Topics on verification and validation techniques for cybersecurity

1) WireGuard Protocol and its formal verification:

https://www.wireguard.com/formal-verification/
https://www.wireguard.com/papers/wireguard-formal-verification.pdf

Two WireGuard models in Tamarin:

https://git.zx2c4.com/wireguard-tamarin/

https://github.com/tamarin-prover/tamarin-prover/tree/develop/examples/wireguard

2) An extention of Tamarin to deal with observational equivalence:

http://www.infsec.ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/information-security-group-dam/research/publications/pub2015/ASPObsEq_full.pdf

3) An extension of Tamarin for the automatic generation of "source lemmas" (source lemmas are hints for the prover, and are usually written by hand)

https://hal.archives-ouvertes.fr/hal-02903620

4) A list of publication on Tamarin and related topics can be found at the Tamarin web site:

https://tamarin-prover.github.io/

It includes a number of cases studies with the corresponding models.

5) ProVerif web site, including a list of publications, software, and manual:

https://prosecco.gforge.inria.fr/personal/bblanche/proverif

Among the publications, the following ones are of particular interest (the third one is about observational equivalence):

https://prosecco.gforge.inria.fr/personal/bblanche/publications/BlanchetFOSAD14.pdf
https://prosecco.gforge.inria.fr/personal/bblanche/publications/BlanchetBook09.pdf
https://prosecco.gforge.inria.fr/personal/bblanche/publications/BlanchetSmythJCS18.pdf