Протокол автентифікації Шнора на основі ЦП

Протокол автентифікації Шнора на основі ЦП є вдосконаленням протокола Шнора. Вдосконалення спрямоване на те, щоб здійснювати автентифікацію за один прохід (раунд), отримавши можливість здійснення групової автентифікації, а також іншим чином генерувати випадковий запит e.

Шнор запропонував генерувати запит на основі використання в якості e значення функції гешування від певного повідомлення m. Вказане дозволило реалізувати криптографічний протокол за один прохід, в тому числі з груповою автентифікацією.

Генерування й розповсюдження загальних параметрів $\{p,q,\Theta\}$ має здійснюватись аналогічно, як і в протоколі Шнора.

Генерувавання асиметричної пари довгострокових ключів (X,Y), має також здійснюватись аналогічно, як і в протоколі Шнора, що наведений.

Протокол автентифікації Шнора на основі ЦП за вказаних вище умов реалізується через виконання таких кроків.

1. Для забезпечення стійкості суб'єкти A та B повинні генерувати випадкове e, яке має співпадати. Ця задача розв'язана за рахунок використання функції гешування, тобто обчислення $h = H(m, \Pr)$.

2. Суб'єкт A генерує особистий ключ $K_A \in (1, q-1)$ та обчислює відкритий ключ:
$r_A = \Theta^{K_A} (\mathrm{mod}\, p)$;

3. Суб'єкт A генерує запит
$e = h(r_A, m)$,
де т – повідомлення (інформація), що підписується.

4. Суб'єкт A генерує значення підпису S у вигляді

$$S = (K_A + eX_A) \bmod q .$$

Необхідно підкреслити особливості протоколу:

1) значення запиту e змінюється для одного й того самого т;

2) сам підпис є сеансовим (залежить від X_A та ключа сеансу K_A).

Суб'єкт B, отримавши значення S та вже знаючи Θ, Y та e, обчислює значення r', яке за відсутності помилок також має співпасти з r_A, що отримане суб'єктом B на першому етапі, тобто обчислюється

$$r' = \Theta^S Y^e (\bmod p),$$

та перевіряється, чи r' = r, причому

$$e \stackrel{?}{=} h(r', m') \qquad (7.38)$$

При оцінці безпеки протоколу Шнора на основі ЕЦП необхідно відзначити, що пасивна атака порушника (криптоаналітика) має зводитися до знаходження довгострокового ключа кожного з абонентів X_A та ключа сеансу K_A. Як у першому, так і в другому випадках необхідно розв'язувати задачі дискретного логарифмування в скінченному полі Галуа. Указана проблематика розглядаються в розділі 9 монографії.

На відміну від трьохетапного протоколу Шнора, протокол Шнора на основі ЦП має такі переваги:

1) для виконання протоколу необхідно виконати тільки один обмін (раунд) (S, r) від A до B;

2) можлива також групова автентифікація A з групою суб'єктів з одночасною перевіркою цілісності повідомлення m.

Проблемними для протоколу Шнора на основі ЦП є такі питання:

1) при помилках в т (7.38) з великою ймовірністю r' також буде помилковим;

2) якщо m' викривлене, h буде відрізнятись та e не обчислюється.

3) забезпечення неспростовності тільки суб'єкта A.

Основним же недоліком, з точки зору обох протоколів Шнора, є те, що він побудований на основі криптографічного перетворення в скінченному полі Галуа. Для цього випадку складність атаки типу «повне розкриття» має субекспоненційний характер. У той же час його можна вдосконалити, скориставшись перетворенням у групі точок еліптичної кривої, в такому разі складність атаки «повне розкриття» вже буде носити субекспоненційний характер.