Факультет компьютерных наук | Программная инженерия | 03.06.2025

ПОСТКВАНТОВЫЕ КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ ЦИФРОВОЙ ПОДПИСИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ И ГЛАВНЫЕ ПРОБЛЕМЫ

POST-QUANTUM CRYPTOGRAPHIC DIGITAL SIGNATURE ALGORITHMS: COMPARATIVE ANALYSIS AND MAIN PROBLEMS

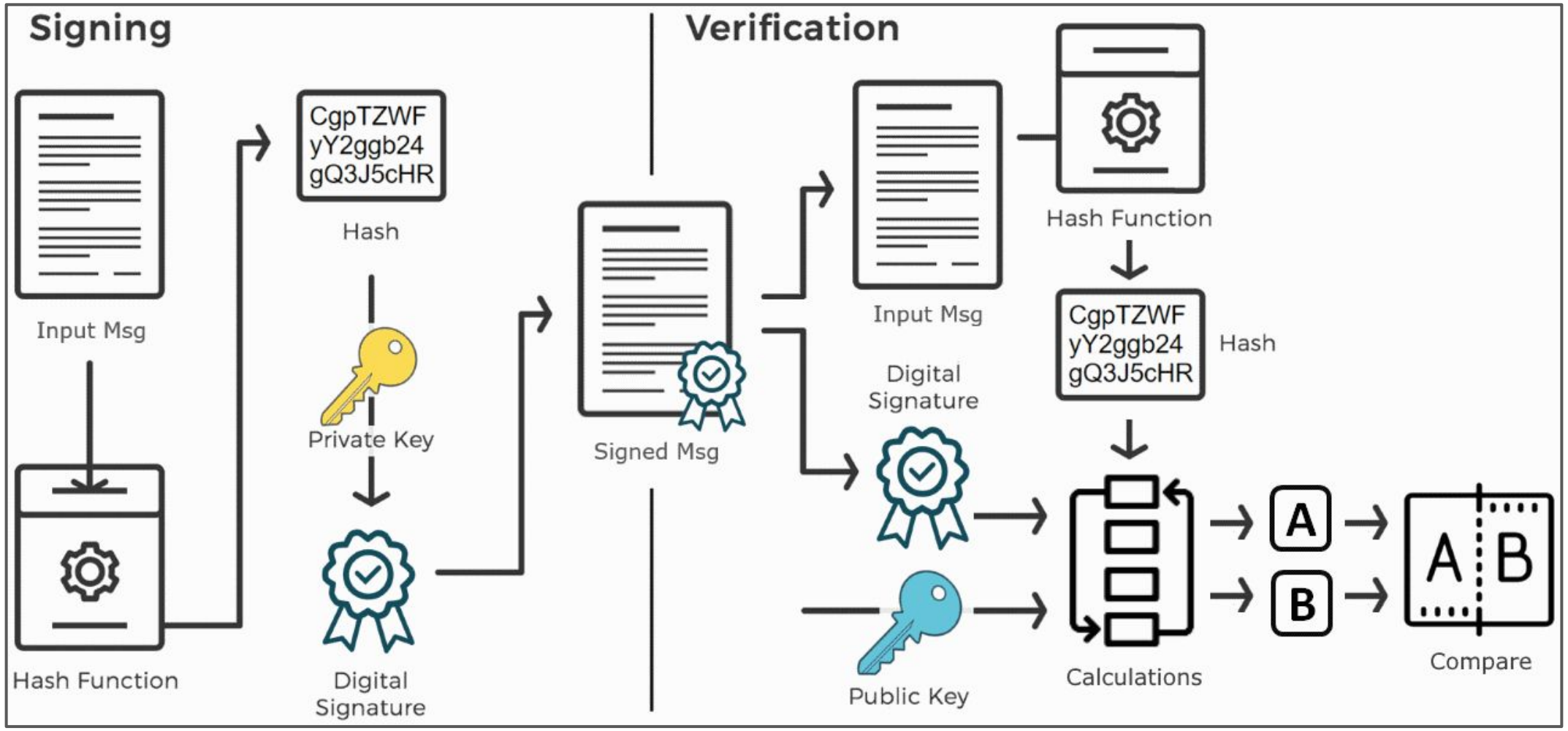
Исполнитель: Качмазов Руслан Александрович, БПИ221
Научный руководитель: Хаустов Александр Иванович

Индивидуальный исследовательский проект

Что такое электронная цифровая подпись (ЭЦП)?

