Evaluating the cost of beyond AES-128 LoRaWAN security

Phithak Thaenkaew*

[phithak.thaenkaew@umons.ac.be]

Bruno Quoitin

Ahmed Meddahi

University of Mons, Belgium

IMT Nord Europe, France

CyberExcellence Day

Salle Académique, Boulevard Dolez 31, 7000 Mons

8 November 2022

UMONS University of Mons

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

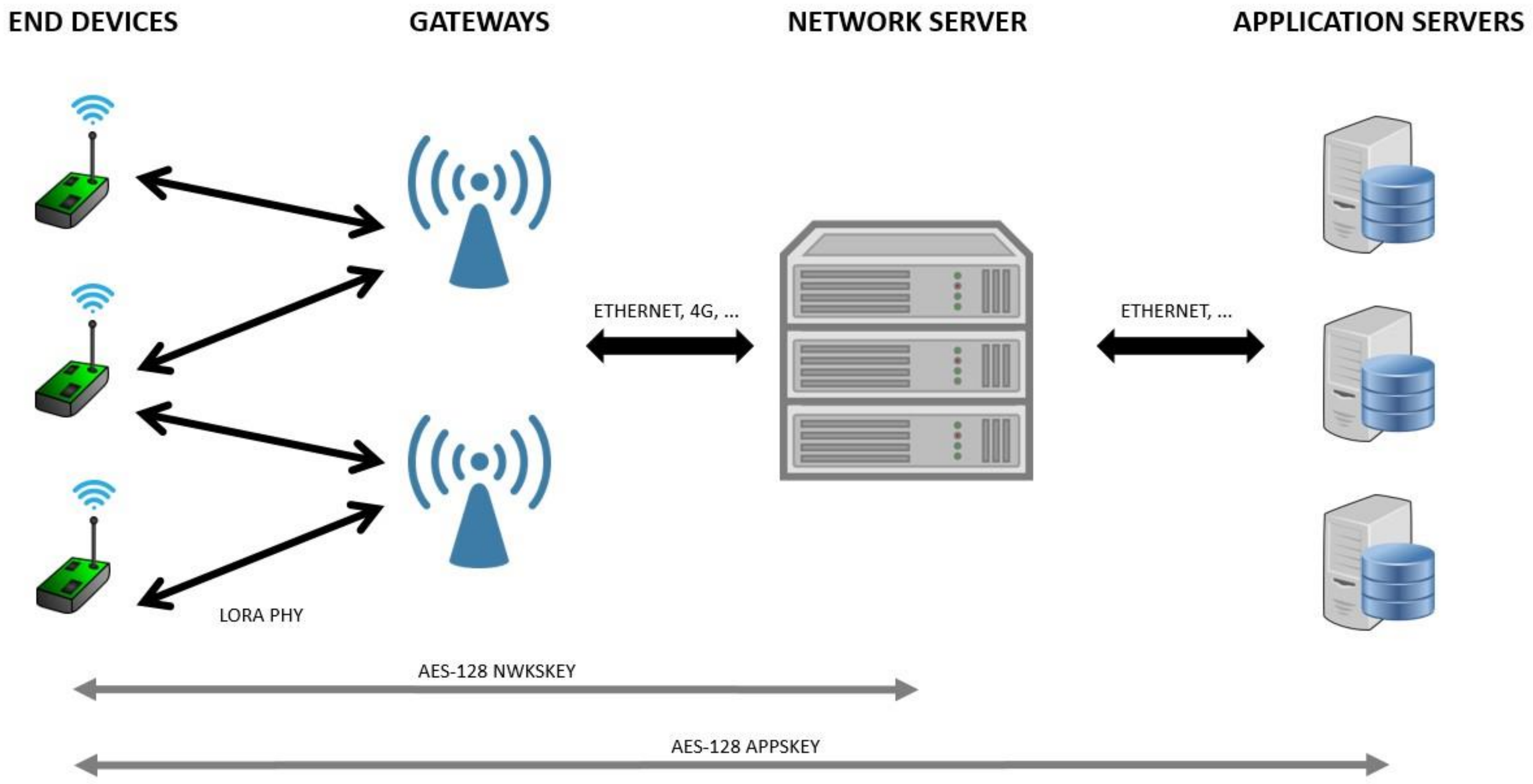
Introduction

- **LoRaWAN** is one of the most popular IoT communication architecture
- All LoRaWAN devices are **resource constrained** and typically consume power from **batteries**
- Strong and sophisticated security mechanism cannot be applied
- LoRaWAN security mechanism is based on PSK **AES-128** encryption
- Using AES with 128-bits keys **might not be strong enough** due to increased computing power available in the future *[F. L. Coman, 2019]*

