2026 СТCRYPT

КуАпп

Анализ стойкости постквантовых хэш-подписей на основе композиции случайных отображений

Алексей Зеленецкий

Старший исследователь «КуАпп»

Старший преподаватель МГТУ им. Н.Э. Баумана

Олег Турченко

Старший исследователь «КуАпп»

Кандидат технических наук

qapp.tech

Sk Участник

НИЖЕГОРОДСКИЙ НОЦ

Московский инновационный кластер

Случайное отображение

КуАпп

Пусть

- $[N] = \{0, 1, \ldots, N-1\}$ — множество целых от 0 до $N-1$
- $\mathcal{F}_N = \{f : [N] \to [N]\}$ — множество всех отображений $[N]$ в себя

Случайное отображение

Случайное отображение F множества $\mathcal{F}_N$ — случайная величина, принимающая значения в множестве $\mathcal{F}_N$ и распределенная на нем равномерно:

$$1. \forall f \in \mathcal{F}_N \ \Pr[F = f] = N^{-N}$$

$$2. \forall x, y \in [N] \ \Pr[F(x) = y] = 1/N$$

Итерации случайного отображения

КуАпп

k-ая итерация случайного отображения

Пусть $k \geq 1$, а F — случайное отображение n-множества $\mathcal{F}_N$. Под его k-ой итерацией понимается случайная величина $F^{(k)} = F(F^{(k-1)})$, где $F^{(1)} = F$.

- Применяются при оценке стойкости криптографических хэш-функций
- Получено множество различных результатов

Некоторые известные результаты об итерации случайного отображения

КуАпп

Пусть $F([N])$ обозначает множество образов отображения $F \in \mathcal{F}_N$, тогда

- При $N \to \infty$

$$E\left[\#F^{(k)}([N])\right] = (1 - \tau_k) \cdot N,$$

  где $\tau_0 = 0$, а $\tau_{k+1} = e^{-1+\tau_k}$
- При $N \to \infty$ и $k \leq \sqrt{N}$

$$E\left[\#F^{(k)}([N])\right] \approx 2^{N-\log_2(k)+1} = \frac{2}{k} \cdot 2^N$$

- Пусть $y \leftarrow F^{(k)}([N])$, тогда

$$E\left[\#\{x \in [N] : F^{(k)}(x) = y\}\right] \geq k$$

Композиция случайных отображений

КуАпп

Композиция k случайных отображений

Пусть $k \in \mathbb{N}$ и $F_1, F_2, \ldots, F_k$ - независимые случайные отображения множества $\mathcal{F}_N$. Под композицией k случайных отображений будем понимать случайную величину

$$G_k = F_k \circ F_{k-1} \circ \cdots \circ F_1.$$

- Могут быть использованы при анализе стойкости постквантовых криптосистем
- Изучены хуже, чем итерации случайного отображения

Некоторые известные результаты о композиции случайных отображений

КуАпп

- Результаты А.М. Зубкова и А.А. Серова о $E[\#G_k(S)]$, где $S \subseteq [N]$.
  Однако точность оценки существенно падает при приближении $\#S$ к N
- При $N = 2^n$ и $k = 2^s \leq N/2$

$$\#G_k([N]) \leq \tilde{O}(2^{n-s})$$

- Пусть T — случайная величина, равная наименьшему k, при котором $G_k(\cdot)$ имеет ровно один образ, тогда при $N \to \infty$

$$E[T] \sim 2N$$

Полученные результаты о композиции случайных отображений

КуАпп

1. Рекуррентная оценка сверху математического ожидания мощности образа композиции k случайных отображений — $E[\#G_k([N])]$
2. Асимптотическая (не рекуррентная) оценка сверху $E[\#G_k([N])]$
3. Асимптотическая (не рекуррентная) оценка снизу математического ожидания среднего числа прообразов элемента образа $G_k(\cdot)$

Рекуррентная оценка сверху $E[\#G_k([N])]$

КуАпп

- Пусть m_i — случайная величина, равная мощности образа композиции i случайных отображений — $m_i = \#G_i([N])$
- Пусть $x_i = E[m_i]/N$. Будем считать, что $x_0 = 1$, тогда

$$x_i \leq 1 - \left(\left(1 - \frac{1}{N}\right)^N\right)^{x_{i-1}}$$

- При $N \to \infty$ последнее можно записать в виде

$$x_i \leq 1 - e^{-x_{i-1}}$$

- Из-за возрастания функций в обоих видах оценки вместо x_{i-1} можно подставить его оценку сверху и т. д.

