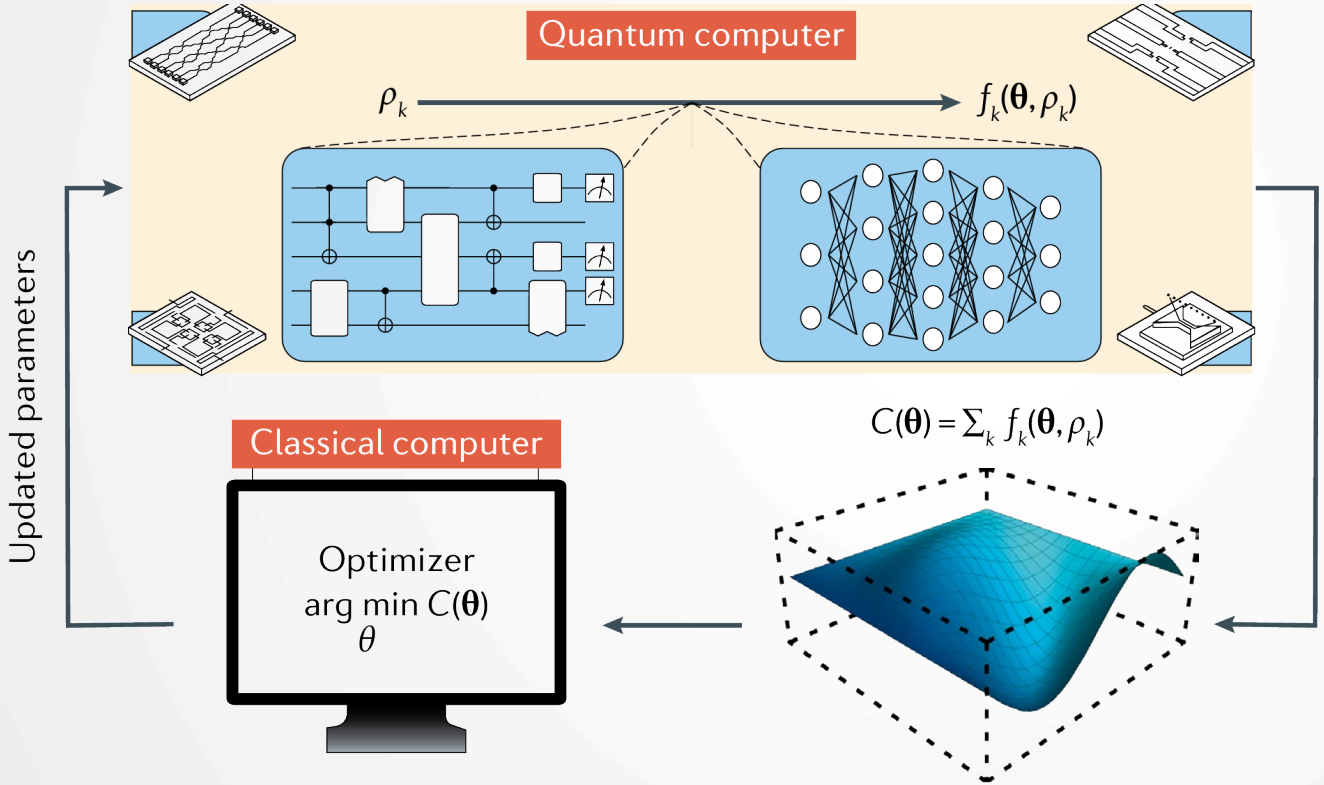
infotecs

Вариационные квантовые алгоритмы как перспективный метод универсального криптоанализа

Алексей Моисеевский, Софья Манько

Вариационные квантовые алгоритмы

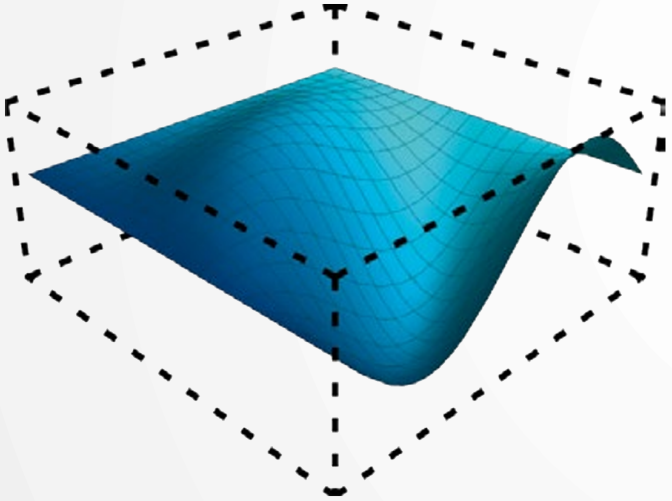


- VQA – Variational Quantum Algorithm
- VQE – Variational Quantum Eigensolver
- VQAA – Variational Quantum Attack Algoritm
- QML – Quantum Machine Learning

Cerezo M. et al. Variational quantum algorithms //Nature Reviews Physics. – 2021. – Т. 3. – №. 9. – С. 625-644.

Концепция вариационных алгоритмов

$$C(\boldsymbol{\theta}) = \sum_k f_k(\boldsymbol{\theta}, \rho_k)$$



VQA, VQE, VQAA, QML

Идея – дать **классическому оптимизатору** исследовать рельеф целевой функции **в гильбертовом пространстве** квантовых состояний

Из-за ненулевой амплитуды глобального минимума, возможно **«тунеллирование» целевой функции**, то есть неклассический градиент

