УДК 004.432

С.О. Гнатюк, Ю.Я. Поліщук, Б.М. Горбаха
(Національний авіаційний університет, Україна)

Аналіз методів забезпечення конфіденційності даних, які передаються з безпілотного літального апарату

Проведений огляд і порівняльний аналіз сучасних методів і засобів забезпечення конфіденційності даних, які передаються радіоканалом (зокрема, для криптографічного захисту даних, які передаються з БПЛА). На основі результатів аналізу в подальшому буде вибраний криптоалгоритм (або набір криптоалгоритмів) та створений датасет (база даних) криптоалгоритмів різної криптостійкості та швидкодії для забезпечення гнучкості та адаптивності передачі даних з БПЛА на наземні системи в різних умовах роботи.

В умовах проведення збройного конфлікту на Сході України питання проведення аеророзвідки засобами безпілотної авіації є задачею важливою та актуальною. Збирання та передавання оперативної інформації потребує розв'язання низки задач, серед яких окреме місце посідає опрацювання даних з камер цільового навантаження безпосередньо на борту літального апарату, підготовка таких даних для передавання та безпосередня трансляція на наземну робочу станцію. Відповідно, інформація, що передається, має бути захищена від несанкціонованого доступу, час трансляції інформації – максимально обмежений, тож фактично маємо потребу забезпечити технічне рішення, яке полягає у створенні системи конфіденційного передавання пакетних даних з обмеженим доступом з борту розвідувального дрона.

Питання вибору криптоалгоритму для вирішення проблеми безпечного передавання інформаціїї було розглянуто в наступних роботах науковців.

Авторами [1] проведене порівняння чотирьох найпоширеніших криптоалгоритмів з симетричним ключем: AES, DES, CAST 128 і Blowfish. Експеримент показав, що в обох режимах DES дає сильний лавинний ефект, а AES і Cast 128 дають значну зміну терміну перевірки цілісності порівняно з іншими алгоритмами.

У [2] статті проведено порівняльний аналіз алгоритму AES з різними режимами роботи (блоковий шифр) і алгоритму RC4 (поточний шифр) з точки зору процесорного часу, часу шифрування, використання пам'яті та пропускної здатності за різних параметрів, таких як змінний розмір ключа та змінний розмір пакета даних. Експерименти показали, що RC4 є швидким і енергоефективним для шифрування та дешифрування. На основі аналізу, проведеного в рамках цього дослідження, RC4 кращий, ніж AES.

У статті [3] автори запропонували систему, яка забезпечує цілісність зображень за допомогою AES та Rivest-Shamir-Adleman (RSA). Результати аналізу довели, що AES більш ефективний як для шифрування, так і для дешифрування.

Автори [4] провели аналіз продуктивності алгоритмів DES, 3DES, AES і Blowfish з різними розмірами та носіями. Результати показують, що Blowfish був найшвидшим алгоритмом; однак автори зазначають, що безпека була здебільшого

проігнорована, і що її слід розглянути в першу чергу. Автори [5] також провели аналіз продуктивності AES і DES і дійшли висновку, що AES є ефективнішим для захисту канали зв'язку між вузлами, ніж DES.

Дослідження [6] було спрямоване на порівняння алгоритмів шифрування з точки зору продуктивності та забезпечення безпеки для БПЛА. Порівнювались алгоритми OTP, AES, DES і RSA. Результати показують, що OTP працює краще, ніж інші алгоритми з точки зору використання оперативної пам'яті, часу обробки, часу шифрування та дешифрування.

В науковій статті [7], поєднуючи шифрування даних за допомогою Elliptic Curve Cryptography (далі ECC) і The Diffie–Hellman (DH) Algorithm, проводилися випробування обміну ключами за допомогою криптографії з відкритим ключем. Результат випробування показав кращі результати, ніж RSA та інші алгоритми.

В [8] проведено порівняння симетричних шифрів, таких як: AES, AES-GCM, HMAC, CHACHA20, CHACHA-POLY, POLY 1305.

В [9] авторами пропонується гібридна криптографічна схема безпеки, яка має прості обчислення, але високий рівень безпеки. Запропонований алгоритм має багатошарове шифрування з використанням AES-256, ECC і SHA256.

