Квантовая криптография, хеширование, цифровая подпись

Фарид Аблаев
Казанский федеральный университет

Computer Science Club
декабрь 2015

- D. Brassard, C. Bennet 1984 Quantum Key Distribution BB84
- P. Shor 1994. Quantum algorithms:
  - integer factorization,
  - discrete logarithm.
- "Post-quantum cryptography" http://pqcrypto.org/
  The book: Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen (editors). Post-quantum cryptography. Springer, 2009.
  - ...
  - Hash-based signature schemes such as L. Lamport signatures and R. Merkle signature schemes.
- Hashing itself is an important basic concept for the organization transformation and reliable transmission of information.
  - In 1995 A. Wigderson characterizes universal hashing as being a tool which "should belong to the fundamental bag of tricks of every computer scientist".

Quantum Algorithms, Quantum Cryptography

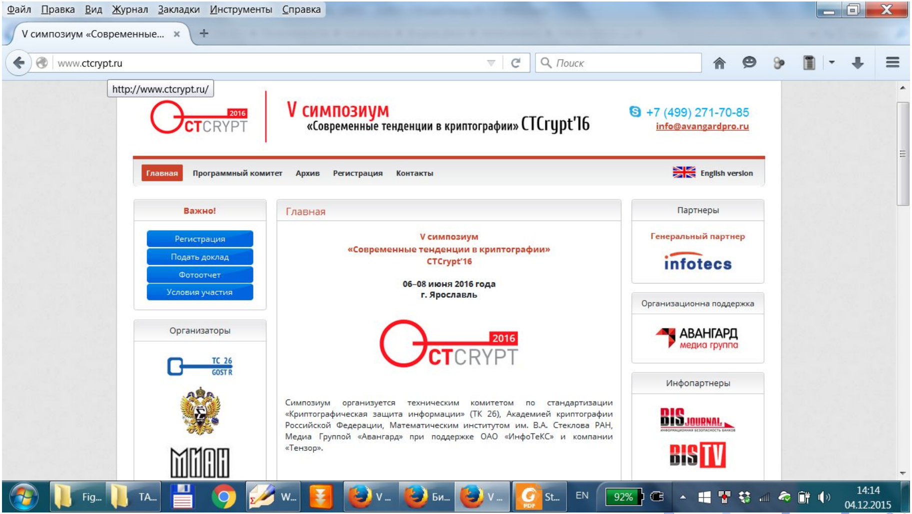
- Quantum Algorithms ZOO: http://math.nist.gov/quantum/zoo/
- Conference Quantum Information Processing (QIP)
  - QIP2014 Barcelona http://benasque.org/2014QIP/
  - QIP2015 Sidney http://www.quantum-lab.org/qip2015/
  - QIP2016 Calgary ...
- Quantum Cryptography $\approx$ QKD:
  http://en.wikipedia.org/wiki/Quantum-cryptography
  Conference on quantum cryptography
  - QCrypt 2014 Paris http://2014.qcrypt.net/
  - QCrypt 2015 Tokyo http://2015.qcrypt.net
  - QCrypt 2016 Washington

QCrypt 2014. 4th international conference on quantum cryptography

Современные тенденции в криптографии 2015

Современные тенденции в криптографии 2016

http://www.ctcrypt.ru/index



Современные тенденции в криптографии 2016

Тематика симпозиума включает следующие вопросы (но не ограничивается ими):

- исследование криптографических алгоритмов, в том числе анализ криптографических алгоритмов, являющихся международными стандартами;
- эффективная реализация методов анализа криптографических алгоритмов;
- оценка криптографической стойкости российских криптографических алгоритмов;
- эффективная реализация российских криптографических алгоритмов.

Современные тенденции в криптографии 2016

Специальная тема симпозиума: "Будущее асимметричной криптографии".

Перспективы развития квантовых компьютеров, а также последние результаты по решению задачи дискретного логарифмирования потенциально являются серьезными угрозами для многих широко используемых механизмов асимметричной криптографии. Следует ли ожидать серьезных прорывов в решении задачи дискретного логарифмирования и как будет развиваться пост-квантовая асимметричная криптография –вопросы для обсуждения на CTCrypt'2016.

Приглашенный докладчик: Игорь Семаев, Университет Бергена, Норвегия

В рамках симпозиума пройдет дискуссионная панель "День открытых дверей ТК 26 тема – гражданская криптография.

Генерация ключа

Ralph Merkle, Martin Hellman and Whit Diffie developed the first public key cryptography exchange in 1975.

Diffie-Hellman Problem (Discrete Logarithm Problem)

- For a prime q a multiplicative group $\mathbb{F}_q^\times = \langle \{1, \dots, q-1\}, \times \rangle$ of the field $\mathbb{F}_q$ is cyclic, i.e. there exists a primitive element (generator) g such that
$$\mathbb{F}_q^\times = \{g^0, g^1, g^2, \dots\}.$$
- Given a primitive element g of a finite field $\mathbb{F}_q$, the discrete logarithm of a nonzero element $u \in \mathbb{F}_q$ is that integer k, $1 \leq k \leq q-1$, for which $u = g^k$.
- Discrete logarithm problem: Given $\mathbb{F}_q^\times, g$ and $h \in \{1, \dots q-1\}$ determine an integer a such that $g^a = h$.
- Computational Diffie-Hellman problem: given $h = g^a$ and $d = g^b$ find $c = g^{ab}$.
- Finding discrete logarithm is conditionally one-way function.

V. Shoup Theorem

- A black-box group G is a finite group whose elements are encoded by (0,1)- strings ("codewords") of uniform length n. ($|G| \leq 2^n$).
- n is the encoding length of the black-box group.
- Group operations on the codewords are performed by a "black box" at unit cost.

The operations are:

1. multiplication, 2. inversion, and 3. identity testing (decision whether or not a given string encodes the identity).
A black-box group is given by a list of generators.

