QApp

Квантовая угроза

Новые вызовы для инфраструктуры открытых ключей

QApp.tech

Sk Киберкластер

КУАПП — СПИН-ОФФ РОССИЙСКОГО КВАНТОВОГО ЦЕНТРА. РАЗРАБОТЧИК ПРОГРАММНЫХ РЕШЕНИЙ НА ОСНОВЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

Решения QApp были представлены **Президенту РФ** в рамках Форума Будущих технологий 2023

ФОРУМ БУДУЩИХ ТЕХНОЛОГИЙ

- Спинофф Российского квантового центра
- Лауреат всероссийских премий и конкурсов ИТ-продуктов
- Участник Кибекластера Сколково
- При стратегической поддержке Газпромбанка
- Разработчик стандартов постквантовой криптографии в РФ
- Научная деятельность поддержана институтами развития РФ

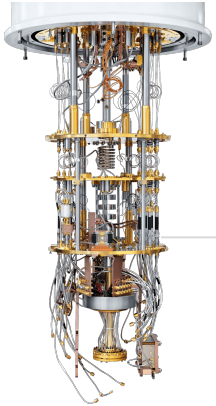
23 сотрудника

6 цифровых продуктов

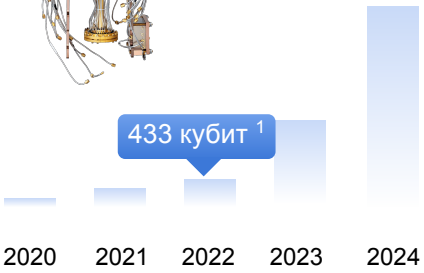
Продукты и услуги уже пилотируются

Банк России, СБЕР, ГАЗПРОМБАНК, ВТБ, Baikal Electronics, МЦСТ Эльбрус, s•terra, QRATE, T1

КВАНТОВАЯ УГРОЗА ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Квантовые компьютеры активно развиваются год от года [2]
Уже доступны через облако



С помощью квантовых компьютеров злоумышленники могут атаковать данные, защищенные традиционными методами

Распространенные сегодня алгоритмы криптографии неустойчивы к квантовой угрозе

Распределение ключей	Асимметричное шифрование	Электронная подпись
ECDH DH	RSA	ECDSA DSA ГОСТ Р 34.10-2012

4098 кубит позволяют взломать популярную криптосистему RSA-2048 [2]

Квантовая угроза усиливает ключевые риски ИБ

- Утечка персональных данных клиентов
- Репутационные риски
- Фрод по платежам и подмена реквизитов
- Финансовые потери
- Санкции и штрафы со стороны регулятора
- Умышленный перехват трафика
- Увеличение задержек соединения вплоть до полной сетевой недоступности сервисов

Источники [1] IBM, [2] Без учета коррекции ошибок (Arxiv)

МОДЕЛЬНЫЕ ЗАДАЧИ

RSA-2048

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2]

[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

2x10 [7] физических кубитов, 8 часов

349143 cat-qubits, 4 суток

ECDLP-256 (ГОСТ Р 34.10-2018)

Improved quantum circuits for elliptic curve discrete logarithms

Thomas Häner[1], Samuel Jaques[2] *†, Michael Naehrig[3], Martin Roetteler[1], and Mathias Soeken[1]

[1] Microsoft Quantum, Redmond, WA, USA
{thhaner,martinro,a-masoek}@microsoft.com
[2] Department of Materials, University of Oxford, UK
samuel.jaques@materials.ox.ac.uk
[3] Microsoft Research, Redmond, WA, USA
mnaehrig@microsoft.com

7x10 [6] физических кубитов

doi:10.1103/PhysRevLett.131.040602

Performance Analysis of a Repetition Cat Code Architecture: Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126 133 Cat Qubits

Élie Gouzien[1,*] Diego Ruiz[2,3] Francois-Marie Le Régent[2,3] Jérémie Guillaud[2] and Nicolas Sangouard[1,†]

[1] *Université Paris–Saclay, CNRS, CEA, Institut de physique théorique, 91 191 Gif-sur-Yvette, France*
[2] *Alice&Bob, 53 boulevard du Général Martial Valin, 75 015 Paris, France*
[3] *Laboratoire de Physique de l'École normale supérieure, École normale supérieure, Mines Paris, Université PSL, Sorbonne Université, CNRS, Inria, 75 005 Paris, France*

(Dated: August 7, 2023)

123133 cat-qubits, 9 часов

ГИБРИДНЫЙ ПОДХОД

RSA-2048: сублинейная сложность?

