# **Лаба 1**

### **ФИО**

Шилина В.В. (группа 6113-100503D)

### **Topic**

Authenticated Encryption; Block Ciphers; Related-Key Attack

### **Описание предметной области**

Данный топик охватывает исследования в области блочного шифрования, в частности режим аутентифицированного шифрования, а также атаки со связанным ключом на блочные шифры. Блочный шифр — это метод шифрования данных в блоках для создания зашифрованного текста с использованием криптографического ключа и алгоритма. Аутентифицированное шифрование (AE) — режим блочного шифрования, при котором часть сообщения шифруется, часть остается открытой, и всё сообщение целиком аутентифицировано. Блочные шифры, как и любая криптографическая система, не защищены от атак. Помимо атак с перебором ключей (brute force), они также могут столкнуться с угрозами со стороны более сложных криптоаналитических атак, таких как атака со связанным ключом, в которой выбирают некоторые математические соотношения, связывающие между собой ключи.

### **Недостаток (Gap)**

В статьях есть много информации про дифференциальный и линейный криптоанализ, связанной с поиском подключей быстрее, чем полный перебор ключей, для защиты существует, например, шифр "квадрат". Интегральный криптоанализ же, в свою очередь, является менее изученным и обладает рядом преимуществ, к примеру, 4-раундовые AES подвержены атакам таким способом.

### **Идея**

Изменение порядка шифрования блочного шифра и добавление в него дополнительного этапа сдвига строк булевыми функциями. Это усложнит задачу во время интегрального криптоанализа против 4-раундовых AES.

### **Краткий текст обзора**

Симметричные блочные шифры являются наиболее широко используемыми криптографическими примитивами. Помимо обеспечения конфиденциальности, блочные шифры используются в качестве базовых компонентов при построении хэш-функций [[1]](https://www.zotero.org/google-docs/?eZgx8c), кодов аутентификации сообщений [[2]](https://www.zotero.org/google-docs/?Er2aJf), генераторов псевдослучайных чисел [[3]](https://www.zotero.org/google-docs/?rNn1rQ). В настоящее время наиболее популярным блочным шифром является AES (Advanced Encryption Standard) [[4], [5]](https://www.zotero.org/google-docs/?RZ57kD). Пик популярности статей на эту тему приходится на период с 2014 по 2022 год.

Естественно, блочные шифры не лишены атак хакеров различными методами, в том числе взаимодействие со связанными ключами [[4], [6], [7]](https://www.zotero.org/google-docs/?YG2W0H). В настройках связанных ключей у злоумышленника есть возможность запрашивать базовую функцию на целевом ключе, а также на некоторых связанных ключах [[2]](https://www.zotero.org/google-docs/?yuAJY1). Конечно, постоянно появляются модификации шифров для защиты от атак, к примеру: [[2], [3], [8], [9]](https://www.zotero.org/google-docs/?gf6R9g). Новая смена ключа — хорошо зарекомендовавший себя метод защиты примитива или режима от атак по побочным каналам [[10]](https://www.zotero.org/google-docs/?IMGyT1): легко защищаемая, но криптографически не столь сложная функция генерирует подключ из главного ключа, и этот подключ затем используется для блочного шифрования одного или нескольких сообщений.

Однако большинство результатов в литературе направлены на достижение псевдослучайности и семантической безопасности и часто приводят к неэффективным конструкциям. Поэтому в настоящей статье мы предлагаем идею изменения порядка шифрования блочного шифра и добавления в него дополнительного этапа сдвига строк булевыми функциями. Это усложнит задачу во время интегрального криптоанализа против 4-раундовых AES.

References

[[1] Y. Naito, ‘Tweakable Blockciphers for Efficient Authenticated Encryptions with Beyond the Birthday-Bound Security’, *IACR Transactions on Symmetric Cryptology*, vol. 2017, no. 2, pp. 1–26, 2017.](https://www.zotero.org/google-docs/?6l0Ww6)

[[2] R. Bhattacharyya and A. Roy, ‘Secure Message Authentication Against Related-Key Attack’, in *Fast Software Encryption*, vol. 8424, S. Moriai, Ed., in Lecture Notes in Computer Science, vol. 8424. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 305–324. doi: 10.1007/978-3-662-43933-3\_16.](https://www.zotero.org/google-docs/?6l0Ww6)

[[3] S. Lucks, ‘Ciphers Secure Against Related-Key Attacks’, in *Fast Software Encryption*, vol. 3017, B. Roy and W. Meier, Eds., in Lecture Notes in Computer Science, vol. 3017. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 359–370. doi: 10.1007/978-3-540-25937-4\_23.](https://www.zotero.org/google-docs/?6l0Ww6)

[[4] D. Kaidalov, R. Oliynykov, and O. Kazymyrov, ‘A Method for Security Estimation of the SPN-Based Block Cipher Against Related-Key Attacks’, *Tatra Mountains Mathematical Publications*, vol. 60, no. 1, pp. 25–45, Sep. 2014, doi: 10.2478/tmmp-2014-0023.](https://www.zotero.org/google-docs/?6l0Ww6)

[[5] A. Albertini, T. Duong, S. Gueron, S. Kölbl, A. Luykx, and S. Schmieg, ‘How to Abuse and Fix Authenticated Encryption Without Key Commitment’, in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 3291–3308. Accessed: Aug. 13, 2024. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/albertini](https://www.zotero.org/google-docs/?6l0Ww6)

[[6] B. Zhao, X. Dong, W. Meier, K. Jia, and G. Wang, ‘Generalized Related-Key Rectangle Attacks on Block Ciphers with Linear Key Schedule: Applications to SKINNY and GIFT’, *Des. Codes Cryptogr.*, vol. 88, no. 6, pp. 1103–1126, Jun. 2020, doi: 10.1007/s10623-020-00730-1.](https://www.zotero.org/google-docs/?6l0Ww6)

[[7] S. Faust, J. Krämer, M. Orlt, and P. Struck, ‘On the Related-Key Attack Security of Authenticated Encryption Schemes’, in *Security and Cryptography for Networks*, vol. 13409, C. Galdi and S. Jarecki, Eds., in Lecture Notes in Computer Science, vol. 13409. , Cham: Springer International Publishing, 2022, pp. 362–386. doi: 10.1007/978-3-031-14791-3\_16.](https://www.zotero.org/google-docs/?6l0Ww6)

[[8] E. Fleischmann, C. Forler, and S. Lucks, ‘McOE: A Family of Almost Foolproof On-Line Authenticated Encryption Schemes’, in *Fast Software Encryption*, vol. 7549, A. Canteaut, Ed., in Lecture Notes in Computer Science, vol. 7549. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 196–215. doi: 10.1007/978-3-642-34047-5\_12.](https://www.zotero.org/google-docs/?6l0Ww6)

[[9] D. Goudarzi *et al.*, ‘Pyjamask: Block Cipher and Authenticated Encryption with Highly Efficient Masked Implementation’, *IACR Transactions on Symmetric Cryptology*, vol. 2020, no. S1, pp. 31–59, 2020.](https://www.zotero.org/google-docs/?6l0Ww6)

[[10] B. Mennink, ‘Beyond Birthday Bound Secure Fresh Rekeying: Application to Authenticated Encryption’, in *Advances in Cryptology – ASIACRYPT 2020*, vol. 12491, S. Moriai and H. Wang, Eds., in Lecture Notes in Computer Science, vol. 12491. , Cham: Springer International Publishing, 2020, pp. 630–661. doi: 10.1007/978-3-030-64837-4\_21.](https://www.zotero.org/google-docs/?6l0Ww6)