Асимптотическая не рекуррентная оценка сверху $E[\#G_k([N])]$

Теорема 1

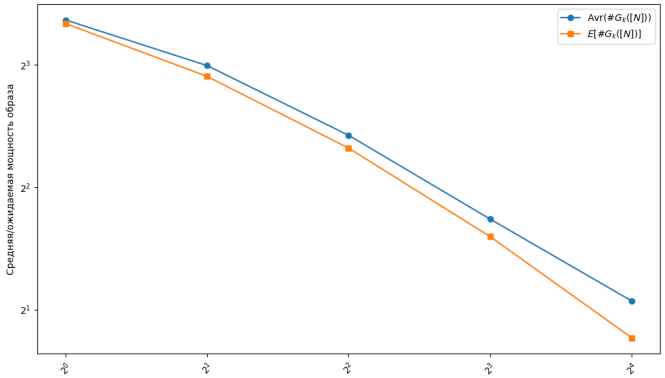
Пусть $G_k = F_k \circ F_{k-1} \circ \cdots \circ F_1$ — композиция $k \geq 1$ независимых случайных отображений множества $\mathcal{F}_N$. Обозначим за $x_k = \frac{E[\#G_k([N])]}{N}$ отношение математического ожидания мощности образа G_k к N.

Тогда при $N \to \infty$ справедливо

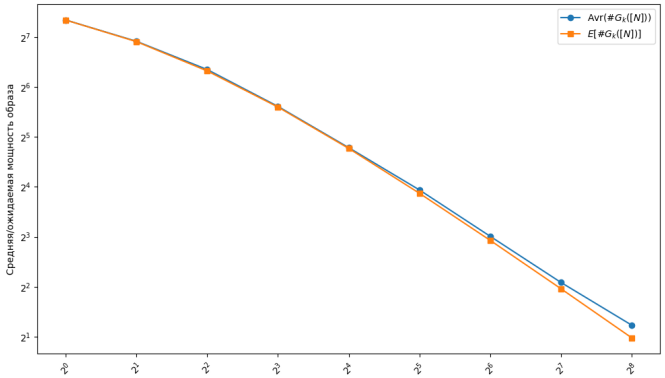
$$x_k \leq \frac{2}{2+k}.$$

- Теорема 1 в полной мере соответствует ранее известным результатам

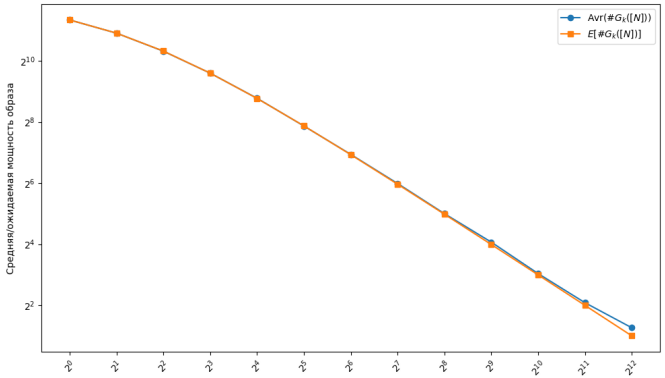
Эмпирические данные



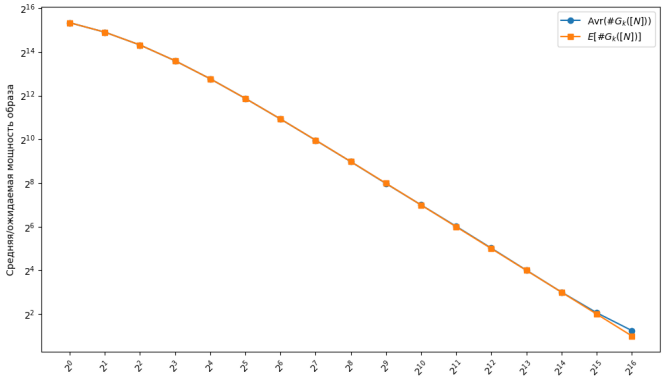
$N = {}^{k} 2^4$



$N = {}^{k} 2^8$



$N = {}^{k} 2^{12}$

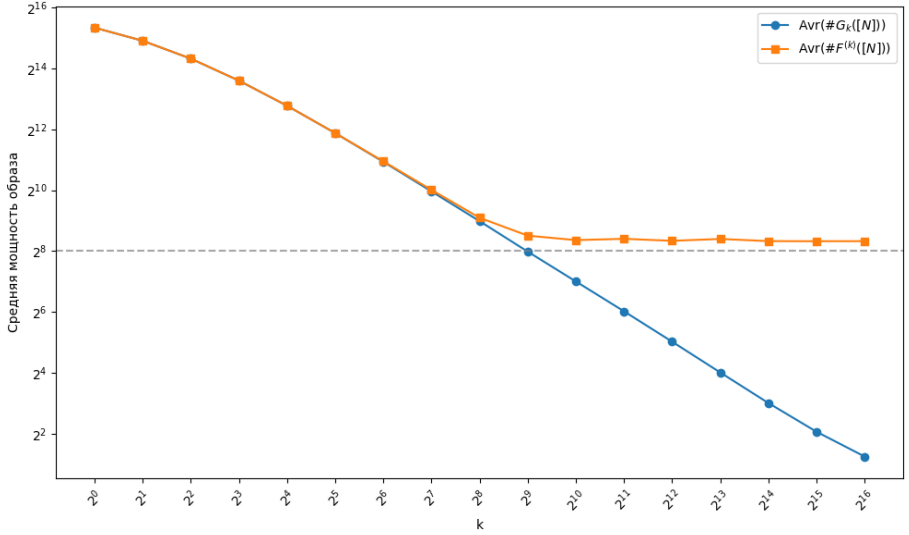


$N = {}^{k} 2^{16}$

Зависимости средней мощности $G_k([N])$ и $E[\#G_k([N])]$ от k для 100 независимых $G_k(\cdot)$

Отличие от k-ой итерации случайного отображения

- Значения средних мощностей образов $G_k(\cdot)$ и $F^{(k)}(\cdot)$ убывают с ростом k по одному закону вплоть до $k = \Theta(\sqrt{N})$
- При $k = \Omega(\sqrt{N})$ мощность образа $F^{(k)}(\cdot)$ асимптотически стремится к $\sqrt{\pi N/2}$ (известный результат)