Factoring integers with sublinear resources on a superconducting quantum processor

Bao Yan,[1,2,*] Ziqi Tan,[3,*] Shijie Wei,[4,*] Haocong Jiang,[5] Weilong Wang,[1] Hong Wang,[1] Lan Luo,[1] Qianheng Duan,[1] Yiting Liu,[1] Wenhao Shi,[1] Yangyang Fei,[1] Xiangdong Meng,[1] Yu Han,[1] Zheng Shan,[1] Jiachen Chen,[3] Xuhao Zhu,[3] Chuanyu Zhang,[3] Feitong Jin,[3] Hekang Li,[3] Chao Song,[3] Zhen Wang,[3,†] Zhi Ma,[1,‡] H. Wang,[3] and Gui-Lu Long[2,4,6,7,§]

[1]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China*
[2]*State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China*
[3]*School of Physics, ZJU-Hangzhou Global Scientific and Technological Innovation Center, Interdisciplinary Center for Quantum Information, and Zhejiang Province Key Laboratory of Quantum Technology and Device, Zhejiang University, Hangzhou 310000, China*
[4]*Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[5]*Institute of Information Technology, Information Engineering University, Zhengzhou 450001, China*
[6]*Beijing National Research Center for Information Science and Technology and School of Information Tsinghua University, Beijing 100084, China*
[7]*Frontier Science Center for Quantum Information, Beijing 100084, China*

Shor's algorithm has seriously challenged information security based on public key cryptosystems. However, to break the widely used RSA-2048 scheme, one needs millions of physical qubits, which is far beyond current technical capabilities. Here, we report a universal quantum algorithm for integer factorization by combining the classical lattice reduction with a quantum approximate optimization algorithm (QAOA). The number of qubits required is $O(\log N/\log\log N)$, which is sublinear in the bit length of the integer N, making it the most qubit-saving factorization algorithm to date. We demonstrate the algorithm experimentally by factoring integers up to 48 bits with 10 superconducting qubits, the largest integer factored on a quantum device. We estimate that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048 using our algorithm. Our study shows great promise in expediting the application of current noisy quantum computers, and paves the way to factor large integers of realistic cryptographic significance.

372 физических кубита!

Валидация на эмуляторе

Pitfalls of the sublinear QAOA-based factorization algorithm

S.V. Grebnev[1], M.A. Gavreev[1], E.O. Kiktenko[1], A.P. Guglya[1], A.R. Efimov[2], and A.K. Fedorov[1]

[1]Russian Quantum Center, Skolkovo, Moscow 121205, Russia
[2]Sberbank of Russia, Sber Innovation and Research, Moscow 121357, Russia
{s.grebnev,m.gavreev,e.kiktenko,apg}@rqc.ru, {AREfimov}@sberbank.ru, akf@rqc.ru

Алгоритм некорректен!
Но сам подход – перспективный

ГИБРИДНЫЙ ПОДХОД

Валидация на эмуляторе

Pitfalls of the sublinear QAOA-based factorization algorithm

S.V. Grebnev[1], M.A. Gavreev[1], E.O. Kiktenko[1], A.P. Guglya[1], A.R. Efimov[2], and A.K. Fedorov[1]

[1]Russian Quantum Center, Skolkovo, Moscow 121205, Russia

[2]Sberbank of Russia, Sber Innovation and Research, Moscow 121357, Russia

{s.grebnev,m.gavreev,e.kiktenko,apg}@rqc.ru, {AREfimov}@sberbank.ru, akf@rqc.ru

A comment on "Factoring integers with sublinear resources on a superconducting quantum processor"

Tanuj Khattar[1,*] and Noureldin Yosri[2,†]

[1]*Google Research, Venice, CA 90291, United States*

[2]*Google, Dublin, Ireland*

(Dated: July 24, 2023)

Quantum computing has the potential to revolutionize cryptography by breaking classical public-key cryptography schemes, such as RSA and Diffie-Hellman. However, breaking the widely used 2048-bit RSA using Shor's quantum factoring algorithm is expected to require millions of noisy physical qubits and is well beyond the capabilities of present day quantum computers. A recent proposal by Yan et. al. tries to improve the widely debated Schnorr's lattice-based integer factorization algorithm using a quantum optimizer (QAOA), and further claim that one can break RSA 2048 using only 372 qubits. In this work, we present an open-source implementation of the algorithm proposed by Yan et. al. and show that, even if we had a perfect quantum optimizer (instead of a heuristic like QAOA), the proposed claims don't hold true. Specifically, our implementation shows that the claimed sublinear lattice dimension for the Hybrid quantum+classical version of Schnorr's algorithm successfully factors integers only up to 70 bits and fails to find enough factoring relations for random 80 bit integers and beyond. We further hope that our implementation serves as a playground for the community to easily test other hybrid quantum + classical integer factorization algorithm ideas using lattice based reductions.

