Ежегодная международная научно-практическая конференция
«РусКрипто’2021»

Доказательство подделки подписей на основе хэш-функций

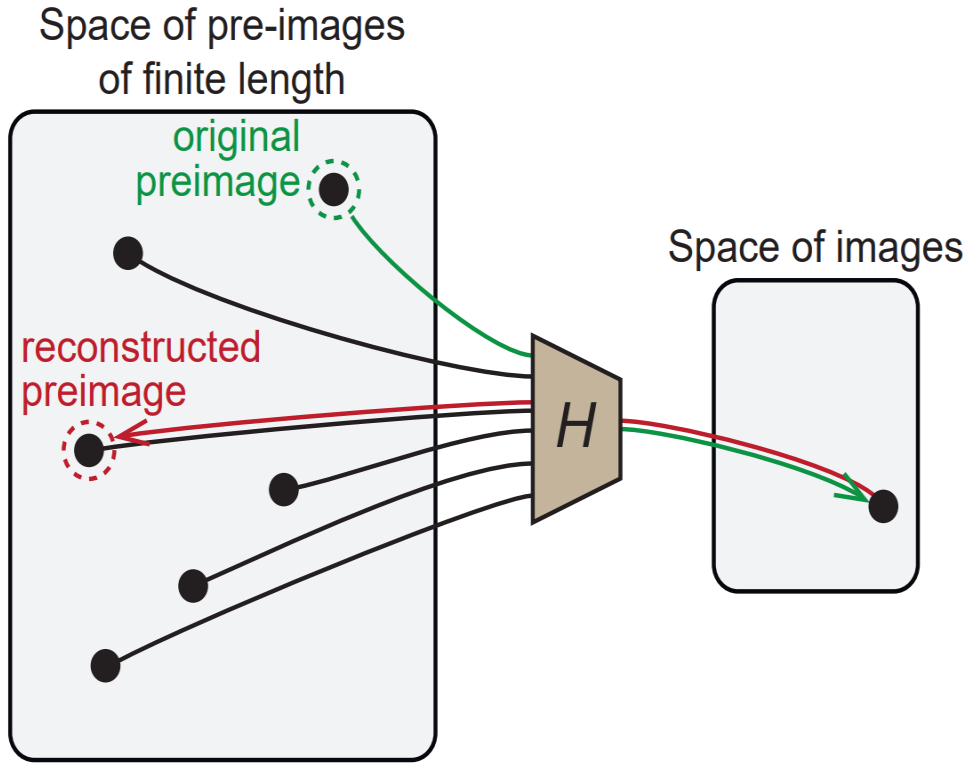
Кудинов Михаил,
Научный сотрудник, QApp - RQC

Введение и постановка задачи

- Сегодня все больше и больше внимание уделяется криптографическим алгоритмам стойким к атакам с использованием квантового компьютера – постквантовым алгоритмам.
- Можно ли снабдить новое поколение постквантовых криптографических алгоритмов каким-либо сигналом тревоги, указывающим на то, что они были взломаны?
- Мы утверждаем, что ответ на этот вопрос частично положительный, и свойство, которое мы называем возможность обнаружения подделки, может быть реализовано с помощью правильно разработанных подписей на основе хэшей.

Основная идея

- Основная идея, лежащая в основе возможности обнаружения подделки, заключается в том, что подделка подписи на основе хэширования, скорее всего, приведет к коллизии, демонстрация этой коллизии может служить убедительным доказательством подделки и наличия уязвимости используемой криптографической хэш-функции.



Определения

- **Детерминированная схема цифровой подписи**
  Детерминированная схема цифровой подписи (DDSS) DSS = (Kg,Sign,Vf) - это тройка алгоритмов, которые позволяют выполнять следующие задачи:

1. Kg (1^n) → (sk, pk) - вероятностный алгоритм генерации ключей, который выводит секретный ключ sk, предназначенный для подписи сообщений, и открытый ключ pk, предназначенный для проверки подписей, при вводе параметра безопасности 1^n.
2. Sign (sk, M) → σ - это детерминированный алгоритм, который выводит подпись σ для секретного ключа sk и сообщения M.
3. Vf (pk, σ, M) → v - алгоритм проверки, который выдает v = 1, если подпись σ подписанного сообщения M правильна под открытым ключом pk, и v = 0 в противном случае.

Определения

- Стандартным требованием к безопасности цифровых подписей является экзистенциальная неподделываемость с атакой по выбранному сообщению (EU-CMA). Данная модель позволяет злоумышленнику выбрать набор сообщений, которые должен подписать легитимный пользователь.

