УДК 681.3.06:006.354

ОСНОВНІ ВЛАСТИВОСТІ НОВОГО НАЦІОНАЛЬНОГО СТАНДАРТУ БЛОКОВОГО ШИФРУВАННЯ ДСТУ 7624:2014

[*]**Р.В. Олійников**, д-р техн. наук, доц.; [*]**І.Д. Горбенко**, д-р техн. наук, проф.;
[**]**О.В.Казимиров**, канд. техн. наук; [**]**В.І. Руженцев**, канд. техн. наук, доц..;
[***]**О.О. Кузнєцов**, д-р техн. наук, проф.; [*]**Ю.І. Горбенко**, канд. техн. наук;
[***]**В.І.Долгов**, д-р техн. наук, проф.; [****]**О.В. Дирда**, канд. техн. наук;
[****]**А.І. Пушкарьов**; [***]**Р.І. Мордвинов**, [***]**Д.С.Кайдалов**
[*]Приватне акціонерне товариство «Інститут інформаційних технологій»
ROliynykov@gmail.com
[**]Харківський національний університет ім. В.Н.Каразіна
[***]Харківський національний університет радіоелектроніки
[****]Державна служба спеціального зв'язку і захисту інформації України

З 1-го липня 2015 р. в Україні вводиться в дію стандарт криптографічного перетворення ДСТУ 7624:2014 [1], що визначає блоковий шифр "Калина" та режими його роботи. Національний стандарт розроблений у співпраці Державної служби спеціального зв'язку та захисту інформації України і провідних українських науковців на основі проведення відкритого конкурсу криптографічних алгоритмів.

Новий шифр підтримує комбінації довжини ключа і розміру блоку від 128 до 512 бітів, забезпечуючи високий і надвисокий рівень криптографічної стійкості. Алгоритм побудований на основі SPN-структури, що включає ітеративне застосування шару нелінійного перетворення (S-блоків), зсуву рядків стану шифру і множення на МДВ-матрицю. Для підвищення складності атак лінійного, диференційного і алгебраїчного криптоаналізу додатково застосовується попереднє и прикінцеве забілювання (pre- and postwhitening) із використанням додавання за модулем 2^{64}.

Стандарт передбачає використання чотирьох S-блоків, які не є CCZ-еквівалентними. При порівнянні характеристик підстановок алгоритму „Калина" та інших перетворень, в т.ч. нових білоруських і російських стандартів [2,3] можна відзначити, що саме національний стандарт України забезпечує найбільшу нелінійність булевих функцій S-блоку, що дає додатковий запас стійкості до лінійного криптоаналізу. Більш високе значення нелінійності для бієктивного S-блока можна отримати використовуючи, наприклад, афінно-еквівалентні степенні функції у скінченому полі, але такі перетворення, можуть бути описані перевизначеною системою 2-го степеня, що ставить шифр під загрозу реалізації алгебраїчної атаки.

Для реалізації блоку лінійного розсіювання було обране множення на МДВ-матрицю як найбільш ефективний метод реалізації впливу кожного вхідного символу на кожний вихідний завдяки отриманню найбільшого індексу галуження (branch number) відображення.

Схема формування ключів використовує односпрямований генератор псевдовипадкових послідовностей, який побудований виключно на базі циклового перетворення блокового шифру „Калина" і задовольняє вимогам як з точки зору криптографічних властивостей, так і обмеження на кількість операцій.

Таким чином, блоковий шифр „Калина" побудований на основі Rijndael-подібної структури із аналітичним обґрунтуванням саме цієї конструкції, але на відміну від AES в новому національному стандарті України застосовуються:

– попереднє и прикінцеве забілювання (pre- and postwhitening) із використанням модульного додавання (2^{64}) для підвищення складності атак лінійного, диференційного і алгебраїчного криптоаналізу;

– чотири S-блока (замість одного), які не є CCZ-еквівалентними, не можуть бути описані перевизначеною системою 2-го степеня, і при порівнянні характеристик з іншими перетвореннями забезпечують найбільшу нелінійність булевих функцій;

– збільшений розмір МДВ-перетворення, що покращує криптографічні властивості і є оптимальним для швидкодіючої реалізації на сучасних 64-бітових платформах;

– нова односпрямована схема розгортання циклових ключів, що забезпечує як захист від атак на схеми розгортання, так і додаткову стійкість до низки методів криптографічного аналізу, спрямованого, в тому числі, і на апаратну або програмну реалізацію перетворення;

– різні комбінації розміру блоку і довжини ключа (128, 256 і 512 бітів).

