Кравцов Г.О., директор ТОВ «НВФ «БКП-Консалтинг», м.Київ.

Однонаправлена функція. Базові визначення та теореми.

Брюс Шнайєр в своїй книзі «Прикладна криптографія» в розділі «2.3. Однонаправлені функції» говорить: «Поняття однонаправленої функції є центральним в криптографії з відкритим ключем. Не будучи протоколами безпосередньо, однонаправлені функції є наріжним каменем більшості протоколів, що обговорюються в цій книзі

Однонаправлені функції легко обчислюються, але інвертуються насилу. Тобто, знаючи x легко обчислити $f(x)$, але по відомому $f(x)$ обчислити x нелегко. Тут, «нелегко» означає, що для обчислення x по $f(x)$ можуть знадобиться мільйони років, навіть якщо над цією проблемою битимуться всі комп'ютери миру.

Хорошим прикладом однонаправленої функції служить розбита тарілка. Легко розбити тарілку на тисячі дрібних осколків, проте нелегко знову скласти тарілку з цих шматочків.

Це звучить красиво, але туманно і незрозуміло. Математично строгого доказу існування однонаправлених функцій немає, немає і реальних свідоцтв можливості їх побудови. Не дивлячись на це, багато функцій виглядають в точності як однонаправлені: ми можемо розрахувати їх і, дотепер, не знаємо простого способу інвертувати їх. Наприклад, в обмеженій області легко обчислити x^2, але набагато складніше $x^{\frac{1}{2}}$. У частині розділу, що залишилася, я прикинуся, що **однонаправлені функції існують**».

Дозвольте послатися на думку Б.Шнайєра і сформулювати все ж таки гіпотезу про існування однонаправлених функцій (далі - ОФ) і спробувати довести її справедливість.

Автор чудово розуміє, що «красивого» математичного доказу можливо ніколи і не одержить, проте, слідуючи принципу «дорогу осилить той, хто йде», прикладе максимум зусиль для досягнення поставленої мети.

Основи

Однонаправленою функцією $A = f(B)$ *в деякому полі* F *називається відображення* $B \to A$, *де* $A, B \in F$, *таке, що поліноміальна складність знаходження значень* A *по відомим значенням* B *відображення* $B \to A$ *нескінченно мала по відношенню до поліноміальної складності знаходження значень* B *зворотного відображення* $A \to B$ *по відомим значенням* A.

Виходячи з визначення ОФ, цілком логічно буде поставити наступне питання: чому так важко знайти значення B по відомим значенням A? Намагаючись відповісти на це питання, ми можемо допустити, що складність інвертування полягає або в трудності (неможливості) аналітичного виразу значення аргументу через значення функції, або в неоднозначній відповідності значенню функції значенням аргументу.

По-перше, ми повинні сформулювати гіпотезу про існування однонаправленої функції.

Гіпотеза: *Існує така функція, що поліноміальна складність обчислення значення функції по відомому значенню аргументу нескінченно мала (не піддається визначенню через свою незначність), поліноміальна складність обчислення значення аргументу по відомому значенню функції прямує до нескінченності, через нескінченне число рішень, і не має зворотного аналітичного виразу (тобто не існує оберненої функції).*

Припустимо, що однонаправлених функцій не існує. Тоді не існує жодної функції такої, «що поліноміальна складність обчислення значення функції по відомому значенню аргументу нескінченно мала (не піддається визначенню через свою незначність), поліноміальна складність обчислення значення аргументу по відомому значенню функції прямує до нескінченності, через нескінченне число рішень». Якщо ми зможемо навести приклад функції, що задовольніть вимогам гіпотези, то наше припущення про відсутність існування однонаправленої функції буде помилковим.

Звернемо увагу на функцію $f(x) = const$, що не вимагає навіть елементарних обчислень значення функції по відомому значенню аргументу, а по відомому значенню функції кількість значень аргументу нескінченно, а зворотне відображення не має сенсу і не може бути виражено в аналітичному вигляді.

Теорема: *Однонаправлені функції існують.*

Будь-яка інша функція на різницю від $f(x) = const$ у меншій мірі задовольнятиме вимогам гіпотези. Для пояснення приведемо приклад функцій $f(x) = \sin(x)$ і $f(x) = const$, де $const = \frac{1}{2}$. При відомому значенні x потрібні більше зусиль, щоб обчислити значення функція $f(x) = \sin(x)$, ніж, щоб обчислити значення функції $f(x) = const$. Це і зрозуміло, оскільки обчислювати значення другої функції просто немає необхідності - воно дано в явному вигляді самим аналітичним виразом. Функція $f(x) = \sin(x)$ до того ж має всім нам відомий аналітичний вираз зворотної (оберненої) функції $x = (-1)^n \arcsin(\sin(x)) + \pi n$, де $n = 0; \pm 1; \pm 2; ...; \pm \infty$.

