Cryptographic games with their transitions are a useful tool for proving cryptographic properties of various security protocols. We have explored together the notions of negligible functions, cryptographic games and their transitions, computational, and perfect security. This served as our basis when analyzing malware protocols, we translated each into a game that tested the property we were trying to expose. Then, using transitions based on negligible functions, we simplified said games to reach desired results.

We have decided to employ Cryptoverif as our tool for implementing these games, it is designed to create sequences of games that lead to games exposing specified properties. We translated the games into series of primitives that form an interface of this tool. Using the theory described above we anchored individual transitions in mathematical arguments and documented the proof strategy Cryptoverif employs.

To illustrate the usage, we have selected a few communication protocols used by several malware families (Emotet, Mirai, Lockcrypt) and used the tooling to prove a few characteristic properties. While this has been challenging for a few cases (especially when the techniques were not entirely inside Cryptoverif's scope) we have managed to design our games accordingly to reach the desired results. We have demonstrated Cryptoverif capabilities by revealing vulnerability in Mirai's key generation, verifying correctness of Emotet's encryption and illustrating of improper usage of one-time pad encryption by ransomware.