Security of Very Dense Cryptography

Jon Callas, Tamzen Cannoy, Nicko van Someren

Introduction

- Scientists have long known that stupidity is the most common element in the universe, even more than hydrogen

Introduction

- Recent advances show that it consists of more than 90% of everything
- This substance was thought to be dark matter, but turns out to be merely very dim

Properties

- Very useful for quantum systems
  - Easily entangled
  - Hard to unentangle
  - Greatly reduced decoherence issues

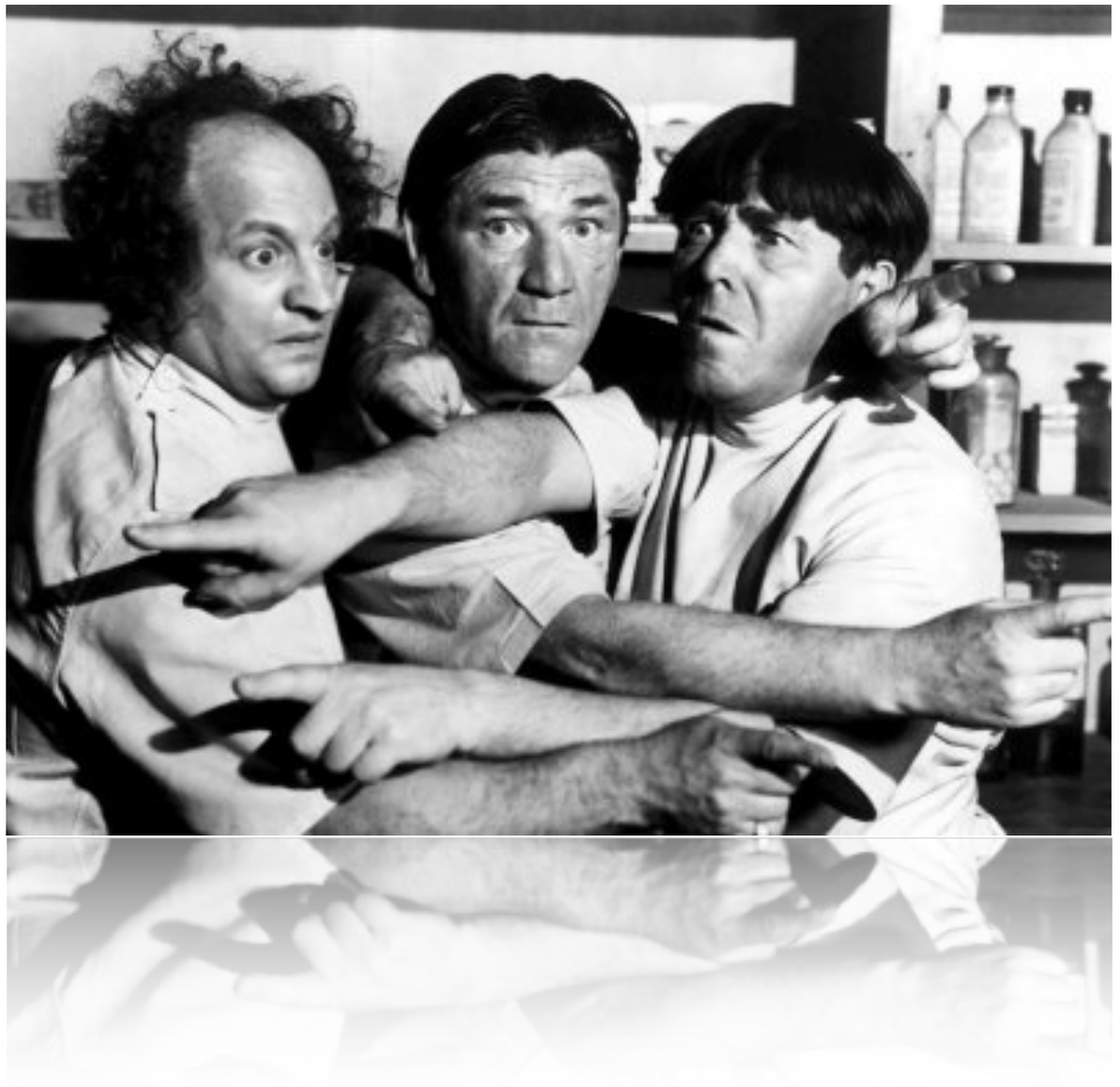
Lack of Complexity

- Emulated dim matter possible with usable limits
- Tosh-Marley Theorem shows that iterated hash leads to very dense systems.
- Leads to using stupidity to generate high-quality PRFs

