NARODOWA AGENCJA WYMIANY AKADEMICKIEJ

SDSU San Diego State University

Towards Networked Airborne Computing in Uncertain Airspace: A Control and Networking Facilitated Distributed Computing Framework

Poznań Workshop, March 2025

Lightweight Cryptography Algorithms in IoT devices and UAV systems

Poznan University of Technology

Szymon Baliński, BSc

supervisor: PhD DSc. Paweł Śniatała, prof. PP
supervisor: Junfei Xie, Ph.D.
co-supervisor / consultant: Anna Grocholewska-Czuryło, Ph.D.

Poznań Workshop, March 2025

POLITECHNIKA POZNAŃSKA

Agenda

POLITECHNIKA POZNAŃSKA

WHAT IS DRONE?

- Unmanned Aerial Vehicle (UAV)
  - aircraft designed to fly without pilot on-board,
  - controlled remotely or able to fly autonomously thanks to embedded systems, software, sensors and GPS,
- Unmanned Ground Vehicle (UGV),
- Unmanned Underwater Vehicle (UUV);

https://www.wired.com/2017/05/the-physics-of-drones/

POLITECHNIKA POZNAŃSKA

UAV TYPES – DESIGN

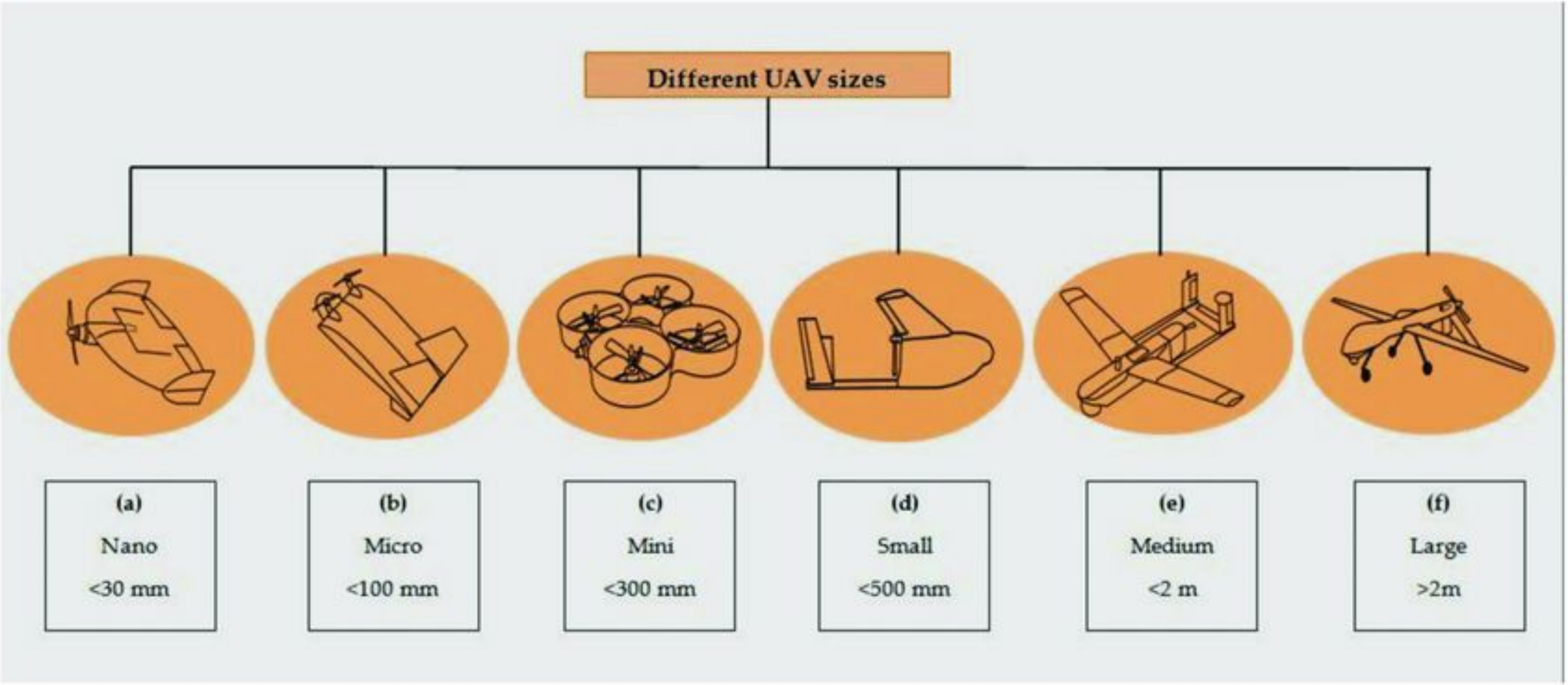
- Rotor-based
- Fixed-wing
- Hybrid

https://geo-jobe.com/drones-uav/multi-rotor-vs-fixed-wing-uav-platforms-considerations-for-evaluating-capabilities-and-limitations/

https://www.researchgate.net/figure/Fixed-wing-UAS-image-source-authors_fig2_318437446

https://www.jouav.com/blog/drone-types.html

UAV TYPES – SIZE



Rahman i in. (2021), „A Comparative Study on Application of Unmanned Aerial Vehicle Systems in Agriculture”

