Міністерство освіти і науки України
Державна наукова установа "Інститут модернізації змісту освіти"
Центральноукраїнський національний технічний університет

Комп'ютерна інженерія і кібербезпека: досягнення та інновації

Матеріали Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених

(м. Кропивницький, 27–29 листопада 2018 р.)

Кропивницький ЦНТУ 2018

УДК 004
ББК 32.97
К63

К63 **Комп'ютерна інженерія і кібербезпека : досягнення та інновації** : матеріали Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених (м. Кропивницький, 27–29 листоп. 2018 р.) / М–во освіти і науки України, Держ. наук. установа "Інститут модернізації змісту освіти", Центральноукр. нац. техн. ун–т. — Кропивницький: ЦНТУ, 2018. — 448 с.

Збірник містить тези доповідей учасників Всеукраїнської науково-практичної конференції здобувачів вищої освіти та молодих учених "Комп'ютерна інженерія і кібербезпека: досягнення та інновації" (м. Кропивницький, 27–29 листопада 2018 року). Праці присв'ячені актуальним питанням інформаційних систем і технологій, технологій проектування комп'ютерних систем та мереж, інженерії програмного забезпечення, комп'ютерних систем штучного інтелекту, мережних ІТ, комп'ютерної електроніки, логіки, схемотехніки, графіки, нормативно-правових засад забезпечення кібернетичної безпеки, інформаційної безпеки національного сегмента кіберпростору, боротьби з кіберзлочинністю, захисту програм та даних в комп'ютерних системах і мережах.

Видання призначене для аспірантів, докторантів, науковців, викладачів і студентів технічних спеціальностей закладів вищої освіти та всіх, хто цікавиться питаннями комп'ютерної інженерії й кібернетичної безпеки.

УДК 004
ББК 32.97
К63

Рекомендовано до друку Науково-технічною радою Центральноукраїнського національного технічного університету (протокол № 11 від 29 листопада 2018 р.)

Відповідальний за випуск: канд. техн. наук Доренський О. П.

Тексти матеріалів конференції друкуються у авторській редакції, мовою оригіналу. За достовірність наведених у публікаціях даних, назв, імен, цитат та іншої інформації відповідальність несуть автори.

Адреса організаційного комітету конференції
Центральноукраїнський національний технічний університет
Кафедра кібербезпеки та програмного забезпечення
просп. Університетський, 8, м. Кропивницький, 25006
(0522) 55-10-49, 39-04-49; cntu-conference@ukr.net; www.kntu.kr.ua

УДК 004.056.55

Федорко М. А., Маслова Н. О.
Донецький національний технічний університет

Застосування вітчизняних стандартів шифрування для захисту даних великих обсягів

Однією з основних проблем сучасності є стрімке зростання обсягів найрізноманітнішої інформації. Особливу роль в організації роботи з великими даними мають методи захисту інформації. Розповсюджені в даний час антивірусні засоби не призначені для забезпечення необхідного рівня безпеки таких даних, а стандарти з захисту великих даних на даний час ще не затверджено, тож проблема забезпечення безпеки Big Data є невирішеною та актуальною.

Метою роботи є дослідження сучасних алгоритмів шифрування та виявлення доцільності застосування вітчизняних стандартів при рішенні задач захисту та забезпечення конфіденційності та цілісності великих даних.

Найбільший внесок у розробку технологій захисту Big Data зроблено міжнародним альянсом Cloud Security Alliance (CSA), Національним інститутом стандартів і технологій США (NIST) та Агентством Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) [3-5]. Спеціалізовані рішення з захисту «великих даних» пропонують фірми IBM, Oracle, Cloudera, Forrester та ряд інших.

Основними напрямками захисту даних великих CSA вважають: захист обчислень в розподілених програмних системах; захист нереляційних баз даних; захист сховищ даних; процедури фільтрації і валідації даних; моніторинг безпеки у режимі online; забезпечення конфіденційності; криптографічний захист; гранульований контроль доступу; контроль походження даних (Data provenance).

Особливостями криптографічних підходів до обробки Big Data є відокремлена обробка інформації та метаданих, організація пошуку за допомогою булевих запитів на зашифрованих даних, порівняння даних без їх розшифрування, виявлення дублікатних даних в великих масивах на основі ключів [4] й інші.

Застосовується як відомі та розповсюджені алгоритми шифрування такі, як, наприклад, DES або AES, так і такі методи, як хешування паролів, наскрізне шифрування даних, пов'язане шифрування, шифрування на базі атрибутів (ABE), шифрування на базі ідентичності (IBE), конвергентне шифрування.

Необхідність застосування швидких криптографічних алгоритмів при роботі з Big Data та вимога мінімізувати ризики, пов'язані з застосуванням неузгоджених один з одним алгоритмів або програмних продуктів з невідомими прихованими функціями, вимагає звернути увагу на вітчизняні розробки.

