УДК 004.056.5

Кулага А. А.

ПРОТОКОЛ ДОВЕДЕННЯ ЗНАННЯ РОЗВ'ЯЗКУ ЗАДАЧІ ДІФФІ–ХЕЛЛМАНА З НУЛЬОВИМ РОЗГОЛОШЕННЯМ

Розглянуто основні поняття теорії інтерактивних доведень, запропоновано протокол доведення знання розв'язку задачі Діффі–Хеллмана з властивістю нульового розголошення, який використовує математичний апарат білінійних відображень.

Ключові слова: інтерактивне доведення, нульове розголошення, білінійне відображення, задача Діффі–Хеллмана, аутентифікація.

Чи можливо переконати когось у тому, що Ви вмієте розв'язувати задачу, не повідомляючи способу її розв'язку, або в тому, що Ви знаєте розв'язок задачі, не розкриваючи його? Ці дві, на перший погляд, взаємовиключні вимоги, задовольняють протоколи доведення з нульовим розголошенням.

Теорія доведення з нульовим розголошенням достатньо точно відображає вимоги, які повинні задовольняти протоколи аутентифікації, тому вона насамперед призначена для дослідження цих протоколів. Самі протоколи доведень із нульовим розголошенням можуть використовуватися як вимоги [1, 2]. Проте виникають проблеми з ефективністю: задовгий таємний ключ, значна кількість раундів, неприйнятно велика комунікаційна складність протоколу та дуже значна обчислювальна складність, тому при розробці протоколів аутентифікації розробники основну увагу приділяють їх ефективності. Крім того, поняття нульового розголошення дає змогу формалізувати інтуїтивне уявлення протоколу, під час роботи якого не повинен відбуватися витік секретної інформації, тому воно стало корисним і для багатьох інших типів криптографічних протоколів.

Оскільки доведення з нульовим розголошенням становить інтерактивне доведення, яке задовольняє певні вимоги, у статті подано основні поняття теорії інтерактивних доведень. Потім вказано приклад того, як довести що Ви знаєте ізоморфізм графів, ніяк не допомагаючи перевіряльнику знайти його (див. працю Гольдрайха, Микалі та Вігдерсона: [7]). Далі зазначено основні властивості білінійних відображень – спарювань точок еліптичних кривих та запропоновано протокол доведення знання розв'язку задачі Діффі–Хеллмана, який використовує математичний апарат білінійних відображень.

Основні визначення

Теорія доведень із нульовим розголошенням базується на понятті інтерактивної системи доведення (*interactive proof system*), яке було введено в 1985 році незалежно у працях Бабаі [3; 4] та Гольдвассер, Микалі і Ракоффа [5; 6]. Слово «*доведення*» тут не використовується у традиційному математичному значенні. Під цим словом, що еквівалентне «*системі доведення»,* розуміють рандомізований протокол, за допомогою якого одна сторона *P*, яка називається *довідна* (*prover*), бажає переконати іншу сторону *V* – *перевірну* (*verifier*), в тому, що задане твердження істинне. Тобто не розкриває будь-яку інформацію, крім істинності твердження, що доводиться. Після того, як перевіряльник завдяки протоколу переконався в істинності твердження, він не може доводити його істинність третім особам.

Формалізуючи модель такого протоколу [1; 2], розглядають дві ймовірнісні машини Тюрінга *P* та *V*, які мають спільну комунікаційну стрічку для обміну повідомленнями. Обчислювальні ресурси, які може використовувати машина *P* необмежені, водночас машина *V* працює за поліноміальний час. Після запису повідомлення на комунікаційну стрічку машина входить у стан очікування та виходить з нього, як тільки буде записано повідомлення у відповідь. Машини *P* та *V* мають також вхідну стрічку, на яку записано вхідне слово *x*. Твердження, яке доводиться, – це суть $x \in L$, де *L* – це деяка фіксована мова. З метою виключення тривіальності, мова *L* повинна бути важкою, наприклад *NP* – повною, інакше перевірна сторона зможе самостійно перевірити, що $x \in L$. Протокол доведення полягає в тому, що перевіряльна сторона випадково вибирає питання, ставить їх стороні, що доводить, та перевіряє правильність відповідей. Виконання протоколу завершується, коли машина *V* зупиняється, при цьому вона видає 1, якщо доведення прийнято, або 0 – якщо ні. Через $[P(x), V(x)]$ позначається випадкова величина, вихідне слово машини *V*, коли *P* та *V* працюють на вхідному слові *x*.

