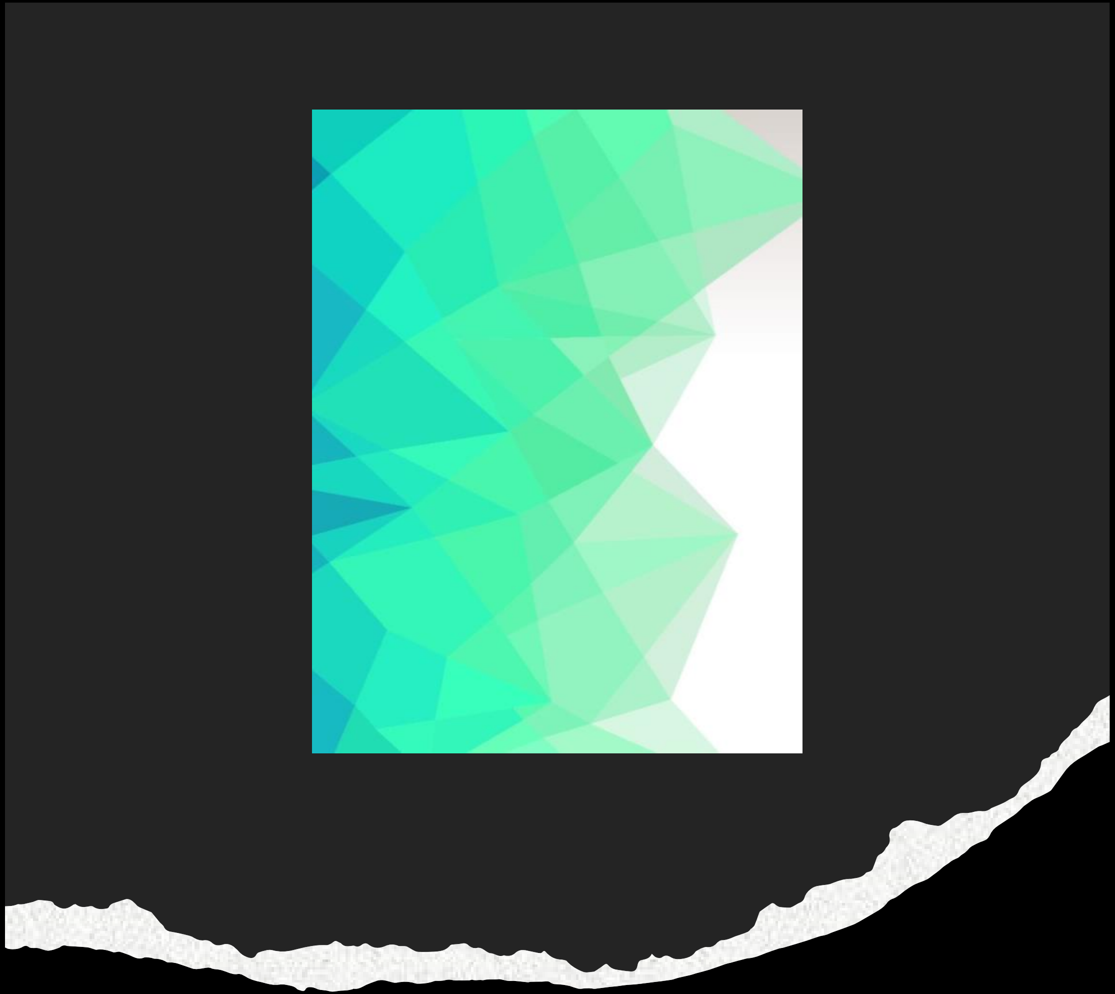
EMBEDDED SEMINAR

- By:
- Nandana Rajan
- Vigneswari
- Prajwal Sundar



Post-Quantum Enabled Cyber-Physical Systems

Cyber-Physical Systems (CPS)

- Cyber-Physical Systems (CPS) are collections of physical and computer components that are integrated with each other to operate a process safely and efficiently. Examples of CPS include industrial control systems, water systems, robotics systems, smart grid,

- Cyber-physical systems (CPS) refer to a new generation of networked embedded systems that bring together sensing, computation, communication, control and actuation in order to sustain a continuous interaction with the physical world (e.g., processes taking place on electrical power grids,

Datagram Transport Layer Security

- Datagram Transport Layer Security (DTLS) is a communications protocol that provides security to datagram-based applications by allowing them to communicate in a way designed to prevent eavesdropping, tampering, or message forgery.
- Datagram Transport Layer Security (DTLS) is a security protocol used by most cyber-physical systems (CPSs). DTLS includes cipher suites for symmetric and public encryption. RSA and elliptic curves (ECC) are used for public key cryptography (PKC) and key exchange.