Problem Statement

- The use of AES on embedded systems and its **impact in terms of resource usage** has been studied in a few papers *[C.-W. Hung, 2018] [L.Casals, 2017]*
- None of them has considered that question in the context of LoRaWAN
- Even though the **power consumption** of LoRaWAN devices has been studied, the impact of **varying the AES key size** has not been considered yet
- In our research, we explore what changes are required in LoRaWAN to make use of **longer AES key sizes** and evaluate experimentally the **impact** on end devices performance in terms of **processing time** and **energy consumption**.

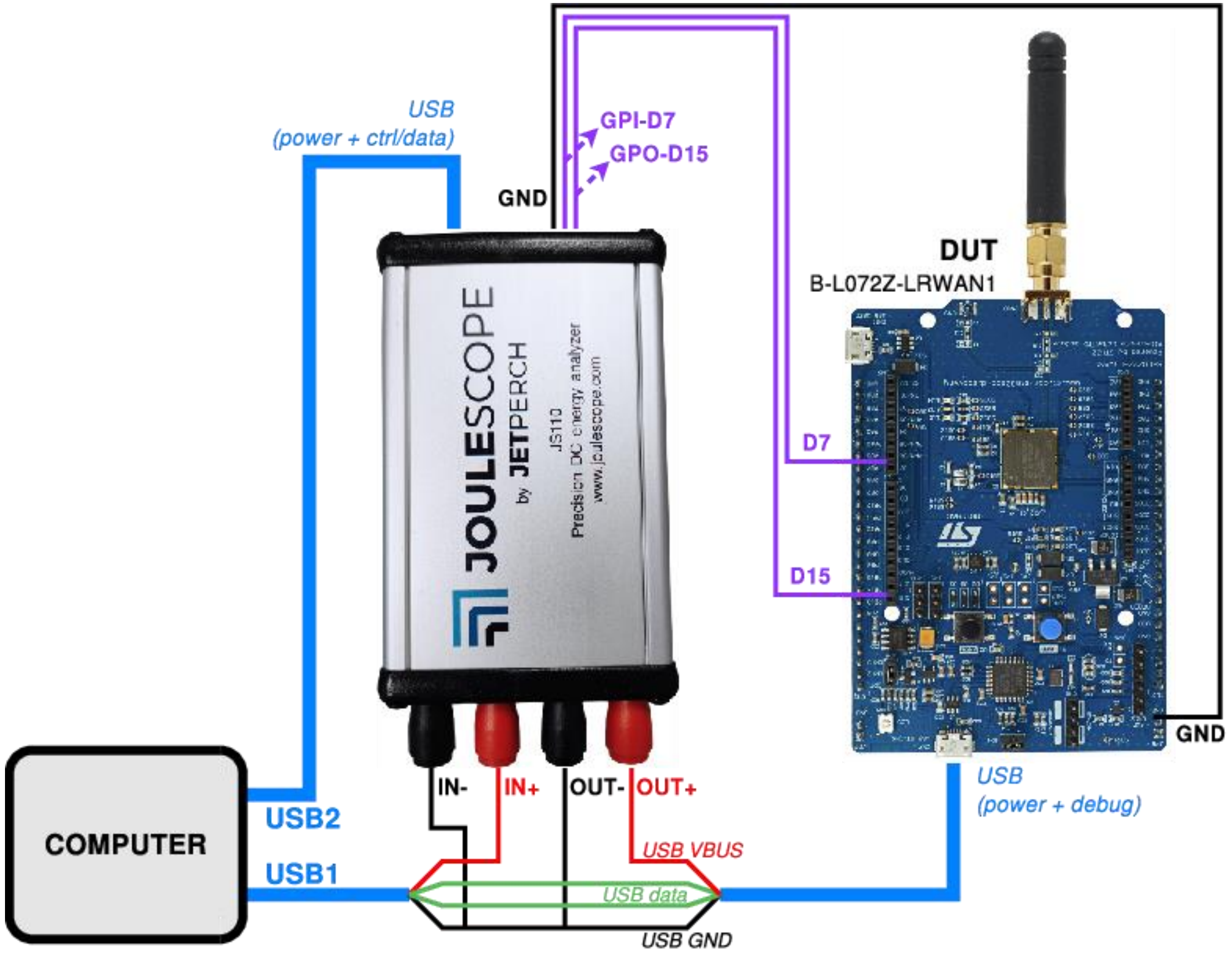
LoRaWAN Network Architecture



AES

- LoRaWAN relies on the **A**dvanced **E**ncryption **S**tandard (**AES**), a symmetric-key block cipher which supports key sizes of 128, 192 and 256 bits
- In LoRaWAN, AES is used for **encryption**, using the **AES-CCM*** scheme but also for computing Message Integrity Code (**MIC**), using **AES-CMAC**
- LoRaWAN security is organized in two layers : 1) Encrypting the message payload thanks to **AES-CCM***, using an **AppSKey** and 2) Using **AES-CMAC** to compute a **MIC** with a **NwkSKey**
- Over-the-Air Activation (**OTAA**) is the preferred activation method for end device authentication, AES is also used in this process

