



E.A. Abdykerimova¹, G.Sh. Omarkulova², B.O. Kabylbekov³

¹Yessenov University, Aktau, Kazakhstan

²Kazakh University of Technology and Business named after K. Kulazhanov,
Astana, Kazakhstan

³National Defense University of the Republic of Kazakhstan,
Astana, Kazakhstan

E-mail: omarkulovagulzada@gmail.com

INTELLIGENT MICROPROCESSOR-BASED CYBER DEFENSE AND HIGH-SPEED DATA ENCRYPTION FOR LEO SATELLITES

Abstract. Low-Earth orbit (LEO) satellites require communication systems that provide high-speed encryption and robust cybersecurity solutions, while addressing resource constraints. This paper proposes a novel solution, a threat-adaptive lightweight onboard security system, which is a unified architecture of the TinyML real-time anomaly detection system and Ascon-128 adaptive authenticated encryption. The lightweight onboard detection system continuously determines the threat level and adjusts the number of encryption rounds to ensure a minimum level of security. A testbed with an adjustable Ascon-128 AEAD module, 221 TinyML detector parameters, and an adaptive closed-loop controller was developed and tested. In the testbed, running on a 200 MHz FPGA, the proposed solution demonstrated remarkable AUC of 0.997, recall of 96.6%, and false positive rate of 0.7%. The adaptive module achieved throughputs of 1.28–3.20 Gbps. During orbital mission simulations, the proposed TALOS-LEO system increased throughput by 100.7%, reduced power consumption by 42% compared to a static, high-safety configuration, and achieved 20.4% higher throughput than a conventional system using the standard Ascon implementation.

Keywords: LEO satellites, adaptive authenticated encryption, Ascon, lightweight cryptography, TinyML, anomaly detection, cyber defense.

Introduction.

Constellations of Low Earth Orbit (LEO) satellites have become an essential part of modern communication, Earth observation and critical infrastructures. However, their wireless communication channels and limited onboard processors may suffer from various cybersecurity-related attacks including transmission interception, packet injection, replay and spoofing of telemetry, tracking and command (TT&C) signals as well as physical attacks, hardware Trojans, malware and side-channel attacks targeting onboard processors. Thus, LEO satellite systems need to implement both high-speed and energy-efficient encryption and continuous monitoring of onboard processors. While these two goals are related, they are



usually treated separately, which results in fragmented security architecture in practice.

Another significant drawback of existing cryptographic approaches is their static configuration. In traditional systems the level of security of the encryption algorithm is determined at the design stage and remains unchanged during the operation. In order to protect themselves from the worst-case scenarios systems use the highest level of security all the time, regardless of the actual level of threat. Since satellites spend most of their time in non-combat conditions this conservative approach represents an excessive cost in terms of processing load, energy use and delay, while reducing throughput.

To solve these issues the paper introduces TALOS-LEO (Threat-Aware Lightweight Onboard Security), an advanced intelligent cybersecurity platform for LEO satellites. Contrary to classical architectures TALOS-LEO employs the real-time feedback loop from cyber-attack detection to authenticated encryption. The proposed system consists of four main components: (1) TA-AE, a threat-adaptive authenticated encryption engine that dynamically controls the number of rounds of Ascon permutation based on the predefined security floor; (2) HPC-AD, a lightweight anomaly detection algorithm based on TinyML technology and operating only with 221 inputs and relying on performance counter and side-channel techniques; (3) a closed-loop adaptive controller which translates the threat level into parameters of cryptographic configuration and key rotation; (4) an experimental performance evaluation based on the prototype and a 200MHz FPGA development board model. The results of the experiments show that the proposed architecture achieves much better performance in terms of throughput and energy-efficient operation in spite of maintaining a high level of security during cyber-attacks.

Literature Review. The increasing use of Low Earth Orbit (LEO) satellite networks has led to the higher demand for dependable onboard cybersecurity technologies, which can secure communication networks and computer systems while abiding by limited power and hardware requirements. Some studies have recently suggested multi-layer security models featuring communication encryption, security key management, authentication, and access control at the satellite, communication link, and ground infrastructure levels [1]. Also, in parallel, real-time encryption technologies applied directly to satellite payloads have been engineered in order to assure the safety of data transmission while utilizing the limited computational resources available onboard the spacecraft [2]. All studies mentioned provide a comprehensive definition of the limitations imposed by using satellite technologies in terms of cybersecurity, which includes limited power consumption, short communication bandwidth, and long duration of missions.

Lightweight cryptography is now regarded as one of the leading strategies when it comes to providing security for embedded platforms with limited resources. The National Institute of Standards and Technology (NIST) has



standardized Ascon family of lightweight cryptographic methods in SP 800-232 [3] by building on the Ascon v1.2 design providing authenticated encryption with high computational efficiency on limited processors [4]. Recent studies have looked at hardware implementations of Ascon and have evaluated tradeoffs in terms of area, throughput, and power consumption [5]. Comparative evaluation of NIST lightweight cryptography executive finalists using FPGA and ASIC show improvements by a factor of twenty to one hundred times in terms of energy efficiency while at the same time obtaining high throughput compared to software implementations [6]. However, present implementations depend on fixed number of rounds of permutation that have been defined during designing stage and do not allow to adjust to change in security conditions during runtime.

