systems

- Security practitioners today are giving early warning of the wide scale security collapse of communications infrastructure due to heavy reliance on Diffie-Hellman, RSA and ECC.
- Almost all public key cryptography products being used today rely on one or more of RSA, DSA, DH, ECDH or ECDSA & their variants.
- Symmetric cryptography algorithms using AES are so far considered safe from quantum computers.
- However, most systems using AES rely on public key cryptography for key distribution which is vulnerable.

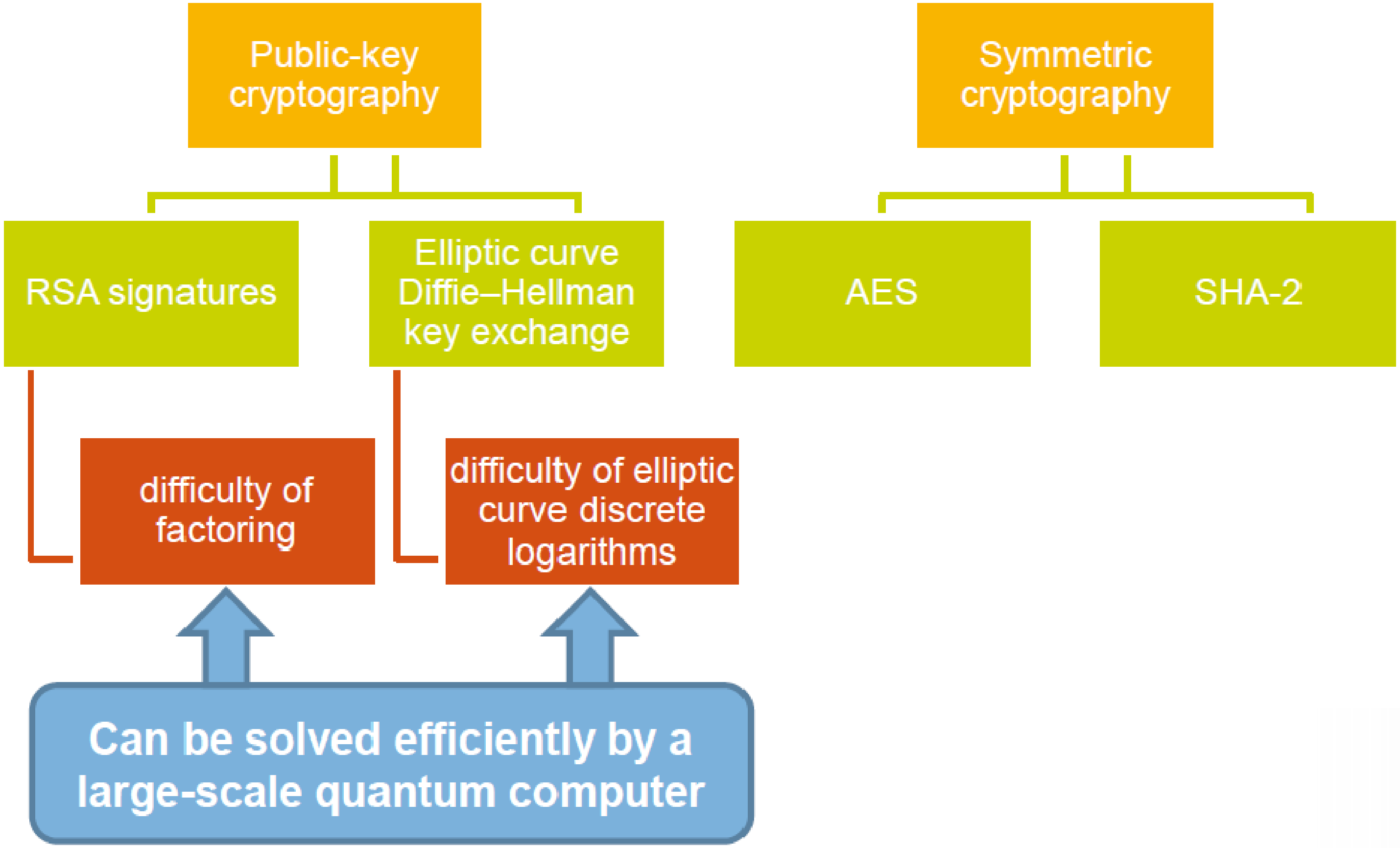
….contd…

Threat to Cryptographic Systems

- Secure Communication Protocols that are under threat include:
  - IPSec
  - SSH and TLS
  - VPN
  - S/MIME
  - HTTPS
- Even encrypted information sitting in a database for past many years will be subject to decryption by those having access to quantum computing platforms
- These include the possible misuse of the previously encrypted banking information, identity information and items relating to state & military security secrets and other sensitive information.

....contd...

Threat to Cryptographic Systems



Public-key cryptography

Symmetric cryptography

RSA signatures

Elliptic curve Diffie–Hellman key exchange

AES

SHA-2

difficulty of factoring

difficulty of elliptic curve discrete logarithms

Can be solved efficiently by a large-scale quantum computer

....contd...

Threat to Cryptographic Systems

Comparison of conventional and Quantum Security levels of some popular ciphers

Algorithm	Key Length	Effective Key Strength / Security Level	
		Conventional Computing	Quantum Computing
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

Reference: ETSI Quantum-safe Whitepaper- June 2015

Definition

Quantum-safe cryptography: The field of cryptography whose objective is to create public key cryptosystems that are expected to be secure against the threat of quantum computers.

This is also called **Quantum-resistant cryptography** or **Post-Quantum cryptography**