Работа вариационного алгоритма

Задать параметры квантовой схемы

↓

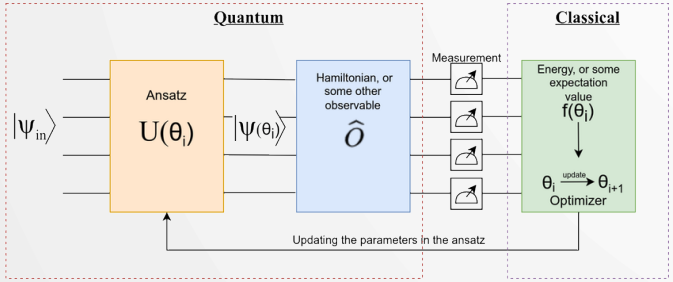
Измерить состояния кубитов

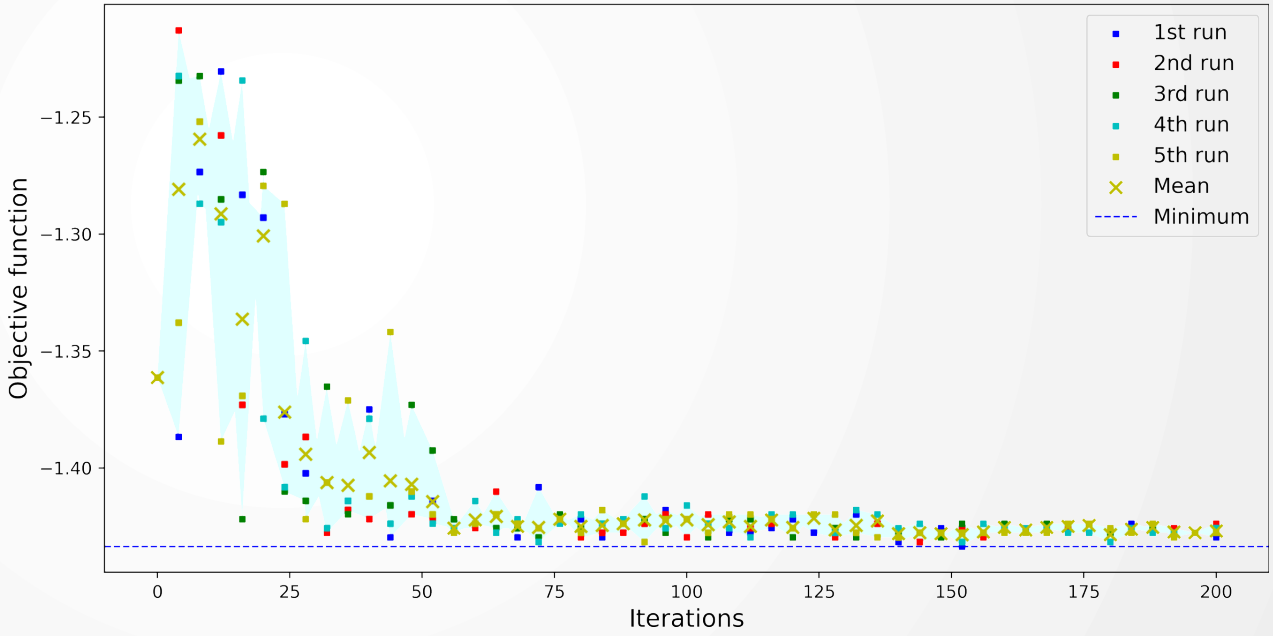
↓

Рассчитать целевую функцию

↓

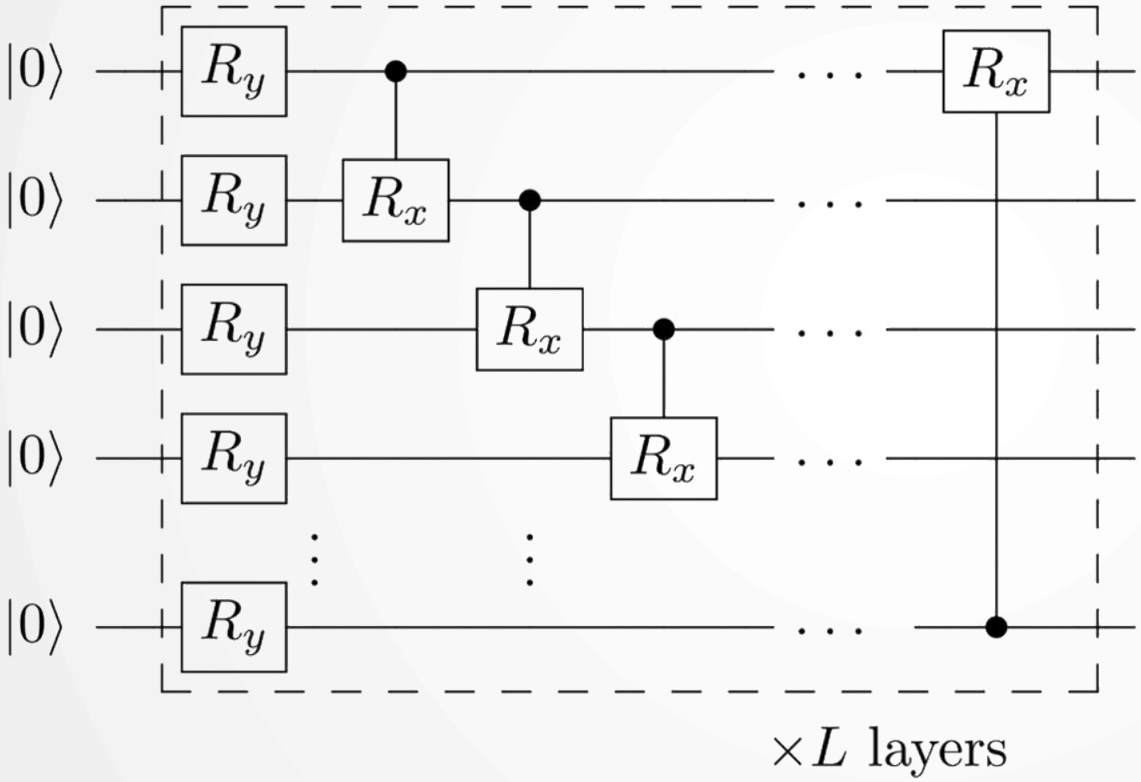
Обновить параметры схемы





Kungurtsev V. et al. Iteration complexity of variational quantum algorithms //Quantum. – 2024. – Т. 8. – С. 1495.
Singh H., Majumder S., Mishra S. Benchmarking of different optimizers in the variational quantum algorithms for applications in quantum chemistry //The Journal of Chemical Physics. – 2023. – Т. 159. – №. 4.