The area of research associated with the security of the processor engaged in cryptographic operations is equally important. The hardware roots of trust, the trusted execution environments, and the secure silicon elements would enable secure booting, isolating of the processor, protection of the key and the remote authentication and thus the trusted execution environment will be created for embedded systems [7]. The RISC-V secure enclaves enable the extension of the above-mentioned functionality through the support of isolated key management as well as protected control circuitry within the architecture of the open processor [8]. OpenTitan, on the other hand, is a provider of the open-source silicon root of trust with integrated hardware support for cryptographic operations [9]. Despite the advantages of these technologies leading to improvement in hardware security, they provide protection mainly with respect to the trust boundaries in static state without guaranteeing protection against physical, hardware Trojan and side-channel attacks during the runtime of the system.

Research has focused on the susceptibility of embedded processors to side-channel threats ever since the advent of the differential power analysis [5]. Following this, various studies have indicated the applicability of strategies for Trojan detection and defined such malicious hardware insertion attacks along with corresponding counteractions [7]. Currently, the rise of lightweight Edge AI and TinyML technologies offer new opportunities for onboard anomaly detection in real-time. First, it should be noted that these solutions use performance counters and side-channel characteristics to highlight the abnormal behavior of a processor without putting excessive pressure on the processor resources [9]. Additionally, electromagnetic side-channel analysis has been used effectively for non-stop detection of hardware Trojans without any need for reference signatures [11]. However, the current anomaly detection mechanisms only report the occurrences of threats but do not have the capability of changing the behavior of the appropriate cryptographic devices.

Another area of research concerns the implementation of post-quantum cryptography in space systems that have a long lifespan. The ML-KEM key encapsulation mechanism has already been standardized by the National Institute of Standards and Technology in FIPS 203, and its application has been analyzed in recent papers in relation to the implementation and design demands of post-



quantum cryptography for satellites. Specifically, the focus has been on the establishment of a secure key and the efficiency of cryptography for the long term rather than on the adjustment of symmetric encryption processes in operation.

Gaps in Research. While advancements have been achieved in both lightweight cryptography and onboard cyber defense applications, these two subfields of research develop separately. Authenticated encryption implementations use the same scheme throughout the whole process; as for onboard anomaly detection systems, they send signals warning of a problem but do not affect the encryption process. That's why current satellite security methods cannot adapt security and efficiency of the cryptographic process at the same time.

To overcome this limitation, TALOS-LEO proposes a combined flexible security architecture which connects an on-board anomaly detection system with a secured cryptographic mechanism by means of a loop control method. This detector continuously estimates the current level of threat and adjusts the security configuration in an adaptive manner. A number of hypotheses are tested in the current analysis. The first hypothesis states that using the flexible optimization of coughing rounds parameters instead of the traditional and costly predicting approach greatly increases the throughput and productivity of the entire system while simultaneously maintaining the high level of security. In terms of the second hypothesis, even a compact Tiny ML detector with no more than 250 parameters can affect the destination of malicious and normal processors keeping within the limits of its mission and power capacity. The third hypothesis states that building an authenticated cryptographic configuration into the selected parameters prevents their unauthorized change during the encryption process.

Materials and Method.

The onboard subsystem has four collaborating layers, as represented shown in Figure 1. A hardware root of trust (L0) and a secure enclave which is physically isolated (L1) ensure boot integrity and keys' protection; the TA-AE crypto core (L2) encrypts every channel; and the HPC-AD detector (L3) supervises the hardware and closes the control loop back to L2. The main novelty is that this is an architecture rather than a specific primitive: the anomaly detector is wired to the cryptography security dial, thus creating an autonomous control loop with formal security minimum and safe configuration with tag-authentication. layers where L3's output is transferred back to L2 for closed-loop control.

The cipher TA-AE extends Ascon-128 duplex in the form of a 320-bit state, 12 prefixed initialization/finalization rounds, and a variable amount of data processing rounds. While, in the original Ascon implementation, a value of $pb = 6$ rounds is predefined, in our improved version, the number of these rounds relies on the current threat score and is limited in the security range from 4 to 10. The lower bound represents the security limit since it can never be lower than 4 rounds, while the upper limit equals the highest diffusion margin tolerated under attack. As a result, by decreasing the value of pb in safe times, the throughput and energy

consumption are achieved, while the increase in the amount of rounds during the attacks brings back the savings policy.