International Standardization Efforts

- ETSI has issued a whitepaper titled "Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges" and has launched an Industry Specification Group on Quantum Safe Cryptography (ISG-QSC) in 2015.
- NIST has already started a process for standardizing the quantum-resistant cryptographic algorithms, for which first list of submissions were made public in Jan'18 and first conference was held in April'18.
- IETF has come up with an RFC draft in Oct 2016 on an extension of IKEv2 for quantum resistance.
- 10 years to maximum 15 years is the Time frame in which most experts predict that quantum computers to break most current cryptographic standards shall be available. However, some experts feel it could be as early as 2025.
- Besides known companies/ universities working in development of quantum computers, there may be top-secret projects by Governments/ large companies for Quantum Computers Development.
- Considering time needed to bring out new cryptographic standards is usually 8-9 years, ETSI says that we may already be late to start building Quantum-Safe cryptography algorithms for critical sectors.

International Proprietary Efforts and Approach

- Google- Tested a proprietary Post-quantum encryption algorithm called "New Hope" in Chrome Web browser.
- Since the proprietary algorithm used in the above scenarios is not yet proven for security, hence the approach in Chrome's testing is Quantum-safe hybrid.
- In Quantum-safe hybrid approach, handshake is done using two key exchange algorithms-one post quantum algorithm and one traditional algorithm. It allows early adopters to retain the current security of traditional algorithms while experimenting with post quantum algorithms and getting the post quantum algorithm & implementation verified through critical public reviews & cryptanalysis.
- This hybrid approach has its performance cost but is going to be the likely approach in introduction of any post quantum crypto algorithm in future.