МОДЕЛЬ КВАНТОВОЙ АТАКИ «СОХРАНЕНИЕ ДАННЫХ СЕЙЧАС — ВЗЛОМ ПОТОМ»

СТАТУС ВАЛИДАЦИИ РЕГУЛЯТОРОМ ПОСТКВАНТОВЫХ ЭЦП

ОТЕЧЕСТВЕННЫЕ ПОСТКВАНТОВЫЕ АЛГОРИТМЫ ЭЦП

Предлагаемые ЭЦП	Статус работ в рамках Технического комитета ТК26
ЭЦП Гиперикум	Первая текущая версия реализации алгоритма полностью поддерживается в продуктах. Ведётся разработка спецификации с учётом замечаний ТК26. Готовность спецификации с учётом правок: 4 квартал 2023 года
ЭЦП Крыжовник	Реализована первая версия алгоритма. Схема находится на стадии переработки для повышения уровня стойкости и нефункциональных характеристик. Планируется переработать схему, оформить документы и отправить на экспертизу в 1 квартале 2024 года
ЭПЦ Шиповник	В феврале 2023 получен первый пакет замечаний по проекту стандарта. Обновлённый пакет документов по ЭЦП Шиповник будет отправлен в ТК26
Предлагаемые KEM	Разработка KEM на кодах и решетках, готовность: 2024 год

ПРОБЛЕМАТИКА НА ПУТИ ВНЕДРЕНИЯ PKI

Технологические

- Поддержка постквантовых / гибридных сертификатов в прикладных протоколах с учетом ограничений сообщений
- Падение производительности, необходимость аппаратного ускорения
  В частности, можно переиспользовать уже имеющиеся СФ-Блоки для ускорения Стрибог, т.к. широко используется во всех отечественных схемах
- Протоколы на основе UDP – не лезет в MTU

Регуляторные

- Необходимость обновления пула стандартов ГОСТ Р 34
- Обновление пула РС и МР по прикладным протоколам для внедрения постквантовой и гибридной криптографии
- Выработка OID
- Сценарии переходного периода

Другие

- Сомнения в необходимости в постквантовой криптографии от отдельно-взятых вендоров текущих криптографических решений асимметричной криптографии

УДОСТОВЕРЯЮЩИЙ ЦЕНТР С ПОДДЕРЖКОЙ ПОСТКВАНТОВЫХ ПОДПИСЕЙ

Квантовая угроза усиливает возможные риски при взломе УЦ или модификации ключевого носителя ЭП:

- Финансовые потери
- Кража персональных данных
- Компрометация банковской, производственной, государственной и других тайны
- Репутационные риски
- Санкции и штрафы со стороны регуляторов
- Несанкционированный доступ к информационным системам

Преимущества перед «классическим» функционалом УЦ

- Поддержка отечественных квантово-устойчивых сертификатов
- Предотвращение попыток модификаций ЭЦП
- Предотвращение финансовых потерь связанных с подменой реквизитов и подписи
- Возможность масштабирования и использование гибридных подписей до принятия стандартов
- Увеличение выручки за счет использования технологического первенства на рынке УЦ
- Масштабирование проекта за счет внедрения постквантового АВЕ

ОСНОВНАЯ ЦЕННОСТЬ ПИЛОТИРОВАНИЯ ПРОДУКТОВ НА ОСНОВЕ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ СЕЙЧАС

- Оценка затрат (время/деньги/прочие ресурсы) ввода в промышленную эксплуатацию квантово-устойчивых решений
  Оценка затрат по переводу ИТ-инфраструктуры на новый вид криптографии в проекции на срок принятия стандартов РФ

- Выработка криптографической гибкости — снижение зависимости от конкретного вендора криптографии
  Исследование уровня криптографической гибкости и точек привязки к определенному поставщику криптографических решений, ограничивающих возможности поддержки и адаптации инфраструктуры к новым типам угроз и уязвимостей

  - Оценка рисков для уже имеющихся информационных активов и приоритезация направлений для интеграции квантово-устойчивых решений
  - Оценка сервисов и продуктов на уязвимость к квантовой угрозе
  - Определение этапности интеграции квантово-устойчивой защиты в инфраструктуру экосистемы

QApp

Сергей Гребнев

Руководитель направления
прикладных исследований

Email: sg@qapp.tech

Телефон: +7 910 469-91-26

Telegram: @pikkunorsu

QApp.tech

Sk Киберкластер