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 probablism (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:

$$g_s(i) = b(f^i(s)),\ i = 0,1,2,\ ...$$