Quantum-Safe Techniques

QKD at physical layer

- QKD or Quantum Key distribution has been proposed as one solution for key distribution problem
- QKD is based on fundamental laws of quantum physics and information is encoded in quantum states of light
- QKD is proven to be theoretically secure against arbitrary attacks, including quantum attacks

Quantum-Safe Techniques

Need for new algorithms

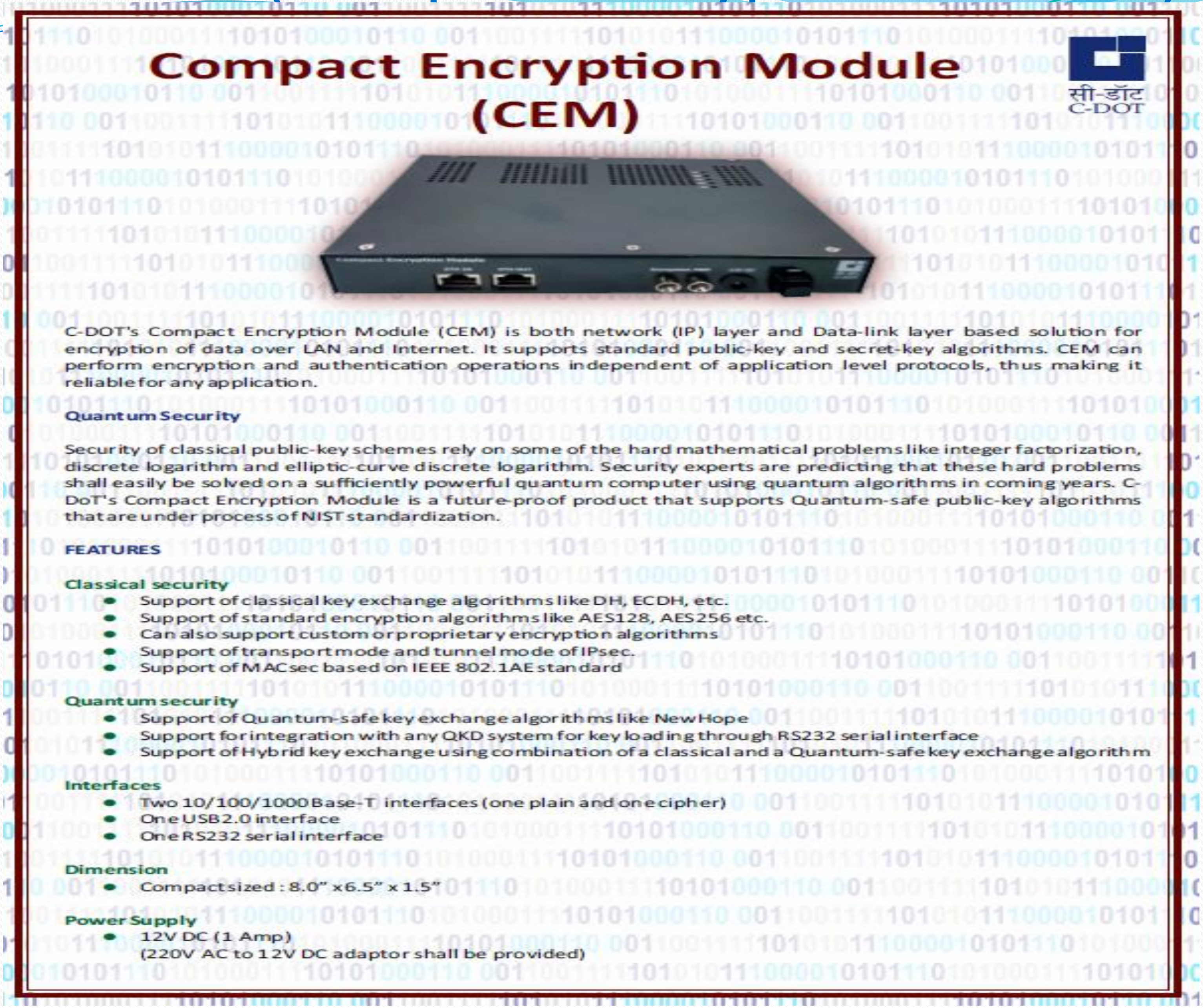
- Many of the quantum safe algorithms based on hard problems of mathematics have also been proposed, which are being discussed and evaluated in NIST & other international forums.
- Unlike QKD approach, these algorithms are easy to deploy and replace the existing crypto systems.
- Cryptographic algorithms usually require years of public review & scrutiny before there security can be established.

