Алгебраическое представление хэш-функции SHA-256 и его использование в атаках на систему Биткойн

Соколов Александр Андреевич

Аспирант

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: alexandro9608@gmail.com

Научный руководитель — *Черепнёв Михаил Алексеевич*

Платёжная система Биткойн [1] считается одной из наиболее защищенных платёжных систем в настоящее время. В основе её стойкости лежит принцип доказательства выполнения работы (Proof-of-Work), суть которого заключается в защите от атак вида на архитектуру , а также в организации защиты серверов от спама [2].

Принцип доказательства выполнения работы подразумевает решение некоторой вычислительно сложной задачи на стороне клиента, решение которой было бы легко проверить на стороне сервера. В качестве подобной задачи в работе [3] была предложена задача нахождения прообраза хэш-функции определённого вида, для которого значение хэш-функции содержало бы в начале своей двоичной записи некоторое заданное количество нулей. Говоря более формально, для заданной хэш-функции H требуется найти такое значение одноразового счётчика $nonce$, чтобы для входных данных s выполнялось условие

$$H(s||nonce) = 0^w||v, \tag{1}$$

где v — некоторое произвольное значение, w — заданное количество нулей, или *сложность* задачи (1).

В системе Биткойн хэш-функция H применяется дважды:

$$H(H(s||nonce)) = 0^w||v \tag{2}$$

В качестве хэш-функции в системе Биткойн используется хэш-функция SHA-256 [4].

В рамках доказательства выполнения работы участники протокола в системе Биткойн решают задачу (2) путём перебора 32-битного значения счётчика $nonce$. При этом максимальная сложность вычислений не превосходит 2^{32} вычислений хэш-функции SHA-256.

В настоящей работе функции, использующиеся в хэш-функции SHA-256, представляются в виде многочленов над кольцом $R =$

$\left\{\frac{2\mathbb{Z}+1}{2^s}, s \in \mathbb{Z}\right\}$ с целью решения уравнения вида

$$F(nonce) \equiv 0 \pmod{2^{32}}, \tag{3}$$

где $F(nonce) \in R[nonce \pmod 2, nonce \pmod 4, \ldots, nonce]$.

Таким образом, в работе предлагается метод сведения задачи (2) к решению уравнения (3). Кроме того, для решения уравнения (3) был предложен эффективный метод.

Литература

1. Документация системы Биткойн: `https://en.bitcoin.it/wiki/Main_Page`
2. Dwork C. Naor M. Pricing via Processing or Combatting Junk Mail
3. Back A. Hashcash — A Denial of Service Counter-Measure
4. Стандарт NIST, содержащий описание алгоритма SHA-256: `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf`