What did Polya Know about One Way Functions and Quantum Randomness

Steve Meyer - Pragmatic C Software Corp  
(sjmeyer@pragmatic-c.com)

I. Problem background observation from Leonid Levin paper.
   Cf. ’The tale of one way functions’ (available from his home page) and the speculations in the January 2003 issue of Journal of the ACM.

II. Problem area.
   Problem area is foundations of mathematics of computational complexity related to undecidability, diagonalization of languages and intuitive inconsistency of probabilism (Kolmogorov complexity?).

III. Levin quotation:
   The importance of [the randomness part of one-way functions] comes from their use in generating perfectly random bits from a small random seed s. In the case of permutation f, such generators are straightforward:

   \[ g_s(i) = b(f^i(s)), \ i = 0,1,2, \ldots \]
I. Is asymmetric cryptography a house of cards built on inconsistent foundations?

II. What did Polya know about cryptography?
I am focusing on on what the founders of quantum physics (QP) such as George Polya, Niels Bohr and Leonard Shiff (and Einstein?) knew about existence of such random seeds.

III. Feyerabend discusses QP founders view in detail.
Cf. section of Feyerabend’s collected works on foundations of QP (Vol. 1, pp 207-333).
I. **Polya criticism of current foundations of complexity.**
Polya knew that QP does not provide perfectly random seeds.

II. **Three value logic needed for QP?**
Reichenbach-Putnam three valued logic needed to make QC ’rational’ eliminates existence of one way functions. Three value logic means there is a ’physical’ concept of ’unknown’ (unobservable).
Remapping of symbols needed for Turing Machine proofs becomes impossible.
Reichenbach-Putnam connection of three value logic to non-Euclidean geometry and relativity theory can be used to criticize foundations of complexity theory.

III. **Bohm’s hidden variables.**
Bohm’s hidden variable theory is more applicable to foundations of mathematics than QP. Think backwards use QP to criticize current complexity.
I. **Bohr’s QP interpretation alternative to ’anomaly’ ridden probability theory.**
Bohr used mathematics and experimental results proven only at the atomic scale to ’disprove’ probability theory and he did it intensionally and rationally.

II. **Polya ’heuristic’ concept misunderstood.**
Polya’s heuristic concept was much closer to what we would call paradox or anomaly and applies to foundations of complexity theory.