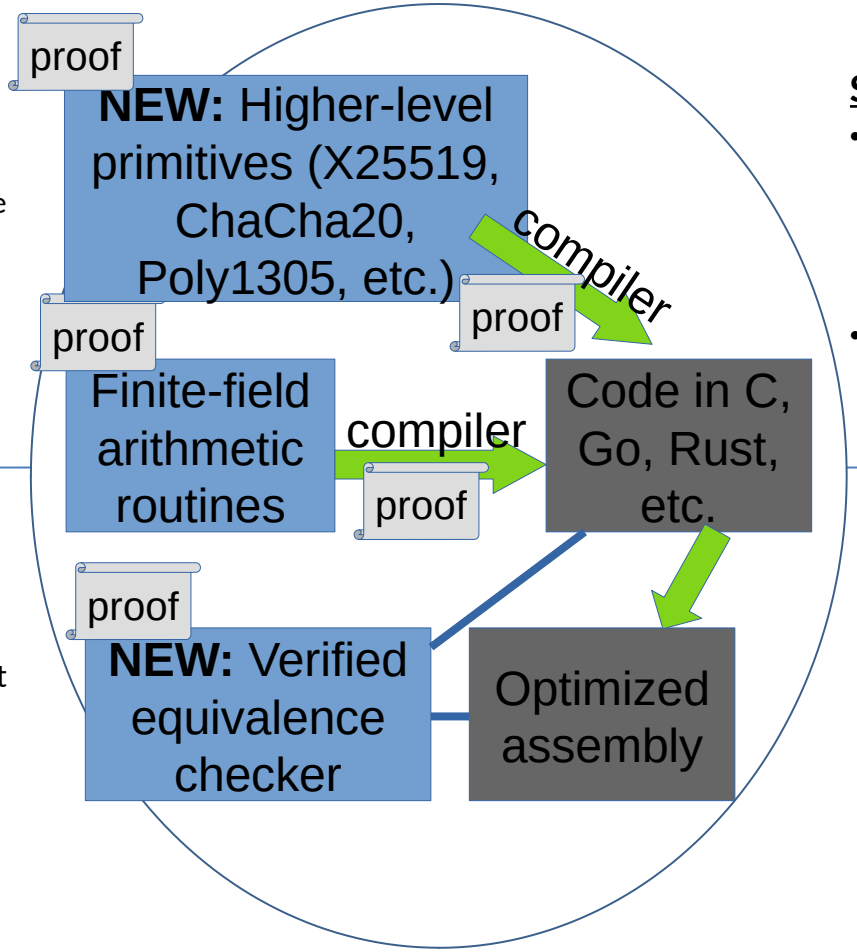
Scaling Correct-by-Construction Code Generation for Cryptography



Challenge:

- Improve the *Fiat Cryptography* high-assurance development tools for cryptographic primitives.
- Maintain the highest levels of rigor via the Coq proof assistant.

Solution:

- *Raise abstraction level:* generate code for elliptic-curve point operations, not just field operations.
- *Lower abstraction level:* validate optimizations of assembly code.

Scientific Impact:

- Demonstrate compiler & formal-methods techniques that raise the level of abstraction in programming without significant performance costs.
- Decrease need to trade off between security & development costs.

Broader Impact and Broader Participation:

- Improve an open-source tool already used in popular projects (e.g., Chrome, Firefox).
- Educate cryptography developers about possibilities to use & extend our tooling.

#2130671, MIT, PI Adam Chlipala <adamc@csail.mit.edu>