The implementation of smart metering into the electric grid provides high resolution real-time data to the energy providers. This real-time data allows energy companies to engage in real-time pricing markets based on the current energy supply and demand. However, real-time data gives energy providers the ability to extract detailed information about consumer’s daily lives, which can be seen as an invasion of privacy and can adversely effect demand.

Each consumer sets their demand through stating whether or not they will use an appliance given a certain price. The utility sets their price given the environmental variables, previous demand, and the ability to meet that demand. A supply and demand curve is created and the market clearing price is calculated at the intersection of the supply and demand, all while remaining private.

To keep data private, we use:

- Paillier cryptosystem to manage the load and aggregate the demand data privately.
- Yao’s Solution to the millionaire problem to check an individual consumer's demand and consumption.

SMC requires more than two parties be able to privately compute on some numbers. Paillier allows for homomorphic encryption such that the sum of the encryptions is the encryption of the sums. This allows the energy company to compute the average consumption, as well as compute the demand at each price over each consumer.

To maintain a zero-knowledge environment, the energy company may not know any information about any consumer. Using Yao’s solution to the millionaire problem, the energy company can compute the bill, check the usage against a threshold, and compare prices from different utilities, all without knowing the actual values. Yao’s solution uses iterative RSA encryption to hide the actual values.

SMC allows utilities to monitor the consumptions of consumers while maintaining the consumer’s privacy. By adding a supply and demand market to the simulation we were able to have real-time pricing without any party knowing the actual consumptions.