В науковому дослідженні [10] проведено порівняння алгоритмів ECC і RSA в пристроях з обмеженими ресурсамию. У результаті цього дослідження використання ECC у пристроях з обмеженими ресурсами має переваги перед RSA, але ECC потребує продовження вдосконалення, щоб задовольнити обмеження нових мікросхем.

У [11] аналізується надійність безпеки двох популярних і практичних методів криптографії з відкритим ключем RSA (Rivest Shamir Adleman) і ECC (Elliptic Curve Cryptography). Головна перевага ECC порівняно з RSA полягає в тому, що найвідоміший алгоритм для розв'язання ECDLP займає повний експоненціальний час, тоді як для розв'язання IFP RSA потрібен субекспоненціальний час. Це означає, що в ECC можна використовувати значно менші параметри, ніж у RSA, з еквівалентними рівнями безпеки.

В роботі [12] запропоновано сумісне використання генетичних алгоритмів і алгоритмів асиметричної криптографії, робота [13] (як і багато інших подібних) пропонує механізм інтеграції штучного інтелекту та блокчейн-технологій, а в роботі [14] авторами розвинено теорію так званої «нейронної криптографії», у якій алгоритми криптографічної обробки даних і розподілу ключів базуються на алгоритмах синхронізації нейронних мереж. Крім того, на сьогодні існує багато публікацій, пов'язаних із використанням штучного інтелекту для задач криптоаналізу [15, 16 та інші] з метою підбору найбільш ефективної криптоаналітичної атаки на основі можливостей зловмисника і характеристик перехоплених даних (фрагментів ключа, шифротексту тощо).

З огляду на велику кількість алгоритмів, які можуть використовуватись в БПЛА необхідно провести порівняльний аналізу за певними критеріями (критерій 1 будемо позначати К1, критерій 2 - К2 і тд). Такими критеріями є: 1) 128-бітний розмір блоку даних, що шифруються (К1); 2) не менше трьох підтримуваних алгоритмом розмірів ключів шифрування: 128, 192 та 256 біт (К2); 3) алгоритм має бути стійким проти криптоаналітичних атак, відомих на цей час (К3); 4) структура алгоритму має бути ясною, простою та обґрунтованою, що гарантувало

б відсутність запроваджених авторами алгоритму «закладок» (тобто в даному випадку, особливостей архітектури алгоритму, якими теоретично могли б скористатися його автори у зловмисних цілях) (К4); 5) повинні бути відсутніми слабкі та еквівалентні ключі (тобто ключі, що є різними, але призводять до одного і того ж результату шифрування) (К5); 6) швидкість шифрування даних має бути високою на всіх потенційних апаратних платформах – від 8-бітових до 64-бітових (К6); 7) алгоритм повинен пред'являти мінімальні вимоги до оперативної та енергонезалежної пам’яті (К7); 8) не повинно бути обмежень для використання алгоритму; зокрема, алгоритм не повинен обмежувати своє використання в різних стандартних режимах роботи, генераторів псевдовипадкових послідовностей і т.д (К8).

Результати критеріального аналізу представлені у Таблиці 1.

Таблиця 1

Порівняльний аналіз алгоритмів

Критерії / Алгоритми	**К1**	**К2**	**К3**	**К4**	**К5**	**К6**	**К7**	**К8**
	Симетричне, блокове шифрування							
AES	+	+	+	+	+	+	+	+
DES	-	-	-	+/-	-	-	+	+
3DES	-	-	+/-	+/-	+	-	+	+
CAST 128	-	-	+	+	+	+	+	+
Blowfish	-	+	-	+	-	-	+	+
	Симетричне, потокове шифрування							
RC4	+	+	-	+	-	+	+	+
OTP	+	-	+	+	+	+	+	+
ChaCha 20	+	-	+	+	+	+	+	+
ChaCha 20-POLY 1305	+	-	+	+	+	+	+	+
	Асиметричне шифрування							
RSA	N/A	+	+	+	+	-	+/-	+
ECC	N/A	+	+	+	+	-	+/-	+

Критерії / Алгоритми	К1	К2	К3	К4	К5	К6	К7	К8
	Хеш-функція							
SHA 256	+	-	+	+	+	+	+	+

*N/A - NOT APPLICABLE, критерій не використовується для алгоритмів асиметричної криптографії.