POLITECHNIKA POZNAŃSKA

UAV TYPES – RANGE/ALTITUDE

Category	NASA UAS Class	Weight (in kg)	Normal Operating Altitude (in m)	Mission Radius, Range (in Km)	Typical Endurance (in hrs)	Payload (in kg)	Available UAV Models in Market
Micro	sUAS Class I	<2	<140	5	<1	<1	DJI Spark, DJI Mavic, Parrot Bebop2
Mini		2–25	<1000	25	2–8	<10	DJI Matrice600, DJI Inspire2, Airborne Vanguard
Small		25–150	<1700	50	4–12	<50	AAI Shadow 200, Scorpion 3 Hoverbike
Medium	Class II	150–600	<3300	200–500	8–20	<200	Griff 300, Ehang 216
Large/Tactical	Class III	>600	>3300	>1000	>20	>200	Boeing X-45A UCAV

Lykou, Moustakas, i Gritzalis (2020), „Defending Airports from UAS”.

POLITECHNIKA POZNAŃSKA

UAV TYPES – APPLICATION AREA

1. **Military**
   Use advanced, encrypted communication channels with the highest level of security, such as AES and military protocols.

2. **Commercial**
   Varying levels of encryption depending on the application. High security for critical infrastructure inspections, medium for marketing and photography.

3. **Recreational (Hobby) / Toy**
   No or very low encryption, simple radio connections (2.4 GHz or 5.8 GHz). Examples: Syma X5C, Holy Stone HS210

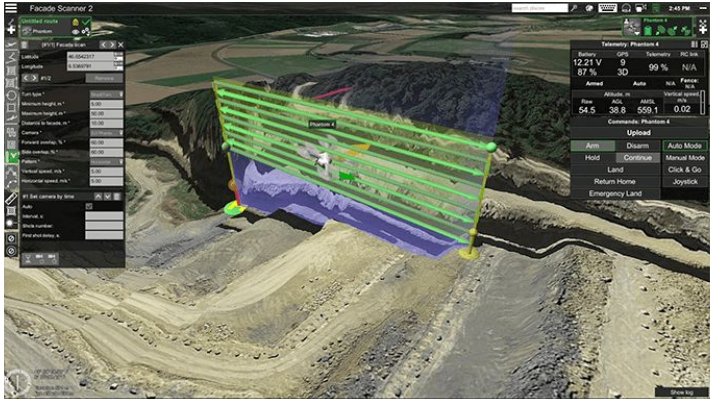
UAV – SAMPLE APPLICATIONS (I)

- photography and filmmaking,
- agriculture,
- rescue and safety;

