DOI: 10.18372/2410-7840.19.11479
УДК 004.056.55+530.145

КВАНТОВИЙ ОДНОНАПРАВЛЕНИЙ СУМАТОР

Ростислав Гончарук

В статті наведені результати аналізу структури, функціональності та криптографічних властивостей однонаправленного суматора, а також можливостей його практичного застосування у схемах цифрових підписів, анонімних облікових системах, протоколах часових міток тощо. Вперше формально визначено поняття квантового однонаправленого суматора – криптографічного примітиву, що дозволяє об'єднати великий набір значень в одне, так, що маючи деяке значення-свідок буде можливість перевірити належність кожного із значень до загальної групи та забезпечує значну стійкість за допомогою законів квантової фізики. Побудовано однонаправлений суматор – Q-OWA та досліджено його властивості; доведено, що побудований примітив Q-OWA є квантовим однонаправленим суматором. На основі суматора Q-OWA побудовано динамічний квантовий суматор, що має окрім властивостей однонаправленого суматора можливість додавати нові, або видаляти старі значення без необхідності загального обрахування суматору.

Ключові слова: *захист інформації, криптографічний однонаправлений суматор, квантові відбитки, квантова геш-функція.*

Вступ. В роботі Бенало та де Маре 1993 року [1] вперше представлено криптографічний примітив – однонаправлений суматор, зазначено його базову структуру, функціональність та криптографічні властивості. Згідно з [1] однонаправлений суматор – це криптографічний примітив, який дозволяє об'єднати великий набір значень в одне, так, що маючи деяке значення-свідок можна перевірити чи включений якийсь певний елемент із набору до загального результату суматора.

Аналіз літератури. У роботах [2, 3, 4, 5] однонаправлені суматори були більш детально вивчені та запропоновано їх використання у схемах цифрових підписів, анонімних облікових системах, протоколах часових міток тощо.

В роботі [3] 2002 року було введено більш складне поняття – динамічні суматори, які дозволяють легко видаляти і додавати елементи до суматора. Запропонований варіант забезпечує значно більшу гнучкість у роботі з елементами суматора, дозволяючи змінювати ці елементи без необхідності розкривати ті, що вже були включені до суматора.

Мета. Введення поняття нового криптопримітива квантового однонаправленого суматора, побудова прикладу квантового суматора, для доведення існування криптопримітиву, аналіз класичних однонаправлених суматорів, та функції квантових відбитків, для доведення властивостей однонаправленності та квазікомутативності створеного прикладу. А також побудувати динамічний квантовий однонаправлений суматор з можливістю додавання та видалення значень без необхідності загального обрахування суматору.

В даній роботі вперше формалізовано новий криптографічний примітив – квантовий однонаправлений суматор, який може використовуватися, наприклад, в схемах квантових електронних грошей. Стійкість цих схем ґрунтуватиметься на фундаментальних законах квантової фізики та теорії квантової інформації, на відміну від більшості класичних схем електронних грошей, стійкість яких ґрунтується переважно на обчислювальній потужності зловмисника.

1. Постановка задачі. Наведемо ряд необхідних означень для подальшого визначення поняття квантового однонаправленого суматора:

Визначення 1 [1]**.** Назвемо *множиною однонаправлених геш-функцій* $\{h_l\}_{l\in\mathbb{N}}$ для приблизно рівних множин $|X_l| \approx |Y_l| \approx |Z_l|$ нескінченний набір функцій $h_l: X_l \times Y_l \to Z_l$, кожна з яких має наступні властивості:

1. Існує поліном P_l такий, що для кожного натурального значення l, можна обчислити значення функції $h_l(x, y)$ за час обмежений зверху значенням $P(\mathrm{Max}(l, |x|, |y|))$ для будь-якого значення $x \in X_l$ та для будь-якого значення $y \in Y_l$;

2. Не існує поліному P_k такого, що існує ймовірнісний поліноміальний алгоритм, який для достатньо великого натурального значення k, за заданими значеннями k, пари $(x, y) \in X_k \times Y_k$ та $y' \in Y_k$ може знайти значення $x' \in X_k$ такий, що $h_k(x,y) = h_k(x',y')$ з ймовірністю більшою за

1/ $P_k(\text{Max}(k, |x|, |y|))$, де пара (x, y) обрані рівноімовірно серед усіх елементів X_k xY_k і y' рівноімовірно із Y_k.