Квантовая схема VQA – «Анзац»



Используются схемы разных топологий

Схема должна быть:

- Параметризована
- Способна готовить целевое состояние (нужное число кубитов и их запутанность)

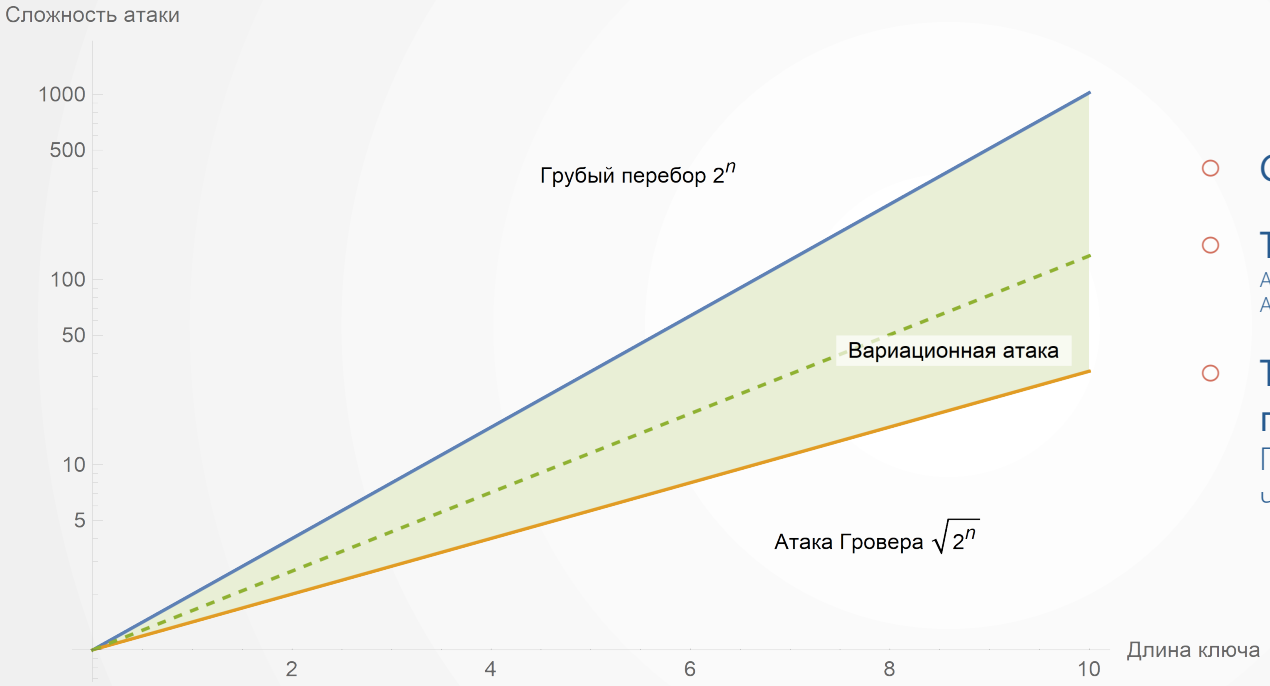
Важно!

Число параметров схемы сильно меньше количества переменных, полностью описывающих состояние

Ненулевая амплитуда целевого классического исхода позволит «ухватить» нужный результат

Jaderberg B. et al. Quantum self-supervised learning //Quantum Science and Technology. – 2022. – Т. 7. – №. 3. – С. 035005.

Сложность вариационного алгоритма



- Скорее всего, не лучше Гровера
- Точно не лучше $2^{n/3}$, иначе P = NP
  Aaronson S. Quantum computing and hidden variables //Phys. Rev. A. – 2005. – Т. 71. – №. 3. – С. 032325.
- Точно не хуже классического перебора
  Потому что классические вычисления – частный случай квантовых

VQA в задаче симметричного криптоанализа

Подход 1 – Квантовый оракул

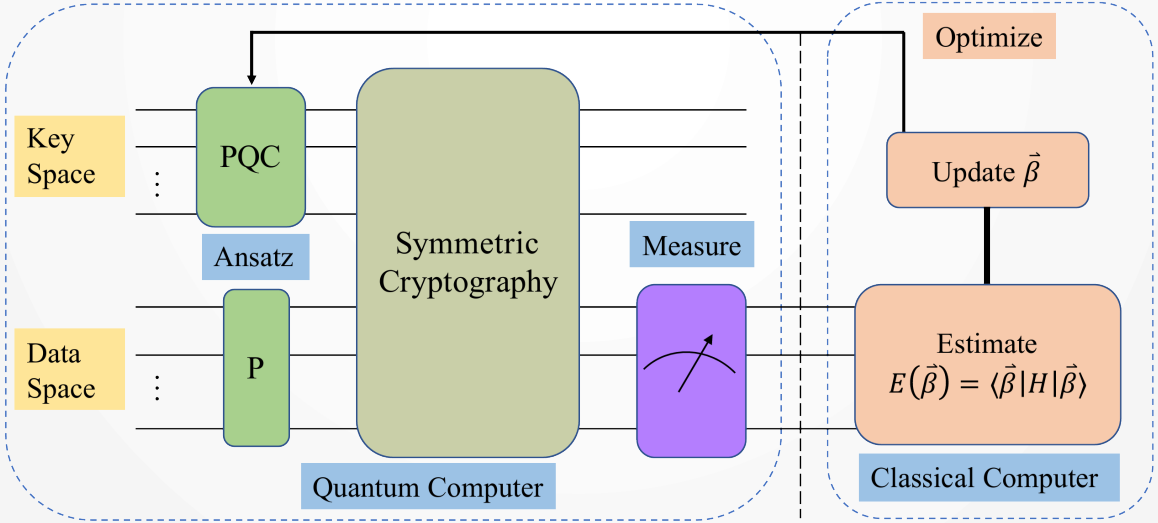
Оракул – подпрограмма, определяющая корректность поданного на вход решения задачи

Решаем задачу атаки на открытый текст: по паре ОТ - ШТ восстановить ключ
Тогда работа оракула – зашифровать ОТ поданным ключом и сравнить с ШТ

