A Web-based Meeting Scheduling Solver with Privacy Guarantees, without Trusted Servers

Marius-Călin Silaghi and Vaibhav Rajeshirke, Richard Wallace

Florida Institute of Technology University College Cork

Some problems having privacy requirements can be modeled with distributed (weighted) constraint satisfaction frameworks [3]. Previous approaches to such problems used trusted servers or some kind of argumentation, inherently leaking data about the secret constraints [5]. We developed techniques$^{\text{patent pending}}$ and a system for solving these problems where an agent does not divulge absolutely any secret information to any attacker controlling less than half of the participants. Agents and servers only learn a randomly picked solution.

We identify the following privacy attacks on distributed CSP techniques:
1. S-attacks against secure multiparty computation-backtracking hybrids. [1]
2. Shadow CSPs against argumentation based solvers. [5]
3. Attacks against search with known orders on variables and domains. [2]
4. Statistical attacks against DisCSP solvers that shuffle domains. [4]

To achieve resistance to these attacks we invented two fundamental cryptographic techniques: a) S-mixnets for shuffling shared secrets; b) Two alternative functions for solving WCSPs using solely '+/*' operations (with no comparison).

We also developed three secure multiparty protocols that combine S-mixnets with the aforementioned functions, obtaining MPC-DisWCSP1 and MPC-DisWCSP2 (resistant to attacks 1-3), and MPC-DisWCSP3 (resistant to attacks 1-4). MPC-DisWCSP1 can be parametrized between polynomial space and linear logic time, but is slower. Only MPC-DisWCSP3 can exploit public constraints.

Results: An applet-based secure meeting scheduling system is deployed at www.cs.fit.edu/~msilaghi/secure. The methods also apply for incentive auctions and stable matchings problems [3]. Our solution to the 4^{th} attack can be used to improve the privacy offered by other computation techniques based on DisCSPs (e.g with trusted servers, choosing a solution randomly among all solutions).

References

1. M. Silaghi. *Asynchronously Solving Problems with Privacy Requirements.* PhD thesis, EPFL, 2002. www.cs.fit.edu/~msilaghi/teza.
2. M. Silaghi. Solving a DisCSP with cryptographic multi-party computations, without revealing constraints and without involving trusted servers. In *IJCAI DCR Workshop*, 2003.
3. M. Silaghi. Incentive auctions and stable marriages problems solved with $\lfloor n/2 \rfloor$-privacy of human preferences. Technical Report CS-2004-11, FIT, 2004.
4. M. Silaghi and V. Rajeshirke. The effect of reordering policies on privacy. In *AAMAS (to appear)*, 2004.
5. R. Wallace. Reasoning with possibilities in multiagent graph coloring. In *IJCAI DCR Workshop*, 2003.