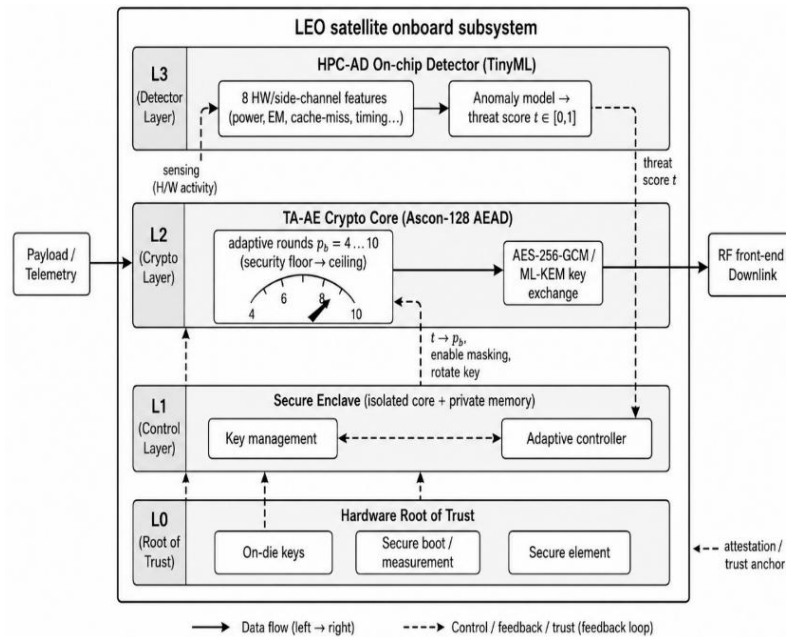


Figure 1 - The architecture of the system and control loop

The control system, which is programmed inside the enclave, has its main function in the mapping of the smooth threat score into the actual amount of rounds, as well as the key change events.

```
>>> t_raw = HPC_AD.threat_score(features)           // in [0,1]
... t     = 0.5*t_prev + 0.5*t_raw                 // EWMA smoothing
... pb    = round(PB_MIN + (PB_MAX-PB_MIN)*t)      // clamp to [PB_MIN, PB_MAX]
... if t > T_HIGH: enable_masking(); rotate_key()
... ct, tag = TA_AE.encrypt(key, nonce, ad|pb, pt, pa=12, pb=pb)
```

Figure 2 - Key change events function

Due to the fact that lead is connected to the related data and originally acknowledged through the tag, a malicious user cannot introduce a weaker configuration without ruining the level of authentication, which suggests the principle explained in hypothesis H3 within the process illustrated in Figure 3 detailing the entire control over the sequence steps from data obtaining to analyzing threats, web budget modification, and the process of encrypting.

The last section of the loop is the detector that generates the threat score. HPC-AD takes into account eight features that are either a low-cost option and thus already provided by a microprocessor, or can be obtained using a small side-channel: mean power and variance, peak electromagnetic spectrum, number of cache misses, number of branch mispredictions, timing jitter, activity on the bus and temperature of the core. There are four detectors used, including supervised TinyML MLP (with hidden layers being 12 and 8), one unsupervised IsolationForest and One-Class SVM using only normal traces, and a logistic



regression linear regression controlled versus three attack types: an always-on hardware Trojan, side-channel key extraction, and malicious firmware profile drift. MLP is characterized by the smallest number of parameters, which is 221, which is good for successfully using it with respect to its power budget.

