УДК 621.391.41; 681.324-75; 65.012.8:004.492

Височіненко М. С., *аспірант*

СИСТЕМА УПРАВЛІННЯ КЛЮЧАМИ З ТЕОРЕТИЧНОЮ СТІЙКІСТЮ

Височіненко М. С. Системи управління ключами з теоретичною стійкістю. Визначення доказової обчислювальної складності доки залишається однією з найбільш важливих теоретичних і практичних проблем в криптології, постає проблема побудови практичних криптосистем з інформаційно-теоретичною стійкістю. В рамках вирішення цієї проблеми запропоновано концепцію керування криптосистемами з безумовною стійкістю на базі квантових системи управління ключами.

Ключові слова:КРИПТО-СИСТЕМА, УПРАВЛІННЯ КЛЮЧАМИ, ОБЧИСЛЮВАЛЬНА СКЛАДНІСТЬ, ІНФОРМАЦІЙНО-ТЕОРЕТИЧНА СТІЙКІСТЬ, КВАНТОВІ СИСТЕМИ

Высочиненко М. С. Системы управления ключами с теоретической стойкостью. Определение доказательной вычислительной сложности пока остается одной из наиболее важных теоретических и практических проблем в криптологии, встает проблема построения практических криптосистем с информационно-теоретической стойкостью. В рамках решения этой проблемы предлагается концепция управления криптосистемами с безусловной устойчивостью на базе квантовых системы управления ключами.

Ключевые слова: КРИПТО-СИСТЕМА, УПРАВЛЕНИЕ КЛЮЧАМИ, ВЫЧИСЛИТЕЛЬНАЯ СЛОЖНОСТЬ, ИНФОРМАЦИОННО-ТЕОРЕТИЧЕСКАЯ УСТОЙЧИВОСТЬ, КВАНТОВЫЕ СИСТЕМЫ

Vysochinenko M. S. Key management system with theoretical resistance. Definition of evidence-based computational complexity is still one of the most important theoretical and practical problems in cryptology; the problem arises of building practical cryptosystems with information-theoretical resistance. As part of this problem, the concept of crypto-systems control with unconditional stability on the basis of quantum key management system is proposed.

Key words: CRYPTOSYSTEM, KEY MANAGEMENT, COMPUTATIONAL COMPLEXITY, INFORMATION AND THEORETICAL STABILITY, QUANTUM SYSTEMS

Постановка завдання. Аналіз сучасних методів захисту інформації свідчить про те, що існує необхідність подальшого удосконалення методів захисту інформації, а також розробки науково-технічних застосувань по їх реалізації, розрахунків і оцінкам ефективності, побудові методик інженерно-технічних розрахунків [1...3].

Одним з перспективних напрямів в розвитку шляхів підвищення безпеки інформації в сучасних інформаційно-телекомунікаційних технологіях є імовірнісна криптографія, одним з напрямів якої є теорія кодового захисту (КЗ). В даний час теорія КЗ досить повно опрацьована для декількох застосувань, у тому числі для кодового регулювання інформаційної доступності в інформаційно-теоретичному розумінні. Захист інформаційних систем та, зокрема, систем електронного документообігу на основі криптокодових ключів представляє науково-технічний інтерес і потребує досконального вивчення.

Основними напрямами досліджень є такі завдання [4...6]:

– дослідження сутності теорії КЗ і можливості її використання для забезпечення безпеки систем електронного документообігу(СЕД);

– інформаційно-аналітичне моделювання передачі інформації через віртуальні канали зв’язку і віртуальні канали перехоплення інформації;

– розробка та отримання основних аналітичних співвідношень для розрахунку ефективності криптокодового захисту для унікальних повідомлень;

– оцінка ефективності захисту інформації за допомогою криптокодових ключів.

