УДК 004.056.55 **DOI:10.30837/rt.2021.1.204.05**

М.В. ЄСІНА, канд. техн. наук, Б.С. ШАХОВ

ДОСЛІДЖЕННЯ ТА АНАЛІЗ РЕАЛІЗАЦІЙ КАНДИДАТІВ ДРУГОГО РАУНДУ КОНКУРСУ NIST PQC, ЩО ОРІЄНТОВАНІ НА СІМЕЙСТВА FPGA XILINX

Вступ

На сьогодні достатньо гостро постає проблема стійкості існуючих криптографічних механізмів захисту до квантових алгоритмів криптоаналізу та квантових комп'ютерів взагалі. Ця проблема є обговорюваною на міжнародному рівні. І задля її вирішення NIST США вирішив організувати та провести конкурс на постквантові криптографічні алгоритми NIST PQC. Результатом конкурсу повинне стати прийняття до стандартизації алгоритмів типу асиметричне шифрування, інкапсуляція ключів та електронний підпис (як мінімум, по одному алгоритму з кожного типу).

На момент початку конкурсу на процес стандартизації було представлено 82 алгоритми. На основі критеріїв мінімальної прийнятності, визначених NIST, для першого раунду було розглянуто 69 алгоритмів. Враховуючи декілька параметрів – безпеку, вартість, продуктивність, характеристики реалізації тощо, 43 і 11 алгоритмів були виключені при завершенні першого і другого раундів відповідно, а інші 15 алгоритмів були збережені для третього раунду [4].

Алгоритми, які залишилися у другому раунді, можна розділити на 5 різних категорій залежно від математичного базису, на якому вони засновуються: на основі ізогеній еліптичних кривих (1 алгоритм), на основі алгебраїчних решіток (12 алгоритмів), на основі математичного коду (7 алгоритмів), на основі багатовимірних перетворень (4 алгоритми) і на основі геш-функцій (2 алгоритми) [4, 5].

Безпека є основним критерієм оцінки, що визначає конкуренцію в конкурсі NIST, і, зрозуміло, що реалізації програмного забезпечення кандидатів в основному зосереджені на ній. Однак, вкрай важливо аби алгоритм мав й ефективну апаратну реалізацію. А своєчасне виявлення апаратної неефективності допоможе сконцентрувати зусилля криптографічної спільноти на більш перспективних кандидатах, потенційно заощадивши велику кількість часу, що може бути витрачена на криптоаналіз [3].

Апаратне і програмне забезпечення

Криптографічні алгоритми зазвичай реалізуються з використанням як програмного, так і апаратного забезпечення. Під програмним розуміються реалізації, які можуть бути виконані з використанням апаратних процесорів. Ці процесори можуть варіюватися від недорогих малопотужних вбудованих процесорів, таких як ARM Cortex-M4, до високопродуктивних мікропроцесорів загального призначення, таких як Intel Core i7, з мікроархітектурою Haswell, що підтримують Advanced Vector Extensions 2 (AVX2) і AES New Instructions (AES-NI). Загальною характеристикою є те, що всі ці процесори зазвичай програмуються з використанням мов програмування високого рівня, таких як C. Код, написаний цими мовами, легко переноситься між різними типами процесорів. Програмне забезпечення може бути додатково оптимізовано за допомогою програмування мовою асемблера, що включає інструкції, специфічні для даного процесора (або, точніше, для його архітектури набору інструкцій (ISA)). Програми мовою асемблера не так легко переносяться між процесорами, що працюють на базі різних ISA [1].

Під апаратним забезпеченням розуміються реалізації, які можуть бути виконані з використанням програмованої користувачем вентильної матриці (FPGA), інтегральних схем спеціального призначення (ASIC), програмованої логіки (PL) системи на чіпі FPGA (SoC FPGA), спеціалізованих стандартних продуктів (ASSP) тощо. Основною особливістю є те, що більшість цих реалізацій розробляється з використанням мов опису апаратури (HDL), таких як

VHDL і Verilog. Ці мови суттєво відрізняються від мов програмування високого рівня тим, що в них вводяться поняття сутності, зв'язку, збігу і синхронізації. Вихідний код HDL перетворюється інструментом синтезу в мережевий список, що складається з основних логічних компонентів і з'єднань між цими компонентами. В силу своєї універсальної природи, HDL код може бути легко перенесений між різними технологіями, такими як FPGA і ASIC. Реалізації ASIC швидше, використовують менше енергії і вимагають менше місця на робочому просторі. Реалізації FPGA мають ряд переваг: менш дорогі засоби розробки, набагато менший цикл проектування, а також реконфігурованість, що розуміється як здатність змінювати функції усіх внутрішніх структурних елементів і з'єднань між ними, навіть після того, як задана інтегральна схема була встановлена у реальних пристроях [1].

Сімейство FPGA

Хоча програмні реалізації, швидше за все, будуть домінувати на першому етапі впровадження стандартів PQC в реальних додатках, апаратні реалізації неминуче будуть наступними. Вони, швидше за все, почнуться з апаратних прискорювачів для обмежених середовищ, таких як смарт-картки та пристрої Інтернету речей. Низьковитратні малопотужні процесори, використовувані в таких додатках, можуть не встигати за підвищеними вимогами до обчислювальної потужності і енергоспоживання. Таким чином, ці процесори, можливо, доведеться розширити за рахунок апаратних прискорювачів. У найближчій перспективі з'являться високопродуктивні процесори безпеки, вдосконалені новими стандартами PQC. Ці процесори будуть оптимізовані для обробки на апаратному рівні всіх алгоритмів, пов'язаних з безпечною комунікацією (наприклад, що використовуються в постквантових версіях протоколів TLS, IPSec, IKE і WTLS/WAP) і безпечним зберіганням. Нарешті, в більш довгостроковій перспективі підтримка нових інструкцій, що забезпечують ефективну і стійку до збоїв реалізацію стандартів PQC, швидше за все, буде додана в найбільш популярні процесорні ISA. Співпроцесори для таких інструкцій є, по суті, апаратною реалізацією PQC. Враховуючи, що нові PQC-стандарти, швидше за все, будуть використовуватися протягом довгого часу, всім вказаним випадкам застосування слід приділити особливу увагу. Зокрема, продуктивність алгоритму на апаратному рівні може вплинути на його довгострокову продуктивність в програмному забезпеченні, на процесорах, обладнаних новими спеціалізованими інструкціями. Навіть, якщо апаратні реалізації 2-го раунду не є остаточними з точки зору продуктивності алгоритму, вони дають перше уявлення про придатність кожного кандидата для апаратного прискорення. Вони також створюють відкриту базу вихідних кодів, на якій в 3-му раунді і далі можуть бути вбудовані більш оптимізовані реалізації і реалізації, захищені від атак бічними каналами і збоїв [1].

При використанні однієї і тієї ж технології апаратні реалізації перевершують програмні, використовуючи як мінімум один і, як правило, декілька показників, таких як швидкість, споживана потужність, енергоспоживання і захист від фізичних атак. Вони також дозволяють значно підвищити гнучкість при використанні одного набору цих показників по відношенню до іншого. З точки зору еталонного тестування і ранжування кандидатів, така гнучкість може стати великою проблемою, особливо з урахуванням того, що жодні два показники, швидше за все, не матимуть простої лінійної залежності один від одного. Практичне розв'язання цієї проблеми полягає в тому, щоб в процесі оцінки зосередитися на двох основних типах реалізації: високій швидкості і малоресурсності [1].

У високошвидкісних реалізаціях основною метою є швидкість. Для схем PQC ця мета зводиться до мінімізації часу виконання основних операцій з використанням відкритого та особистого ключа відповідно. Для механізмів інкапсуляції ключів (KEM) ці операції являють собою інкапсуляцію і декапсуляцію; для схем електронного підпису – перевірку і генерацію підписів; для шифрування з відкритим ключем (PKE) – шифрування і розшифрування. Час генерації ключів може також відігравати значну роль у тому випадку, коли з міркувань безпеки пара відкритий/особистий ключ не може бути повторно використана. Використання

ресурсів є другорядним. Проте, розробники апаратного забезпечення, як правило, прагнуть досягнення оптимальності закону Парето, в якому будь-яке подальше покращення швидкості досягається за рахунок непропорційно великих витрат з точки зору використання ресурсів. Головною перевагою високошвидкісних реалізацій є те, що вони розкривають закладений в них потенціал даного алгоритму розпаралелювання. Поки межа використання ресурсів досить висока, вона не впливає на ранжування алгоритмів. У результаті, ранжування сильно співвідноситься з особливостями самих алгоритмів і не схильне до істотного впливу будь-яких додаткових припущень і вибору технології. Крім того, тільки високошвидкісні апаратні реалізації можуть ефективно конкурувати з оптимізованими програмними реалізаціями, націленими на високопродуктивні процесори з векторними інструкціями (наприклад, AVX2) [1].