- Мощность образа $G_k(\cdot)$ продолжает убывать, пока не станет равной 1



Зависимости средней мощности $G_k([N])$ и $F^{(k)}([N])$ от k при $N = 2^{16}$

Оценка математического ожидания среднего числа прообразов элемента образа $G_k(\cdot)$

КуАпп

- Пусть $g \in \mathcal{F}_N$ и $y \in g([N])$, введем обозначение

$$\text{Pre}(y) = \{x \in [N] : g(x) = y\}$$

- Под **средним числом прообразов элемента образа** g будем понимать

$$A(g) = E[\#\text{Pre}(y)], \text{ где } y \leftarrow g([N])$$

- Для композиции k случайных отображений G_k значение $A(G_k)$ будет случайной величиной
- Получена оценка снизу для математического ожидания $A(G_k)$

Оценка математического ожидания среднего числа прообразов элемента образа $G_k(\cdot)$

КуАпп

Теорема 2

Пусть $g \in \mathcal{F}_N$, а $A(g) = E[\#\text{Pre}(y)]$, где y выбран случайно и равномерно из образа g. Пусть также $G_k = F_k \circ F_{k-1} \circ \cdots \circ F_1$ — композиция $k \geq 1$ независимых случайных отображений множества $\mathcal{F}_N$. Тогда при $N \to \infty$

$$E[A(G_k)] \geq \frac{k+2}{2}.$$

- **Интерпретация оценки**: Для случайного элемента образа $G_k(\cdot)$ в среднем ожидается не менее $(k+2)/2$ прообразов