В даний час на практиці в якості імовірнісних потокових шифросистем широко використовуються потокові режими блокових шифрів, в яких рандомізація шифротекста досягається за рахунок випадкового вибору векторів ініціалізації [7], званих також синхропосилками, і передачі їх, як правило, у відкритому вигляді разом з криптограмою відкритого тексту. Іншим методом рандомізації шифротекста в блокових алгоритмах є додавання у відкритий текст наборів випадкових літер з шифруванням перетвореного тексту.

У статті дається визначення імовірнісної потокової шифросистеми, під яке підпадають всі відомі в літературі шифросистеми цього класу. За даним визначенням, можна побудувати багато нових імовірнісних потокових шифросистем. Також є можливість побудови стійких імовірнісних потокових шифросистем з нестійкими компонентами.

Сутність квантових систем управління ключами. У квантовій криптографії виділено два основні напрями розвитку систем розподілу ключів.

Перший напрям заснований на кодуванні квантового стану одиночної частки і базується на принципі неможливості розрізнити абсолютно надійно два неортогональні квантові стани. Довільний стан будь-якої дворівневої квантово-механічної системи можна представити у вигляді лінійної суперпозиції її власних станів $|\Psi|=\alpha|0|+\beta|1|$, де $|0|$ і $|1|$– власні стани системи; α і β–комплексні коефіцієнти,причому $|\alpha|^2+|\beta|^2=1$. Закони квантової механіки не дозволяють абсолютно надійно розрізнити два квантові стани $|\Psi_1|=\alpha_1|0|+\beta_1|1|$та $|\Psi_2|=\alpha_2|0|+\beta_2|1|$, якщо не виконана умова неортогональності, тобто – стани ортогональні.

Захищеність першого напряму ґрунтується на теоремі про заборону клонування невідомого квантового стану. Завдяки унітарності і лінійності квантової механіки, неможливо створити точну копію невідомого квантового стану без дії на вихідний стан. Нехай, наприклад, відправник (А) і одержувач (В) використовують для передачі інформації дворівневі квантові системи, кодуючи стани цих систем [8]. Якщо зловмисник (Е) перехоплює посланий (А) носій інформації, вимірює його стан і пересилає далі (В), то стан цього носія буде іншим, ніж до виміру. Таким чином, підслуховування квантового каналу призводить до помилок передачі, які можуть бути виявлені легальними користувачами. Основним протоколом квантового розподілу ключів є протокол BB84 .

Другий напрям розвитку заснований на ефекті квантового переплутування (заплутування). Дві квантово-механічні системи (у тому числі і розділені просторово) можуть знаходитися в стані кореляції, так що вимір вибраної величини, здійснюваний над однією з систем, визначить результат виміру цієї величини на іншій. Жодна із “заплутаних” систем не знаходиться в певному стані. Тому “заплутаний” стан не може бути записаний як прямий добуток станів систем. Стан двох часток із спіном 1/2 може служити прикладом “заплутаного”стану: $|\Psi_0\rangle=\frac{\|01|-\|10|}{\sqrt{2}}$. Вимір, проведений на одній з двох підсистем, дає з однаковою ймовірністю стани $|0|$ або $|1|$. Стан же іншої підсистеми буде протилежним, тобто $|0|$, якщо результат виміру на першій системі був $|1|$, і навпаки. Базовим протоколом квантового розподілу ключів на основі ефекту квантового заплутування є протокол EPR (Einstein-Podolsky-Rosen) (друга його назва – E91).

Базові принципи цих двох напрямів лягли в основу розробки всіх протоколів квантового розподілу ключів. Існує безліч протоколів квантової криптографії, заснованих на передачі інформації за допомогою кодування в станах одиночних фотонів, наприклад: BB84, B92, BB84(4+2), з шістьма станами, Гольденберга-Вайдмана, Коаші-Імото і їх модифікації. Єдиний протокол, розроблений для кодування інформації в сплутаних станах, – E91.