Назвемо функцію $h: X$ x $Y \to X$ *квазікомутативною*, якщо для будь-якого значення x $\in X$, і для будь-яких з значень $y_1, y_2 \in Y$ виконується рівність:

$$h(h(x, y_1), y_2) = h(h(x, y_2), y_1).$$

Криптографічний однонаправлений суматор – це множина однонаправлених геш-функцій кожна з яких є квазікомутативною.

Визначення 2 [6]. Нехай функція ψ є функцією, яка приймає на вхід класичну інформацію у вигляді скінченного двійкового рядка, а повертає значення одного з квантових станів $\psi: \{0, 1\}^n \to H^{2s}$, де H^{2s} – це 2^s вимірний простір Гільберта, який є простором станів системи з s кубітів, кожний з яких описується простором H^2.

Тоді функція ψ називається квантово однонаправленою якщо:

1. Існує поліноміальний(відносно вхідних даних та кількості квантових вентилів) алгоритм, який для вхідних даних $\omega \in \{0, 1\}^n$ обчислює значення $|\psi(\omega)\rangle$.

2. Для відомого значення стану $|\psi(\omega)\rangle$ знаходження ω є складним у квантовій моделі обчислень завдяки законам квантової інформаційної теорії.

Це забезпечує наступну властивість – якщо n >> s тоді маючи $|\psi(\omega)\rangle$ обчислювано неможливо знайти прообраз ω.

Функція $\psi: \omega \to |\psi(\omega)\rangle$ являється δ-стійкою, якщо для будь якої пари вхідних значень ω, $\omega' \in \{0, 1\}^n$, $\omega \neq \omega'$ вихідне значення скалярного добутку ω **та** ω' буде δ-ортогональним: $|\langle\psi(\omega)|\psi(\omega')\rangle| < \delta$.

Функція $\psi: \{0, 1\}^n \to H^{2s}$ називається *(n, s, δ)* – квантовою геш-функцією, якщо вона є квантово однонаправленою та має δ-стійкість.

2. Квантовий однонаправлений суматор. Використовуючи наведене вище введемо поняття квантового однонаправленого суматора.

Визначення 3. Нехай $X = \{0,1\}^n$ – множина двійкових рядків довжини n, $\Gamma = H^{2s}$ – простір з s-квантових станів з простору Гільберта H^2, та існує однонаправлена та квазікомутативна функція $h(x, \psi)$ виду $h: X$ x $\Gamma \to \Gamma$.

Назвемо множину таких функцій $z = \{h(x,\psi): X \times \Gamma \to \Gamma\}$ – квантовий однонаправлений суматор.

Щоб довести можливість існування квантового однонаправленого суматору побудуємо його приклад. Для цього наведемо визначення квантових відбитків, які можуть мати необхідні властивості однонаправленності та квазікомутативності.

Визначення 4 [7]. Припустимо, що для фіксованих значень **c** > 1 і **δ** <1 є коригуючий помилки код $E: \{0,1\}^n \to \{0,1\}^m$, для кожного **n**, де m = cn. Відстань Хеммінга між різними кодовими словами E(x) і E(y), дорівнює (1 − δ)m. Доречне використання кодів Юстесена $E_i(x)$, які дають відстань Хеммінга $\delta < 9/10 + 1/(15c)$ для будь-якої обраної константи **c** > 2. Тепер, при будь-якому виборі n, визначимо (log(m) + 1)-кубітів як $|h_x$ тоді: $|h_x\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle|E_i(x)\rangle$ для кожного x $\in \{0,1\}^n$ – це квантовий відбиток двійкового рядку x.

Щоб забезпечити неможливість знайдення прообразу наведемо визначення границі Холево.

Визначення 5 [8]. Нехай $\{q_1, q_2, ..., q_n\}$ – набір переплутаних квантових станів, також нехай q_x – один із цих станів, обраний згідно з розподілу ймовірностей P = $\{p_1, p_2, ..., p_n\}$. Тоді, для будь якого вимірювання описаного операторами POVM (операторами вимірювання) та виконаних над q_x, кількість доступної інформації про змінну x знаючи результат вимірювання Y обмежена наступною границею: $I(X,Y) \leq S(p) - \sum_i p_i S(p_i)$, де $p = \sum p_i p_i$ та S(.) ентропія фон Неймана.

Дана границя забезпечує той факт, що неможливо із log(n) кубітів, що були використані для кодування n класичних біт, отримати більше ніж O(log(n)) класичних біт інформації.