Визначення 1. Інтерактивним доведенням для мови *L* називається пара інтерактивних машин Тюрінга (*P*, *V*) така, що виконуються такі вимоги.

1. Повнота (*Completeness*). $\forall x \in L$

$$\Pr\{[P(x), V(x)] = 1\} = 1.$$

2. Коректність (*Soundness*). Для будь-якої машини Тюрінга P^*, для будь-якого поліному *p* та $\forall x \notin L$

$$\Pr\{[P^*(x), V(x)] = 1\} < \frac{1}{p(|x|)}.$$

Повнота означає, якщо вхідне слово належить мові *L* та обидва учасника дотримуються протоколу, то доведення буде завжди прийнято. Вимога коректності захищає *V* від прийняття хибного твердження, при цьому може відбуватися відхилення від дій, приписаних протоколом (може використовуватись будь-яка машина Тюрінга P^*), потрібно, щоб ймовірність обману була в будь-якому випадку надто низька.

Визначення 2. Інтерактивний протокол доведення для мови *L* називається доведенням з абсолютно нульовим розголошенням, якщо, крім цих умов, виконується й ще одна умова – нульове розголошення.

3. Властивість нульового розголошення (*Zero-knowledge*). Для будь-якої поліноміальної ймовірнісної машини Тюрінга V^* існує імовірнісна машина Тюрінга M_{V^*}, яка працює в середньому за поліноміальний час, і така, що $\forall x \in L$

$$M_{V^*} = [P(x), V^*(x)].$$

Машина M_{V^*} називається моделювальною машиною для V^*. Припускають, Що математичне сподівання часу її роботи обмежено поліномом

від $|x|$. Для кожної машини V^* будується окрема моделювальна машина, яка може використовувати V^* як підпрограму. Властивість нульового розголошення захищає довідну сторону P від нечесного перевіряльника V^*, який, довільно відхиляючись від дій, прописаних протоколом, намагається добути із його виконання додаткову інформацію. Ця умова означає, що V^* може отримати тільки таку інформацію, яку він міг би обчислити і самостійно без виконання протоколу за поліноміальний час.

Припустимо, що задана інтерактивна система (P, V), де гравець P доводить гравцю V істинність твердження S, яке полягає в тому, що деякі графи G_0 та G_1 ізоморфні. Для досягнення своєї мети гравець P може просто пред'явити гравцю V ізоморфізм між G_0 та G_1, який гравець V самостійно обчислити не здатен, але надання такої інформації гравцю V за припущенням не в інтересах гравця P, він бажає зберегти цю інформацію в секреті. Таким чином, мета гравця P – переконати гравця V, що надані графи дійсно ізоморфні, при цьому не надаючи ніяких відомостей, які гравець V не міг би отримати самостійно. Більше того, потрібно, щоб ця мета досягалась навіть якщо гравець P матиме справу з будь-яким іншим гравцем V^* з поліноміально обмеженими можливостями, який бажає отримати від P якомога більше відомостей. Як виявилося, можна розробити протокол (P, V), що становить інтерактивне доведення з урахуванням цих інтересів гравця P.

У випадку, якщо графи G_0 і G_1 дійсно ізоморфні, гравець V та навіть будь-який інший гравець V^* з довільною поліноміально обмеженою ймовірнісною стратегією, який вступив у гру з P замість гравця V, не отримає від гравця P ніякої додаткової інформації, бо вся інформація, яка внаслідок гри стала йому доступною (послідовність результатів підкидання власної монети, власних повідомлень і повідомлень гравця P), є випадковою величиною, яка може бути промодельована певним ймовірнісним поліноміальним алгоритмом. Отже, гравець V і без участі гравця P міг би за допомогою цього алгоритму отримати цю інформацію. При цьому моделювальний алгоритм не придатний для розв'язання питання, чи ізоморфні графи G_0 та G_1.

Припускаємо, що графи G_0 і G_1 задані на одній й тій самій множині вершин N, $|N| = m$ і що ϕ – перестановка вершин N, яка є ізоморфізмом графів G_0 та G_1, що позначимо як $G_1 = \phi G_0$.

Наступний протокол повторюється m разів:

1) P вибирає випадкову перестановку вершин π, обчислює граф $H = \pi G_1$ та передає його гравцю V;
2) V вибирає випадковий біт α і передає його гравцю P;
3) Якщо $\alpha = 1$ то P передає V перестановку π, інакше – перестановку $\pi \circ \phi$;
4) Якщо перестановка, яку отримав V не є ізоморфізмом між графами G_α та H, то V зупиняється і заперечує доведення. Інакше виконання протоколу триває.

