РусКрипто XXVIII научно-практическая конференция

КуАпп

Компания Актив

Оптимизация ресурсоёмкости алгоритма «Гиперикум» при реализации в устройствах с ограниченными ресурсами

Олег Турченко

Старший исследователь «КуАпп»

Кандидат технических наук

Сергей Панасенко

Директор по научной работе Компании «Актив»

Кандидат технических наук

Применение постквантовых алгоритмов в низкоресурсных устройствах

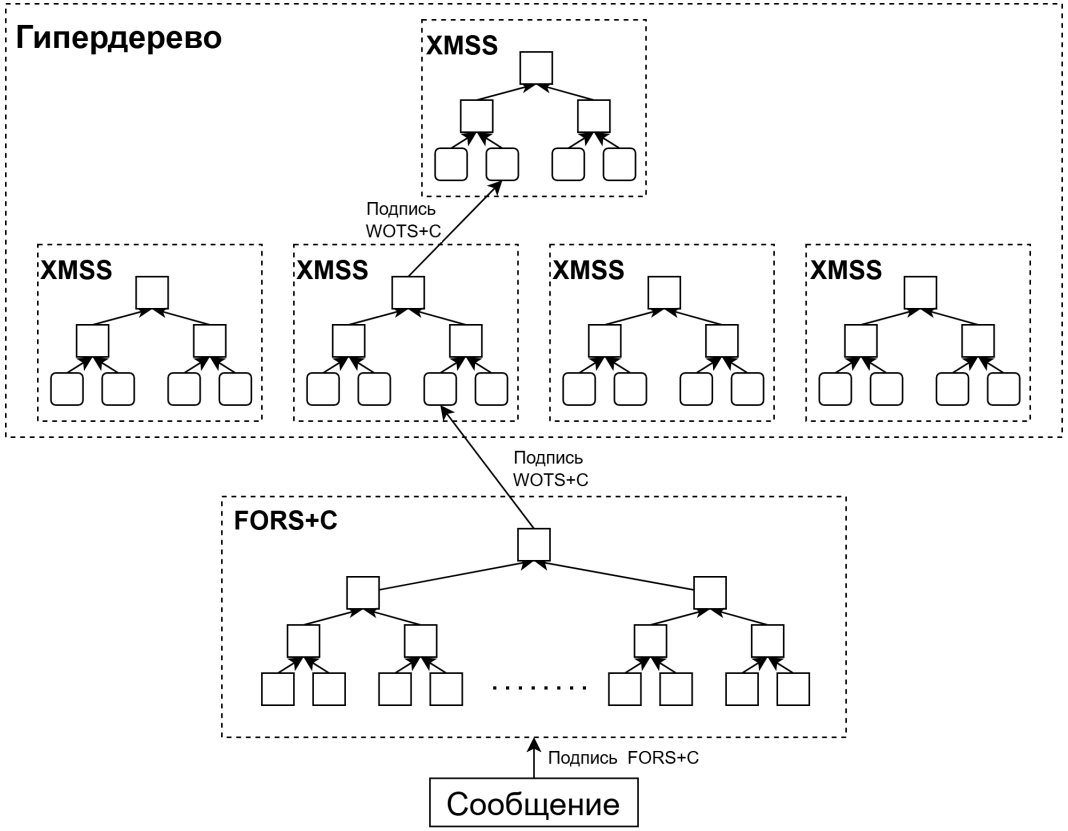
Одним из востребованных применений постквантовых ЭЦП является их применение в низкоресурсных устройствах (например, смарт-карты, сенсоры интернета вещей и т. п.)

Наиболее критичными ограничениями для реализации в таких устройствах постквантовых ЭЦП можно считать следующие:

- ограниченность ресурсов используемого в устройстве вычислителя и его энергопотребление
- ограниченная полоса пропускания канала связи с устройством

Рассмотрим возможность реализации постквантового алгоритма ЭЦП «Гиперикум» с учетом вышеописанных ограничений

Схема ЭЦП «Гиперикум»



Параметры схемы «Гиперикум»

