



University of HUDDERSFIELD

University of Huddersfield Repository

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

Cryptographic Techniques in Metrology Software

Original Citation

Parkinson, Simon, Longstaff, Andrew P., Fletcher, Simon, Crampton, Andrew, Allen, Gary and Myers, Alan (2011) Cryptographic Techniques in Metrology Software. In: University of Huddersfield Annual Research Festival School of Computing and Engineering 12th March 2010, Friday 12th March 2010, University of Huddersfield. (Submitted)

This version is available at <http://eprints.hud.ac.uk/10418/>

The University Repository is a digital collection of the research output of the University, available on Open Access. Copyright and Moral Rights for the items on this site are retained by the individual author and/or other copyright owners. Users may access full items free of charge; copies of full text items generally can be reproduced, displayed or performed and given to third parties in any format or medium for personal research or study, educational or not-for-profit purposes without prior permission or charge, provided:

- The authors, title and full bibliographic details is credited in any copy;
- A hyperlink and/or URL is included for the original metadata page; and
- The content is not changed in any way.

For more information, including our policy and submission procedure, please contact the Repository Team at: E.mailbox@hud.ac.uk.

<http://eprints.hud.ac.uk/>

S. Parkinson, PhD Student.

Supervisors: A. P. Longstaff, S. Fletcher, G. Allen, A. Crampton, A. Myers
Engineering Control and Machine Performance Group,
School of Computing and Engineering
University of Huddersfield

1. Challenges

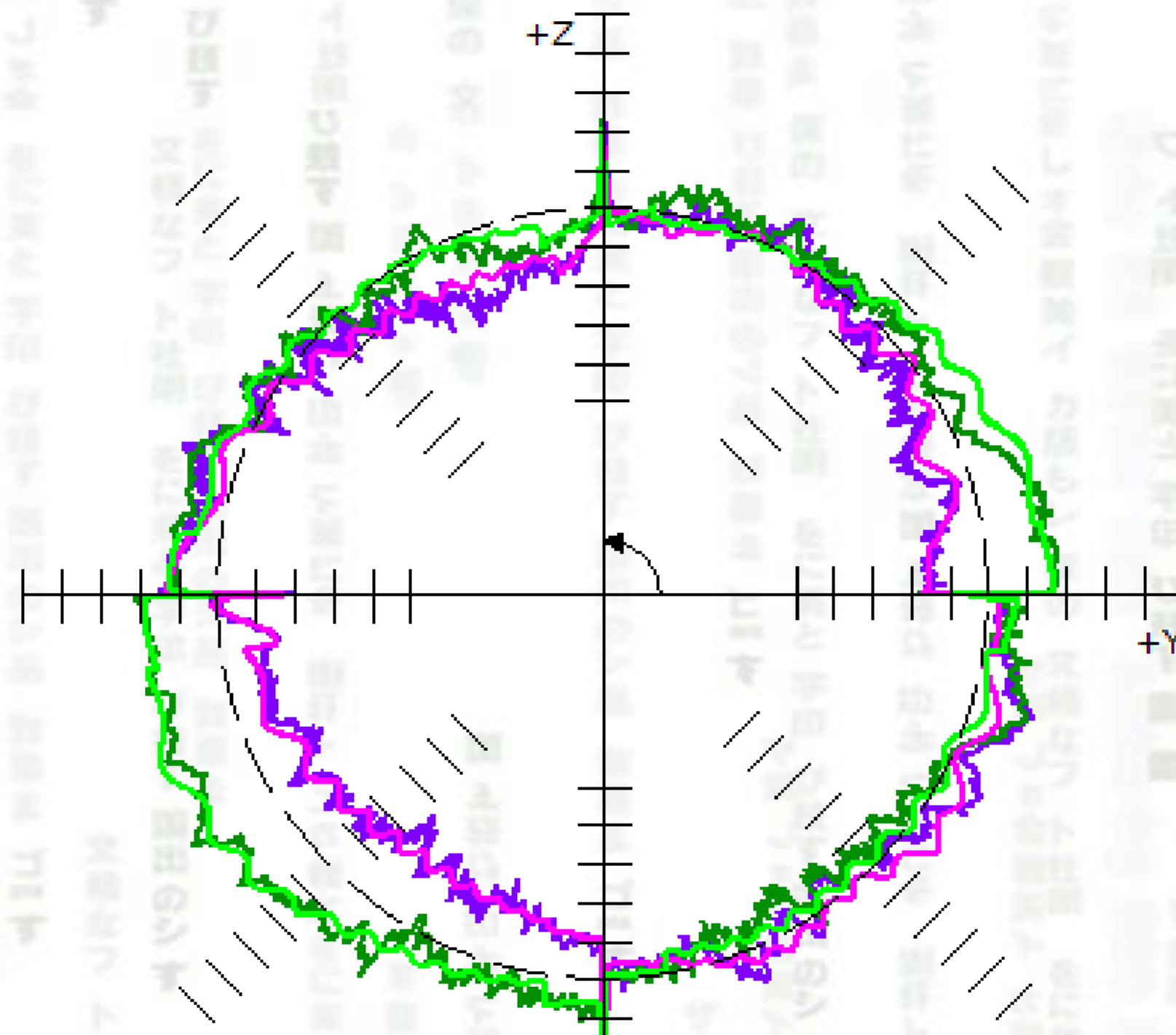
Security

- 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.

Validity

- 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.

Is enough being done to protect commercially 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.

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

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.