Недостаточно обеспечивать конфиденциальность и целостность данных.

- Шифрование - конфиденциальность
- Имитовставка - целостность
- Цифровая подпись - авторство и невозможность отказа от действий


Signing
Verification
Input Msg
Hash Function
CgpTZWF
yY2ggb24
gQ3J5cHR
Hash
Private Key
Digital
Signature
Signed Msg
Input Msg
Hash Function
Digital
Signature
CgpTZWF
yY2ggb24
gQ3J5cHR
Hash
Public Key
Calculations
A
B
A B
Compare

В чем проблема?

Алгоритм Шора – теоретически, на квантовом компьютере позволяет выполнять факторизацию чисел и считать дискретный логарифм за полиномиальное время. Под угрозой ассиметричная криптография (RSA, (EC)DSA, (EC)DH и другие)

Алгоритм Гровера – теоретически, на квантовом компьютере уменьшает пространство перебора в два раза. Под угрозой симметричные алгоритмы и хэш-функции.
Проблема решается увеличением ключей или выходной последовательности в два раза.

В чем проблема?

Алгоритмы RSA, (EC)DSA, (EC)DH, ГОСТ 34.10 и многие другие не устойчивы перед достаточно мощными квантовыми вычислениями.

Могут быть скомпрометированы данные, которые перехватывали многие годы, а потом расшифровали, используя взломанные квантовым компьютером ключи.

Нужны новые алгоритмы, устойчивые к квантовым и классическим атакам.

Появляется новый раздел криптографии - постквантовая (PQC).

Что делать?

Постквантовую криптографию.

Основой для постквантовых асимметричных схем криптографии, и цифровой подписи в частности, выступают следующие математические структуры:

1) **Теория решеток**
2) **Хэш-функции**
3) **Коды исправления ошибок**
4) **Многомерные квадратичные системы**
5) **Изогении эллиптических кривых**
6) ...

Что сделали?

NIST, США:

1) **CRYSTALS-Dilithium (ML-DSA, FIPS-204)** – решетки, LWE и SIS.
2) **Falcon (FN-DSA)** – решетки. NTRU и быстрое преобразование Фурье. Константное выполнение операций, операции с плавающей точкой.
3) **SPHINCS+ (SLH-DSA, FIPS-205)** – хэш-функции. Гипердерево, без сохранения состояния.

ТК 26, Россия:

1) **Гиперикум** - хэш-функции. Модификация SPHINCS+ с оптимизациями на разных этапах. Использует Стрибог-256.
2) **Шиповник** - коды. Преобразование Фиата-Шамира к протоколу идентификации Штерна, Стрибог-512.

Цель и задачи

Цель работы – изучение и сравнительный анализ постквантовых криптографических алгоритмов цифровой подписи. Программная имплементация собственных модификаций этих алгоритмов.

Задачи:

1) **Изучение постквантовых алгоритмов ЭЦП**
2) **Разработка модели сравнения алгоритмов**
3) **Программная имплементация собственных модификаций**
4) **Проведение сравнительного анализа**

Проведенная работа

1) Реализация “Гиперикума” на SHA2 и SHA3
2) Реализация “Шиповника” на SHA2
3) Сравнительный анализ в собственной модели сравнения в равных условиях
4) Рассмотрение главных проблем
5) Выступление на конференции

Репозиторий с программной реализацией

Сравнительный анализ

1) 3 конфигурации **ML-DSA**
2) 2 конфигурации **Falcon**
3) 12 конфигураций **SLH-DSA**
4) 3 конфигурации **Гиперикума** (SHA2 и SHA3 реализованы автором)
5) 2 конфигурации **Шиповника** (SHA2 реализована автором)