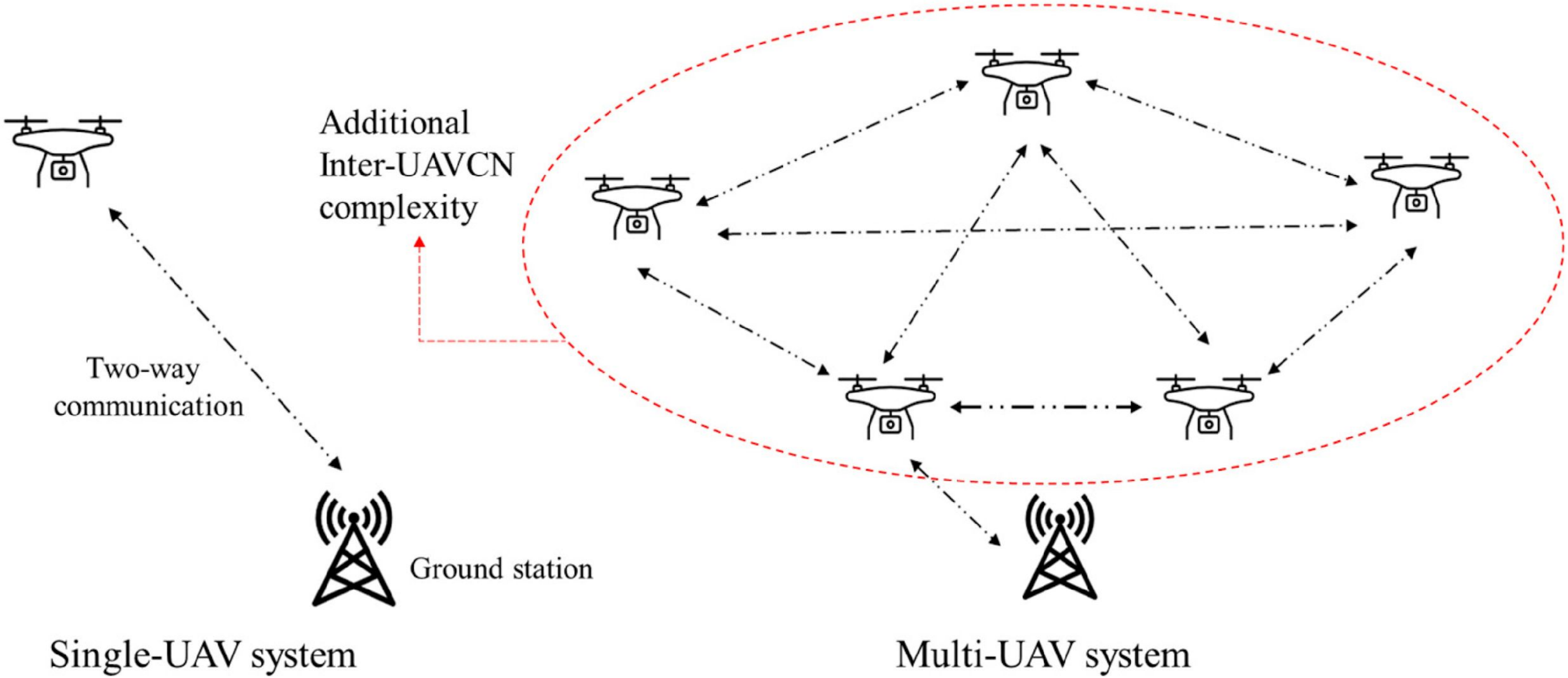
POLITECHNIKA POZNAŃSKA

UAV – SAMPLE APPLICATIONS (II)

- inspections and monitoring,
- logistics and deliveries,
- military;



MULTI-UAV VS SINGLE-UAV (I)



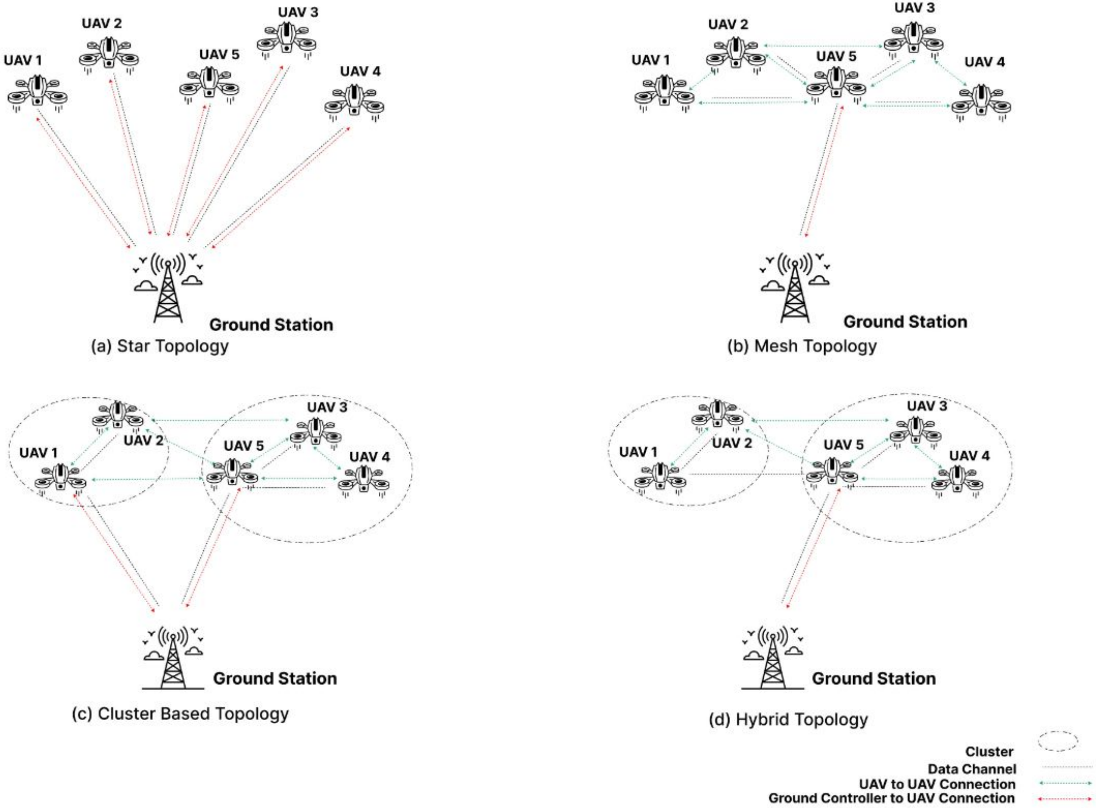
Afrin i in. (2024), „Advancements in UAV-Enabled Intelligent Transportation Systems".

MULTI-UAV VS SINGLE-UAV (II)

Feature	Multi-UAV	Single-UAV
Scalability	High	Limited
Antenna	Directional	Omni-directional
mission speed	Fast	Slow
Required bandwidth	Medium	High
Control complexity	High	Low
Failure effect	System can reconfigure	Mission fails
Topology	Direct, and simple connection	Complex topology
Survivability	High	Poor
Heterogeneous configuration	Applicable	Inapplicable
Coverage area	Large	Small

Al-Absi i in. (2021), „Moving Ad Hoc Networks—A Comparative Study”.

