Список використаних джерел:

1. Steve Rura/ A fresh take on an icon/ Google Inc.
2. Julia Angwin / Sun Valley: Schmidt Didn't Want to Build Chrome Initially, He Says. *WSJ Digits Blog*.

Науковий керівник: доцент Ахмаметьєва Г.В.

ПРОТОКОЛ АВТЕНТИФІКАЦІЇ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ НАД РОЗШИРЕНИМ ПОЛЕМ $GF(2^m)$ ЕЛІПТИЧНИХ КРИВИХ

Онацький О. В.

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Жарова О. В.

кандидат фізико-математичних наук, доцент кафедри вищої математики Національного університету «Одеська політехніка»

В роботі запропоновано протокол автентифікації з нульовим розголошенням (zero-knowledge) на основі математичного апарату еліптичних кривих (elliptic curves – EC) з використанням особистих даних користувача та секретних ключів абонентів. Безпека криптосистем на еліптичних кривих (elliptic curves cryptography) [1], заснована на труднощах розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої (elliptic curve discrete logarithm problem) [2]. У криптосистем на EC запропоновано використовувати криптоперетворення, що базуються на перетвореннях у групі точок еліптичних кривих над полями $GF(p)$, $GF(2^m)$, $GF(p^m)$ [1, 2].

У криптосистемах над розширеним полем $GF(2^m)$ рівняння EC має вигляд [1, 2]:

$$y^2 + xy \equiv (x^3 + ax^2 + b) \bmod (f(x), 2) \text{ – несуперсингулярна крива;}$$

$$y^2 + cy \equiv (x^3 + ax + b) \bmod (f(x), 2) \text{ – суперсингулярна крива,}$$

де x, y – точки EC, $x, y \in E(GF(2^m))$; a, b, c – коефіцієнти EC; $f(x)$ – незведений поліном над полем $GF(2)$ вигляду

$$f(x) = x^m + h_1 x^{m-1} + h_2 x^{m-2} + \ldots + h_{m-1} x^1 + h_m,$$

причому $h_i \in GF(2)$.

Визначимо над точками з $E(GF(2^m))$ операцію складання та подвоєння. Нехай відомі координати двох точок $P = (x_1, y_1)$ і $Q = (x_2, y_2)$, то сума $P + Q = (x_3, y_3)$ визначається згідно з правилами [1, 2]:

1) несуперсингулярна крива

$$x_3 \equiv (\lambda^2 + \lambda + x_1 + x_2 + a) \bmod (f(x), 2);$$

$$y_3 \equiv [\lambda(x_1 + x_3) + x_3 + y_1] \bmod (f(x), 2);$$

2) суперсингулярна крива

$$x_3 \equiv (\lambda^2 + x_1 + x_2) \bmod (f(x), 2);$$
$$y_3 \equiv [\lambda(x_1 + x_3) + y_1 + c] \bmod (f(x), 2),$$

де $\lambda \equiv \left(\frac{y_1 + y_2}{x_1 + x_2} \right) \bmod (f(x), 2)$.

Точка, що подвоєна $2P = 2(x_1, y_1) = (x_3, y_3)$, визначається згідно з правилами:

1) несуперсингулярна крива

$$x_3 \equiv (\lambda^2 + \lambda + a) \bmod (f(x), 2);$$
$$y_3 \equiv [x_1^2 + (\lambda + 1)x_3] \bmod (f(x), 2),$$

де $\lambda \equiv \left(x_1 + \frac{y_1}{x_1} \right) \bmod (f(x), 2)$.

2) суперсингулярна крива

$$x_3 \equiv \lambda^2 \bmod (f(x), 2);$$
$$y_3 \equiv [\lambda(x_1 + x_3) + y_1 + c] \bmod (f(x), 2),$$

де $\lambda \equiv \left(\frac{x_1^2 + a}{c} \right) \bmod (f(x), 2)$.

Усі параметри є поліномами не вище m-степеня, а $f(x)$ – примітивний поліном над полем $GF(2)$.

Нехай $E_p(a, b)$ – еліптична крива, відома учасникам інформаційного процесу; $f(x)$ – незведений поліном над полем $GF(2)$; G – попередньо погоджена точка цієї кривої; $\#E_p(a, b) = n$ – порядок групи кривої; M – особисті дані абонента A; k_a і k_b – секретні ключі абонентів A, B; $h(MG) = m$ – геш-функція.

Абонент A обчислює значення відкритого ключа $Y_a = k_aG \bmod (f(x), 2)$ та заявку $\gamma = rG \bmod (f(x), 2)$, які передає абоненту B. Абонент B обчислює значення відкритого ключа $Y_b = k_bG \bmod (f(x), 2)$, який передає абоненту A. Абонент A обчислює два значення $x_1 = [k_aY_b + MG] \bmod (f(x), 2)$ і $x_2 = [(k_a + r)Y_b] \bmod (f(x), 2)$, які передає абоненту B. Абонент B перевіряє рівності: $MG = [x_1 - k_bY_a] \bmod (f(x), 2)$, $h(MG) = m$ та $k_b\gamma = [x_2 - k_bY_a] \bmod (f(x), 2)$.

