Защита информации

Павел Юдаев

МГТУ им. Баумана, Кафедра ИУ-9

Москва, 2014

Раздел 21 - Специальные протоколы

Цель: доказать что-либо другому, не сообщая доказательство и не добавляя никакой новой информации к тому, что другой знал априори. И чтобы было невозможно подделать доказательство.

Рассмотрим интерактивные доказательства.

Пример

Другой (V, verifier) не может различить два предмета, а я могу.
Я (P, prover) хочу доказать ему этот факт.
Выбрать один, спрятать, предъявить, выбрать. Повторить.
Если P не умеет различать предметы, вероятность его успеха равна 2^{-t}.

Определения

Пусть L - некоторый язык, т.е. подмножество слов из $\{0,1\}^*$.
Пусть $L \in \mathrm{NP}$.

Опр.

Пара алгоритмов (P, V) и правила их взаимодействия $(\leftrightarrow)$ являются интерактивным доказательством, если
1. Полнота. $\forall x \in L$ существует способ доказать этот факт, т.е. $\exists y \in \{0,1\}^*$ - описание доказательства: $(P(x, y) \leftrightarrow V(x)) \mapsto 1$.
2. Непротиворечивость. $\forall x \notin L, \forall P \in \mathrm{PT}, \forall y \in \{0,1\}^*$ вероятность того, что $(P(x, y) \leftrightarrow V(x)) \mapsto 0$, равна $1 - \varepsilon(|x|)$.
3. $V \in \mathrm{PPT}$, $P \in \mathrm{PPT}$ по $|x|$.

Протокол Файге, Фиата, Шамира.
Fiege-Fiat-Shamir.

1. Простые числа Блюма $p = 4k + 3$.
См. http://blog.cs.miami.edu/burt/2012/04/23/quadratic-residues-in-z-mod-a-blum-integer/

Утверждение

-1 - не QR в Z_p^*.

Док-во

Если $x^2 = a$, то $(-x)^2 = a$.
$x^2 = 1$ имеет не более 2 корней (осн. теорема алгебры). 1, -1 - корни.
Пусть $x^2 = -1$ имеет 2 корня в Z_p^*. Тогда множество корней 4 степени из 1 имеет мощность 4: $\{1, -1, i, -i\}$ и является группой по умножению. При этом $|Z_p^*| = p - 1$ не делится на 4.

Утверждение

Ровно половина членов Z_p^* являются QR.

Док-во

Пусть $x = y^2$ и $-x = y'^2$, тогда $(y/y') = -1$. Значит не более половины элементов - QR.
$\forall x^2 = a = (-x)^2$. Отображение 2 в 1, значит не менее полвины элементов - QR.

2. Числа Блюма $n = pq$, где p, q - простые числа Блюма.

Утверждение

$x^2 = y \bmod pq \Leftrightarrow x^2 = y \bmod p, \; x^2 = y \bmod q,$

Док-во

$x^2 = y + pqk$

$\Rightarrow x^2 = y \bmod p, \; x^2 = y \bmod q,$

исп. Китайскую Теорему об Остатках.

Утверждение

Если $c \in \mathbb{Z}_p$ - квадр. вычет, то $c^{1/2} = c^{(p+1)/4}$

Док-во

$c = 1 \cdot c = c^{(p-1)/2} c = c^{(p+1)/2} \bmod p.$

$c^{1/2} = c^{(p+1)/4} \bmod p.$

Опр.

Символ Якоби как произведение символов Лежандра.

$y = (\pm x_q)^2 \bmod q$, $y = (\pm x_p)^2 \bmod p$.
Т.к. по КТО $Z_p \times Z_q \simeq Z_{pq}$, если y - QR, в $Z_{pq}\exists$ ровно 4 корня из y: $(x_p, x_q), (-x_p, x_q), (x_p, -x_q), (-x_p, -x_q)$, из которых ровно один QR - пара (QR, QR). $J(QR) = +1$. При этом есть не QR a, у которых $J(a) = +1$. Аналогично предыдущему, ровно половина элементов Z_{pq} имеет $J(a) = +1$, и ровно половина из этих являются QR. $J(-1) = +1$.

3. Протокол идентификации:
3.1.
$s \neq \pm 1$ - секретное значение. $v = s^2$ - публичное значение. Размещено в справочнике как ключ Peggi.

Peggy: $r \stackrel{R}{\leftarrow} Z_n^*$, $z \stackrel{R}{\leftarrow} \{-1, 1\}$ и вычисляет $x = z \cdot r^2 \bmod n$.
Отправляет x to Victor.
Victor выбирает $b \in \{0, 1\}$. Victor отправляет b Peggy. - Найти корень из xv или x.
Peggy вычисляет $y = rs^b \bmod n$. Peggy отправляет y to Victor.
Victor проверяет, что $y^2 = \pm xv^b \bmod n$.

