

Secure Supply Chain Protocols (IIS-0325345)

Mikhail Atallah, Vinayak Deshpande, Leroy Schwarz

Purdue University

www.cs.purdue.edu/homes/mja/

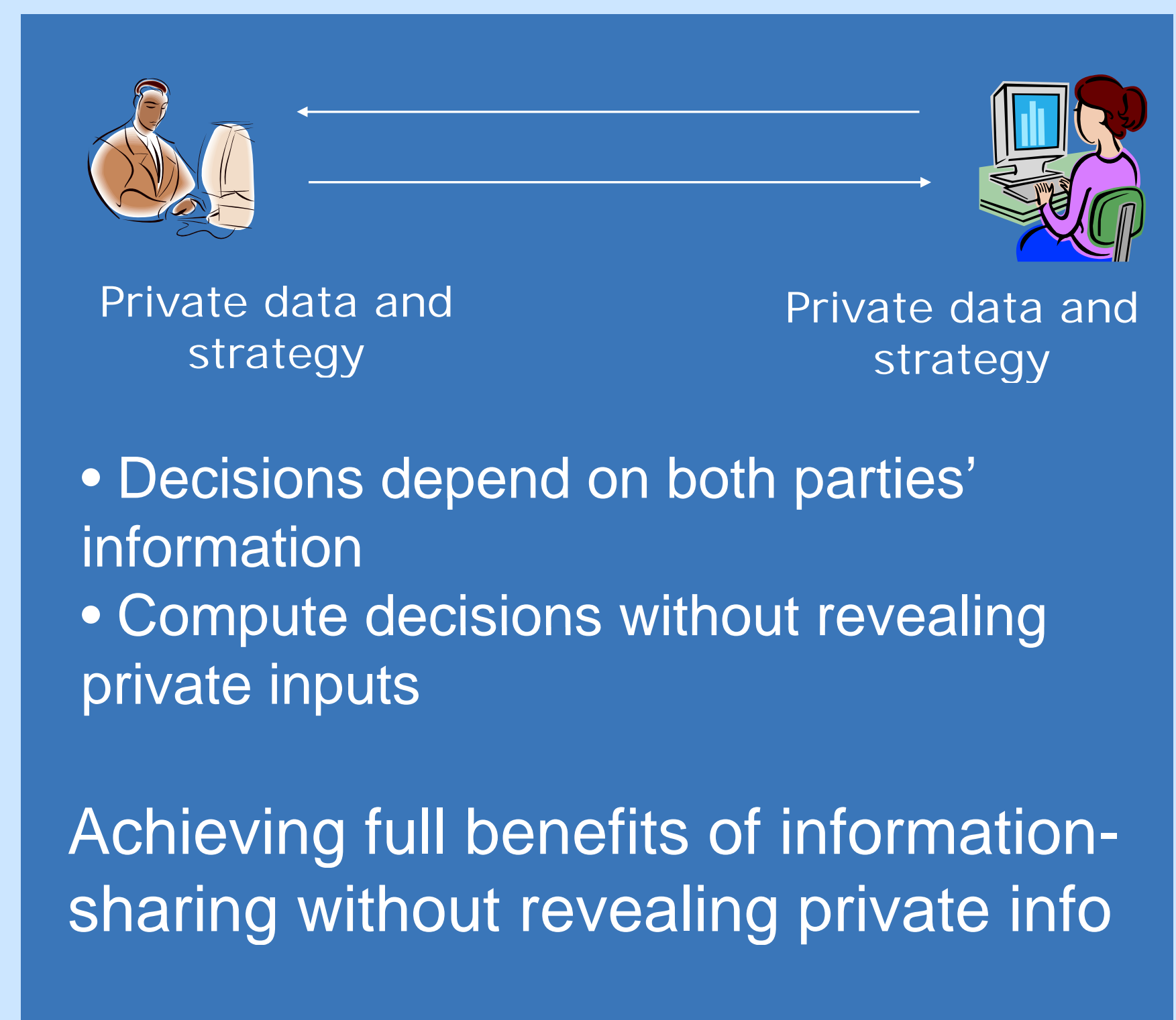


Objectives:

Huge potential benefits of supply-chain collaborations go unrealized due to a reluctance to share information. The reluctance to share is understandable: The information could be proprietary, embarrassing, illegal to share, ...etc; and the counterpart could be a competitor, or an otherwise trustworthy partner but whose computer system does not meet high enough security standards.

The goal of this project is to develop methods that make possible supply-chain collaborations of the same quality as if information-sharing had taken place, yet without revealing the participants' private information.

The project will make possible more efficient supply supply chains, with better use of capacity, better allocation of resources, better customer service, and less unnecessary costs.



Approach and Impact

New Approach

- Truthfulness of participants
- Incentive-compatibility
- Off-line certification of inputs

Research Impact

- Protocols that incentivize participants' honesty
- Protocols for certified inputs
- Off-line certification

- Organizations predict future demand based on their demand signals; most are confidential, e.g.,
 - Depend on planned (but not yet announced) future price cuts, changes in production capacity, product quality, new product warranties, a new marketing campaign, etc.
 - Depend on current pricing, product failure rates, customer satisfaction, etc.
- They could all make better demand forecasts if they collaborated (based on broader inputs)
 - More informed decisions (avoid costly mistakes and the boom-bust cycles)
- Our protocols make possible better forecasts without compromising confidentiality of signals

Collaborative forecasting and benchmarking

- Original equipment manufacturer (OEM) wants Electronic Manufacturing Service (EMS) to assemble a product made of components
- A component can be supplied by OEM or EMS
 - Each has negotiated a different price from component manufacturers, and does not want to reveal it (else it erodes their price advantage)
- Protocol to determine which components should be supplied by OEM, and which by EMS
 - No individual component price is revealed (only aggregates are revealed)
 - Incentive-compatible (a party cannot gain by misstating their component price)

Secure price-masking