1117-68-257 **Scott C. Batson*** (scott.batson@navy.mil), **Bryan Williams** (bryan.l.williams1@navy.mil), **Evan Austin** (evan.austin@navy.mil) and **Adam Wazzan** (adam.wazzan@navy.mil). *On Automated Verification of Security Proofs in Elliptic Curve Cryptography.* Preliminary report.

Modern cryptography is rapidly evolving to include elaborate functionalities, and cryptographic proofs of security have become significantly more complicated as a result. The use of automated tools to assist in constructing these proofs would potentially increase the confidence in them, and address the difficulty in verifying implementations. In 2014, Barthe et. al. introduced EasyCrypt, a tool that supports game-based verification of security for cryptographic constructions in generic group models. The aim of our work is to extend the EasyCrypt results to elliptic curve cryptographic schemes. We first present the intuition behind the automated verification of elliptic curve ElGamal in EasyCrypt, and discuss how one may adapt these ideas to additional elliptic curve schemes. (Received January 15, 2016)