An algebraic approach to secure multilinear maps for cryptography

Challenge:

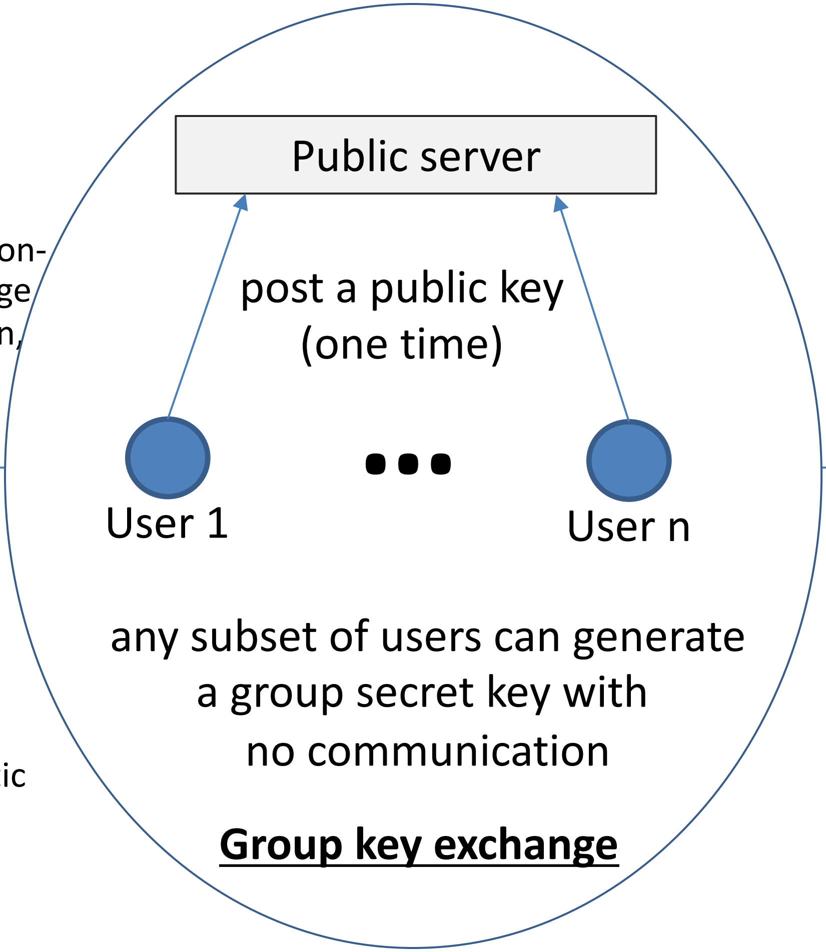
The goal of this project is to construct cryptographic multilinear maps for use in non-interactive group key exchange and homomorphic encryption, a real-world problem open for over thirty years.

Solution:

One approach is to use cup product pairings on the cohomology of algebraic varieties.

We quantify the difficulty of this approach using arithmetic geometry.

CNS-1703321, 1701567, 1701785.
University of California Irvine, Stanford University, Institute for Advanced Study, University of Pennsylvania.



Public server

post a public key
(one time)

User 1

•••

User n

any subset of users can generate
a group secret key with
no communication

Group key exchange

Scientific Impact:

Cup products are central to many basic conjectures in arithmetic geometry. One outcome of our project is to quantify the difficulty of computing them.

Broader Impact:

Group key exchange is currently being standardized in the IETF MLS working group. A cryptographic multilinear map will greatly simplify the design currently under consideration.