Theorem (Shoup 1997)

In a "black box group" of prime order ℓ it takes at least $\sqrt{\ell}$ operations to solve the discrete logarithm problem

Diffie-Hellman Protocol for Key Generation 1976

Choose a large prime q and a primitive element (generator) $g \in \mathbb{F}_q^\times$

Stage I.

- Alice randomly selects $a \in \{1, \ldots, q-1\}$, computes $K_A = g^a$,
- sends K_A to Bob
- Bob randomly selects $b \in \{1, \ldots, q-1\}$, computes $K_B = g^b$,
- sends K_B to Bob

Stage II.

- Alice computes $K = K_B^a = g^{ba}$ on her side,
- Bob computes $K = K_A^b = g^{ab}$ on his side

Passive Melory: Security based on Diffie-Hellman problem: given g^a and g^b compute g^{ab}.

Active Melory: ...

Diffie-Hellman Protocol Example.

q=23, $\mathbb{F}_{23}^{\times}$
Найти генератор g (все генераторы)
Alice: a=6,
Bob: b=5.
Сгенерировать общий ключ.

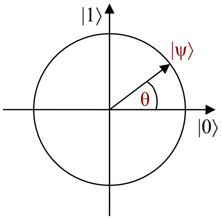
1. Quantum Postulates. Qubit.

- Qubit is a unit vector in the two-dimensional Hilbert complex space $\mathcal{H}^2$.

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle, \qquad |||\psi\rangle||^2 = |a_0|^2 + |a_1|^2 = 1$$

- Case of real amplitudes.

$$|\psi(w)\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$$



1. Quantum Postulates. Qubit Transformation.

Quantum transformation U of qubits is a unitary transformation

$$U : \mathcal{H}^2 \to \mathcal{H}^2, \qquad |\psi'\rangle = U|\psi\rangle.$$

Example

$$|0\rangle = (1,0)^T, \qquad |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|1\rangle = (0,1)^T, \qquad |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

$$|+\rangle = H|0\rangle \qquad |-\rangle = H|1\rangle$$

- Computational basis (C-basis): $\{|e_0\rangle, |e_1\rangle\} = \{|0\rangle, |1\rangle\}$,
- Hadamar (Diagonal) basis (H-basis): $\{|e_0\rangle, |e_1\rangle\} = \{|+\rangle, |-\rangle\}$

Extracting information from $|\psi\rangle$

$$|\psi\rangle = a_0|e_0\rangle + a_1|e_1\rangle$$

Measuring $|\psi\rangle$ in respect to basis $\{|e_0\rangle, |e_1\rangle\}$.

$$Pr[\text{extract } 0 \text{ from } |\psi\rangle] = (\langle e_0 \mid \psi\rangle)^2 = |a_0|^2.$$

$$Pr[\text{extract } 1 \text{ from } |\psi\rangle] = (\langle e_1 \mid \psi\rangle)^2 = |a_1|^2.$$

1. Quantum Postulates. Qubit Extracting an Information

Example

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

- Measuring $|\psi\rangle$ in respect to C-basis $\{|0\rangle, |1\rangle\}$.

$$Pr[\text{extract 0 from } |\psi\rangle] = Pr[\text{extract 1 from } |\psi\rangle] = 1/2$$

- Measuring $|\psi\rangle$ in respect to H-basis $\{|+\rangle, |-\rangle\}$.

$$Pr[\text{extract 0 from } |\psi\rangle] = (\langle + \mid \psi\rangle)^2 = 1.$$

$$Pr[\text{extract 1 from } |\psi\rangle] = (\langle - \mid \psi\rangle)^2 = 0.$$

Quantum key Distribution. Protocol BB844

1. One cannot measure the polarization of a photon in the H-basis and simultaneously in the C-basis.
   - Нельзя одновременно измерить поляризацию фотона в двух различных базисах.
2. One cannot duplicate an unknown quantum state (No cloning theorem).
   - Невозможно копировать неизвестное квантовое состояние.
3. Every measurement perturbs the system.
   - Каждое измерение изменяет (возмущает) квантовую систему.

Protocol BB84 “на пальцах”

Protocol BB84

In the BB84 scheme, Alice begins with two strings of bits, a and b, each n bits long. She then encodes these two strings as a string of n qubits,

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle.$$

a_i and b_i are the i^{th} bits of a and b, respectively. Together, $a_i b_i$ give us an index into the following four qubit states:

$$|\psi_{00}\rangle = |0\rangle, \qquad |\psi_{10}\rangle = |1\rangle$$

$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad |\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

The bit b_i is responsible for basis (C-basis or the H-basis) in which a_i is encoded in. The qubits are now in states which are not mutually orthogonal, and thus it is impossible to distinguish all of them with

Protocol EPR

EPR pair

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

$$|\psi\rangle \neq |\phi_1\rangle \otimes |\phi_2\rangle$$

- In the EPR protocol scheme, Alice wishes to send a private key to Bob. She begins with n string of EPR pairs, ...
- The protocol proceeds then similar to the BB84...

Контроль целостности информации, аутентификация, цифровая подпись на основе хеширования

One-way function

Let $f : \Sigma^* \to \Sigma^*$ be a function. Consider the following experiment defined for any inverting probabilistic polynomial-time algorithm A and any value $n \in \mathbb{N}$:

The inverting experiment $Invert_{A,f} : \mathbb{N} \to \{0, 1\}$

1. Choose input $x \in \Sigma^n$. Compute $y = f(x)$.
2. probabilistic polynomial-time algorithm A is given 1^n and y as input, and outputs x'.
3. The output of the experiment is defined to be 1 if $f(x') = y$, and 0 otherwise.

One-way function

Defintion

A function $f : \Sigma^* \rightarrow \Sigma^*$ is one-way if the following two conditions hold:

1. (Easy to compute:) There exists a polynomial-time algorithm $\mathcal{M}_f$ computing f; that is, $\mathcal{M}_f(x) = f(x)$ for all x.
2. (Hard to invert:) For every probabilistic polynomial-time algorithm A, for any polynomial $p(n) \in POLY$ it is hold

$$Pr[Invert_{A,f}(n) = 1] \leq 1/p(n).$$

Theorem

If One-way function exist then $NP \neq P$.

