

Vitalik talks about MPC again, in this great primer about Garbled Circuits <https://vitalik.ca/general/2020/03/21/garbled.html>.

For those who don't know, MPC has two main flavors:

1. Linear secret sharing scheme (this is what my thesis and the original Enigma whitepaper were focused on)
2. Garbled circuits

In the beginning of the previous decade, most advances in general-purpose MPC were around LSSS, but in recent years garbled circuits have regained their fame with papers such as [this](#).

A recommended read!