Рассмотрение хэш-функций как случайных отображений

КуАпп

- Для современных стандартизированных хэш-функций не существует эффективных различителей, способных отличить выход хэш-функции со случайным входом от случайного отображения
- Дополнительным аргументом является результат работы [1], согласно которому, если используемый внутри хэш-функции «Стрибог» шифр E является идеальным, а вычислительные возможности атакующего значительно меньше, чем $\approx 2^{252}$, то для коротких сообщений данная хэш-функция неотличима от случайного оракула

[1] Akhmetzyanova L. R., Babueva A., Bozhko A. Streebog as a Random Oracle. IACR Cryptol. ePrint Arch. 2023

Важные свойства случайного отображения

КуАпп

Пусть $f : X \to Y$ — случайное отображение и $X = X_1 \times X_2 \times X_3$.

Пусть отображение $g : X_2 \to Y$ имеет вид $g_{x_1,x_3}(x) = f(x_1, x, x_3)$ для некоторых $x_1 \in X_1, x_3 \in X_3$.

Тогда справедливы следующие утверждения:

- $g_{x_1,x_3}(x)$ — случайное отображение
- $g_{x_1,x_3}(x)$ и $g_{x'_1,x'_3}(x)$ — являются независимыми случайными отображениями для любых таких $x_1, x'_1 \in X_1;\ x_3, x'_3 \in X_3$, что $(x_1, x_3) \neq (x'_1, x'_3)$