Сравнительный анализ: длина ключей и подписи, категория безопасности NIST

Алгоритм	Длина открытого ключа, байт	Длина подписи, байт	Категория безопасности NIST
ML-DSA-44	1312	2420	2
ML-DSA-65	1952	3309	3
ML-DSA-87	2592	4627	5
Falcon-512	897	666	1
Falcon-1024	1793	1280	5
SLH-DSA-SHA2-128s SLH-DSA-SHAKE-128s	32	7 856	1
SLH-DSA-SHA2-128f SLH-DSA-SHAKE-128f	32	17 088	1
SLH-DSA-SHA2-192s SLH-DSA-SHAKE-192s	48	16 224	3

Алгоритм	Длина открытого ключа, байт	Длина подписи, байт	Категория безопасности NIST
SLH-DSA-SHA2-192f SLH-DSA-SHAKE-192f	48	35 664	3
SLH-DSA-SHA2-256s SLH-DSA-SHAKE-256s	64	29 792	5
SLH-DSA-SHA2-256f SLH-DSA-SHAKE-256f	64	49 856	5
Гиперикум по-умолчанию	64	28 068	5
Гиперикум быстр. подпись	64	58 460	5
Гиперикум мал. подпись	64	18 292	5
Шиповник	181	671026	1

Сравнительный анализ: скорость генерации ключей, подписи и проверки подписи

Алгоритм	ГК, мс	ГП, мс	ПП, мс
ML-DSA-44	0.12	0.55	0.14
ML-DSA-65	0.23	0.94	0.23
ML-DSA-87	0.35	1.14	0.37
Falcon-512	24.17	6.43	0.03
Falcon-1024	65.32	14.92	0.07
SLH-DSA-SHA2-128s	257.41	1945.297	1.81
SLH-DSA-SHAKE-128s	389.69	2886.708	2.77
SLH-DSA-SHA2-128f	7.02	109.532	5.766
SLH-DSA-SHAKE-128f	5.47	133.139	7.787

Алгоритм	ГК, мс	ГП, мс	ПП, мс
SLH-DSA-SHA2-192s	380.79	3562.826	3.696
SLH-DSA-SHAKE-192s	555.41	4958.737	4.44
SLH-DSA-SHA2-192f	10	206.239	8.565
SLH-DSA-SHAKE-192f	8.11	228.546	11.389
SLH-DSA-SHA2-256s	567.99	5019.726	5.46
SLH-DSA-SHAKE-256s	352.88	4058.402	6.216
SLH-DSA-SHA2-256f	21.99	414.546	11.778
SLH-DSA-SHAKE-256f	22.07	435.172	11.576
Гиперикум по-умолчанию (Стрибог)	2998.34	51410.16	38.65

Алгоритм	ГК, мс	ГП, мс	ПП, мс
Гиперикум быстр. подпись (Стрибог)	90.54	3478.13	119.87
Гиперикум мал. подпись (Стрибог)	1509907.48	6371005.79	37.62
Шиповник (Стрибог)	1.46	242.42	42.95
Гиперикум по-умолчанию (SHA2)	167.87	2457.56	1.69
Гиперикум быстр. подпись (SHA2)	4.25	151.91	6.24
Гиперикум мал. подпись (SHA2)	66913.72	282767.90	1.01
Шиповник (SHA2)	1.41	211.42	29.13
Гиперикум по-умолчанию (SHAKE)	385.03	6459.60	4.96
Гиперикум быстр. подпись (SHAKE)	24.43	460.66	13.67

Модель сравнения алгоритмов

Для сравнения алгоритмов используем таблицы выше. Выведем из всех столбцов единый показатель – финальный показатель эффективности (ФПЭ). Для этого нормализуем значения ГК, ГП, ПП, ПК и подписи в логарифмическом виде, а КБ - в линейном.