Так, одним з сучасних вітчизняних алгоритмів шифрування є шифр Kalyna («Калина»), в основі якого лежить національний криптографічний стандарт України ДСТУ 7624:2014. Стандарт визначає структуру шифру та режими його роботи. Шифр є прикладом блочного симетричного перетворення і підтримує розмір блоку і довжину ключа шифрування 128, 256 і 512 біт.

Дослідження виконувалось на комп'ютерах під управлінням Windows - версій операційної системи. В процесі проведення експерименту застосовано персональні комп'ютери з характеристиками процесорів:

- Intel Core i7-7700HQ CPU @ 2.8Gz 2.8 GHz. 2-4 ядра. Кеш 1-го рівня (L1) - 256 КБ, 2-го рівня (L2) - 1024 КБ, 3-го рівня (L3) - 6144Кб.
- Intel Core i5-4200U CPU @ 2.3GHz 2.4 GHz, 2-4 ядра. Кеш 1-го рівня (L1) - 128КБ, 2-го рівня (L2) - 512 КБ, 3-го рівня (L3) - 3072Кб

- Intel Pentium® CPU N3700. Тактова частота 1600-2400 МГц. Кеш 1-го рівня (L1) - 224КБ, 2-го рівня (L2) - 2048 КБ, 3-го рівня (L3) – немає.

- Intel(R) Core(TM) i3-2310M CPU @ 2.10GHz 2 ядра. 3 MB SmartCache.

Розмір оперативної пам'яті у всіх випадках дорівнював 6Гб, включено 2 ядра, без прискорення. Криптографічні алгоритми, які досліджувалися для обрання найбільш ефективного варіанту: AES, Blowfish, IDEA, Camellia, Kalyna. Застосовані криптографічні бібліотеки Crypto API (C#), Cryptography (C++).

Проведені експерименти та результати.

Експеримент 1. Обрання швидкодіючого алгоритму.

Для виконання порівняння шифрів було розроблено програмне забезпечення, яке підтверджувало їх роботу і дозволяло заміряти час виконання криптографічних операцій.

Дослідження швидкодії алгоритмів (режим шифрування, розмір блоку 256, довжина повідомлення (10 304 байт = 82432 біт) кратна довжині блоків всіх алгоритмів).

Результати. Алгоритм AES показав найвищу швидкодію на всіх типах процесорів, що було задіяно в дослідженні.

Підтверджено, що в цілому, час виконання алгоритму «Калина» на тих самих пристроях має той же рівень швидкодії, що й стандартного AES – алгоритму з відповідною довжиною ключа.

Більш того, український шифр Kalyna продемонстрував ті ж тенденції зміни показників швидкодії, що й AES на блоках довжиною 128 та 256 бітів, а на сучасних типах процесорів шифр Kalyna випередив за швидкодією алгоритми IDEA і Camellia.

Відомо, що зараз Kalyna єдиний у світі стандарт блокового шифрування, що підтримує 512-бітові симетричні ключі. Можливість швидкої роботи з блоками даних значної довжини є перспективною при обробці даних великих обсягів.

Експеримент 2. Обрання технічних засобів (процесору) для роботи алгоритму.

В процесі досліджень доказано вплив архітектурних особливостей процесора на показники швидкодії алгоритму Kalyna. Експеримент проводився на означеному вище наборі пристроїв. На процесорі з кешем першого рівня L1 у 256КБ отримані найкращі результати на усіх трьох досліджених розмірах блоку - 128, 256, 512 біт (довжина ключа дорівнювала розміру блоку). Трохи нижча швидкодія виявилася для випадку, коли розмір кешу L1 дорівнював 128 КБ. Третя та четверта конфігурації обладнання доцільність застосування алгоритму Kalyna не показали.

Висновки. З оглядом на всі переваги вітчизняного алгоритму (нормальний, високий і надвисокий рівень стійкості, довжина блока і ключа 128, 256 і 512 бітів, односпрямована конструкція схеми розгортання ключів, циклове перетворення, стійкість до переборних атак та відомих методів аналізу), застосування шифру «Калина» для захисту великих даних на сучасних пристроях є перспективним.

Список використаних джерел

1. *Big Data Threat Landscape and Good Practice Guide. URL: https://www.enisa.europa.eu/publications/ bigdata-threat-landscape/at_download/fullReport*
2. *Big Data Security and Privacy Handbook: 100 Best Practices in Big Data Security and Privacy. Cloud Security Alliance: https://downloads.cloudsecurityalliance.org/assets/research/big-data/BigData_*
3. *NIST Special Publication 1500-1. NIST Big Data Interoperability Framework. URL: https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1.pdf (дата звернення 15.07.2018).*
4. *Принципи побудови і основні властивості нового національного стандарту блокового шифрування України / Р. Олійников, І. Горбенко, О. Казимиров, В. Руженцев, Ю. Горбенко // Захист інформації, том 17, №2, квітень-червень 2015, С.142-157.*