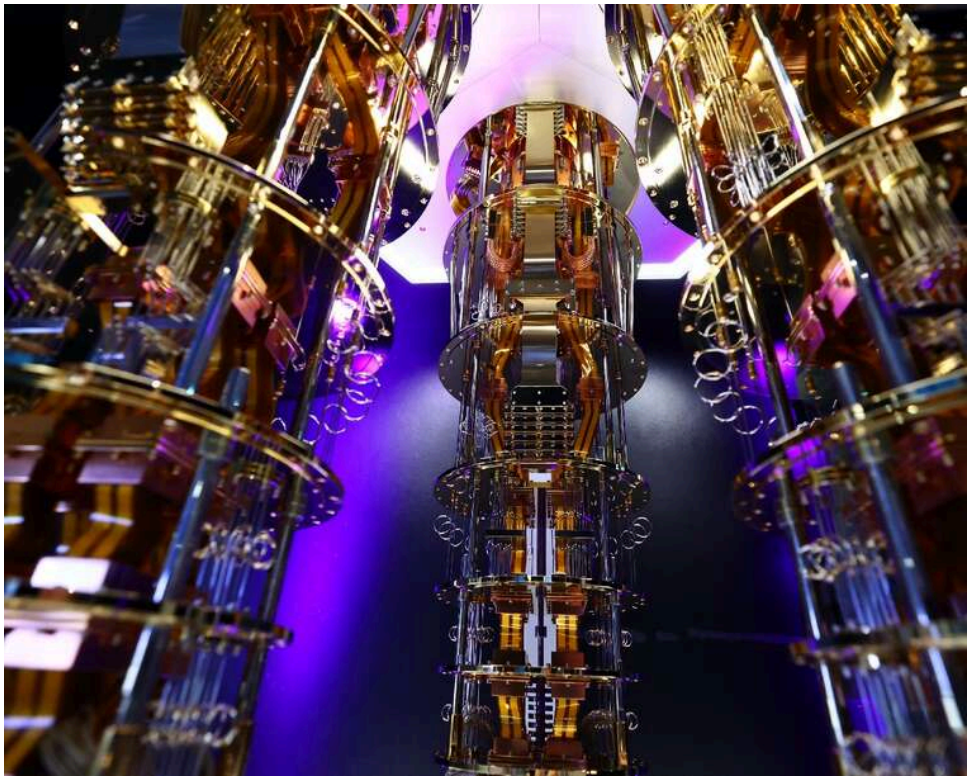
Отримали нагороду в 1 BTC: Квантовий комп'ютер зламав ключ біткоїна

Читать на русском



Отримали нагороду в 1 BTC: Квантовий комп'ютер зламав ключ біткоїна

Незалежний дослідник Джанкарло Леллі отримав премію Q-Day Prize від Project Eleven, успішно зламавши 15-бітний ключ еліптичної криптографії за допомогою доступного квантового комп'ютера — це наймасштабніша публічна демонстрація квантової атаки такого типу на сьогодні.

Про це повідомила компанія Project Eleven 24 квітня.

Леллі відтворив приватний ключ із публічного, перебираючи простір із 32 767 можливих варіантів за допомогою вдосконаленого алгоритму Шора. Цей алгоритм призначений для розв'язання задачі дискретного логарифмування на еліптичних кривих — математичної основи цифрових підписів, що захищають біткоїн, Ethereum та більшість блокчейнів.

Простими словами: цифровий підпис — це криптографічний «замок» на гаманці. Завдання полягає в тому, щоб, знаючи публічну частину замка (доступну всім), обчислити його приватну частину (секретний ключ власника).

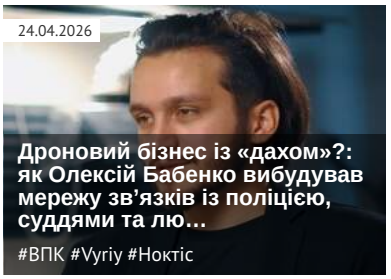
Леллі провів атаку на пристрої з приблизно 70 кубітами (кубіт — квантовий еквівалент біта), а весь процес тривав лише кілька хвилин.

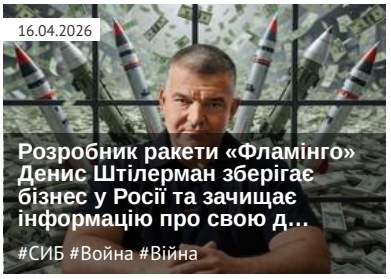
Project Eleven, стартап у галузі постквантової безпеки, виплатила Леллі винагороду в 1 BTC, що на момент оголошення перевищувало $78 000.

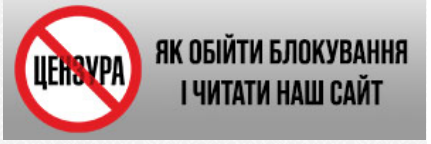
Масштаб прогресу

За останні сім місяців квантові атаки на еліптичну криптографію перейшли від теорії до практики. Першою публічною демонстрацією на квантовому обладнанні стала 6-

Важливі новини







Останні новини

По даті | По переглядам | По коментарям

18:43 Наслідки ворожої атаки: з'явилися фото поніveченого Ямполя після авіаційного удару
18:38 «Київська російська»: Анастасія Приходько потрапила у гучний скандал та «перевзулася» після хвилі хейту
18:33 У Броварах попрощаються із загиблим захисником України Фесюком
18:27 Смерть 12-річної дитини через лікарську помилку: на Чернігівщині судитимуть сімейну лікарку
18:22 Асфальт на дев'ять мільярдів: кожна четверта гривня у «Прозорро» пішла на дороги, але лише «на папері»

Підписуйтесь на наш канал в Telegram. Оперативно про головне

18:18 На війні загинув 37-річний захисник з Прикарпаття Михайло

бітна атака інженера Стіва Тіппеконніка у вересні 2025 року з використанням 133-кубітного комп'ютера IBM. Досягнення Леллі на 15 бітів перевершує це в 512 разів.