Для простоты, пусть $z = 1$.

Доказать:

3.1.1. Полнота. (Очевидно.)

3.1.2. Непротиворечивость.

E не знает s.

- Предполагает, что $b = 0$. Выбирает r, выч. $x = r^2$, $y := r$.
- Предполагает, что $b = 1$. Выбирает r, выч. $x = r^2 v^{-1}$, $y := r$.

Шанс угадать - $1/2$. После t раундов - $1/2^t$.

3.1.3. Не разглашение информации.
Что узнает зл-к, слушающий канал?
$b = 0$. (x, y) где y - случ. число, x - его квадрат $\bmod n$. Не зависят от s.
$b = 1$. $(x, y) = (r^2 \bmod n,\ rs \bmod n)$.
r - произв. случайный эл-т, значит rs - тоже произв. случайный. Не выдает инф. об s.
$x = y^2 * v$, v - пуб. ключ, y - изв. и так. Это можно выч. самост-но. Не выдает инф. об s.

$x \in \{a | J(a) = +1\}$, любое, случайное.
Знак $z = \pm 1$ нужен. Без него V узнает, что присланное ему число x - QR. Это новая информация.
Ч.т.д.

3.1.4. Повторное использование r.
Предположим, что переданы $y_0 = r$ и $y_1 = rs$ удовл. равенствам $y_b^2 = xv^b \bmod n$.
след-но $y_0^2 = x \bmod n$ и $x = y_1^2 v^{-1} \bmod n$.
решая их отн. v, находим
$v = y_0^{-2} y_1^2 \bmod n$
т.е. нашли $v^{1/2} = y_0^{-1} y_1$ без факторизации n.

3.2. Параллельная версия.

s_i - секретные значения.
$v_i = s_i^2$ - публичные значения. Размещены в справочнике как ключ Peggi.

Peggy выбирает $r \overset{R}{\leftarrow} Z_n^*$, $z \overset{R}{\leftarrow} \{-1, 1\}$ и вычисляет $x = z \cdot r^2 \bmod n$. Отправляет x to Victor.
Victor выбирает $b_1, ..., b_k$, $b_i \in \{0, 1\}$.
Victor отправляет их Peggy.
Peggy вычисляет $y = rs_1^{b_1} ... s_k^{b_k} \bmod n$. Peggy отправляет y to Victor.
Victor проверяет, что $y^2 = \pm x v_1^{b_1} ... v_k^{b_k} \bmod n$.
Вероятность имперсонализации после t раундов - $1/2^{kt}$.

Пример.

$n = 7 * 11 = 77$. (В реальности длина n - 1024 бита.)

$\varphi(7 * 11) = 60$. $|QR(Z_{77}^*)| = 15 = 60/4$, все имеют обратные.

$QR(Z_{77}^*) = \{1, 4, 9, 15, 16, 23, ...\}$.

Пуб. ключ $\{v_i\} = \{4, 9, 15, 23\}$

$\{v_i^{-1}\} = \{58, 60, 36, 67\}$

Секр. ключ $\{v_i^{-1/2}\} = \{17, 26, 6, 12\}$

1) A: случ. $r = 9$, $z = +1$, $9 \cdot 9 \bmod 77 = 4$ -> B
2) B -> A: 1101
3) A: $z \cdot 9 \cdot (17^1 \cdot 26^1 \cdot 6^0 \cdot 12^1) \bmod 77 = 73$ -> B
4) B: провер. $73^2 \cdot 4^1 \cdot 9^1 \cdot 15^0 \cdot 23^1 \bmod 77 = \pm 4$ - верно.

Идентификация с помощью этого протокола.

Пусть I - информация о человеке A (уникальный ID). Арбитр T знает простые $p, q, n = pq$. Пусть H(x) - криптографическая хэш-функция. Пусть $x = I||j$ - конкатенация I и нек. небольшого числа j.

T находит набор j (перебором...) таких, что $H(I||j)$ - квадр. вычет по мод. n. Он может каждую проверку делать быстро.

След-но, имеет набор $v_j = H(I||j)$. Открытый ключ для A - I и набор значений j. Удостоверен подписью T. Секретный ключ A - корни из v_j.

После проведения авторизации (A перед B) по выше указанному протоколу, B удостоверяется, что T удостоверил факт того, что I и j принадлежат A: он сообщил A корни из v_j.

Раздел 21 - Специальные протоколы

Схема интерполяционных полиномов Лагранжа
Автор - Шамир (Shamir)

Это пороговая схема (t, n): n - число долей, на которые был разделен секрет, t - число долей, которые необходимы, чтобы его восстановить.