Квантовий протокол BB-84. Квантовий протокол BB-84 використовує 4 квантових стани фотонів, наприклад, напрям вектора поляризації, один з яких пункт (А) обирає в залежності від передаваного біта: 90° або 135° для «1», 45° або 0° для «0». Одна пара квантових станів відповідає $0\left(|0(+)|\right)$ та $1\left(|1(+)|\right)$і належить базису «+». Інша пара квантових станів відповідає $0\left(|0(\times)|\right)$ та $1\left(|1(\times)|\right)$і належить базису «×». Усередині обох базисів стани ортогональні, але ті, що складаються з різних базисів є попарно неортогональними (неортогональність необхідна для детектування спроб знімання інформації).

Квантові стани системи можна описати таким чином:

$$|0_\times| = \frac{1}{\sqrt{2}}\left(|0_+| + |1_+|\right); \qquad |1_\times| = \frac{1}{\sqrt{2}}\left(|0_+| - |1_+|\right).$$

Тут стани $|0_+|$ і $|1_+|$ кодують значення «0» і «1» в базисі «+», а $|0_\times|$ і $|1_\times|$ кодують ті ж значення в базисі «×». Базиси повернені один відносно одного на 45° (рис. 1).

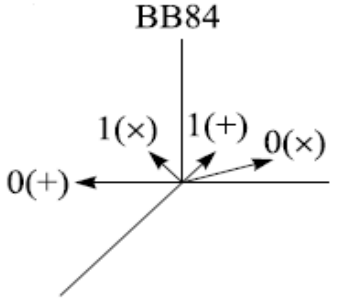

Рис. 1. Стани поляризації фотонів в протоколі BB84

Етапи формування ключів:

1) Пункт (A) випадковим чином вибирає один з базисів, потім усередині базису випадково вибирає один із станів відповідно«0» або «1» і посилає фотони (рис. 2).

2) Пункт (B) випадково і незалежно від пункту (A) вибирає для кожного прийнятого фотона прямолінійний (+) або діагональний (×) базис (рис. 3) і потім зберігає результати вимірів (рис. 4).

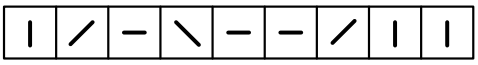

Рис. 2. Фотони з різною поляризацією

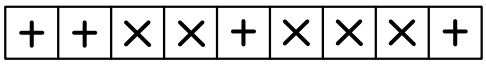

Рис. 3. Вибраний тип вимірів

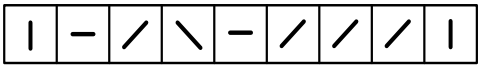

Рис. 4. Результати вимірів

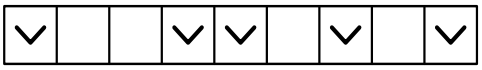

Рис. 5. Випадки правильних вимірів

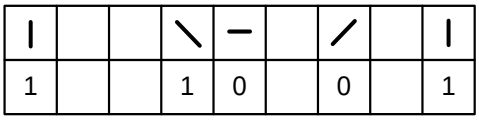

Рис. 6. Здобуття ключа за результатами правильних вимірів

3) Пункт (B) по відкритому загальнодоступному каналу зв'язку повідомляє, який тип вимірів був використаний для кожного фотона, тобто який був вибраний базис, але результати вимірів залишаються в таємниці.

4) Пункт (A) повідомляє пункт (B) по відкритому загальнодоступному каналу зв'язку, які виміри були вибрані відповідно до вихідного базису пункту (A) (рис. 5).

5) Далі користувачі залишають лише ті випадки, в яких вибрані базиси збіглися. Ці випадки переводять в біти (0 і 1), і отримують таким чином ключ (рис. 6).

Число випадків, в яких вибрані базиси збіглися, складатиме в середньому половину довжини вихідної послідовності. Приклад визначення кількості фотонів, прийнятих пунктом (B), показаний в табл. 1.

Таким чином, в результаті передачі ключа пунктом (B), в разі відсутності завад і спотворень будуть правильно зареєстровані в середньому 50% фотонів.