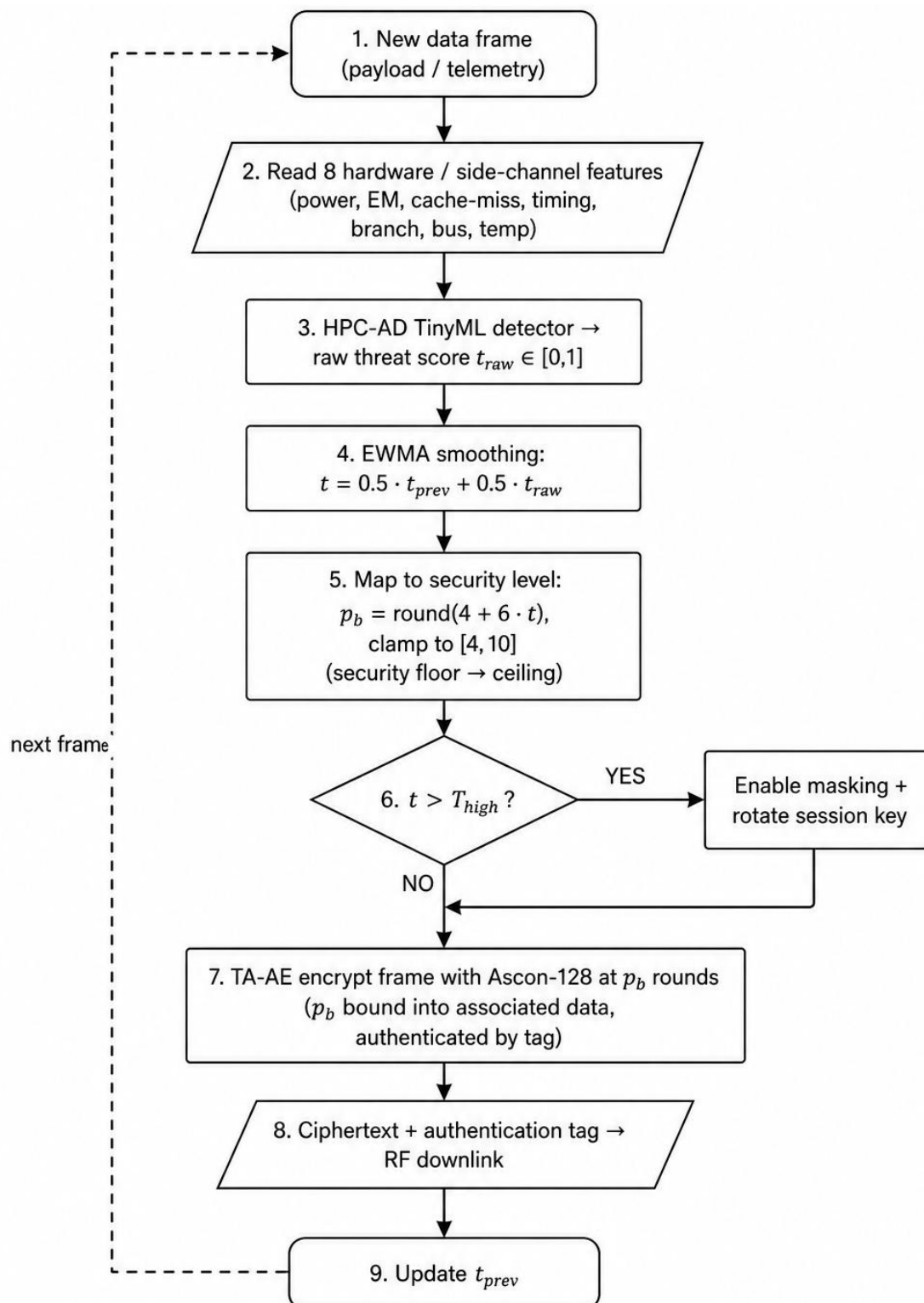


Figure 3 - Adaptive threat management process for each proposed system frame

In the cipher, the adaptive round budget takes effect on the Ascon-128 duplex sponge as shown in Figure 4, which indicates where the variable p_b rounds of data take place in the path of the data. That is by changing p_b , one can alter the properties of the diffusion margin without having to alter the whole construction.

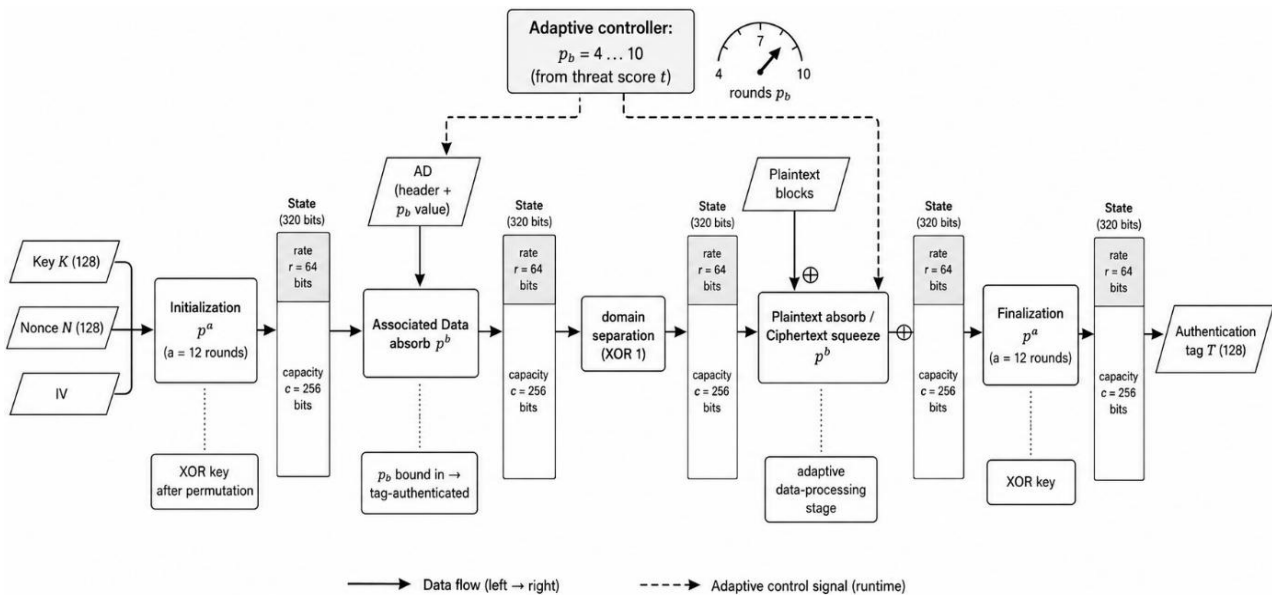


Figure 4 - TA-AE data transmission path

The prototype was built in Python (NumPy/scikit-learn) as a functioning reference model. The cipher used is an accurate implementation of Ascon-128 AEAD with regard to 320-bit state, canonical S-box, linear diffusion, 10* padding and finalizing with p_a and p_b as parameters. The correct functioning of the prototype was confirmed by encrypting and decrypting messages (checking all rounds) and by carrying out tamper-detection experiments which indicate that flipping any one bit in the ciphertext is sufficient to invalidate the tag for all p_b values between 2 and 12 and for messages of different sizes of 0, 1, 7, 8, 15, 64 and 129 bytes. Hardware throughput, cycles per byte and energy are evaluated via an FPGA model based on one permutation round per cycle at 200 MHz, which has been verified by comparing the cost ratios and round execution times to obtain errors within a few percent. The detectors in this case use the scikit-learn library on the dataset that has significant overlaps with 2% noise added to training labels. Moreover, the closed loop performance is tested in simulation for 300 steps with two injected attacks and two frames for detection.

Results and Discussion.

When it comes to cost versus security with adaptive ciphers, as the round budget (p_b) increases throughput decreases and power use increases. In essence, this means the security can be controlled smoothly instead of simply turning it to either on or off. Figure 5 shows the modeled throughput of the FPGA as it relates to security.