Need for cryptographic products integration with new quantum-safe algorithms

- Many new algorithms have already been made public by NIST in Jan'18.
- There is a need to integrate new quantum-safe algorithms with existing cryptographic products such that new quantum-safe algorithms co-exist with existing non-quantum-safe/classical algorithms.
- Integration of a new quantum-safe algorithm should only be done after thorough comparison of all the popular algorithms in cryptographic community.

C-DOT's CEM (Compact Encryption Module)

Page 1



Compact Encryption Module (CEM)

सी-डॉट
C-DOT

C-DOT's Compact Encryption Module (CEM) is both network (IP) layer and Data-link layer based solution for encryption of data over LAN and Internet. It supports standard public-key and secret-key algorithms. CEM can perform encryption and authentication operations independent of application level protocols, thus making it reliable for any application.

Quantum Security

Security of classical public-key schemes rely on some of the hard mathematical problems like integer factorization, discrete logarithm and elliptic-curve discrete logarithm. Security experts are predicting that these hard problems shall easily be solved on a sufficiently powerful quantum computer using quantum algorithms in coming years. C-DoT's Compact Encryption Module is a future-proof product that supports Quantum-safe public-key algorithms that are under process of NIST standardization.

FEATURES

Classical security

- Support of classical key exchange algorithms like DH, ECDH, etc.
- Support of standard encryption algorithms like AES128, AES256 etc.
- Can also support custom or proprietary encryption algorithms
- Support of transport mode and tunnel mode of IPsec.
- Support of MACsec based on IEEE 802.1AE standard

Quantum security

- Support of Quantum-safe key exchange algorithms like NewHope
- Support for integration with any QKD system for key loading through RS232 serial interface
- Support of Hybrid key exchange using combination of a classical and a Quantum-safe key exchange algorithm

Interfaces

- Two 10/100/1000Base-T interfaces (one plain and one cipher)
- One USB2.0 interface
- One RS232 serial interface