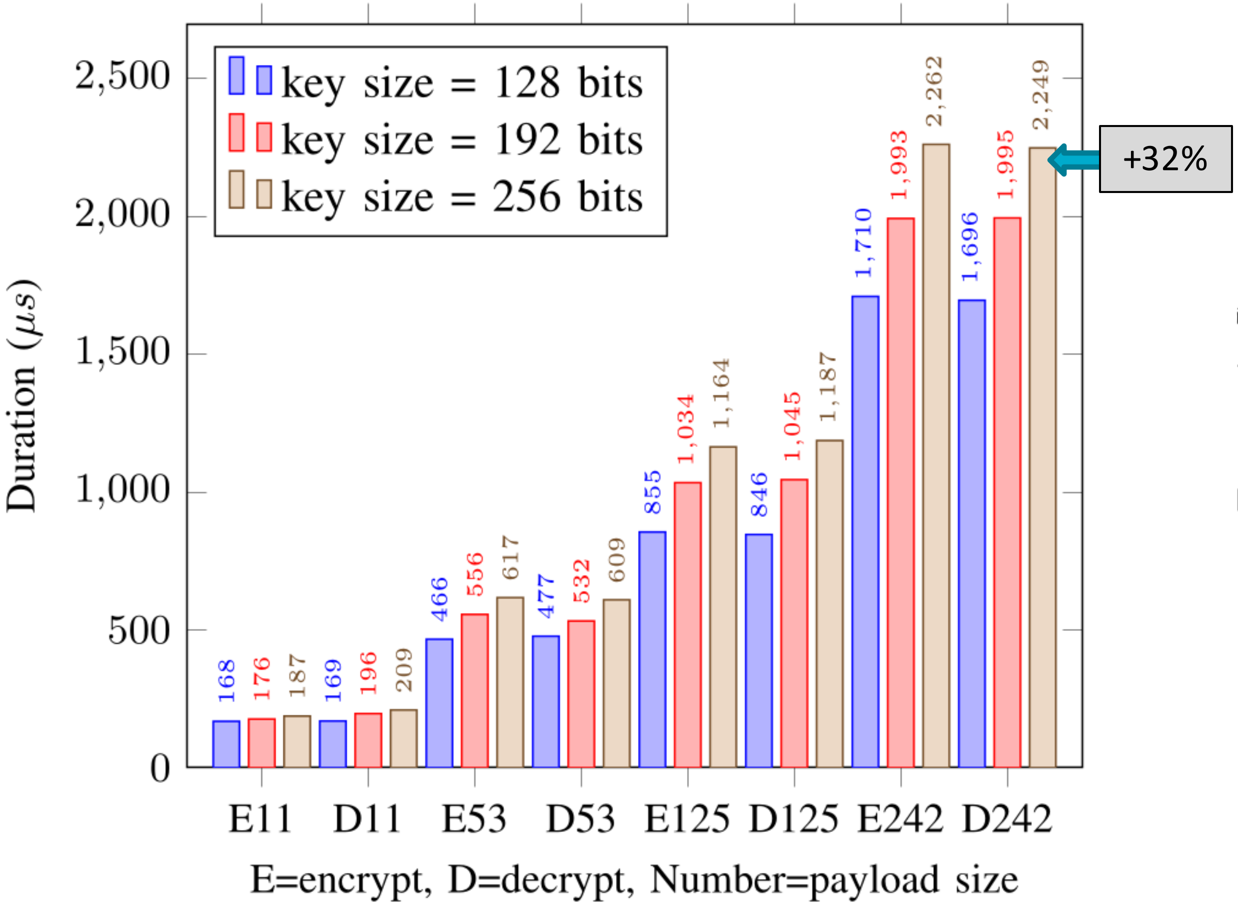
Preliminary Evaluation



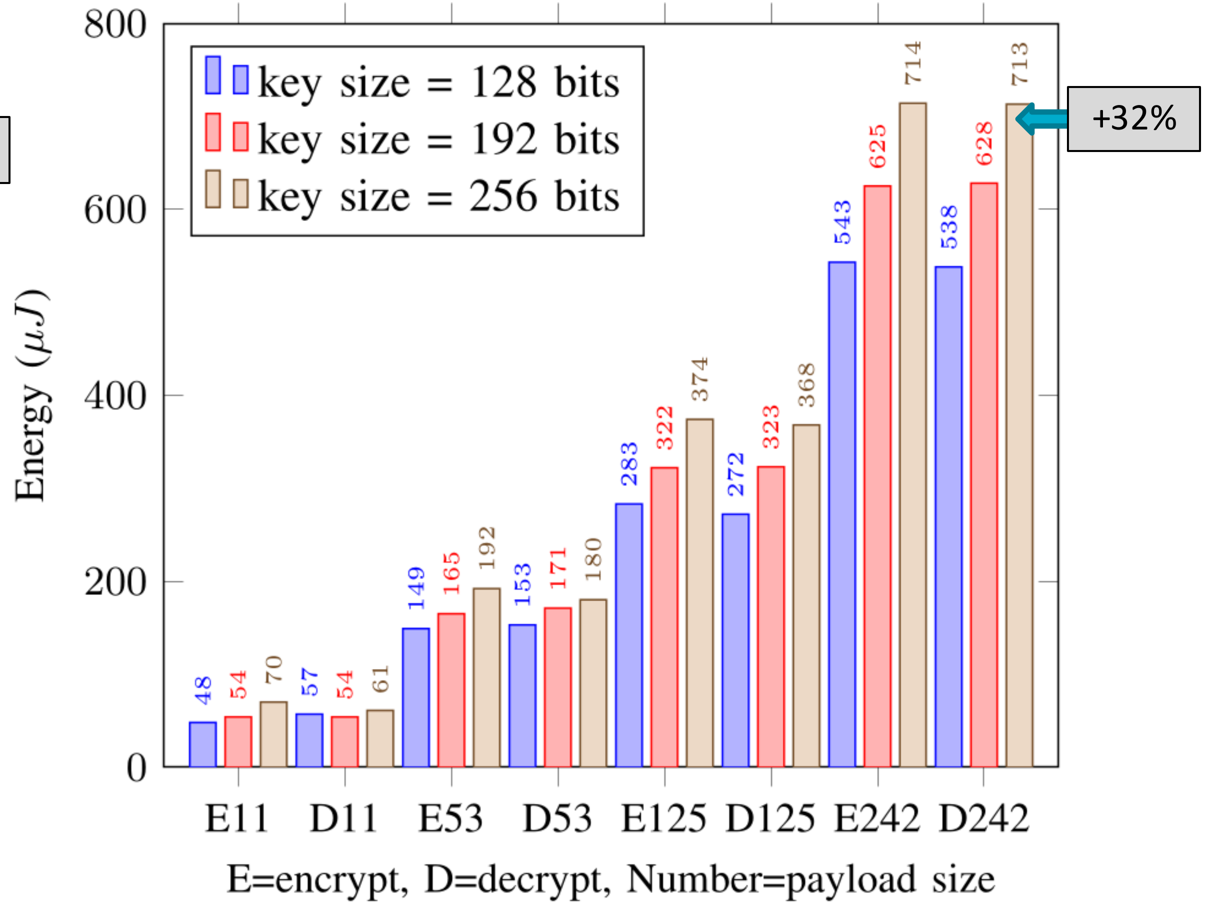
Wiring diagram of the measurement testbed

- Relied on **MBED OS**,
- Library **LoRaMacCrypto**
- 3 functions
  - encrypt_payload (AES-CCM*)
  - decrypt_payload (AES-CCM*)
  - compute_mic (AES-CMAC)
- 3 AES key sizes : 128, 192, 256 bits
- 4 payload sizes : 11, 53, 125, 242 bytes
- Using **JouleScope** for energy consumption measurement
- Run 10 times (use **average** values)

Preliminary Evaluation



Duration of AES encryption and decryption



Energy consumption of AES encryption and decryption

Preliminary Evaluation

	Payload Size			
	11 Bytes	**53 Bytes**	**125 Bytes**	**242 Bytes**
Duration (μs)	621	919	1,353	2,218
Energy (μJ)	186	287	430	692