VQAA – симметричная вариационная атака

Подход 1 – Квантовый оракул

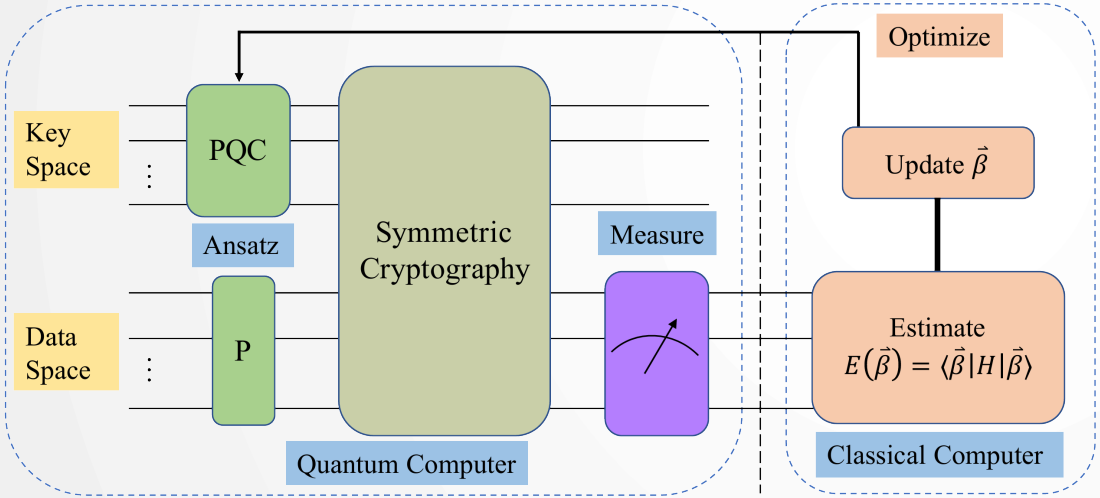
Пусть квантовая схема подобно оракулу в алгоритме Гровера генерирует в определённых кубитах состояние $|0\rangle$ тогда и только тогда, когда подан верный ключ



Wang Z. et al. Variational quantum attacks threaten advanced encryption standard based symmetric cryptography //Science China Information Sciences. – 2022. – Т. 65. – №. 10. – С. 200503.

VQAA – симметричная вариационная атака

Подход 1 – Квантовый оракул



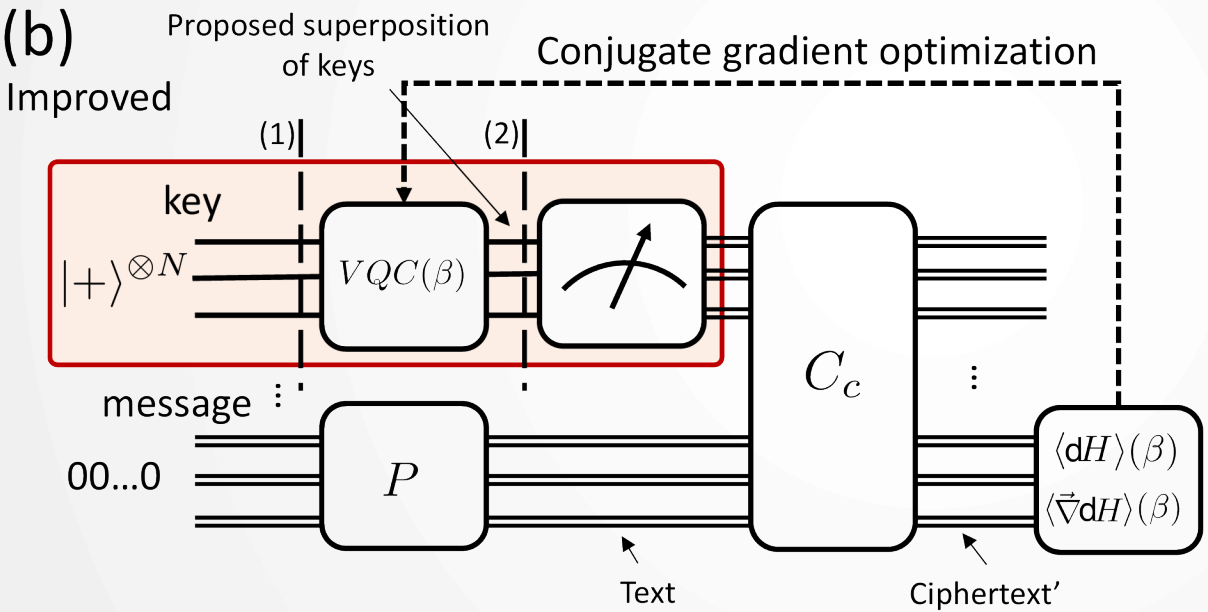
+ Показывает ускорение примерно как атака Гровера
+ Считывается градиент гильбертова пространства – целевая функция фактически квантовая
+ **Может сойтись быстрее Гровера**
− **Может не сойтись вообще**
− Схема шифра находится в квантовой части, что делает программу очень сложной

  Хотя в атаке алгоритмом Гровера такой недостаток неизбежен

Wang Z. et al. Variational quantum attacks threaten advanced encryption standard based symmetric cryptography //Science China Information Sciences. – 2022. – Т. 65. – №. 10. – С. 200503.

Enhanced (Improved?) **VQAA**

Подход 2 – Классический оракул



Пусть квантовая схема генерирует **только ключ**

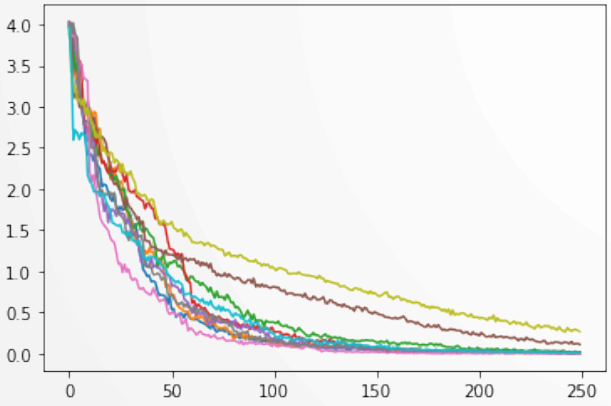
Если оптимизатор в гильбертовом пространстве отличит шифр от случайной подстановки, алгоритм сойдётся

+ Квантовая схема становится тривиальной и компактной, **максимально NISQ-Friendly**
+ ***Квантовая схема не зависит принципиально от логики в основе атакуемого шифра***
+ Может сойтись быстрее Гровера
− Может не сойтись вообще

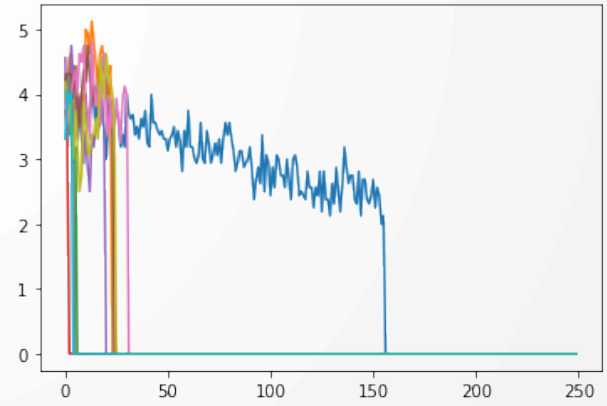
Aizpurua B. et al. Hacking cryptographic protocols with advanced variational quantum attacks //ACM Transactions on Quantum Computing. – 2025.