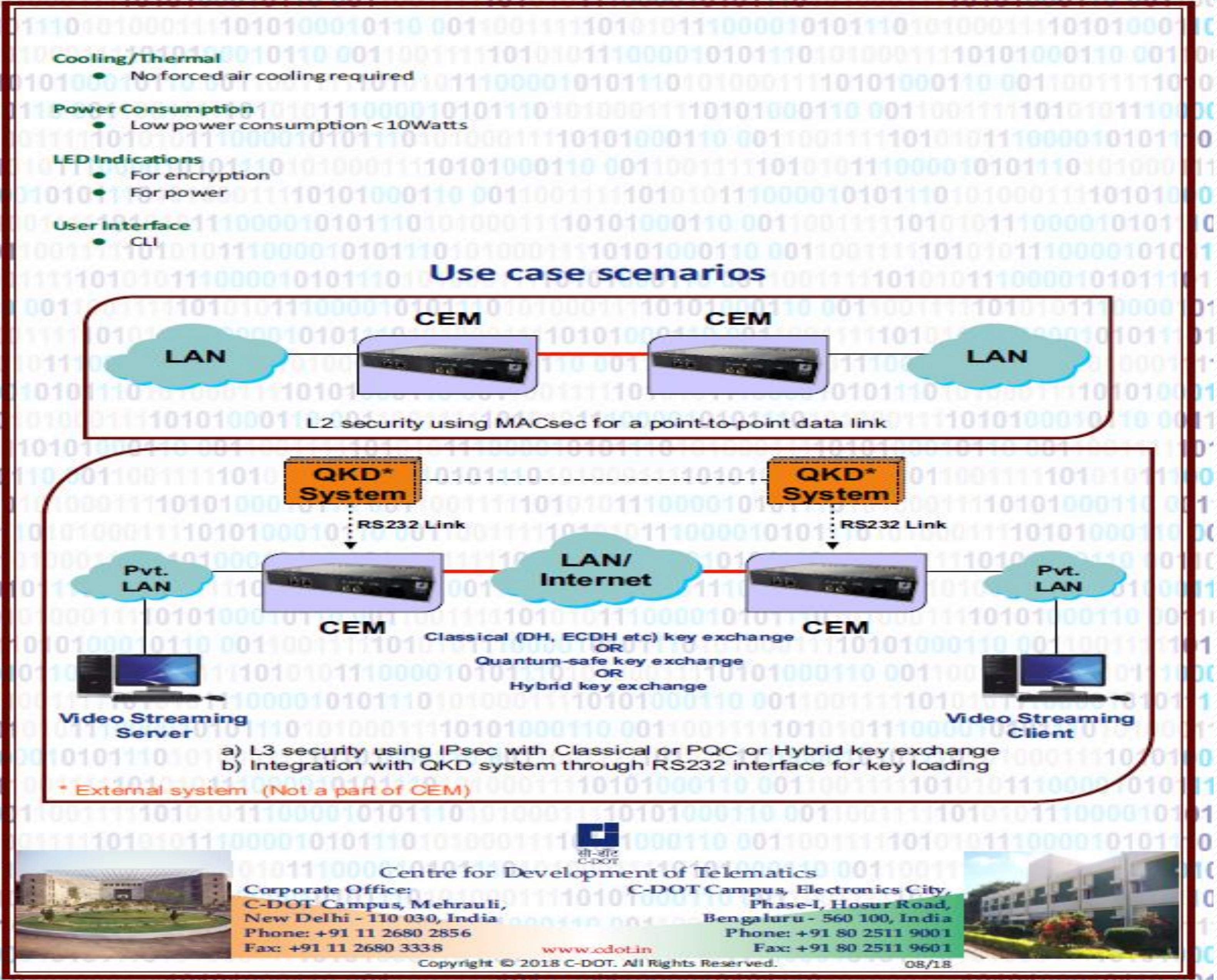
Dimension

- Compact sized : 8.0" x6.5" x 1.5"

Power Supply

- 12V DC (1 Amp)
(220V AC to 12V DC adaptor shall be provided)

Contd…C-DOT's CEM (Compact Encryptor Module)



Cooling/Thermal

- No forced air cooling required

Power Consumption

- Low power consumption <10Watts

LED Indications

- For encryption
- For power

User Interface

- CLI

Use case scenarios

LAN
CEM
CEM
LAN
QKD* System
QKD* System
RS232 Link
RS232 Link
Pvt. LAN
CEM
LAN/ Internet
CEM
Pvt. LAN
Video Streaming Server
Video Streaming Client
Classical (DH, ECDH etc) key exchange
OR
Quantum-safe key exchange
OR
Hybrid key exchange

L2 security using MACsec for a point-to-point data link

a) L3 security using IPsec with Classical or PQC or Hybrid key exchange
b) Integration with QKD system through RS232 interface for key loading

* External system (Not a part of CEM)

