Maybe Non Number Theory Cryptography is Worth Trying

Steve Meyer - Pragmatic C Software Corp.

1. Claim: all complexity theory and cryptography is number theory

1. I do not think there is disagreement with this. Calculating with numbers is concrete and finite avoiding any foundational philosophical problems.
2. Current cryptography works and is self consistent. Decryption slowly progresses while encryption slowly uses larger numbers.

1. Problem is that Crypto does not contribute to computational thinking

1. There are developing Kuhnian crises in physics and philosophy of computation.
2. For the crisis in physics see Lee Smolin’s "The Trouble with Physics: The Rise of String Theory, The Fall of Science and What Comes Next". The crises can be viewed as the result of still using un-examined 19th century methods of calculating.
3. Computational complexity theory stopped progressing maybe as early as when complexity theory was redefined as polynomial time Turing machine complexity.

1. Complexity theory is just a Feyerabendian fairy tale

1. My claim here is more controversial. I claim that complexity theory is just definitions and explanations of consequences of definitions to create a closed and self consistent religion. For example, 'proving' multiple tapes do not increase computational power just restates the definition of unbounded tape.
2. Swiss mathematician Paul Finslers's simple example showed the definitions unconnected to reality problem. He used the following simple example:
    1. Write 1, 2, 3 and x on a blackboard.
    2. Define x to be the smallest number not on the blackboard
    3. x seemingly should exist.
    4. But if x is 4 then x becomes 5, but if x if 5 the smallest number not on the blackboard becomes 4.

1. Complexity theory's infinity problems

1. Compare Finslers example with this FSM transition description from Sipser's introductory textbook, p. 40: Delta(qj, 1) = qk where k = j + 1 modulo i
2. In Finsler's case we define x to be 4 by convention and in this case we agree an algebraic formula has meaning in describing an infinite table.
3. Try substituting integers for letters in language recognition theory and see how it appears. The attempted unconscious tie to the philosophy of human language disappears.

1. The two way Loschmidt paradox to Boltzmann's H equation

1. Physicists have been re-examining the Boltzmann H formula that gives the non equilibrium average number of gas molecules at position x with velocity v at time t.
2. The Loschmidt paradox says reverse the velocity at time t (run the film backwards) creating a system the has decreasing entropy and correlated molecules.
3. The existence of minus v is like Finsler's x. What is it. It may not exist, but such reversibility is needed by some mathematical formalisms for Quantum mechanics.
4. This suggests that use of information and information entropy in crypto arguments is just definition explication.
5. Can a public key crypto system be built using Boltzmann's mostly discrete calculation? If -v does not exist, maybe machines that implement one way functions can be built, but no one is trying.

1. Penrose's (and Godel's) claim the number of states of the brain is infinite

1. Some of the strongest skeptics of the 19th century molecular mathematics is Roger Penrose and his colleagues. One of Penrose's arguments is that AI is impossible because the number of states in the brain is infinite. He imagines some kind of molecular fluid process (ref. Shadows of the Mind).
2. Godel, at the end of his career, argued that the number of states of the brain was infinite from criticism of the Church-Turing thesis. If the Church-Turing thesis is wrong, there should be some better alternatives to P=NP complexity theory.

2. It seems that cryptography should be testing these problems