Специфика VQAA по сравнению с VQE

- Заранее известно значение целевой функции в глобальном минимуме
- Достаточно достичь глобального минимума один раз – возникает «режим угадывания»
- Возникает параметр «числа шотов» – число перезапусков квантовой схемы с одним набором параметров и измерений ключа, по которому оценивается целевая функция

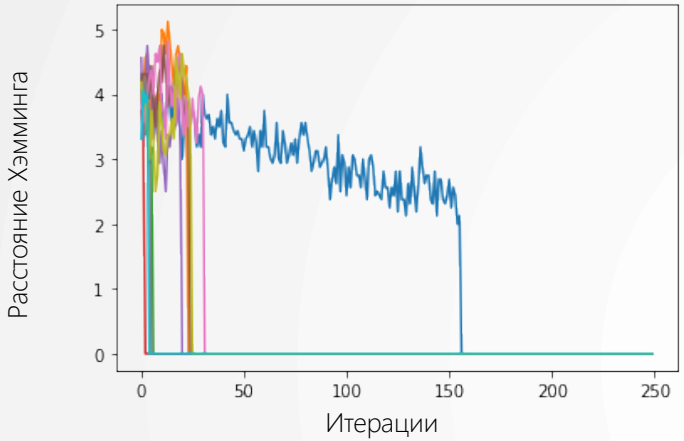


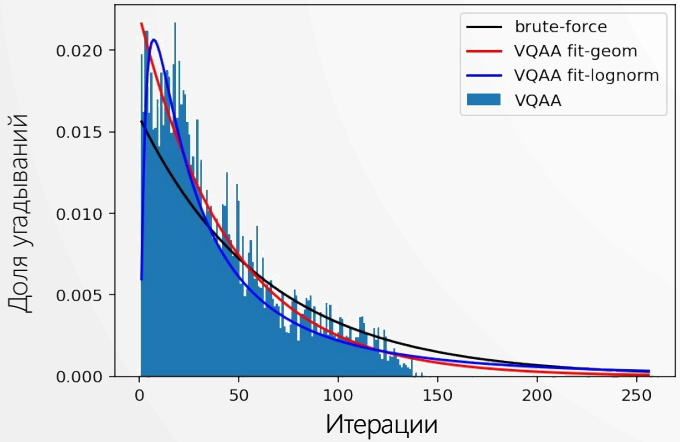
Обычная сходимость VQA



«Режим угадывания»