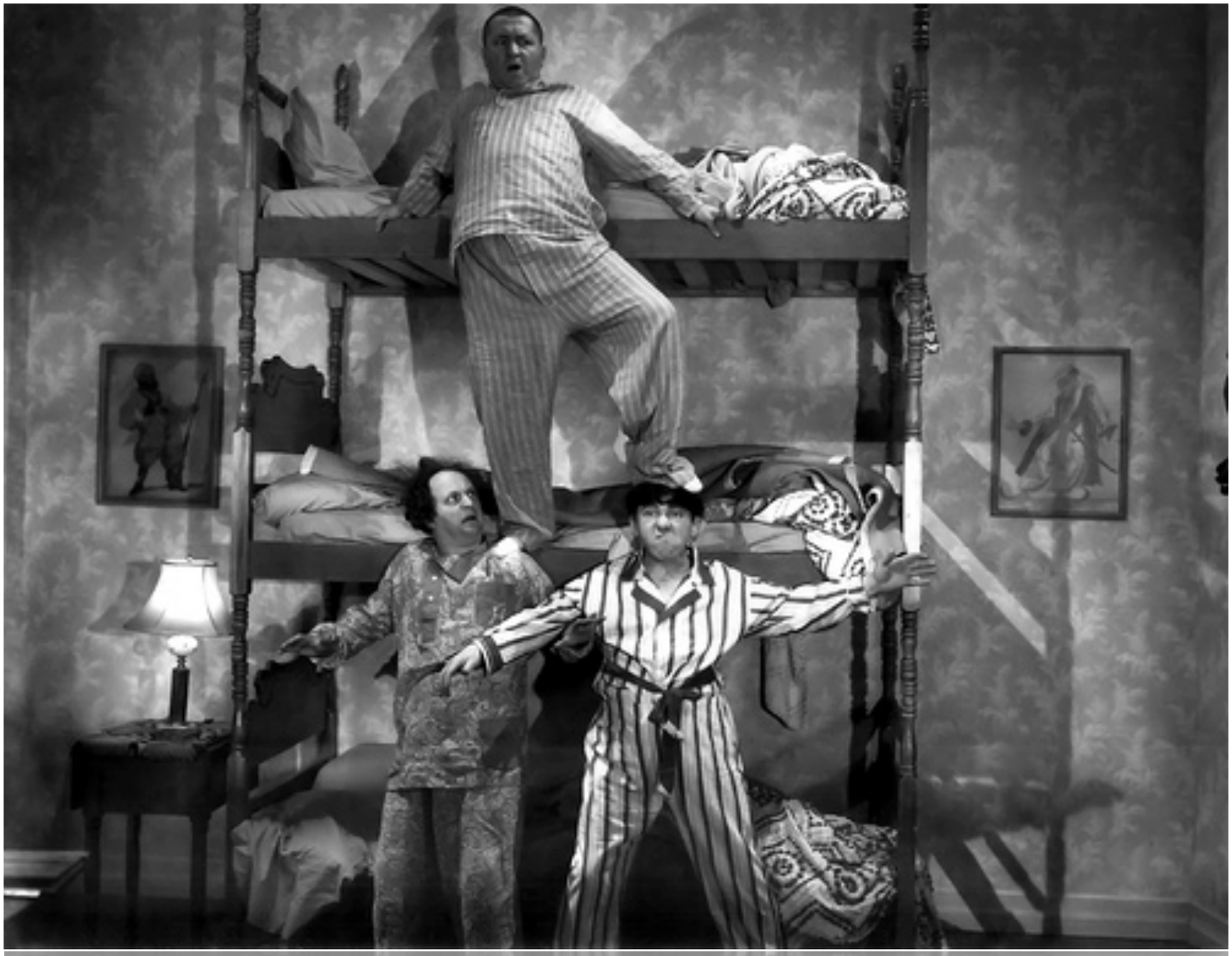
Physical Dimness

- Recent work at the CERN-LHC has identified six elementary dim particles
- Pictures also obtained