Используются полиномы над конечным полем.

M - секрет. Выберем простое $p : p > n$, $p > \max_{M \in \mathbb{M}} M$.

Чтобы разделить секрет, создадим произвольный полином степени $t - 1$. Например, для $(3, n)$ схемы - степени 2. При этом свободный член - это всегда наш секрет M.

$F(x) = (ax^2 + bx + M) mod\ p$

a, b - случ., секретные, после разделения секрета не нужны.
p - известно всем.

Доли секрета получаются путем выч-я полинома в n точках:
$K_i = F(x_i)$.
Др. словами, первая доля может быть получена как $F(1)$, вторая $F(2)$ и т.д.

Для восстановления полинома степ. $(t - 1)$ по его значениям, необх. и достаточно знать его значения в t точках.

Пример 1: можно создать схему, когда секрет делится между 5 участниками, и любые 3 могут его восстановить.

Пример 2: можно создать схему, когда секрет делится между N участниками, при этом первый участник может его восстановить, скооперировавшись с любым из остальных.

Решение: например, первому сообщаем $t-1$ долей секрета, остальным по одной. Варьируя кол-во долей у каждого, а также t, можно, например, добиться, что участие первого необходимо для раскрытия секрета: он получает $t/2+1$ долю, остальные - по одной.

Пример 3: Пусть есть 2 группы людей, A и B. Хотим, чтобы набор любых двух людей из A и трех из B вместе могли восстановить секрет.

Решение: полином - произведение линейной и квадратичной ф-й. Значения линейной ф-и в ряде точек сообщают людям из A, значения квадратичной - из B. Только соравшись вместе, они могут восст. секрет.

Векторная схема
автор - Blakley.

Секрет - точка в t-мерном пр-ве. Каждая доля - ур-е $(t-1)$-мерной гиперпл-ти (или меньшей размерности), содержащей эту точку. Пересечение опред. числа г-пл-тей (непаралл., несовп.) однозн. определяет точку.

Пример: 3 доли. 3-мерное пространство. Доля - ур-е пл-ти. Две доли определяют прямую. Все три определяют точку.

Сущ. и другие схемы.

Раздел 21 - Специальные протоколы

Авторизации без раскрытия информации

Разделение секрета

Подбрасывание монеты по телефону

А и В подбрасывают монету по телефону. Коммуникация только последовательная. Арбитра нет.

1. А выбир. случ. p, q - простые числа Блюма ($\equiv 3 \bmod 4$), выч. $n = pq$, отправляет n В.

2. В выбир. $x \xleftarrow{R} Z_n$, выч. $y \equiv x^2 \bmod n$, отпр. y А. y - квадр. вычет.

3. А выч.
$z_p \equiv y^{(p+1)/4} \equiv y^{1/2} \bmod p$,
$z_q \equiv y^{(q+1)/4} \equiv y^{1/2} \bmod q$.

А знает все 4 корня квадратных из $(y \bmod p, y \bmod q)$ в $Z_p \times Z_q$:
$(\pm z_p, \pm z_q)$, знаки независимы.

Кит. т. об ост. (изоморфизм) $\Rightarrow$ знает корни из y в Z_n: обозн. $(\pm w, \pm \tilde{w})$.

В одну из этих пар входит исходный $x: \ y \equiv x^2 \bmod n$. А не знает, в какую.

4. А пытается угадать, в какой паре есть x. А выбир. одну из пар, напр. $\pm w$, отпр. В.

5. Если А не угадала, т.е. $x \not\equiv \pm w \bmod n$, В выиграл. Он это доказывает, присылая А факторизацию $n = pq$.

Обоснование: в этом случае В знает все 4 корня из y: $\pm w, \pm \tilde{w}$.
Справедливо тождество $w^2 - \tilde{w}^2 \equiv 0 \bmod n$
$\Rightarrow (w - \tilde{w})(w + \tilde{w}) \equiv 0 \bmod n$
$\Rightarrow w - \tilde{w}$ кратно одному из p, q и НОД$(w - \tilde{w}, n) \in \{p, q\}$.

(Иначе $w + \tilde{w}$ кратно $pq \Rightarrow w = -\tilde{w}$.)

Литература к лекции:

1. Fiege, Fiat, Shamir. *Zero Knowledge Proofs of Identity*
`http://www.fi.muni.cz/~xslaby/kr/9/p210-fiege.pdf`

2*. *Zero-knowledge for graph isomorphism*,
`http://www.cs.cornell.edu/courses/cs687/2006fa/lectures/lecture21.pdf`

3. *Coin Flips by Telephone*.
`http://people.reed.edu/~jerry/361/lectures/coins.pdf`