

Summer School Project Summary

Graphene Tamper Resistant Seal

Mentor: Alessandro Cattaneo

1. **Abstract** – Fostering nuclear safety and security is a multi-faceted problem that is of growing importance on the global stage. One of the top priorities is to maintain continuity of knowledge (CoK) with regard to nuclear material in containers and nuclear equipment, and to ensure the authenticity of any instrument data used to draw conclusions about these materials. A commonly adopted approach consists of using tamper-evident seals installed and surveyed by an appointed inspector. The goal of this project is to study a new type of remotely-readable tamper-evident seal that exploits the tunable electrical properties of (reduced) graphene-oxide paper. The project will also explore the use of compressed sensing techniques for the encryption of data stream between seal and remote reader in a low-power manner.

2. Project Outline –

- a. **Goal** – The goal of this project is to develop a prototype for a new generation of remotely-readable (reduced) graphene-oxide based anti-tamper seals. Students involved in this project will gain valuable experience implementing signal processing techniques on low-power embedded devices, with application to security-related unattended monitoring systems. Special attention will be given to solving the engineering challenges that arise in the development a fully working prototype.
- b. **Motivation** – Tamper-evident seals are devices that have unique identifiers with non-erasable tamper-indicating features designed to indicate intrusion. They are typically applied at the interface of a container where normal access occurs. A tamper-evident seal must have mechanical features that are sensitive to physical or chemical stresses beyond those that occur during examination. Furthermore, a tamper-evident seal must exhibit unique features that guarantee it cannot be easily duplicated. This project aims to improve over traditional tamper-evident seals on the basis of two key elements of novelty directed towards the development of a remotely-readable smart tag. First, the possibility of using reduced graphene-oxide (rGO) to build a seal is unique in that the electrical properties of GO are sensitive to many of the common techniques used to defeat conventional tamper-evident seals. Second, by incorporating a compressed sensing acquisition scheme to encrypt messages shared between the remote reader and the seal in a low-power manner.

Procedure – The students will familiarized themselves with compressed sensing and microcontroller programming basics. The project will actively involve students in laboratory activities necessary to build the smart-tag prototype. Students will be trained to use a CO₂ laser that will be used to reduce GO paper in order to transform it into conductive patterns. The messages shared between the remote reader and the seal will be processed by sending them through the rGO circuitry and encrypted according to the compressed sensing acquisition protocol. A microcontroller unit will be programmed to perform the signal processing operations. Special attention will be paid to adopt an object-oriented programming style in order to develop a modular, extensible and reusable code.

3. Background Literature

- IAEA, “The Safeguards System of the International Atomic Energy Agency,” <https://www.iaea.org/topics/safeguards-and-verification>
- J.E. Doyle, Ed., *Nuclear Safeguards, Security, and nonproliferation: Achieving Security with Technology and Policy*, Butterworth-Heinemann (2008) – especially chapter 6 on IAEA unattended monitoring systems.
- Candès, E. J., and Wakin, M. B., "An Introduction to Compressive Sampling," *IEEE Signal Processing Magazine*, 25(2), 21-30 (2008).
- Y. Rachlin, D. Baron, “The Secrecy of Compressed Sensing Measurements”, Forty-Sixth Annual Allerton Conference Allerton House, UIUC, Illinois, USA September 23-26, 2008.
- J. Rumbaugh, M. Blaha, W. Premerlani, F. Eddy, W. Lorensen, *Object-oriented Modeling and Design*, Prentice-Hall, Inc. (1991) – especially chapter 16 on non-object-oriented languages.
- E. Marinari, L.M. Barone, G. Organtini, *Scientific Programming*, World Scientific Publishing Company (2013) – especially chapters 5, 6, 7 on arrays, pointers and functions and paragraph 9.3 on structures.
- Atmel AVR XMEGA128A1 microcontroller datasheet, http://www.atmel.com/Images/Atmel-8067-8-and-16-bit-AVR-Microcontrollers-ATxmega64A1-ATxmega128A1_Datasheet.pdf

4. Week by Week Plan

(Plan subject to change based on results during work)

Week	Task
1	Review background literature, familiarize with CO ₂ laser unit
2	Familiarize with compressed sensing data analysis
3	Familiarize with microcontroller programming
4	Plan software and data flow
5	Write software

6	Test and debug software
7	Seal prototyping
8	Tamper-evident seal demonstration
9	Prepare report and presentation

5. Real World Design Issues as a Project Consideration

- Product engineering – what technical solutions can be adopted to practically realize a working prototype of the tamper-evident seal?
- Design of the system – how the software can be designed in order to be easily reconfigured to accommodate different implementations of the anti-tamper seal?
- Eavesdropper – how difficult is for an eavesdropper to intercept and decrypt the messages sent between the remote reader and the seal?
- Cracking attempts – what strategies can be implemented to detect the attempts to crack the encryption key by an adversarial facility operator?
- Sensitivity to tampering attempts / environmental and load changes – what is the minimum alteration that can be inflicted to the seal without causing any tamper evidence?
- Power consumption – what strategies can be adopted to preserve power consumption of the smart tag and keep guaranteeing the secrecy of the encrypted messages?

6. Equipment Requirements

- CO₂ laser unit
- Graphene-oxide (GO) papers
- Microcontroller and programmer
- Soldering station, cables, passive electronic components
- Oscilloscope, function generator, power supply
- Laptop

7. Software Requirements

- Atmel Studio Atmel Studio 6 © 2011
- Eclipse IDE for C/C++ Developers
- Terminal by Br@y++
- Notepad++, <http://notepad-plus-plus.org/>
- MATLAB