Формування квантового ключа по протоколу BB84 **Табл. 1**

Двійковий сигнал пункту (A)	0	1	0	1
Поляризаційний код пункту (A)	↔	↕	⤡	⤢
Детектування пунктом (B)	✥	✥	✥	✥
Двійковий сигнал пункту (B)	0	1	?	?

Проте ідеальних каналів зв'язку не існує і для передачі ключа необхідно провести додаткові процедури пошуку помилок і посилення секретності. Наприклад, при передачі через загальнодоступний канал зв’язку частини послідовності біт користувачів, в яких базиси збіглися, вони випадковим чином розкриваються і порівнюються. Далі розкриті біти відкидаються. У ідеальному квантовому каналі (без завад) досить виявити невідповідність в одній розкритій позиції для виявлення зловмисника. У реальній ситуації неможливо розрізнити помилки, викликані завадами чи діями зловмисника. Відомо, що якщо відсоток помилок QBER ≤ 11%, то користувачі з нерозкритою послідовністю, після корекції помилок через відкритий загальнодоступний канал зв'язку і посилення секретності, можуть

видобути секретний ключ, який буде у них однаковим і не буде відомий пункту Е. Ключ, отриманий до додаткових операцій з послідовністю, називається “сирим” ключем.

При корекції помилок ефективним способом для узгодження послідовностей (А) і (В) є їх “перемішування” для більш рівномірного розподілу помилок і розбиття на блоки розміром k, при якому ймовірність появи блоків з більш ніж однією помилкою нехтовно мала. Для кожного такого блоку сторони здійснюють перевірку парності. Блоки із співпадаючою парністю визнаються правильними, а решта діляться на декілька дрібніших блоків, і перевірка парності відбувається над кожним таким блоком, до тих пір, поки помилка не буде знайдена і виправлена [4, 9]. Процедура може бути повторена з блоками більш відповідного розміру. Найбільш дрібні блоки відкидаються за наявності в них помилки.

Коли в якому-небудь блоці кількість помилок виявиться парною, то навіть з оптимальним розміром блоку деякі з них можуть бути не виявлені. Для їх виключення застосовують перемішування послідовності біт, розбиття її на блоки і порівняння їх парності виконується ще декілька разів, кожного разу із зменшенням розміру блоків, до тих пір, поки (А) і (В) не прийдуть до висновку, що вірогідність помилки в отриманій послідовності дуже мала. В результаті всіх цих дій (А) і (В) отримують ідентичні послідовності біт. Ці біти і є ключем, за допомогою якого користувачі отримують можливість кодувати і декодувати секретну інформацію і обмінюватися нею по незахищеному каналу зв'язку.

Квантовий протокол E91(EPR). Протокол E91(EPR) був запропонований А. Екертом в 1991 році. Друга назва протоколу – EPR, оскільки він заснований на парадоксі Ейнштейна-Подольськи-Розена. У протоколі пропонується використовувати, наприклад, пари фотонів, що народжуються в антисиметричних поляризаційних станах. Перехоплення одного з фотонів пари не приносить пункту (Е) жодної інформації, але є для (А) і (В) сигналом про те, що їх розмова підслуховується. Ефект EPR виникає, коли сферично симетричний атом випромінює два фотони в протилежних напрямах у бік двох спостерігачів. Фотони випромінюються з невизначеною поляризацією, але через симетрію їх поляризації завжди протилежні. Важливою особливістю цього ефекту є те, що поляризація фотонів стає відомою лише після виміру. На основі EPR парадоксу А. Екерт запропонував протокол, який гарантує безпеку пересилки і зберігання ключа. Відправник генерує деяку кількість EPR фотонних пар. Один фотон з кожної пари він залишає для себе, другий посилає своєму партнерові. При цьому, якщо ефективність реєстрації близька до одиниці, то при здобутті відправником значення поляризації «1» його партнер зареєструє значення «0» і навпаки. Ясно, що таким чином партнери всякий раз, при необхідності, можуть отримати ідентичні псевдовипадкові кодові послідовності.

