DOI 10.31891/2307-5732-2020-281-1-191-195
УДК 621.121

Н.І. ПРАВОРСЬКА
Хмельницький національний університет

ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ОБМІНУ ІНФОРМАЦІЇ В МЕРЕЖІ ЕЛЕМЕНТІВ ІНТЕРНЕТУ РЕЧЕЙ

Пристрої інтернету речей дозволяють передавати інформацію від малих до великих обсягів даних. Однією з типових проблем речей інтернету речей є необхідність захисту інформації від втручення в канал зв'язку. Пристрої IoT часто володіють односторонністю дії, тобто передачею даних лише до приймача. За апаратною складністю, кінцеві вузли IoT, на відміну від потужних серверів мережі, мають обмежені ресурси як в пам'яті пристрою так і в обчислювальній потужності процесору. Зростання обчислювальної потужності обмежується доступним енергоспоживанням. Тому важливим є забезпечення надійної аутентифікації та захисту даних із застосуванням простих та ефективних оалгоритмів.

Ключові слова: інтернет речей, захист інформації.

N.I. PRAVORSKA
Khmelnytskyi National University

PROVIDING SECURITY OF INFORMATION EXCHANGE ON THE ELEMENTS OF THE INTERNET OF THINGS

Internet of Things devices allow you to transfer information from small to large amounts of data. One of the common problems with the Internet of Things is the need to protect information from interference with a communication channel. IoT devices often have a one-sided effect, that is, transferring data only to the receiver. In hardware complexity, IoT endpoints, unlike powerful network servers, have limited resources in both device memory and processor computing power. The increase in computing power is limited by the available power consumption. Therefore, it is important to ensure reliable authentication and data protection using simple and efficient algorithms.

Keywords: Internet of Things, information security.

Вступ

Зі швидким розвитком Інтернету речей (IoT) і «розумних» міст світ рухається у напрямі інтелектуалізації, при якій об'єкти здатні взаємодіяти з іншими об'єктами. У епоху IoT автостоянки можуть направляти вас до незайнятих парковочным місць, заводи можуть автоматично вирішувати проблеми виробничої лінії, а готелі можуть регулювати температуру і освітлення відповідно до переваг гостя. Усе вищевикладене забезпечує рішення завдань «розумного» міста.

Ця нова екосистема «речей» нині формує новаторську бізнес-модель для наступного покоління вбудовуваних продуктів/виробів.

Постановка проблеми

Розумні міста застосовують передові інформаційні технології, такі як Інтернет речей, хмарні обчислення і мобільний інтернет до рішень у сфері комунальних послуг, будівлям і системам, які оточують нас. Інтелектуальні рішення дозволяють нам підвищити ефективність роботи і якість життя за рахунок інтеграції інтелекту в технології.

Згідно із звітом Gartner в 2020 році, використовуватиметься більше 30 мільярдів підключених пристроїв. Cisco має ще більші прогнозовані показники, обумовлені зниженням ціни на підключення і подальшим швидким ростом числа з'єднань між машинами (M2M). Фірма Cisco очікує, що число підключених до мережі пристроїв досягне 50 мільярдів до 2020-2022 року. Крім того, згідно із сміливішим прогнозом компанії Morgan Stanley [2], 75 мільярдів пристроїв по всьому світу будуть підключено до 2023 року. Тобто, виходячи з різних ресурсних джерел, до 2020-2022 року прогнозується 50-100 мільярдів приладів, приєднаних до мережі Інтернет.

Захист персональних даних має бути надійно забезпечений через здатність пристроїв обробляти конфіденційну інформацію.

Основна частина

Впродовж останнього десятиліття Інтернет речей (IoT) плавно увійшов до нашого життя завдяки появі систем безпровідного зв'язку, таких як RFID, Wi - Fi, 4G, IEEE 802.15.x, які найчастіше використовуються в основі додатків моніторингу і контролю. У теперішній же час, концепція Інтернету речей має складну структуру. Вона включає багато різних технологій, служб і стандартів, і це широко сприймається в якості основи ринку ІКТ, принаймні, в найближчі десять років.