У малоресурсних реалізаціях основними цілями, як правило, є мінімальне використання ресурсів і мінімальне енергоспоживання, за умови, що час виконання не перевищує визначеного максимуму. Інший метод формулювання мети – досягнення мінімального часу виконання, припускаючи заданий максимальний бюджет з точки зору використання ресурсів, енергоспоживання або енерговитрат. Максимальний бюджет з використання ресурсів пов'язаний з вартістю реалізації; при цьому бюджет з потужності забезпечує правильну роботу без перегріву або виділення додаткових ресурсів на охолодження. Максимальне використання енергії впливає на те, як довго пристрій, що працює від акумулятора, може функціонувати до наступної зарядки акумулятора. У контексті процесу стандартизації криптографічних алгоритмів вказані максимальні бюджети вибрати дуже складно. Будь-яка зміна цих порогових значень може сприятливо позначитися на іншому наборі кандидатів. У зв'язку з тим, що нові стандарти залишаються в експлуатації протягом десятиліть, вимоги до термінів, вартості та потужності нових, і додатків, які ще з’являться, дуже важко передбачити [1].

Крім того, зміни в технології істотно впливають на те, які апаратні архітектури задовольняють конкретним вимогам. Наприклад, архітектура, здатна досягти часу виконання 0.1 секунди (або нижче) при певному бюджеті на електроенергію або енергоспоживання, може істотно змінитися з покращенням технології. В результаті, більшість поточних лімітів обираються різними розробниками довільно або залишаються невизначеними в своїх звітах. Отже, ранжування кандидатів PQC на основі їх полегшених впроваджень, особливо розроблених різними групами, є надзвичайно складним і залежним від припущень. Таке ранжирування має мало спільного з розпаралелюванням, допустимим кожним алгоритмом, так як більшість операцій повинно виконуватися послідовно через малий об'єм ресурсів. Основною особливістю алгоритмів, які виявляються в цих реалізаціях, є кількість і складність окремих елементарних операцій. Кожна головна операція містить в собі додатковий функціональний модуль, збільшуючи використання ресурсів і енергоспоживання. Крім того, малоресурсні апаратні реалізації можуть перевершити тільки програмні реалізації, націлені на конкретні недорогі вбудовані процесори з низьким енергоспоживанням, такі як Cortex-M4 [1].

У разі реалізації FPGA використання ресурсів є вектором, таким як (#LUT, #flip-flops, #DSP модулів, #BRAM). Жоден елемент цього вектора не може бути виражений в термінах інших елементів. У результаті, введення ліміту ресурсів передбачає вказівку значень всіх компонентів цього вектора ресурсів. Одним з можливих підходів може бути вибір ресурсів найменшої FPGA із заданого недорогого сімейства FPGA. Однак сімейства FPGA і їх ресурси з часом змінюються, тому цей обмежувач має тільки фізичне значення протягом обмеженого періоду часу, що охоплює період оцінки, і може втратити свою значимість лише через кілька років після публікації і застосування стандарту. Нарешті, один і той же пристрій FPGA може також знадобитися для розміщення будь-яких накладних витрат, пов'язаних з протидією атакам побічними каналами. У той же час ці надлишкові або навіть ефективні заходи протидії, можуть залишитися невідомими під час оцінки кандидатів [1].

Сімейство FPGA Xilinx

Однією з основних проблем є рекомендація NIST сфокусуватися на порівняльному аналізі апаратного забезпечення з використанням сімейства FPGA Xilinx Artix-7. Ця рекомендація була представлена у декількох презентаціях NIST, пов'язаних з 2-м раундом процесу стандартизації NIST, наприклад, під час PQCrypto 2019 у травні 2019 р. і другій конференції з стандартизації PQC в серпні 2019 р. У своїй нинішній формі ця рекомендація недоцільна і швидше перешкоджає, ніж підтримує справедливе і всеосяжне апаратне і програмно-апаратне еталонне тестування [1].

Сімейство FPGA представляє собою набір пристроїв FPGA, що мають однакову внутрішню структуру і одну й ту ж технологію (також відому як технічний вузол або вузол процесу), що описується числом, пов'язаним з розмірами і щільністю транзисторів, які можуть бути виготовлені з використанням певного промислового процесу. Завдяки неухильному вдосконаленню технології виробництва, описаного в законі Мура, максимальна ємність і швидкість роботи FPGA-пристроїв неухильно ростуть, в той час як їх ціни залишаються приблизно на тому ж рівні. Кожне нове покоління FPGA-пристроїв певного виробника отримує унікальне ім'я, так зване сімейство. Кожне сімейство складається з декількох пристроїв різного розміру для задоволення потреб різних додатків. Всі пристрої певного сімейства мають однакову внутрішню архітектуру і технологію обробки, але відрізняються кількістю ресурсів певного типу, таких як таблиця пошуку (LUT), flip-flops (FF), блок пам'яті та цифрові блоки обробки сигналів (DSP) або мультиплікатори. Більшість виробників випускають як недорогі сімейства (наприклад, Xilinx Artix-7), так і високопродуктивні (наприклад, Xilinx Virtex-7). Більшість з них також випускають сімейства середнього класу, такі як Xilinx Kintex-7. Максимальна кількість ресурсів, доступних в найбільшому пристрої дешевого сімейства, звичайно, значно менша, ніж аналогічна кількість в найбільшому пристрої сімейства високопродуктивних пристроїв (наприклад, більш ніж в п’ять разів менше для Artix-7 у порівнянні з Virtex-7) [1].

Крім того, останнім часом виробники FPGA почали випускати нові типи програмованих пристроїв, які покращують програмувальну логіку традиційних FPGA за допомогою системи обробки, заснованої на вбудованому процесорі з жорсткою проводкою, наприклад ARM. Так як цей процесор спроектований на замовлення, він повною мірою використовує переваги даного технологічного процесу і працює на тактовій частоті значно вище, ніж програмувальна логіка. Завдяки швидкому процесору і ефективному інтерфейсу між цим процесором і програмувальною логікою ці пристрої ідеально підходять для спільного проектування програмних/апаратних засобів, націлених на високу швидкість. Хоча ці типи пристроїв з'являються під декількома комерційними назвами, їх часто колективно називають SoC FPGA. Першим сімейством такого типу був Xilinx Zynq-7000, випущений в 2011 р., заснований на вбудованих процесорах ARM Cortex-A9 [1].

Конструкція обладнання описується мовами апаратного опису. Код HDL, як правило, ідентичний для всіх родин FPGA. На відміну від програмного забезпечення, де для кожного процесора може знадобитися свій оптимізований код на асемблері, для апаратного забезпечення таких концепцій не існує. У результаті, легко синтезувати один і той же код HDL, призначений для різних сімейств FPGA від різних виробників, за умови, що максимальна ємність найбільшого пристрою даного сімейства не буде перевищена.

Загальні характеристики сімейства FPGA Xilinx

Сьогодні найсучаснішою є серія 7 FPGA Xilinx – Artix-7, Kintex-7, Virtex-7. У цій серії анонсовано сімейство FPGA з процесорним ядром ARM Cortex-A9 – Zynq-7000. У новій серії тільки Virtex-7 продовжує існуючу лінійку високопродуктивних FPGA, а два інших сімейства – Artix і Kintex – замінили лінійку Spartan. FPGA Artix призначені для масової продукції, і відрізняються малим енергоспоживанням і невисокою вартістю, а Kintex являє собою, деякою мірою, Spartan, спеціалізований для цифрової обробки сигналів. Досі серія Virtex

традиційно використовувалася і в додатках, побудованих навколо високошвидкісних послідовних приймачів, і в проектах, заснованих на цифровій обробці сигналів. Сімейство Kintex-7 вдало вписується в нішу, де потрібна велика кількість паралельно працюючих блоків ЦОС за помірною ціною, а для систем з великою кількістю апаратних приймачів призначені більш дорогі Virtex-7 (табл. 1) [6].