Криптографічне перетворення є стійким при 6 циклах для 128-бітового блоку, 7 циклах для 256-бітового і 9 циклах для 512-бітового. Таким чином, шифр, який містить 10, 14 і 18 циклів, заданих у стандарті, для розміру блоку 128, 256 і 512 біт відповідно, забезпечує захист від всіх розглянутих методів криптоаналізу і має достатній запас стійкості.

Додатково, нові національні стандарти шифрування ДСТУ 7624:2014 і ґешування ДСТУ 7564:2014 мають спільний набір S-блоків та однакову МДВ-матрицю, за рахунок чого отримується компактна реалізація обох перетворень.

Тестування швидкодії було спрямоване на моделювання особливостей роботи засобів криптографічного захисту, що потребують високої продуктивності перетворень (захист IP-трафіку та ін.). Вимірювання швидкодії оптимізованої програмної реалізації мовою C++ з компілятором gcc v4.9.2 виконувалось через шифрування однакового обсягу відкритих текстів (режим простої заміни) на комп'ютері під управлінням 64-бітової ОС Linux з процесором Intel Core i5-4670@3.40GHz для всіх комбінацій розміру блоку і довжини ключа: Калина-128/128 (2611.77 Мб/с), Калина-128/256 (1779.52 Мб/с), Калина-256/256 (2017.97 Мб/с), Калина-256/512 (1560.89 Мб/с), Калина-512/512 (1386.46 Мб/с) та AES-128 (2525.89 Мб/с), AES-256 (1993.53 Мб/с), ГОСТ 28147-89 (639.18 Мб/с), СТБ 34.101.31-2011 (1055.92 Мб/с), «Кузнечик» (1081.08 Мб/с). Таким чином, на 64-бітовій платформі швидкодія „Калини" порівняна з AES (вища на 86 Мбіт/с, або 3% для 128-бітового блоку, і т.д.). При відповідній довжині ключа „Калина" швидша за ГОСТ 28147-89 у 2,8 рази або 3,16 рази (залежно від розміру блоку), і приблизно у 2 рази вища, ніж у нових стандартів шифрування Білорусії і Росії. Додатково слід зазначити, що „Калина" забезпечує суттєво більш високий запас стійкості до криптоаналітичних атак, ніж AES.

Література

1. **ДСТУ 7624:2014**. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Текст]. – Введ. 01–07–2015. – К. : Мінекономрозвитку України, 2015.
2. **СТБ 34.101.31–2011**. Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности [Текст]. – Взамен СТБ П 34.101.31–2007 ; введ. 31–01–2011. – Минск, 2011. – 35 с.
3. **Проект национального стандарта Российской Федерации**. Информационная технология. Криптографическая защита информации. Блочные шифры. М. : Стандартинформ, 2015. – 25 с. [Electronic resource]. – Mode of access : www. URL: http://www.tc26.ru/standard/draft/GOSTR-bsh.pdf.

Р.В. Олійников, І.Д. Горбенко та ін. **Основні властивості нового національного стандарту блокового шифрування ДСТУ 7624:2014.**

У доповіді розглянуті сучасні проблеми розробки блокових шифрів та їхні вирішення, впроваджені розробниками у новому національному стандарті України. Наведені результати аналізу криптографічної стійкості, а також порівняння швидкодії на сучасних програмних платформах із іншими шифрами, які є міжнародними та національними стандартами.

Ключові слова: *ДСТУ 7624:2014, блоковий шифр, криптоаналіз, швидкодія шифрування, національний стандарт.*

R.V.Oliynykov, I.D. Gorbenko et. al. **Main properties of the new national standard of block encryption DSTU 7624:2014.**

It is considered modern problems of block ciphers design and its solutions introduced by the developers at the new national standard of Ukraine. It is given results of cryptographic strength analysis as well as performance comparison on modern software platforms with other international and national standards of the block encryption.

Key words: DSTU 7624:2014, block cipher, cryptanalysis, encryption performance, national standard.