$$X_{\text{норм}} = 1 - \frac{lg(X) - lg(X_{min})}{lg(X_{max}) - lg(X_{min})}$$

$$\text{КБ}_{\text{норм}} = \frac{\text{КБ} - 1}{4}$$

$$\text{ФПЭ} = 0.1 * \text{ГК}_{\text{норм}} + 0.15 * \text{ГП}_{\text{норм}} + 0.15 * \text{ПП}_{\text{норм}} + 0.15 * \text{ПК}_{\text{норм}} + 0.15 * \text{Подпись}_{\text{норм}} + 0.3 * \text{КБ}_{\text{норм}}$$

Весовые коэффициенты расставлены таким образом, что скорость генерации ключей (ГК) имеет наименьшее значение, так как она происходит только один раз. Несколько большее влияние имеет категория безопасности NIST (КБ).

Все остальные показатели поделили веса поровну, за исключением генерации ключей (ГК).

ТОП алгоритмов по ФПЭ

№	Алгоритм	ФПЭ
1	Falcon-1024	**0.7645**
2	ML-DSA-87	**0.75**
3	Гиперикум быст. подпись (SHA2)	**0.708**
4	Гиперикум по-умолчанию (SHA2)	**0.6995**
5	SLH-DSA-SHAKE-256f	**0.6815**
6	SLH-DSA-SHA2-256f	**0.6815**
7	Гиперикум быст. подпись (SHAKE)	**0.673**
8	Гиперикум по-умолчанию (SHAKE)	**0.666**
9	SLH-DSA-SHAKE-256s	**0.666**

№	Алгоритм	ФПЭ
10	Гиперикум мал подпись (SHA2)	**0.6385**
11	ML-DSA-65	**0.6285**
12	Гиперикум быст. подпись (Стрибог)	**0.6065**
13	Гиперикум мал подпись (SHAKE)	**0.603**
14	Гиперикум по-умолчанию (Стрибог)	**0.599**
15	ML-DSA-44	**0.5905**
16	SLH-DSA-SHA2-192f	**0.5665**
17	SLH-DSA-SHAKE-192f	**0.56**
18	SLH-DSA-SHA2-192s	**0.5505**

№	Алгоритм	ФПЭ
19	SLH-DSA-SHAKE-192s	**0.5415**
20	Falcon-512	**0.5315**
21	Гиперикум мал подпись (Стрибог)	**0.525**
22	SLH-DSA-SHA2-256s	**0.513**
23	SLH-DSA-SHA2-128f	**0.4605**
24	SLH-DSA-SHAKE-128f	**0.455**
25	SLH-DSA-SHA2-128s	**0.4505**
26	SLH-DSA-SHAKE-128s	**0.435**
27	Шиповник (SHA2)	**0.2965**
28	Шиповник (Стрибог)	**0.289**

Главные проблемы

1) Падение производительности

2) Трудности перехода и интеграции

3) Прикладная неисследованность

4) Неопределенность

Главные проблемы – падение производительности

Размеры ключей и подписи постквантовых алгоритмов намного больше классических.

Больше всего пострадает TLS.