Квантові бінарні програми [9]– це прототип реалізації майбутнього квантового комп'ютера, який складається з квантової частини для обчислень, та класичної частини для керування обчисленнями.

За допомогою даного прототипу можлива побудова квантового суматора за поліноміальний час.

Визначення 6 [10]. Квантова бінарна програма Q над простором Гільберта H^d визначається як

$$Q = T, |\psi_0, M_{accept}\rangle,$$

де T – послідовність інструкцій $Tj = (t_i, Uj(0), Uj(1))$, які визначені змінними x_{i_j}, та $U_j(0), U_j(1)$ які є унітарними операторами у просторі H^d.

Використовуючи наведені вище визначення побудуємо квантовий однонаправлений суматор Q-OWA (quantum one-way accumulator).

Приклад 1. Нехай $X = \{0,1\}^n$ –множина двійкових рядків довжини n, $E_i(x)$ – коригуючий помилки код Юстесена, $\Gamma = H^{2S}$ – простір з s-квантових станів із простору Гільберта H^2, розмір s = log(n), та однонаправлена квазікомутативна функція $h: X \times \Gamma \to \Gamma$ визначена наступним чином:

$$h(x, \psi) = \frac{1}{\sqrt{s}} \sum_{i=1}^{s} (-1)^{E_i(x)} \alpha_i |i\rangle,$$

де x – це двійковий рядок із множини X, $|\psi\rangle = \sum_{i=1}^{s} \alpha_i |i\rangle$ – це набір квантових станів із простору Γ.

Далі, використовуючи квантові бінарні програми та границю Холево, доведемо властивість однонаправленості функції h.

Твердження 7. Існує поліном P_l такий, що для кожного натурального значення l може бути обчислено функцію $h_l(x, \psi)$ за час $P_l(\text{Max}(l, |x|, |\psi|))$ для будь-якого значення $x \in X_l$ та для будь-якого значення $\psi \in \Gamma_l$.

Доведення. Алгоритм для побудови квантового однонаправленого суматору, який використовує функцію квантових відбитків h, можна побудувати за допомогою квантової бінарної програми (див. рис. 1)

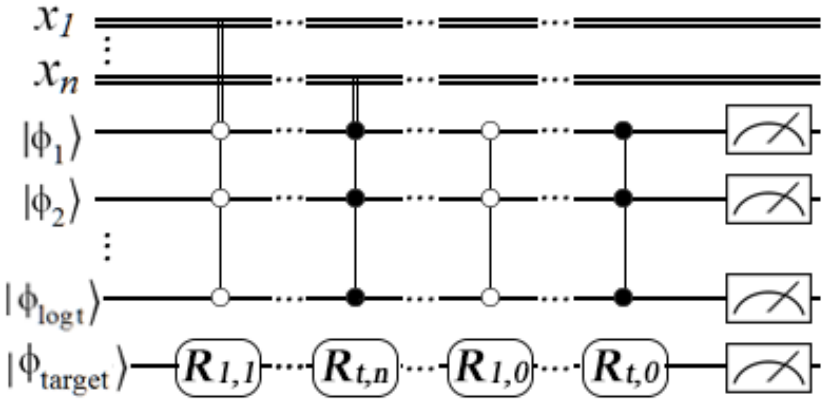

Рис. 1. Квантова бінарна програма для побудови квантових відбитків.

де $|\phi_{1,2,\ldots,\log t,target}\rangle$ – початкові стани квантової частини суматору, та $R_{i,j} = R\left(\frac{4\pi k_i c_j}{m}\right)$ – оператори повороту, які залежать від вхідних значень двійкових рядків $x_1, x_2, \ldots, x_n$, що діють на ці квантові стани. Доведено.

Твердження 8. Не існує поліному P_k такого, що існує ймовірнісний поліноміальний алгоритм, який для заданих натурального значення l, пари $(x, \Gamma) \in X_k \times \Gamma_k$ і $\psi' \in \Gamma_k$ зможе знайти $x' \in X_k$ такий, що $h_k(x, \psi) = h_k(x', \psi')$ з ймовірністю більшою за $1/P_l(\text{Max}(k, |x|, |\psi|))$, де пара (x, ψ) обрані з однаковою імовірністю серед усіх елементів $X_l \times \Gamma_l$.