Високий рівень неоднорідності, у поєднанні з широкою гаммою систем Інтернету речей, як очікується, підвищить існуючий рівень загроз безпеки в глобальній мережі, яка все частіше використовується для взаємодії людей, машин і роботів. Зокрема, традиційні заходи дотримання конфіденційності і протидії загрозам не можуть бути безпосередньо застосовані до технологій IoT із-за їх обмеженої обчислювальної потужності. Крім того, велика кількість сполучених пристроїв створює проблему масштабованості. В той же час, для досягнення повного визнання з боку користувачів визначення і досягнення необхідного рівня безпеки, конфіденційності і довіри моделей, відповідних для Інтернету речей, є обов'язковим. Окрім цього мають бути гарантовані безпека і анонімність даних, їх конфіденційність і цілісність, а також надійність механізмів аутентифікації і авторизації. Це необхідно для запобігання несанкціонованому доступу неавторизованих користувачів до системи.

Таблиця 1

Порівняльна характеристика стандартів безпровідних мереж

Стандарт	ZigBee (IEEE 802.15.4)	Wi-Fi (IEEE 802.11b)	Bluetooth (IEEE 802.15.1)
Частотний діапазон	2,4-2483 ГГц	2,4-2,483 ГГц	2,4-2,483 ГГц
Пропускна спроможність, кбіт/с	250	11000	723,1
Розмір стека протоколу, кбайт	32-64	Більше 1000	більше 250
Час безперервно роботи від батареї, дні	100-1000	0,5-5	1-10
Максимальна кількість вузлів в мережі	65536	10	7
Діапазон дії, м	10-100	20-300	10-100
Сфера застосування	Видалений моніторинг і управління	Передача мультимедійної інформації	Заміщення дротяного з'єднання

Незважаючи на різноманіття стандартів Інтернету речей (таблиця 1) у всіх них є спільні проблеми.

1) Перша загальна проблема це речі IoT або пристрої – використовуються сенсори, контролери, актуатори, а також фізичні об'єкти, які спочатку не призначені для підключення до мережі. Кожна річ повинна бути однозначно ідентифікована. Пристрої ідентифікуються програмно-апаратними засобами, передбаченими розробниками пристроїв, традиційний ідентифікатор – MAC-адресу мережевого адаптера. Діапазон доступних адрес кінцевий, але більш широкі можливості надає, нова версія протоколу IP – протокол IPv6, з довжиною адреси 128 біт замість 32 в IPv4. А фізичні об'єкти можуть бути ідентифіковані за допомогою RFID-міток, радіо-маяків, та ін.

2) Другий спільною проблемою є мережі Інтернету речей. Провідні та безпровідні, в складі яких хаби і шлюзи, з усім зоопарком численних протоколів. Для бездротових мереж важливу роль відіграють такі якості, як ефективність в умовах низьких швидкостей, відмовостійкість, адаптивність, можливість самоорганізації, низьке енергоспоживання.

3) Третя загальна проблема, це центри обробки даних (ЦОД), як правило, в хмарі (cloud computing). У цих центрах здійснюється збір, зберігання, обробка, аналіз і візуалізація даних. А також виробляються прогнози, рекомендації і команди пристроїв для розумного взаємодії між собою і між пристроями і зовнішнім середовищем відповідно до заданих алгоритмів.

З усіма загальними проблемами зростає ризик нестабільної роботи IoT систем. Забезпечити вирішенню можливе шляхом аналізу проекту, розділяючи систему на модулі. Кожен модуль варто досліджувати, скласти базу можливих несправностей, підготувати тести і досліджувати рішення усунення і підвищення стійкості до цих несправностей.

Визначення невирішених питань

Які проблеми є в IoT сьогодні в розрізі забезпечення захисту інформації?

