COMP4DRONES

Framework of Key Enabling Technologies for Safe and Autonomous Drones

WP5-08-ROT Lightweight Cryptography

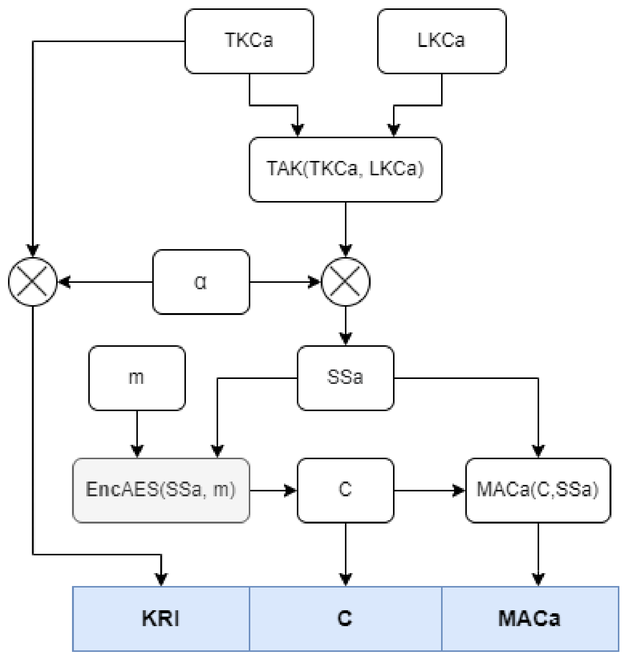
Component description

The **Lightweight Cryptographic** component secures the communication between entities (i.e., drone, rover and infrastructure) through two different modules:

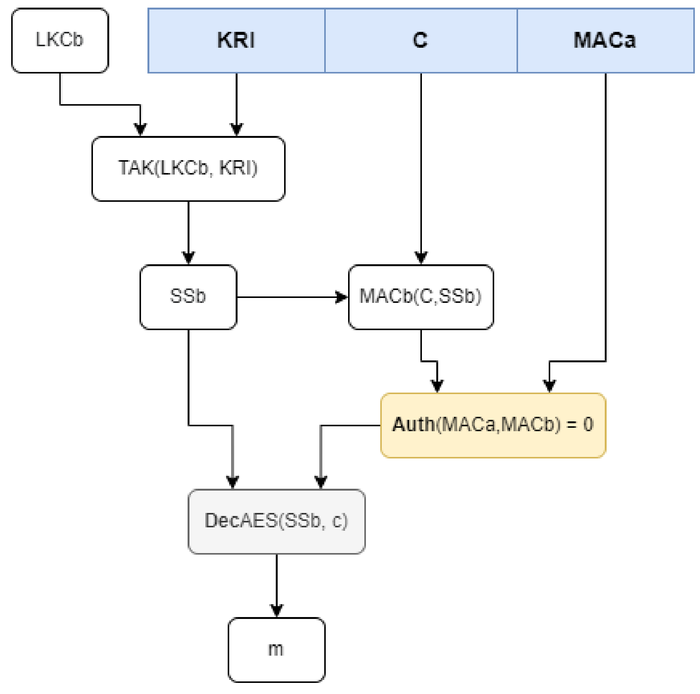
- **Data encryption**: to ensure data privacy and integrity of drone-to-infrastructure and rover-to-infrastructure communication
- **Intrusion detection**: to ensure authentication when the encrypted data was sent by a trusted node

The component is based on **TAKS2** scheme, a network topology-based scheme which provides passive security at link layer along a topology-based authentication with minimal performance overhead.

Encryption



Decryption



The scheme works in two different phases: *encryption* and *decryption*, the second of which implicitly carries out also Intrusion Detection functionality through the authentication operation.

SMART AND PRECISION AGRICULTURE FROM DRONE TO ROVER

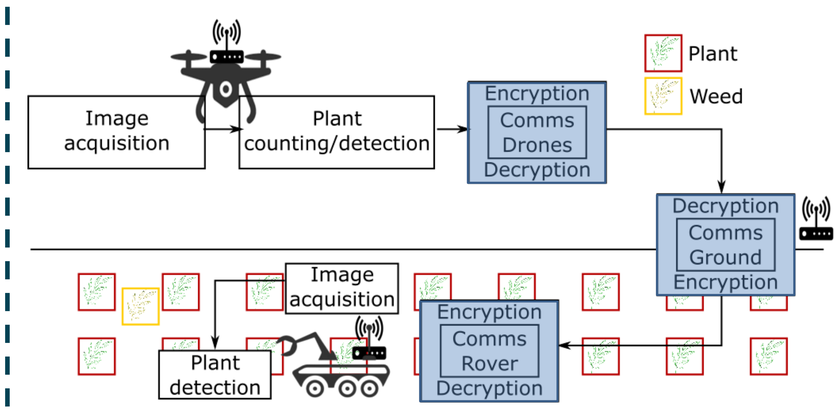
The component operates in the middle between drone and rover communication towards the infrastructure. It has been integrated through components that provide an integrated methodology to implement ready-to-use accelerators from an FPGA-based companion computer, that can be used both in the drone and the rover.

Scenario #1: Non-real-time processing

Scenario #2: Real-time monitoring and inspection

Scenario #3: Cooperative actions for on-field intervention

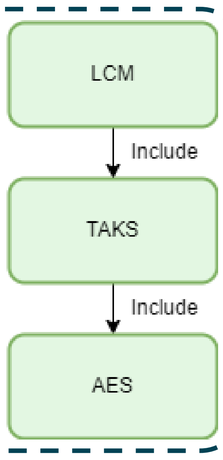
OVERALL SET-UP



Results

The software developed is architecturally composed of three different modules:

- **LCM**: configuration of the nodes and provides encryption and decryption functionalities;
- **TAKS**: performs TAKS, executing the encryption, decryption and authentication functions;
- **AES**: contains the AES standard primitives



Metric	Measured
Communication performance degradation - SW	369us
Communication performance degradation - HW	125us
Number of packets detected as sent from not authorized source.	100%

Encrypt

```
################################## ENCRYPT ##############################

ENCRYPT - PLAINTEXT: COMP4DRONES

ENCRYPT - SOURCE MAC: c627e5cd

ENCRYPT - MESSAGE ENCRYPTED: d54f569b458cd98ae5e8f49dbd31d238

#########################################################################

Encryption took 0.002140 seconds to execute
```

Decrypt

```
################################## DECRYPT ##############################

DECRYPT - CIPHERTEXT: d54f569b458cd98ae5e8f49dbd31d238

DECRYPT - COMPUTED SOURCE MAC: c627e5cd

DECRYPT - SOURCE MAC = COMPUTED MAC

DECRYPT - MESSAGE DECRYPTED: COMP4DRONES

#########################################################################

Decryption took 0.003264 seconds to execute
```

Intrusion Detection

```
################################## DECRYPT ##############################

DECRYPT - CIPHERTEXT: d54f569b458cd98ae5e8f49dbd31d238

DECRYPT - COMPUTED SOURCE MAC: 732e04ac

DECRYPT - SOURCE MAC != COMPUTED MAC

Decryption took 0.001720 seconds to execute


   DECRYPT ERROR
||-----------------------------------------------------------------------||
```


The C4D consortium would like to thank EU commission for funding the ECSEL-JU Comp4Drones project under grant agreement no 826610

https://www.comp4drones.eu/ @ECSEL_C4D