Таблиця 1

Зведені характеристики сімейств FPGA Xilinx серії 7

Максимальні параметри	Artix-7	Kintex-7	Virtex-7
Логічні комірки, тис.	352	407	1955
Блочна пам'ять	12	29	65
Секції DSP	700	1540	3960
Пікова продуктивність цифрової обробки сигналів для фільтрів з симетричними коефіцієнтами, GMAC/с	504	1965	5053
Приймачі	4	16	88
Максимальна швидкість передачі, Гб/с	3,75	10.325	28,05
Пікова пропускна здатність приймачів, Гб/с	30	330	2784
Інтерфейси PCI Express	Gen1x4	Gen2x8	Gen3x8
Швидкість обміну інтерфейсами пам'яті, МБ/с	800	2133	2133
Зовнішні виводи	450	500	1200

Мікросхеми Zynq-7010 і Zynq-7020 виконані на базі програмованих ресурсів сімейства Artix, а Zynq-7030 і Zynq-7040 – на базі Kintex. Це відображається на піковій продуктивності підсистеми цифрової обробки сигналів – тактова частота молодших FPGA Zynq нижче, в них немає блоків PCI Express і високошвидкісних приймачів (табл. 2) [6].

Таблиця 2

Характеристики FPGA сімейства Zynq-7000

Параметри	Z-7010	Z-7020	Z-7030	Z-7040
Програмовані логічні комірки (вентилі ASIC)	28 K (430 K)	85 K (1,3 M)	125 K (1,9 M)	235 K (3,5 M)
Блоки пам'яті (36 кб)	60	140	265	760
Секції DSP (18x25 MACC)	80	220	400	760
Пікова продуктивність DSP для KIX з симетричними коефіцієнтами, GMAC/с	58	158	480	912
Блоки PCI Express	-	-	Gen2 x4	Gen2 x8
АЦП	2x12 біт, 1 M вибірок/с, 17 диф. каналів			
Шифрування	AES і SHA 256-біт			
Блоки вводу-виводу, 3.3 В	100	195	100	200
Блоки вводу-виводу, 1.8 В	-	-	150	150
Високошвидкісні приймальники	-	-	4	12

Ключова властивість нового покоління FPGA – уніфікація програмованих ресурсів. Передбачається, що для нового покоління FPGA стане можливою швидка міграція між сімействами Virtex/Kintex/Artix без коригування проекту.

Детальні характеристики сімейства FPGA Xilinx

Далі наведені характеристики FPGA сімейства Xilinx, а саме: Spartan-7, Artix-7, Virtex-7, Kintex-7 [2].

Таблиця 3

Характеристика FPGA Spartan-7

				Оптимізація вводу-виводу при найменших витратах і максимальній продуктивності на ват (1.0V, 0.95V)					
Номер деталі				XC7S6	XC7S15	XC7S25	XC7S50	XC7S75	XC7S100
Логічні ресурси	Логічні комірки			6,000	12,800	23,360	52,160	76,800	102,400
	Частини			938	2,000	3,650	8,150	12,000	16,000
	Тригери CLB			7,500	16,000	29,200	65,200	96,000	128,000
Ресурси пам'яті	Максимум розподіленої оперативної пам'яті (Кб)			70	150	313	600	832	1,100
	Блок RAM/FIFO з ECC (по 36 Кб)			5	10	45	75	90	120
	Всього блоків ОЗП (Кб)			180	360	1,620	2,700	3,240	4,320
Часові ресурси	Елементи керування часом (1 MMCM + 1 PLL)			2	2	3	5	8	8
Ресурси вводу-виводу	Максимум контактів вводу/виводу з одним кінцем			100	100	150	250	400	400
	Максимум диференційних пар вводу/виводу			48	48	72	120	192	192
Вбудовані ресурси жорсткої IP-адреси	Фрагменти DSP			10	20	80	120	140	160
	Аналоговий змішаний сигнал (AMS)/XADC			0	0	1	1	1	1
	Налаштування блоків AES/HMAC			0	0	1	1	1	1
Марки швидкості	Комерційна температура (C)			-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2
	Промислова температура (I)			-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L
	Розширена температура (Q)			-1	-1	-1	-1	-1	-1
	Упаковка	Площа (мм)	Крок (мм)	Доступний ввід-вивід користувача: 3.3V SelectIO™ Ввід-вивід HR					
	CPGA196	8x8	0.5	100	100				
	CSGA225	13x13	0.8	100	100	150			
	CSGA324	15x15	0.8			150	210		
	FTGB196	15x15	1.0	100	100	100	100		
	FGGA484	23x23	1.0				250	338	338
	FGGA676	27x27	1.0					400	400

Таблиця 4

Характеристика FPGA Artix-7

		Оптимізація приймача при найменших витратах і максимальній пропускній здатності DSP (1.0V, 0.95V, 0.9V)							
Номер деталі		XC7A12T	XC7A15T	XC7A25T	XC7A35T	XC7A50T	XC7A75T	XC7A100T	XC7A200T
Логічні ресурси	Логічні комірки	12800	16,640	23,360	33,280	52,160	75,520	101,440	215,360
	Частини	2,000	2,600	3,650	5,200	8,150	11,800	15,850	33,650
	Тригери CLB	16,000	2,800	29,200	41,600	65,200	94,400	126,800	269,200
Ресурси пам'яті	Максимум розподіленої оперативної пам'яті (КБ)	171	200	313	400	600	892	1,188	2,888
	Блок RAM/FIFO з ECC (по 36 Кб)	20	25	45	50	75	105	135	365
	Всього блоків ОЗП (Кб)	720	900	1,620	1,800	2,700	3,780	4,860	13,140
Часові ресурси	Елементи керування годинами (1 MMCM + 1 PLL)	3	5	3	5	5	6	6	10
Ресурси вводу-виводу	Максимум контактів вводу/виводу з одним кінцем	150	250	150	250	250	300	300	500
	Максимум диференційних пар вводу/виводу	72	120	12	120	120	144	144	240

продовження табл. 4

Вбудовані ресурси жорсткої IP-адреси	Фрагменти DSP			40	45	80	90	120	180	240	740
	PCIe® Gen2			1	1	1	1	1	1	1	1
	Аналоговий змішаний сигнал (AMS)/XADC			1	1	1	1	1	1	1	1
	Налаштування блоків AES/HMAC			1	1	1	1	1	1	1	1
	Приймачі GTP (не більше 6,6 Гбіт/с)			2	4	4	4	4	8	8	16
Марки швидкості	Комерційна температура (C)			-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2
	Розширена температура (E)			-2L -3	-2L -3	-2L -3	-2L -3	-2L -3	-2L -3	-2L -3	-2L -3
	Промислова температура (I)			-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L	-1 -2 -1L
	Упаковка	Площа (мм)	Крок (мм)	Доступний ввід-вивід користувача: 3.3V SelectIO™ Ввід-вивід HR (Приймачі GTP)							
	CPG236	10x10	0.5		106(2)		106(2)	106(2)			
	CPG238	10x10	0.5	112(2)		112(2)					
	CSG324	15x15	0.8		210(0)		210(0)	210(0)	210(0)	210(0)	
	CSG325	15x15	0.8	150(2)	150(4)	150(4)	150(4)	150(4)			
	FTG256	17x17	1.0		170(0)		170(0)	170(0)	170(0)	170(0)	
	SBG484	19x19	0.8								285(4)
Сумісне місце	FGG484	23x23	1.0		250(4)		250(4)	250(4)	285(4)	285(4)	
	FBG484	23x23	1.0								285(4)
Сумісне місце	FGG676	27x27	1.0						300(8)	300(8)	
	FBG676	27x27	1.0								400(8)
	FFG1156	35x35	1.0								500(16)