Цей протокол є інтерактивним доведенням для мови ізоморфізм графів. Справді, якщо гравець P пред'являє граф H, який є ізоморфним до G_1, а гравець V потребує довести ізоморфність H та G_0 або H і G_1, то це можливо з ймовірністю 1 у випадку, якщо G_1 й G_0 ізоморфні. Якщо ці графи не ізоморфні, то це можливо з ймовірністю $\frac{1}{2}$ на кожній ітерації протоколу та з імовірністю $\frac{1}{2^m}$ при всіх m ітераціях.

Цей протокол стає протоколом із нульовим розголошенням, позаяк у випадку ізоморфних G_1 та G_0 гравець V не отримує ніякої інформації, крім ізоморфізмів графів G_1 і G_0 з деякими їхніми випадковими перенумераціями, які він міг би отримати і самостійно, вибираючи випадкові α та перенумеровуючи випадковим чином граф G_α.

Білінійні відображення

Наступне визначення задає умови, необхідні для того, щоб білінійне відображення було корисним для криптографічних потреб. Для спрощення пояснення, розглядається тільки такий випадок, коли обидва аргументи спарювання належать одній й тій самій групі.

Визначення 3. Нехай G_1 та G_2 – циклічні групи простого порядку ${}^0v$ (G_1 – адитивна група, G_2 – мультиплікативна). Відображення $e : G_1 \times G_1 \to G_2$ є криптографічним спарюванням або парним відображенням, якщо виконуються наступні умови:

1. *Білінійність*. Для будь-яких $P, Q, R \in G_1$: $e(P + Q, R) = e(P, R)\, e(Q, R)$ та $e(P, Q + R) = e(P, Q)\, e(P, R)$, з чого випливає: $\forall P, Q \in G_1$ і $\forall a, b \in Z_q^*$: $e(aP, bQ)\, e(P, Q)^{ab}$.
2. *Невиродженість*. Існує $P \in G_1$, що $e(P, P) \neq 1$. Тобто якщо P є твірним елементом G_1, то $e(P, P)$ буде твірним елементом G_2, тому що G_1 та G_2 – групи простого порядку.
3. *Обчислювальність*. Існує ефективний поліноміальний алгоритм обчислення $e(P, Q) \in G_2$ для будь-яких $P, Q \in G_1$.

Криптографічні спарювання з такими властивостями будуються на основі спарювань Вейля і Тейта над еліптичними кривими, які визначаються над скінченними полями. Вивчення цих груп викликає великий інтерес у сучасних учених. Проте в описі протоколу, структура груп не розглядатиметься, а спарювання використовуватиметься як «чорна скринька».

Доведення знання розв'язку певної задачі Діффі–Хеллмана з нульовим розголошенням

Припустимо, що G_1 – це скінченна адитивна підгрупа точок еліптичної кривої E з N елементів, P – базова точка цієї кривої, aP та bP елементи G_1, за якими гравець P розв'язав задачу Діффі–Хеллмана, тобто знайшов точку кривої abP. Гравцю P потрібно довести перевіряльнику V, що він справді знає розв'язок цієї задачі, не допомагаючи йому знайти це значення. При цьому припустимо, що перевіряльнику V відомий порядок q групи G_1. Послідовність кроків, які повинні зробити гравці, така:

1) Гравець P випадково вибирає число e та посилає V значення $B' = ebP$;
2) V вибирає випадковий біт α. Якщо α = 1, то гравець P повинен розкрити значення e і гравець V може перевірити, що дійсно $B' = ebP$.
3) Якщо α = 0, то гравець P повинен обчислити та передати V значення $eabP$, гравець V повинен перевірити рівність $e(P, eabP) = e(aP, B')$.
4) Кроки 1–3 повторюються доти, доки гравець V не переконається, що P дійсно знає значення abP.

Властивість повноти тривіальним чином випливає з конструкції самого протоколу, оскільки виникає тотожність

$$e(P, eabP) = e(P, P)^{eab} = e(aP, P)^{eb} = e(aP, B').$$

Якщо гравець P насправді не знає значення abP, то він може давати правильну відповідь не більше ніж при одному варіанті значення α. Так, якщо виконуючи крок 1 гравець P сподівається, що α прийме значення 1, то він може, не знаючи abP, послати V значення $B' = ebP$. Якщо P сподівається, що α прийме значення 0, то він може послати значення $B' = eP$ (тоді на кроці 3 він повинен замість $eabP$ послати значення eaP, тому що $e(P, eaP) = e(aP, e\,P) = e(aP, B')$). Однак якщо в цьому випадку α прийме значення 1, гравець P не зможе надати правильну відповідь, бо не знає значення eb^{-1}, яке потрібно скалярно помножити на точку bP, щоб отримати B' ($B' = eP = eb^{-1}\,bP$). Ймовірність того, що гравець V прийме доведення дорівнює $\frac{1}{2^m}$ при m ітераціях протоколу, це обґрунтовує властивість коректності.

