ITMO UNIVERSITY

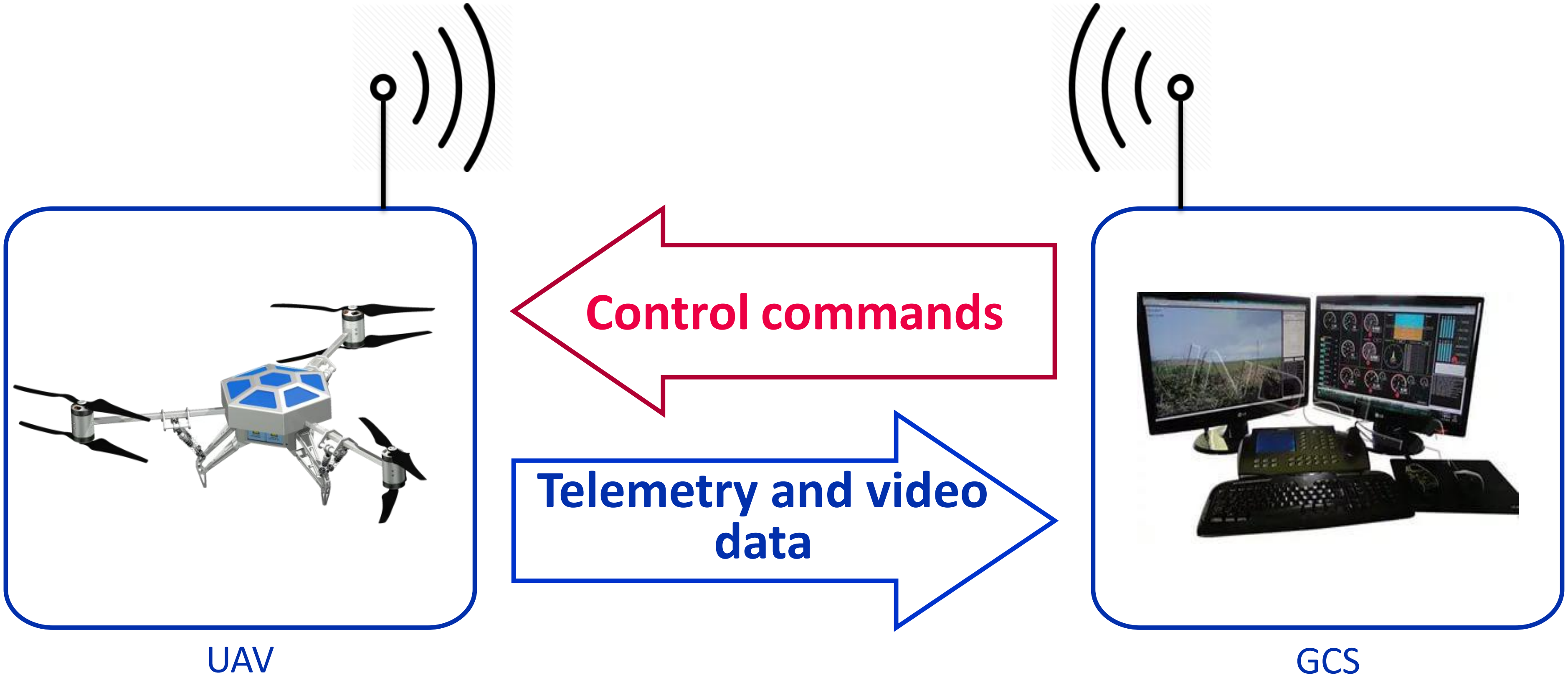
A Method of Securing Data Transferred between Unmanned Aircraft System and Ground Control Station Based on One-Time Pads