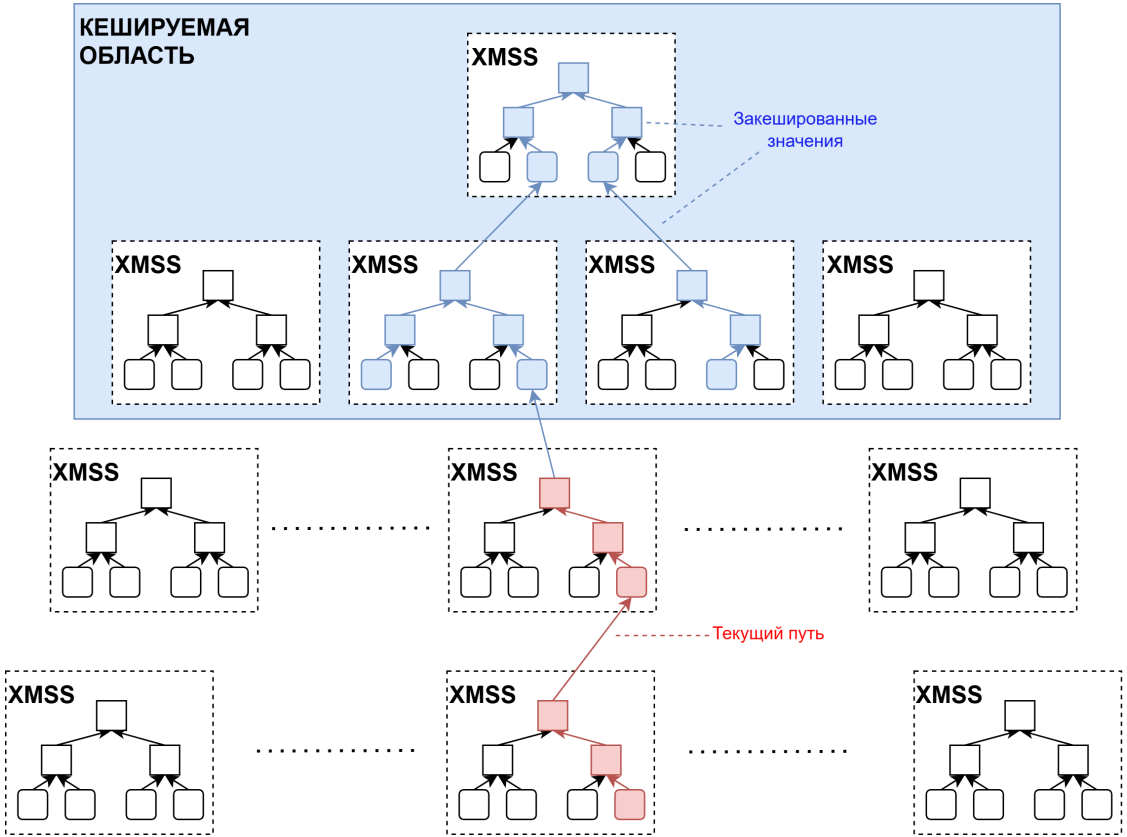
РусКрипто XXVIII научно-практическая конференция

КуАпп

Название	h	d	b	k	Подпись, Б	H для под.	H для пров.
Гиперикум_Б_256_64	66	22	9	38	59 132	220 309	11 663
Гиперикум_М_256_64	68	4	18	15	18 932	544 997 215	2368
Гиперикум_Б_256_20	21	7	10	36	27 392	130 233	3955
Гиперикум_М_256_20	26	2	18	15	13 484	24 395 435	1302
Гиперикум_Б_128_20	20	5	9	18	16 376 (8188)[1]	99 864	2733
Гиперикум_М_128_20	20	2	11	14	9772 (4886)[1]	2 154 158	1187

[1] При использовании хэш-функции «Стрибог» с длиной выхода 128 бит

Кеширование деревьев



Кеширование является стандартным подходом для снижения вычислений в схемах на основе хэш-функций

Недостатки кеширования

Основная проблема при применении кеширования — высокая нагрузка на память и отсутствие влияния на пропускную способность интерфейса передачи

Например, на типовых смарт-картах суммарный объем памяти не превышает 500 КБ, из которых пользователю доступно менее 150 КБ. Это позволит кешировать лишь 1-2 уровня гипердерева и не даст ощутимого прироста

Решение — перенести кеширование с низкоресурсного устройства (формирования подписи) на управляющее устройство (проверки подписи)

Предлагаемая реализация

1. Низкоресурсное устройство вычисляет рандомизирующую часть ЭП R и промежуточное значение s и отправляет их на управляющее устройство
2. Управляющее устройство на основе значений M, R и s определяет путь в гипердереве и производит поиск ветвей в своем кеше. После этого управляющее устройство отправляет команду завершить вычисление ЭП, содержащую признак наличия или отсутствия ветвей в кеше
3. Низкоресурсное устройство вычисляет оставшуюся часть ЭП целиком или до указанного уровня гипердерева в зависимости от отсутствия или наличия части требуемых ветвей гипердерева в кеше управляющего устройства

