# Position Paper: Privacy-Preserving Techniques in the Context of Transportation CPS

Susanne Wetzel

Stevens Institute of Technology
Department of Computer Science
Castle Point on Hudson
Hoboken NJ 07030, USA
swetzel@stevens.edu

For the future of transportation CPS it will be of paramount importance to introduce proper and suitable mechanisms w.r.t. security and privacy. While there is a number of efforts ongoing—especially in the automotive arena, there certainly is a lot of room for improvement—in particular when it comes to privacy. Relatedly, there also is the issue of usability—and in particular the individual gaining and understanding what his/her needs are w.r.t. security and privacy. Specifically, today in most cases it is not transparent to the user what data is transmitted to whom, when, and where—especially when it comes to automotive technologies. Yet, the services are manifold - ranging from built-in services to ones that a customer may elect to subscribe to (e.g., EZ-Pass, or Progressive Snapshot).

In the security community, homomorphic cryptography is seeing great interest. And over the past few years there has been a lot of developments that suggest great promise in the context of various fields of application. Homomorphic cryptography allows for computations on encrypted data and is as an enabler for many modern privacy-preserving techniques—especially in the context of secure multi-party computation.

It seems prudent to investigate the potential of homomorphic cryptography in the context of transportation CPS for the benefit of introducing improved security and privacy to future approaches. Today, fully homomorphic cryptography still suffers from the fact that known methods are too computationally expensive to be deployed in practical applications such as transportation CPS. Nevertheless, given recent developments, further breakthroughs are to be expected. Also, it seems reasonable to rely on either multiplicative or additively homomorphic schemes as a first step and explore what functionality in transportation CPS might benefit from that.

Questions that should be addressed include:

- How can homomorphic cryptography improve security and privacy in transportation CPS.
- How suitable are additive/multiplicative homomorphic cryptosystems to introduce security and privacy to the functionality of transportation CPS. I.e., what functionality can be protected, where are shortcomings and/or compromises necessary?

– How can the user benefit from the introduction of homomorphic cryptography to transportation CPS.
– What are the performance implications of introducing homomorphic cryptography to transportation CPS.