Нехай спочатку створюється N максимально заплутаних EPR-пар фотонів, потім один фотон з кожної пари посилається (А), а інший – (В). Три можливі квантові стани для цих EPR-пар представляються виразами:

$$|\psi_1| = \frac{1}{\sqrt{2}}\left(|0|_A|\frac{3\pi}{6}|_B - |\frac{3\pi}{6}|_A|0|_B\right); \quad (1) \qquad |\psi_2| = \frac{1}{\sqrt{2}}\left(|\frac{\pi}{6}|_A|\frac{4\pi}{6}|_B - |\frac{4\pi}{6}|_A|\frac{\pi}{6}|_B\right); \quad (2)$$

$$|\psi_3| = \frac{1}{\sqrt{2}}\left(|\frac{2\pi}{6}|_A|\frac{5\pi}{6}|_B - |\frac{5\pi}{6}|_A|\frac{2\pi}{6}|_B\right). \quad (3)$$

Вирази (1)...(3) можна привести до загального виразу:

$$|\psi_i| = \frac{1}{\sqrt{2}}\left(|0_i|_A|1_i|_B - |1_i|_A|0_i|_B\right). \quad (4)$$

Вираз (4) явно вказує, що кожен з цих трьох станів кодує біти «0» і «1» в унікальному базисі. Потім (A) і (B) здійснюють вимір на своїх частинах розділених EPR-пар, застосовуючи відповідні проектори: $P_1 = |0\|0|$; $P_2 = |\frac{\pi}{6}\|\frac{\pi}{6}|$; $P_3 = |\frac{3\pi}{6}\|\frac{3\pi}{6}|$.

Пункт (A) записує виміряні біти, а пункт (B) – їх доповнення до «1». Результати вимірів, в яких користувачі вибрали однакові базиси, формують “сирий ключ”. Для останніх результатів (A) і (B) проводять перевірку виконання нерівності Белла, як тест на присутність (E). Експерименти по реалізації даного протоколу почалися нещодавно. Їх проведення стало можливим після здобуття джерел “сплутаних пар” з високим ступенем кореляції і тривалим часом життя.У системах квантової криптографії в даний час застосовують три види кодування квантових станів: поляризаційне, фазове і кодування часовими зсувами.

При створенні практичних криптосистем, заснованих на квантовому поширенні ключа,виникають такі проблеми: *низька* швидкість передачі; *невеликі* відстані; *неможливість* створення квантових повторювачів; *інтенсивність* імпульсів квантів; *атаки* зловмисників на квантовий канал.

При формуванні передаваних імпульсів квантів доводиться вирішувати проблему їх інтенсивності. У теоретичній частині ми виходимо з припущення, що повідомлення передається і приймається імпульсами по одному кванту. На практиці такого результату досягти не вдається – джерело з ненульовою ймовірністю випромінюватиме більше одного фотона. Якщо квантів в імпульсі 1000, є ймовірність того, що 100 квантів по дорозі буде відведено зловмисником на свій приймач. Аналізуючи пізніше відкриті переговори між передавальною і приймаючою стороною, він може отримати потрібну йому інформацію. У ідеальному випадку число квантів в імпульсі має бути біля одного. Тут будь-яка спроба відведення частини квантів зловмисником приведе до істотного зростання числа помилок в приймаючої сторони. В цьому випадку прийняті дані мають бути відкинуті і спроба передачі повторена. Але, роблячи канал стійкішим до перехоплення, ми в цьому випадку стикаємося з проблемою “темнової” завади (видача сигналу у відсутності фотонів на вході) приймача (адже ми вимушені підвищувати його чутливість).