- Аутентифікація датчиків/сенсорів/контроллерів/шлюзів
- Аутентифікація запитів для доступу до датчиків/сенсорам/контроллерам/шлюзам і їх конфігурації
- Конфіденційність передаваних даних
- Забезпечення цілісності даних і команд
- Анонімність і приватность (для консьюмерского IoT)

Основна частина

IoT є новим кроком в технологічному прогресі. Інтернет речей дозволяє людям і речам "з'єднатися" для спільного використання у будь-який час і у будь-якому місці, використовуючи різні мережі зв'язку. У документах замість терміну "річ" ("things") застосовують такі терміни як – об'єкт ("objects"), вузол ("node"), прилад або пристрій ("device") та ін. Основними компонентами IoT є сенсорні мережі USN (Ubiquitious Sensor Networks) і радіочастотна ідентифікація RFID (Radio Frequency IDentification) [1].

Річчю в RFID є RFID-мітка (RFID-тег), а в USN - сенсорний датчик або група датчиків. Мережеві структури мереж USN побудовані на базі варіанту протоколу IPv.6 - 6LoWPAN (Low energy IPv6 based Wireless Personal Area Networks protocol) або "протокол безпроводової мережі низького споживання на базі IPv6". В самій назві протоколу вже робляться акценти на:

1) мінімізація споживання енергії;
2) досягнення максимальної кількості елементів в мережі, що не заважають один одному.

Можливість протоколу 6LoWPAN присвоїти усім сенсорним датчикам і RFID-міткам IP-адреси дозволяє реалізувати саму ідеологію реконфігурованої мережі IoT. Вже сьогодні можна спостерігати, як через інтернет між собою пов'язані різні пристрої, працюючі без участі людини, - системи управління освітленням, системи управління, автоматичні системи поливу, датчики пожежної і охороною сигналізації, світлофори та ін. [3]. Однією з головних проблем IoT є забезпечення інформаційної безпеки (ІБ).

Чим відрізняються сенсорні мережі від мереж IoT?

Сенсорні мережі використовуються для конкретних застосувань, а IoT повинен підтримувати різні види додатків і може розглядатися як сенсорна мережа загального призначення. На рис. 1 показані складові операцій, що виконуються в мережі речей.

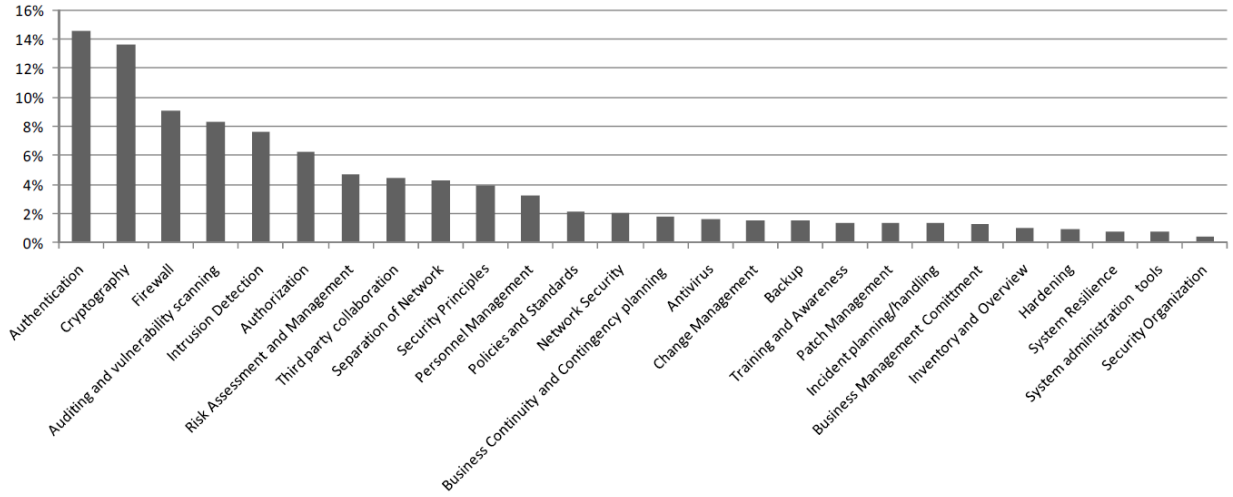

Рис. 1. Елементарні операції інтернету речей.
Джерело: SCADA System Cyber Security - A Comparison of Standards