Avdonin Ivan, Budko Marina, Budko Mikhail, Grozov Vladimir, Guirik Alexei

Jyvaskyla, Finland

7-11 November 2016

Drone – Ground Control information interaction



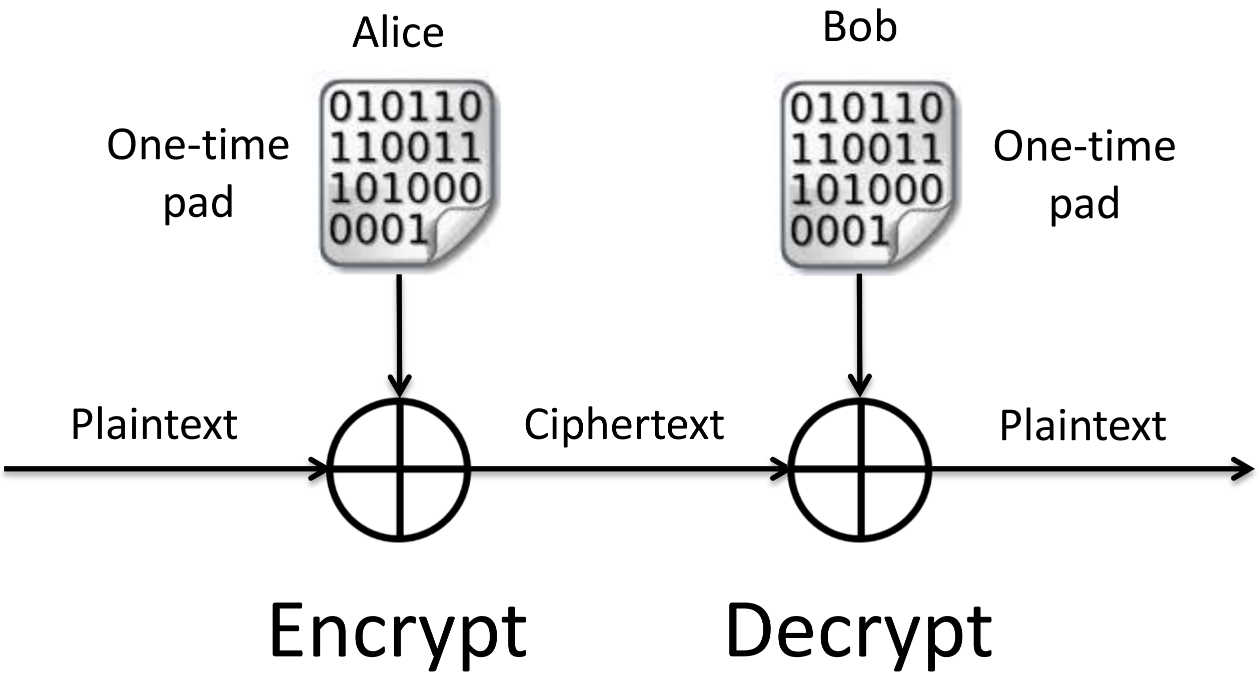
Control commands

Telemetry and video data

UAV

GCS

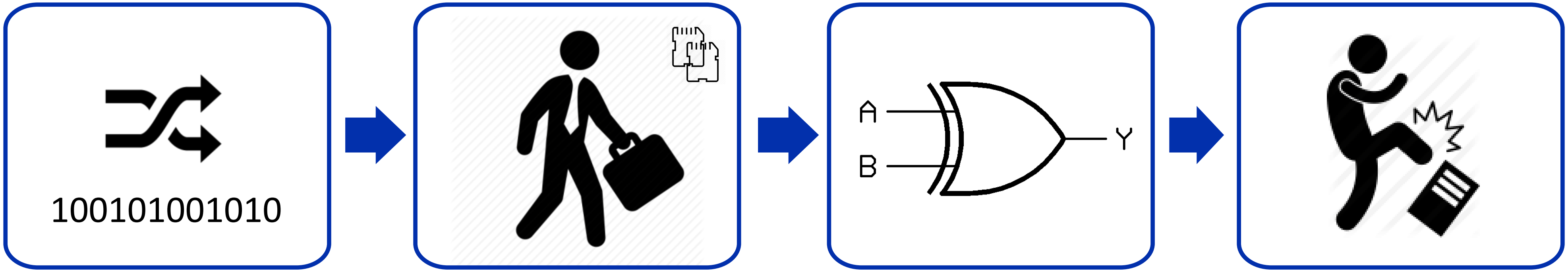
One-time pad (Vernam cypher)