Імовірнісні системи. Всі шифросистеми можна розділити на два класи –імовірнісні і детерміновані. По-перше, результат шифрування залежить не лише від ключа шифрування і відкритого тексту, але і від деякого випадкового елементу – рандомізатора. Серед сучасних шифросистем більшість з них є детермінованими і лише одиниці – імовірнісними. В той же час відомо, що внесення елементу випадковості до процесу шифрування дозволяє набути наступних найважливіших властивостей шифросистеми [6]: *збільшується* складність проведення атак на основі виявлення статистичних закономірностей функції шифрування;*одному* і тому ж відкритому тексту, зашифрованому на одному і тому ж ключі, може відповідати багато різних шифротекстів, що робить неефективною атаку по словнику; *збільшується* складність проведення атак з відомим відкритим текстом, оскільки криптоаналітик може бути обмежений у необхідній кількості відкритого тексту (зашифрованого на одному ключі) для успішної реалізації атаки; *з'являється* додатковий параметр безпеки, змінюючи який можна керувати стійкістю схеми, з'являється можливість збільшення часу життя ключа.

До недоліків імовірнісного шифрування слід віднести збільшення довжини шифротексту в порівнянні з довжиною вихідного відкритого тексту і зменшення швидкості шифрування.

Під шифром далі розуміється будь-який набір з п'яти об'єктів Σ=(X, K, Y, E, D), де X – множини повідомлень (відкритих текстів), K – ключі, Y – криптограми (шифротексти), E і D – функції. Тобто, функції $E(K\times X) \rightarrow Y$, $D(K\times Y) \rightarrow X$, зв'язані співвідношенням оборотності $E(k, x)=y \Rightarrow D(k, y)=x$ для всіх $x \in X$ и $y \in Y$, званих функціями шифрувань і розшифрування, відповідно. Передбачається, що повідомлення, ключі, криптограми і рандомізатори є словами в деяких алфавітах. Алфавіт слів в деякій множині V позначається A_V. Передбачається також, що всякий ключ *k* в множині K представляється парою

взаємозалежних ключів k_1, k_2 так, що $k=(k_1, k_2)$, де k_1 є ключем шифрування: $y= E(k, x)= =E(k_1, x)$, а k_2 – ключем розшифрування: $D(k, y)=D(k_2, y=x$. В разі, якщо k_2 обчислюється по k_1 важко (з експоненціальною складністю), то Σ називається шифром з відкритим ключем, інакше – шифром із закритим ключем.

Схематично імовірнісна потокова шифрсистема (PSC) представлена на рис. 7. Вона складається з ключової системи K і блоків рандомізації Raта блоку шифрування En. Склад ключової системи не розкривається, її функція полягає у виробленні трійки ключів $k_i \in K_i$, $k_w \in K_w$ и $k_g \in K_g$, званих ключами, відповідно, ініціалізації, свідоцтва і генератора. Блок рандомізації складається з джерела (множини) рандомізаторів R і вузлів свідоцтва W і ініціалізації h.

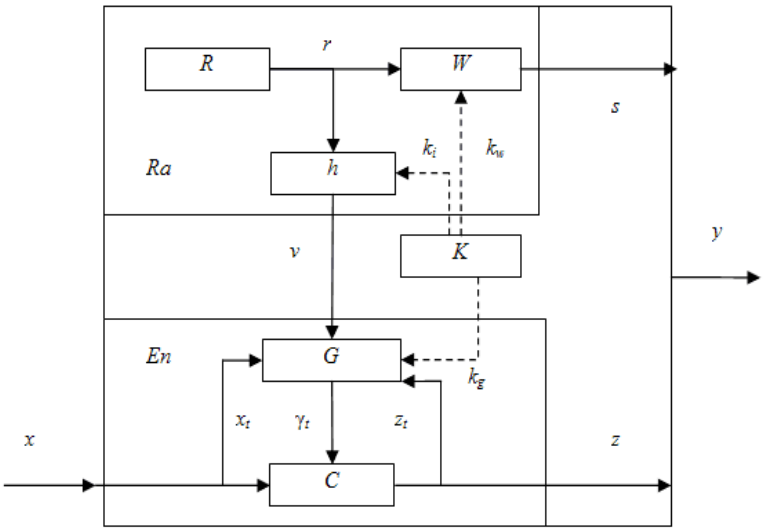

Рис. 7. Схема імовірнісної шифросистеми PSC

Формально *вузол свідоцтва* є де-яким шифром $W=(R, K_w, S, e', d')$. Він призначений для створення свідоцтва $s = e'(r, k_w) \in S$ ран-домізатора $r \in R$ залежно від ключа свідоцтва k_w.