Отже, за оцінками спеціалістів, найбільш використовуваними операціями в мережі є:

1) аутентифікація (14,3%);
2) криптографічна обробка даних (13,5%).

Причини, чому аутентифікація та криптографічна обробка даних використовують рівні частини дій є цілком очовидні:

- Підключення від недовіреного середовища до контрольованої зони вимагає захист даних;
- Підтвердження дійсності та прав доступу при передачі інформації;
- Низьке енергоспоживання та довготривала автономність роботи з одночасною передачею малих порцій даних;
- Однонапрямлена взаємодія та довготривала відсутність адміністратора пристрою.

Задача забезпечення низького енергоспоживання є сукупністю двох факторів:

1) задача швидкого призначення довільного адресу для IoT-пристрою;
2) задача швидкого захисту відкритого контенту шляхом інкапсулювання його у захищений контейнер.

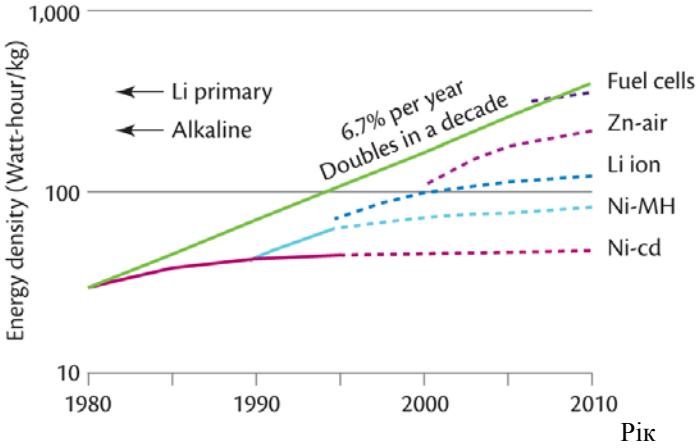

Рис. 2. Тенденції забезпечення автономного живлення пристроїв IoT

Чому не будь-яка криптографія підходить для використання в IoT-пристроях?

- Передача даних в IoT оцінюється не лише і не стільки швидкістю передачі, а обсягом корисної інформації, яка зазвичай вимірюється на великих пакетах (400+ байт).
- У IoT набагато більше значення має розмір інформації і вимога по затримках. Часто захистити потрібно всього декілька біт інформації. У окремих стандартах електроенергетики вимагається забезпечувати передачу даних із затримкою не більше 10^{-3}…10^{-6} с.

Таблиця 2

Можливості ввведення додаткових функцій для протоколів пристроїв IoT

Частина протоколу взаємодії	Вбудована в устаткування	Накладена поверх існуючих
• ZigBee • Secure DNP3 • DNPSec • Secure Modbus • OPC • 6LoWPAN	• Непридатна для «застарілого» устаткування • Не усі пристрої з--за нестачі системних ресурсів і вимог до автономної роботи підтримують «зайвий» функціонал • Деякі виробники контроллерів стали оснащувати свої рішення вбудованою криптографією	• Найпопулярніший варіант • Підходить для «старих» пристроїв і зарубіжних АСОВІ ТП, в яких необхідно забезпечити додаткові гарантії • Ідеальна для видаленого доступу
Вплинути не можна	Вплинути можна тільки при виборі устаткування	Максимально керована ситуація

На рис. 2 показано зростання потужності джерел живлення для автономних систем, проте одночасно з цим зростає і обсяг даних, що обробляється в пристроях.