Таблиця 5

Характеристика FPGA Kintex-7

		Оптимізовано для кращої ціни і продуктивності (1.0 В, 0.95 В, 0.9 В)						
Номер деталі		XC7K70T	XC7K160T	XC7K325T	XC7K355T	XC7K410T	XC7K420T	XC7K480T
Логічні ресурси	Логічні комірки	10,250	25,350	50,950	55,650	63,550	63,150	74,650
	Частини	65,600	162,240	326,080	356,160	406,720	416,960	477,760
	Тригери CLB	82,000	202,800	407,600	445,200	508,400	521,200	597,200
Ресурси пам'яті	Максимум розподіленої оперативної пам'яті (КБ)	838	2,188	4,000	5,088	5,663	5,938	6,778
	Блок RAM/FIFO з ECC (по 36 Кб)	135	325	445	715	795	835	955
	Всього блоків ОЗП (Кб)	4,860	11,700	16,020	25,740	28,620	30,060	34,380
Часові ресурси	Елементи керування годинами (1 MMCM + 1 PLL)	6	8	10	6	10	8	8
Ресурси вводу-виводу	Максимум контактів вводу/виводу з одним кінцем	300	400	500	300	500	400	400
	Максимум диференційних пар вводу/виводу	144	192	240	144	240	192	192
Вбудовані ресурси жорсткої IP-адреси	Фрагменти DSP	240	600	840	1,440	1,540	1,680	1,920
	PCIe® Gen2	1	1	1	1	1	1	1
	Аналоговий змішаний сигнал (AMS)/XADC	1	1	1	1	1	1	1
	Налаштування блоків AES/HMAC	1	1	1	1	1	1	1
	Приймачі GTP (не більше 12,5 Гбіт/с)	8	8	16	24	16	32	32

продовження табл. 5

Марки швид-кості	Комерційна температура (C)			-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2
	Розширена температура (E)			-2L -3	-2L -3	-2L -3	-2L -3	-2L -3	-2L -3	-2L -3
	Промислова температура (I)			-1 -2 -2L	-1 -2 -2L	-1 -2 -2L	-1 -2 -2L	-1 -2 -2L	-1 -2 -2L	-1 -2 -2L
	Упаков-ка	Площа (мм)	Крок (мм)	Доступний власний ввід-вивід: 3.3V ввід-вивід HR, 1.8V ввід-вивід HP (GTX)						
	FBG484	23x23	1.0	185, 100 (4)	185, 100 (4)					
Сумісне місце	FBG676	27x27	1.0	200, 100 (8)	250, 150 (8)	250, 150 (8)		250, 150 (8)		
	FFG676	27x27	1.0		250, 150 (8)	250, 150 (8)		250, 150 (8)		
Сумісне місце	FBG900	31x31	1.0			350, 150 (16)		350, 150 (16)		
	FFG900	31x31	1.0			350, 150 (16)		350, 150 (16)		
	FFG901	31x31	1.0				300, 0 (24)		380, 0 (28)	380, 0 (28)
	FFG1156	35x35	1.0						400, 0 (32)	400, 0 (32)

Таблиця 6

Характеристика FPGA Virtex-7

		Оптимізовано для максимальної продуктивності та ємності системи (1.0 В)										
Номер деталі		XC7V 585T	XC7V2 000T	XC7VX 330T	XC7VX 415T	XC7VX 485T	XC7VX 550T	XC7VX 690T	XC7VX 980T	XC7VX 1140T	XC7VH 580T	XC7VH 870T
Логічні ресурси	Частини	91,050	305,400	51,000	64,400	75,900	86,600	108,300	153,000	178,000	90,700	136,900
	Логічні комірки	582,720	1,954,560	326,400	412,160	485,760	554,240	693,120	979,200	1,139,200	580,480	876,160
	Тригери CLB	728,400	2,443,200	408,000	515,200	607,200	692,800	866,400	1,224,000	1,424,000	725,600	1,095,200
Ресурси пам'яті	Максимум розподіленої оперативної пам'яті (КБ)	6,938	21,550	4,388	6,525	8,175	8,725	10,888	13,838	17,700	8,850	13,275
	Блок RAM/FIFO з ECC (по 36 Кб)	795	1,292	750	880	1,030	1,180	1,470	1,500	1,880	940	1,410
	Всього блоків ОЗП (Кб)	28,620	46,512	27,000	31,680	37,080	42,480	52,920	54,000	67,680	33,840	50,760
Часові ресурси	Елементи керування годинами (1 MMCM + 1 PLL)	18	24	14	12	14	20	20	18	24	12	18
Ресурси вводу-виводу	Максимум контактів вводу/виводу з одним кінцем	850	1,200	700	600	700	600	1,000	900	1,100	600	300
	Максимум диференційних пар вводу/виводу	408	576	336	288	336	288	480	432	528	288	144
Вбудовані ресурси жорсткої IP-адреси	Фрагменти DSP	1,260	2,160	1,120	2,160	2,800	2,880	3,600	3,600	3,360	1,680	2,520
	PCIe® Gen2	3	4	-	-	4	-	-	-	-	-	-
	PCIe Gen3	-	-	2	2	-	2	3	3	4	2	3
	Аналоговий змішаний сигнал (AMS)/XADC	1	1	1	1	1	1	1	1	1	1	1
	Налаштування блоків AES/HMAC	1	1	1	1	1	1	1	1	1	1	1

продовження таблиці 6

	Приймачі GTP (не більше 12,5 Гбіт/с)			36	36	-	-	56	-	-	-	-	-	-	
	Приймачі GTP (не більше 13,1 Гбіт/с)			-	-	28	48	-	80	80	72	96	48	72	
	Приймачі GTP (не більше 28,05 Гбіт/с)			-	-	-	-	-	-	-	-	-	8	16	
Марки швидкості	Комерційна температура (C)			-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	
	Розширена температура (E)			-2L -3	-2L -2G	-2L -3	-2L -3	-2L -3	-2L -3	-2L -3	-2L	-2L -2G	-2L -2G	-2L -2G	
	Промислова температура (I)			-1 -2	-1	-1 -2	-1 -2	-1 -2	-1 -2	-1 -2	-1	-1	-	-	
	Упаковка	Площа (мм)	Крок (мм)	Доступний власний ввід-вивід: 3.3V ввід-вивід HR, 1.8V ввід-вивід HP (GTX, GTH)									1.8V Ввід/вивід HP (GTH, GTZ)		
	FFG1157	35x35	1.0	0, 600 (20, 0)		0, 600 (20, 0)	0, 600 (20, 0)	0, 600 (20, 0)		0, 600 (20, 0)					
Сумісне місце	FFG1761	42.5x42.5	1.0	100, 750 (36, 0)		50, 650 (0, 28)		0, 700 (28, 0)		0, 850 (0, 36)					
	FHG1761	45x45	1.0		0, 850 (36, 0)										
	FLG1925	35x35	1.0		0, 1200 (16, 0)										
	FFG1158	45x45	1.0				0, 350 (0, 48)	0, 350 (0, 48)	0, 350 (0, 48)	0, 350 (0, 48)					
Сумісне місце	FFG1926	45x45	1.0							0, 720 (0, 64)	0, 720 (0, 64)				
	FLG1926	45x45	1.0									0, 720 (0, 64)			
	FFG1927	45x45	1.0				0, 600 (0, 48)	0, 600 (56, 0)	0, 600 (0, 80)	0, 600 (0, 80)					
Сумісне місце	FFG1928	45x45	1.0								0, 480 (0, 72)				
	FLG1928	45x45	1.0									0, 480 (0, 96)			
Сумісне місце	FFG1930	45x45	1.0					0, 700 (24, 0)		0, 1000 (0, 24)	0, 900 (0, 24)				
	FLG1930	45x45	1.0									0, 1100 (0, 24)			
	FLG1155	35x35	1.0										400 (24, 8)		
	FLG1931	45x45	1.0										600 (48, 8)		
	FLG1932	45x45	1.0											300 (72, 16)	

Перевага, що віддається сімейству Xilinx Artix-7, має кілька небажаних наслідків, про які коротко говориться нижче:

1. Artix-7 – бюджетне сімейство FPGA. Як таке, воно не дуже підходить для високошвидкісних реалізацій. Апаратних ресурсів, навіть найбільшого пристрою цього сімейства, часто виявляється недостатньо для демонстрації повного потенціалу розпаралелювання операцій даного алгоритму PQC. Таким чином, використання Artix-7 має сенс для порівняльного аналізу легких реалізацій, але може привести до отримання недостатньо оптимальних результатів для високошвидкісних реалізацій.

2. Artix-7 – це традиційна FPGA, а не SoC FPGA. В результаті, єдиний спосіб розробки однокристальної програмно-апаратної реалізації за допомогою Artix-7 – це використання так званих "м'яких" процесорних ядер, тобто процесорів, реалізованих з використанням

програмувальної логіки. До "м'яких" процесорів, сумісних з Artix-7, належать MicroBlaze і полегшені версії RISC-V. Всі вони працюють на значно низькій тактовій частоті, ніж вбудовані твердотільні процесори SoC FPGA.

3. Artix-7 не підходить для проектів HLS. Такі проекти, як правило, вимагають значно більше ресурсів, ніж проекти, засновані на написанні коду вручну в HDL.