1.Suppose $f : \{0,1\}^* \to \{0,1\}^*$ is a strong one-way function, Define

$$L_f = \{(x, y, 1^k) : \text{there exists } u \in \{0,1\}^k \text{such that } f(xu) = y\},$$

2. $L_f \in NP$ since given $(x, y, 1^k) \in L_f$ a certificate is any $u \in \{0,1\}^k$ such that $f(xu) = y$.
3. $L_f \in NP \backslash P$:

Suppose that $P = NP$. Then inverting polynomial algorithm A :
Input: $(f(x), 1^k)$
$z := \emptyset$; $i := 1$;
while $i \leq k$ do
if $(z0, f(x), 1^{k-i}) \in L_f$ then $z := z0$ else $z := z1$;
$i := i + 1$;
if $f(z) = f(x)$ output z
end-while

Криптографические хеш-функции. Cryptographic hash-function

$$h : \Sigma^* \to \Sigma^*, \qquad h : \Sigma^k \to \Sigma^m, \quad k > m$$

1. Функция h должна быть однонаправленной (точнее “условно однонаправленной” на сегодняшний день).
2. Функция h должна быть коллизия устойчивой:
   1. Для заданного сообщения w должно быть “вычислительно сложно” подобрать другое сообщение v, для которого $h(w) = h(v)$.
   2. Должно быть “вычислительно сложно” подобрать пару сообщений (w, v) такую, что $h(w) = h(v)$.
3. h должна изменяться “лавинообразно” (изменение одного символа аргумента должно вести к изменению большого числа символов значения функции).

Date integrity. Целостность информации.

Криптографическая проверка целостности передаваемой информации от Алисы (A) к Бобу (B) заключается в вычислении Алисой хеша $h(w)$ для передаваемого сообщения w и передачи пары $(w, h(w))$ Бобу. Боб, получив пару $(w', h(w))$ на своей стороне вычисляет значение $h(w')$ и сравнивает значения $h(w)$ и $h(w')$.

Authetification. Аутентификация — проверка подлинности пользователя.

Схема аутентификации вызов-ответ CHAP (Challenge Handshake Authentication Protocol).
Протокол MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)

1. пользователь посылает серверу запрос на доступ (login)
2. сервер отправляет клиенту случайную последовательность v
3. на основе этой случайной последовательности v и пароля w пользователя клиент вычисляет значение $h(vw)$ хеш-функции на vw
4. клиент пересылает хеш $h(vw)$ серверу
5. сервер сверяет присланный хеш $h(vw)$ со своим вычисленным $h(vw)$
6. в случайные промежутки времени сервер отправляет новую последовательность v' и повторяет шаги с 2 по 5.

Основные требования к цифровой подписи

1. Целостность. Нарушитель не должен иметь возможность фальсификации. Message integrity
2. Аутентификация – Гарантия подлинности. Message authentication
3. Автор не может отказаться от подписанного сообщения. Message non-repudiation

Lamport digital scheme

Discrete Logarithm (recall)

- For a prime q a multiplicative group $\mathbb{F}_q^\times = \langle\{1, \ldots, q-1\}, \times\rangle$ of the field $\mathbb{F}_q$ is cyclic, i.e. there exists a primitive element (generator) g such that

$$\mathbb{F}_q^\times = \{g^0, g^1, g^2, \ldots\}.$$

- Given a primitive element g of a finite field $\mathbb{F}_q$, the discrete logarithm of a nonzero element $u \in \mathbb{F}_q$ is that integer k, $1 \leq k \leq q-1$, for which $u = g^k$.
- Discrete logarithm problem: Given $\mathbb{F}_q^\times, g$ and $h \in \{1, \ldots q-1\}$ determine an integer a such that $g^a = h$.

ElGamal signature scheme. Схема цифровой подписи Эль-Гамаля.

q — (large enough) prime number. g — generator of $\mathbb{F}_q^\times$.

- k — private key. $a = g^k$ — public key.
- r — random key. $c = g^r$ — second public key.
- m — message.
- Signature equation for the message and keys and its solution:

$$g^m = g^{kc+rx} \quad \Rightarrow \quad x = \frac{m - kc}{r}.$$

Then

$$g^m = \left(g^k\right)^c \cdot (g^r)^x = a^c \cdot c^x$$

Protocol.

1. Alice sends a everybody. Alice sends Bob m, c, x.
2. Bob reads m and check whether $g^m = a^c \cdot c^x$?

Quantum hashing. Basic idea

The basic idea of our work is

to hash (to encode) words (classical information) into quantum state.

Such encoding:

- Must be One-way function.
  Quantumly one-way (physically one-way).
- Must be collision (almost) free.
  Quantumly resistant (physically resistant) – encoding must be designed to have maximum output difference between adjacent inputs.

1. Quantum Postulates for Quantum Cryptography

- Mathematically. Qubit

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle, \qquad |||\psi\rangle||^2 = |a_0|^2 + |a_1|^2 = 1$$

  is a unit vector in the two-dimensional Hilbert complex space $\mathcal{H}^2$.

