30. В чому сутність вимог коректності та повноти до криптографічного протоколу? В чому сутність та які можливості криптографічного протоколу з нульовим розголошенням?

На цей час достатньою мірою розвинуті дві плідні математичні моделі доведення їх безпеки чи аналізу властивостей – інтерактивні системи доведення та системи доведення з нульовим розголошенням. Також в своїй більшості криптопротоколи можна поділити на інтерактивні протоколи та не інтеративні. Також окремо необхідно виділити протоколи з нульовим розголошенням (нульовими знаннями).

Відповідно під інтерактивною системою доведення, або (*P,V,S*) системою розуміється протокол взаємодії двох суб'єктів/об'єктів: *P* – пред'явник, що доводить, *V* – перевірник інформації пред'явника, *S* – твердження пред'явника, що перевіряється. У такій системі суб'єкт/об'єкт *P* хоче (повинен) довести *V*, що твердження *S* істинне. Також суб'єкт/об'єкт *V* самостійно не в змозі без участі пред'явника *P* перевірити, чому твердження *S* істинне. Суб'єкт *P* в цій моделі може бути й порушником, він може зробити спробу довести *V*, що твердження *S* істинне, хоча насправді воно є хибним.

Як зазначалося раніше, протоколи можуть бути інтерактивними або неінтерактивними. Інтерактивним протоколом називається протокол, під час виконання якого між суб'єктами, що виконують протокол, відбувається обмін даними. Неінтерактивний протокол – це протокол, під час виконання якого між суб'єктами, що виконують протокол, не здійснюється обмін даними. У свою чергу інтерактивні протоколи можна класифікувати за кількістю раундів (сеансів зв'язку) на одноразундові та багатораундові. Одноразундові протоколи вимагають не більше одного сеансу передачі даних. Багатораундові протоколи для виконання всіх встановлених протоколом дій вимагають 2 та більше раундів. Інтерактивний протокол може складатися з багатьох раундів обміну між суб'єктами/об'єктами повідомленнями, які отримали назву маркерів, та задовольняти, як мінімум, таким двом умовам:

1) *повнота* протоколу, сутність якої полягає в тому, що якщо *S* істинне, то суб'єкт/об'єкт *P* з великою ймовірністю переконає про це перевірника і той згодиться, що *S* істинне;

2) *коректність* протоколу, яка проявляється в тому, що якщо *S* хибне, то суб'єкт *V* виявить це з великою ймовірністю, тобто *P* не переконає *V*, що *S* істинне.

Згідно прийнятої моделі (*P,V,S*) протоколу вважалося, що *V* не може бути порушником. У разі якщо *V* є порушником і бажає отримати хоч якусь інформацію про те, чому *S* істинне, захист *P* від таких дій *V* може здійснюватися на основі застосування протоколу з нульовим розголошенням. У цьому випадку, крім уже вказаних вище вимог

повноти й коректності, протокол з нульовим розголошенням має задовольняти ще й такій умові:

- нульове розголошення інформації про S – у результаті виконання протоколу (P,V,S) перевірник не зменшує свою апріорну невизначеність відносно твердження S, тобто він на отримує ніякої інформації про те чому S істинне.

Забезпечення нульового розголошення на практиці може бути здійснене, якщо:

- кожен субєкт, який має намір діяти або як пред'явник P або як перевірник V, повинен мати засоби генерації випадкових чисел;
- абоненти групи мають дійти згоди щодо того, яка функція гешування буде використовуватися;
- кожен об'єкт, який має намір діяти як пред'явник, має бути забезпечений асиметричною ключовою парою, обраною згідно з рекомендаціями, які наведено вище;
- кожен об'єкт, який має намір діяти як перевірник, має бути забезпечений засобами обчислення довірчих копій відкритих ключів перевірки для об'єктів, чия ідентичність перевіряється.