Вузол ініціалізації формально є деякою функцією $h: R\times K_i \rightarrow A_X\times A_Z\times Q$. Він створює для блоку шифрування вектор ініціалізації $v=(x_0, z_0, q_0)=h(r, k_i)$.

Блок шифрування складається з генератора ключових потоків G, що є множиною кінцевих автоматів $M_k=(A_X\times A_Z, Q, \Gamma, \Psi_k, \varphi_k)$, $k\in Kg$, з вхідним алфавітом $A_X\times A_Z$, вихідним алфавітом Γ, множиною станів Q і функціями переходів і виходів відповідно Ψ_k: $(A_X \times A_Z) \times Q \rightarrow Q$та φ_k: $(A_X\times A_Z)\times Q \rightarrow \Gamma$, і шифра $C=(A_X, A_Z, \Gamma, e, d)$. При фіксованих ключах k_i, k_w и $k=k_g$ шифросистема PSC відправника відкритий текст $x=x_1 \ldots x_l \in X$ перетворить в шифротекст $z=z_1\ldots z_l \in Z$ таким чином: вибирається випадково рандомізатор $r\in R$, обчислюються його свідоцтво $s= e'(r, k_w)$, вектор ініціалізації $(x_0, z_0, q_0)=h(r, k_i)$, ключовий потік $\gamma=\gamma_1 \ldots \gamma_l$, де для будь-якого $t=1,\ldots l$; $\gamma_t= \varphi_k((x_{t-1}, z_{t-1}), q_t)$; $q_t= \Psi_k((x_{t-1}, z_{t-1}),), q_{t-1})$; $z_t = e(\gamma_t, x_t)$.

Пара (s, z) передається в канал зв'язку. Шифросистема PSC одержувача відновлює відкритий текст, обчислюючи послідовно $r=d'(s, k_w)$, $(x_0, z_0, q_0)=h(r, k_i)$ для $t=1,\ldots,l$.

PSC називається шифросистемою з *відкритим рандомізатором*, якщо $e'(r, k_t)=r$ для всіх $k_w \in K_w$, та із закритим рандомізатором, якщо при невідомому ключі k_w значення рандомізатора r важко обчислюється за його значенням $s=e'(r, k_w)$. PSC називається шифросистемою з *відкритим або закритим ключем*, якщо відповідно таким є шифр W в ній. Вона називається *синхронною*, якщо всі автомати M_k в G автономні: їх функції $\varphi_k((x, z), q)$ і $\Psi_k((x, z), q)$ залежать від (x, z) фіктивно, тобто є по суті функціями лише від q. В цьому випадку вважається, що значення функції h лежать в Q, тобто $h: R \times K_i \rightarrow Q$.

PSC називається шифросистемою із *закритим вектором ініціалізації*, якщо при невідомому ключі k_i значення $h(r, k_i)$ важко обчислюване по рандомізатору r. Вона називається шифросистемою з *тотожною ініціалізацією*, якщо $h(r, k_i) = r$ для всіх $k_i \in K_i$.

Багаточисельні приклади шифросистеми PSC різних типів можна отримати, вибираючи в ній різними способами компоненти W, G, C, h, K, R. Наприклад, при відповідних h, K, R в якості (W, G, C) в PSC можуть виступати комбінації: (AES, RC4 + mod 256), (RSA, BBS), (RSA, RSA), (LFSR+filter) та інші.

Прикладом шифросистеми із закритим вектором ініціалізації може слугувати PSC, в якій ключем k_i служить багаточлен $f(x)$ над кінцевим полем, оновлюваний після зашифрування не більш $n-1$ відкритих текстів, де n– степінь f; $h(r, k_i)=f(r)$. У інших PSC із закритим вектором ініціалізації в ролі h можуть використовуватися різні ключові хеш-функції [7].

