УДК 004.78

ВИЗНАЧЕННЯ СТІЙКОСТІ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ НА ОСНОВІ ЇХ ІМОВІРНІСНИХ МОДЕЛЕЙ

Я.І. Заячук
Кандидат технічних наук, доцент*
Контактний тел.: 098-977-49-53
E-mail: yarikotm@gmail.com

О.В. Мойсеєнко
Кандидат технічних наук, доцент*

А.П.Толстокоров
Магістр
*Кафедра комп'ютерних систем та мереж
Івано-Франківський національний технічний університет нафти і газу
вул. Карпатська, 15, м. Івано-Франківськ, Україна, 76019

В статті розглянуті імовірнісні моделі протоколів з нульовим розголошенням. На основі цих моделей визначена стійкість криптопротоколів

Ключові слова: криптографія, криптопротокол, нульове розголошення

В статье рассмотрены вероятностные модели протоколов с нулевым разглашением. На основе этих моделей определена стойкость криптопротоколов

Ключевые слова: криптография, криптопротокол, нулевое разглашение

The article discusses the probabilistic models of cryptography zero-knowledge protocols

Keywords: cryptography, cryptography protocol , zero-knowledge protocol

Вступ

Одне з основних завдань криптографії представляє собою двосторонню інтерактивну гру, в якій один учасник доказує іншому учаснику істинність твердження, не розкриваючи суті доказу. Ця гра називається протоколом інтерактивного доказу або IP-протоколом (interactive proof protocol).

Скільки раундів повинна виконати сторона, що доводить, щоб переконати сторону, що перевіряє?

Ідеальною відповіддю на це питання було б «*аніскільки*», або «*нуль*». IP-протокол, що володіє такою властивістю, називається протоколом з нульовим розголошенням або ZK-протоколом (zero-knowledge).

Обчислювальна модель

Розглянемо обчислювальну модель інтерактивної системи доказу, яку запропонували Голдвассер, Мікалі і Раков [1]. Позначимо основну модель протоколу інтерактивного доказу через (P, V), де P– сторона, що доводить (*prover*), а V– сторона, що перевіряє (*verifier*). Як правило, протокол $p \approx 2^{1024}$ призначений для перевірки приналежності певного речення мові.

Нехай L – мова з алфавітом {0,1}. Сторони P і V одержують зразок $x \in L$, що є загальними вхідними даними. Доказ приналежності зразка позначається як (P,V)(x). Обидві сторони протоколу пов'язані каналом зв'язку, через який вони обмінюються інформацією $a_1, b_1, a_2, b_2, ..., a_l, b_l$.

Ця послідовність повідомлень називається стенограмою доказу. Як загальна довжина стенограми доказу l, так і довжина кожної стенограми $|a_i|, |b_i|, (i = 1, 2..., l)$ обмежена поліномом, що залежить від параметра $|x|$. Доказ приналежності зразка (P,V)(x) мові L також повинен бути обмежений поліномом, який залежить від об'єму вхідних даних $|x|$.

Результат роботи протоколу записується у вигляді [2]:

$$(P,V)(x) \in \{\text{Прийняти}, \text{Відхилити}\}.$$

Оскільки система (P,V) є імовірнісною, при кожному x результат (P,V)(x) є випадковою величиною, залежною від загальних вхідних даних x, закритих вхідних даних (private input) користувача P і деяких

випадкових вхідних даних (random input), загальних для користувачів P і V.

Нехай L- мова, задана на алфавіті {0,1}. IP-протокол (P,V) називається системою інтерактивного доказу для мови L, якщо [1-2]:

$$Prob[(P,V)(x)=Прийняти|x \in L] \geq \varepsilon, \quad (1)$$

$$Prob[(P,V)(x)=Прийняти|x \notin L] \leq \delta \quad (2)$$

де числа ε і δ є константами, що задовольняють умовам: .

$$\varepsilon \in \left(\frac{1}{2},1\right), \delta \in \left(0,\frac{1}{2}\right)$$

Оцінка (1) характеризує повноту протоколу (P,V). Величина ε називається імовірністю повноти протоколу (P,V). Це означає, що коли $x \in L$, то сторона V приймає припущення x з імовірністю, яка не менше величини ε.