सी-डॉट
C-DOT

Centre for Development of Telematics

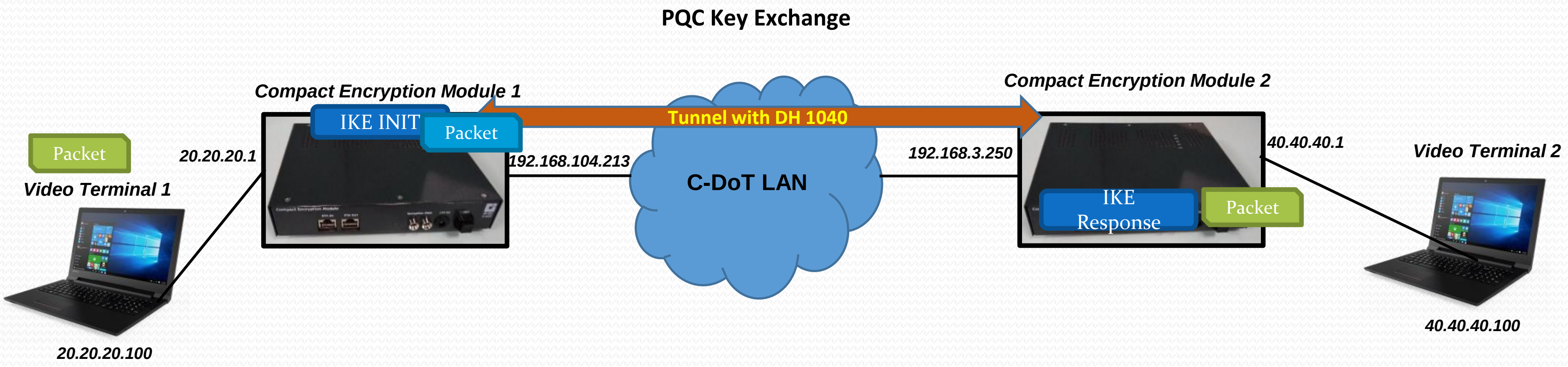
Corporate Office:
C-DOT Campus, Mehrauli,
New Delhi - 110 030, India
Phone: +91 11 2680 2856
Fax: +91 11 2680 3338

C-DOT Campus, Electronics City,
Phase-I, Hosur Road,
Bengaluru - 560 100, India
Phone: +91 80 2511 9001
Fax: +91 80 2511 9601