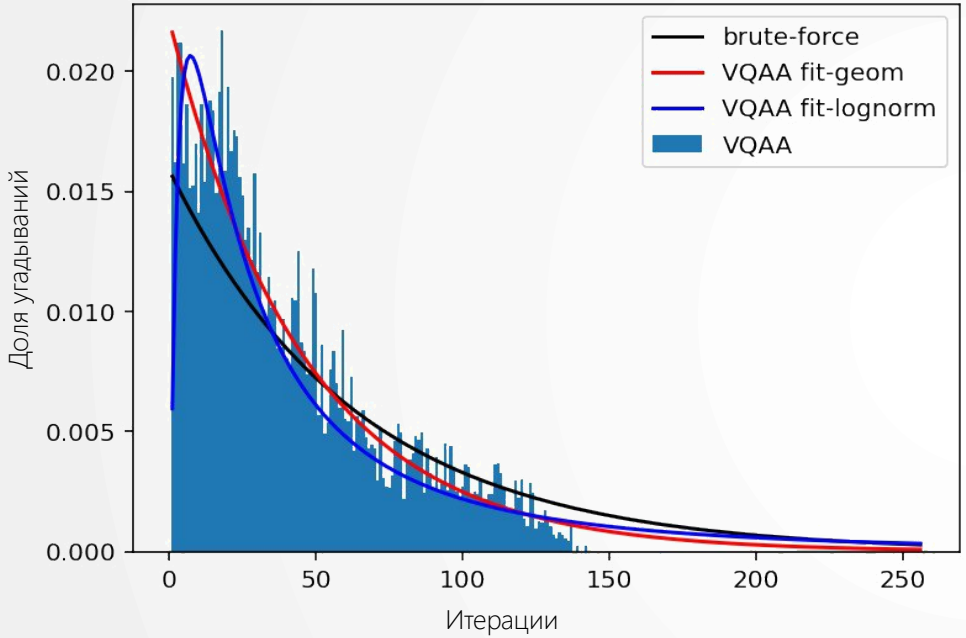
Специфика вариационного криптоанализа



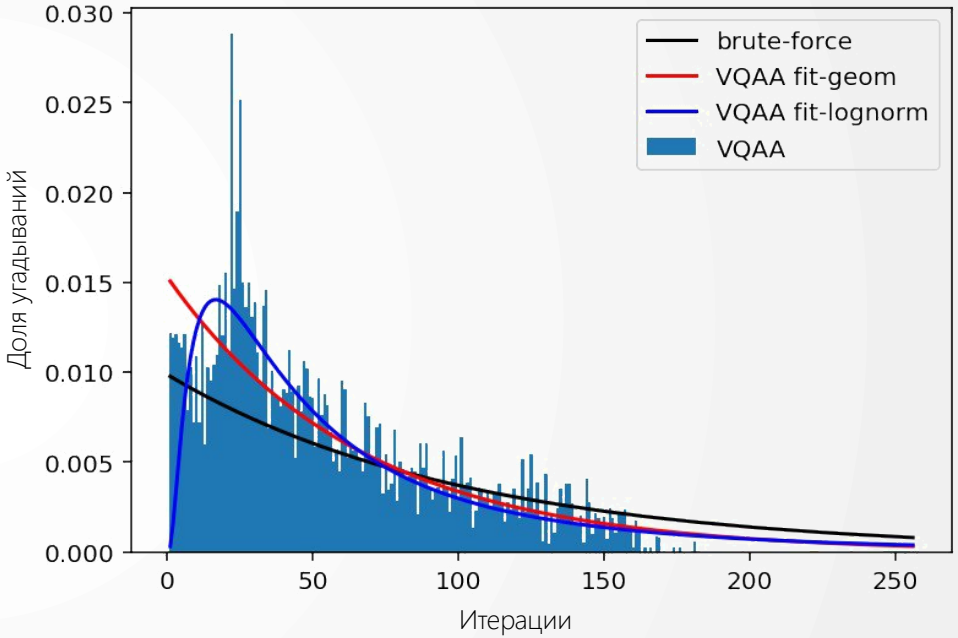


- В «режиме угадывания» интерес представляет зависимость вероятности угадывания от числа попыток
- Распределение вероятности будет меняться также с изменением числа шотов
- Надо помнить, что вероятность успеха атаки (сходимости оптимизатора) может быть ограничена и зависеть от числа шотов

Моделирование атаки S-AES с утечкой

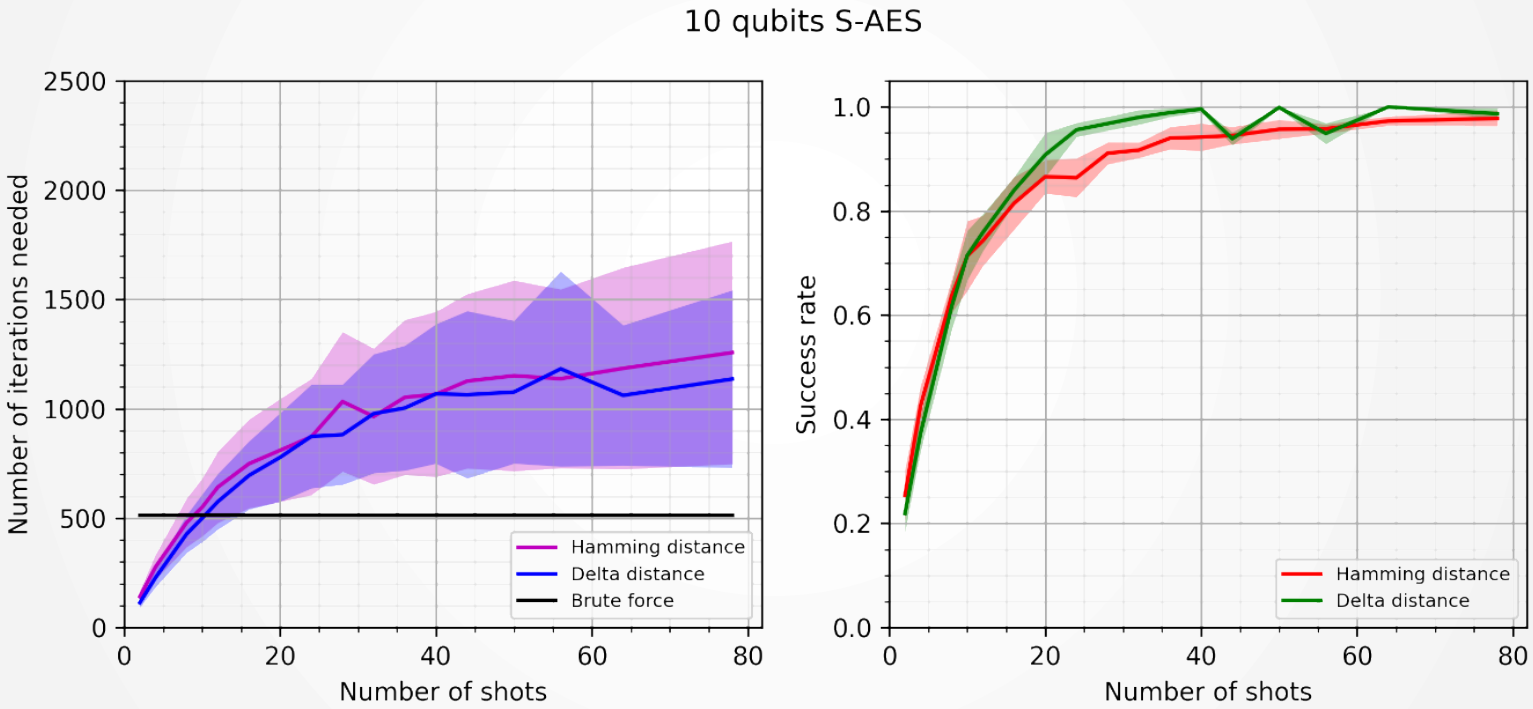


Атака на 8 битов ключа при 4 шотах на итерацию
Случайное гадание: Успех 98.18 ± 0.44 %, $P_{успеха}$ = 0.0156
VQAA: Успех 81.40 ± 8.30 %, $P_{успеха}$ = 0.0216 ± 0.0004

