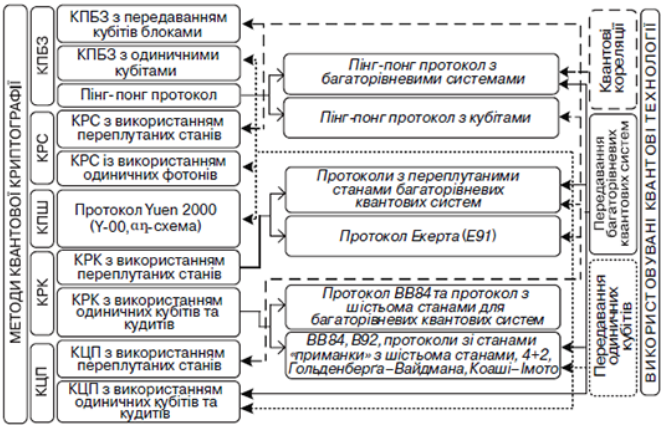
КВА́НТОВА КРИПТОГРА́ФІЯ — наука, що вивчає методи захисту систем зв'язку і базується на принциповій непорушності закономірностей квантової фізики, об'єкти якої забезпечують процеси безпечного передавання інформації між легітимними користувачами. Осн. засадами є постулат вимірювання (результат принципу невизначеності Гейзенберґа) та т. зв. теорема про заборону клонування. Принцип невизначеності — це фундам. нерівність (відношення невизначеностей), згідно з якою усі динам. параметри поділяють на 2 групи (перша — часові та простор. координати; друга — імпульс та енергія), при чому неможливо одночасно виміряти параметри з різних груп (напр., місцерозташування та енергію об'єкта). Теорема про заборону клонування стверджує неможливість створення точних (на 100 %) копій квант. об'єктів. Ці властивості не притаманні класич. системам зв'язку і забезпечують теор.-інформ. (абсолютну й безумовну) стійкість К. к. В останні роки знач. інтерес серед світ. наук. спільноти викликають системи захисту інформації на базі методів К. к. Вагоме місце посідає квант. розподіл ключів (КРК), також виокремлюють такі напрями, як квант. прямий безпеч. зв'язок (КПБЗ), квант. розділення секрету (КРС), квант. поток. шифр (КПШ), квант. цифр. підпис (КЦП) та квант. стеганографія (див. Рис.).

Рис. **Класифікація методів квантової криптографії**



Осн. терміни, що використовують у галузі К. к.: квант. система захисту інформації, у якій хоча б одна із задач розв'язується за допомогою квант. методів захисту інформації, — сукупність взаємопов'яз. заходів, засобів та методів, спрямов. на вирішення завдань захисту інформації (забезпечення конфіденційності, цілісності та доступності за умови впливу загроз природ. чи штуч. характеру, реалізація яких може завдати шкоди легітим. користувачам та власникам інформації); квант. метод захисту інформації — сукупність теор. принципів та практ. прийомів, що використовують властивості квантів, ґрунтуються на непорушності постулатів квант. фізики (механіки) і спрямов. на забезпечення захищеності базових характеристик інформації; квант — елементарна неподільна порція фіз. величини, яка є носієм певного типу взаємодії (напр., фотон, що є носієм електромагніт. взаємодії, фонон, гравітон тощо); кубіт — мін. величина квант. інформації (аналог у класич. інформації — біт), дворівнева квант. система, що на відміну від класич. біта може перебувати у стані суперпозиції (тобто приймати значення «1» та «0» у певний момент часу з певною ймовірністю). Математично кубіт є вектором у двовимір. гільбертовому просторі. Ідею використання квант. об'єктів для захисту інформації вперше запропонував 1970 С. Вайснер, 1984 Ч. Беннет (компанія IBM) та Ж. Брассар (Монреал. університет) розвинули її і запропонували перший протокол К. к. BB84, що став альтернат. і нетрадиц. вирішенням проблеми розподілу ключів шифрування (досить актуал. для криптографії). У ньому, як і в більшості протоколів з одинич. поляризов. фотонами, використовують 4 поляризов. стани фотонів (0º, 45º, 90º, 135º), що передаються квант. каналом зв'язку. Пошук та виправлення помилок виконують з використанням відкритого класич. каналу, який не повинен бути конфіденційним, а тільки аутентифікованим. Для виявлення факту дій зловмисника використовують процедуру контролю помилок, а для забезпечення теор.-інформ. стійкості — класичну процедуру підсилення секретності. Протокол BB84 вважають основоположником протоколів К. к., яких на сьогодні запропоновано вже кілька десятків. Нині існують декілька систем К. к., які вийшли на світ. ринок і позиціонуються як надійні системи розподілу ключів та криптограф. захисту інформації. Першим у світі комерц. рішенням К. к. була система QPN Security Gateway (QPN-8505), запропонована амер. компанією MagiQ Technologies (економічно вигідна, зорієнтована на уряд. та фінанс. організації). Вона пропонує захист VPN за допомогою КРК (бл. 100 ключів 256 біт за секунду на відстань до 140 км) та інтегров. шифрування. Система QPN-8505 використовує такі протоколи: квантовий BB84, традиційні 3DES (112 біт) та AES (256 біт). За допомогою цієї системи можна організувати захищену квант. мережу. Ін. ефектив. рішенням є система КРК Clavis[2] швейцар. компанії ID Quantique. Вона побудована на автокомпенсуючій оптич. платформі, завдяки чому забезпечується стабільність і низький рівень квант. помилок, що підтверджено числен. експериментами. За допомогою неї можна здійснювати захищений розподіл ключів шифрування між двома абонентами на відстань до 100 км. Крім того, компанія пропонує квант. систему Cerberis — сервер з автомат. створенням і секрет.