Схема WOTS+

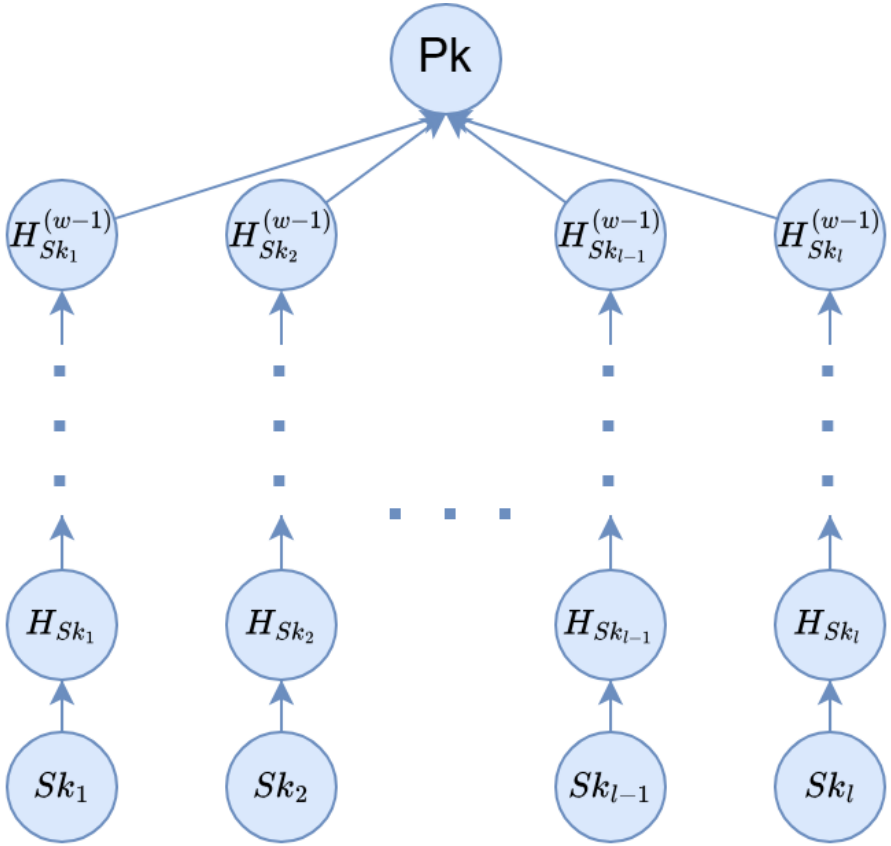


Схема WOTS+