4. Artix-7 – досить старе покоління FPGA, випущене Xilinx в 2010 р. На момент прийняття стандарту PQC цьому сімейству буде вже як мінімум 12 років. Незважаючи на те, що це сімейство як і раніше відносно популярно для недорогих додатків, воно не являє собою сучасну технологію FPGA.

5. Не прийнято засновувати ранжування кандидатів в криптографічних конкурсах на результатах, отриманих для одного сімейства одного постачальника. Хоча Xilinx є найбільшим розробником FPGA і SoC FPGA, Intel посідає друге місце, а інші постачальники, такі як Microchip і Lattice Semiconductor, також розробляють FPGA, які підходять для реалізації криптографічних алгоритмів. Під час конкурсу SHA-3 були оголошені результати за семи родинами FPGA від двох основних постачальників, Xilinx і Altera. Під час конкурсу CAESAR були прийняті в роботу чотири сімейства Xilinx і чотири сімейства Altera. Для всіх цих сімейств результати були сформовані на основі одного і того ж HDL коду. Не було необхідності купувати кілька пристроїв або плат. Досить було безкоштовних або пробних версій інструментів. Конструкції закінчувалися генерацією звітів після розміщення та маршрутизації, в яких правильно описувалися найгірші показники продуктивності конкретного екземпляра даного FPGA-пристрою.

6. Ґрунтуючись на досвіді авторів, численні експерти при рецензуванні робіт, присвячених реалізації кандидатур 2-го раунду PQC, розглядали вибір NIST Artix-7 як абсолютну вимогу. Заявки, що не відповідають цій вимозі, підлягали відхиленню або запитам на внесення великих змін. В результаті благородна мета зробити результати більш зіставними між собою була перетворена в привід для заборони або затримки публікації необхідних результатів [1].

Беручи до уваги ці побоювання, рекомендація для 3-го раунду полягає в тому, щоб заохочувати подання звітів про результати, принаймні, для наступних сімей FPGA:

1. Для малоресурсних апаратних і програмно-апаратних реалізацій на базі програмних процесорних ядер: Xilinx Artix-7 (для сумісності з результатами 2-го раунду) і Intel Cyclone 10 LP.

2. Для малоресурсних програмних та апаратних реалізацій на основі використання жорстких процесорних ядер: серії Xilinx Zynq 7000 та FPGA Intel Cyclone V SoC.

3. Для високошвидкісних апаратних засобів та швидкісних програмно-технічних реалізацій: Zynq Xilinx UltraScale+ та Intel Stratix 10 SoC.

Однією з причин вибору Zynq Xilinx UltraScale+, навіть для чистих апаратних реалізацій, які не потребують використання можливостей SoC, є підтримка цих пристроїв безкоштовною версією інструментарію Xilinx, так званого Vivado HL WebPACK, якого достатньо для отримання всіх необхідних результатів еталонного тестування. FPGA Xilinx Virtex-7 UltraScale+, які можна було б вважати природним претендентом, не підтримуються тією ж безкоштовною версією утиліт. Сімейство Zynq Xilinx UltraScale+ також рекомендується для високошвидкісних програмно-апаратних реалізацій, заснованих на використанні жорстких процесорних ядер, завдяки помірній ціні відповідних прототипних плат і наявності безкоштовного еталонного набору для програмно-апаратних реалізацій схем PQC, розробленого в Університеті Джорджа Мейсона [7].

Реалізації орієнтовані на FPGA

У табл. 7 та 8 підсумовано реалізації, орієнтовані на FPGA Xilinx Artix-7 та пов'язані з ними FPGA Xilinx Zynq-7000 SoC. Для 1-го рівня стійкості шість кандидатів – Classic McEliece, Crystals-Kyber, FrodoKEM, NewHope, SIKE та Saber – повідомили про реалізацію всіх трьох операцій. Попередні реалізації BIKE були зосереджені лише на генерації ключів. Для NewHope не має 3-го рівня стійкості. Щодо рівня 5, то для Classic McEliece результати відсутні.

Для більшості KEM час декапсуляції перевищує час інкапсуляції. Записи в таблиці впорядковуються відповідно до часу декапсуляції в мкс (і, якщо потрібно, відповідно до часу декапсуляції в тактах).

Рейтинг кандидатів, перелічених у табл. 2 та 3, дуже складно визначити на основі наявних результатів. По-перше, може бути несправедливим порівнювати чисто апаратні реалізації з програмно-апаратними. По-друге, важко порівнювати малоресурсні реалізації з швидкісними реалізаціями, оскільки вони оптимізовані з урахуванням різних первинних показників. По-третє, програмно-апаратні реалізації на основі різних процесорів дуже складно порівняти один з одним. Нарешті, навіть для реалізацій, що використовують однаковий тип реалізації (програмну/апаратну) та аналогічний тип процесора (RISC-V) порівняння може бути ненавмисно необ'єктивним. У конкретному випадку [8] було запропоновано суттєво іншу апаратну підтримку алгоритмів, які можуть скористатися теоретико-числовим перетворенням – Kyber та NewHope – проти алгоритму, який не може ним скористатися – Saber. Додатковим, відносно незначним фактором є те, що кілька результатів для класичного McEliece та NewHope стосуються їх IND-CPA-стійкого АСШ, а не IND-CCA-стійкого KEM.

Враховуючи всі ці фактори, майже єдиним способом ранжування, який цілком зрозумілий з табл. 2 та 3, є ранжування кандидатів, які мають результати для чисто апаратної реалізації, орієнтованої на швидкісну. У цій конкретній категорії ранжування для рівня стійкості 1 становить: 1) NewHope, 2) Classic McEliece, 3) FrodoKEM. Якщо припустити, що програмно-апаратна реалізація SIKE з процесором користувача майже настільки ж ефективна як і чисто апаратна реалізація, то також можна додати SIKE на позиції 4). На рівні 3 у NewHope немає варіанту, а на рівні 5 Classic McEliece та FrodoKEM не повідомляють про високошвидкісні чисто апаратні реалізації [1].

У табл. 9 та 10 підсумовано реалізації, орієнтовані на FPGA Xilinx Virtex-7. На жаль, єдиний висновок, який можна зробити з цих таблиць, – це перевага Classic McEliece перед SIKE з точки зору всіх показників продуктивності, окрім кількості LUT та тригерів.

У табл. 11 порівнюються результати, про які було повідомлено наприкінці 2019 р., та результати, про які повідомляли інші групи відповідно до Saber та NewHope. Усі результати були отримані з використанням тієї ж SoC FPGA, Zynq UltraScale+. Програмна/апаратна реалізація Round5 була дуже схожа на чисто апаратну реалізацію. Те ж саме не стосувалось програмного забезпечення та апаратного забезпечення Saber, значний відсоток часу виконання був присвячений функціям, що залишаються в програмному забезпеченні, та передачі даних і контролю між програмним та апаратним забезпеченням. Як результат, найбільш точне порівняння між Round5 та Saber можливе на 3-му рівні стійкості, який має чисто апаратну реалізацію Saber. За рахунок цієї реалізації Saber перевершує Round5 з невеликим відривом у плані часу виконання інкапсуляції та декапсуляції. У той же час, навіть найшвидша реалізація Saber використовує в 1,6 разів менше LUT, ніж Round5, з однаковою кількістю одиниць BRAM та DSP. Показано, що FrodoKEM набагато повільніше, ніж Saber і Round5 для всіх рівнів стійкості.

Дещо інакше, для 5-го рівня стійкості чисто апаратна реалізація NewHope, про яку повідомляється в роботі [9], недостатньо швидка для того, щоб перевершити програмно-технічну реалізацію Round5 з [10]. Однак порівняння дещо ускладнюється тим, що в [9] результати свідчать не про IND-CPA-стійке асиметричне шифрування (а не про IND-CCA-стійкий KEM), а лише про суму генерації та розшифрування ключів (а не про саме розшифрування).