Requirements

- Key sequences are truly random
- OTP pages are used only once
- Plaintext length ≤ key length
- Used page should be destroyed

Practical implementation



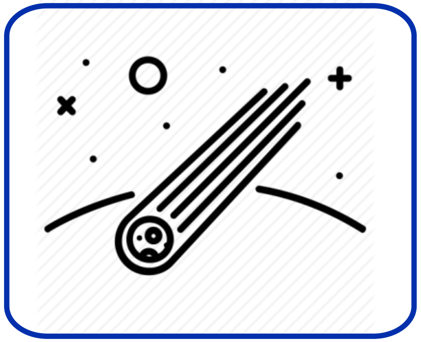
OTP generation

Secure transfer to the message receiver

Encryption/ Decryption

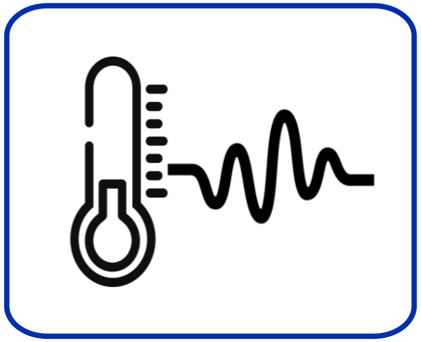
Erasing used OTP pages

Possible sources of a truly random data

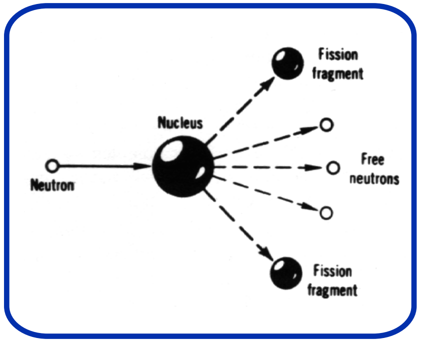


Cosmic radiation