www.cdot.in

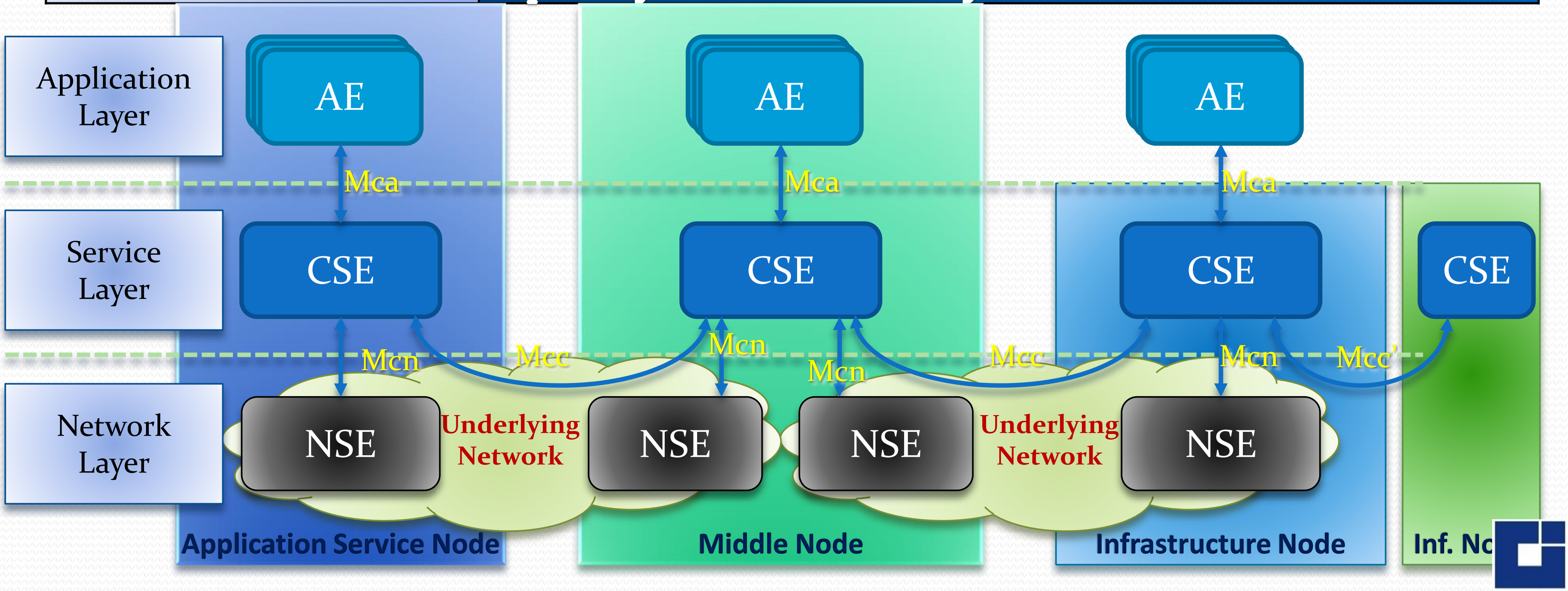
08/18

PQC Use case (encrypted video streaming) using C-DOT's CEM

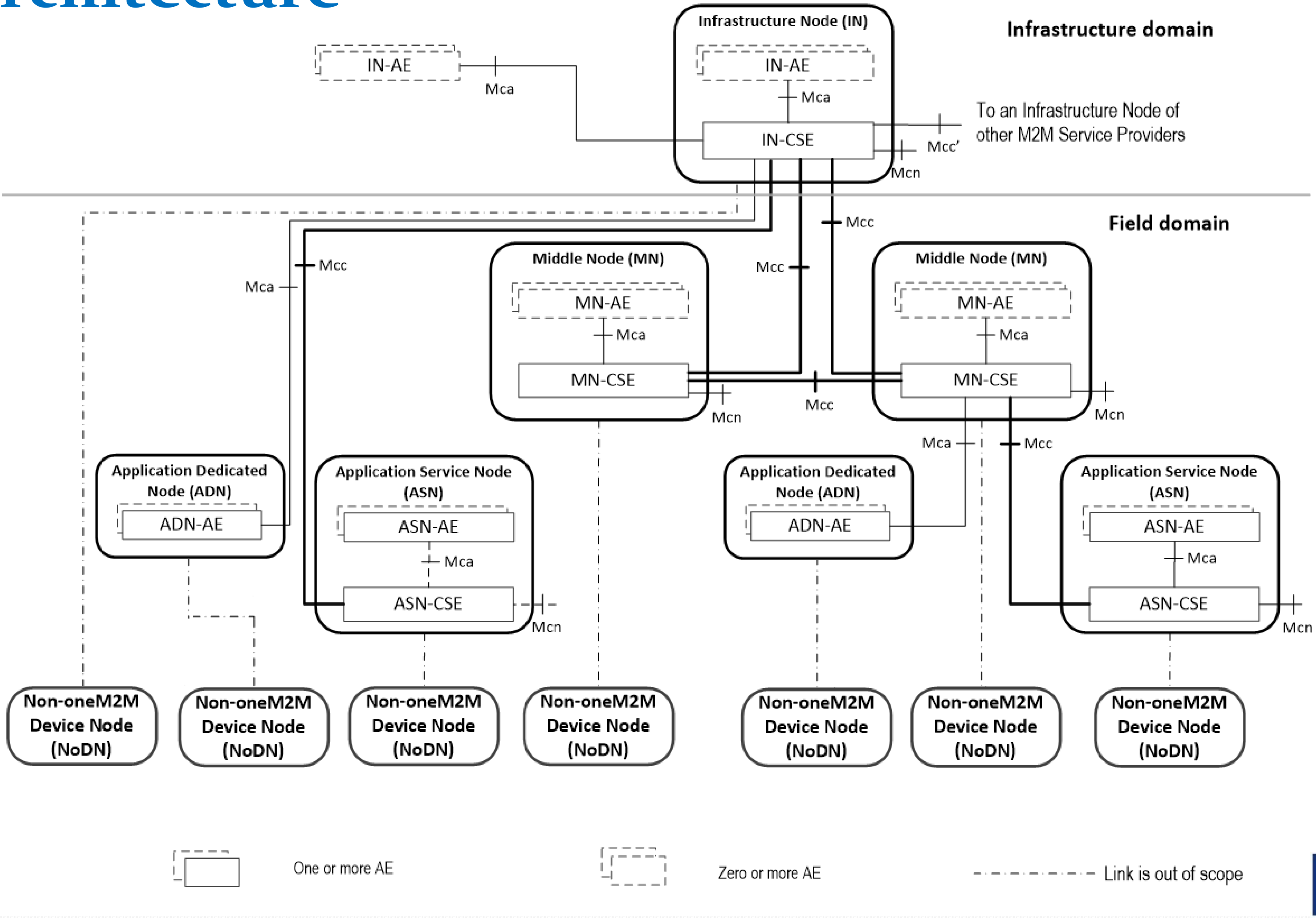


A recall of M2M Architecture

Reference Point	One or more interfaces - Mca, Mcn, Mcc and Mcc' (between 2 service providers)
Common Services Entity	Provides the set of "service functions" that are common to the M2M environments
Application Entity	Provides application logic for the end-to-end M2M solutions
Network Services Entity	Provides services to the CSEs besides the pure data transport
Node	Logical equivalent of a physical (or possibly virtualized, especially on the server side) device



Configurations supported by oneM2M Architecture



Infrastructure Node (IN)
Infrastructure domain
IN-AE
Mca
IN-AE
Mca
IN-CSE
To an Infrastructure Node of other M2M Service Providers
Mcc'
Mcn
Field domain
Mcc
Mcc
Mca
Mcc
Middle Node (MN)
MN-AE
Mca
MN-CSE
Mcn
Mcc
Middle Node (MN)
MN-AE
Mca
MN-CSE
Mcn
Mca
Mcc
Application Dedicated Node (ADN)
ADN-AE
Application Service Node (ASN)
ASN-AE
Mca
ASN-CSE
Mcn
Application Dedicated Node (ADN)
ADN-AE
Application Service Node (ASN)
ASN-AE
Mca
ASN-CSE
Mcn
Non-oneM2M Device Node (NoDN)
Non-oneM2M Device Node (NoDN)
Non-oneM2M Device Node (NoDN)
Non-oneM2M Device Node (NoDN)
Non-oneM2M Device Node (NoDN)
Non-oneM2M Device Node (NoDN)
Non-oneM2M Device Node (NoDN)
One or more AE
Zero or more AE
Link is out of scope

Copyright © C-DOT

Description of Nodes in OneM2M Architecture

Application Dedicated Node (ADN):

An Application Dedicated Node is a Node that contains at least one Application Entity and does not contain a Common Services Entity.Example of physical mapping: an Application Dedicated Node could reside in a constrained M2M Device.

Application Services Node(ASN):

An Application Service Node is a Node that contains one Common Services Entity and contains at least one Application Entity.

Example of physical mapping: an Application Service Node could reside in an M2M Device.

Description of Nodes in OneM2M Architecture

Infrastructure Node (IN):

An Infrastructure Node is a Node that contains one Common Services Entity and contains zero or more Application Entities.

Example of physical mapping: an Infrastructure Node could reside in an M2M Server.

Middle Node (MN):

A Middle Node is a Node that contains one Common Services Entity and contains zero or more Application Entities.

Example of physical mapping: a Middle Node could reside in an M2M Gateway.

Quantum-safe encryption in M2M

- Quantum-safe-encryption offers future-proof security and may be used between various nodes in M2M architecture such as between:
  - NSE and CSE
  - AE and CSE

- C-DOT based Compact Encryptor Module which offers Quantum-safe-hybrid implementation can be used for the same.

Thank You