Оцінка (2) характеризує несуперечність протоколу (P,V). Величина δ називається імовірністю суперечності протоколу (P,V). Якщо $x \notin L$, то сторона V приймає припущення x з імовірністю, що не перевищує величини δ.

Розглянемо приклад протоколу інтерактивного доказу.

Загальні вхідні дані:

1. r: однонаправлена функція, визначена в групі Z_n і задовольняюча гомоморфній умові:.

$$\forall x, y \in Z_n : r(x+y) = r(x) \cdot r(y)$$

2. X=r(z) для деякого $z \in Z_n$.

Закриті вхідні дані сторони А: z<n.

Висновок сторони Б: $X \in \langle r(1) \rangle$, елемент X породжується елементом r(l).

Наступні кроки виконуються m разів.

1. А генерує число $k \in Z_n$, знаходить число

Commit ← r(k) і відсилає його Б.

2. Б генерує число Challengeє{0,1} і відсилає його А.

3. А обчислює

$$Response \leftarrow \begin{cases} k, якщоChallenge=0, \\ k+z(mod\ n), якщо\ Callenge=1 \end{cases}$$

і відсилає його Б.

4. Б перевіряє значення

$$r(Response) \leftarrow \begin{cases} Commit, якщо\ Challenge=0, \\ CommitX, якщо\ Challenge=1 \end{cases}$$

Якщо перевірка завершується невдало, Б відсилає відмову і завершує роботу протоколу. Б приймає доказ.

У цьому протоколі А є стороною, що доводить, а Б стороною, що перевіряє. Загальними вхідними даними А і Б є число X=r(x), де функція r є однонаправленою і гомоморфною функцією, заданою над групою Z_n . Твердження про приналежність формулюється А і виглядає таким чином:

$$X \in \{r(x) | x \in Z_n\}$$

Закритими даними А є елемент zєZ_n– прообраз елементу X при однонаправленому і гомоморфному відображенні r.

В даному протоколі обидві сторони вступають в контакт m разів і створюють наступну стенограму доказу: $Commit_1$, $Challenge_1$, $Response_1$,..., $Commit_m$, $Challenge_m$, $Response_m$.

Протокол виводить результат «прийняти», якщо кожна перевірка, що виконується Б, завершується успішно. Інакше результатом є слово «відхилити». Описаний протокол є повним. Інакше кажучи, якщо А знає прообраз z і слідує інструкціям, то Б завжди відповідатиме: «прийняти».

Оцінка імовірності повноти протоколу виконується, причому ε=1, оскільки відповіді А завжди успішно проходять перевірку у Б, тобто

$$r(Response) \leftarrow \begin{cases} Commit, якщо\ Challenge=0, \\ CommitX, якщо\ hCallenge=1 \end{cases}$$

при будь-якому виборі випадкового числа Challenge є{0,1}.

Протокол є несуперечливим.

Оцінимо імовірність суперечності δ.

Результат перевірки, що виконується Б на етапі 4, залежить від випадкового числа Challenge після отримання числа Commit від *A*. Перевірка завершується успішно в двох випадках.

Варіант 1: Challenge=0: Б бачить, що А відомий прообраз числа Commit.

Варіант 2: Challenge=1: Б бачить число

$$прообраз(X)=Responce-(Commit)(mod\ n).$$

Якщо А не знає число прообраз(X), вона може зшахраювати, спробувавши вгадати випадковий біт оклику перед відправкою своєї передачі. У «нечесному» доказі А обчислює значення, що передається таким чином.

- Вибирає випадкове число Responce єZ_n.
- Вгадує число Challenge.
- Обчислює число

$$Commit \leftarrow \begin{cases} f(Responce), якщо\ Challenge=0, \\ f(Responce)/X, якщо\ hCallenge=1 \end{cases}$$

Очевидно, що на кожному кроці Б може відкинути помилковий доказ з імовірністю 1/2. Отже, імовірність суперечності (тобто імовірність успішного обману) рівна δ=1/2. Якщо протягом m ітерацій Б жодного разу не відкинув доказ, імовірність успішного обману не перевершує 2^{-m}. Обман стане практично неможливим, якщо число m достатньо велике, тобто число 2^{-m} є дуже малим.

Таким чином, завдання про приналежність елементу підгрупі зводиться до факторизації великого цілого числа. Отже, ціле число n в протоколі повинне бути достатньо великим. Саме з цієї причини параметр безпеки в протоколі повинен мати довжину log n.