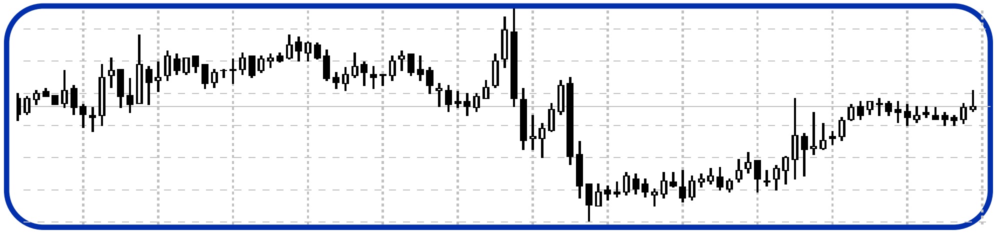
Atmospheric noise



Thermal noise

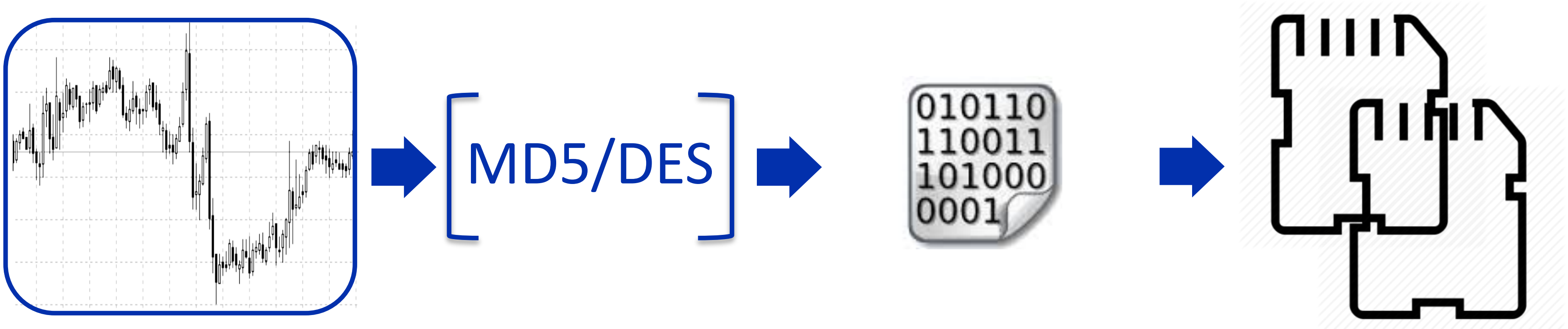


Radioactive decay



Stochastic data

One-time pad generation



MD5/DES

Stochastic data

One-way function adjustment

OTP pages forming

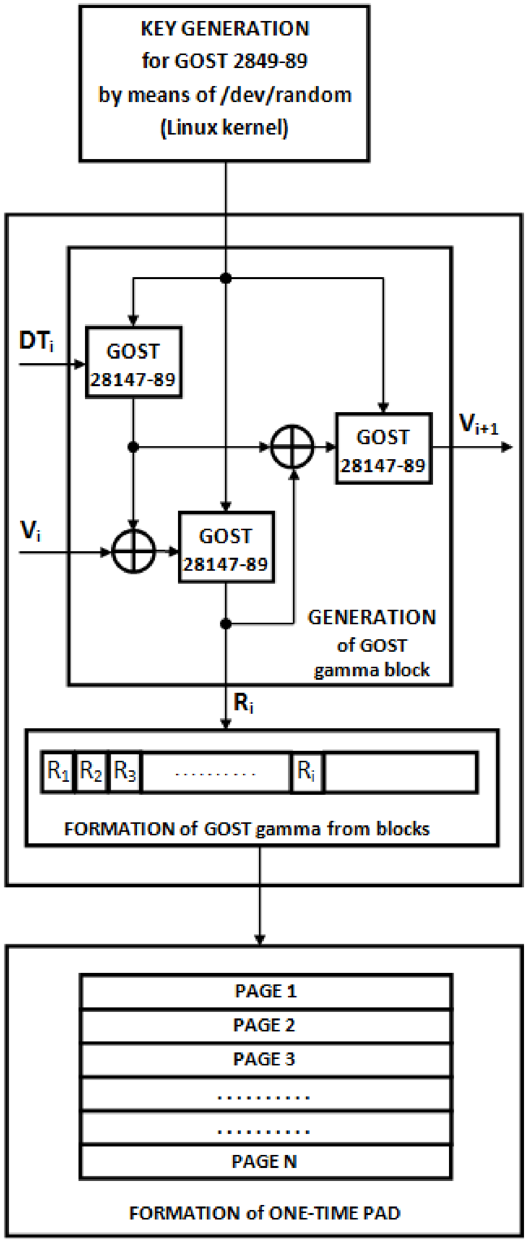
Pseudo-random OTP generation

- Key generation by means of **/dev/random** from Linux kernel
- Generation of **GOST 28147-89** gamma block
- **OTP** pages formation