Для аналізу та перевірки запропонованого протоколу автентифікації на стійкість до атак противника був застосований програмний продукт AVISPA [3]. В роботі виконано перевірку моделі запропонованого протоколу (рис. 1) та результат моделювання зловмисника на протокол представлено на рис. 2.

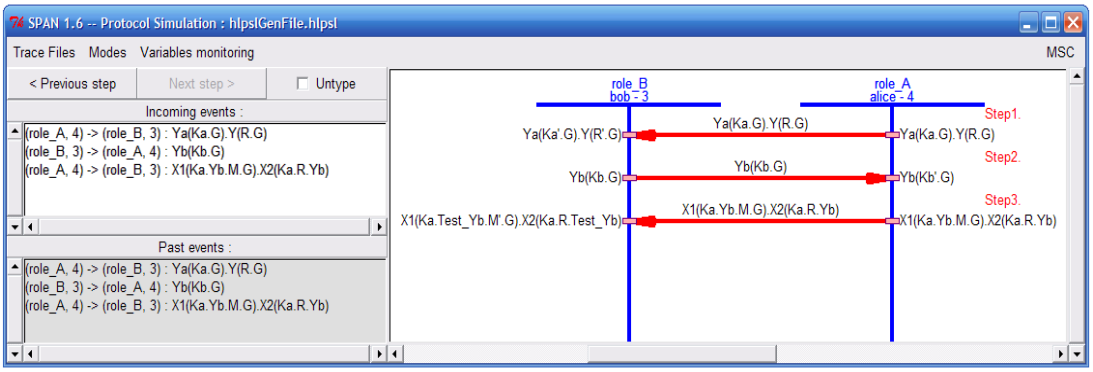

Рис. 1. Перевірка моделі криптографічного протоколу автентифікації

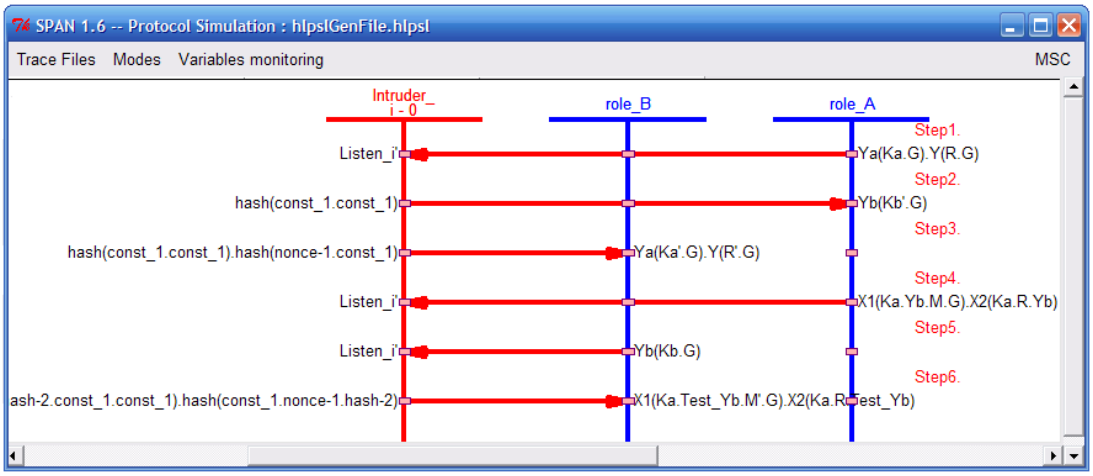

Рис. 2. Результат моделювання дії зловмисника на протокол автентифікації

Програмна верифікація протоколу і стійкість протоколу до атак зловмисника була виконана за допомогою програмних модулів OFMC та CLAtSe AVISPA. В результаті перевірки запропонованого протоколу автентифікації відомих атак не знайдено (рис. 3).