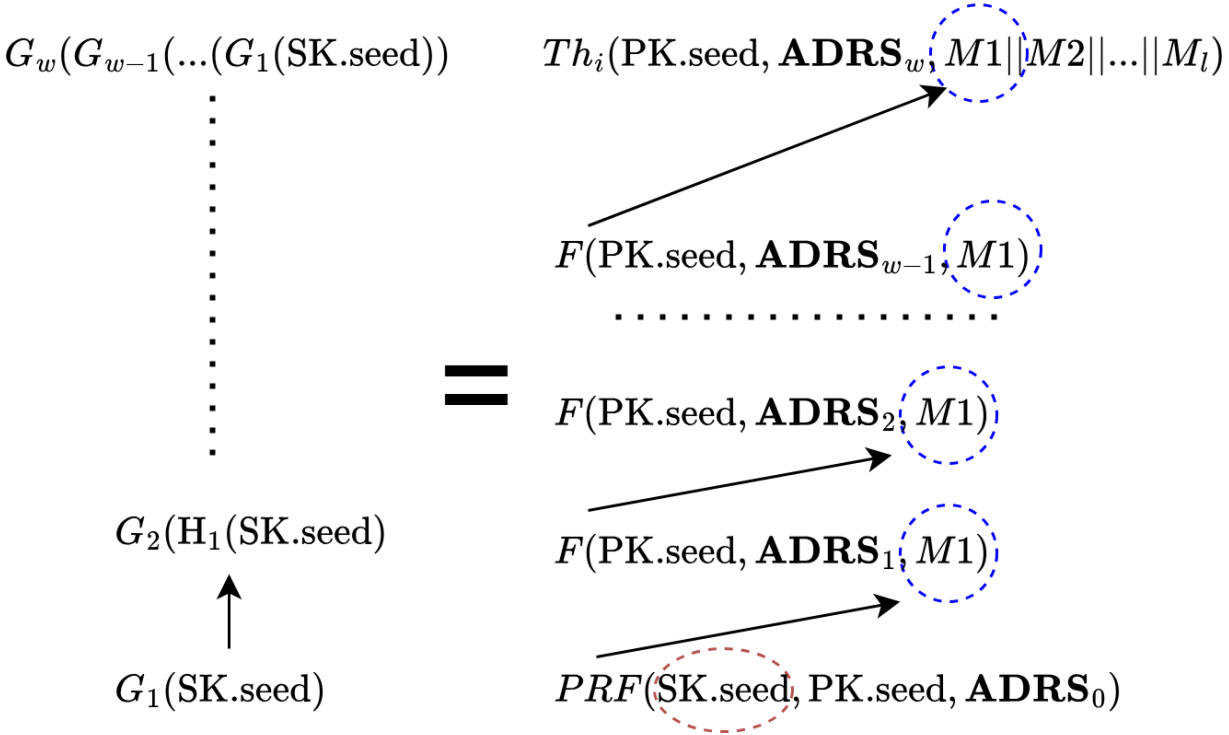
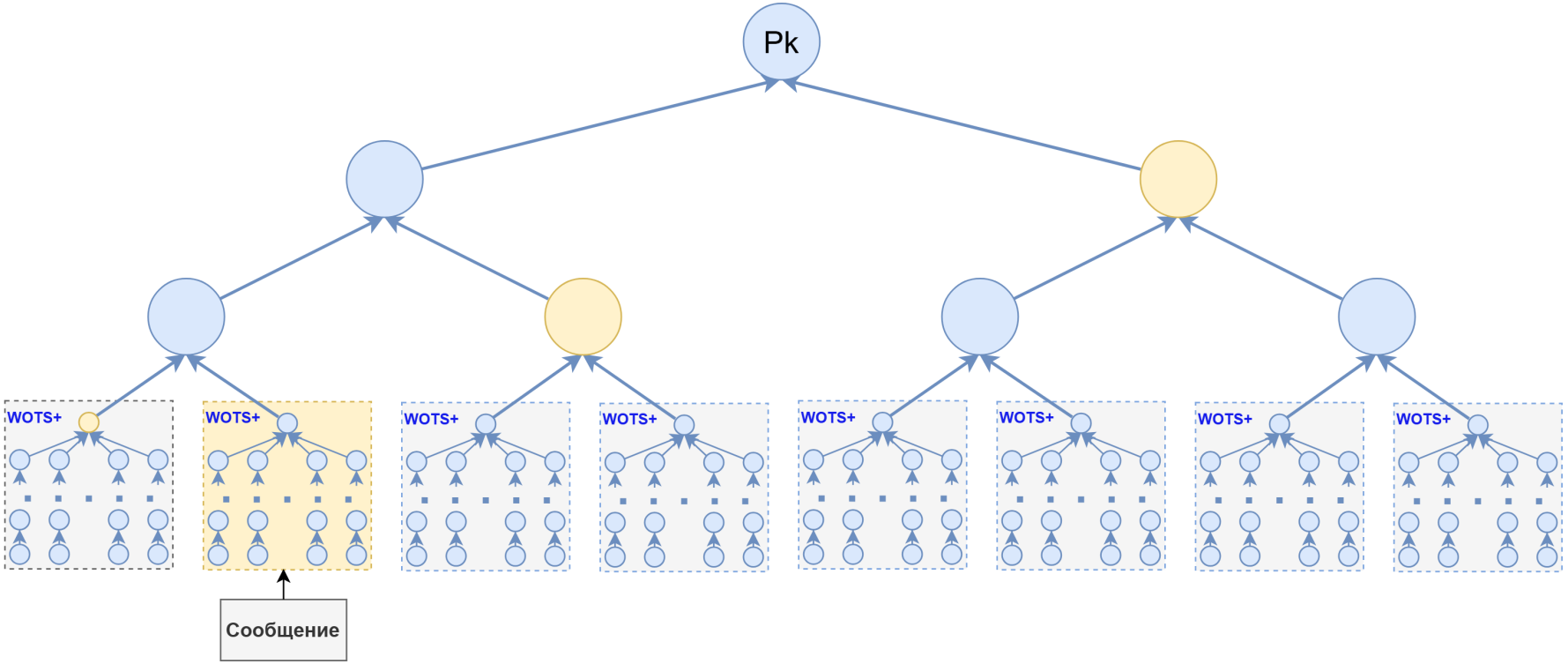