Главные проблемы – трудности перехода и интеграции

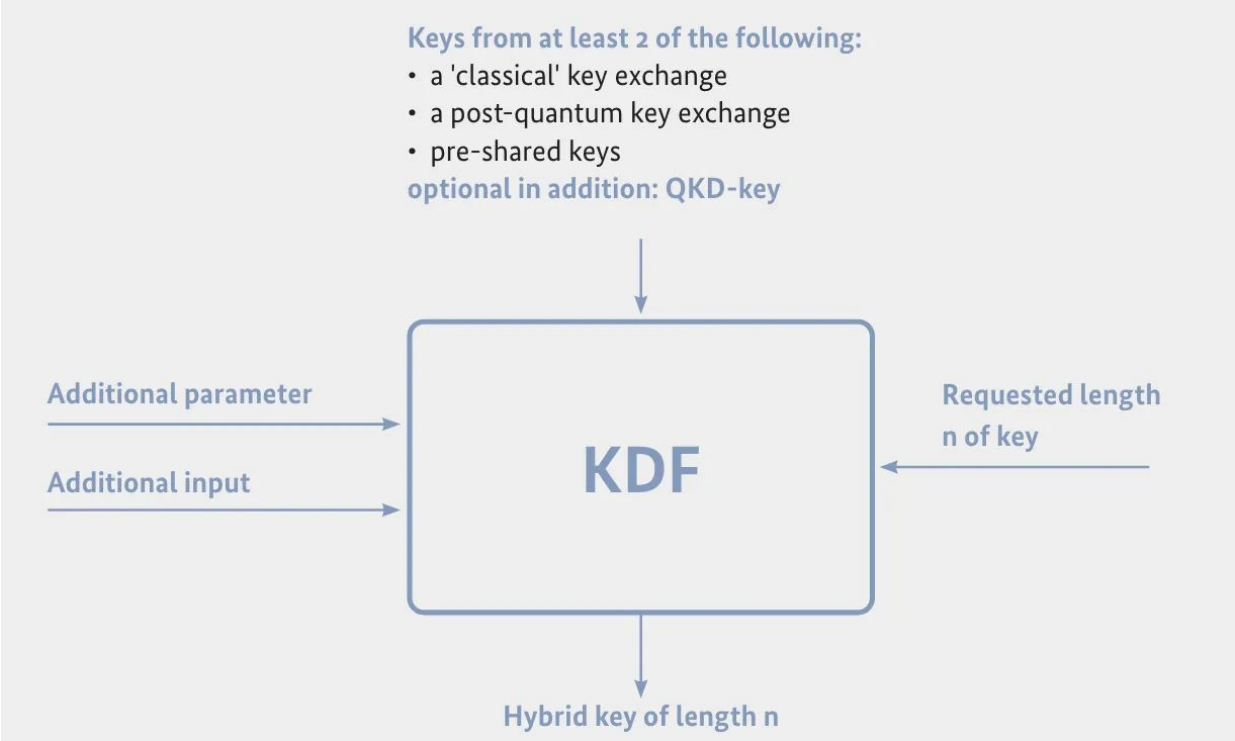
Атаки типа **“Harvest Now, Decrypt Later”** заставляют переходить на постквантовые схемы уже сейчас.

Переходы на новые схемы уже были, но их математический базис был схожий.

Логичным началом перехода являются **гибридные схемы** – объединение классических и постквантовых алгоритмов.

Композитный гибрид

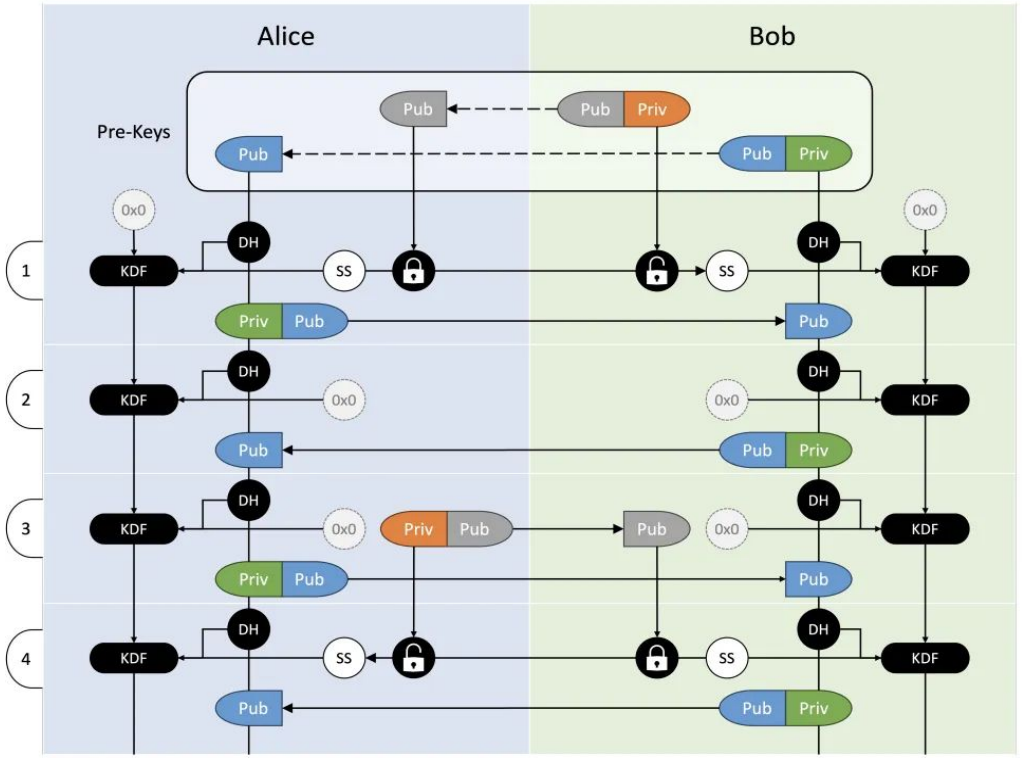
Композитный вариант является сложным в реализации и дальнейшем изменении, но остается надежным вариантом, который позволяет использовать преимущества обоих алгоритмов.