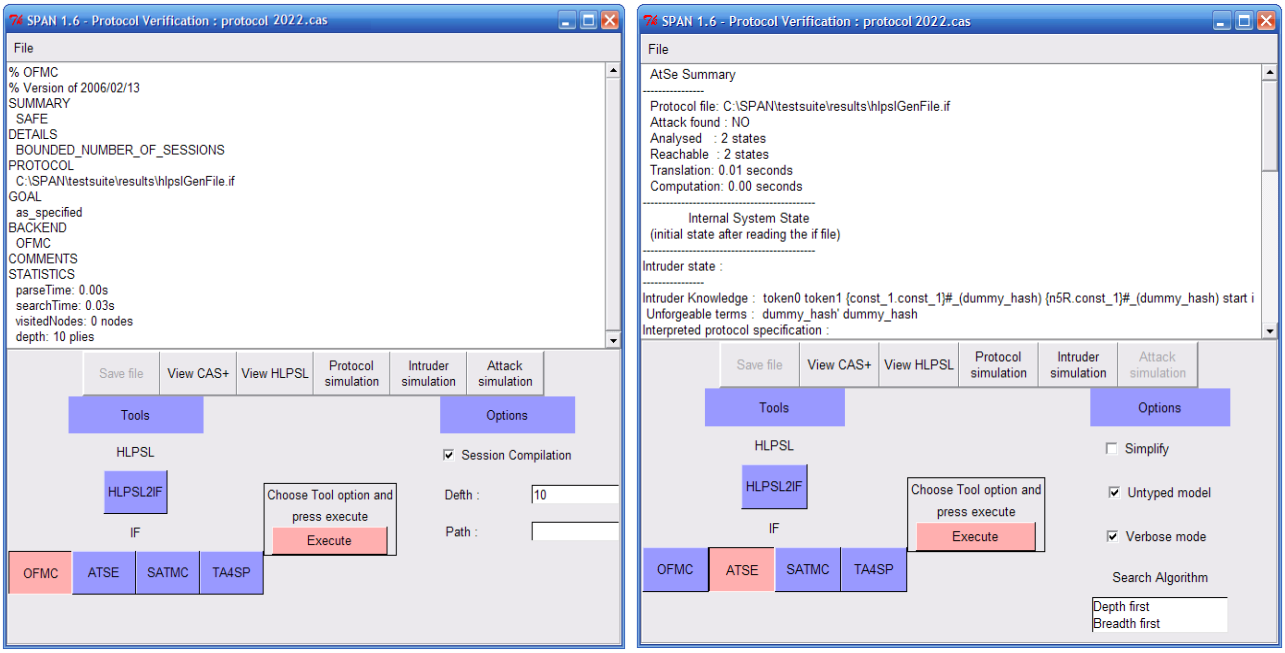

Рис. 3. Верифікація і стійкість протоколу автентифікації до атак

Таким чином, у роботі запропоновано новий криптографічний протокол автентифікації з нульовим розголошенням на основі математичного апарату еліптичних кривих над розширеним полем $GF(2^m)$. Визначено повнота і коректність протоколу, була виконана перевірка моделі і верифікація протоколу. В результаті перевірки протоколу відомих атак на протокол, не знайдено. Для реалізації запропонованого протоколу автентифікації можна використовувати рекомендовані еліптичні криві згідно FIPS 186-4 [4], SEC 2 [4] та ДСТУ 4145-2002 [6].

Список використаних джерел:

1. Stavroulakis P., Stamp M. Handbook of Information and Communication Security: Berlin: Springer-Verlag, 2010. 863 p.
2. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика: монографія, Харків: Видавництво «Форт», 2012. 880 с.
3. AVISPA. URL: http://www.avispa-project.org/
4. FIPS 186-4. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
5. SEC 2. URL: https://www.secg.org/SEC2-Ver-1.0.pdf
6. ДСТУ 4145-2002. URL: https://ru.wikipedia.org/wiki/ДСТУ_4145-2002

СУЧАСНІ СИСТЕМИ ПОЖЕЖНОЇ БЕЗПЕКИ

Раєв О. Д.

студент 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Засоби новітньої протипожежної сигналізації – це є, зокрема, сукупністю технічних засобів, які винайдено для пожежовиявлення, а також обробки зібраної інформації та її передачі, наприклад, у вигляді сповіщення про займання у приміщенні, а також підключення команд автоматичних установок для системи захисту проти диму, їхнього технічного та інженерного наповнення [1].

Бездротова пожежна сигналізація є одним із актуальних для сьогодення видів охоронних систем, які використовуються під час організації захисту об'єктів від пожежі. Сфера їхнього застосування і пристосування досить широка, її ефективність ґрунтується на можливості вести роботу в діалоговому режимі та використовувати резервні станції зв'язку.

Бездротова пожежна сигналізація створена вирішувати цілий комплекс завдань із забезпечення безпеки об'єкту, таких як:

1) постійне сканування контрольованого об'єкта;

2) фіксація параметрів пожежі: температура, задимленість, електромагнітне випромінювання, порівняння отриманих даних із граничними значеннями, занесеними на згадку про приймально-контрольний пристрій;

3) виявлення осередку займання на ранніх стадіях;

4) формування та пересилання тривожного сигналу на одну із зазначених у пам'яті системи адрес: центральний диспетчерський пульт; віддалений пульт управління оператора пожежної охорони; телефонний номер власника об'єкта чи відповідальної особи;

5) активація засобів оповіщення та системи евакуації;

6) активація засобів автоматичного пожежогасіння.

Переваги та недоліки бездротових систем пожежної сигналізації.