- $(\mathcal{H}^2)^{\otimes s} = \mathcal{H}^2 \otimes \cdots \otimes \mathcal{H}^2$ – (2^s)-dimensional Hilbert space of s qubits

$$|\psi\rangle = \sum_{i=0}^{2^s-1} a_i|i\rangle, \qquad \sum_{i=0}^{2^s-1} |a_i|^2 = 1.$$

Quantum (classical-quantum) function maps words to quantum states

$$\psi : \Sigma^k \to (\mathcal{H}^2)^{\otimes s}, \qquad \psi : w \mapsto |\psi(w)\rangle \qquad (\psi : |0\rangle, w \mapsto |\psi(w)\rangle).$$

Quantum Transformation, Extracting Information

Quantum Transformation

$$\psi : \mathcal{H}^{2^s} \times \Sigma^k \to \mathcal{H}^{2^s} \qquad \psi : |0\rangle, w \mapsto |\psi(w)\rangle$$

determined by an $2^s \times 2^s$ unitary matrix $U(w)$.

$$|\psi(w)\rangle = U(w)|0\rangle.$$

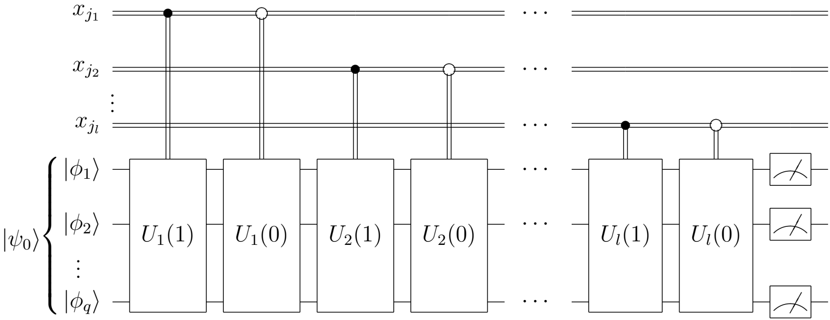
Extracting information from $|\psi\rangle$

$$|\psi\rangle = \sum_{i=0}^{2^s-1} a_i|i\rangle, \qquad \sum_{i=1}^{2^s} |a_i|^2 = 1.$$

Measuring $|\psi\rangle$ in respect to orthonormal basis $\{|0\rangle, \dots, |2^s - 1\rangle\}$.

$$Pr[\text{extract } |0\rangle \text{ from } |\psi\rangle] = (\langle 0 \mid \psi(w)\rangle)^2 = |a_0|^2.$$

Quantum Branching Program — computational model for quantum functions



One-way ϵ-Resistant Function

Definition

- Let X be random variable distributed over $\mathbb{X}$ $\{Pr[X = w] : w \in \mathbb{X}\}$. Let $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ be a quantum function.
- Let Y is any random variable over $\mathbb{X}$ obtained by some mechanism $\mathcal{M}$ making some measurement to quantum state $|\psi(X)\rangle$ (of the encoding ψ of X) and decoding the result of measurement to $\mathbb{X}$.
- Let $\epsilon > 0$. We call a quantum function ψ a one-way ϵ-resistant function if for any mechanism $\mathcal{M}$, the probability $Pr[Y = X]$ that $\mathcal{M}$ successfully decodes Y is bounded by ϵ

$$Pr[Y = X] \leq \epsilon.$$

Quantum One-Way property. Holevo-Nayak theorem

A. Holevo. (Проблемы передачи информации 1973)

We can not extract from s-qubit quantum state $|\psi\rangle$ more than s bits of information.

Theorem (Holevo-Nayak)

- Let w is a k bit binary word.
- Let w be encoded into s qubit quantum state $|\psi(w)\rangle$.
- Let then the state $|\psi(w)\rangle$ is decoded via some mechanism back to a k bit word v.

Then our probability of correct decoding is given by

$$Pr[v = w] \leq \frac{2^s}{2^k}.$$

Collision δ-Resistant Function

Definition

Let $\delta > 0$. We call a quantum function

$$\psi : \Sigma^k \to (\mathcal{H}^2)^{\otimes s}$$

a collision δ-resistant function if for any pair w, w' of different elements,

$$\left|\langle \psi(w) \mid \psi(w') \rangle\right| \leq \delta.$$

REVERSE-test

- given w and $|\psi(v)\rangle = U(v)|0\rangle$, applies $U^{-1}(w)$ to the state $|\psi(v)\rangle$ and measures the resulting state in respect the state $|0\rangle$.
- The test outputs $v = w$ iff the measurement outcome is $|0\rangle$.

$$Pr_{REVERSE}(v = w) = (\langle 0 \mid U^{-1}(v)|\psi(w)\rangle\rangle)^2 \tag{1}$$

- If $w = v$, then $U^{-1}(v)|\psi(w)\rangle$ would always give $|0\rangle$, and REVERSE-test would give the correct answer.

$$Pr_{REVERSE}(v = v) = 1.$$

- If $v \neq w$

$$Pr_{REVERSE}(w = v) \quad \text{can be (unfortunately) close to 1}$$

Property

Let hash function $\psi : w \mapsto |\psi(w)\rangle$ satisfy the following condition. For any two different elements $v, w \in \mathbb{X}$ it is true that

$$|\langle \psi(v) \mid \psi(w) \rangle| \leq \delta.$$

Then

$$Pr_{reverse}[v = w] \leq \delta^2.$$

Proof. Using the property that unitary transformation keeps scalar product we have that

$$\begin{aligned} Pr_{reverse}[v = w] &= |\langle 0 \mid U^{-1}(v)\psi(w)\rangle|^2 \\ &= |\langle U^{-1}(v)\psi(v) \mid U^{-1}(v)\psi(w)\rangle|^2 \\ &= |\langle \psi(v) \mid \psi(w)\rangle|^2 \leq \delta^2. \end{aligned}$$

Quantum Hash Function

Definition (ϵ, δ)-Resistant $(|\Sigma^k|, s)$ Quantum Hash-function

We call a function

$$\psi : \Sigma^k \to (\mathcal{H}^2)^{\otimes s}$$

an (ϵ, δ)-Resistant $(|\Sigma^k|, s)$ Quantum Hash-function if:

- ψ is easily computed, that is, for a particular $w \in \Sigma^k$ a state $|\psi(w)\rangle$ can be determined using a polynomial-time algorithm
- ψ is a one-way ϵ-resistant function
- ψ is a collision δ-Resistant $(|\Sigma^k|, s)$ function: for different words $w, w' \in \Sigma^k$

$$\left|\langle\psi(w) \mid \psi(w')\rangle\right| \le \delta.$$

Example 1.

