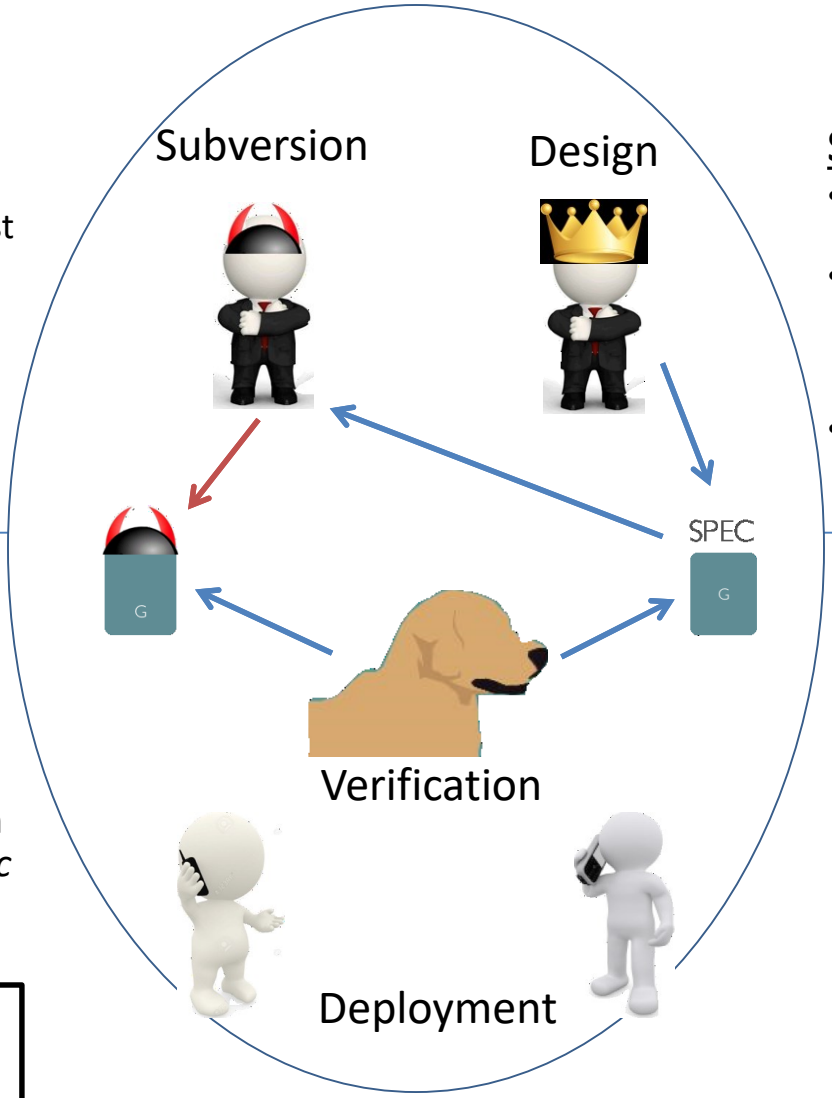
Theory and Practice of Cryptosystems Secure Against Subversion

Challenge:

- Preserve security against **subversion attacks** that target cryptographic algorithms;
- Specifically, rigorously protect against "backdoors."

Solution:

- Formal approach to modular design;
- Analysis rigorously combines *testing* with *classical cryptographic security definitions*.



Scientific Impact:

- Rigorous study of modularity & testing;
- Solutions defend against an array of attacks, from bugs to stealthy algorithm subversions;
- Feasibility/complexity tradeoff.

Broader Impact:

- Subversion & poor parameter selection are serious security problems;
- Techniques can be compatible with current infrastructure;
- Development of courses; graduate training.

JHU (M. Green) – SaTC:1801479
NJIT (Q. Tang) – SaTC:1801492
UConn (A. Russell) – SaTC:1801487
VCU (H.-S. Zhou) – SaTC:1801470