Замечание: вычисление подписи на управляющее устройство не делегируется

Оценка эффективности кеширования

РусКрипто XXVIII научно-практическая конференция

КуАпп

Кеширование подписи для параметров Гиперикум_Б_256_64

Уровень	Размер кеша, Б	Снижение размера подписи, Б	Снижение времени подписи, Н	Снижение размера подписи, %	Снижение времени подписи, %
1	16 608	2112	7777	3	3
2	147 904	4224	15 554	7	7
3	1 196 704	6336	23 331	10	10
4	9 585 536	8448	31 108	14	14
5	76 694 624	10 560	38 885	17	17
6	613 565 760	12 672	46 662	21	21
7	4 908 533 280	14 784	54 439	25	24

Снижение размера и времени подписи указывают на сколько подпись стала короче или быстрее (в хэшах)

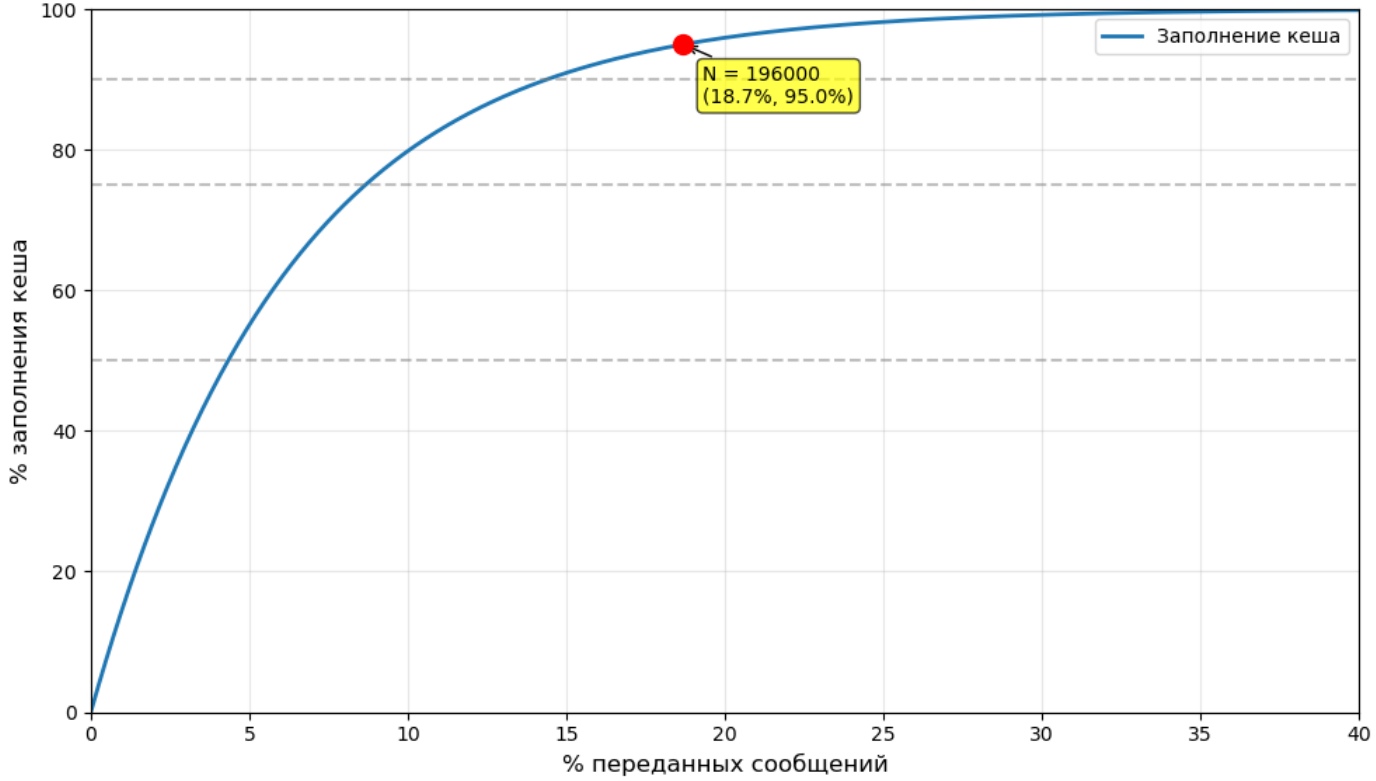
Оценка эффективности кеширования

Кеширование подписи для параметров Гиперикум_Б_128_20

Уровень	Размер кеша, Б	Снижение размера подписи, Б	Снижение времени подписи, Н	Снижение размера подписи, %	Снижение времени подписи, %
1	33 248	2144	15 976	13	15
2	558 016	4288	31 952	26	31
3	8 947 104	6432	47 928	39	47
4	143 165 312	8576	63 904	52	63