Security Issue in DTLS

It has been shown that cryptography based on these mathematical problems will be broken in polynomial time by Shor’s algorithm once a large enough quantum computer is built [4]. Integrating quantum resistant (also called post-quantum) cryptography is mandatory to achieve the long-term security of CPSs. When quantum computers become a reality, all the industries and systems that adopt traditional cryptography could be threatened. Thus, DTLS must be updated and integrated with post-quantum cryptography.

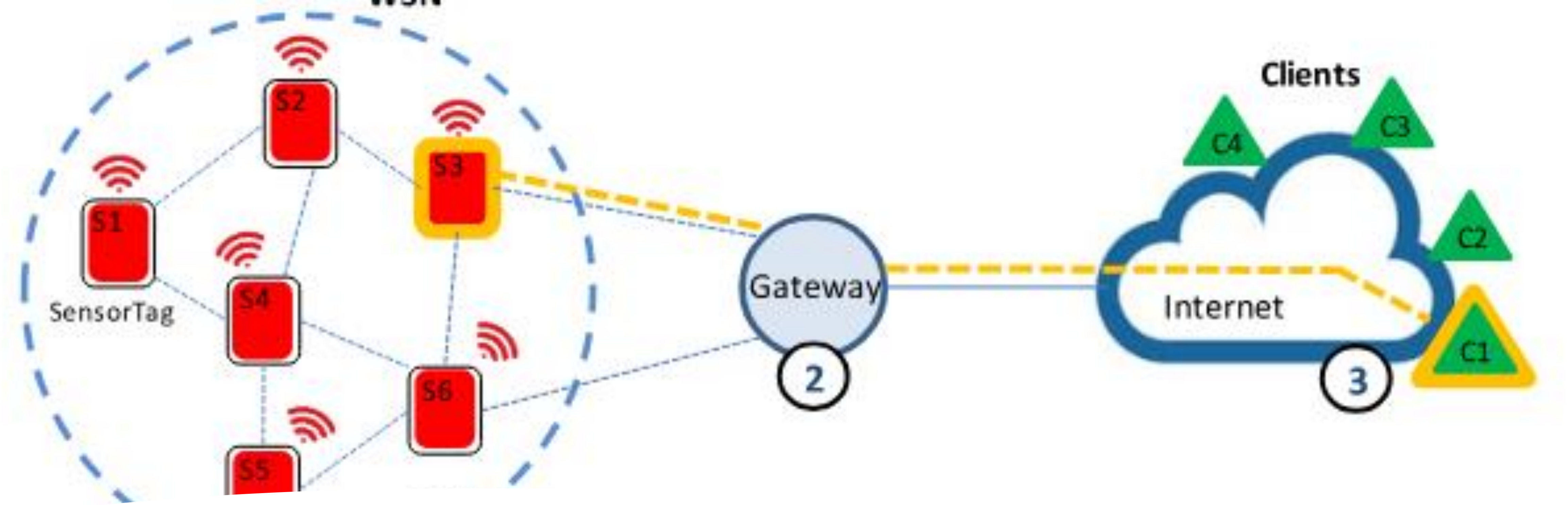
NTRU Cryptosystem

- NTRU is an open-source public-key cryptosystem that uses lattice-based cryptography to encrypt and decrypt data. It is based on the shortest vector problem in a lattice. NTRU is one of the fastest known public key cryptosystems. NTRU is the only post-quantum algorithm which has been standardized in the IEEE Standard Specification for Public Key Cryptographic Techniques.
- In this paper, authors have proposed a post-quantum enhanced DTLS based on NTRU. Our protocol uses NTRU for key transfer among the communication parties.
- Our key transfer protocol includes two stages.

1) Generate a secret and public NTRU keys for each communication entity (sensor nodes, sensing provider/gateway, and clients).

2) Generate and distribute the secret session key.

- This is the first NTRU-enhanced DTLS protocol able to transport session keys avoiding man-in-the-middle and replay attacks.