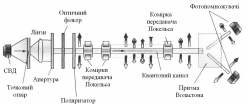
обміном ключами, захищеним оптоволокон. каналом (FC-1G, FC-2G та FC-4G). Ця система може розподіляти ключі на відстань до 50 км, а її характер. особливістю є 12 паралел. криптообчислень, що значно підвищує швидкодію. Система Cerberis використовує для шифрування протокол AES (256 біт), а для КРК — протоколи BB84 та SARG. На поч. 21 ст. британ. компанією Toshiba Research Europe Ltd представлено систему КРК Quantum Key Server, яка відрізняється простотою своєї архітектури та забезпечує генерацію бл. 100 ключів 256 біт за секунду та їхнє одностороннє передавання від передавача до приймача. До її складу входить інтегров. модуль автомат. керування, що проводить безперерв. моніторинг системи Quantum Key Server і регулює оптичні характеристики. Ін. британ. компанія QinetiQ запропонувала першу у світі комп'ютерну мережу, що використовує К. к., — Quantum Net (Qnet). Макс. довжина ліній зв'язку цієї мережі становить 120 км, та найголовнішим є те, що система Qnet — це перша квантово-криптограф. система, що використовує більше 2-х серверів (їх у цій системі 6, і всі вони є інтегрованими в Інтернет). Нині дослідження щодо розроблення квант. криптосистем інтенсивно проводять відомі у світі н.-д. інституції — Institute for Quantum Optics and Quantum Information, Northwestern University, SmartQuantum, BBN Technologies of Cambridge, TREL, NEC, Mitsubishi Electric, ARS Seibersdorf Research, Los Alamos National Laboratory та ін. В Україні теор. розробками займаються вчені у Нац. авіац. університеті, Нац. тех. університеті України «Київ. політех. інститут», Одес. академії зв'язку та Інституті фізики НАНУ (Київ). Ці дослідження переважно зорієнтовані на розроблення нових протоколів К. к., методів підсилення секретності існуючих протоколів, а також на моделювання процесів передавання (та перехоплення) інформації квант. каналами з шумом. Знач. внесок у розвиток К. к. зробили Ч. Беннет, Ж. Брассар, Є. Василіу, С. Гнатюк, О. Гомонай, А. Еккерт, С. Кілін, О. Корченко, С. Молотков, М. Нільсен, К. Румянцев, А. Семенов, В. Усенко, Д. Хорошко, А. Цайлінґер, І. Чанґ та ін.

Рекомендована література

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация / Пер. с англ. Москва, 2006;
2. Гомонай О. В. Лекції з квантової інформатики: Навч. посіб. В., 2006;
3. Василиу Е. В. Стойкость квантовых протоколов распределения ключей типа «приготовление–измерение» // Georgian Electronic Scientific J.: Computer Science and Telecommunications. 2007. № 2(13); Килин С. Я., Хорошко Д. Б., Низовцев А. П. Квантовая криптография: Идеи и практика. Минск, 2008;
4. Корченко О. Г., Василіу Є. В., Гнатюк С. О. Сучасні квантові технології захисту інформації // Захист інформації. 2010. № 1.

О. Г. Корченко

Фотоілюстрації



Бібліографічний опис:
Квантова криптографія / О. Г. Корченко // Енциклопедія Сучасної України [Електронний ресурс] / Редкол.: І. М. Дзюба, А. І. Жуковський, М. Г. Железняк [та ін.] ; НАН України, НТШ. — К. : Інститут енциклопедичних досліджень НАН України, 2012. — Режим доступу: https://esu.com.ua/article-11921. – Останнє поновлення : 2023.