Доведення. Так як для формування $O(\log n)$-кубітів, які представляють квантову частину суматора використовується n-бітів класичної інформації тоді, згідно з границею Холево, не більше ніж $O(\log n)$-бітів інформації обчислено, тобто ніхто не матиме можливості відтворити усі n біт. Доведено.

Твердження 9. Нехай $h: X \times \Gamma \to \Gamma$ і для будь-яких $\psi \in \Gamma$, $x_1, x_2 \in X$. Тоді виконується наступне: $h(h(\psi, x_1), x_2) = h(h(\psi, x_2), x_1)$.

Доведення. Нехай x_1, x_2 довільні значення з множини $X = \{0,1\}^n$, ψ довільне значення з простору $\Gamma = H^{2S}$ та функція h це квантовий відбиток виду:

$$h(x, \psi) = \frac{1}{\sqrt{s}} \sum_{i=1}^{s} (-1)^{E(x)} \alpha_i |i\rangle$$

тоді

$$h(h(\psi,\mathrm{x}_1),x_2)=h(\frac{1}{\sqrt{s}}\sum_{i=1}^{s}(-1)^{E(\mathrm{x}_1)}*a_i\,|\,i\rangle,x_2)=h(\frac{1}{\sqrt{s}}\sum_{i=1}^{s}(-1)^{E(\mathrm{x}_1)*\mathrm{E}(\mathrm{x}_2)}*a_i\,|\,i\rangle)$$

$$h(h(\psi,\mathrm{x}_2),x_1)=h(\frac{1}{\sqrt{s}}\sum_{i=1}^{s}(-1)^{E(\mathrm{x}_2)}*a_i\,|\,i\rangle,x_1)=h(\frac{1}{\sqrt{s}}\sum_{i=1}^{s}(-1)^{E(\mathrm{x}_2)*\mathrm{E}(\mathrm{x}_1)}*a_i\,|\,i\rangle)$$

Таким чином функція h є квазікомутативною:

$$h\left(h\left(\psi,x_1\right),x_2\right)=h\left(h\left(\psi,x_2\right),x_1\right).$$

Також, для побудови фукнції h використовуються квантові бінарні програми, згідно з якими в залежності від класичної частини суматору, двійкових рядків x_1, x_2, до набору квантових станів ψ застосовуються оператори повороту $R_{i,j}=R\left(\frac{4\pi k_i c_j}{m}\right)$. Так як поворот $R_{i,j}$ операція комутативна, і немає різниці у якому порядку його здійснювати – $h\left(h\left(\psi,x_1\right),x_2\right)$ або $h\left(h\left(\psi,x_2\right),x_1\right)$. – тоді усю функцію h можливо вважати квазікомутативною. Доведено.

3. Аналіз Q-OWA. Розглянемо властивості представленого криптопримітива Q-OWA та побудуємо динамічний криптографічний протокол на основі квантового однонаправленого суматора.

Визначення 7 [4]. Динамічний протокол на основі суматора складається із 7 алгоритмів (*Gen, Eval, Wit, Ver, Add, Del, Upd*), де:

– *Gen*, алгоритм генерування ключа, є ймовірнісним алгоритмом, що використовується для налаштування параметрів суматора. *Gen* приймає на вході λ параметрів безпеки і порогове значення N (верхню межу загального числа значень, які можуть бути надійно накопичені) і повертає ключ до суматора з відповідного ключового простору $\mathrm{K}_{\lambda,N}$;

– *Eval,* алгоритм накопичення значень, є ймовірнісним алгоритмом, що використовується для накопичення множини $L=\{y_1,...,y_{N'}\}$ з $N'\le N$ елементів з масиву ефективного домену Y_k, де k – певний ключ акумулятору від $\mathrm{K}_{\lambda,N}$.. *Eval* приймає в якості вхідного вектор $(k,y_1,...,y_{N'})$ і повертає накопичене значення (суматор) $z\in Z_k$ і деякі допоміжні факти aux, які будуть використовуватися іншими алгоритмами. Зверніть увагу, що кожне виконання *Eval* на той же вхід $(k,y_1,...,y_{N'})$ повинно давати один і той же накопичений суматор z, тоді як допоміжна інформація aux може відрізнятися;

– *Wit*, алгоритм вилучення свідку, є ймовірнісним алгоритмом, який приймає в якості вхідних параметрів ключ суматора $k\in\mathrm{K}_{\lambda,N}$, значення $y_i\in Y_k$ і допоміжну інформацію aux раніше отриману (разом з суматором z) по *Eval* $(k,y_1,...,y_{N'})$, і повертає або свідок w_i (від ефективного простору свідка W_k), що «доводить», що y_i був накопичений протягом z, якщо це дійсно так, або спеціальний символ $\perp$, якщо $y_i\neq\{y_1,...,y_{N'}\}$.

