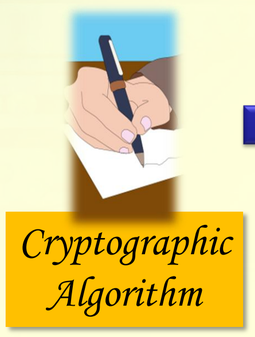
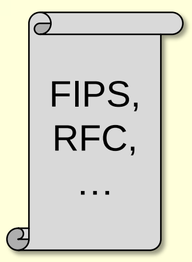
Secure Cryptographic Software

Reynald AFFELDT and David NOWAK Research Team for Software Security

State of the art

Research → Standardization → Software development → Validation (CAVP, …)





Problems

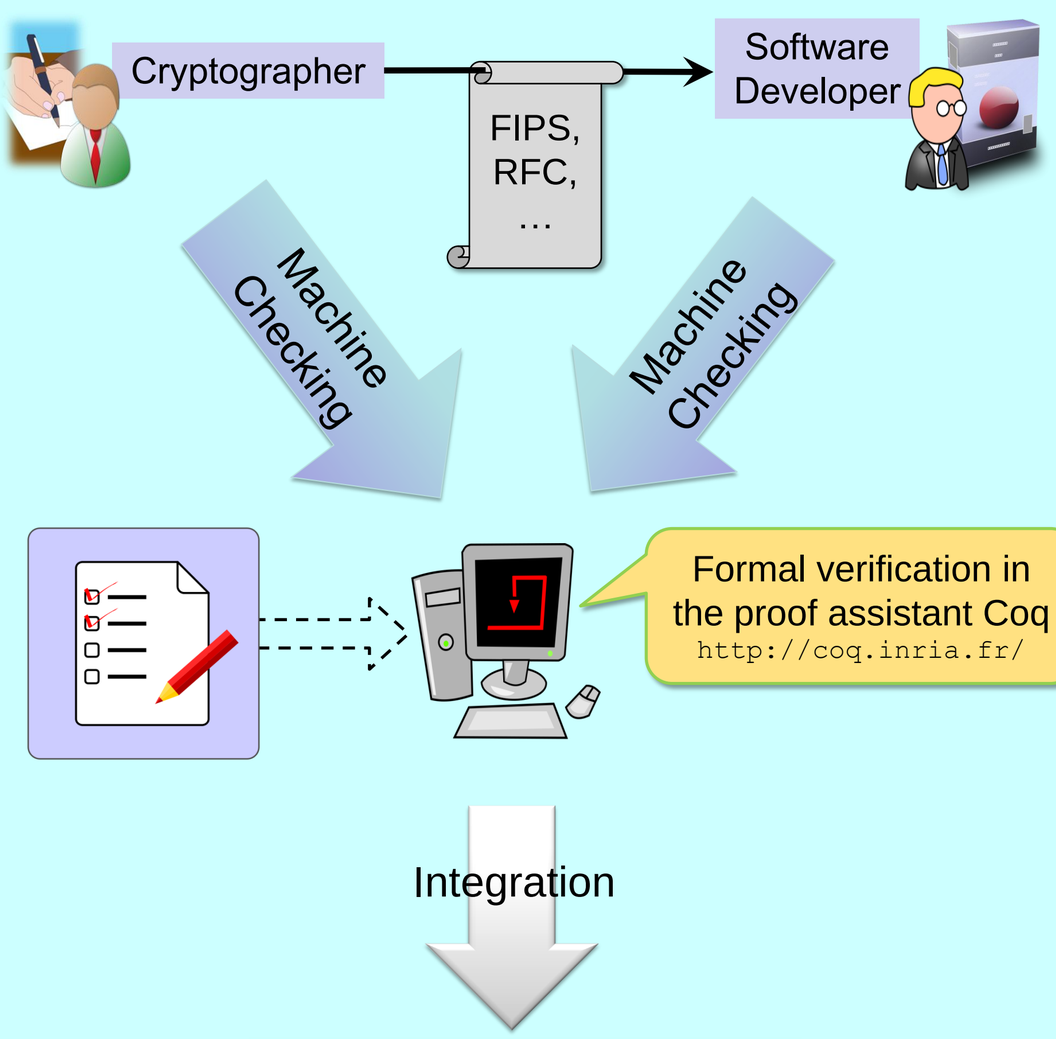
- Hidden assumptions
- Specification and security proof in natural language
- Optimizations by programmers can lead to security holes
  - Example: Security bug in GNU Privacy Guard [Phong Q. Nguyen, 2004]
- Partial and not fully formal validation