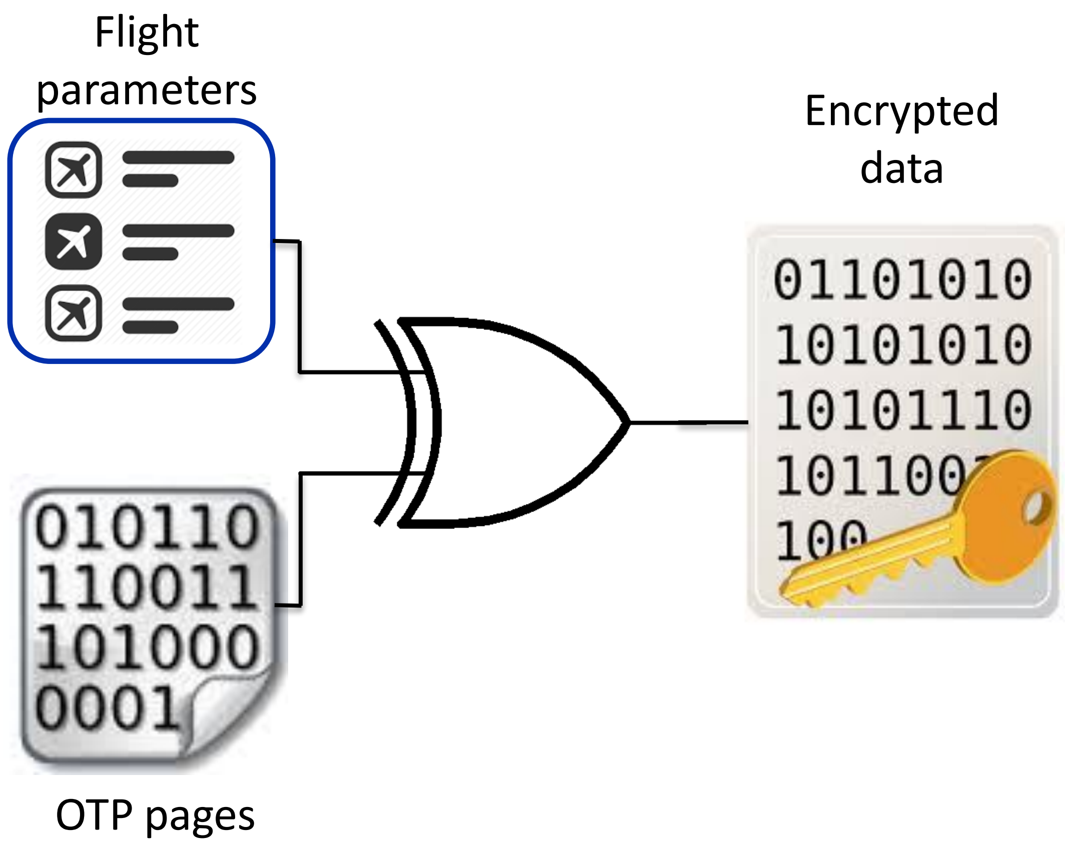
DT_i – current date and value for the beginning of *i* generation step