– *Ver*, алгоритм перевірки, який є детермінованим алгоритмом, що на вході (k,y_i,w_i,z), повертає Так/Ні відповідь згідно того чи є свідок w_i чинним посвідченням того, що y_i було накопичено в z чи ні.

– *Add*, алгоритм що додає новий елемент, крім того що, це (як правило, детермінований) алгоритм, який маючи ключ k суматора, значення $z\in Z_k$, отриманого у вигляді накопичення деякої множини L яка менше за N елементів із Y_k,, а інший елемент $y'\in Y_k$,, повертає новий акумулятор z', відповідно встановленої $L\cup\{y'\}$, поряд з новим свідком $w'\in\mathrm{W}_k$ для y' і деякі оновлення інформації $\mathrm{aux}_{\mathrm{Add}}$, яка буде використовуватися алгоритмом Upd;

– *Del,* алгоритм елемент видалення, є (як правило, детермінований) алгоритм, який отримуючи ключ k акумулятора, значення $z\in Z_k$, отриманого у вигляді накопичення деякої множини L елементів Y_k і елемент $y'\in L$, повертає новий акумулятор z' відповідний набору $L\setminus\{y'\}$, поряд з деякими оновлення інформації $\mathrm{aux}_{\mathrm{Del}}$, яка буде використовуватися алгоритмом Upd;

– *Upd*, алгоритм оновлення свідку, є детермінованим алгоритмом, що використовується для оновлення свідка $w\in\mathrm{W}_k$ для елемента $y\in Y_k$ раніше накопиченого в акумуляторі $z\in Z_k$, після додавання (чи видалення) елемента $y'\in Y_k\setminus\{y\}$ в (або з) z. *Upd* приймає в якості вхідного вектору $(k,y,w,b,\mathrm{aux}_{\mathrm{op}})$ (де *op* або *Add* або *Del*) і повертає оновлений свідок w', що «доводить» наявність у в оновленому акумуляторі z'.

Для побудови протоколу на основі квантового однонаправленого суматору Q-OWA алгоритм Gen має включати в себе формування параметру k в такий спосіб:

1. Вибір функції

$$h_k=\frac{1}{\sqrt{s}}\sum_{i=1}^{s}(-1)^{E_i(x)}\,\alpha_i\,|\mathrm{i}\rangle.$$

2. Вибір початкових станів кубітів ψ_0 із простору Гільберта H^{2s}.

Далі шляхом n-кратного використання функції h_k до $\psi_0, x_1,\ldots,x_n$, формується коротке значення $z \in Z_k$ яке включатиме у себе усі значення $x_1,\ldots,x_n \in X = \{0,1\}^n$.

Використання функції h_k зазначене у алгоритмі Eval:

Eval(k, $x_1,\ldots,x_n$):

0. Секретний параметр k це пара (h_k, ψ_0).
1. $z_0 \leftarrow \psi_0$.
2. $z_i \leftarrow h_k(z_{i-1}, x_i)$, $i = 1,\ldots,n$.
3. $z \leftarrow z_n$.
4. aux $\leftarrow (x_1,\ldots,x_n)$.

Результат алгоритму: пара (z, aux).

Для формування свідка w_i застосовується алгоритм Wit:

Wit(k, x_i, aux):

0. k = (h_k, ψ_0).
1. aux = $(x_1,\ldots,x_n)$.
2. Якщо $x_i \notin \{x_1,\ldots,x_n\}$ тоді алгоритм завершує роботу із результатом: помилка.
3. $L' \leftarrow \{x_1,\ldots,x_n\} \setminus \{x_i\}$.
4. $w_i \leftarrow$ Eval(k, L').

Результат алгоритму: w_i.

Для перевірки належності елемента x_i до сумматору z алгоритм Ver перевіряє рівність $h_k(w_i, x_i)$ та z.

Зазначені алгоритми свідчать про те, що на базі Q-OWA можливо створити базовий криптографічний протокол. Для того щоб даний протокол був динамічним зазначимо наступні 3 алгоритми.

