The farmers felt that their bids reflected their capabilities and costs, which they did not want to reveal to Danisco, the only company in Denmark that processed sugar beets. At the same time, Danisco needed to be involved in the auction as the contracts were securities directly affecting the company.

The auction was implemented as a three-party MPC among representatives for Danisco, the farmer's association (DKS) and the researchers (SIMAP project). As explained by Bogetoft *et al.* (2009), a three party solution was selected, partly because it was natural in the given scenario, but also because it allowed using efficient information theoretic tools such as secret sharing. The project led to the formation of a company, Partisia, that uses MPC to support auctions for industries such as spectrum and energy markets, as well as related applications such as data exchange (Gallagher *et al.*, 2017).

Estonian students study. In Estonia, a country with arguably the most advanced e-government and technology awareness, alarms were raised about graduation rates of IT students. Surprisingly, in 2012, nearly 43% of IT students enrolled in the previous five years had failed to graduate. One potential explanation considered was that the IT industry was hiring too aggressively, luring students away from completing their studies. The Estonian Association of Information and Communication Technology wanted to investigate by mining education and tax records to see if there was a correlation. However, privacy legislation prevented data sharing across the Ministry of Education and the Tax Board. In fact, k-anonymity-based sharing was allowed, but it would have resulted in low-quality analysis, since many students would not have had sufficiently large groups of peers with similar qualities.

MPC provided a solution, facilitated by the Estonian company Cybernetica using their Sharemind framework (Bogdanov *et al.*, 2008a). The data analysis was done as a three-party computation, with servers representing the Estonian Information System's Authority, the Ministry of Finance, and Cybernetica. The study, reported in Cybernetica (2015) and Bogdanov (2015), found that there was no correlation between working during studies and failure to graduate on time, but that more education was correlated with higher income.

Boston wage equity study. An initiative of the City of Boston and the Boston Women's Workforce Council (BWWC) aims to identify salary inequities across various employee gender and ethnic demographics at different levels of employment, from executive to entry-level positions. This initiative is widely supported by the Boston area organizations, but privacy concerns prevented direct sharing of salary data. In response, Boston University researchers designed and implemented a web-based MPC aggregation tool, which allowed employers to submit the salary data privately and with full technical and legal protection, for the purposes of the study.

As reported by Bestavros *et al.* (2017), MPC enabled the BWWC to conduct their analysis and produce a report presenting their findings. The effort included a series of meetings with stakeholders to convey the risks and benefits of participating in the MPC, and considered the importance of addressing usability and trust concerns. One indirect result of this work is inclusion of secure multi-party computation as a requirement in a bill for student data analysis recently introduced in the United States Senate (Wyden, 2017).

Key management. One of the biggest problems faced by organizations today is safeguarding sensitive data as it is being used. This is best illustrated using the example of authentication keys. This use case lies at the core of the product offering of Unbound Tech (Unbound Tech, 2018). Unlike other uses of MPC where the goal is to protect data owned by multiple parties from exposure, here the goal is to protect from compromise the data owned by a single entity.

To enable a secure login facility, an organization must maintain private keys. Let's consider the example of shared-key authentication, where each user has shared a randomly chosen secret key with the organization. Each time the user U authenticates, the organization's server S looks up the database of keys and retrieves U's public key sk_U, which is then used to authenticate and admit U to the network by running key exchange.

The security community has long accepted that it is nearly impossible to operate a fully secure complex system, and an adversary will be able to penetrate and stealthily take control over some of the network nodes. Such an advanced adversary, sometimes called Advanced Persistent Threat (APT), aims to quietly undermine the organization. Naturally, the most prized target for APT and other types of attackers is the key server.

MPC can play a significant role in *hardening* the key server by splitting its functionality into two (or more) hosts, say, S_1 and S_2, and secret-sharing