Варіанти реалізації криптографії при застосуванні різних протоколів та устаткування показана в таблиці 2.

Атрибутно-засноване шифрування

Атрибутно-засноване шифрування (Attribute - Based Encryption, ABE) було уперше описане Амитом Сахаи і Брентом Уотерсом в 2004 році [3]. Основна ідея такого шифрування полягає в тому, щоб використати певні атрибути користувача в якості його ключа. Для генерації і видачі ключів потрібний так званий авторизований центр видачі атрибутів (Attribute Authority, AA).

У деяких схемах передбачається наявність декількох таких центрів, що відповідають за різні види атрибутів. Такі схеми дістали назву Multi-Authority ABE або MA-ABE. Залежно від того, хто визначає політику доступу до зашифрованих повідомлень, розрізняють два можливі підходи до реалізації ABE схеми: Key-Policy ABE (KP-ABE) і Ciphertext-Policy ABE (CP-ABE). У KP-ABE політика доступу включена в закритий ключ одержувача, а набір атрибутів пов'язаний з шифр-текстом. У CP-ABE політика доступу включена в шифр-текст, а набір атрибутів пов'язаний з ключем одержувача. У обох випадках через шифрування також здійснюється контроль доступу, що робить використання ABE привабливим для Інтернету речей.

Оскільки розумні речі можуть бути суттєво обмежені в обчислювальних потужностях і обсягах доступної пам'яті, нерідко постає питання про те, що фактично реалізовується ABE-схеми в мережах інтернету речей. На їх реалізацію також впливають типи і число атрибутів, визначених політикою доступу.

Так, в оригінальній CP-ABE–схемі, описаній в [3], для кожного атрибуту з політики доступу потрібні дві операції піднесення до степеня при шифруванні. Розшифровка в тій же CP–ABE схемі вимагає k піднесень до степеня і 2k білінійних відображень, тоді як в KP–ABE схемі – тільки k білінійних відображень, де k–число атрибутів, що задовольняють політиці. Проте в роботі [4] була продемонстрована адаптація ABE схем до використання на таких платформах працездатності, на рівні Intel Atom як Raspberry Pi, Intel Galileo Gen 2 і Intel Edison.

Ще однією особливістю, яка ставить під сумнів можливість застосування існуючих ABE-схем в інтернеті речей, є використання в них 62 білінійних відображень.

Легковагі криптографічні примітиви

Безпека інтернету речей безпосередньо пов'язана з використовуваними в протоколах примітивами: шифрами, хеш-функциями. Здебільшого для таких пристроїв використовують блокове шифрування, оскільки воно вимагає менше ресурсів і пам'яті, у порівнянні з асиметричними криптографічними алгоритмами.

Одні з відомих легковагих шифрів — це Present–80 і MIBS–80. Проте згідно з роботами [7, 8], можуть бути дешифровані з вірогідністю 100 % із складністю 278.98 і 279.34 відповідно. Такі шифри, як Khudra і SKINNY, піддаються криптоаналізу [9, 10], для повного Khudra складність злому — 268.46, а для SKINNY — 64-64 з 18 раундами складність злому — 257.1.

PRINCE [11] — блоковий шифр, оптимізований для роботи в режимі реального часу, з легким впровадженням в апаратне забезпечення, на нього робилися атаки [12], проте вони не привели до повного розкриття ключа за оптимальний час. Таким чином, існує ряд блокових шифрів, які можуть використовуватися для ряду завдань в області інтернету речей.

Також запропонована ABE-схема, заснована на еліптичних кривих, які повинні замінити ваговиті білінійні відображення [5]. Використання як основи алгоритму еліптичних кривих повинно спростити апаратну реалізацію алгоритму, зменшити розмір зашифрованого повідомлення і ключів. Іншим способом зменшити навантаження на кінцеві пристрої може бути побудова моделі, запропонованої в [6]. Ця модель припускає наявність додаткового напівдовіреного центру (semi-trusted-authority, STA), який повинен здійснювати взаємодію з центрами видачі атрибутів від імені користувача, не порушуючи при цьому конфіденційності ключа користувача.

