Kryptografické hry společně s jejich tranzicemi jsou užitečný nástroj pro zkoumání kryptografických vlastností různých bezpečnostních protokolů. Spojili jsme teorie za zanedbatelnými funkcemi, kryptografickými hrami a jejich tranzicemi, výpočetní a perfektní bezpečenost. Toto nám posloužilo jako teoretický základ pro analyzování protokolů, každý jsme převedeli na hru, která měla odhalit konkrétní vlastnost, která nás zajímala. Následně využívajíc tranzicí postavených na zanedbatelných funkcích jsem zjednodušili hry na jejich podobu odhalující kýžené vlastnosti.

Rozhodli jsme se využít Cryptoverif jako náš hlavní nástroj pro implementaci těchto her. Ten je navržen na navrhování posloupoností kryptografických her, které vedou na hry odhalující specifikované vlastnosti. Přeložili jsme naše hry do primitiv, které utváří interface tohoto nástroje. Za použití teorie popsané výše jsme ukotvili jednotlivé tranzice v přesných matematických argumentech and zdokumentovali důkazovou teorii Cryptoverif používá.

Pro ilustraci jsme si vybrali několik komunikačních protokolů, které jsou využívány různými malwarovými rodinami (jako Emotet, Mirai, LockCrypt) a použili Cryptoverif společně s teorií kryptografických her k dokázání jistých vlatností těchto protokolů. Ačkoli toto bylo náročné hlavně v případech, které neodpovídaly typickému využití Cryptoverifu, povedlo se nám dojít k uspokojivým řešením těchto problémů vhodným navržením kryptografických her. Předvedli jsme schopnosti Cryptoverif odhalením zranitelnosti v generování klíče u Miraie, ověřením bezpečnosti šifrování u Emotetu a nastíněním špatného využívání šifry jednorázové tabulky u ransomwaru.