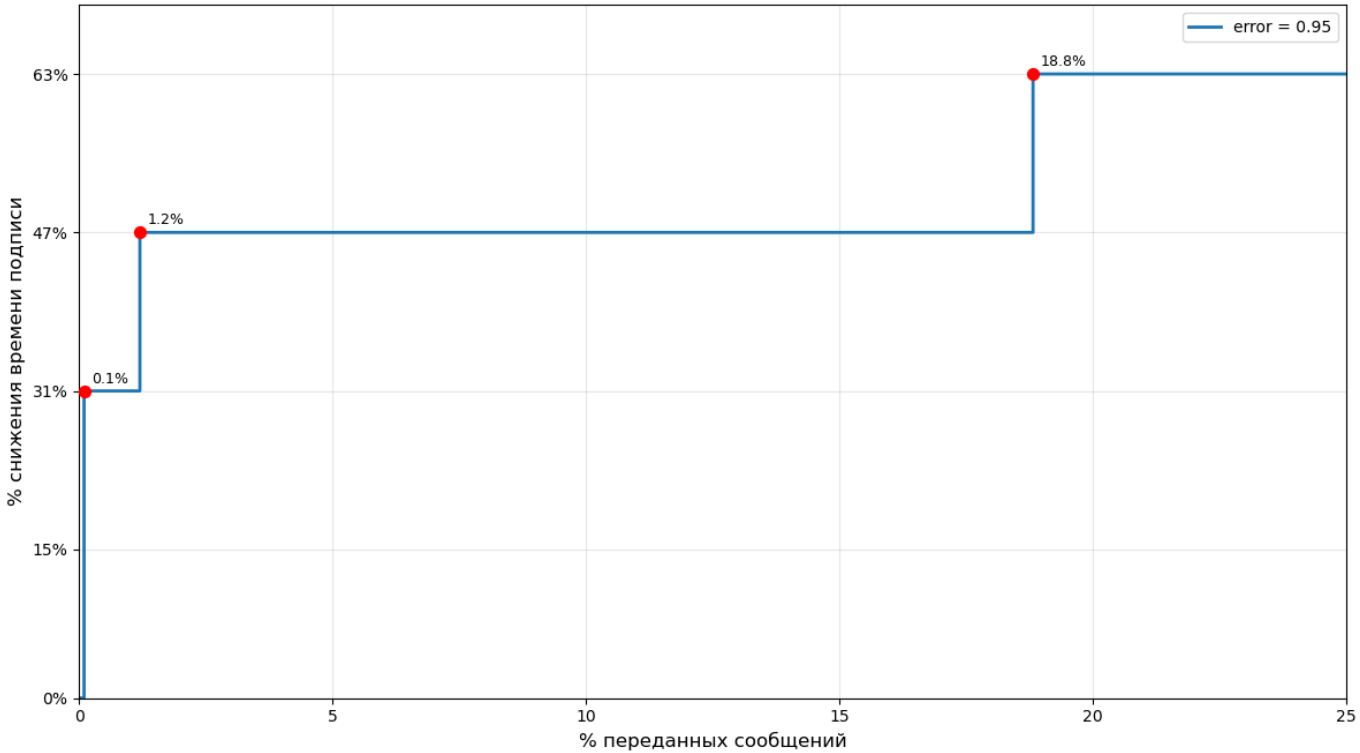
Снижение размера и времени подписи указывают на сколько подпись стала короче или быстрее (в хэшах)

Скорость заполнения кеша для хранения 4 уровней гипердерева



Скорость заполнения кеша для набора параметров Гиперикум_Б_128_20

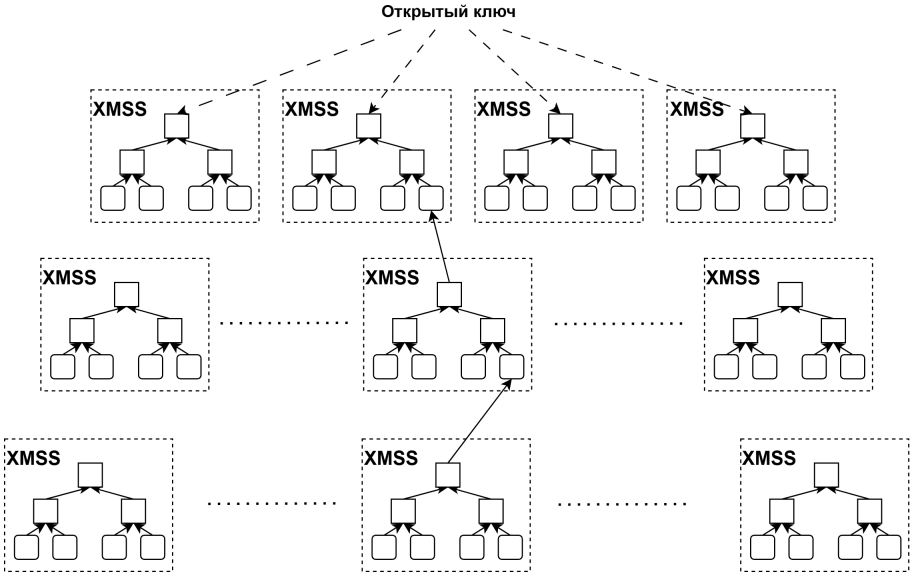
Зависимость ускорения от числа переданных подписей