- Word (binary) $w = w_0 \dots w_{k-1}$.
- Number $w = \sum_{i=0}^{k-1} w_i 2^i$.

Example

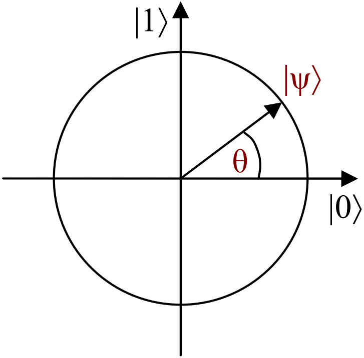
We encode a word $w \in \{0,1\}^k$ into one qubit:

$$\psi : \{0,1\}^k \to \mathcal{H}^2$$

$$|\psi(w)\rangle = \cos\left(\frac{2\pi w}{2^k}\right)|0\rangle + \sin\left(\frac{2\pi w}{2^k}\right)|1\rangle,$$

$|\psi(w)\rangle$ – one qubit

$$|\psi(w)\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle = \cos\left(\frac{2\pi w}{2^k}\right)|0\rangle + \sin\left(\frac{2\pi w}{2^k}\right)|1\rangle,$$



Example 2.

Example

We consider a number $v \in \{0, \ldots, 2^k - 1\}$ to be also a binary word $v \in \{0,1\}^k$. Let $v = \sigma_1 \ldots \sigma_k$. We encode v by k qubits:

$$\psi : v \mapsto |v\rangle = |\sigma_1\rangle \cdots |\sigma_k\rangle$$

Lower bound for s for δ-Resistant $(|\Sigma^k|, s)$ quantum function

Theorem (Lower Bound)

If $\psi : \Sigma^k \to (\mathcal{H}^2)^{\otimes s}$ is δ-Resistant $(|\Sigma^k|, s)$ quantum function then

$$s \geq \log k - \log\log\left(1 + \sqrt{2/(1-\delta)}\right) - 1.$$

$$|||\psi\rangle|| = \sqrt{\langle\psi \mid \psi\rangle}$$

$$|||\psi\rangle - |\psi'\rangle||^2 = |||\psi\rangle||^2 + |||\psi'\rangle||^2 - 2\langle\psi \mid \psi'\rangle = 2 - 2\langle\psi \mid \psi'\rangle.$$

Property

If ψ is δ-Resistant, then for w, w'

$$\rho(|\psi(w)\rangle, |\psi(w')\rangle) = |||w\rangle - |w'\rangle|| \geq \sqrt{2(1-\delta)} = \Delta.$$

Balanced Quantum Hash Functions

- The above properties provide a basis for building a "balanced" one-way ϵ-resistance and collision δ-resistance properties.
- That is, roughly speaking, if we need to hash elements w from a domain Σ^k with $|\Sigma^k| = K$ and if one can build for a $\delta > 0$ a collision δ-resistant $(K; s)$ hash function ψ with

$$s \approx \log k \log |\Sigma| - c(\delta)$$

qubits then the function f will be a one-way ϵ-resistant with $\epsilon \approx (\log K/K)$.

Quantum fingerprinting function (2001)

H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf

- Let $E : \{0,1\}^k \to \{0,1\}^n$ be an (n,k,d) error correcting code with Hamming distance d.
- Family $E = \{E_1, \dots E_n\}$, here $E_i(w)$ – i-th bit of code word.
- Quantum fingerprinting function $\psi_E : \{0,1\}^k \to (\mathcal{H}^2)^{\otimes s}$,

$$|\psi_E(w)\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle |E_i(w)\rangle$$

Quantum fingerprinting = binary quantum hash function

Property

For $s = \log n + 1$, $\delta \geq (1 - d/n)$ function ψ_{F_E} is an $\left(\frac{2n}{2^k}, \delta\right)$-Resistant $(2^k, s)$ quantum hash function.

w, w' $\langle \psi(w) \mid \psi(w') \rangle =?$

Examples

Repeation codes

Hadamard Matrix $H_1 = [1]$.

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad H_4 = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix} \quad H_{2^l} = H_2 \otimes H_{2^{l-1}}$$

Hadamard code $\mathcal{H}$.

$1 \mapsto 0$; $-1 \mapsto 1$.

“Non binary” quantum hash function (2008)

F. Ablayev, A. Vasiliev

$\mathbb{F}_q$ – finite field, q – prime power. $H = \{h_1, \dots h_T\}$ where

$$h_j : \mathbb{F}_q \to \mathbb{F}_q \qquad h_j(w) = b_j w \pmod q.$$

For $s = \log T + 1$ Quantum function $\psi_H : \mathbb{F}_q \to (\mathcal{H}^2)^{\otimes s}$,

$$|\psi_H(w)\rangle = \frac{1}{\sqrt{T}} \sum_{j=1}^{T} |j\rangle \left(\cos \frac{2\pi h_j(w)}{q} |0\rangle + \sin \frac{2\pi h_j(w)}{q} |1\rangle \right).$$

Property (Ablayev, Vasiliev 2013)

For $\delta > 0$, for $T = \lceil (2/\delta^2) \ln(2q) \rceil$, for $s = \log T + 1$ there exists a family

$$H_{\delta,q} = \{h_1, \dots, h_T\}$$

such that $\psi_{H_{\delta,q}}$ is an δ-R (q, s) quantum hash function.