У табл. 12 підсумовано результати, які доступні для реалізації цифрових підписів. Реалізації, орієнтовані на FPGA, розглядаються першими в табл. 12. На жаль, кілька результатів для qTESLA стосуються наборів евристичних параметрів, які були відкликані представниками 20 серпня 2019 р. Серед решти конструкцій, для Artix-7, рейтинг кандидатів на 1-му рівні стійкості: 1) Picnic, 2) Dilithium і 3) qTESLA. Різниці між цими кандидатами щодо часу виконання для створення підписів (більш критично) та перевірки підписів дуже істотні. У той же час, лише реалізація Picnic – це швидкісна та чиста апаратна реалізація. Решта реалізації – це реалізація програмного забезпечення та обладнання на основі RISC-V. Крім того, кількість LUT для Picnic приблизно в шість разів більша, ніж для Dilithium, а кількість BRAM у 3,75 рази більше. У той же час, порівняно з Picnic, час створення підписів у Dilithium-I в 12 разів і у Dilithium-II в 16 разів довший.

Для 3-го рівня реалізація для Picnic відсутня. Реалізації Dilithium-III та qTESLA-p-III схожі за типом, цільовим призначенням та використанням ресурсів. У той же час реалізація Dilithium на порядок ефективніша. Реалізації схем електронного підпису, орієнтованих на Kintex-7 та Virtex-7, узагальнені в одній таблиці. Що стосується реалізації Kintex-7, Rainbow істотно перевершує Picnic для рівня стійкості 1. Для решти родин та рівнів безпеки повідомляється лише про одного кандидата із оновленим набором параметрів [1].

Таблиця 7

1-й рівень KEM та PKE на Artix-7 (за замовчуванням) та Zynq-7000 (позначається верхнім індексом Z)

Algorithm	**Type**	**Target**	**Max. Freq.**	**LUT**	**FF**	**Slice**	**DSP**	**BR AM**	**Key Generation**		**Encaps./Enc.**^{cpa}		**Decaps./(Dec.+Enc.)**^{cpa}	
									cycles	*µs*	**cycles**	*µs*	**cycles**	*µs*
						Security Level 1								
NewHope-512^{cpa}	HW	HS	200	6,780	4,026	–	2	7.0	4,200	21.0	6,600	33.0	9,100	45.5
mceliece348864^{cpa}	HW	HS	106	81,339	132,190	–	0	236.0	202,787	1,920.3	2,720	25.8	12,743	120.7
mceliece348864^{cpa}	HW	HS	108	25,327	49,383	–	0	168.0	1,599,882	14,800.0	2,720	25.2	18,358	169.8
Kyber-512	SW/HW^{RV}	LW	–	23,925	10,844	–	21	32.0	150,106	–	193,076	–	204,843	–
FrodoKEM-640			172	2,587	2,994	855	16	0						
	HW	HS							204,766	1,190.5	207,269	1,212.1	209,867	1,408.5
16x			149	6,881	5,081	1,947	16	12.5						
Kyber-512	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	74,519	2,980.8	131,698	5,267.9	142,309	5,692.4
NewHope-512	SW/HW^{RV}	LW	–	23,925	10,844	–	21	32.0	123,860	–	207,299	–	226,742	–
NewHope-512	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	97,969	3,918.8	236,812	9,472.5	258,872	10,354.9
LightSaber	SW/HW^{RV}	LW	–	23,925	10,844	–	21	32.0	366, 837	–	526, 496	–	657,583	–
Kyber-512	SW/HW^{RV}	LW	59	1,842	1,634	–	5	34.0	710,000	11,993.2	971,000	16,402.0	870,000	14,695.9
NewHope-512	SW/HW^{RV}	LW	59	1,842	1,634	–	5	34.0	904,000	15,270.3	1,424,000	24,054.1	1,302,000	21,993.2
SIKEp434	SW/HW^{c}	HS	162	22,595	11,558	7,491	162	37.0	1,474,200	9100	2,494,800	15,400.0	2,656,800	16,400.0
SIKEp503	SW/HW^{c}	HS	162	22,595	11,558	7,491	162	37.0	1,733,400	10,700.0	2,932,200	18,100.0	3,126,600	19,300.0
FrodoKEM-640			191	971	433	290	1	0						
	HW	LW							3,237,288	16,949.2	3,275,862	17,241.4	3,306,122	20,408.2
1x														
			162	4,446	2,152	1,254	1	12.5						
	SW/HW^{c}													
SIKEp434		LW	143	10,976	7,115	3,512	57	21.0	2,187,902	15,300.0	3,718,004	26,000.0	3,946,804	27,600.0
SIKEp503	SW/HW^{c}	LW	143	10,976	7,115	3,512	57	21.0	2,602,603	18,200.0	4,390,104	30,700.0	4,676,105	32,700.0
FrodoKEM-640	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	11,453,942	458,157.7	11,609,668	464,386.7	12,035,513	481,420.5
BIKE-1 Level 1^{cs}	HW	HS	165	1,907	1,049	608	0	7.0	95,500	578.0	–	–	–	–
BIKE-3 Level 1^{cs}	HW	HS	170	1,397	925	453	0	4.0	98,500	579.0	–	–	–	–
BIKE-2 Level 1^{cs}	HW	HS	160	3,874	2,141	1,312	0	10.0	2,150,000	13,437.0	–	–	–	–
BIKE Level 1	HW	HS	135	1,865	589	590	0	4.0	7,370,429	54,540.0	–	–	–	–

Таблиця 8

3-й та 5-й рівні KEM та PKE на Artix-7 (за замовчуванням) та Zynq-7000 (позначається верхнім індексом Z)

Algorithm	**Type**	**Target**	**Max.**	**LUT**	**FF**	**Slice**	**DSP**	**BR**	**Key Generation**		**Encaps./Enc.**^{cpa}		**Decaps./(Dec.+Enc.)**^{cpa}	
			Freq.					**AM**	**cycles**	*µs*	**cycles**	*µs*	**cycles**	*µs*
						Security Level 3								
mceliece460896^{cpa}	HW	HS	107	38,669	74,858	–	0	303.0	5,002,044	46,704.4	3,360	31.4	31,005	289.5
FrodoKEM-976			169	2,869	3,000	908	16	0						
16x	HW	HS	168	6,188	4,678	1782	16	0	476,056	2,816.9	479,993	2,857.1	483,073	3,076.9
			157	7,213	5,087	2042	16	19.0						
	SW/HW^{A9}													
Saber^{Z}		HS	125	7,400	7,331	–	28	2.0	–	3,273.0	–	4,147.0	–	3,844.0
Kyber-768	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	111,525	4,461.0	177,540	7,101.6	190,579	7,623.2
SIKEp610	SW/HW^{c}	HS	162	22,595	11,558	7,491	162	37.0	2,916,000	18,000.0	5,443,200	33,600.0	5,508,000	34,000.0
FrodoKEM-976			189	1,243	441	362	1	0						
1x	HW	LW	187	4,650	2,118	1,272	1	0	7,560,000	40,000.0	7,480,000	40,000.0	7,714,286	47,619.0
			162	4,888	2,153	1,390	1	19.0						
	SW/HW^{c}													
SIKEp610		LW	143	10,976	7,115	3,512	57	21.0	4,347,204	30,400.0	8,108,108	56,700.0	8,208,208	57,400.0
FrodoKEM-976	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	26,005,326	1,040,213.0	29,749,417	1,189,976.7	30,421,175	1,216,847.0
BIKE Level 3	HW	HS	135	1,884	557	593	0	5	30,447,947	231,400.0	–	–	–	–
						Security Level 5								
NewHope-1024^{cpa}	HW	HS	200	6,781	4,127	–	2	8.0	8,000	40.0	12,500	62.5	17,300	86.5
NewHope-1024^{cpa}	HW	HS	190	13,244	8,272	–	24	18.0	–	–	34,000	178.0	30,600^{KD}	160.0^{KD}
Kyber-1024	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	148,547	5,941.9	223,469	8,938.8	240,977	9,639.1
NewHope-1024	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	97,969	3,918.8	236,812	9,472.5	258,872	10,354.9
Kyber-1024	SW/HW	LW	–	23,925	10,844	–	21	32.0	349,673	–	405,477	–	424,682	–
NewHope-1024	SW/HW	LW	–	23,925	10,844	–	21	32.0	235,420	–	392,734	–	450,541	–
NewHope-1024^{cpa}	SW/HW	HS	25	26,606	26,303	–	32	1.0	357,052	14,282.1	589,285	23,571.4	756,932	30,277.3
FireSaber	SW/HW	LW	–	23,925	10,844	–	21	32.0	1,300,272	–	1,622,818	–	1,898,051	–
Kyber-1024	SW/HW^{RV}	LW	59	1,842	1,634		5	34.0	2,203,000	37,212.8	2,619,000	44,239.9	2,429,000	41,030.4
SIKEp751	SW/HW^{c}	HS	162	22,595	11,558	7,491	162	37.0	3,742,200	23,100.0	6,188,400	38,200.0	6,658,200	41,100.0
NewHope-1024	SW/HW^{RV}	LW	59	1,842	1,634		5	34.0	1,776,000	30,000.0	2,742,000	46,317.6	2,528,000	42,702.7
SIKEp751	SW/HW^{c}	LW	143	10,976	7,115	3,512	57	21.0	7,965,108	55,700.0	13,156,013	92,000.0	14,185,614	99,200.0
FrodoKEM-1344	SW/HW^{RV}	LW	25*	14,975	2,539	4,173	11	14.0	67,994,170	2,719,766.8	71,501,358	2,860,054.3	72,526,695	2,901,067.8

