Secure Computation with Honest Majority in Expected Constant Rounds

Jonathan Katz

Chiu-Yuen Koo

University of Maryland

College Park, Maryland

Secure Computation with Honest Majority

(cryptographic setting)

- Feasiblity. . . [Goldreich-Micali-Wigderson ’87].
- Assuming a broadcast channel, the problem can be solved in *constant* rounds [Beaver-Micali-Rogaway ’90, Damgard-Ishai’05].
- In reality, the broadcast channel must typically be simulated over existing point-to-point channels using a *broadcast protocol*, thus increasing the round complexity.

Prior Work (Broadcast)

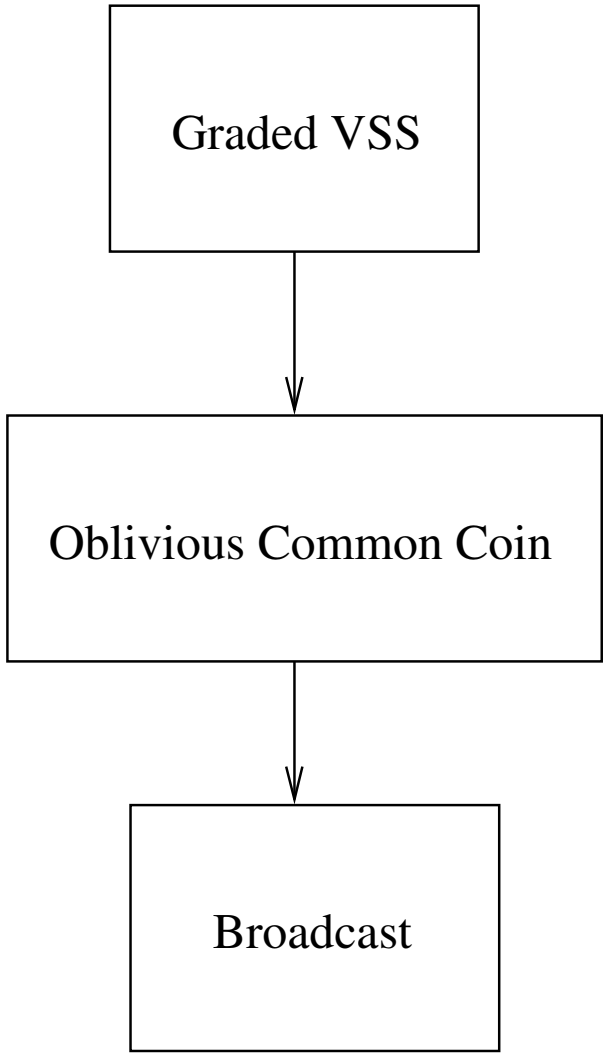
1. When $t < n/3$ of the parties are dishonest, there exists a broadcast protocol running in (expected) constant rounds [Feldman-Micali '85].
2. When $t \geq n/3$, the problem cannot be solved at all without prior setup (e.g., a PKI).
3. When $t < n$, there is a broadcast protocol using signatures which requires $O(t)$ rounds. [Dolev-Strong '83].
4. When $t < n/2$ there is a protocol relying on a specific number-theoretic assumption which requires (expected) constant rounds [Fitzi-Garay '03].

Extending/adapting the approach of [Feldman-Micali '85] to the setting of $t < n/2$ (based on signatures rather than specific assumptions) has been open since their work.

Overview of Our Results

1. We show an authenticated Byzantine agreement protocol for $t < n/2$ running in expected *constant* rounds.
   - Our construction uses a slightly different approach than [Feldman-Micali '85].
   - Our approach also yields a simpler construction of Byzantine agreement (with simpler proof) for the case of $t < n/3$ (with no PKI).
2. We show how to use our protocol for round-efficient secure computation.
3. Applying our results to the (constant-round) protocol of [Beaver-Micali-Rogaway '90, Damgard-Ishai '05] yields a protocol for secure computation running in expected constant rounds.

A Brief Review of [Feldman-Micali '85]



Problem: Seems difficult to construct a *constant-round* graded VSS protocol for $n/3 \leq t < n/2$ (even with a PKI).

Our Approach