Зависимость ускорения от числа подписей для набора параметров Гиперикум_Б_128_20

Альтернативный вариант

В литературе также встречается схожая идея, в которой открытым ключом является набор вершин деревьев на более низких уровнях. Таким образом, можно сократить размер и время вычисления подписи за счет увеличения размера открытого ключа



Сравнение подходов кеширования и расширения открытого ключа

РусКрипто XXVIII научно-практическая конференция

КуАпп

- Кеширование не требует добавление новых наборов параметров
- Состав ключей и подписи не изменяется

- Требуемый размер кеша превосходит размер увеличенного открытого ключа

Влияние на стойкость

- Накопление вычисленных частей подписи может осуществлять любой участник, но проводить вычисления может только участник, обладающий секретным ключом (низкоресурсное устройство)
- Атакующий также может накапливать переданные части подписи, но наличие этих частей не даёт преимуществ для проведения атак (если не превышен допустимый лимит числа подписей)
- Пассивный атакующий не получает дополнительной информации при использовании протокола относительно стандартного использования

Возможности активного атакующего

- Если атакующий выдает себя за подписывающего, то ему необходимо сформировать нижнюю часть гипердерева и подпись FORS. Для этого ему необходимо обладать секретным ключом, либо уметь формировать подделку для исходной схемы. В противном случае сформированная часть будет несогласованной с верхней и проверка подписи выдаст отрицательный ответ
- Если атакующий выдаёт себя за проверяющего, то он может выслать номер уровня, который ранее не передавался и не мог быть закеширован. В таком случае переданная подпись будет непроверяемой. Однако данная угроза не выглядит существенной для типового применения низкоресурсного устройства

Общие рекомендации по применению схемы «Гиперикум» в низкоресурсных устройствах

- Применение предложенного протокола позволяет сократить размер подписи и объём вычислений на треть при передаче около 1 000 сообщений — до 5 КБ и 60 000 хэшей соответственно
- Использование потоковой выдачи[1,2] позволяет существенно снизить необходимый объём памяти в низкоресурсном устройстве. В таком случае потребуется оперативная память для вычисления дерева — от 64 до 160 Б

[1] Панасенко, С. П. О ПРИМЕНИМОСТИ ПОСТКВАНТОВОГО СТАНДАРТА ЭЛЕКТРОННОЙ ПОДПИСИ SLH-DSA В СМАРТ-КАРТАХ / С. П. Панасенко // Вопросы кибербезопасности. – 2025. – № 3(67). – С. 29-37.
[2] Niederhagen, R., Roth, J., Walde, J. (2022). Streaming SPHINCS+ for Embedded Devices Using the Example of TPMs. In: Batina, L., Daemen, J. (eds) Progress in Cryptology - AFRICACRYPT 2022. AFRICACRYPT 2022. Lecture Notes in Computer Science, vol 13503. Springer, Cham.

Общие рекомендации по применению схемы «Гиперикум» в низкоресурсных устройствах

- Для применения вышеуказанных оптимизаций целесообразно использовать интерфейс с асинхронной выдачей
- Необходим переход на усовершенствованный протокол APDU для работы с потоковой передачей и добавлением управляющих сигналов (для передачи признака и закешированного уровня)

Важно отметить, что данные оптимизации применимы ко всем схемам на хэшах, в том числе к схемам с сохранением состояния, таким как XMSS и «Спартиум»

Спасибо за внимание!

РусКрипто XXVIII научно-практическая конференция

КуАпп

Компания Актив

Олег Турченко

Старший исследователь «КуАпп»

Кандидат технических наук

oturchenko@qapp.tech

@Oleg_Turchenko

qapp.tech

Сергей Панасенко

Директор по научной работе Компании «Актив»

Кандидат технических наук

panasenko@guardant.ru

aktiv-company.ru