Multivariate Polynomial-Based Cryptography

Sedat Akleylek

Department of Computer Engineering and
Cyber Security and Information Technologies Research and Development Center,
Ondokuz Mayıs University,
Samsun, TURKEY
akleylek@gmail.com

This research is partially supported by TÜBITAK under grant no.EEEAG-116E279

Outline

1. Fast Overview
2. Multivariate Cryptography
3. UOV
4. Rainbow
5. GUI
6. GeMSS