УДК 004.6
Д. Дзюба, Л. Дмитроца, канд. техн. наук; доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПРИСТРОЇ З ФІЗИЧНОЮ НЕКЛОНОВАНОЮ ФУНКЦІЄЮ (PUF)

UDC 004.6
D. Dziuba, L. Dmytrotsa, Ph.D., Assoc. Prof.

DEVICES WITH PHYSICAL NON-CLONED FUNCTION (PUF)

Фізичні неклоновані функції (PUF) доцільно застосувати для генерації криптографічних ключів [1]. PUF використовує виробничі варіації, які вводяться в інтегральну схему (IC) під час її виготовлення. Варіації непередбачувані, неконтрольовані, неминучі і природні [2]. Отже, ключі, які генеруються за допомогою модуля PUF, також повністю випадкові й унікальні для відповідного модуля PUF.

Пристрої PUF генерують унікальний відбиток пальців для вразливих елементів в екосистемі IoMT. Ці унікальні відбитки пальців/підписи виникають внаслідок різниць у виготовленні пристроїв. Відбитки пальців можна використовувати для створення ключів криптографії, що захищають пристрої та їхні дані в екосистемі IoMT, де кінцеві девайси піддаються ризику атак апаратного втручання [3].

На рисунку 1 запропонована концепція безпеки на основі PUF для IoMT.

Рисунок 1. Безпека на основі PUF для IoMT.

Впровадження PUF в IoMT забезпечує захист інформації та охороняє від неконтрольованих дій. Також досліджено, що використання IoMT на основі PUF зменшує ризик випадкового або навмисного втручання і, як результат, запобігає створенню помилок чи нещасних випадків під час передачі даних кінцевими девайсами.

Література.

1. V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, “PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things,” IEEE Transactions on Consumer Electronics, vol. 65, no. 3, pp. 388–397, Aug 2019.
2. V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Novel FinFET based Physical Unclonable Functions for Efficient Security in Internet of Things,” in Proc. IEEE Int. Symp. Nanoelect. Inf. Sys. (iNIS), 2016, pp. 172–177
4. Ahmed Z., Mohamed K., Zeeshan S. And Dong X. Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine. *Database*, Vol. 2020, p.345, 2020.