# Cryptology ePrint Archive: Report 2013/220

**Towards Efficient Private Distributed Computation on Unbounded Input Streams**

*Shlomi Dolev and Juan Garay and Niv Gilboa and Vladimir Kolesnikov and Yelena Yuditsky*

**Abstract:** In the problem of private ``swarm" computing, $n$ agents wish to securely and distributively perform a computation on common inputs, in such a way that even if the entire memory contents of some of them are exposed, no information is revealed about the state of the computation. Recently, Dolev, Garay, Gilboa and Kolesnikov [ICS 2011] considered this problem in the setting of information-theoretic security, showing how to perform such computations on input streams of {\em unbounded length}. The cost of their solution, however, is exponential in the size of the Finite State Automaton (FSA) computing the function.

In this work we are interested in efficient (i.e., polynomial time) computation in the above model, at the expense of {\em minimal} additional assumptions. Relying on the existence of one-way functions, we show how to process unbounded inputs (but of course, polynomial in the security parameter) at a cost {\em linear} in $m$, the number of FSA states. In particular, our algorithms achieve the following:

\begin{tiret}

\item In the case of $(n,n)$-reconstruction (i.e., in which all $n$ agents participate in the reconstruction of the distributed computation) and at most $n-1$ agents are corrupted, the agent storage, the time required to process each input symbol, and the time complexity for reconstruction are all $O(mn)$.

\item In the case of $(n-t,n)$-reconstruction (where only $n-t$ agents take part in the reconstruction) and at most $t$ agents are corrupted, the agents' storage and time required to process each input symbol are $O(m{n-1 \choose n-t})$. The complexity of reconstruction is $O(mt)$.

\end{tiret}

We achieve the above through a carefully orchestrated use of pseudo-random generators and secret-sharing, and in particular a novel share re-randomization technique which might be of independent interest.

**Category / Keywords:** cryptographic protocols / Secure-Multi-Party-Computation, Streamin Input

**Publication Info:** A brief announcement of the paper was published at DISC 2012, and a version of the paper was accepted to ACNS 2013

**Date:** received 14 Apr 2013

**Contact author:** yuditskyl at gmail com