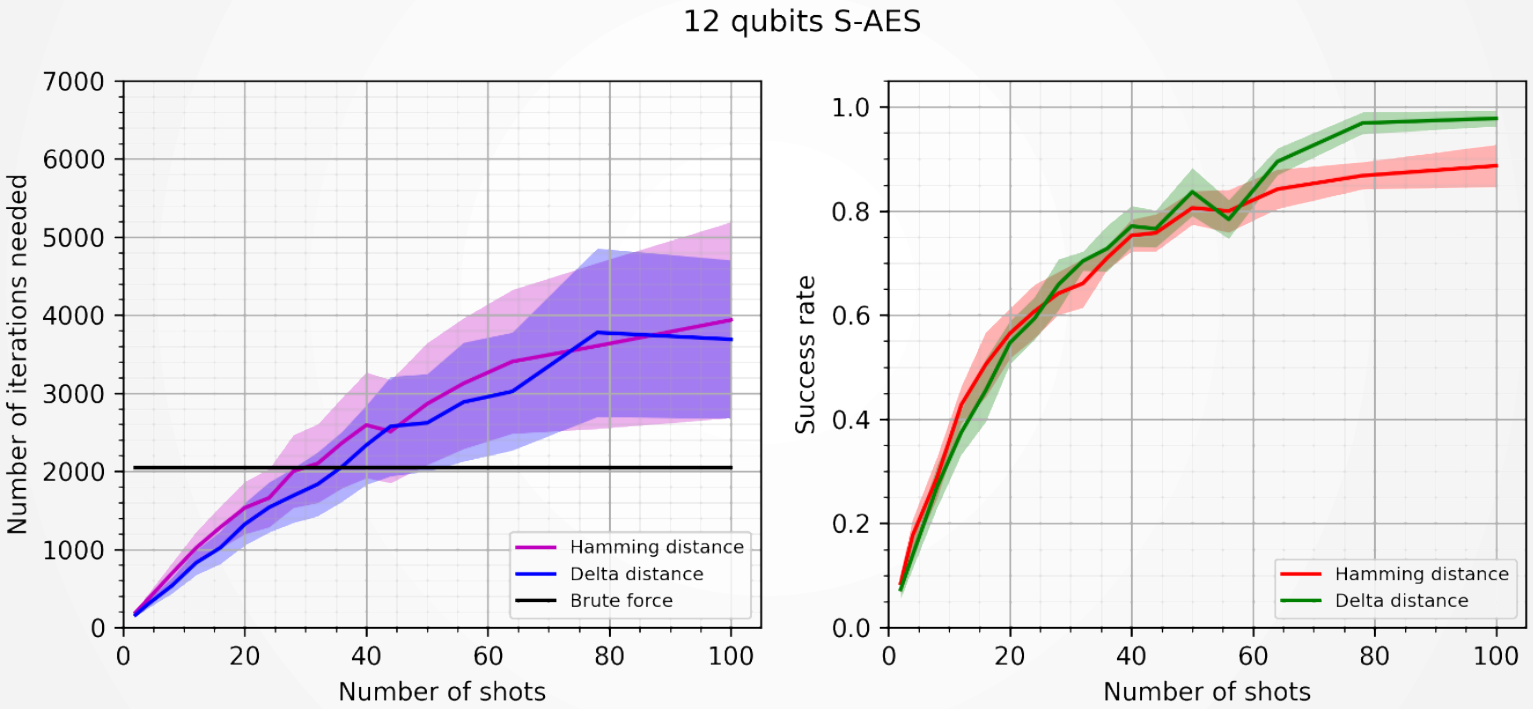


Атака на 10 битов ключа при 10 шотах на итерацию
Случайное гадание: Успех 99.97 ± 0.03%, $P_{успеха}$ = 0.0098
VQAA: Успех 78.76 ± 6.83 %, $P_{успеха}$ = 0.0151 ± 0.0005

Зависимость успеха от числа шотов



Зависимость успеха от числа шотов



Выводы

- VQAA-криптоанализ позволяет «разменивать» снижение вероятности успеха на снижение числа попыток – принцип «либо сойдётся быстрее, либо не сойдётся совсем»
- С учётом ограниченной вероятности успеха наблюдается измеримая область квантового преимущества
- **Отечественные квантовые вычислители уже сегодня способны экспериментально продемонстрировать атаку на упрощённые шифры с утечкой**

	Общее число итераций	Ключей генерируется за итерацию	Доля успешных атак	$P_{угадывания}$
Случайное угадывание (8 бит)	256	4	98.18 ± 0.44 %	0.0156
VQAA (8 бит)	256	4	81.40 ± 8.30 %	0.0216 ± 0.0004
Случайное угадывание (10 бит)	256	10	99.97 ± 0.03%	0.0098
VQAA (10 бит)	256	10	78.76 ± 6.83 %	0.0151 ± 0.0005

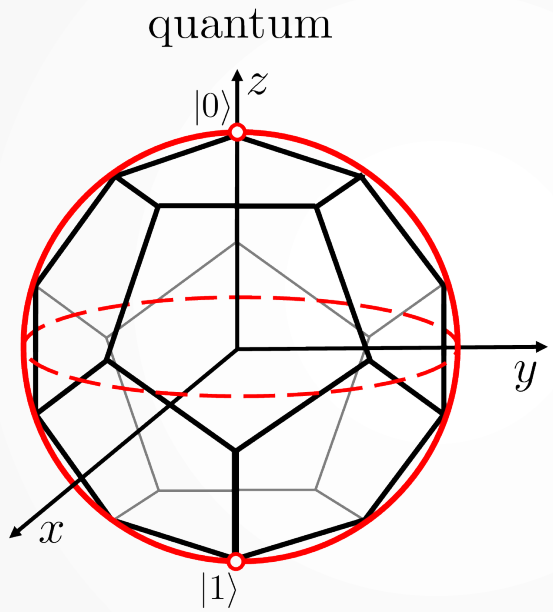
Замечания

- Все атаки промоделированы для однослойного анзаца. Увеличение числа слоёв приводит к снижению доли успеха – избыточные параметры
- Должна считаться «попыткой угадывания» генерация результатов измерений кубитов или шаг итерации оптимизатора? От этого существенно зависит область преимущества
- Нормировка «доли угадывания» в гистограммах проведена на число запусков с успешными исходами. Но даже при нормировке на общее число запусков сохраняется область преимущества за пределами стандартного отклонения
- **Может ли быть область превосходства увеличена доработкой алгоритма? – Да!**

Улучшение 1 – неортогональное кодирование

classical

$q_\alpha = 0, 1, \cdots, 19$



С использованием неортогональных состояний в один кубит может быть закодировано более одного бита