Таблиця 9

КЕМ 1-го рівня на Virtex-7 (за замовчуванням) та Virtex-6 (позначено верхнім індексом ^{V6})

Algorithm	Type	Target	Max. Freq.	LUT	FF	Slice	DSP	BR AM	Key Generation		Encap./Enc.^{cpa}		Decaps./Dec.^{cpa}	
									cycles	μs	cycles	μs	cycles	μs
					Security Level 1									
SIKEp503	HW	HS	171	25,094	26,971	9,514	264	34.0	640,000	3,738.3	1,120,000	6,542.1	1,210,000	7,067.8
SIKEp434	SW/HW	HS	142	21,210	13,657	7,408	162	38.0	981,180	6,900.0	1,677,960	11,800.0	1,777,500	12,500.0
SIKEp503	SW/HW	HS	142	21,210	13,657	7,408	162	38.0	1,166,040	8,200.0	1,976,580	13,900.0	2,104,560	14,800.0
LEDAkem-128^{o,cpa,V6}	HW	LW	235	104	53	33	0	1.0	–	–	712,000	3,029.8	2,620,000	18,714.3
			140	2,222	658	870	0	13.0						
SIKEp434	SW/HW	LW	152	10,937	7,132	3,415	57	21.0	2,191,781	14,400.0	3,713,851	24,400.0	3,957,382	26,000.0
SIKEp503	SW/HW	LW	152	10,937	7,132	3,415	57	21.0	2,602,740	17,100.0	4,383,562	28,800.0	4,672,755	30,700.0

Розробка варіанту КЕМ, стійкого до атаки з обраним відкритим текстом (CPA)

^{V6} Проект реалізовано на Virtex-6

^{o} Проект старого набору параметрів змінено поданими 19 березня 2020 р.

Таблиця 10

КЕМ та АСШ 3-го та 5-го рівнів стійкості на Virtex-7

Algorithm	Type	Target	Max. Freq.	LUT	FF	Slice	DSP	BR AM	Key Generation		Encaps./Enc.^{cpa}		Decaps./(Dec.+Enc.)^{cpa}	
									cycles	μs	cycles	μs	cycles	μs
						Security Level 3								
mceliece460896^{cpa}	HW	HS	131	109,484	168,939	–	0	446.0	515,806	3,943.5	3,360	25.7	17,931	137.1
SIKEp610	SW/HW	HS	142	21,210	13,657	7,408	162	38.0	1,962,360	13,800.0	3,654,540	25,700.0	3,711,420	26,100.0
SIKEp610	SW/HW	LW	152	10,937	7,132	3,415	57	21.0	4,353,120	28,600.0	8,097,412	53,200.0	8,219,178	54,000.0
						Security Level 5								
mceliece6960119^{cpa}	HW	HS	130	116,928	188,324	–	0	607.0	974,306	7,500.4	5,413	41.7	25,135	193.5
mceliece6688128^{cpa}	HW	HS	137	122,624	186,194	–	0	589.0	1,046,139	7,658.4	5,024	36.8	29,754	217.8
mceliece8192128^{cpa}	HW	HS	130	123,361	190,707	–	0	589.0	1,286,179	9,901.3	6,528	50.3	32,765	252.2
mceliece6960119^{cpa}	HW	HS	141	44,154	88,963	–	0	563.0	11,179,636	79,570.4	5,413	38.5	46,141	328.4
mceliece6688128^{cpa}	HW	HS	136	44,345	83,637	–	0	446.0	12,389,742	91,034.1	5,024	36.9	52,333	384.5
mceliece8192128^{cpa}	HW	HS	134	45,150	88,154	–	0	525.0	15,185,314	113,154.4	6,528	48.6	55,330	412.3
SIKEp751	HW	HS	167	45,893	50,390	17,530	512	43.5	1,240,000	7,407.4	2,170,000	12,963.0	2,330,000	13,918.8
SIKEp751	SW/HW	HS	142	21,210	13,657	7,408	162	38.0	2,516,940	17,700.0	4,166,460	29,300.0	4,479,300	31,500.0
SIKEp751	SW/HW	LW	152	10,937	7,132	3,415	57	21.0	7,960,426	52,300.0	13,150,685	86,400.0	14,185,693	93,200.0

Таблиця 11

Усі КЕМ та АСШ на Zynq Ultrascale+

Algorithm	Type	Target	Max. Freq.	LUT	FF	Slice	DSP	BRAM	Key Gen.		Encapsulation		Decapsulation	
									cycles	us	cycles	us	cycles	us
					Security Level 1									
R5ND_1KEM_0d	SW/HW	HS	260	55,442	82,341	10,627	0	2	–	–	–	19.0	–	24.0
LightSaber	SW/HW	HS	322	12,343	11,288	1,989	256	3.5	–	–	–	53.0	–	56.0
FrodoKEM-640	SW/HW	HS	402	7,213	6,647	1,186	32	13.5	–	–	–	1,223.0	–	1,319.0
					Security Level 3									
Saber	HW	HS	250	45,895	18,705	–	0	2	4,320	17.3	5,231	20.9	6,461	25.8
Saber	HW	HS	250	25,079	10,750	–	0	2	5,435	21.8	6,618	26.5	8,034	32.1
R5ND_3KEM_0d	SW/HW	HS	249	73,881	109,211	14,307	0	2	–	–	–	24.0	–	33.0
Saber	SW/HW	HS	322	12,566	11,619	1,993	256	3.5	–	–	–	60.0	–	65.0
FrodoKEM-976	SW/HW	HS	402	7087	6693	1190	32	17	–	–	–	1,642.0	–	1,866.0
					Security Level 5									
R5ND_5KEM_0d	SW/HW	HS	212	91,166	151,019	18,733	0	2	–	–	–	32.0	–	42.0
NewHope-1024^{cpa}	HW	HS	406	13,961	8,149	–	25	18	–	–	34,000	83.0	30,600^{KD}	75.0^{KD}
FireSaber	SW/HW	HS	322	12,555	11,881	2,341	256	3.5	–	–	–	74.0	–	80.0
FrodoKEM-1344	SW/HW	HS	417	7,015	6,610	1,215	32	17.5	–	–	–	2,186.0	–	3,120.0

Таблиця 12

Схеми ЕП на Artix-7, Kintex-7 та Virtex-7

Algorithm	Type	Target	Max.	LUT	FF	Slice	DSP	BR	Key Gen.		Signature Verification		Signature Generation		Family
			Freq.					AM	cycles	us	cycles	us	cycles	us	
						Security Level 1 & 2									
Picnic-L1-FS	HW	HS	91	90,535	23,516	25,160	0	52.5	–	–	29,600	325.6	31,300	344.3	
qTESLA-I [o2]	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	4,846,949	193,878.0	38,922	1,556.9	168,273	6,730.9	
Dilithium-I	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	95,202	3,808.1	142,576	5,703.0	376,392	15,055.7	Artix-7
Dilithium-II	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	130,022	5,200.9	184,933	7,397.3	514,246	20,569.8	
qTESLA-p-I	SW/HW	LW	121	7,212	4,378	2,438	15	139.0	925,431	7,648.2	946,520	7,822.5	4,165,160	34,422.8	
Rainbow-Ic [o1]	HW	HS	90	52,895	32,476	15,112	0	67.0	–	–	–	–	979	10.9	
Rainbow-Ia	HW	HS	111	27,712	27,679	8,939	0	59.0	–	–	–	–	1,980	17.8	Kintex-7
Picnic-L1-FS	HW	HS	125	90,037	23,105	–	0	52.5	–	–	29,600	237.0	31,300	250.0	
Rainbow-Ic [o1]	HW	HS	167	52,721	32,475	15,976	0	67.0	–	–	–	–	979	5.9	
Rainbow-Ia	HW	HS	181	27,556	27,675	7,065	0	59.0	–	–	–	–	1,980	10.9	Virtex-7
							Security Level 3								
qTesla-III-speed [o2]	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	11,898,241	475,929.6	67,712	2,708.5	317,083	12,683.3	
qTesla-III-size [o2]	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	11,479,190	459,167.6	69,154	2,766.2	348,429	13,937.2	
Dilithium-III	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	167,433	6,697.3	229,481	9,179.2	634,763	25,390.5	Artix-7
qTESLA-p-III	SW/HW	LW	121	7,475	4,518	2,473	15	147.0	2,305,220	19,051.4	2,315,950	19,140.1	7,745,088	64,009.0	
						Security Level 4 & 5									
Picnic-L5-FS	HW	HS	125	167,530	33,164	–	0	98.5	–	–	146,600	1,173.0	154,500	1,236.0	Kintex-7
Dilithium-IV	SW/HW	LW	25*	14,975	2,539	4,173	11	14.0	223,272	8,930.9	276,221	11,048.8	815,636	32,625.4	Artix-7