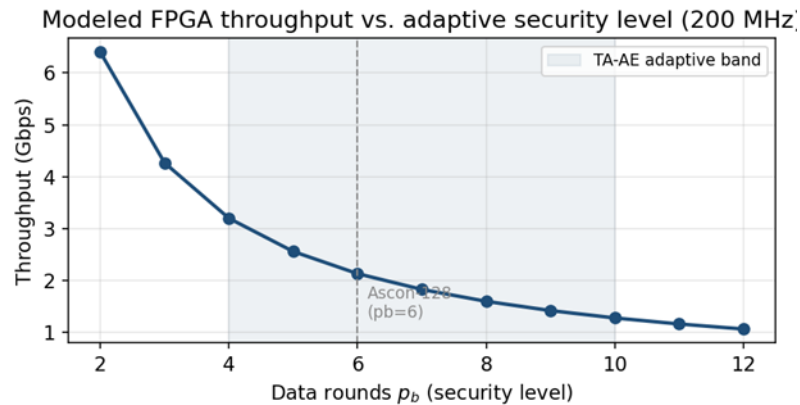


Figure 5 - Simulated FPGA throughput as a function of the adaptive round budget

Performance measurement. The performance of the four detectors was observed that the best performing detector is the supervised TinyMLP which achieved a good AUC value of 0.997 and a fairly high recall of 96.6% while only having 0.7% false-positive rate and 221 parameters while achieving 48.34 μ s for each inference thus confirming that the hypothesis H2 holds true. The performance of the unsupervised One-Class SVM and IsolationForest, which were trained on nominal traces only, is impressive with the models achieving AUC values of 0.9922 and 0.9846 respectively, which makes them a good fallback when there are no labeled attacks available. It was also found that the performance of the linear baseline is the poorest thus confirming that the nonlinear model performs better than its counterparts.

Table 3 - Anomaly-detection performance across four models

Detector	Type	AUC	Acc.	Prec.	Recall	FPR	F1	Size
TinyMLP	supervised	0.997	98.3%	98.8%	96.6%	0.7%	0.9766	221 p
One-Class SVM	unsuperv.	0.9922	95.5%	92.2%	96.2%	4.9%	0.9415	kernel
IsolationForest	unsuperv.	0.9846	94.0%	92.2%	91.7%	4.7%	0.9192	80 tr
LogReg (baseline)	supervised	0.9891	95.7%	95.3%	93.1%	2.8%	0.9415	9 p

The ROC depicted in Figure 6 is the corresponding operation curve that goes through the upper left corner of the chart. Residual errors take place in the area where they do not do much harm, which is in the stealthy and low-amplitude Trojan attempts, while there is near-perfect detection of the high signal side-channel and firmware attacks. The ROC curves of the four detectors are shown in Figure 6, while the confusion matrix of the TinyMLP can be found in Figure 7.

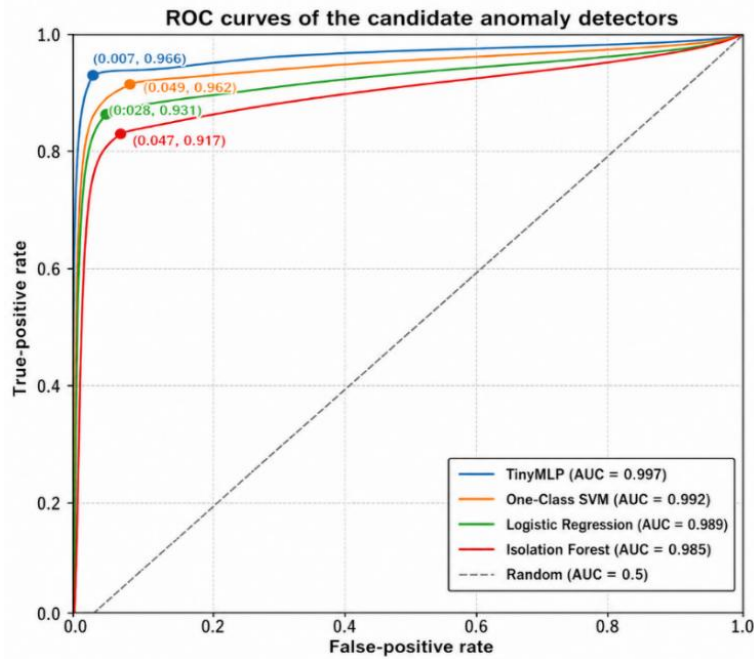


Figure 6 - ROC curves for the anomaly detectors under consideration

All curves are located in the upper left corner, and TinyMLP is closest to the ideal operating point.