NETWORK TOPOLOGIES (I)



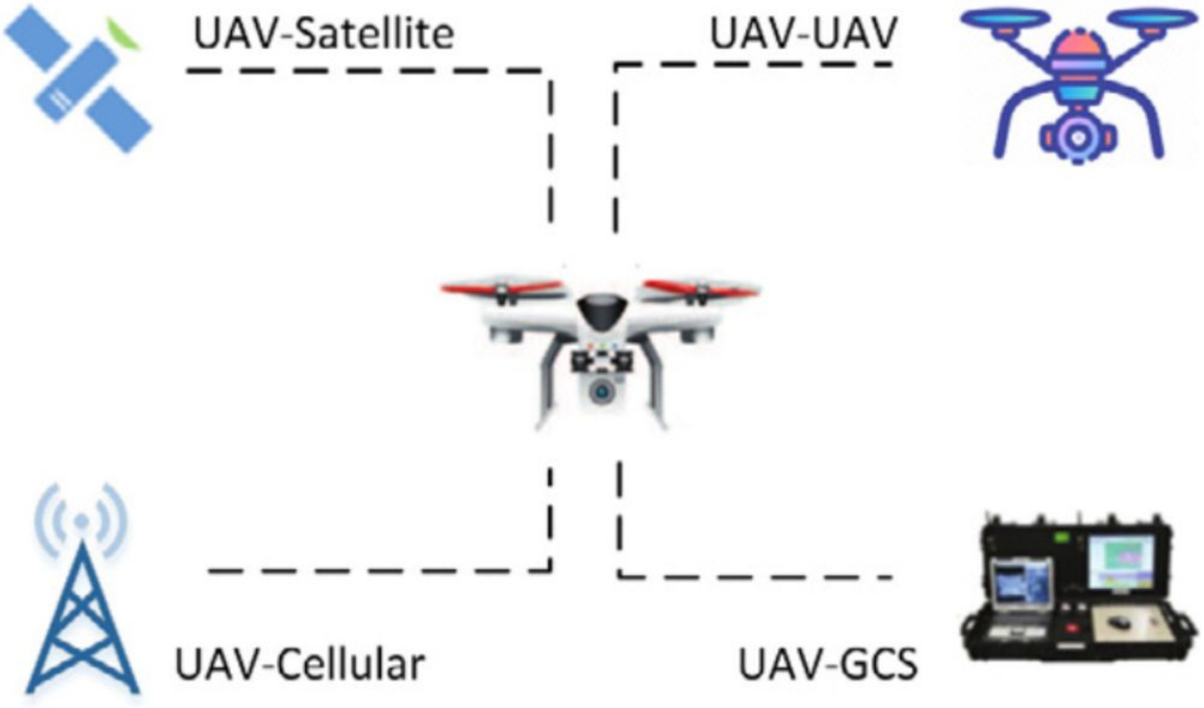
Mansoor i in. (2023), „A Fresh Look at Routing Protocols in Unmanned Aerial Vehicular Networks".

NETWORK TOPOLOGIES (II)

Star Network	Mesh Network
Point-to-point	Multi-point to multi-point
Central control point present	Infrastructure based may have a control center, Ad hoc has no central control center
Infrastructure based	Infrastructure based or Ad hoc
Not self configuring	Self configuring
Single hop from node to central point	Multi-hop communication
Devices cannot move freely	In ad hoc devices are autonomous and free to move. In infrastructure based movement is restricted around the control center
Links between nodes and central points are configured	Inter node links are intermittent
Nodes communicated through central controller	Nodes relay traffic for other nodes
Scalable	Not scalable

Gupta, Jain, i Vaszkun (2016), „Survey of Important Issues in UAV Communication Networks”.

COMMUNICATION METHODS (I)



Bai, Hu, i Wang (2024), „A Survey on Unmanned Aerial Systems Cybersecurity”

POLITECHNIKA POZNAŃSKA

COMMUNICATION METHODS (II)

- Wi-Fi networks:
  - short-range communication between GS and UAV(s),
- cellular networks:
  - long-range communication between GS and UAV(s),
- satellite networks:
  - global communication coverage for UAV(s);

Madhuvanthi T., Revathi A. (2024), „A Survey on UAV Network for Secure Communication and Attack Detection”

ESP32 (I)

- ESP32 is a popular microcontroller developed by Espressif Systems.
- It features built-in Wi-Fi and Bluetooth, making it ideal for IoT projects.
- Energy-efficient and available in different versions (e.g., ESP32-WROOM-32, ESP32-S3).
- Can be programmed using Arduino IDE, MicroPython, ESP-IDF.
- Includes multiple interfaces: GPIO, SPI, I2C, PWM, ADC, DAC, UART.