Six Dim Particles



Dim Particles Entangled



Dim Particles Entangled

Very Dense Encryption

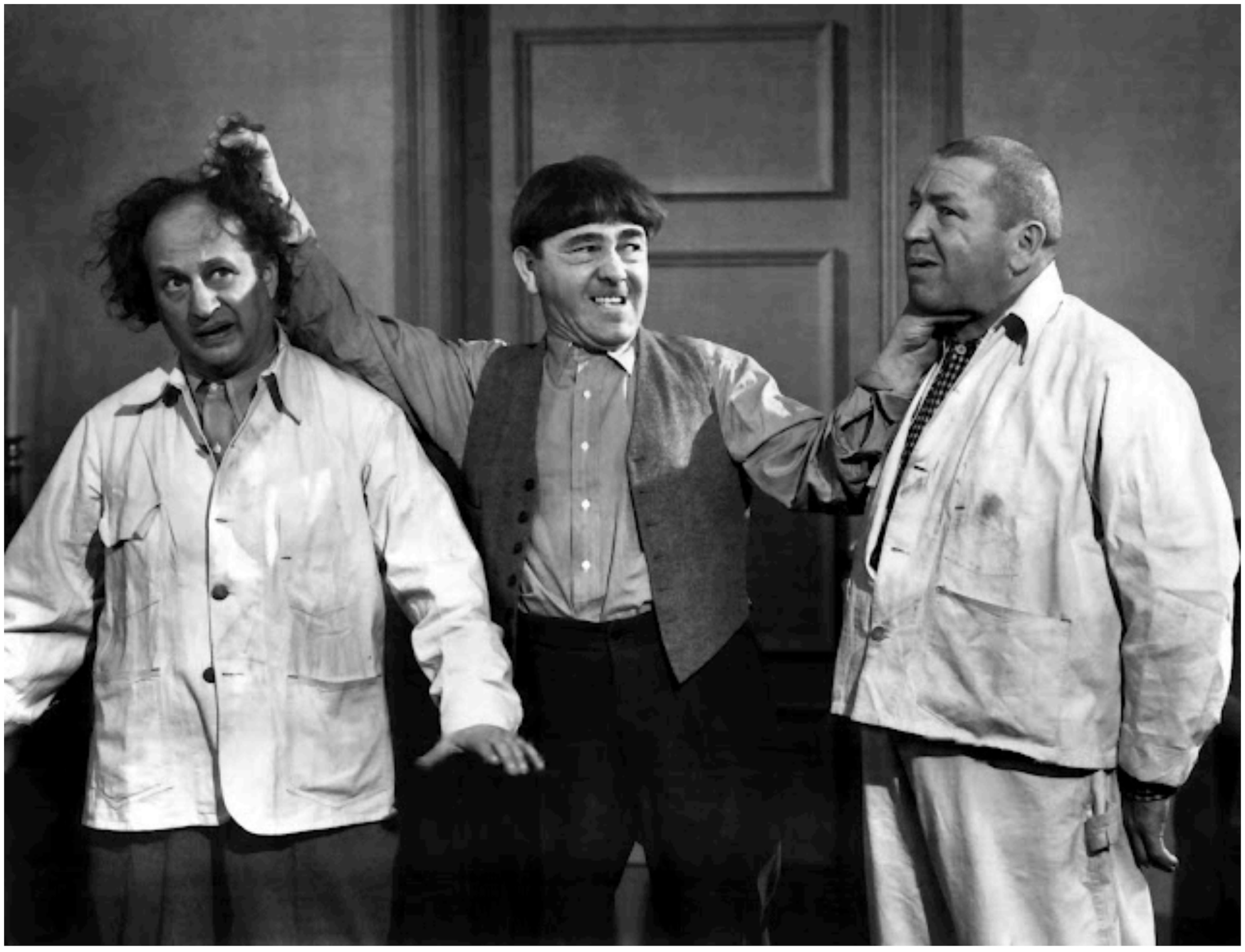
- Similar to Zero-Knowledge Systems
  - Except has less than zero knowledge
    - Quasi-knowledge leads to universal one-way arguments
    - Easily expandable into Dysfunctional Encryption