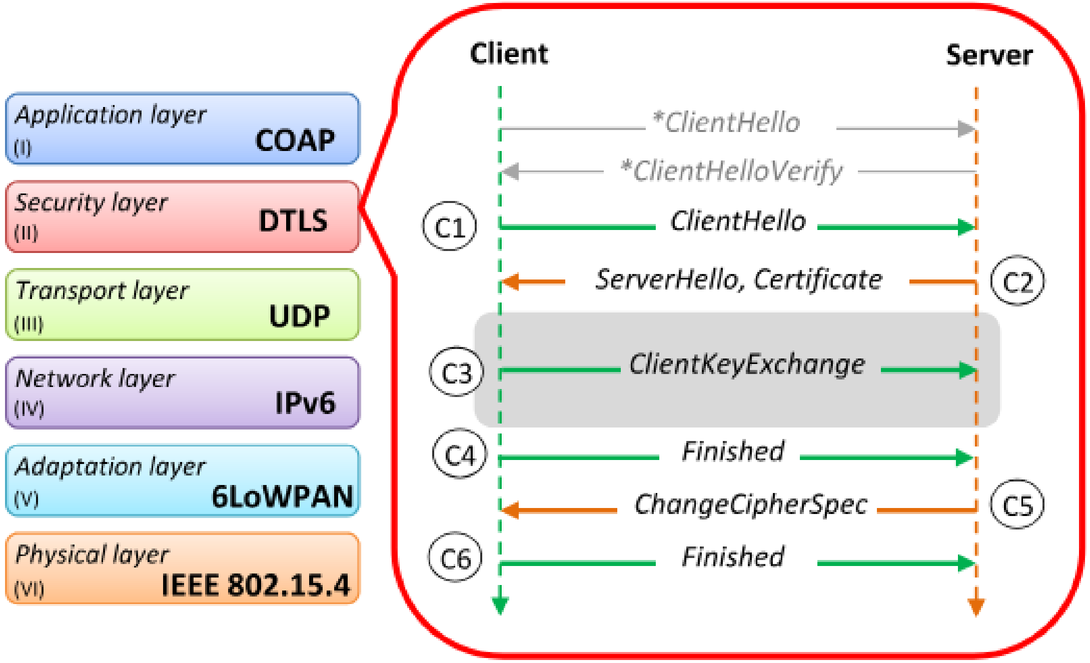


Sensing As a Service (SaaS)

CPSs raises the development of the SAAS (sensing as a service) concept, which allows a sensing provider (sensor owner) to offer its sensor measurement data directly to a world-wide data market composed by clients (sensor data consumers),