Многоуровневый гибрид

Многоуровневый или двойной гибрид позволяет сделать “обертку” над классическим алгоритмом, что позволяет изменить обе схемы на другие.

Часть с постквантовой схемой выделена оранжевым цветом.



Совместимый гибрид

Совместимый гибрид используется в случае, когда нет уверенности в том, что другая сторона поддерживает постквантовые схемы.

Такой подход используется в TLS 1.3 в браузере Chrome для создания сеансового ключа.

Главные проблемы – прикладная неисследованность

Математический базис был придуман давно, схемы хорошо исследованы теоретически.

Но не практически.

Действенные атаки находятся в процессе массового использования, например, “20 лет атак на RSA”.

Из этих соображений третьим финалистом стал SPHINCS+ – как альтернатива на случай уязвимости в решетках.

Главные проблемы – неопределенность

На сегодняшний день не существует общеизвестных квантовых компьютеров, которые смогут взломать стойкие классические ассиметричные алгоритмы, но есть еще и неизвестные мощности, про которые общество может узнать только после их неудачного применения. В работе NIST “Getting Ready for Post-Quantum Cryptography” говорится:

“***We cannot accurately predict when a quantum computer capable of executing Shor’s algorithm will be available to adversaries, but we need to be prepared for it as many years in advance as is practical***”.

Это буквально можно трактовать так, что никто не знает, когда у желающих рассекретить ваши каналы связи появится для этого техническая возможность, поэтому следует оберегать себя от угрозы настолько заранее, насколько это возможно.

Что в области будет дальше?

1) Стандартизация Falcon в FIPS-206
2) Гиперикум 2.0
3) ЭЦП на решетках “Облепиха”
4) KEM на решетках “Земляника”
5) …