Определения

- **Подделка подписи и ее виды**
  Подпись $\sigma^{\star}$ называется поддельной подписью сообщения $M^{\star}$ под открытым ключом pk и схемой подписи DSS, если Vf (pk, $\sigma^{\star}$, $M^{\star}$) $\rightarrow$ 1 , где сообщение $M^{\star}$ не было подписано легитимным отправителем, обладающим секретным ключом sk. Возможны следующие два случая.

1. Пара ($\sigma^{\star}$, $M^{\star}$) называется подделкой типа I, если подпись $\sigma^{\star}$ была ранее сгенерирована легитимным пользователем как подпись для некоторого сообщения, отличного от $M^{\star}$.
2. Пара ($\sigma^{\star}$, $M^{\star}$) Называется подделкой типа II, если подпись $\sigma^{\star}$ не была ранее создана легитимным пользователем.

Определения

- **Доказательство подделки типа I**
  Набор E = (pk, $\sigma^{\star}$, $M^{\star}$, M) Называется доказательством подделки типа I (PoF-I) для DDSS, если для $M^{\star} \neq M$ существует валидная подпись $\sigma^{\star}$, т.е. имеют место следующие соотношения:
  Vf (pk, $\sigma^{\star}$, M) → 1, Vf (pk, $\sigma^{\star}$, M) → 1.
- **Доказательство подделки типа II**
  Набор E = (pk, $\sigma^{\star}$, σ, $M^{\star}$) называется доказательством подделки типа II (PoF-II) для DDSS, если для сообщения $M^{\star}$ существуют разные валидные подписи $\sigma^{\star} \neq \sigma$ т.е. имеют место следующие соотношения: Vf (pk, $\sigma^{\star}$, $M^{\star}$) → 1, Vf (pk, σ, $M^{\star}$) → 1.

Определения

ε- возможность обнаружения подделки

ε-возможность обнаружения подделки (ε-FDA) для одноразовой схемы DDSS определяется следующим экспериментом.

1. (sk, pk) ← Kg (1^n)
2. ($\sigma^\star$, $M^\star$)← $A^{\{Sign\,(sk,\cdot)\}}$(pk)
3. Пусть (M, σ) - ответ на запрос к $Sign(sk,\cdot)$.
4. Вернуть 1, если Sign (sk , $M^\star$) → $\sigma^\star$, Vf (pk, $\sigma^\star$, $M^\star$) → 1, и $M^\star \neq M$.

   Схема DSS имеет ε-FDA, если нет противника A, который преуспевает с вероятностью ≥ε.

Лемма

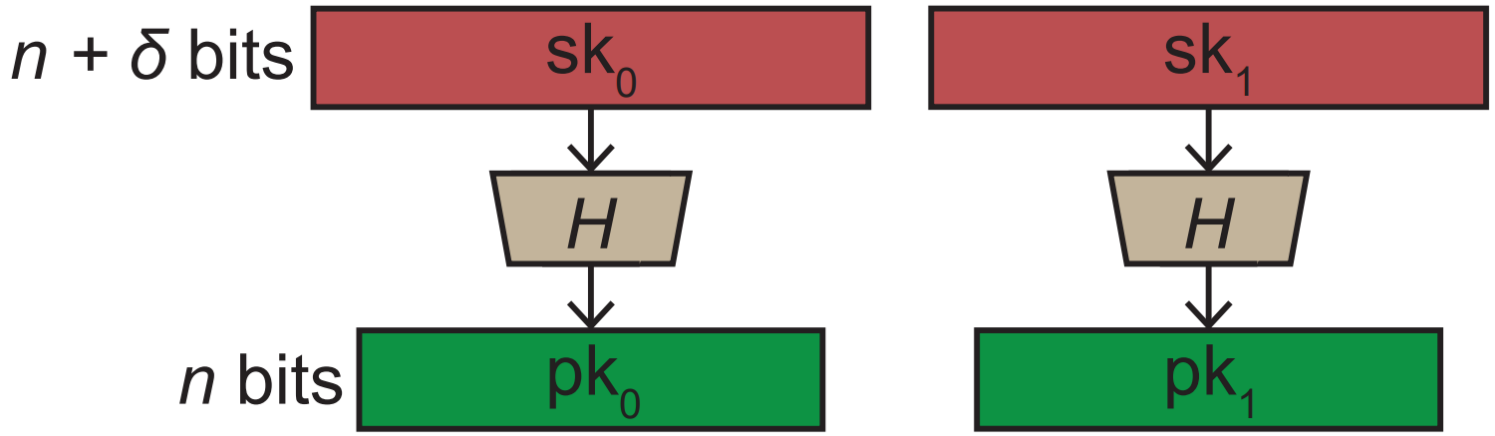
- Рассмотрим функцию f: $\{0,1\}^{n+\delta} \to \{0,1\}^n$ с $n \gg 1$ и $\delta \geq 0$, которая соответствует модели случайного оракула. Пусть $f(x_0) = y_0$ для некоторого $x_0 \in \{0,1\}^{n+\delta}$.
- Определим набор

$$Inv(y_0) := \{x \in \{0,1\}^{n+\delta} \mid f(x) = y_0\}$$

всех прообразов y_0. Рассмотрим случайно взятый прообраз $X \leftarrow Inv(y_0)$. Тогда вероятность получить исходный прообраз $X = x_0$ имеет следующие нижнюю и верхнюю границы:

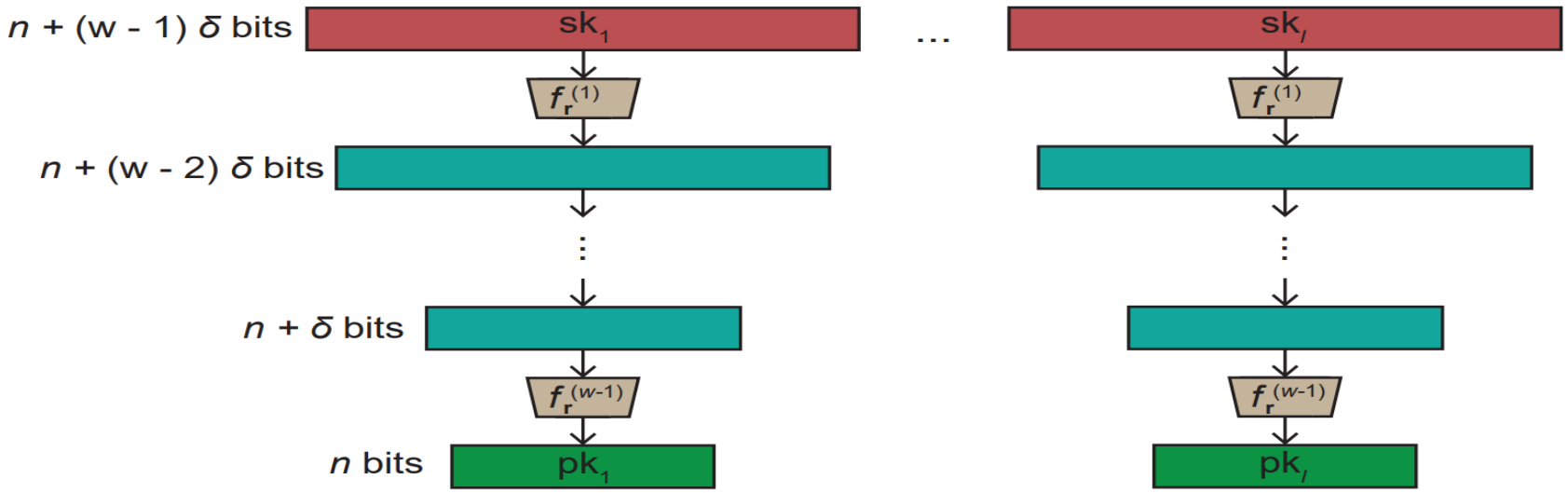
1. $\Pr(X = x_0) > \exp(-2^{\delta})$
2. $\Pr(X = x_0) < 5.22 \times 2^{-\delta}$

Модифицированная схема Лэмпорта



- Рассмотрим криптографическую хэш-функцию $H: \{0,1\}^{n+\delta} \rightarrow \{0,1\}^{n}$, которая удовлетворяет предположению о случайном оракуле. Тогда модифицированная схема Лэмпорта построенная на данной хэш-функции обладает свойством ε -FDA с $\varepsilon < 5.22 \times 2^{-\delta}$.

Модифицированная схема Винтерница



- Зададим параметры модифицированной схемы Винтерница, построенной на хэш функциях удовлетворяющих предположению о случайном оракуле, тогда модифицированная схема Винтерница построенная на данных хэш-функциях обладает свойством ε -FDA с $\varepsilon < 5.22 \times 2^{-\delta}$.

Выводы

- В этой работе мы рассмотрели свойство ε-FDA DDSS, которое позволяет обнаруживать событие подделки.
- Мы показали, что это свойство выполняется для правильно спроектированных хэш-подписей, в частности, для схем L-OTS и W-OTS + с правильно настроенными параметрами.
- Вероятность успешной демонстрации события подделки DDSS зависит от превышения размеров пространства прообразов над размерами пространства образов.
- Следующим важным шагом является изучение этого свойства для других типов подписей на основе хэшей.

Вопросы

Контактная информация

Электронная почта:

mkudinov@qapp.tech

Телефон:

+7 916 575 41 66

Facebook:

https://www.facebook.com/postquantum/

Сайт:

https://qapp.tech/