02.06.2021

Coin-flipping by telephone

(интересно генериране на случайни числа)

$$\boxed{x^2 \equiv a \pmod n} \qquad (*)$$

$n = pq$

$$\begin{cases} x^2 \equiv a \pmod p \\ x^2 \equiv a \pmod q \end{cases} \qquad \begin{matrix} \pm\alpha \text{ корени} \\ \pm\beta \text{ корени} \end{matrix}$$

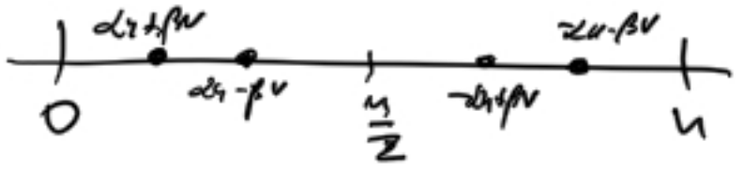
$$\begin{cases} u \equiv 1 \pmod p \\ u \equiv 0 \pmod q \end{cases} \qquad \begin{cases} v \equiv 0 \pmod p \\ v \equiv 1 \pmod q \end{cases}$$

$\pm\alpha u \pm \beta v$ са всички

корени на $x^2 \equiv a \pmod n$

$\alpha u + \beta v \qquad -\alpha u - \beta v$

$\alpha u - \beta v \qquad -\alpha u + \beta v$



Задача. Да се генерира случаен бит от две партии без арбитър.

↓

всеки бит да се случва с вероятност $\frac{1}{2}$

Стъпка 1. А пуска две големи прости числа p и q (~300 цифри) умножава ги и съобщава произведението $n = pq$ на B.

Стъпка 2. B пуска случайно число (ъгъл) α от интервала $(0, \frac{\pi}{2})$, $(\alpha, n) = 1$. (А дали, се числото ѝ пуска от допълнителното на $(0, n)$.)

B съобщава на A квадрата

$$a = \alpha^2 \pmod n$$

Стъпка 3. А пресмята горните квадратни корени на a:

$$\pm\gamma, \pm\delta$$

Тук е възможно, тъй като A вече разлагаемо на n на прости множители.

Ясно е, че едно от $\pm\gamma$ е в $(0, \frac{n}{2})$, а другото е в $(\frac{n}{2}, n)$

Аналогично за $\pm\delta$.

Ще приемем, че $\gamma, \delta \in (0, \frac{n}{2})$.

Стъпка 4. А се опитва да отгатне дали $\alpha = \gamma$ или $\alpha = \delta$.

То-специално, A намери най-малкото i, в което γ и δ се различават и сравнява a в тях и възможностите:

"i-тия бит на твоето число α е 0"
или
"i-тия бит на твоето число α е 1".

<u>Стъпка 5.</u> B отговаря на A дали изборът е правилен (ези, 1) или грешен (тура, 0).

<u>Стъпка 6.</u> По-късно B получава от A числото α и A проверява, че наистина $a = \alpha^2 \pmod{n}$

<u>Стъпка 7.</u> A разкрива на B разлагането на n на прости множители.

Обща схема за генериране на случаен бит

- A и B са се договорили за едноместна функция $f(x)$
  $f(x)$ се смята лесно,
  $f^{-1}(x)$ се смята трудно.
- B пуска случайно число x и съобщава на A - $f(x)$
- A прави някакво предположение за някое свойство на x, което се случва с вероятност $\frac{1}{2}$
  (например дали x е четно или не).
- B казва на A дали предположението е правилно или не
- B връща на A числото x.

Още един протокол

Стъпка 1. В първия просто число p и q и отбелязва на A произведението $n = pq$, както и случайно число a, за което

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right) = 1$$

Стъпка 2. A се опитва да отгатне дали a е квадратичен остатък по модул n

Стъпка 3. В зависимост от A дали първият е правилно или не.

Стъпка 4. В редицата пред A просто p и q.

В стъпка 4 е важно А да провери, че p и q наистина са прости. В противен случай В може да мисли по следния начин:

В първо три прости числа p_1, p_2, q_1 и число a:

$$\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = -1 \,, \quad \left(\frac{a}{q_1}\right) = 1$$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{a}{q_1}\right) = 1$$

Ако В иска „еди" (А е отгатнал правилно)

- В редица $p = p_1 p_2$, $q = q_1$ в случай, че А може „остане"

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right)\cdot\left(\frac{a}{p_2}\right) = (-1)\cdot(-1) = 1, \left(\frac{a}{q}\right) = 1$$

- В редица $p = p_1$, $q = p_2 q_1$

$$\left(\frac{a}{p_1}\right) = -1 \,, \left(\frac{a}{pq}\right) = \left(\frac{a}{p_2}\right)\cdot\left(\frac{a}{q_1}\right) = (-1)\cdot 1 = -1$$

Ако B иска да излъже A, че A е отгатнал неправилно:

- B разкрива $p = p_1$, $q = p_2 q_1$, ако A каже остатък;
- B разкрива $p = p_1 p_2$, $q = q_1$, ако A каже неостатък.