Висновки

У роботі розглянуто попередні дослідження щодо апаратної та програмно-апаратної імплементації PQC-схем в рамках 2-го раунду конкурсу NIST PQC. З 26 кандидатів шість – NewHope, Crystals-Kyber, FrodoKEM, Saber, Round5 та SIKE – отримали найбільше покриття за кількістю реалізацій та пов'язаних публікацій. Усі вони мають як швидкісні, так і малоресурсні реалізації. Було застосовано спільне проектування програмно-технічного забезпечення для швидкісних, а не малоресурсних реалізацій, що призвело до вибору Xilinx Zynq UltraScale+, найсучаснішої групи SoC FPGA, у якості основної платформи. Відмінним фактором є те, що ця платформа включає в себе провідний процесор ARM Cortex-A53, який працює на частоті 1,2 ГГц, і значна кількість програмованої логіки підтримує апаратні прискорювачі, які працюють на тактових частотах до 500 МГц.

Для кожного кандидата була зроблена спроба вивантажити якомога більше операцій на обладнанням. Для 50 % досліджуваних KEM цей відсоток сягав 100 %. Таким чином, відповідні реалізації можуть сприйматись у якості апаратних реалізацій, припускаючи, що випадкове початкове число (розміром 16, 24 або 32 байти) було передано апаратному модулю під час інкапсуляції. KEM, реалізований за допомогою цього підходу, включав Kyber, LAC (v3a та v3b), NewHope та Round5 (з кодом для виправлення помилок та без нього). Їх код був протестований за допомогою FPGA Artix-7 та Virtex-7.

Що стосується часу виконання та використання ресурсів, Round5 з кодом виправлення помилок (R5ND_5d) перевершував Round5 без коду виправлення помилок (R5ND_0d). Аналогічно, LAC-v3b виявився кращим за LAC-v3a як за швидкістю, так і у відношенні FPGA-ресурсів. При порівнянні найкращих представників чотирьох кандидатів – Kyber, LAC, NewHope та Round5 можна було зробити наступні висновки. Часи виконання цих кандидатів були надзвичайно близькими один до одного. Для інкапсуляції терміни виконання були в межах 10 % один від одного на рівні безпеки 5, у межах 22 % на рівні безпеки 3 та в межах 32 % на рівні безпеки 1. Для декапсуляції найбільші відмінності складали 26 % на рівні 5, 22 % на рівні 3 та 48 % на рівні 1. У декількох випадках лише зміна сімейства FPGA з недорогого Artix-7 на високоефективний Virtex-7 спричинила суттєві зміни в рейтингу, навіть, якщо код HDL залишився точно таким же. Таким чином, можна зробити висновок, що різниця між цими схемами за швидкістю занадто мала, щоб віддати перевагу будь-якому конкретному кандидату. Ці результати суперечать одному з попередніх звітів, який свідчить про відставання LAC від NewHope та Kyber.

Говорячи про використання ресурсів, підкреслимо, що невелика перевага належить NewHope та Kyber. Обидва використовують меншу кількість LUT та тригерів (FF), ніж LAC та Round5, а використання ними DSP-одиниць та BRAM, хоча і є дещо вищим, але дуже помірне. Крім того, і NewHope, і Kyber використовують майже однакову кількість ресурсів незалежно від рівня безпеки. У випадку LAC та Round5 використання ресурсів різко зростає зі збільшенням рівня безпеки. Здається, колишня властивість є перевагою для програм, які потребують підтримки найвищого або всіх рівнів безпеки. Зокрема, конструкції k-в-1, які підтримують усі k рівні безпеки та дозволяють змінювати їх під час виконання, як правило, мають лише дещо більший рівень використання ресурсів, ніж максимальний рівень безпеки. Таким чином, плоска залежність використання ресурсів від рівня безпеки передбачає потенціал для дуже економічних проектів k-в-1. У той же час, цей потенціал все ж повинен бути підтверджений за допомогою повних проектів.

Також була наведена детальна характеристика FPGA сімейства Xilinx. Кожна конкретна FPGA має використовуватися залежно від мети, очікуваної вартості та продуктивності.

Список літератури:

1. Viet Ba Dang. Implementation and Benchmarking of Round 2 Candidates in the NIST Post-Quantum Cryptography Standardization Process Using Hardware and Software/Hardware Co-design Approaches / Viet Ba Dang, Farnoud Farahmand, Michal Andrzejczak, Kamyar Mohajerani, Duc Tri Nguyen, Kris Gaj. Режим доступу: https://eprint.iacr.org/2020/795.pdf.

2. Xilinx. 7 Series Product Selection Guide. [Електронний ресурс]. Режим доступу: https://www.xilinx.com/support/documentation/selection-guides/7-series-product-selection-guide.pdf.
3. Malik Imran. A Systematic Study of Lattice-based NIST PQC Algorithms: from Reference Implementations to Hardware Accelerators / Malik Imran, Zain Ul Abideen, Samuel Pagliarini. Режим доступу: https://arxiv.org/pdf/2009.07091.pdf.
4. Gorjan Alagic. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone. 22 July 2020. Режим доступу: https://doi.org/10.6028/NIST.IR.8309.
5. Post-quantum cryptography, round 2 submissions. Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.
6. Тарасов И. ПЛИС Xilinx и цифровая обработка сигналов. Особенности, преимущества, перспективы. Режим доступу: https://www.electronics.ru/files/article_pdf/2/article_2788_434.pdf.
7. Farnoud Farahmand et al. Software/Hardware Codesign of the Post Quantum Cryptography Algorithm NTRUEncrypt Using High-Level Synthesis and Register-Transfer Level Design Methodologies // 29th International Conference on Field Programmable Logic and Applications, FPL 2019. Barcelona, Spain: IEEE, Sept. 2019, pp. 225–231. ISBN: 978-1-72814-884-7. DOI: 10.1109/FPL.2019.00042.
8. Kris Gaj. Challenges and Rewards of Implementing and Benchmarking Post-Quantum Cryptography in Hardware // 2018 Great Lakes Symposium on VLSI, GLSVLSI 2018. Chicago, IL, USA: ACM Press, 2018, pp. 359–364. ISBN 978-1-4503-5724-1. DOI: 10/ggbscs.
9. Jens-Peter Kaps et al. Lightweight Implementations of SHA-3 Candidates on FPGAs. In: 12th International Conference on Cryptology in India, Indocrypt 2011. Vol. 7107. LNCS. Chennai, India, Dec. 2011, pp. 270–289. ISBN: 978-3-642-25577-9 978-3-642-25578-6. DOI: 10.1007/978-3-642-25578-6_20. – Режим доступу: https://2011.indocrypt.org/slides/gurung.pdf.
10. Viet B Dang et al. Implementing and Benchmarking Three Lattice-Based Post-Quantum Cryptography Algorithms Using Software/Hardware Codesign // 2019 International Conference on Field Programmable Technology, FPT 2019. Tianjin, China: IEEE, Dec. 9-13, 2019, pp. 206–214. DOI: 10.1109/ICFPT47387.2019.00032.

Надійшла до редколегії 06.02.2021

Відомості про авторів:

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, старший викладач кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна; e-mail: rinayes20@gmail.com; ORCID: https://orcid.org/0000-0002-1252-7606

Шахов Богдан Сергійович – Харківський національний університет імені В.Н. Каразіна, студент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна; e-mail: bogdanshahov2000@gmail.com