9 Отпечатки пальцев

Задача. Боб использует в качестве пароля случайную двоичную строку длины n. Пароль вводится на сенсорном устройстве Dapi. Виктор может разглядеть отпечатки пальцев Боба и узнать, сколько в пароле единиц и сколько нулей. Виктор может воспользоваться наблюдениями и уменьшить число паролей, которые требуется проверить. Если, например, Виктор знает, что в пароле ровно одна единица, то ему требуется проверить не 2^n, а только n паролей. Во сколько раз уменьшается среднее число паролей, которые требуется проверить Виктору?

Решение. В случайном пароле встретится k единиц и, соответственно, $n-k$ нулей с вероятностью $2^{-n}\binom{n}{k}$. Для такого пароля Виктору потребуется проверить $\binom{n}{k}$ вариантов. Таким образом, среднее число вариантов есть $2^{-n}S(n)$, где

$$S(n) = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}.$$

Сумма $S(n)$ совпадает с коэффициентом при x^n в произведении

$$(x+1)^n(1+x)^n = \left(\sum_{k=0}^{n} \binom{n}{k}x^k\right)\left(\sum_{k=0}^{n} \binom{n}{n-k}x^{n-k}\right).$$

Но $(x+1)^n(1+x)^n = (1+x)^{2n}$ и, следовательно,

$$S(n) = \binom{2n}{n}.$$

Воспользовавшись формулой Стирлинга, получаем

$$2^{-n}S(n) \sim \frac{2^n}{\sqrt{\pi n}}.$$

Как видим, среднее число паролей, которые требуется проверить Виктору, уменьшается (асимптотически) в $\sqrt{\pi n}$ раз. □