Припустимо, що на поставлене питання існує ідеальна відповідь (P,V) – протокол з нульовим розголошенням, тобто користувач V переконується у коректності твердження користувача P, не дізнавшись нічого нового про закриті вхідні дані.

Для того, щоб протокол (P,V) володів цією властивістю, необхідно обмежити обчислювальну потужність користувача V поліномом, що залежить від розміру його вхідної інформації. Очевидно, що без цього обмеження неможна гарантувати нульове розголошування, оскільки користувач V, що володіє необмеженими обчислювальними ресурсами може самостійно розкрити секретні вхідні дані користувача P.

Доведемо тепер, що розглянутий протокол є ідеальним ZK-протоколом.

Стенограма доказу виглядає таким чином:

$$Commit_1, Challenge_1, Response_1,..., Commit_m, Challenge_m, Response_m,$$

де для i=1,2,...,m виконуються наступні умови: $Commit_i=r(k_i)$, де $k_i \epsilon Z_n$; $Chllenge_i \epsilon \{0,1\}$; $Responce_i=k_i+zChallenge(\mathrm{mod}\ n)$.

Очевидно, оскільки сторона A витягує числа ki з рівномірно розподіленої генеральної сукупності, величини $Commit_i$ також рівномірно розподілені по простору значень функції r і не залежать від загальних вхідних даних X.

Отже, дані, що передані стороною A є рівномірно розподіленими і не представляють для сторони Б ніякої додаткової інформації про її закриті дані. Таким чином цей протокол є ідеальним протоколом з нульовим розголошенням, навіть якщо сторона Б веде нечесну гру.

Протокол ідентифікації Шнорра

В протоколі, який розглянутий вище, сторона Б використовує біти оклику. Це призводить до великої імовірності суперечності протоколу: δ=1/2. Отже для того, щоб зменшити помилку до 2^{-m} необхідно повторити протокол m разів. Для запобігання шахрайства з боку *A* достатньо прийняти m=100. Але необхідність великої кількості раундів знижує ефективність протоколу.

При деяких параметрах безпеки ймовірність суперечності протоколу можна понизити, що приведе до зменшення кількості необхідних раундів. Для цього сторона Б повинна знати розклад числа n на прості множники. Особлива ситуація виникає, коли число n є простим. Розглянемо протокол ідентифікації Шнора [1-5].

Загальні вхідні дані.

p,q: два простих числа, що задовольняють умові q|p-1 (типовий розмір: |q|=1024, |p|=160.); g: $ord_p(g)=q$;
y: $y=g^{-a}(\mathrm{mod}\ p)$.

Кортеж (p,q,g,y) складається з параметрів відкритого ключа сторони A, сертифікованого органом авторизації.

Закриті вхідні дані сторони A: a<q.

Висновок сторони Б :

A відомий деякий елемент $a \epsilon Z_q$, що задовольняє умові

$$y=g^{-a}(\mathrm{mod}\ p).$$

Наступні кроки виконуються $\log_2\log_2 p$ разів.

1. A генерує число $k \epsilon Z_n$, знаходить $Commit \leftarrow g^k(\mathrm{mod}\ p)$ і відсилає його Б.
2. Б генерує число $Challenge \epsilon \{0,1\}^{\log_2\log_2 p}$ і відсилає його A.
3. A обчислює $Responce \leftarrow k+aChallenge(\mathrm{mod}\ p)$ і надсилає його Б.
4. Б перевіряє число $Commit=g^{Responce}y^{Challenge}(\mathrm{mod}\ p)$.

Якщо перевірка завершується невдало, сторона Б посилає відмову і припиняє роботу протоколу. Сторона Б ідентифікує сторону A.

Цей протокол є різновидом попереднього протоколу, в якому функція r(x) реалізується за допомогою операції $g^{-x}(\mathrm{mod}\ p)$ над кінцевим полем F_p, де підгрупа (g) має простий порядок q|p-1. Легко побачити, що функція $g^{-x}(\mathrm{mod}\ p)$ є гомоморфною. Більш того, для достатньо великих простих чисел *q* і *p*, наприклад |p|=1024, |p|=160, функція $g^{-x}(\mathrm{mod}\ p)$ є однонаправленою.