Не варто забувати, проте, про те, що у ряді випадків IoT -устройства фізично доступні зловмисникові, що робить можливим, приміром, атаки по енергоспоживанню (power attacks). Наприклад, описана така атака на криптографічний модуль "розумних ламп", працюючих в режимі аутентифицированного шифрування CCM [13]. Показано, що для окремих завдань, таких як оновлення прошивки, потрібна асиметрична криптографія, а також потрібний контроль і стандартизація з боку держави [14].

Висновки

Компанія Gartner прогнозує, що постачальники продуктів і послуг Інтернету речей в 2020 році отримають додатковий доход, що перевищує 300 мільярдів доларів США, в основному у сфері послуг. Ще один звіт IDC містить ще більше вражаючий прогноз, що припускає, що витрати на технології і послуги IoT дозволять витягати глобальні доходи у розмірі 4,8 трлн. доларів США в 2012 році і 8,9 трлн. доларів США до 2020 року, збільшившись при сукупному річному темпі росту (CAGR) в 7,9%.

Необхідність захисту конфіденційності циркулюючою в мережах інтернету віщої інформації очевидна, а з розвитком безпровідних мереж і ростом числа розумних пристроїв як ніколи актуальна. Між тим такі особливості IoT -систем, як велике число взаємодіючих пристроїв, їх обмеженість в ресурсах і необхідність безперервної роботи в реальному часі вимагають особливого підходу у виборі і створенні криптографічних протоколів. Атрибутно-засноване шифрування дозволяє здійснювати 63 контроль доступу і адресувати одне зашифроване повідомлення відразу декільком пристроям, що мають однакові набори

атрибутів, що є корисним в IoT -системах. З іншого боку, ABE -схемы повинні допрацьовуватися, щоб задовольняти умові обмеженості ресурсів. Легковагі криптографічні примітиви задовольняють цій умові, проте не усі з них є досить стійкими.

Література

1. Куприяновский В.П. Интернет вещей на промышленных предприятиях / В.П. Куприяновский, Д.Е. Намиот, В.И. Дрожжинов, Ю.В.Куприяновская, М.О. Иванов // Журн. International Journal of Open Information Technologies.– 2016. – vol.4,№12. – С. 69-78.

2. Отказоустойчивость [Электронный ресурс] – Режим доступа : www/ URL: https://dic.academic.ru/dic.nsf/ruwiki/1080344 – 01.10.2019 – Загл. З екрану.

3. On the Feasibility of Attribute-Based Encryption on Internet of Things Devices / M. Ambrosin et al. // IEEE Micro Special Issue on Internet of Things — 2016.

4. Li F., Rahulamathavan Y., Rajarajan M., Phan R.C.-W. Low Complexity MultiAuthority Attribute Based Encryption Scheme for Mobile Cloud Computing // 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering. 2012. P. 573–577.

5. Xuanxia Y., Chen Z., Tian Y. A lightweight attribute-based encryption scheme for the Internet of Things // Future Generation Computer Systems, Elsevier B.V.— 2014.

6. Abed F., Forler C., List E., Lucks S., Wenzel J. Biclique cryptanalysis of present, led, and klein // Cryptology ePrint Archive: Report 2012/591–2012.

7. Sereshgi F., Dakhilalian M., Shakiba M. Biclique cryptanalysis of MIBS ‐ 80 and PRESENT ‐ 80 block ciphers // Security and Communication Networks. 2016. Т. 9. № 1. P. 27–33.

8. Yang Q., Hu L., Sun S., Song L. Related-key impossible differential analysis of full khudra // International Workshop on Security. Springer International Publishing, 2016. P. 135–146.