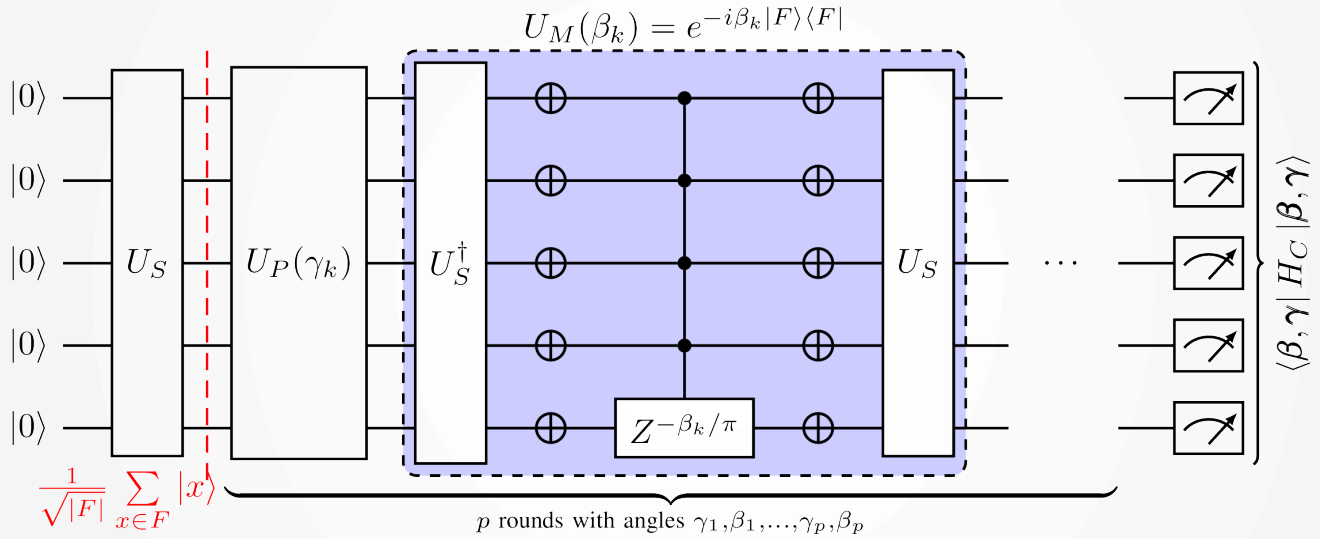
Для декодирования битовой последовательности из одного кубита проводится квантовая томография, **требующая значительного, но константного числа шотов**

Вопрос о принципе подсчёта итераций в данном случае встаёт особенно остро

Bermejo P., Orús R. Variational quantum non-orthogonal optimization //Scientific Reports. – 2023. – Т. 13. – №. 1. – С. 9840.

Улучшение 2 – Гроверовское усиление

«Grover Mixer»



Единичная итерация алгоритма Гровера для состояния в суперпозиции большого числа вариантов со значительными вероятностями увеличит шанс считывания верного ответа

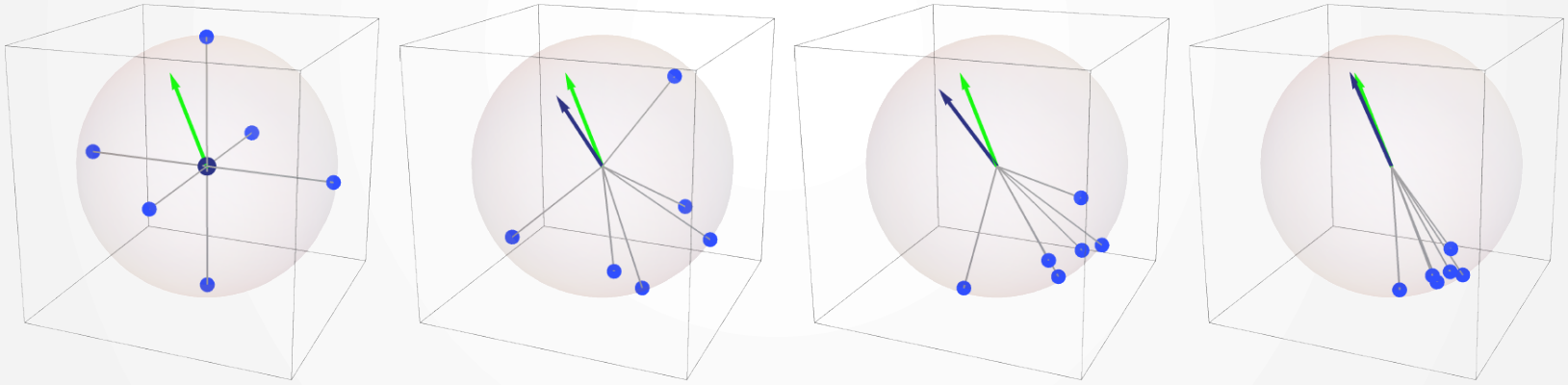
Её можно добавить к итерации VQA

Bärtschi A., Eidenbenz S. Grover mixers for QAOA: Shifting complexity from mixer design to state preparation //2020 IEEE International Conference on Quantum Computing and Engineering (QCE). – IEEE, 2020. – С. 72-82.

Улучшение 3 – Адаптивная томография

«Adaptive tomography»» / Shadow tomography»

В предположении, что за одну итерацию оптимизатора генерируемое состояние меняется несильно, можно полезно использовать информацию о ранее полученных измерениях состояния для более удачной подстройки измерительного базиса



(a) Initial view. (b) The first iteration. (c) Ten iterations. (d) Fifty iterations.

Пост-квантовый квантовый криптоанализ?

- Шифры, предлагаемые в качестве пост-квантовых стандартов не обладают строго доказанной математической стойкостью
- Алгоритм VQAA, являясь методом решения задачи без заранее определённого сценария, может атаковать шифры вне зависимости от их внутренней логики
- При неудачном выборе потенциально квантово-ускоряемой задачи в качестве основы пост-квантового шифра, попытка квантовой вариационной атаки может указать на наличие неявного градиента на рельефе целевой функции

Экспериментальная реализация?

«Каждые 5 лет нам объявляют, что до эры квантового превосходства остаётся 5 лет»

Характеристик отечественных квантовых вычислителей на момент начала 2025 года – 12-50 кубитов, доступная глубина схемы 10-20 слоёв – **вполне достаточно для экспериментальной демонстрации** по крайней мере частичной VQAA-атаки на упрощённые шифры S-AES, S-DES и Blowfish

Техника неортогонального кодирования может позволить продемонстрировать на российских вычислителях частичную атаку на шифры типа **AES-128 к 2030 году, при условии** концентрации усилий над **повышением качества кубитов** и обеспечением возможности **работы со всем объёмом регистра** в ходе выполнения одной программы

Для данной цели 300 операций в алгоритме важнее 300 кубитов

infotecs

Алексей Моисеевский

Ведущий специалист по квантовым вычислениям

+7 968 016 97 32

Aleksey.Moiseevsky@infotecs.ru
Amoiseevskiy@gmail.com