Оскільки умова q|p-1 накладається явно, протокол ідентифікації Шнорра більше не повинен вирішувати задачу про приналежність елементу певній підгрупі. Тепер Б може самостійно визначити, чи належить елемент у підгрупі (g), не вдаючись до допомоги сторони A: $y^q=g^q=1(\mathrm{mod}\ p)$. Отже, протокол ідентифікації Шнорра вирішує конкретніше завдання: чи знає сторона A дискретний логарифм числа y за g, що є її криптографічним мандатом.

Проаналізуємо стійкість даного протоколу.

Властивість повноти виконується тривіальним чином, причому ε=1.

Припустимо, що сторона A шахраює, тобто не знає правильне значення дискретного логарифма. Одержавши число Commit від A, сторона Б генерує число $Challenge \epsilon \{0,1\}^{\log_2\log_2 p}$ і чекає відгуку:

$$Response\text{-}\log_g[Commit \cdot y^{Chaleng}(\mathrm{mod}\ p)](\mathrm{mod}\ q).$$

Це рівняння демонструє, що при заданих числах Commit і y існують $\log_2 p$ різних значень Response, що відповідають $\log_2 p$ різним значенням Challenge. При невеликому значенні $\log_2 p$ найкращою стратегією обчислення правильної відповіді за величиною $Commit \cdot y^{Chaleng}(\mathrm{mod}\ p)$ є вгадування числа Challenge перед фіксацією числа Commit.

Очевидно, що імовірність суперечності при правильному вгадуванні на кожної ітерації рівна $1/\log_2 p$, тобто імовірність суперечності протоколу, що складається з одного раунду, рівна $\delta = 1/\log_2 p$.

Оскільки імовірність суперечності протоколу ідентифікації Шнорра, що складається з одного раунду, менше, ніж у попереднього протоколу, його ефективність вище. В попередньому протоколі для зниження імовірності помилки до величини $\delta=2^{-m}$ необхідно виконати т ітерацій, в той час, коли в протоколі ідентифікації Шнорра для цього достатньо $l = \frac{m}{\log_2\log_2 p}$ раундів.

Отже, при $p \approx 2^{1024}$ і m=100 одержуємо l=100/10=10. Інакше кажучи, збільшення довжини оклику в протоколі ідентифікації Шнорра скорочує кількість

ітерацій в порівнянні з протоколом Голдвассера, Мікалі та Ракова в 10 разів при тій же імовірності суперечності.

На основі імовірнісних моделей протоколів з нульовим розголошенням, які є представниками області криптографії, пов'язаної з комп'ютерними науками, що активно розробляється, визначена стійкість криптоторотоколів. Результати розрахунків дають змогу зробити висновок, що задача приналежності елемента підгрупі є такою, що легко вирішується (або такою, що важко вирішується), якщо існує (відповідно не існує) додаткова інформація, що полегшує роботу алгоритму. У випадку відомості стороні, яка доводить, розкладу складеного числа (N) на прості множники, незалежно від довжини оклику (Challenge), ймовірність суперечності рівна всього лише $\delta=1/2$. Тобто для зменшення цієї імовірності в будь-якому випадку потрібно збільшити кількість раундів протоколу.

Література

1. S. Goldwasser. The knowledge complexity of interactive proof-systems [Текст] / S. Goldwasser, S. Micali, and C. Racko – In Proceedings of 17th Ann. ACM Symp. On Theory of Computing, pages 291-304, 1985. A journal version under the same title appears in: SIAM Journal of Computing vol. 18. - pp. 186-208. - 1989.
2. Венбо Мао. Современная криптография: теория и практика: Пер. с англ. [Текст] / Венбо Мао. – М.: Издательский дом «Вильямс», 2005. – 768 с.
3. Диффи, У. "Новые направления в криптографии" [Текст] / У. Диффи, М. Хэллман. // ТИИЭР - 1979. - т.67., №3. - С. 71-109.
4. Скляров, Д. В. Искусство защиты и взлома информации [Текст] / Д. В. Скляров. – СПб.: БХВ. – Петербург, 2004. – 288 с.
5. Программирование алгоритмов защиты информации: Учебное пособие. [Текст] / А. В. Домашев, В. О. Попов, Д. И. Правиков и др. – М.: «Нолидж», 2000. – 288 с.