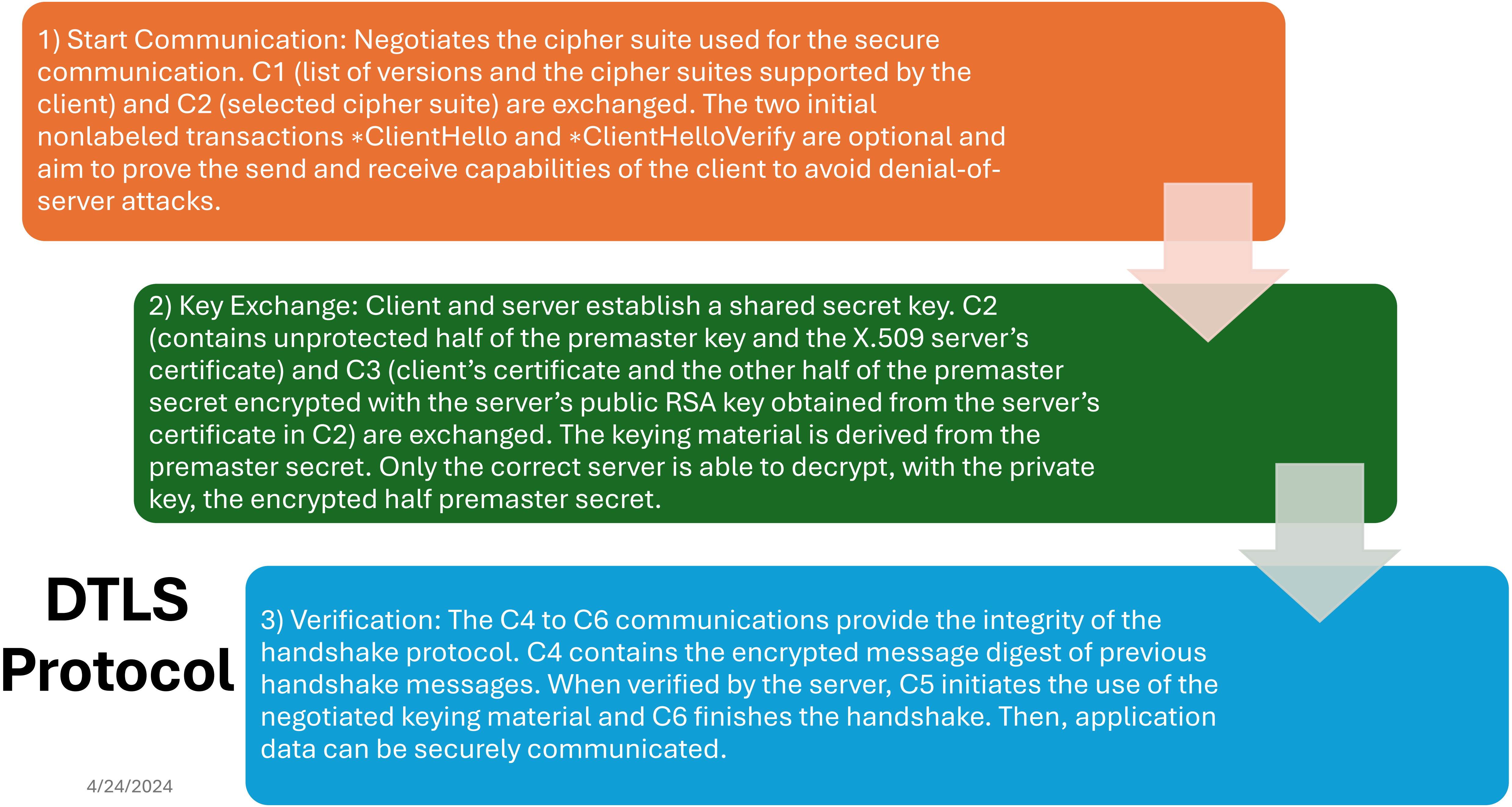
Communication Layers

The Internet engineering task force (IETF) has defined and standardized a set of protocols that promote the hyperconnectivity among different Internet-of-Things (IoT) infrastructures. The six communication layers defined by the IETF are shown in Fig. 2(a). DTLS is integrated in the security layer of IETF to provide end-to-end security. It provides data integrity, secrecy, and authenticity



(a) (b)

DTLS Protocol



1) Start Communication: Negotiates the cipher suite used for the secure communication. C1 (list of versions and the cipher suites supported by the client) and C2 (selected cipher suite) are exchanged. The two initial nonlabeled transactions ∗ClientHello and ∗ClientHelloVerify are optional and aim to prove the send and receive capabilities of the client to avoid denial-of-server attacks.

2) Key Exchange: Client and server establish a shared secret key. C2 (contains unprotected half of the premaster key and the X.509 server's certificate) and C3 (client's certificate and the other half of the premaster secret encrypted with the server's public RSA key obtained from the server's certificate in C2) are exchanged. The keying material is derived from the premaster secret. Only the correct server is able to decrypt, with the private key, the encrypted half premaster secret.

3) Verification: The C4 to C6 communications provide the integrity of the handshake protocol. C4 contains the encrypted message digest of previous handshake messages. When verified by the server, C5 initiates the use of the negotiated keying material and C6 finishes the handshake. Then, application data can be securely communicated.

NTRUEncrypt Cryptosystem

- NTRUEncrypt is a public key cryptosystem based on the shortest vector problem
- NTRUEncrypt is defined by three public parameters (N, p, q), where N is a prime number that defines the degree of R, and gcd(p, q) = 1, where q should be larger than p. For ternary polynomial representation p is set to 3 and q is an integer number power of two q = 2k.
- Three cryptographic operations can be performed by NTRUEncrypt:
- 1) key-generation: Key-generation creates the private key f and the public key h
- 2) encryption: Encryption transforms any plaintext, m, into a ciphertext, e

$$e(x) \equiv r(x) * h(x) + m(x) \bmod q$$

- 3) decryption:

Decryption retrieves the original m from e

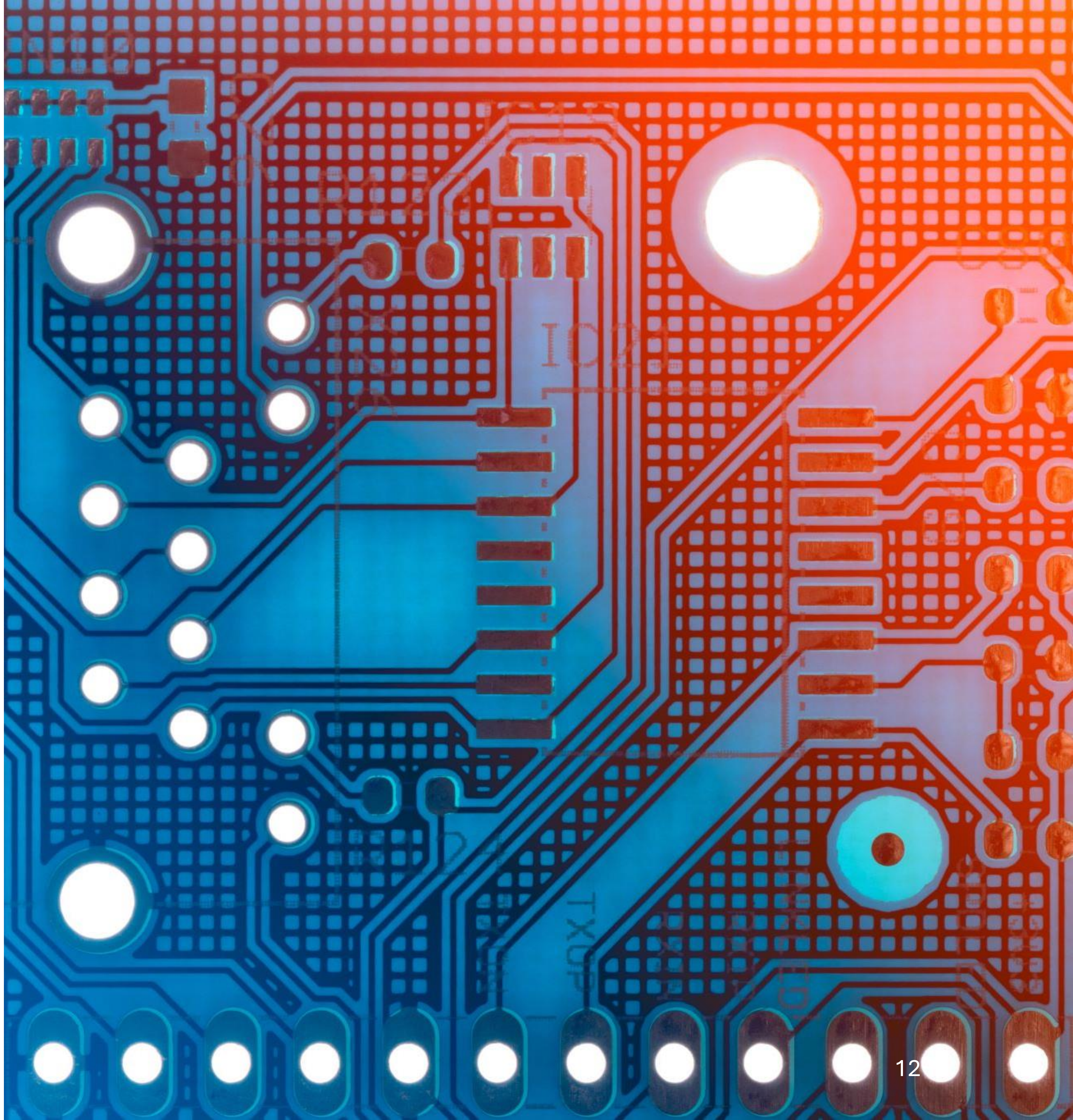
$$m(x) = m(x) - MGF(r(x) * h(x)) \bmod p$$