Dysfunctional Encryption

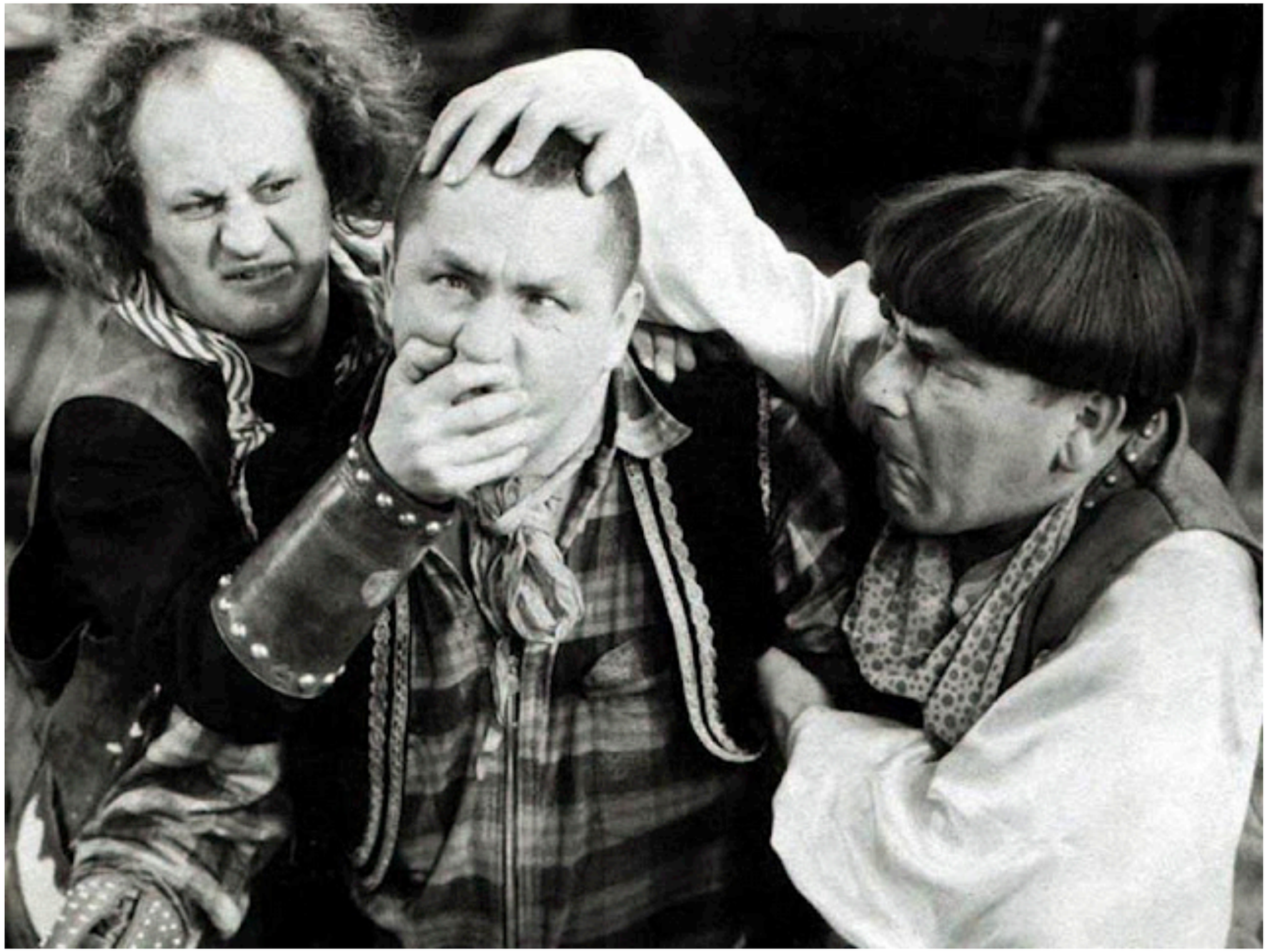
- Knucklehead Cipher
- Assembles iterated dimness through an S-P (Slapstick-Permutation) Network

