Steve Meyer's QCs as analog computers rump session references

My Eurocrypt 2019 slides are posted on the Eurocrypt conference web site rump session section. Here are the back ground references I said I would post. It still bugs me that cryptographers assume properties of QCs that do not correspond to physical reality.

Best introduction to ion trap quantum computers is is to listen to one of Chris Monroe's (U of Maryland professor and IonQ company CEO) physics colloquim presentations such as: https://www.youtube.com/watch?v=9aOLwjUZLm0 Also see web page https://ionq.co/resources for mostly PR and software simulation type articles. I think IonQ wants to run crypto algorithms (if interested contact them).

Here are references on von Neumann's thinking during his VNC design.

Aspray[1990] Aspray, W. *John von Neumann and The Origins of Modern Computing.* MIT Press, 1990.

Neumann[2005] Von Neumann, J. (Redei, M. ed.) *John Von Neumann: Selected Letters. History of Mathematics Series, Vol. 27,* American Mathematical Society, 2005.

Kohler[2001] Kohler, E. Why von Neumann Rejected Carnap's Dualism of Information Concepts. In Redei, M. and Stoltzner, M. (eds.) *John von Neumann and the Foundations of Quantum Physics.* Vienna Circle Institute Yearbook 8, Kluwer, 2001, 97-134.

Here are the references on Heisenberg's in my view too formal interpretation of Niels Bohr's Copenhagen interpretation and Paul Feyerabend's defense of Bohr. Also a reference from Popper falsifying quantum logic.

Heisenberg[1958] Heisenberg, W. *Physics and Philosophy - The Revolution in Modern Science.* Prometheus, 1958.

Heisenberg[1971] Heisenberg, W. *Physics and Beyond - Encounters and Conversations.* Harper, 1971.

Feyerabend[2016] Feyerabend, P. (Gattei, S. ed.) *Physics and Philosophy, Philosophical Papers Volume 4.*, Cambridge Press, 2016.

Feyerabend[1981] Feyerabend, P. Niels Bohr's world view. in *Philosophical papers. Vol. 1. Realism, Rationalism & Scientific Method.* essays appeared 1968,1969, 247-297, Cambridge, 1981.

Popper[1968] Popper, K. Birkhoff and Von Neumann's Interpretation of Quantum Mechanics. *Nature 219(1968),* 682-685.

Here is some sociological background on why Feyerabend stopped studying physics after 1970. A physicist claimed Feyerabend was an unskilled physicist in spite of his being invited to lecture to Stanford physicists in the late 1960s. He was then ignored by the Lawerence Berkeley Labs fundamental fysiks group that popularized Bell's inequality.

Svozil[2011] Svozil, K. Feyerabend and Physics. in *Paul Feyerabend: ein Philisoph aus Wien* (eds. Stadler, F. and Fischer, K.), Instituts Wiener Kreis, 49-60.

Kaiser[2011] Kaiser, D. *How the Hippies Saved Physics - Science, Counter Culture and the Quantum Revival.* Norton, 2011.

Here is Shor's paper that assumes P=NP in the weak TM model for his quantum computer algorithms.

Shor[1997] Shor, P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. arXiv:quant-ph/9508027v2.