NTRUE BASED KEY TRANSPORTATION

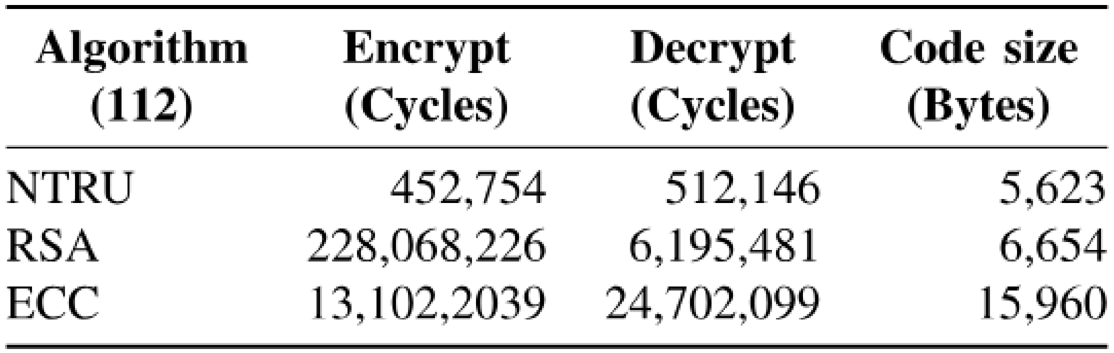
- Before any sensor node SN measurement can be transferred to a client (C), secure channels should be established. Gateways (G) are used as a root of trust and are in charge of generating and transfer the secret shared service session key kv to SN and C.
- NTRU-based key transfer protocol for CPSs is composed by two steps. 1) Establish a public (hs, hg, hc) and secret (ss, sg, sc) NTRU keys for each communication entity (SN, G, C). 2) Generate and distribute session keys (Kv), communicated encrypted by using the public NTRU key of each entity. These steps are integrated into the key exchange step of the DTLS protocol
- Security Analysis Our NTRU-based key transport mechanism is resistant to man-in-the-middle and replay attacks

EXPERIMENTAL RESULTS

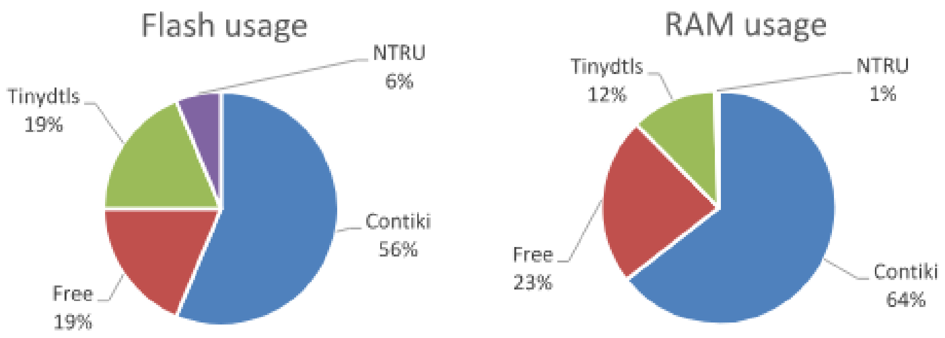
- Wireless Sensor Networks are based on a set of SimpleLink SensorTag,
- 32-bits ARM Cortex-M3 CC2650 Wireless microcontroller,
- 28KB of Flash memory,
- 8KB cache,
- 20KB SRAM
- Each SN integrates ten low-power MEMS sensors that are able to measure the different characteristics of an environment.
- Gateways and Clients are implemented through two Raspberry Pi 3, each based on four 64-bit ARM Cortex-A53 microcontrollers and a Broadcom VideoCore IV GPU, 1GB RAM, wireless LAN 802.11n, Bluetooth 4.0 Low Energy on board and maximal operation frequency of 1.2GHz.
- Contiki OS and Tinydtls were deployed into the SensorTags and Gateway. In addition, CETIC 6LBR, a 6LoWPAN/RPL Contiki application, was deployed into the Gateway to perform the interface between the IPv6 (SensorTags) and IPv4 (Client) domains. Raspbian OS was deployed on the Clients.



RESULTS



Algorithm (112)	Encrypt (Cycles)	Decrypt (Cycles)	Code size (Bytes)
NTRU	452,754	512,146	5,623
RSA	228,068,226	6,195,481	6,654
ECC	13,102,2039	24,702,099	15,960



It shows that NTRU presents a low overhead, being responsible for 5% and 2% of the Flash and RAM occupancy. Contiki OS is the software layer that requires more memory space, with 56% and 64%. However, despite the integration of the full IETF Stack, there is still 19% and 23% of the SN Flash and RAM memories free. Thus, is feasible to integrate post-quantum enhanced DTLS into constrained elements of the CPSs.

CONCLUSION

- Long-term security requirements for the CPSs demand the integration of post-quantum cryptography solutions.
- The IETF has defined DTLS as the de facto security protocol for IoT. Thus, DTLS should be enhanced with post-quantum capabilities.
- For the first time, post-quantum enhanced DTLs was proposed and implemented. A key transport mechanism based on the until now unbroken postquantum algorithm NTRU was proposed.
- Results show that is feasible to integrate this solution into WSN. As DTLS is used for many IoT devices, our solution also can be integrated to many other applications.

Professor Dr Shameedha Begum

THANK YOU!