В роботі проведений огляд сучасних методів і засобів забезпечення конфіденційності даних, які передаються радіоканалом для криптографічного захисту даних, які передаються з БПЛА. З огляду на специфіку та функції роботи БПЛА проведено порівнялиний аналіз криптоалгоритмів. Наступним кроком виконання поставленого завдання є створення датасета (бази даних) криптоалгоритмів (виявлених під час проведення аналізу, включаючи розробки авторів проєкту) різної криптостійкості та швидкодії для забезпечення гнучкості та адаптивності системи в різних умовах роботи.

References

1. Y.M. Koukou, S.H. Othman, M. M. Siraj and H. Nkiama. (2016) .Comparative Study of AES, Blowfish, CAST-128 and DES Encryption Algorithm. IOSR Journal of Engineering (IOSRJEN). Vol. 6. Issue 6. P. 1-7.
2. Nidhi Singhal, J.P.S.Raina. (2011). Comparative Analysis of AES and RC4 Algorithms for Better Utilization. International Journal of Computer Trends and Technology (IJCTT). V1(3). P. 259-263.
3. B. J. S. Kumar, V. K. R. Raj and A. Nair. (2017). Comparative study on AES and RSA algorithm for medical images. I*nternational Conference on Communication and Signal Processing (ICCSP).* P. 501-504.
4. A. Nadeem and M. Y. Javed. (2005). A Performance Comparison of Data Encryption Algorithms. *International Conference on Information and Communication Technologies.* P. 84-89.
5. A. K. Mandal, C. Parakash, and A. Tiwari. (2012). A. Performance evaluation of cryptographic algorithms: DES and AES. I*EEE Students' Conference on Electrical, Electronics and Computer Science.* P. 1-5.
6. T. Khoei, E. Ghribi, P. Ranganathan, N. Kaabouch. (2021). A performance comparison of encryption/decryption algorithms for UAV swarm communications. Academic Press.
7. Usman, M., Amin, R., Aldabbas, H., Alouffi, B. (2022). Lightweight Challenge-Response Authentication in SDN-Based UAVs Using Elliptic Curve Cryptography. Electronics 2022. Vol. 11. P. 1026. https://doi.org/10.3390/electronics11071026.
8. Muslum Ozgur Ozmen, Rouzbeh Behnia, Attila A Yavuz. (2019). IoD-crypt: A lightweight cryptographic framework for Internet of drones. arXiv. Vol. 1.
9. F. Ronaldo, D. Pramadihanto and A. Sudarsono. (2020). Secure Communication System of Drone Service using Hybrid Cryptography over 4G/LTE

Network. *2020 International Electronics Symposium (IES).* P. 116-122. doi: 10.1109/IES50839.2020.9231951.

10. Bafandehkar, Mohsen et al. (2013). Comparison of ECC and RSA Algorithm in Resource Constrained Devices. 2*013 International Conference on IT Convergence and Security (ICITCS).* P. 1-3.

11. Mahto, Dindayal et al. (2016). Security Analysis of Elliptic Curve Cryptography and RSA. *Proceedings of the World Congress on Engineering 2016.* Vol. I. P. 1-4.

12. S. Jhajharia, S. Mishra and S. Bali. (2013). Public key cryptography using neural networks and genetic algorithms. *2013 Sixth International Conference on Contemporary Computing (IC3).* P. 137-142.

13. B. Chavali, S. K. Khatri and S. A. Hossain. (2020). AI and Blockchain Integration. *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO).* P. 548-552.

14. T. Dong and T. Huang. (2020). Neural Cryptography Based on Complex-Valued Neural Network. IEEE Transactions on Neural Networks and Learning Systems. Vol. 31. No. 11. P. 4999-5004.

15. M. Danziger and M. A. Amaral Henriques. (2014). Improved cryptanalysis combining differential and artificial neural network schemes. *2014 International Telecommunications Symposium (ITS)*. P. 1-5.

16. Y. Xiao, Q. Hao and D. D. Yao. (2019). Neural Cryptanalysis: Metrics, Methodology, and Applications in CPS Ciphers. *2019 IEEE Conference on Dependable and Secure Computing (DSC).* P. 1-8.