9. Tolba M., Abdelkhalek A., Youssef A.M. Impossible Differential Cryptanalysis of Reduced-Round SKINNY // Cryptology ePrint Archive: Report 2016/1115–2016.

10. PRINCE — a low-latency block cipher for pervasive computing applications / Borghoff J. et al. // International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2012. P. 208–225.

11. Rasoolzadeh S., Raddum H. Faster key recovery attack on round-reduced PRINCE // International Workshop on Lightweight Cryptography for Security and Privacy. Springer, Cham, 2016. P. 3–17.

12. Ronen E., Shamir A., Weingarten A.O., O'Flynn C. IoT goes nuclear: Creating a ZigBee chain reaction // Security and Privacy (SP), 2017 IEEE Symposium on.— IEEE, 2017. P. 195–212.

13. Shamir A., Biryukov A., Perrin L.P. Summary of an Open Discussion on IoT and Lightweight Cryptography // Proceedings of Early Symmetric Crypto workshop, 2017. University of Luxembourg, 2017.

References

1. Kuprijanovskij V.P. Internet veshhej na promyshlennyh predprijatijah / V.P. Kuprijanovskij, D.E. Namiot, V.I. Drozhzhinov, Ju.V.Kuprijanovskaja, M.O. Ivanov // Zhurn. International Journal of Open Information Technologies.– 2016. – vol.4,№12. – S. 69-78.

2. Otkazoustojchivost' [Jelektronnyj resurs] – Rezhim dostupa : www/ URL: https://dic.academic.ru/dic.nsf/ruwiki/1080344 – 01.10.2019 – Zagl. Z ekranu.

3. On the Feasibility of Attribute-Based Encryption on Internet of Things Devices / M. Ambrosin et al. // IEEE Micro Special Issue on Internet of Things — 2016.

4. Li F., Rahulamathavan Y., Rajarajan M., Phan R.C.-W. Low Complexity MultiAuthority Attribute Based Encryption Scheme for Mobile Cloud Computing // 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering. 2012. P. 573–577.

5. Xuanxia Y., Chen Z., Tian Y. A lightweight attribute-based encryption scheme for the Internet of Things // Future Generation Computer Systems, Elsevier B.V.— 2014.

6. Abed F., Forler C., List E., Lucks S., Wenzel J. Biclique cryptanalysis of present, led, and klein // Cryptology ePrint Archive: Report 2012/591–2012.

7. Sereshgi F., Dakhilalian M., Shakiba M. Biclique cryptanalysis of MIBS ‐ 80 and PRESENT ‐ 80 block ciphers // Security and Communication Networks. 2016. T. 9. № 1. P. 27–33.

8. Yang Q., Hu L., Sun S., Song L. Related-key impossible differential analysis of full khudra // International Workshop on Security. Springer International Publishing, 2016. P. 135–146.

9. Tolba M., Abdelkhalek A., Youssef A.M. Impossible Differential Cryptanalysis of Reduced-Round SKINNY // Cryptology ePrint Archive: Report 2016/1115–2016.

10. PRINCE — a low-latency block cipher for pervasive computing applications / Borghoff J. et al. // International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2012. P. 208–225.

11. Rasoolzadeh S., Raddum H. Faster key recovery attack on round-reduced PRINCE // International Workshop on Lightweight Cryptography for Security and Privacy. Springer, Cham, 2016. P. 3–17.

12. Ronen E., Shamir A., Weingarten A.O., O'Flynn C. IoT goes nuclear: Creating a ZigBee chain reaction // Security and Privacy (SP), 2017 IEEE Symposium on.— IEEE, 2017. P. 195–212.

13. Shamir A., Biryukov A., Perrin L.P. Summary of an Open Discussion on IoT and Lightweight Cryptography // Proceedings of Early Symmetric Crypto workshop, 2017. University of Luxembourg, 2017.

Рецензія/Peer review : 14.1.2020 р. Надрукована/Printed :22.2.2020 р.
Стаття рецензована редакційною колегією