International Science Group

ISG-KONF.COM

III

INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE «RESEARCH ON THE DEVELOPMENT OF SCIENCE AND THE IMPLEMENTATION OF TECHNOLOGY»

Hamburg, Germany

September 16-19, 2025

ISBN 979-8-89814-220-9

DOI 10.46299/ISG.2025.2.3

RESEARCH ON THE DEVELOPMENT OF SCIENCE AND THE IMPLEMENTATION OF TECHNOLOGY

Proceedings of the III International Scientific and Practical Conference

Hamburg, Germany
September 16-19, 2025

UDC 01.1

The 3rd International scientific and practical conference “Research on the development of science and the implementation of technology” (September 16-19, 2025) Hamburg, Germany. International Science Group. 2025. 245 p.

ISBN – 979-8-89814-220-9
DOI – 10.46299/ISG.2025.2.3

ПРО АПАРАТНІ МЕХАНІЗМИ ПРОТИДІЇ АТАКАМ ПОБІЧНИХ КАНАЛІВ У RISC-V IOT-ПРИСТРОЯХ

Грек Єгор
студент групи ІНФм-24-1
Харківський національний університет радіоелектроніки,

Науковий керівник:
Яковлева Олена Володимирівна
к.т.н., доц., доцент кафедри інформатики
Харківський національний університет радіоелектроніки,

Сучасні системи комп'ютерного зору [1-10] потребують якісного захисту від різного роду можливих атак. Відкрита архітектура RISC-V швидко поширюється в IoT-системах завдяки гнучкості та відкритому екосередовищу. Проте обмежені за ресурсами пристрої особливо вразливі до атак побічних каналів: за споживанням енергії, електромагнітним випромінюванням, мікроархітектурними ефектами та часовими варіаціями.

Сучасні підходи до протидії атакам побічних каналів у RISC-V переважно концентруються на трьох рівнях: схемотехнічному, мікроархітектурному та інструкційному. На схемотехнічному рівні застосовується маскування, яке передбачає поділ секретних даних на випадкові частки.

Прикладом такої реалізації є проєкт OpenTitan [11], де модуль AES [12] реалізований із першопорядковим маскуванням, що гарантує відсутність кореляції між виміряними трасами споживання та секретними ключами. Маскування суттєво знижує ризик успіху диференціального аналізу потужності, але водночас призводить до збільшення апаратних витрат і зниження швидкодії. Іншим напрямком є використання випадкових затримок, вставки шумових або фіктивних інструкцій та рандомізації порядку виконання операцій.

Такі методи не усувають витік повністю, проте ускладнюють статистичний аналіз та вимагають від зловмисника значно більшої кількості вимірювань.

У IoT-контексті, де ресурси обмежені, часто застосовується поєднання помірного рівня маскування з техніками випадкової рандомізації для досягнення прийнятного балансу між рівнем захисту та енергоспоживанням.

На мікроархітектурному рівні ключовим завданням є зменшення впливу особливостей ядра на витоки часу виконання. Відмова від кешів, передбачення переходів та спекулятивного виконання, як це зроблено у спеціалізованому модулі OTBN [13] у складі OpenTitan, дозволяє уникнути значної частини таймінгових атак.

Якщо ж кеші та інші оптимізації все ж використовуються, то застосовуються методи поділу ресурсів, очищення буферів і предикторів під час перемикання контексту, а також методи кольорування кешу для ізоляції чутливих даних. Важливою стратегією також є забезпечення виконання в сталому часі, коли

апаратні блоки гарантують однакову кількість тактів незалежно від значення секретних даних.

На рівні інструкційного набору з'являються розширення, що полегшують реалізацію захищеного програмного забезпечення. Прикладом є модифікації ядра Ibex у проєкті CoCo-Ibex [14], де апаратні зміни дають змогу безпечно виконувати масковане програмне забезпечення без появи нових витоків, що могли б виникати внаслідок небажаних взаємодій між частками даних.

Крім того, наукові роботи пропонують введення нових інструкцій для роботи з поділеними секретами, що зменшує накладні витрати при маскованих обчисленнях і стимулює розробників використовувати безпечні практики.

OpenTitan сьогодні є найбільш відомим відкритим проєктом, у якому втілено комплекс заходів протиатак побічних каналів. Його модулі AES і OTBN інтегрують маскування, відмову від небезпечних оптимізацій, очищення регістрів після завершення роботи та навіть шифрування вмісту внутрішніх пам'ятей для ускладнення аналізу споживання.

Проєкт CoCo-Ibex показав можливість спільного застосування апаратних змін і маскованого програмного забезпечення, що разом формує стійку до першопорядкових атак платформу.

Дослідження, представлені на конференціях з криптографічного обладнання та вбудованих систем, та на конференціях з автоматизації проєктування [15], підтверджують, що повністю масковані ядра RISC-V здатні забезпечити високий рівень захисту при відносно невеликих накладних витратах.

