1163-00-985 **Delaram Kahrobaei*** (dk2572@nyu.edu). *Quantum-safe E-Voting Schemes.*

A carefully set-up homomorphic encryption scheme can be self-tallying, in that given a specific set of encrypted values, certain summation operation results can be carried out without requiring the decryption key. Such self-tallying homomorphic encryption schemes are quite desirable since they enable certain applications with minimal trust assumptions, e.g.e-voting systems without trusted tallying authorities and privacy-preserving smart metering systems that do not require trusted third parties. However, the security of current self-tallying homomorphic encryption schemes is based on mathematical problems such as the discrete logarithm problem which can be feasibly solved if quantum computers are built; hence, many current schemes are not 'quantum-safe', whereas applications require so-called ever-lasting privacy. Recent proposals for quantum-safe schemes include public-key encryption schemes that use semidirect product of (semi)groups. In this talk, we show how one such scheme can be adapted to provide a self-tallying homomorphic encryption scheme and how our proposed scheme can be used to realise a verifiable e-voting system without tallying authorities and a privacy-preserving smart metering system. This a joint work with Simons (Oxford) and Shahandashti (York). (Received September 14, 2020)