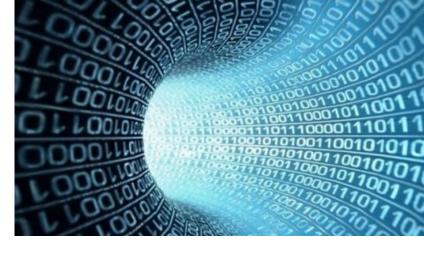# SAMSON ZHOU

PhD Candidate
Purdue University
Expected Graduation: May 2018

Advisors: Greg Frederickson and Elena Grigorescu

Finding Structure in Noisy Data Streams

❖ Motivation: Removing regions of low complexity to preprocess

❖ Resilient to k human error, noise, or mutation

❖ $O(poly(k, \log n))$ space algorithms for periodicity, palindromes, alignments

ITCSPATTERNMEVKBYDQCDPLOILMUUPATTERNBOSTON
PERIODPERIODPERIODPERTHEORYSCASMITBXCAUONZ
IOLONGPALINDROMEEMORDNILAPGNOLBOMBCYCLONE
STREAMINGALGORITHMSALIGNMENTEIBHLAKISNDFIWE
YGOVGRADUATINGBITSIIIALIGNMENTIGENASDFIEMIXAS

Graph Pebbling for Password Hashing

❖ Motivation: Server attacks inevitable, try to mitigate offline attacks

❖ Specialized hardware (ASIC) can compute 10^{12} hashes per second.

❖ Black pebbling = computing memory hard functions

❖ Red-blue pebbling = computing bandwidth hard functions

❖ Complexity of functions proposed for IRTF standardization

$pwd \rightarrow h_1 \rightarrow h_2 \rightarrow h_3 \rightarrow h_4 \rightarrow h_5 \rightarrow h_6 \rightarrow h_7$

$$h_6 = H(h_4, h_5)$$