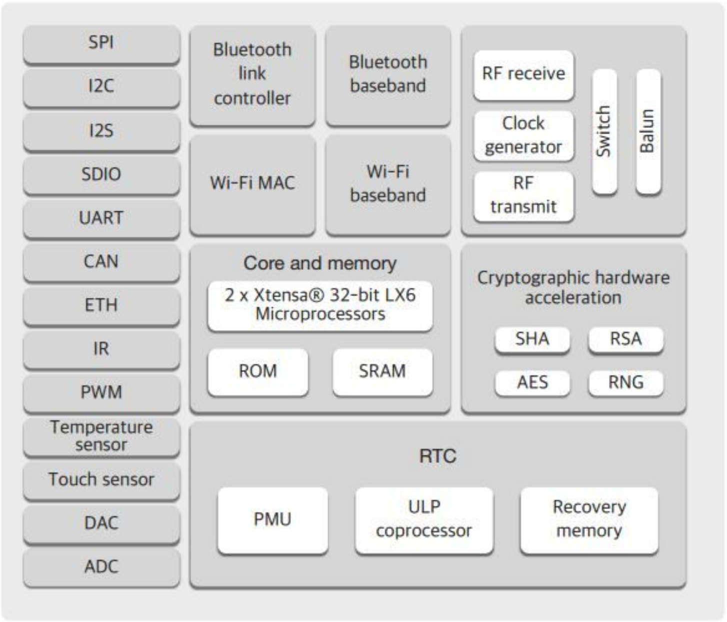
ESP32 (II)

Some of the most common uses of the ESP32 include:

- IoT (Internet of Things) Devices
- Drones
    - Flight control assistance
    - Real-time telemetry
    - FPV (First-Person View) Systems
    - Remote control via Wi-Fi/Bluetooth
- Robotics
- Home Automation
- Wearable Devices

Key Features of ESP32

- Dual-core processor (Xtensa LX6, up to 240 MHz)
- Supports 2.4 GHz Wi-Fi and Bluetooth BLE & Classic
- Low power consumption (Deep Sleep, power-saving modes)
- Multiple I/O pins – over 30 for controlling external devices
- Supports various communication protocols (SPI, I2C, UART, CAN)
- Easy to program with Arduino IDE and MicroPython
- Built-in ADC/DAC converters – allows reading analog signals



Lightweight Cryptography

- What is the difference between cryptography and lightweight cryptography?
- Role of the lightweight cryptography in IoT
- Lightweight cryptography in UVAs

https://www.adsgroup.org.uk/knowledge/countering-the-malicious-usage-of-drones/

Criteria when choosing an algorithm (I)

1. Security:
   - Cryptographic Resistance
   - Analysis and verification
   - Key and block length

2. Performance:
   - Capacity
   - Delay

3. Resource Consumption:
   - Memory
   - Energy

4. Implementation complexity:
   - Ease of implementation
   - Potential Errors

5. Resistance to side-channel attacks:
   - Physical attacks
   - Protection measures

6. Licensing and Intellectual Property:
   - Licensing
   - Open Source

Criteria when choosing an algorithm (II)

7. Compliance with standards:
   - International standards
   - Interoperability

8. Scalability and Flexibility:
   - Adaptability
   - Support for different platforms

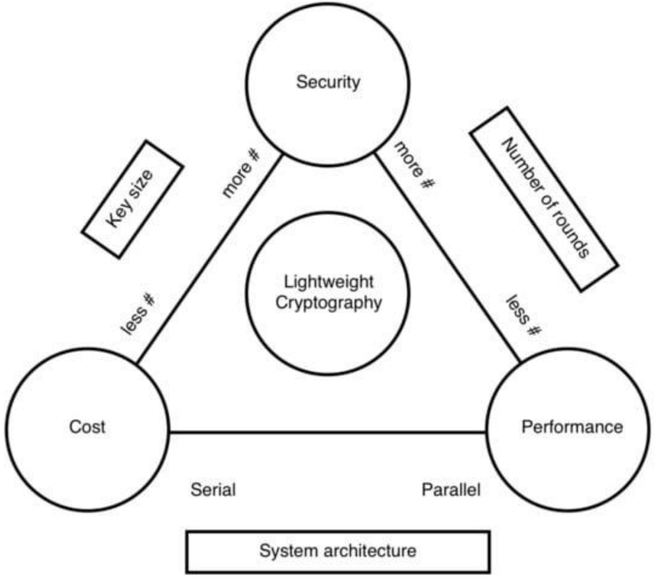
9. Implementation experience:
   - Case studies
   - Community and support

https://www.nokia.com/sites/default/files/2022-01/cybersecurity4_0.jpg

POLITECHNIKA POZNAŃSKA

NIST LWC Competition

- National Institute of Standards and Technology
- Genesis of the Contest
- Contest Goals
- Contest Phases