Quantum function generated by a family of functions. Example

Binary word $w = w_0 \dots w_{k-1}$, number $w = \sum_{i=0}^{k-1} w_i 2^i$, $b_j \in \mathbb{F}_q$.
Family $H = \{h_1, \dots, h_T\}$

$$h_j(w) = b_j w \pmod{q}.$$

Quantum function $\psi_{h_j} : \{0,1\}^k \to \mathcal{H}^2$ generated by $h \in H$

$$|\psi_{h_j}(w)\rangle = \cos \frac{2\pi h_j(w)}{q}|0\rangle + \sin \frac{2\pi h_j(w)}{q}|1\rangle$$

Quantum function $\psi_H : \{0,1\}^k \to (\mathcal{H}^2)^{\otimes(\log T+1)}$ generated by H

$$|\psi_H(w)\rangle = \frac{1}{\sqrt{T}} \sum_{j=1}^{T} |j\rangle|\psi_{h_j}(w)\rangle =$$

$$\frac{1}{\sqrt{T}} \sum_{j=1}^{T} |j\rangle \left(\cos \frac{2\pi h_j(w)}{q}|0\rangle + \sin \frac{2\pi h_j(w)}{q}|1\rangle\right).$$

Quantum hash generator

Let $G = \{g_1, \ldots, g_D\}$ be a family of functions $g_j : \Sigma^k \to \mathbb{F}_q$. Let $\ell \geq 1$ be an integer and ψ_{g_j}, $j \in \{1, \ldots, D\}$, be a quantum functions

$$\psi_{g_j} : \Sigma^k \to (\mathcal{H}^2)^\ell,$$

determined by $g_j \in G$. Let $d = \log D$. We define a quantum function

$$\psi_G : \Sigma^k \to (\mathcal{H}^2)^{\otimes(d+\ell)}$$

by the rule

$$\psi_G(w) = \frac{1}{\sqrt{D}} \sum_{j=1}^{D} \underbrace{|j\rangle}_{d} \underbrace{|\psi_{g_j}(w)\rangle}_{\ell}.$$

We call G a δ-R $(|\Sigma^k|, d+\ell)$ quantum hash generator, if ψ_G is an δ-R $(|\Sigma^k|, d+\ell)$ quantum hash function.

Examples of quantum hash generator

Binary

For binary (n, k, d) error correcting code $E : \{0,1\}^k \to \{0,1\}^n$ with Hamming distance d the following is true.
For $\delta = 1 - d/n$ The family

$$E = \{E_1, \dots E_n\}$$

is δ-R $(2^k, \log n + 1)$ quantum hash generator

Non binary

For $\delta > 0$, for q prime power, for $T = \lceil (2/\delta^2) \ln(2q) \rceil$ there exists a set

$$H_{\delta,q} = \{h_1, \dots, h_T\}$$

which is an δ-R $(q, \log T + 1)$ quantum hash generator.

ϵ-Universal Hash Family (Carter, Wegman 1979).

q — prime, $\mathbb{F}_q$ — field, $K = |\mathbb{F}_q^k| = q^k$.

ϵ-Universal (n, q^k, q) hash family

- A hash function is a map $f : \mathbb{F}_q^k \to \mathbb{F}_q$.
- A hash family $F = \{f_1, \ldots, f_n\}$ is called ϵ-Universal, if the $f \in F$ is chosen uniformly at random, then the probability $Pr[f(w) = f(w')]$ that any two distinct words $w, w' \in \Sigma^k$ collide under f is at most ϵ

$$Pr[f(w) = f(w')] \leq \epsilon.$$

- The parameter ϵ is often referred to as the collision probability of the hash family F.
- The case of $\epsilon = 1/n$ is known as universal hashing.

ϵ-Universal Hash Family

q — prime, $\mathbb{F}_q$ — field, $K = |\mathbb{F}_q^k|$.

A hash function is a map $f : \mathbb{F}_q^k \to \mathbb{F}_q$.

ϵ-Universal hash family

A hash family $F = \{f_1, \ldots, f_n\}$ is called ϵ-Universal, if for any two distinct words w, w':

$$|\{f \in F : f(w) = f(w')\}| \le \epsilon n.$$

F – ϵ-U $(n; K, q)$

Quantum hashing via classical hashing constructions

- Let $F = \{f_1, \dots, f_N\}$ be an ϵ-U $(N; |\Sigma^k|, q)$ hash family

$$f_i : \Sigma^k \to \mathbb{F}_q.$$

- Let $H = \{h_1, \dots, h_T\}$

$$h_j : \mathbb{F}_q \to \mathbb{F}_q.$$

  be an δ-R $(q, \log T + \ell)$ quantum hash generator.
- Define composition $G = F \circ H$ of families F and H

$$G = \{g_{ij}(w) = h_j(f_i(w)) : i \in \{1, \dots, N\}, j \in \{1, \dots, T\}\},$$

Theorem

ArXiv http://arxiv.org/abs/1404.1503
$G = F \circ H$ is an Δ-R $(|\Sigma^k|, s)$ quantum hash generator, where

$$\Delta \leq \epsilon + \delta \quad \text{and} \quad s = \log N + \log T + \ell.$$

Quantum hashing based on Freivalds' fingerprinting 1979

For $w \in \{0,1\}^k$ (also $w \in \mathbb{F}_{2^k}$), for the i-th prime p_i a function

$$f_i : \{0,1\}^k \to \mathbb{F}_{p_i} \qquad f_i(w) = w \pmod{p_i}.$$

is a fingerprint of w.

Freivalds 1979

- Pick $c > 1$, pick $M = ck \ln k$.
- $\pi(M)$ – the number of primes less than or equal to M.
- $\pi(M) \sim M/\ln M$ as $M \to \infty$.
- The set

$$F_M = \{f_1, \ldots, f_{\pi(M)}\}$$

of fingerprints is a $(1/c)$-U $(\pi(M); 2^k, M)$ hash family.

Quantum hashing based on Freivalds' fingerprinting

Theorem

1. Let $c > 1$, let $M = ck \ln k$. Let $F_M = \{f_1, \dots, f_{\pi(M)}\}$ be a $(1/c)$-U $(\pi(M); 2^k, M)$ hash family.
2. Let $q \in \{M, \dots, 2M\}$ be a prime, let $\delta > 0$. Let $H_{\delta,q} = \{h_1, \dots, h_T\}$ be an δ-R $(q, \log T + 1)$ quantum hash generator.