Окремі проєкти демонструють використання спеціалізованих криптопроцесорів, які позбавлені кешів та спекулятивних механізмів, але водночас мають інтегровані масковані алгоритми, що робить їх оптимальними для IoT-застосувань.

Апаратні механізми протидії атакам побічних каналів у RISC-V активно розвиваються та вже довели свою ефективність у низці відкритих і промислових проєктів.

Маскування, шумові та часові контрзаходи, виконання у сталому часі, поділ мікроархітектурних ресурсів та використання спеціалізованих криптографічних блоків формують багаторівневий підхід, що значно підвищує стійкість IoT-пристроїв до атак. Попри це, лишаються відкритими завдання підвищення порядку маскування без істотних витрат ресурсів, захисту складних мікроархітектурних блоків у потужних ядрах, а також формальної верифікації відсутності витоків.

Подальші дослідження у цьому напрямі мають дати змогу створювати сертифіковані та довірені рішення на базі RISC-V, здатні забезпечити високий рівень безпеки в умовах зростання загроз у сфері IoT.

Список літератури:

1. Гороховатський В., Передрій О., Творошенко І., Марков Т. (2023) Матриця відстаней для множини компонентів структурного опису як інструмент для

створення класифікатора зображень, *Сучасні інформаційні системи*, 7(1), С. 5-13.

2. Pomazan, V., Tvoroshenko, I., and Gorokhovatskyi, V. (2023). Development of an application for recognizing emotions using convolutional neural networks, *International Journal of Academic Information Systems Research*, 7(7), pp. 25-36.

3. Daradkeh Y.I., Gorokhovatskyi V., Tvoroshenko I., and Zeghid M. (2024) Improving the effectiveness of image classification structural methods by compressing the description according to the information content criterion, *Computers, Materials & Continua*, vol. 80, no. 2, pp. 3085-3106.

4. Gorokhovatskyi V., and Tvoroshenko I. (2024) An effective method for transforming an image description into a compact vector for classification. *Information Technology and Implementation (Satellite): Conference Proceedings, November 21, 2024*, Kyiv, Ukraine, Publishing House «Caravela», pp. 25-28.

5. Gorokhovatskyi V., Chmutov Y., Tvoroshenko I., and Kobylin O. (2025) Reducing computational costs by compressing the structural description in image classification methods, *Advanced Information Systems*, vol. 9, no. 1, pp. 5-12.

6. Gorokhovatskyi V., Tvoroshenko I., Yakovleva O., Hudáková M., and Gorokhovatskyi O. (2024) Application a committee of Kohonen neural networks to training of image classifier based on description of descriptors set, *IEEE Access*, vol. 12, pp. 73376-73385.

7. Gorokhovatskyi V., Tvoroshenko I., Yakovleva O., and Hudáková M. (2025) Image description compression in classification structural methods, *IEEE Access*, vol. 13, pp. 43631-43641.

8. Tvoroshenko I., Gorokhovatskyi V., Kobylin O., and Tvoroshenko A. (2023) Application of deep learning methods for recognizing and classifying culinary dishes in images, *International Journal of Academic and Applied Research*, 7(9), pp. 57-70.

9. Yakovleva O., Matúšová S., Tvoroshenko I., and Isaiev Y. (2024) Visitor counting based on video stream analysis from surveillance cameras to solve various business problems, *Verejná správa a regionálny rozvoj ekonómia, manažment a marketing*, XX(1), pp. 67-87.

10. Gorokhovatskyi V., Tvoroshenko I., Yakovleva O. (2024) Transforming image descriptions as a set of descriptors to construct classification features, *Indonesian Journal of Electrical Engineering and Computer Science*, 33 (1), 113-125.

11. Ciani, M., Parisi, E., Musa, A., Barchi, F., Bartolini, A., Kulmala, A., ... & Davide, R. (2024). Unleashing OpenTitan's Potential: a Silicon-Ready Embedded Secure Element for Root of Trust and Cryptographic Offloading. ACM Transactions on Embedded Computing Systems.

12. Abdullah, A. M. (2017). Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Cryptography and Network Security, 16(1), 1

13. Urquhart, E. (2024). Acceleration of Post-Quantum Cryptography on OpenTitan Big Number Accelerator using Instruction Set Extensions.

14. Gigerl, B., Hadzic, V., Primas, R., Mangard, S., & Bloem, R. (2021). Coco:{Co-Design} and {Co-Verification} of masked software implementations on

{CPUs}. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 1469-1468).

15. Sajadi, A., Zidaric, N., Stefanov, T., & Mentens, N. (2024, October). A Systematic Comparison of Side-channel Countermeasures for RISC-V-based SoCs. In 2024 IEEE Nordic Circuits and Systems Conference (NorCAS) (pp. 1-7). IEEE.