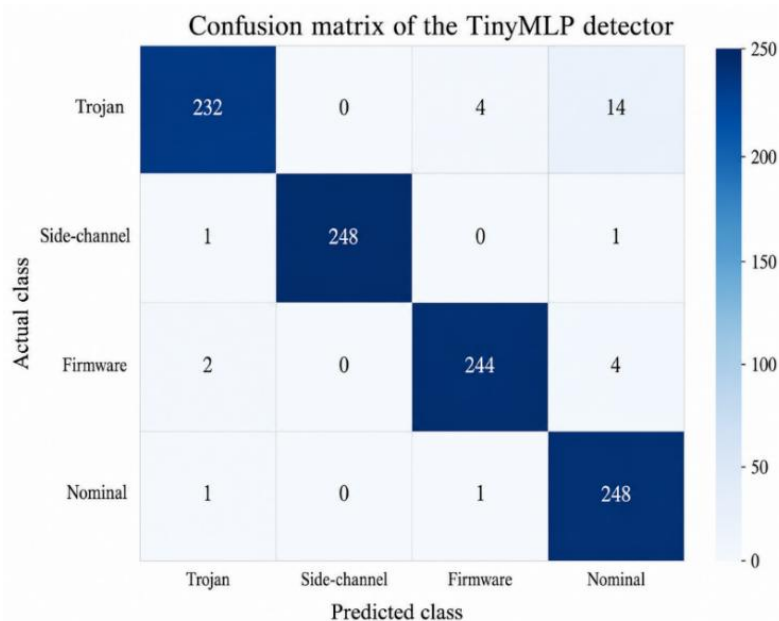


Figure 7 - Confusion matrix of the TinyMLP detector

The mistakes focus on low-amplitude Trojan traces that evade detection; meanwhile, side-channel and firmware attacks get identified almost perfectly, and false alerts still remain minimal. Closed-loop performance. Figure 8 provides a simulation of the orbital trajectory, which reveals two attack windows. The threat score goes up during those windows; then the pb signal rises from 4 to 10 in just a couple of frames.

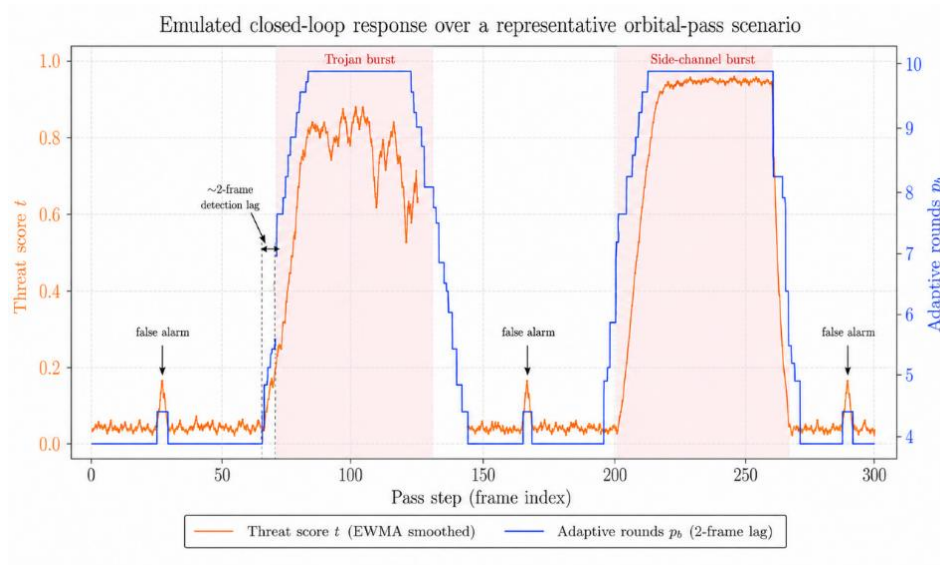


Figure 8 - Closed-loop adaptation

The entire passage maintains strict security (eight rounds and above) for 91.1% of the attack operations, while consuming the quiescent majority of the passage rapidly and with low energy.

Figure 9 illustrates where it stands in the throughput-energy tradeoff above the static frontier.

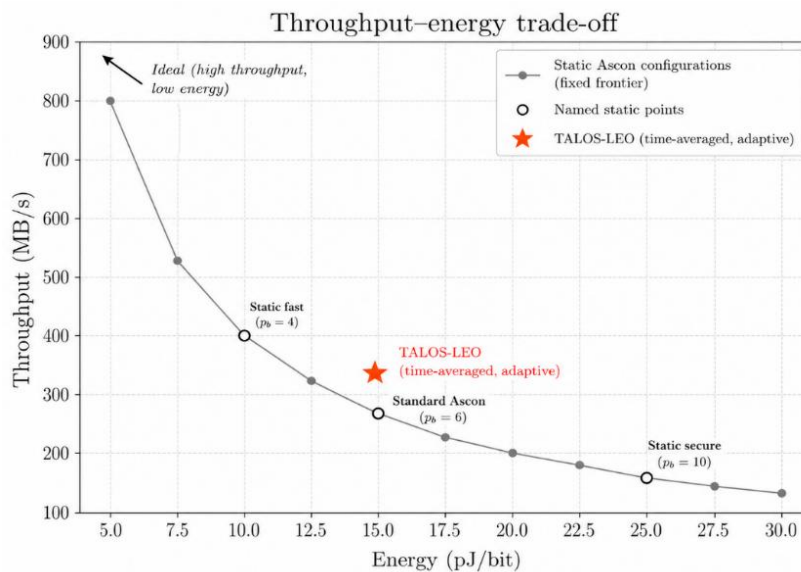


Figure 9 - Throughput/power tradeoff positioning TALOS-LEO relative to static baselines

In this way, the adaptive policy obtains the speed of the fast benchmark without taking over its risk and verifies hypothesis H1. The contribution consists in including a reference to run time feedback loop from the on-chip detector to the ciphers' round schedule a security loop instead of novel primitive or merely signal-like alarm which has never been utilized in LEO protection as far as the authors know.

Conclusion.