Then family $G = F_M \circ H_{\delta,q}$ is a Δ-R $(2^k; s)$ quantum hash generator, where

$$\Delta \leq \frac{1}{c} + \delta \qquad s \leq \log ck + \log\log k + \log\log q + 2\log 1/\delta + 3.$$

Lower bond

$$s \geq \log k + \log\log q - \log\log\left(1 + \sqrt{2/(1-\delta)}\right) - 1.$$

Quantum hashing from universal linear hash family

1979-1980

Let $k > 0$ – integer, q – prime power, $\mathbb{X} = (\mathbb{F}_q)^k \backslash \{(0, \ldots, 0)\}$.
For every vector $a \in (\mathbb{F}_q)^k$ define hash function $f_a : \mathbb{X} \to \mathbb{F}_q$ by the rule

$$f_a(w) = \sum_{i=1}^{k} a_i w_i.$$

Then

$$F_{lin} = \{f_a : a \in (\mathbb{F}_q)^k\}$$

is an $(1/q)$-U $(q^k; (q^k - 1); q)$ hash family (universal hash family).

Quantum hashing from universal linear hash family

Theorem

For arbitrary $\delta \in (0,1)$ composition $G = F_{lin} \circ H_{\delta,q}$ is a Δ-R $(q^k; s)$ quantum hash generator with $\Delta \leq (1/q) + \delta$ and

$$s \leq k \log q + \log \log q + 2 \log 1/\delta + 3.$$

Lower bound

$$s \geq \log k + \log \log q - \log \log \left(1 + \sqrt{2/(1-\delta)}\right) - 1.$$

This lower bound shows that the quantum hash function ψ_G is not asymptotically optimal in the sense of number of qubits used for the construction.

ϵ-Universal Hash Family

q — prime, $\mathbb{F}_q$ — field, $K = |\mathbb{F}_q^k|$.

A hash function is a map $f : \mathbb{F}_q^k \to \mathbb{F}_q$.

ϵ-Universal hash family

A hash family $F = \{f_1, \ldots, f_n\}$ is called ϵ-Universal, if for any two distinct words w, w':

$$|\{f \in F : f(w) = f(w')\}| \leq \epsilon n.$$

F – ϵ-U $(n; K, q)$

Error Correcting Codes

q — prime, $\mathbb{F}_q$ — field.

$[n, k, d]_q$ linear code

$[n, k, d]_q$ linear error correcting code with Hamming distance at least d.

$$\mathcal{C} : \mathbb{F}_q^k \to \mathbb{F}_q^n, \qquad \mathcal{C} = \{C(w_1), C(w_2), \ldots, C(w_{|q^k|})\}$$

ϵ-Universal Hash Family and Error Correcting Codes

Theorem (Bierbrauer, Johansson, Kabatianskii 1994)

1. If there exists an $[n, k, d]_q$ code, then there exists an ϵ-Universal (n, q^k, q) hash family with

$$\epsilon \leq \left(1 - \frac{d}{n}\right).$$

   Conversely.

2. If there exists an ϵ-Universal (n, q^k, q) hash family, then there exists an $[n, k, d]_q$ code with

$$d = n(1 - \epsilon).$$

ϵ-Universal Hash Family and Error Correcting Codes

q — prime, $\mathbb{F}_q$ — field.

ϵ-Universal Hash Family

- $f : \mathbb{F}_q^k \to \mathbb{F}$
- $F = \{f_1, \ldots, f_n\}$
- F — ϵ-Universal $(n; k, q)$, if for any two distinct words $w, w' \in \mathbb{F}_q^k$:

$$|\{f \in F : f(w) = f(w')\}| \leq \epsilon N.$$

$d \geq n - \delta n.$

Theorem

Quantum hash functions based on error correcting codes

Theorem

Let $\mathcal{C}$ – be a linear $[n, k, d]_q$ ECC

$$\mathcal{C} : \mathbb{F}_q^k \to \mathbb{F}_q^n.$$

Then for arbitrary $\delta \in (0, 1)$ there exists Δ-R $(q^k; s)$ quantum hash generator G, where

$$\Delta = (1 - d/n) + \delta,$$

$$s \leq \log n + \log \log q + 2 \log 1/\delta + 4.$$

Proof idea. Having $[n, k, d]_q$ ECC $\mathcal{C}$ one can construct $(1 - d/n)$-U $(n; q^k; q)$ hash family $F_{\mathcal{C}}$. J. Bierbrauer, T. Johansson, G. Kabatianskii, B. Smeets 1994

Quantum hash functions based on $[n, k, d]_q$ RS-code

q – prime power, $k \leq n \leq q$. A common special case is $n = q - 1$. Each word $w \in (\mathbb{F}_q)^k$, $w = w_0 w_1 \ldots w_{k-1}$ associated with the polynomial

$$P_w(x) = \sum_{i=0}^{k-1} w_i x^i.$$

$$C_{RS} : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n \quad w \mapsto C_{RS}(w) = (P_w(1) \ldots P_w(n))$$

$(k-1)/q$-U $(q; \mathbb{F}_q^k; q)$ hash family $F_{RS} = \{f_a : a \in A\}$ For $a \in \mathbb{F}_q \backslash 0$ define f_a

$$f_a : (\mathbb{F}_q)^k \to \mathbb{F}_q \quad f_a(w_0 \ldots w_{k-1}) = \sum_{i=0}^{k-1} w_i a^i.$$

Quantum hash functions based on Reed-Solomon codes

Theorem.

Let q be a prime power and let $1 \le k \le q$. Then for arbitrary $\theta \in (0,1)$ there is a δ-R (q^k, s) quantum hash generator G_{RS} such that $\delta \le \frac{k-1}{q} + \theta$ and $s \le \log(k \log q) + 2\log 1/\theta + 4$.

- If we select $n \in [ck, c'k]$ for constants $c < c'$, then $\Delta \le 1/c + \delta$ for $\delta \in (0,1)$ and

$$s \le \log(q \log q) + 2\log 1/\Delta + 4.$$

Lower bound

$$s \ge \log(q \log q) - \log\log\left(1 + \sqrt{2/(1-\Delta)}\right) - \log c'/2$$

Thus, Reed Solomon codes provides good enough parameters for resistance value Δ and for a number s of qubits we need to construct quantum hash function ψ_{RS}.