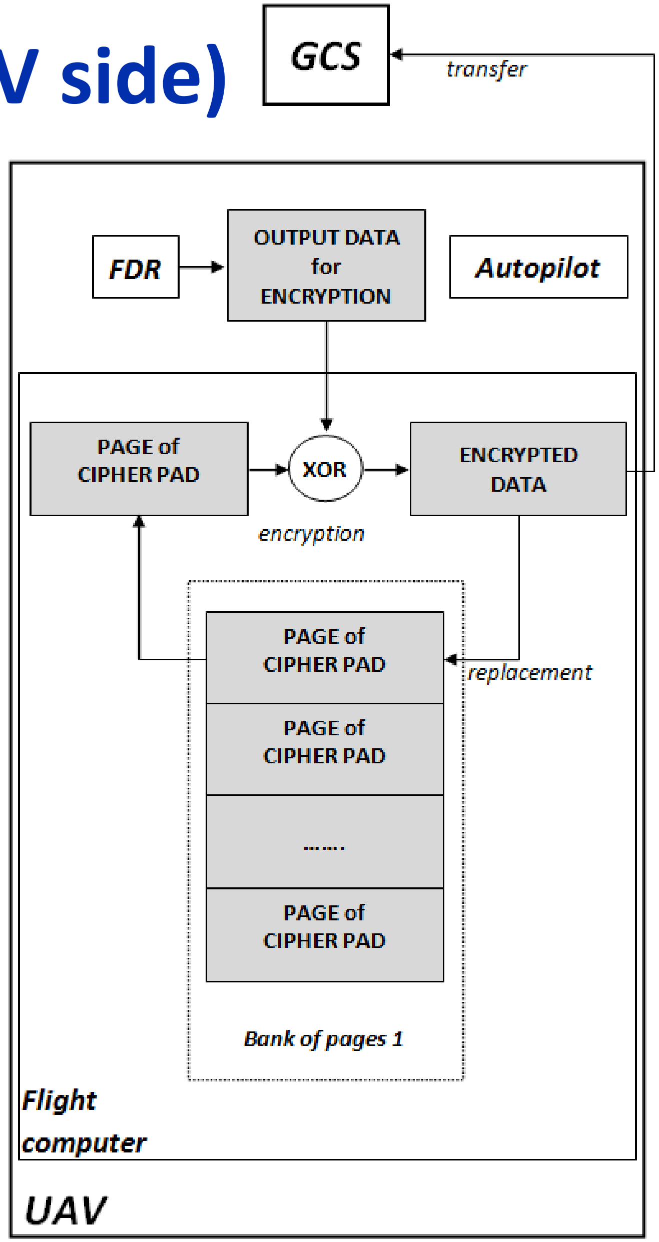
V_i – initial value for *i* generation step

