2019年10月3日 午後2:41

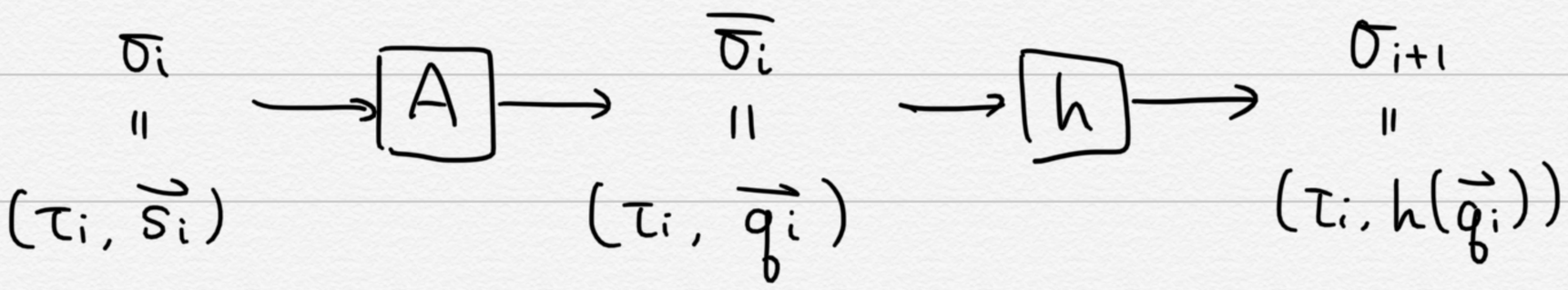
Leo scrypt paper notes

§2. Preliminaries

State : $\sigma = (\tau, \vec{s})$ of type (str, str[])

A round of operation (diagram)

(STATE$_i$) (SCRYPT EVALUATOR) (RANDOM ORACLE) (STATE$_{i+1}$)



Measure of Complexity

string $x \longmapsto |x|$

state $\sigma = (\tau, \vec{s}) \longmapsto |\tau| + \sum_{\text{all } i} |s_i|$

evaluation $A^h(x) = A^h((\tau_x, \vec{s}_x)) \longmapsto \sum_{\text{all } i} |\sigma_i|$

CCmem

N.B. input to h doesn't matter

Scrypt Naive Implementation.

Ommitted

Graph pebbling.

Start with a DAG. The rules are:

① if pre($v \in V$) all pebbled, v can be pebbled

② if v is pebbled in $t-1$, v can be pebbled.

Notations: 1. $pre(v)$: all predecessors of v.

2. U^+ : { all nodes that can be pebbled by rule 1
because of U.

Obviously: $P_{t+1} \subseteq P_t \cup P_t^+$

DEF: cumulative pebbling complexity : $(\sum_{all\ i} |P_i|)$

N.B. pebbling in this paper do not allow pebbling source at no cost.
(differs from Alwen paper)

This paper considers pebbling w/ rounds.

each round a new sink is revealed

§3. Main result & overview.

Thm 1. Scrypt-mem-hardness thm

$\forall X \in \{0,1\}^w . \forall n \in \mathbb{Z}_{>2} . \forall A \in$ function

$$P[A^h(X,n) = scrypt^h(X,n)] = \chi \Rightarrow$$

$$P[CC_{mem}(A^h(X)) > \frac{1}{25} \cdot n^2 \cdot (w - 4\log n)] \geq \chi - 0.08 n^6 \cdot 2^{-w} - 2^{-n/20}$$

Interpretation:

When w is large w.r.t. n : $CC_{mem} A^h(X) \in \Omega(n^2 w)$ w.h.p.

note this is best result possible since it's consistent w/ naive scrypt.

※ The rest of the paper proves the theorem

§4 - §6 are proofs. outlined below.