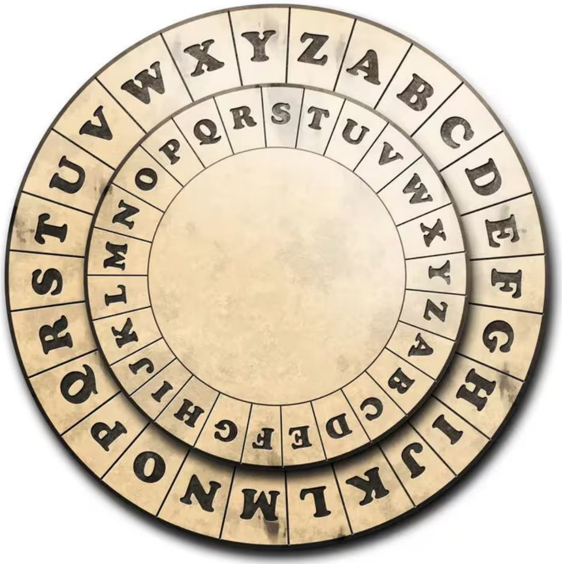
National Institute of Standards and Technology
U.S. Department of Commerce

https://csrc.nist.gov/projects/lightweight-cryptography

List of LWC algorithms

- ASCON
- PHOTON-Beetle
- TinyJAMBU
- ISAP
- Grain

- ACORN
- PRESENT
- ChaChaPoly / BLAKE2s



https://www.coindesk.com/learn/what-is-cryptography/

A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses, Hasindu Madushan, DOI: 10.3390/electronics11244199

Performance Analysis

Why It Matters?

- Cryptographic performance impacts secure communication, data protection, and authentication.
- Evaluating encryption, decryption, and hashing speeds helps determine efficiency for high-performance and resource-constrained environments.

Tested Algorithms:

- AEAD (Encryption & Authentication): ChaChaPoly, ASCON-128, TinyJAMBU, ISAP, PHOTON-Beetle.
- Hashing (Integrity Verification): BLAKE2s, ASCON-HASH, PHOTON-Beetle-HASH.

POLITECHNIKA POZNAŃSKA

Methodology & Testing

Benchmarking Approach

- Performance measured in **µs/byte**, converted to **throughput (bytes/sec)**.
- Tested **128-byte (large)** and **16-byte (small)** packets to assess variations.

Testing Environment

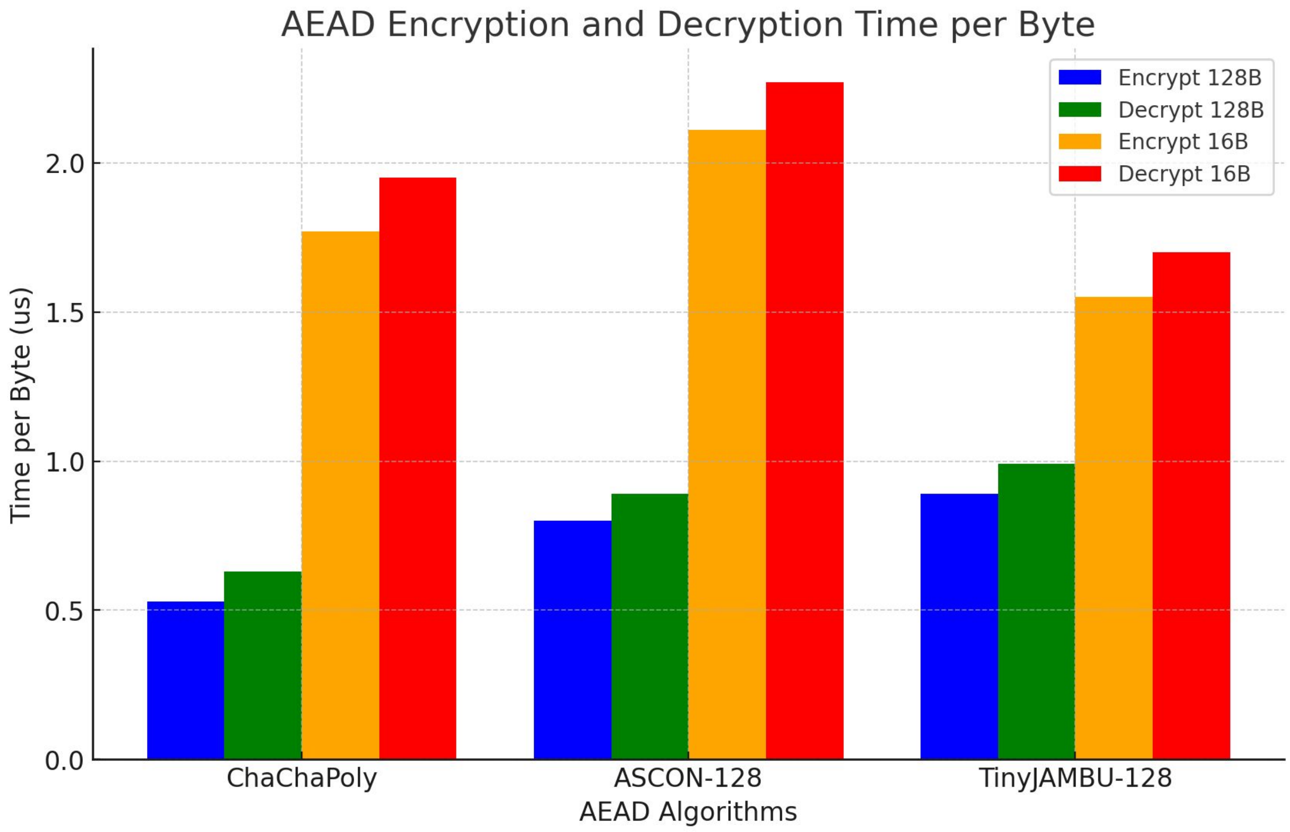
- Simulated **microcontroller-based** setup (for embedded & IoT use).
- Uniform conditions for **consistent** results.
- Included **masked AEAD** versions to analyze security-performance trade-offs.

Algorithm	Operation	Time per Byte (us)	Throughput (bytes/sec)
ChaChaPoly	Encrypt 128B	0.53	1,899,899.07
ChaChaPoly	Decrypt 128B	0.63	1,580,520.09
ChaChaPoly	Encrypt 16B	1.77	566,184.62
ChaChaPoly	Decrypt 16B	1.95	514,133.31
BLAKE2s	Hash 1024B	0.21	4,775,451.20
BLAKE2s	Hash 128B	0.21	4,678,918.37
BLAKE2s	Hash 16B	0.87	1,149,652.41
ASCON-128	Encrypt 128B	0.80	1,252,630.03
ASCON-128	Decrypt 128B	0.89	1,119,370.35
ASCON-128	Encrypt 16B	2.11	473,358.78
ASCON-128	Decrypt 16B	2.27	441,476.74
TinyJAMBU-128	Encrypt 128B	0.89	1,125,304.40
TinyJAMBU-128	Decrypt 128B	0.99	1,010,523.66

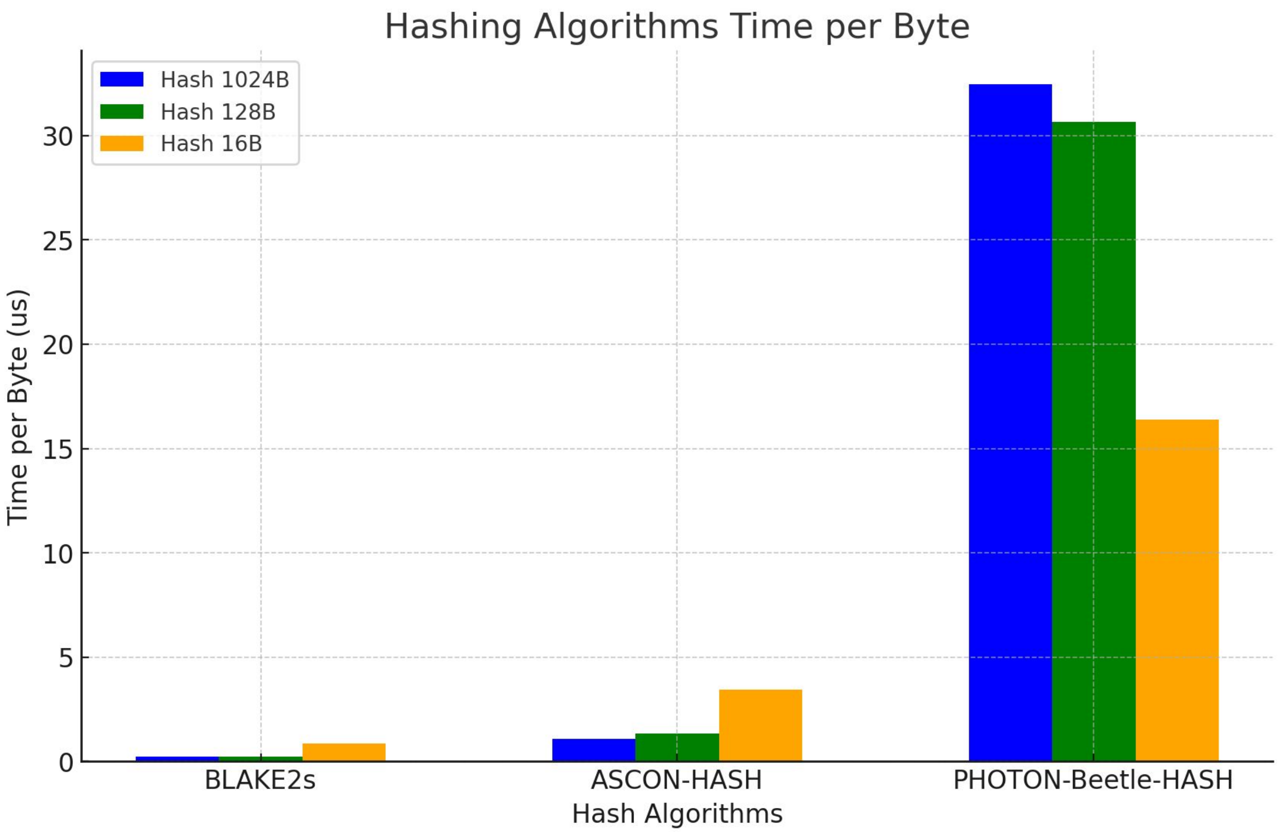
...