Необхідно зауважити, що при доведенні стійкості криптографічних протоколів будують зведення певної важко обчислювальної задачі до задачі, яка стоїть перед супротивником. Тобто якщо супротивник зможе зламувати протокол, то алгоритм, який використовує супротивник, можна використовувати для обчислювання певної важко обчислювальної задачі. Так зробив, наприклад, Шнор у [8] зі схемою аутентифікації, де здійснюється зведення задачі обчислення дискретного логарифму до задачі, яку повинен розв'язувати противник. У нашому випадку противник, не знаючи значення abP, повинен уміти обчислювати значення $eabP$. Якщо припустити, що він це вміє якось робити, то тоді він зможе розв'язувати задачу Діффі–Хеллмана, тобто обчислювати abP множенням e^{-1} на $eabP$.

Властивість нульового розголошення можна обґрунтувати використовуючи відомий метод імітації, який використовується в доведеннях наявності цієї властивості в протоколах такого типу. Нехай деяка третя сторона K не знає значення розв'язку задачі Діффі–Хеллмана abP при відомих P, aP та bP, однак знає заздалегідь, яке значення прийме випадковий біт α. Тоді вона може імітувати гравця P, посилаючи $B' = ebP$ перед тим, як α прийме значення 1 і $B' = eP$ перед тим, як α прийме значення 0. Та інформація, яку гравець V отримуватиме, не відрізнятиметься від тієї інформації, яку він міг би отримувати від гравця P. При цьому третя сторона K не може передати ніякої інформації щодо розв'язку задачі, тому що сама не знає його.

Висновок

Подано основні відомості з теорії інтерактивних доведень із прикладом доведення з нульовим розголошенням для мови ізоморфізму графів. Запропоновано протокол доведення знання розв'язку задачі Діффі–Хеллмана з нульовим розголошенням, де у криптографічних перетвореннях використовуються білінійні спарювання точок еліптичної кривої. Як і будь-який із запропонованих в літературі протоколів доведень з нульовим розголошенням він може використовуватись як схема аутентифікації.

Література

1. Введение в криптографию / [Ященко В. В., Варновский Н. П., Нестеренко Ю. В. и др.] . – [3-е изд.]. – М. : МЦНМО : «ЧеРо», 2000. – 288 с.
2. Криптография в банковском деле / [Анохин М. И., Варновский Н. П., Сидельников В. М., Ященко В. В.]. – 1997.
3. Babai L. Trading group theory for randomness / Proceeding STOC '85 Proceedings of the seventeenth annual ACM symposium on Theory of computing, 1985. – P. 421–429.
4. Babai L. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes / L. Babai, S. Moran // Journal of Computer and System Sciences. – 1988. – Vol. 36. – № 2. – P. 254–276.
5. Goldwasser S. The knowledge complexity of interactive proof systems / S. Goldwasser, S. Micali, C. Rackoff // Proceeding STOC '85 Proceedings of the seventeenth annual ACM symposium on Theory of computing, 1985. – P. 291–304.
6. Goldwasser S. The knowledge complexity of interactive proof systems / S. Goldwasser, S. Micali, C. Rackoff // SIAM J. on Comput. 1989. – Vol. 18. – № 1. – P. 186–208.
7. Goldreih O. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems / O. Goldreih, S. Micali, A. Wigderson // J.ACM, 1991. – Vol. 38. – № 3. – P. 691–729.
8. Schnorr C. P. Efficient identification and signatures for smart cards / Advances in Cryptology : Proceedings of CRYPTO '89, 1990. – Vol. 435. – P. 239–252.

A. Kulaga

ZERO-KNOWLEDGE PROOF OF DIFFIE–HELLMAN PROBLEM SOLUTION

The paper contains main concepts of the interactive proof theory and suggests zero-knowledge proof of Diffie–Hellman problem solution with bilinear maps.

Keywords: interactive proof, zero-knowledge, bilinear map, Diffie–Hellman problem, authentication.

Матеріал надійшов 15.11.2011