Explicit constructions of G_{RS} and $\psi_{G_{RS}}$.

Let $H_{\delta,q} = \{h_1, \ldots, h_T\}$, where $h_j : \mathbb{F}_q \to \mathbb{F}_q$ and $T = \lceil (2/\delta^2) \ln 2q \rceil$.
composition

$$G_{RS} = F_{RS} \circ H_{\delta,q} = \{g_{j\,i} = h_j(f_{a_i}) : j \in [T], i \in [n]\}$$

For $s = \log n + \log T + 1$ defines function $\psi_{G_{RS}}$ for a word $w \in (\mathbb{F}_q)^k$ by the rule.

$$\psi_{G_{RS}}(w) = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle \otimes \left(\frac{1}{\sqrt{T}} \sum_{j=1}^{T} |j\rangle |\psi_{g_{ji}}(w)\rangle \right).$$

$$= \frac{1}{\sqrt{nT}} \sum_{i=1,j=1}^{n,T} \underbrace{|i\rangle|j\rangle}_{\log n + \log T} \otimes \underbrace{\left(\cos \frac{2\pi h_j(f_{a_i}(w))}{q} |0\rangle + \sin \frac{2\pi h_j(f_{a_i}(w))}{q} |1\rangle \right)}_{|\psi_{g_{ji}}(w)\rangle \text{ -- one qubit}}.$$

Application for Digital Signature. Lamport scheme (Quantum variant)

1. Alice private keys:
   - a word $w = \sigma_1 \dots \sigma_k$ for the bit 0
   - a word $v = \sigma'_1 \dots \sigma'_k$ for the bit 1.
2. Alice prepares two pairs – public key (quantum state) and a classical bit:

   $$(|\psi(w)\rangle, 0) \qquad \text{and} \qquad (|\psi(v)\rangle, 1)$$

   by preparing states $\psi : |0\rangle, w \mapsto |\psi(w)\rangle$ and $\psi : |0\rangle, v \mapsto |\psi(v)\rangle$
3. Alice sends pairs $(|\psi(w)\rangle, 0)$ and $(|\psi(1)\rangle, 1)$ to Bob.
   Bob keeps these pairs.
4. Sign procedure:
   - Alice decided to sign the bit 1. Then
   - Alice sends (classical) pair $(v, 1)$ to Bob.
5. Verifying Signature: Bob using v Reverse $|\psi(v)\rangle$ to $|\psi\rangle$.
   Bob verify whether $|\psi\rangle = |0\rangle$.

Double key Signature. (Quantum variant)

$\psi : \mathbb{Z}_n \to (\mathcal{H}^2)^{\otimes s}$ – public Quantum Hash Function (QHF)

1. Alice private key:
   - an element $a \in \mathbb{Z}_n$
2. Alice public key (quantum state) $|\psi(a)\rangle$
3. Alice sends $|\psi(a)\rangle$ to Bob.
4. Alice Sign procedure:
   - message $m \in \mathbb{Z}_n$,
   - Signature equation $x + m = a$.
   - second private key x, second Public key $|\psi(x)\rangle$.
   - Pair (message,signature) is $(m, |\psi(x)\rangle)$.
5. Bob

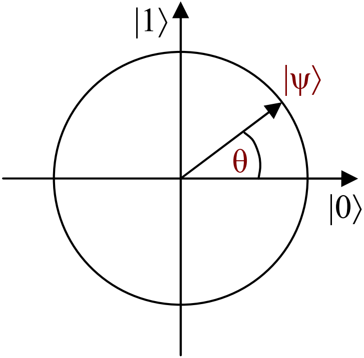
   Verifying Signature: using m computes state $|\psi(x+m)\rangle$ verify whether $|\psi(a)\rangle = |\psi(x+m)\rangle$.

The probability $Pr[y = a]$ to find $y = a$ from $|\psi(a)\rangle$ ($y = x$ from $|\psi(x)\rangle$)

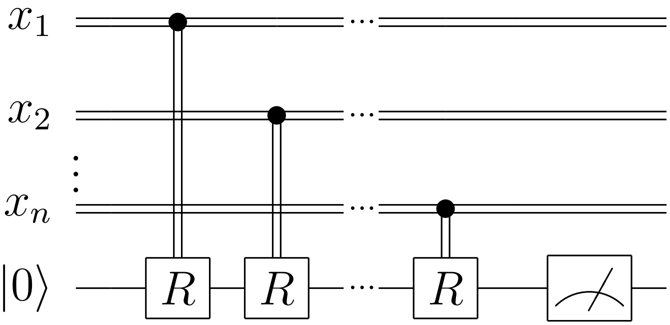
$$Pr[y = a] = \log |\mathbb{Z}_n| / |\mathbb{Z}_n|.$$

How to compute $|\psi(w)\rangle$ – one qubit quantum function

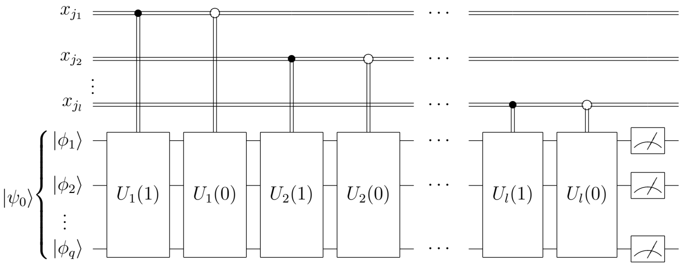
$$|\psi(w)\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle = \cos\left(\frac{2\pi w}{2^k}\right)|0\rangle + \sin\left(\frac{2\pi w}{2^k}\right)|1\rangle,$$



Computational model



Computational model – Quantum Branching Program – quantum case of Algebraic Branching Program



$$\mathbf{cNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathbf{cNOT}\ \psi = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \delta \\ \gamma \end{pmatrix}$$