Problem 1
Is constructing the Return-oriented Programming (ROP) chain an NP-hard problem?

Formally, constructing an ROP chain $R$ that achieves an exploitation goal $G$ in a program $P$ from an initial status $S$ can be described by the following specification: $\exists R \forall P, G : \{S\} R \{G\}$. This is a second-order formula. Clearly, it is an undecidable problem which is NP-hard.

Problem 2
Are there any good references for the weird machine concept?

- Thomas Dullien, "Weird machines, exploitability, and provable unexploitability"
- Dmitry Evtyushkin, Thomas Benjamin, Jesse Elwell, Jeffrey A. Eitel, Angelo Sapello, Abhrajit Ghosh, "Computing with Time: Microarchitectural Weird Machines"