R_i – pseudorandom number created on *i* generation step

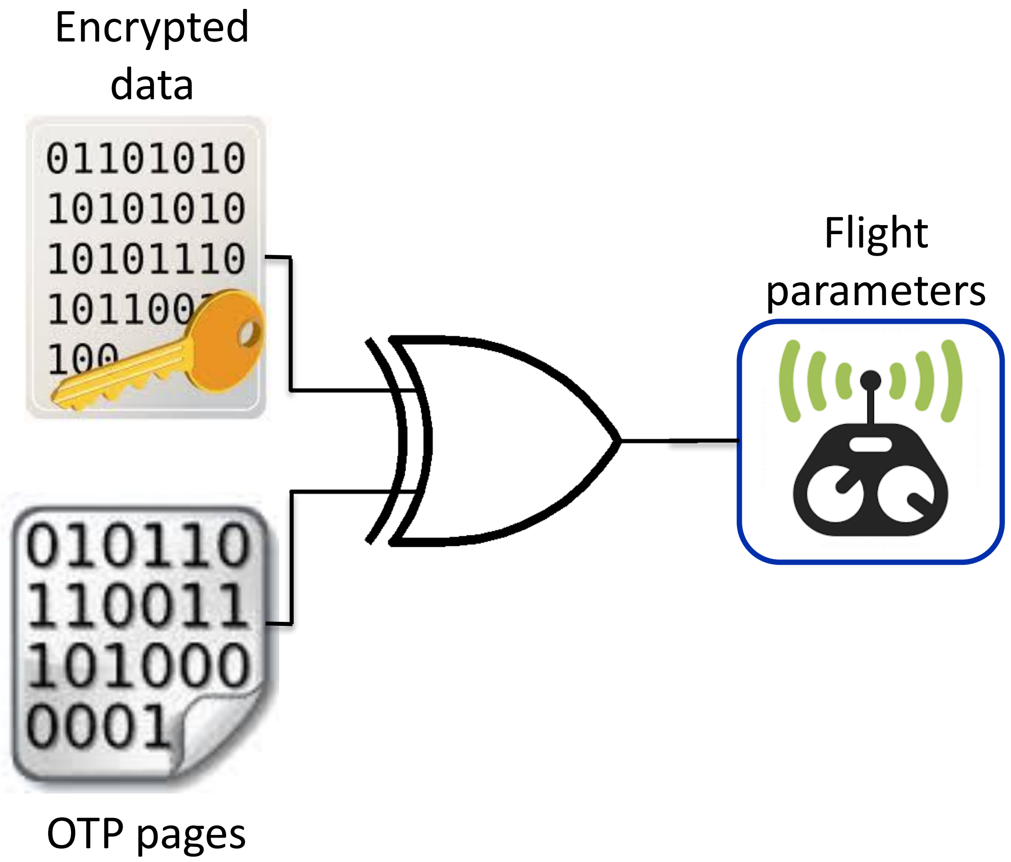


Encryption of telemetry data (UAV side)





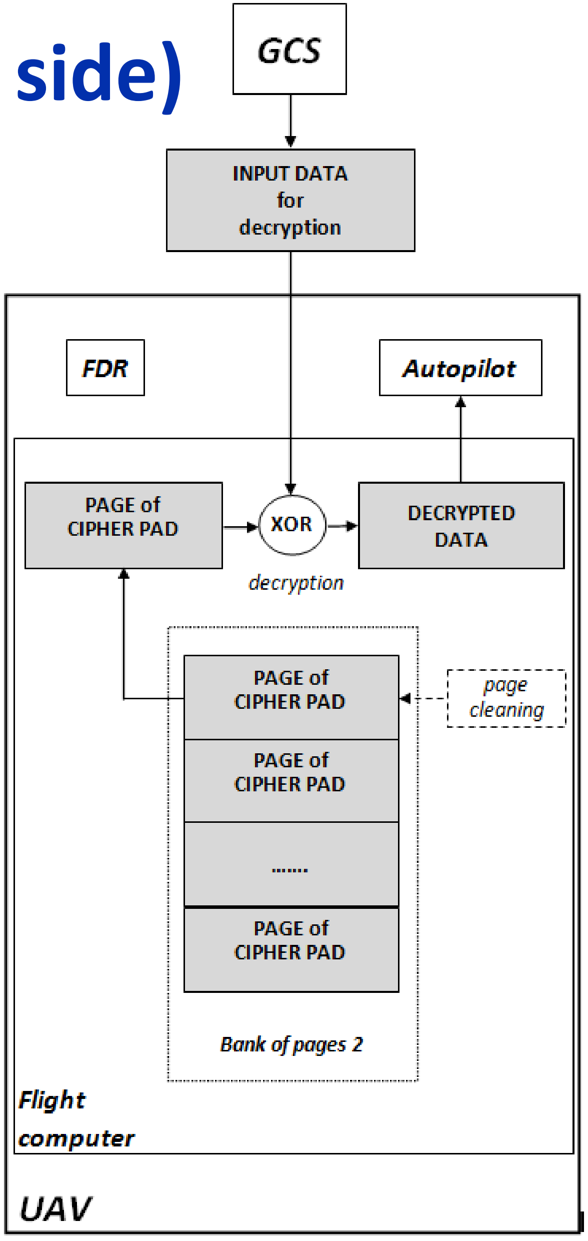
Decryption of command data (UAV side)