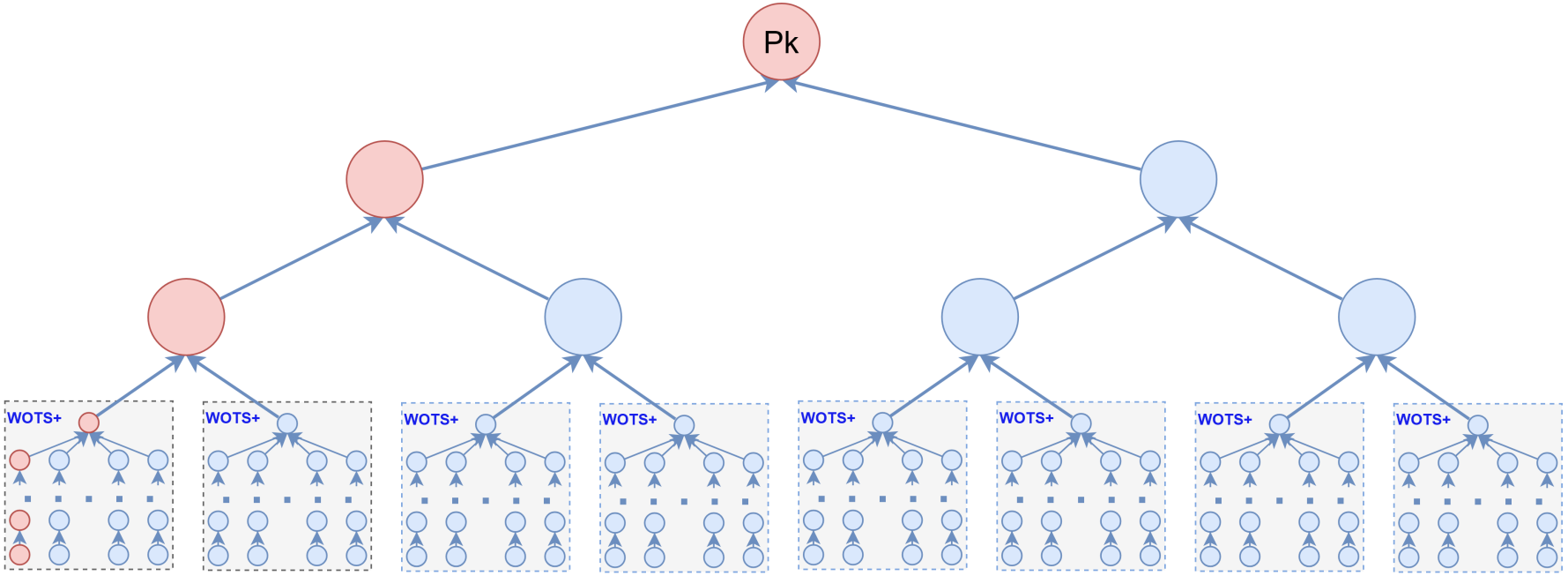
Схема XMSS

КуАпп



Композиция вызовов в схеме XMSS

КуАпп



Композиция вызовов в схеме XMSS

КуАпп

Открытый ключ Pk_{xmss} схемы XMSS может быть выражен через открытый ключ Pk_{wots} схемы WOTS+ как:

$$Pk_{xmss} = H_h(H_{h-1}(...(H_1(G_w(G_{w-1}(...(G_0(SK.seed))))))).$$

Используя полученный результат в теореме о математическом ожидании количества прообразов, имеем, что в среднем существует не менее $\frac{h+w+3}{2}$ подходящих секретных зерен, соответствующих одному открытому ключу XMSS, при рассмотрении одной цепочки одной ветви дерева.

Нахождение подходящего секретного ключа

КуАпп

Отсюда имеем следующую оценку вероятности нахождения подходящего секретного зерна для одной цепочки одной ветви XMSS:

$$\mathrm{P}_{\mathrm{xmss}}^{\mathrm{keyfound}} \geq \frac{h+w+3}{2^{n+1}} = \frac{h+19}{2^{n+1}},$$

где n — длина выхода хэш-функции, а h — высота дерева.

Трудоемкость одного опробования составляет $w+h$ вызовов хэш-функции.

Средняя вычислительная трудоемкость нахождения подходящего секретного зерна:

$$\mathrm{Complex}_{\mathrm{xmss}}^{\mathrm{keyfound}} = \frac{h+w}{h+w+3} \cdot 2^{n+1}. \quad (1)$$

В уравнении (1) используется равенство вместо оценки сверху согласно эмпирическим результатам

Построение атаки

КуАпп

После нахождения подходящего секретного ключа цепочки атакующий может построить подделку подписи для сообщений определенного вида. При этом сообщения не выбираются напрямую, а получаются как результат хэширования. Если подделывалась цепочка полной длины, то мощность множества подходящих сообщений будет около 2^{51}.

Тогда вероятность нахождения подходящего сообщения при тотальном опробовании будет равна: $2^{-(n-51)}$.

Трудоемкость одного опробования для простоты будем считать как один вызов хэш-функции (на практике больше, но зависит от параметров и конкретной схемы).

Общая сложность

КуАпп

Учитывая оба компонента, имеем, что общая сложность атаки для формирования подделки подписи вычисляется как:

$$\mathrm{Complex}_{\mathrm{xmss}}^{\mathrm{forgery}} = \frac{h+w}{h+w+3} \cdot 2^{n+1} + 2^{n-51}.$$

Несмотря на повышение вероятности успеха, данная атака менее эффективна, чем тотальное опробование секретного ключа, за счет увеличения трудоемкости одного опробования.

2026 СТCRYPT

КуАпп

Алексей Зеленецкий

Старший исследователь «КуАпп»

Старший преподаватель МГТУ им. Н.Э. Баумана

azelenetskiy@qapp.tech

@Leshachi

Олег Турченко

Старший исследователь «КуАпп»

Кандидат технических наук

oturchenko@qapp.tech

@Oleg_Turchenko

qapp.tech