Литература

1. ISO/IEC 14888-1:2008 [электронный ресурс] - 2008 - URL: https://www.iso.org/ru/standard/44226.html (дата обращения 11.11.2024)
2. "Post-Quantum Cryptography Standardization – Post-Quantum Cryptography". *Csrc.nist.gov*. 3 January 2017. Retrieved 31 January 2019
3. Проект РГ 2.5 “Постквантовые криптографические системы” Технического комитета ТК26 “Криптографическая защита информации”
4. Shor, P.W. (1994). "Algorithms for quantum computation: Discrete logarithms and factoring". *Proceedings 35th Annual Symposium on Foundations of Computer Science*. pp. 124–134.
5. Regev, Oded (2023). "An Efficient Quantum Factoring Algorithm"
6. Grover, Lov K. (1996-07-01). "A fast quantum mechanical algorithm for database search". *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*. Philadelphia, Pennsylvania, USA: Association for Computing Machinery. pp. 212–219.
7. FIPS-204, NIST - 2023 - URL: https://csrc.nist.gov/pubs/fips/204/final (дата обращения 12.12.2024)
8. FIPS-205, NIST - 2024 - URL: https://csrc.nist.gov/pubs/fips/205/final (дата обращения 12.12.2024)
9. FIPS-203, NIST - 2024 - URL: https://csrc.nist.gov/pubs/fips/203/final (дата обращения 12.12.2024)
10. Lyubashevsky V (2009) Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. Advances in Cryptology – ASIACRYPT 2009, ed Matsui M (Springer Berlin Heidelberg, Berlin, Heidelberg), pp 598–616. https://doi.org/10.1007/978-3-642-10366-7_35
11. Комарова А.В.2 , Коробейников А.Г (2019) АНАЛИЗ ОСНОВНЫХ СУЩЕСТВУЮЩИХ ПОСТ-КВАНТОВЫХ ПОДХОДОВ И СХЕМ ЭЛЕКТРОННОЙ ПОДПИСИ, DOI: 10.21681/2311-3456-2019-2-58-68
12. Falcon - 2024 - URL: https://falcon-sign.info/ (дата обращения 13.12.2024)
13. Иваненко В. Г., Иванова И. Д., Иванова Н. Д. (2024) ВЫЧИСЛЕНИЯ НАД ПОЛИНОМАМИ В ПОСТКВАНТОВЫХ СХЕМАХ ПОДПИСИ, DOI: 10.21681/2311-3456-2024-4-65-70
14. Andreas Hülsing, Mikhail Kudinov, Eyal Ronen, Eylon Yogev – SPHINCS+C Compressing SPHINCS+ With (Almost) No Cost – URL: https://csrc.nist.gov/csrc/media/Presentations/2022/sphincsc-compressing-sphincs-with-almost-no-cost/images-media/session-1-ronen-compressing-sphincs-plus-no-cost-pqc2022.pdf (дата обращения 15.12.2024)
15. О. Ю. Турченко, С. Р. Усманов – АНАЛИЗ ПАРАМЕТРОВ ПОСТКВАНТОВОЙ СХЕМЫ ПОДПИСИ ГИПЕРИКУМ, DOI 10.17223/2226308X/17/28
16. Victoria Vysotskaya and Ivan Chizhov – The security of the code-based signature scheme based on the Stern identification protocol – URL: https://eprint.iacr.org/2021/1075.pdf (дата обращения 17.12.2024)
17. Виктория Высоцкая, Диана Дас – Анализ устойчивости постквантовой электронной подписи «Шиповник» к атакам, нацеленным на хэш-функции – URL: https://ruscrypto.ru/resource/archive/rc2024/files/05_vysotskaya_das.pdf (дата обращения 17.12.2024)
18. Шиповник ТК26, QAppTech, программная реализация – URL: https://github.com/QAPP-tech/shipovnik_tc26/tree/master (дата обращения 17.12.2024)
19. iMessage with PQ3: The new state of the art in quantum-secure messaging at scale – URL: https://security.apple.com/blog/imessage-pq3/ (дата обращения 01.04.2025)
20. Protecting Chrome Traffic with Hybrid Kyber KEM – URL: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html (дата обращения: 01.04.2025)
21. *Boneh D.* Twenty Years of attacks on the RSA Cryptosystem (англ.) // *Notices of the American Mathematical Society* / F. Morgan — AMS, 1999. — Vol. 46, Iss. 2. — P. 203–213. — ISSN 0002-9920; 1088-9477
22. William Barker, William Polk, Murugiah Souppaya – Getting Ready for Post-Quantum Cryptography – 2021 – P. 6
23. Репозиторий с исходным кодом исследовательского проекта - 2024 - URL: https://gitlab.com/ruhakachmaz/comparison-of-post-quantum-digital-signature-algorithms (дата обращения 25.03.2024)


ВЫСШАЯ • ШКОЛА • ЭКОНОМИКИ •