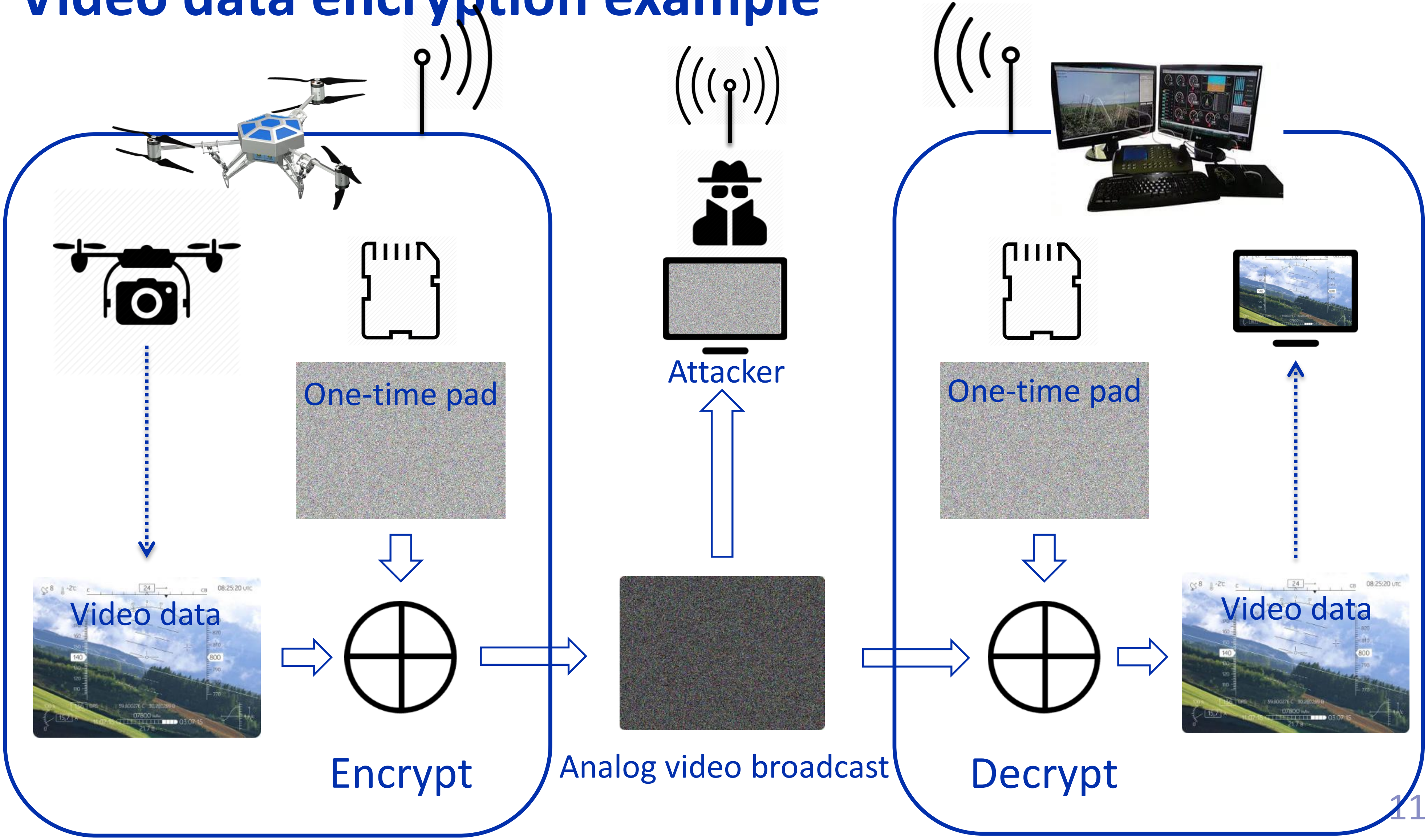
Encrypted data

OTP pages

Flight parameters



Video data encryption example



Video data

One-time pad

Encrypt

Analog video broadcast

Attacker

One-time pad

Video data

Decrypt

Conclusions

- ✓ The proposed method uses such advantages of one-time pad as theoretically proven perfect security, high encryption speed and implementation simplicity.
- ✓ It allows raising data protection level without additional expenses on significant computational capability and high-capacity memory.

Further work

- ✓ Improvement of OTP degree of randomness
- ✓ Solving of data integrity and availability problems
- ✓ Implementation of the method in the University ITMO project of multirotor UAV
- ✓ Integration in MAVLink protocol (Micro Air Vehicle Link), commonly used for micro UAVs communication

ITMO UNIVERSITY

Thank you!