Якщо поставити задачу знаходження значення аргументу по відомому значенню функції, то вочевидь, що кількість рішень для функції $f(x) = \sin(x)$ значно менше, ніж для функції $f(x) = const$.

Теорема: Існує ідеальна однонаправлена функції, яка єдина, і має вигляд $f(x) = const$.

Докажемо теорему:

Ідеальна однонаправлена функція повинна відповідати вимозі максимуму ентропії. Враховуючи, що на відрізку (a, b), для значення функції $const$ рівноймовірно кожне з значень аргументу, то ентропія максимальна (згідно ознак ентропії). Теорему доведено.

Автор не претендує на найоптимальніший шлях доказу запропонованої їм теореми, але повинен визнати - ідеальна ОФ абсолютно даремна для практичної криптографії.

Не зважаючи на даремність запропонованої ідеальної ОФ, вона має своє унікальне місце в теорії, як всім відомий нуль для системи відліку.

Класифікація однонаправлених функцій.

Спочатку в даному підрозділі ми розглянемо декілька цікавих функцій, що мають певні ознаки однонаправленості (неоднозначне знаходження аргументу по відомому значенню функції):

Функція $f(x) = x^2$. Зворотна функція має вигляд $x = \pm\sqrt{f(x)}$ або $x = \pm\sqrt{x^2}$. І кожен, хто хоч трошки вивчав математику у школі, пам'ятає - рівняння другого ступеня має два кореня. Це і є першим чинником, що ускладнює пошук рішення.

Другим чинником є то, що обчислення самого кореня є більш складним, ніж возведення у другій ступень.

Функція модулю $f(x) = |x|$.Для кожного значення функції аргумент або дорівнює значенню функції, або є протилежним відносно нуля.

Функція $f(x) = \sin(x)$. Аналітичний вираз зворотної (оберненої) функції $x = (-1)^n \arcsin(\sin(x)) + \pi m$, де $n = 0;\pm1;\pm2;...;\pm\infty$, каже нам про існування великої кількості значень аргументу по відомому значенню функції. Аналогічна ситуація з функцією $f(x) = \cos(x)$, яка має зворотну функцію $x = \pm\arccos(\cos(x)) + 2\pi m$, де $n = 0;\pm1;\pm2;...;\pm\infty$. Неоднозначність значення аргументу по відомому значенню функції є наслідком періодичності функції, і в деякій мірі, обмеженості з гори та з долу.

Функція $f(x) = x \bmod p$. Результатом функції є залишок від ділення числа x на просте p націло.

Всі перелічені функції дуже відомі, тому не має сенсу приділяти їм більше уваги.

Виконавши низку досліджень, автор дійшов висновку, що ОФ бувають простими та складними. Прості поділяються на класи: базовомодульні, базовоперіодичні та базовосиметричні. Складні ОФ – функції, в яких зустрічається декілька простих класів.

Базовоперіодичні ОФ – клас функцій, в яких неоднозначність відповідності значення аргументна до значення функції обумовлена періодичністю. Періодичність таких функцій в основному обумовлюється тригонометричними функціями або функцією остатку від ділення націло.

Базовосиметричні ОФ – функції графік яких лінійно симетричний, в чому і полягає неоднозначність обчислення значення аргументу по відомому значенню функції. Базовосиметричні ОФ поділяються на базовоквадратичні та базовомодульні.

Базовомодульні ОФ – підклас базовосиметричних ОФ, в яких неоднозначність відповідності значення аргументна до значення функції визначається якостями арифметичного модуля.

Базовоквадратичні ОФ – підклас базовосиметричних ОФ, в яких неоднозначність відповідності значення аргументна до значення функції визначається квадратичною функцією і мають загальний вид $f(x) = x^{2n}$, де $n = \pm1;\pm2;...;\pm\infty$.

Слова подяки

В даній статті автор приводить дві теореми - теорему про існування однонаправленних функцій і теорему про існування ідеальної однонаправленної функції. Якщо станеться так, що теореми знайдуть своє місце в теоретичній криптографії, то в знак великої подяки автор просив би їх називати ім‘ям найулюбленішої вчительки з математики середньої школи №54 м.Миколаєва **Гедеш Ніни Михайлівни** (теорема про існування ідеальної однонаправленої функції) і людини, яка стала батьком автору після переїзду до Києва, партнера **Богатирьова Ігоря Олександровича** (теорема про існування однонаправлених функцій).

Бібліографія

Б.Шнаер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.-М.: Издательство ТРИУМФ, 2002 – 816 с.: ил. [стр.46-47]

Григорий А. Кравцов

Digitally signed by Григорий А. Кравцов
DN: cn=Григорий А. Кравцов, ou=SMTP, dc=org
Reason: I am the author of this document
Date: 2006.02.06 15:31:09 +02'00'