The authors of this paper presented TALOS-LEO which refers to a cyber-defense and threat-adaptive encryption system that uses microprocessor for LEO satellites, and successfully completed the testing phase of the prototype. It is built with the help of linking the light non-machine learning-based anomaly detector to the on-chip circuit utilizing Ascon technology. The obtained measures reveal the presence of the 221-parameter detector characterized by the rate below AUC 0.997 and recall equal to 96.6%. It also has the throughput of between 3.20 Gbps and 1.28 Gbps and also shows the throughput exceeding the bad-case solution by 100% with 42% energy recovery and determined attack coverage of approximately 91%.

The planned work for the future can be directed towards enabling the transition from modeling to silicon along with ensuring the integrity of each layer. The overall throughput and power is drawn from the hardware-based FPGA model hence; an RTL platform needs to be created to ensure the actual indices and check the radiation resistance, and that of the reduced round band. The first line of work in the area will be to train the detector on real traces and not synthetic ones depending on the version of the device; ensure its resilience against the attacks of adversaries; implement the ML-KEM technique for post-quantum KEY establishment; and develop a federated cross-constellational approach where the attack spotted on one satellite strengthens the others.

REFERENCES

1. Mahmood, N. T. (2025). Securing IoT Devices against Quantum Threats: Developing a Framework for Future-Proof Encryption. *CyberSystem Journal*, 2(2), 106-120. <https://doi.org/10.57238/csj.2025.1019>
2. Tang, H., Yu, N., Min, P., Guo, R., & Zhang, G. (2026). In-sensor-memory computing for post-Von Neumann intelligence: a perspective. *Nano-micro letters*, 18(1), 338. <https://doi.org/10.1007/s40820-026-02191-y>
3. Roper, James. "The rise of e-commerce: From dot to dominance." (2023): 1-304. <https://doi.org/10.3828/liverpool/9781789620818.003.0003>
4. Ryu, C., Lee, J. H., Kim, D. H., Lee, H. S., Kim, Y. S., Han, J. H., & Kim, J. N. (2024). A Comprehensive Survey of TPM for Defense Systems. *KSII Transactions on Internet & Information Systems*, 18(7), 1953. <https://doi.org/10.3837/tiis.2024.07.012>
5. Chandel, P. A Systematic Review of Cyber Security on Smart Energy Meter Analytics: Cyber Attacks, Applications, Methodologies, and Challenges. <https://doi.org/10.4018/978-1-5225-5634-3.ch013>
6. Nygård, A. R., & Katsikas, S. K. (2023). Leveraging Hardware Reverse Engineering to Improve the Cyber Security and Resilience of the Smart Grid. In *SECRYPT* (pp. 610-616). <https://doi.org/10.5220/0012046000003555>



7. Masood, T., Abdo, J., & Iqbal, A. (2025). Protection of Electrical Power Distribution Systems: Smart Grid, Microgrid, AI, and Cyber Security. John Wiley & Sons. <https://doi.org/10.1002/9781394327676>
8. Hossain, M. R., & Bhardwaj, T. (2023). Deep Learning Aided Intrusion Detection for Smart Grid Cyber Security. In Artificial Intelligence in Cyber Security: Theories and Applications (pp. 99-112). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-28581-3_10
9. Bakyt, M., La Spada, L., Moldamurat, K., Kadirbek, Z., & Yermekov, F. (2024, December). Review of Data Security Methods using Low-Earth Orbiters for High-Speed Encryption. In 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) (pp. 1366-1375). IEEE. <https://doi.org/10.1109/icuis64676.2024.10867245>
10. Zhang, C., Yu, H., Shi, S., Li, S., Shi, Y., Burger, E., ... & Lou, W. (2025, May). StarCast: a secure and spectrum-efficient group communication scheme for LEO satellite networks. In 2025 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN) (pp. 1-10). IEEE. <https://doi.org/10.1109/dyspan64764.2025.11115935>
11. Zuo, P., Wei, J., Zhang, K., Liu, X., Guo, C., & Hu, R. (2023). An intelligent encryption decision method for autonomous domain of multilayer satellite network. Alexandria Engineering Journal, 81, 337-346. <https://doi.org/10.1016/j.aej.2023.08.072>
12. Rashid, F. B., Rankothge, W., Sadeghi, S., Mohammadian, H., & Ghorbani, A. (2024). Privacy-Preserving for Images in Satellite Communications: A Comprehensive Review of Chaos-Based Encryption. arXiv preprint arXiv:2410.21177. <https://doi.org/10.1016/j.cose.2024.104156>
13. Xia, M., Hu, S., Luo, H., Yan, T., & Shi, Y. (2022). Data naming mechanism of LEO satellite mega-constellations for the Internet of Things. Applied Sciences, 12(14), 7083. <https://doi.org/10.3390/app12147083>
14. Coppola, D., Mumtaz, A., Camurati, G., Sathaye, H., Singh, M., & Capkun, S. (2025). {LEO-Range}: Physical Layer Design for Secure Ranging with Low Earth Orbiting Satellites. In 34th USENIX Security Symposium (USENIX Security 25) (pp. 7059-7075). <https://doi.org/10.14722/ndss.2022.23151>
15. Yue, P., An, J., Zhang, J., Ye, J., Pan, G., Wang, S., ... & Hanzo, L. (2023). Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead. IEEE Communications Surveys & Tutorials, 25(3), 1604-1652. <https://doi.org/10.1109/comst.2023.3296160>