Алгоритм Add – додавання нового члену x' до сумматору z нічим не відрізняється від процесу формування сумматору:

Add(k, z, x'):

1. $z' \leftarrow h_k(z, x')$.
2. $w' \leftarrow z$.
3. $aux_{Add} \leftarrow x'$.

Результат алгоритму: (z', w', aux_{Add}).

Можливість видалення елементу досягається за рахунок будови Q-OWA, так як стани квантової частини сумматору ψ залежать від двійкового рядку **x** і процес зміни цих станів полягає у застосуванні оператора повороту $R_{i,j} = R\left(\frac{4\pi k_i c_j}{m}\right)$. Тоді для видалення елементу необхідно інвертувати x і обчислити значення z від входу з інвертованим елементом **x**.

Алгоритм Del – видалення елементу x' із сумматору z:

Del(k, z, x'):

1. $x_{invert} \leftarrow$ Якщо $x' = \{b_1,\ldots,b_n\}$ тоді $x_{invert} = \{b_1',\ldots,b_n'\}$, де $b_i' = \begin{cases} 0, & якщо\ b_i = 1 \\ 1, & якщо\ b_i = 0 \end{cases}$.
2. $z' \leftarrow h_k(z, x_{invert})$.
3. $w' \leftarrow z$.
4. $aux_{Del} \leftarrow x'$.

Результат алгоритму: (z', w', aux_{Del}).

І останній алгоритм оновлення Upd, оновлення свідку w для старого елементу x після додавання або видалення нового елементу сумматора x':

Upd(k, x, w, op, aux_{op}):

Якщо op = Add

1. $w' \leftarrow$ Eval(w, aux_{op}).

Якщо op = Del

1. $aux_{invert} \leftarrow$ Якщо $aux_{op} = \{b_1,\ldots,b_n\}$ тоді $aux_{invert} = \{b_1',\ldots,b_n'\}$, де $b_i' = \begin{cases} 0, & якщо\ b_i = 1 \\ 1, & якщо\ b_i = 0 \end{cases}$.
2. $w' \leftarrow$ Eval(w, aux_{invert}).

Результат алгоритму: w.

Висновки. Використовуючи поняття однонаправленого сумматора вперше введено поняття нового криптопримітива – квантового однонаправленого сумматора стійкість якого ґрунтується на фундаментальних законах квантової фізики. Побудовано квантовий однонаправлений сумматор – Q-OWA, та доведено, що запропонована функція квантових відбитків, на основі якої побудовано сумматор, має властивості однаправленності та квазікомутативності. Також побудований динамічний квантовий сумматор на основі сумматора Q-OWA, що дозволяє великий набір значень об'єднати в одне, перевіряти належність кожного із елементів набору до загальної групи, та додавати нові, або видаляти старі значення без необхідності загального обрахування сумматору.

ЛІТЕРАТУРА

[1]. Benaloh J. One-Way Accumulators: A Decentralized Alternative to Digital Signatures / J. Benaloh, M. de Mare. // EUROCRYPT. – 1994. – №765. – pp. 274-285.

[2]. Fazio N., Cryptographic Accumulators: Definitions, Constructions and Applications / N. Fazio, A. Nicolosi // New York. – 2004.

[3]. Baric N., Collision-free accumulators and fail-stop signature schemes / Bari´c N. and B. Pfitzmann // Eurocrypt'97. – №1233. – 1997. – pp. 480-494.

[4]. Camenisch J., Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials / J. Camenisch, A. Lysyanskaya // In CRYPTO. – 2002. – pp. 61-76.

[5]. Nguyen. L., Accumulators from Bilinear Pairings and Applications. / Nguyen L. // CT-RSA. – 2005. – pp. 275-292.

[6]. Albayev F., Quantum hashing / F. Albayev, A. Vasiliev // 2013.
[7]. Buhrman H., Quantum fingerprinting. / H. Buhrman, R. Cleve, J. Watrous, R. de Wolf // Phys. Rev. Lett. – 2001. – №87. – pp. 15-16.
[8]. Holevo A., Some estimates of the information transmitted by quantum communication channel / A. Holevo // Probl. Inf. Transm. – 1973. – №9. – pp. 311.
[9]. Ablayev F., On computational power of quantum branching programs / F. Albayev, A. Gainutdinova // Lecture Notes in Computer Science. – 2001. – pp. 59-70.
[10]. Ablayev F., Algorithms for quantum branching programs based on fingerprinting / F. Albayev, A. Vasiliev // Electronic Proceedings in Theoretical Computer Science. – 2009. – vol. 9. – pp. 1-11.