Прикладами шифросистем з тотожною ініціалізацією є блокові шифри в режимі потокового шифрування, а також синхронні потокові шифри, побудовані на основі генераторів ключового потоку з функціональними блоками як закритий ключ. Розуміючи під стійкістю обчислювальну стійкість до атак з відомим відкритим текстом з метою визначення невідомого ключа, розглянемо шифрсистему PSC в припущенні, що вимозі стійкості задовольняє лише деякі з її компонент. Так, якщо стійкий генератор в *G*, то криптоаналітик, знаючи *x, s, z*, ключовий потік на виході генератора, не зможе обчислити вектор ініціалізації. За відсутності останнього він не може знати рандомізатора і не може провести ні атаку на *R* (з метою передбачення наступного рандомізатора), ні атаку з відомим відкритим текстом на *W*. Якщо ж стійкими є шифр *W* і джерело рандомізаторів *R*, то можна допустити нестійкий генератор *G*. Те ж саме можливо в разі однобічної функції *h*. Особливе місце в імовірнісних системах займає концепція відвідного каналу.

Висновки. За результатами проведеного дослідження можна зробити висновок, що основною вимогою до процедур корекції помилок і посилення секретності ключа є збереження якомога більшого числа біт у фінальному ключі, при чому виникає необхідність мінімізації числа обмінів через відкритий канал зв'язку в перерахунку на один біт в фінальному секретному ключі. Зрозуміло, що стартовий ключ може бути використаний для шифрування нового ключа і передачі його легітимному користувачеві,однак при цьому абсолютна секретність нового ключа гарантується лише, якщо його довжина не більше довжини ключа, на якому він шифрується. У квантовій криптографії стартовий ключ не використовується безпосередньо для передачі нового ключа по квантовому каналу зв'язку, а число біт відкритої інформації, переданої на один біт нового секретного ключа – менше одиниці, тому можливе розширення ключа. Підхід з невеликим стартовим ключем є кращим, оскільки при цьому можливо звести до мінімуму число раундів обміну по відкритому каналу зв'язку в процесі обміну і посилення секретності ключа. Основна задача зводиться до з'ясування довжини секретного ключа, який може бути отриманий при спостереженні за змінами статистики результатів вимірювань на приймальному кінці. Як правило величиною, яка характеризує відхилення статистики вимірювань від ідеальної, є величина ймовірності помилки,точніше ймовірності того, що переданий біт був «0», а зареєстрований як «1», і навпаки, хоча можливі й інші критерії для виявлення зміни статистики.

Література

1. Котенко В. В. Стратегия формирования виртуальных выборочных пространств ансамблей ключа при решении задач защиты информации / В. В. Котенко, С. В. Поликарпов // Вопросы защиты информации. – 2002. – №2. – С. 34-51.

2. Сидельников В.М. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона. / В. М. Сидельников, С. О. Шестаков. // Дискретная математика. – 1992. –Т.4. №3. – С. 120-148.

3. Исследование протоколов и механизмов защиты информации в компьютерных системах и сетях / А. А. Кузнецов,С. П. Евсеев, Б. П.Томашевский, Ю. И. Жмурко // Збірник наукових праць ХУ ПС. – 2007. – Вип. 2(14). – С. 28-52.

4. C. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing // in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (Institute of Electrical and Electronics Engineers, New York, 1984).

5. Ekert A. Quantum cryptography based on Bell's theorem // Phys. Rev. Lett. 67, 1991.

6. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography // J. Cryptology 5. – 1992.

7. C. H. Bennett. Quantum cryptography using any two non-orthogonal states // Phys. Rev. Lett. 68. – 1992.

8. Wyner A. D. The Wire-Tap Channel // Bell System Techn. J. – 1975. – V.54, № 8.

9. Питерсон У. Коды исправляющие ошибки / Питерсон У., Уэлдон Э. – М.: Мир, 1976. – 354 с.