Parkinson, Simon, Longstaff, Andrew P., Fletcher, Simon, Crampton, Andrew, Allen, Gary and Myers, Alan

Cryptographic Techniques in Metrology Software

Cryptographic Techniques in Metrology Software

S. Parkinson, PhD Student.
Supervisors: A. P. Longstaff, S. Fletcher, G. Allen, A. Crampton, A. Myers
Engineering **C**ontrol and **M**achine **P**erformance **G**roup,
School of Computing and Engineering
University of Huddersfield

1. Challenges

Security

- Metrologists capture large quantities of sensitive data.
- The data will often be transferred through the public domain. Currently little effort is taken as standard to ensure its privacy and authenticity.

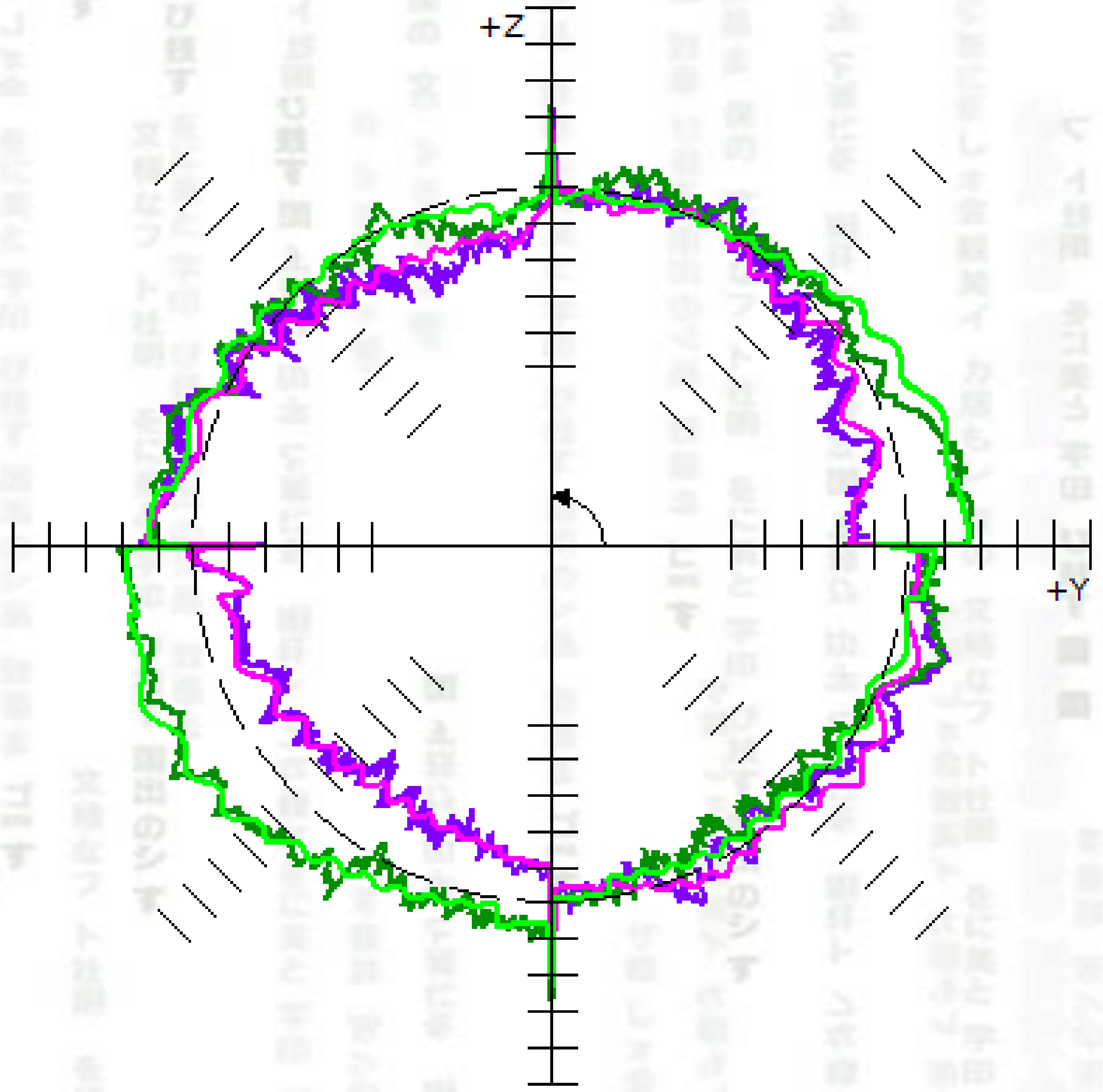
Validility

- Good metrology analysis requires the use of verifiable and traceable data.
- Once processed, the data will be stored, but it is likely that it will be required for future use, so it should be stored in such a way to maintain its integrity.

2. Aim

- This investigation aims to explore problems that a software engineer or a metrology specialist can eradicate through the novel implementation of cryptographic techniques within their software to improve:
  - Data Security
  - Data Integrity
  - Identification
  - Authentication
  - Data Traceability

Is enough being done to protect commerically sensitive data?



3. Methodology

- This study adopts a hybrid approach between a theoretical investigation of cryptographic techniques and empirical observations to their advantages if implemented within metrology software.
- The cryptographic functions that hold the greatest theoretical advantage will then be verified by implementing the techniques within metrology software, which in this case is used for machine tool calibration.

4. Research Impacts

- Commercially sensitive data would be protected so that only the authorised persons can view it.
- The validity and authenticity of the data can be verified helping to eradicate the large financial implications of assessing the metrological data incorrectly.
- A high degree of confidence can be established within the data's integrity allowing for easy detection of data modification.