Pseudo-Random Scuffle

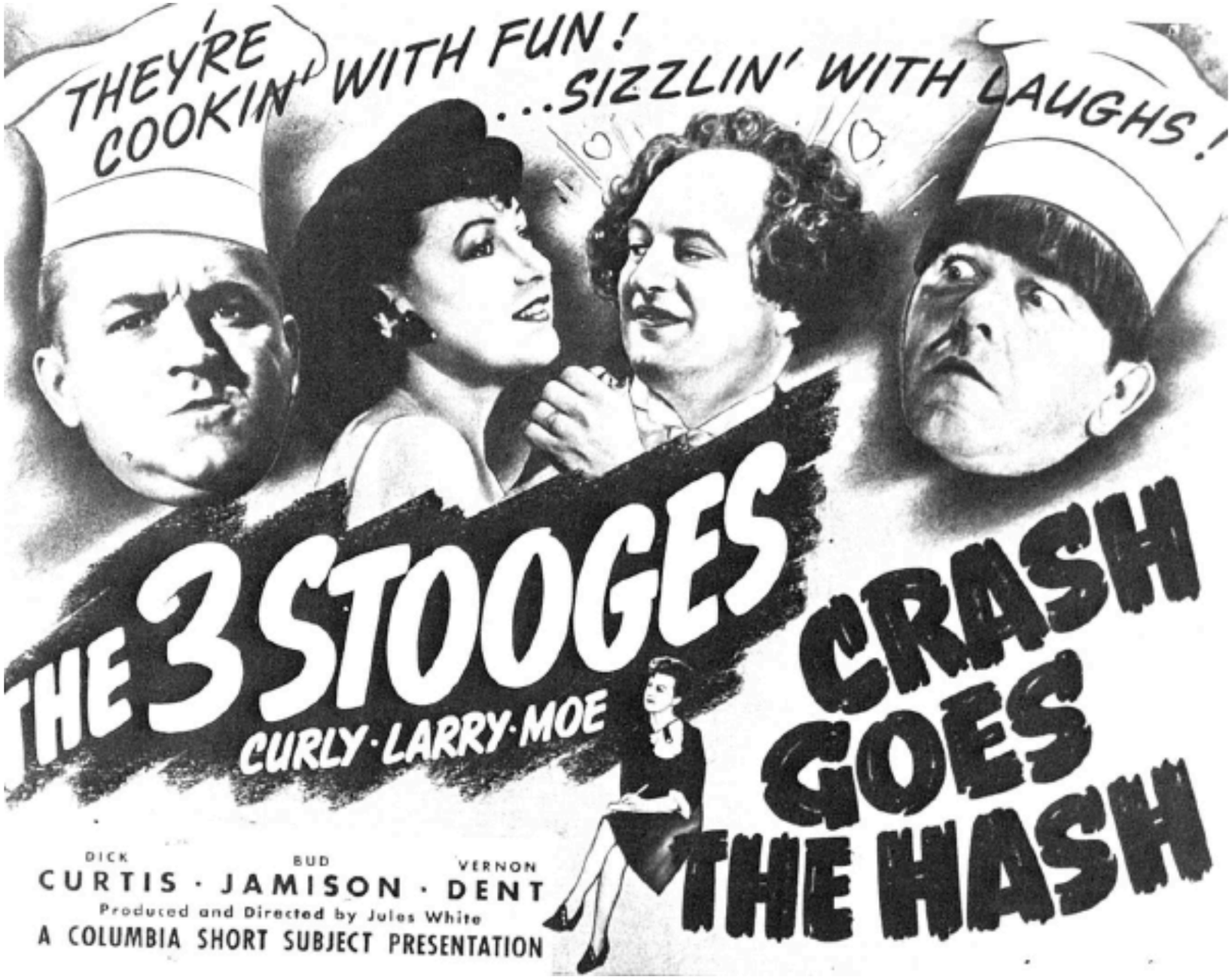
- Uses the "*Slap-or-Scuffle*" network
- Each bit is subjected to a series of pokes, jabs, hair pulls, etc.
- Bits defend themselves via blocks, dodges, sheer obliviousness as well as counter-attacks
- Iterated over 845 rounds (a.k.a. "shorts") to produce a PRP



Slap-or-Scuffle



Oblivious Bit Defense



Cryptanalysis Applications

Cryptanalysis & Unnatural Proofs

- Linear Cryptanalysis
  - Following bits across multiple S-boxes leads to wincing, laughter, and confusion
- Differential Cryptanalysis
  - After less than 845 rounds, cryptanalysts can no longer distinguish the CCA difference between shorts $\leq 10^{-10}$

Current Work

- Application to analyzing Three Card Monte as a protocol between dim particles
  - Not presented here because it was actually a good paper
- Privacy applications
  - This work was aided by a grant from MSR, which wishes to remain anonymous