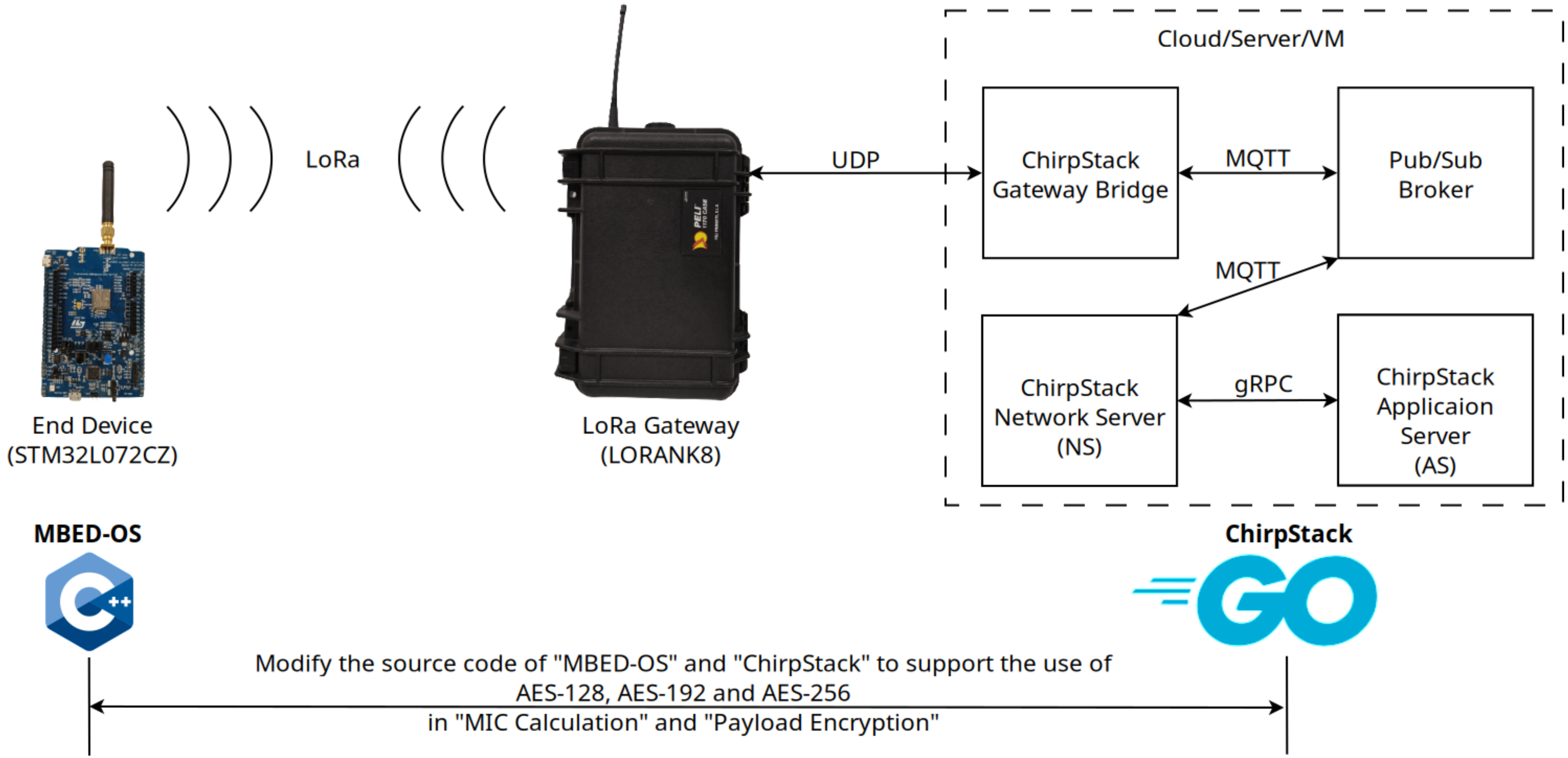
Note: *AES key size 128 bits*

Duration and energy consumption of MIC calculation

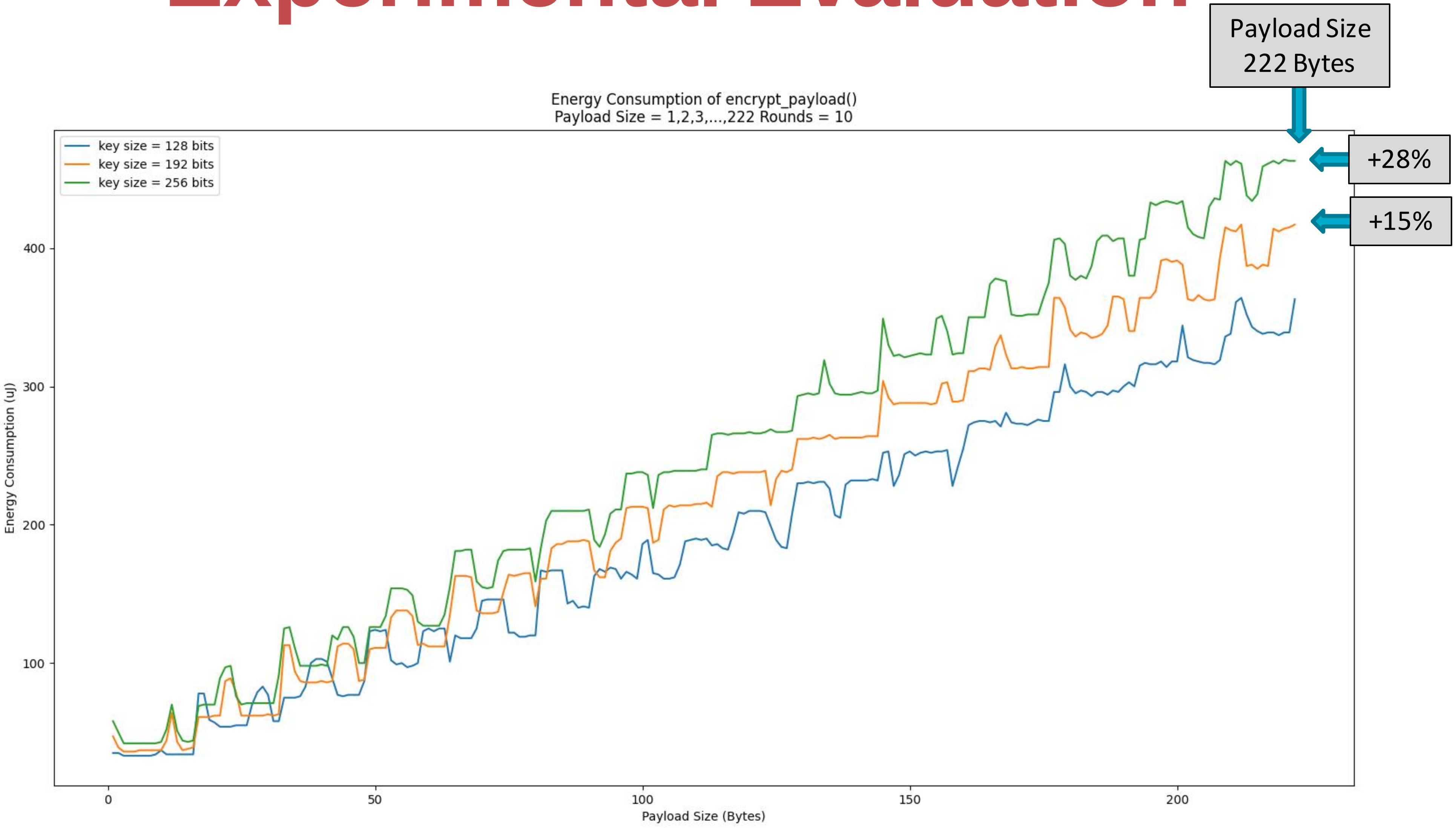
Conclusion

- Our objective was to **evaluate the cost** of using longer AES key size on resource-constrained devices
- From the results, the considered metrics indeed **increase** with key and payload sizes (+32% for payload 242 bytes) but the time dedicated to **payload encryption** (2.25 ms) represents only 2.5% of the **transmission time** (90 ms)
- The **impact is moderate**, making using larger AES key size a **practical solution**
- The **additional energy** is very low compared to the cost of other operations eg. radio communications

Implementation in The Real Environment



Experimental Evaluation



Further Work

- In addition, **stronger** authentication using **asymmetric cryptography** (eg. ECC) would be applied in the activation method or coupled with other security methods such as **fingerprinting**

Thank You

contact

phithak.THAENKAEW@umons.ac.be
bruno.QUOITIN@umons.ac.be
ahmed.MEDDAHI@imt-nord-europe.fr