Goal: Certify cryptographic software against security bugs

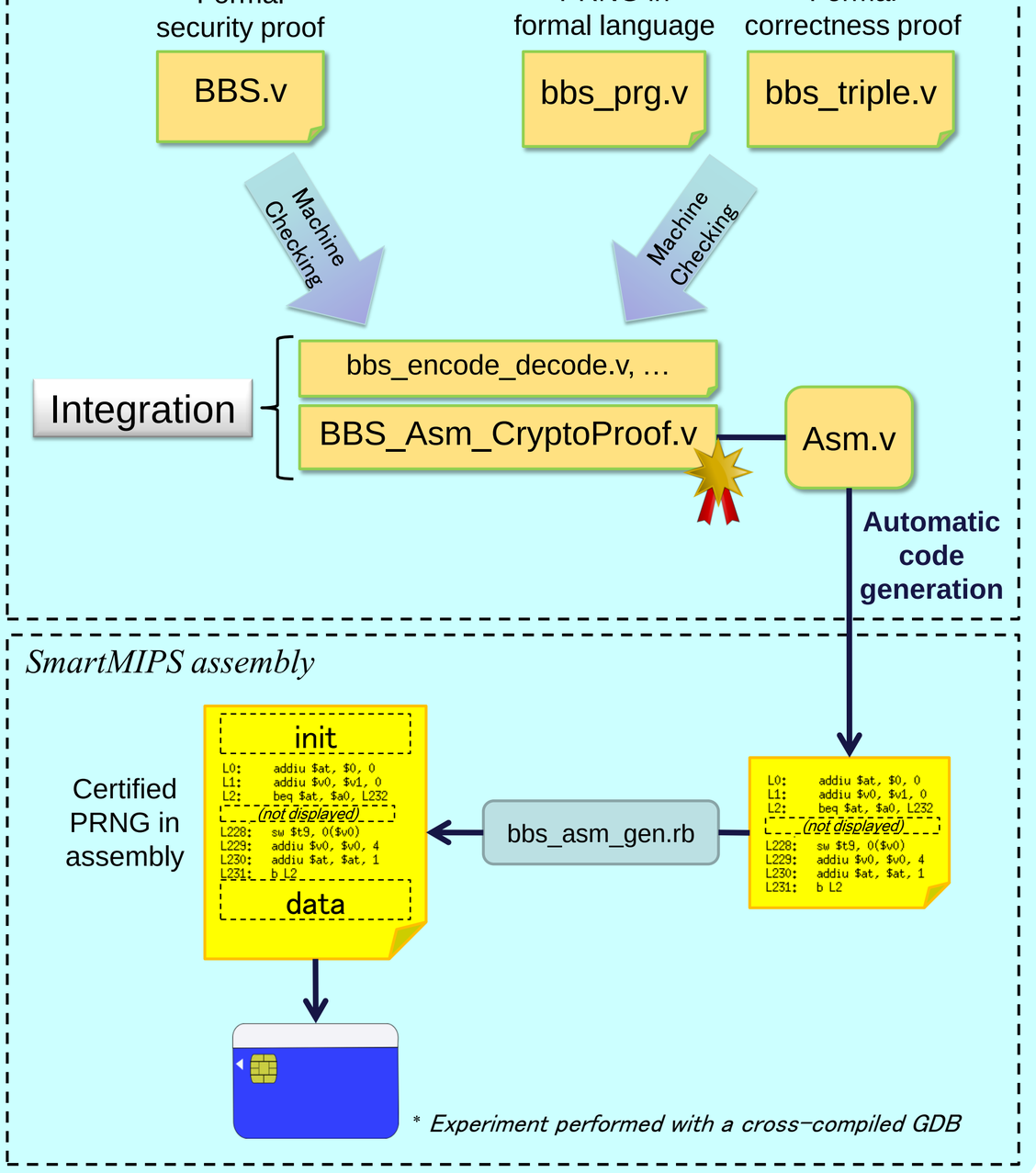
Our solution

Handmade security proof for the cryptographic algorithm

Software implementation written in a low-level programming language



Demo — The Blum-Blum-Shub PRNG



Reference
Reynald Affeldt, David Nowak, and Kiyoshi Yamada. Certifying assembly with formal cryptographic proofs: the case of BBS.
In *Automated Verification of Critical Systems 2009, volume 23 of Electronic Communications of the EASST.*
Formal development: `http://staff.aist.go.jp/reynald.affeldt/bbs`

Future Work
Reuse our certified implementation of BBS as the source of pseudorandomness in the implementations of other cryptographic algorithms.

Acknowledgment
Based on joint work with Kiyoshi Yamada

2010-5-11