POLITECHNIKA POZNAŃSKA

Performance Analysis of AEAD Algorithms



Performance Analysis of Hashing Algorithms



Summary of Results

The results highlight significant differences in performance across different cryptographic schemes. Some key observations include:

- **BLAKE2s** has the highest throughput, making it an excellent choice for fast hashing applications.
- **ChaChaPoly** provides high-speed encryption and decryption, particularly for larger data packets.
- **ASCON-128** and **TinyJAMBU-128** show reasonable performance, though they are slightly slower than ChaChaPoly.
- Performance decreases significantly for smaller data packets across all algorithms.

Further sections will analyze these results in more depth, comparing masked and unmasked versions of AEAD algorithms and assessing their suitability for different security applications.

POLITECHNIKA POZNAŃSKA

References (I)

- Madushan, Hasindu, Iftekhar Salam, i Janaka Alawatugoda. „A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses”. Electronics 11, nr 24 (2022): 4199. https://doi.org/10.3390/electronics11244199.
- Dobraunig, Christoph, Maria Eichlseder, Florian Mendel, i Martin Schläffer. „Ascon v1.2: Lightweight Authenticated Encryption and Hashing”. Journal of Cryptology 34, nr 3 (2021): 33. https://doi.org/10.1007/s00145-021-09398-9.
- Berzati, Alexandre, Cecile Canovas, Guilhem Castagnos, Blandine Debraize, Louis Goubin, Aline Gouget, Pascal Paillier, and Stephanie Salgado. „Fault Analysis of GRAIN-128.” In 2009 IEEE International Workshop on Hardware-Oriented Security and Trust, 7+. San Francisco, CA, July 27, 2009. https://doi.org/10.1109/HST.2009.5225030.
- Zaky, Ahmed, Eslam Elmitwalli, Mostafa Hemeda, Yehea Ismail, and Khaled Salah. „Ultra Low-Power Encryption/Decryption Core for Lightweight IoT Applications.” In 2019 15th International Computer Engineering Conference (ICENCO), 39–43. Cairo, Egypt, December 2019. https://doi.org/10.1109/ICENCO48310.2019.9027471.
- Shi, Tairong, i Jie Guan. „Cryptanalysis of the Authentication in ACORN”. KSII Transactions on Internet and Information Systems 13, nr 8 (2019): 4060–4075. https://doi.org/10.3837/tiis.2019.08.013.

POLITECHNIKA POZNAŃSKA

References (II)

- Aranzazu Suescun, Catalina, i Mihaela Cardei. 2016. „Unmanned Aerial Vehicles Networking Protocols". W Proceedings of the 14th LACCEI International Multi-Conference for Engineering, Education, and Technology: "Engineering Innovations for Global Sustainability". Latin American and Caribbean Consortium of Engineering Institutions. https://doi.org/10.18687/LACCEI2016.1.2.078.
- Chen, Xi, Jun Tang, i Songyang Lao. 2020. „Review of Unmanned Aerial Vehicle Swarm Communication Architectures and Routing Protocols". Applied Sciences 10 (10): 3661. https://doi.org/10.3390/app10103661.
- Ko, Yongho, Jiyoon Kim, Daniel Gerbi Duguma, Philip Virgil Astillo, Ilsun You, i Giovanni Pau. 2021. „Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone". Sensors 21 (6): 2057. https://doi.org/10.3390/s21062057.
- Lu, Yuxi, Wu Wen, Kostromitin Konstantin Igorevich, Peng Ren, Hongxia Zhang, Youxiang Duan, Hailong Zhu, i Peiying Zhang. 2023. „UAV Ad Hoc Network Routing Algorithms in Space–Air–Ground Integrated Networks: Challenges and Directions". Drones 7 (7): 448. https://doi.org/10.3390/drones7070448.
- Samir Labib, Nader, Grégoire Danoy, Jedrzej Musial, Matthias R. Brust, i Pascal Bouvry. 2019. „Internet of Unmanned Aerial Vehicles—A Multilayer Low-Altitude Airspace Model for Distributed UAV Traffic Management". Sensors 19 (21): 4779. https://doi.org/10.3390/s19214779.
- Semendiai, Serhii, Yuliia Tkach, Mykhailo Shelest, Oleksandr Korchenko, Ruslana Ziubina, i Olga Veselska. 2023. „Improving the Efficiency of UAV Communication Channels in the Context of Electronic Warfare". International Journal of Electronics and Telecommunications, wrzesień, 727–32. https://doi.org/10.24425/ijet.2023.147694.
- Shi, Liping, Néstor J. Hernández Marcano, i Rune Hylsberg Jacobsen. 2021. „A review on communication protocols for autonomous unmanned aerial vehicles for inspection application". Microprocessors and Microsystems 86 (październik):104340. https://doi.org/10.1016/j.micpro.2021.104340.

POLITECHNIKA POZNAŃSKA

Thank you very much.