Эльмира Абдыкеримова, п.ф.к., Yessenov University, Ақтау, Қазақстан, abdykerimova_el@mail.ru

Гульзада Омаркулова, магистр, сеньор-лектор, K.Kulazhanov Kazakh University of Technology and Business, Астана, Қазақстан, omarkulovagulzada@gmail.com



Бауыржан Кабылбеков, магистр, аға оқытушы, полковник, National Defence University of the Republic of Kazakhstan, Астана, Қазақстан

ЛЕО СПУТНИКТЕРІНЕ АРНАЛҒАН МИКРОПРОЦЕССОРЛЫҚ ИНТЕЛЛЕКТУАЛДЫ КИБЕРҚОРҒАНЫС ЖӘНЕ ЖОҒАРЫ ЖЫЛДАМДЫҚТЫ ДЕРЕКТЕРДІ ШИФРЛАУ

Андатпа. Жердің төменгі орбитасындағы (LEO) спутниктер ресурстардың шектеулерін ескере отырып, жоғары жылдамдықты шифрлауды және сенімді киберқауіпсіздік шешімдерін қамтамасыз ететін байланыс жүйелерін қажет етеді. Бұл мақалада TinyML нақты уақыт режиміндегі аномалияларды анықтау жүйесінің және Ascon-128 бейімделгіш аутентификацияланған шифрлаудың бірыңғай архитектурасы болып табылатын қауіпке бейімделгіш жеңіл борттық қауіпсіздік жүйесі деген жаңа шешім ұсынылады. Жеңіл борттық анықтау жүйесі қауіп деңгейін үздіксіз анықтайды және қауіпсіздіктің минималды деңгейін қамтамасыз ету үшін шифрлау раундтарының санын реттейді. Реттелетін Ascon-128 AEAD модулі, 221 TinyML детектор параметрлері және бейімделгіш тұйық циклді контроллері бар сынақ алаңы жасалып, сыналды. 200 МГц FPGA-да жұмыс істейтін сынақ алаңында ұсынылған шешім 0,997 AUC, 96,6% еске түсіру және 0,7% жалған оң нәтиже жиілігін көрсетті. Бейімделгіш модуль 1,28–3,20 Гбит/с өткізу қабілетіне қол жеткізді. Орбиталық миссияны модельдеу кезінде ұсынылған TALOS-LEO жүйесі өткізу қабілеттілігін 100,7%-ға арттырды, статикалық, жоғары қауіпсіздік конфигурациясымен салыстырғанда энергия тұтынуды 42%-ға азайтты және стандартты Ascon іске асыруын пайдаланатын дәстүрлі жүйеге қарағанда 20,4%-ға жоғары өткізу қабілеттілігіне қол жеткізді.

Түйінді сөздер: LEO спутниктері, адаптивті аутентификацияланған шифрлау, Ascon, жеңіл криптография, TinyML, аномалияларды анықтау, киберқорғаныс.

Эльмира Абдыкеримова, к.п.н., Yessenov University, Актау, Казахстан, abdykerimova_el@mail.ru

Гульзада Омаркулова, магистр, сеньор-лектор, K.Kulazhanov Kazakh University of Technology and Business, Астана, Казахстан, omarkulovagulzada@gmail.com

Бауыржан Кабылбеков, магистр, старший преподаватель, полковник, National Defence University of the Republic of Kazakhstan, Астана, Казахстан

ИНТЕЛЛЕКТУАЛЬНАЯ КИБЕРЗАЩИТА НА ОСНОВЕ МИКРОПРОЦЕССОРА И ВЫСОКОСКОРОСТНОЕ ШИФРОВАНИЕ ДАННЫХ ДЛЯ СПУТНИКОВ LEO



Аннотация. Спутники на низкой околоземной орбите (НОО) нуждаются в системах связи, обеспечивающих высокоскоростное шифрование и надежные решения в области кибербезопасности, при этом учитывая ограничения доступных ресурсов. В данной статье предлагается новое решение, адаптивная к угрозам облегченная бортовая система безопасности, представляющая собой унифицированную архитектуру системы обнаружения аномалий TinyML в реальном времени и адаптивного аутентифицированного шифрования Ascon-128. Облегченная бортовая система обнаружения непрерывно определяет уровень угрозы и корректирует количество раундов шифрования, чтобы обеспечить минимальный уровень безопасности. Была разработана и протестирована тестовая установка с регулируемым модулем AEAD Ascon-128, 221 параметром детектора TinyML и адаптивным контроллером с замкнутым контуром. В тестовой установке, работающей на FPGA с частотой 200 МГц, предложенное решение продемонстрировало замечательные показатели AUC 0,997, полноты 96,6% и частоты ложных срабатываний 0,7%. Адаптивный модуль смог достичь пропускной способности 1,28–3,20 Гбит/с. В ходе моделирования орбитальной миссии предложенная система TALOS-LEO увеличила пропускную способность на 100,7%, снизила потребление на 42% по сравнению со статической конфигурацией повышенной безопасности и достигла на 20,4% большей пропускной способности по сравнению с обычной системой, использующей стандартную реализацию Ascon.

Ключевые слова: спутники LEO, адаптивное аутентифицированное шифрование, Ascon, легковесная криптография, TinyML, обнаружение аномалий, киберзащита.

Received: July 12, 2026

Peer-reviewed: August 20, 2026

Accepted: August 28, 2026