REFERENCES

[1]. Benaloh J. One-Way Accumulators: A Decentralized Alternative to Digital Signatures / J. Benaloh, M. de Mare. // EUROCRYPT. – 1994. – №765. – pp. 274-285.
[2]. Fazio N., Cryptographic Accumulators: Definitions, Constructions and Applications / N. Fazio, A. Nicolosi // New York. – 2004.
[3]. Baric N., Collision-free accumulators and fail-stop signature schemes / Bari´c N. and B. Pfitzmann // Eurocrypt'97. – № 1233. – 1997. – pp. 480-494.
[4]. Camenisch J., Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials / J. Camenisch, A. Lysyanskaya // In CRYPTO. – 2002. – pp. 61-76.
[5]. Nguyen. L., Accumulators from Bilinear Pairings and Applications. / Nguyen L. // CT-RSA. – 2005. – pp. 275-292.
[6]. Albayev F., Quantum hashing / F. Albayev, A. Vasiliev // 2013.
[7]. Buhrman H., Quantum fingerprinting. / H. Buhrman, R. Cleve, J. Watrous, R. de Wolf // Phys. Rev. Lett. – 2001. – № 7. – pp. 15-16.
[8]. Holevo A., Some estimates of the information transmitted by quantum communication channel / A. Holevo // Probl. Inf. Transm. – 1973. – № 9. – pp. 311.
[9]. Ablayev F., On computational power of quantum branching programs / F. Albayev, A. Gainutdinova // Lecture Notes in Computer Science. – 2001. – pp. 59-70.
[10]. Ablayev F., Algorithms for quantum branching programs based on fingerprinting / F. Albayev, A. Vasiliev // Electronic Proceedings in Theoretical Computer Science. – 2009. – vol. 9. – pp. 1-11.

КВАНТОВЫЙ ОДНОНАПРАВЛЕННЫЙ СУММАТОР

В статье приведены результаты анализа структуры, функциональности и криптографических свойств однонаправленного сумматора, а также возможности его практического применения в схемах цифровых подписей, анонимных учетных системах, протоколах временных меток, схем электронных денег и так далее. Впервые формально определено понятие квантового однонаправленного сумматора – криптографического примитива, что позволяет объединить большой набор значений в одном, так, что имея некоторое значение свидетель будет возможность проверить принадлежность каждого из значений к общей группе и что обеспечит значительную устойчивость с помощью законов квантовой физики. Построено однонаправленный сумматор – Q-OWA и исследованы его свойства; доказано, что построенный примитив Q-OWA является квантовым однонаправленным сумматором. На основе сумматора Q-OWA построено динамический квантовый сумматор, что кроме свойств однонаправленного сумматора имеет возможность добавлять новые или удалять старые значения без необходимости перерасчета всего сумматора.

Ключевые слова: защита информации, криптографический однонаправленный сумматор, квантовые отпечатки, квантовая хеш-функция.

QUANTUM ONE-WAY ACCUMULATOR

Here presented analysis of the structure, function and properties of cryptographic one-way accumulator and possibility of its practical application in the digital signature scheme, anonymous credential systems, time stamps protocols, digital money and so on. First formally defined the concept of a quantum one-way accumulator - cryptographic primitive that allow you to combine a large set of values into one value, so that by having a witness you will be able to verify the ownership of each of the values from the total group and by that it would provide significant cryptographic security because of using the basic laws of quantum physics. Built quantum one-way accumulator – Q-OWA and studied its properties; proved that primitive built Q-OWA is a quantum one-way combiner. Based on the Q-OWA accumulator built dynamic quantum accumulator that in addition to the properties of the one-way accumulator has the ability to add or delete values without the need to recalculate the entire accumulator.

Keywords: information security, cryptographic one-way accumulator, quantum fingerprints, quantum hash function.

Гончарук Ростислав Ігорович, аспірант кафедри математичних методів захисту інформації ФТІ НТУУ «КПІ».
E-mail: rosstik@hotmail.com
Гончарук Ростислав Игоревич, аспирант кафедры математических методов защиты информации ФТИ НТУУ «КПИ».
Honcharuk Rostyslav, PhD student at PTI NTUU «KPI» (Kyiv, Ukraine).