Програма Q-Day Prize, назва якої походить від гіпотетичної дати, коли квантовий комп'ютер зламає сучасну криптографію, створена для перевірки: чи здатні доступні квантові системи перевершити тривіальні обчислення.

Наскільки реальна загроза для ринку

Поточний результат ще далекий від справжньої небезпеки:

- 15-бітний тест значно поступається 256-бітним ключам, які захищають реальні гаманці в мережі Bitcoin.

- Однак атаки цього класу загрожують Bitcoin, Ethereum та цифровим активам на суму в понад $2,5 трлн, що використовують такий тип шифрування.

- Розробники не вважають цю прірву непереборним фізичним бар'єром — вони бачать у ній інженерний виклик.

Теоретичні оцінки ресурсів для атаки на 256-бітну систему різко знизилися: квітневий звіт Google 2026 року визначив поріг нижче 500 000 фізичних кубітів, а подальша публікація Каліфорнійського технологічного інституту та Oratomic показала, що з процесорами на нейтральних атомах вистачить лише 10 000 кубітів.

Гендиректор Project Eleven Алекс Прюден підкреслив, що переможну роботу подав незалежний дослідник, який використовував хмарне обладнання, доступне широкому загалу, — без участі національних лабораторій чи приватних виробників квантових чипів.

Чому це важливо

Цей експеримент показує, що квантові атаки на криптографію гаманців криптовалют перейшли від теорії до реальних, публічно відтворюваних тестів — не в закритих лабораторіях, а на комерційному хмарному обладнанні. Крім того, він загострює дискусію про захист мережі: технічні рішення існують, але будь-яке примусове оновлення протоколу Bitcoin стикається з конфліктом між безпекою та принципом недоторканності приватної власності в децентралізованих фінансах.

Теги: Джанкарло Лелли | Джанкарло Леллі | криптовалюта биткоин | Биткоин | Криптовалюта

Максим Левченко
ВИПУСКОВИЙ РЕДАКТОР

27 квітня 2026 г., 12:26 Переглядів: 1699 Коментарі: 0

Роздрукувати | Надіслати товаришу

Коментарі:

comments powered by Disqus

Олійник

18:15 **На Дніпропетровщині чоловік помер у ТЦК через шість днів після затримання**
18:11 «ГУЛАГ придумав Ізраїль»: ексчемпіон UFC Тактаров відзначився дикою антисемітською заявою та виправданням Сталіна
18:06 Захоплення землі в центрі Києва: до скандального будівництва на Князів Острозьких може бути причетний депутат Баленко
18:01 У Польщі різко зросли масові звільнення: бізнес скорочує персонал на 50%
17:58 **У Тернополі школярка поранила однокласницю ножем: поліція відкрила справу**
17:53 31 мільярд за рік: співзасновник мережі «Аврора» Лев Жиденко очолив рейтинг бізнесменів Полтавщини
17:49 Гроші на ЗСУ замість пісні: 1000 доларів за участь у «Караоке на Майдані» виявилися волонтерським збором
17:45 Зеленський: Україна наростила контракти на 25 тисяч наземних роботизованих систем
17:41 «Повний захист інтересів РФ»: Кім Чен Ин підтвердив підтримку російської війни проти України
17:36 «Немає місця політичній ненависті»: Мелоні підтримала Трампа після стрілянини на вечері кореспондентів
17:31 Єдина зупинка в ЄС: Португалія не стала скасовувати концерт Каньє Веста попри заборони в інших країнах
17:25 **Угода зі слідством та 12 мільйонів гривень для ЗСУ: ВАКС виніс вирок ексдиректору Житомирського БТЗ Бутенку**
17:20 Сили оборони утримують північні околиці Покровська: у ДШВ розповіли про наступ ворога
17:16 Дедлайн змінено: Уряд продовжив термін подання заявок на виплати ВПО до 1 червня
17:11 Президент Естонії: Європа має вже зараз готуватись до завершення війни в Україні
17:06 Частину підробок готували для України: у Польщі ліквідували потужну лінію з виробництва фальшивих євро

Теги новин

COVID-19 агрессия России Атака Війна Война ВСУ Вторжение Дональд Трамп Донбасс ДТП Зеленский

ЗСУ Киев Київ коронавирус Коррупция Напад Росії на Україну Нападение России на Украину оккупанты окупанти Порошенко Путин Росія Россия СБУ США Украина Україна ЧП Эпидемия коронавируса

Наші опитування

Чи вірите ви, що Дональд Трамп зможе зупинити війну між Росією та Україною?

- Так, повністю зможе
- Частково зможе, але не відразу
- Ні, не зможе
- Це залежить від дій інших сторін
- Важко відповісти

Голосувати

Показати результати опитування
Показати всі опитування на сайті

Головна
Про нас
Статті
Архів
Закони
Контакти

Новини
Рейдерство
Корупція
Економіка
Новини світу

Конфлікти
Політика
Корпоративні конфлікти
Кримінал

Позиція
Коментарі
Різне

Думка
Політика
Економіка

Події

Війна

Відео

Блоги

Facebook
Twitter
YouTube
RSS-підписка
Email-розсилка
Мобільна версія