

## Construction of a preliminary file backup system for surface analysis data using secret sharing technique

*Nobuharu Okamitsu, Tomonori Tabe, Ryota Matsuda, Noriyuki Yamada, Toyoharu Takemoto, Takeshi Tanaka*

---

*We have established a preliminary file backup system to study the outline of secret sharing technology and test operations. Secret sharing scheme is a key management scheme or key establishment scheme invented separately in 1979 by Shamir [1] and Blakley [2] as a solution to safeguard cryptographic keys. Secret sharing schemes are also used to protect other types of secrets, such as a secret recipe, etc. In “Secure Explorer” [3], information is stored in three separate data files using secret sharing technology. When two of three distributed files are combined, the original information can be reproduced. Secure Explorer performs the file distribution process at the moment of closing the file, and it can establish a secure process that guards against infection of malware. In this process, separate uninfected pieces do to overwrite and rewrite a file. So, using this system, it is always possible to maintain a secure environment. In this study, we will construct a preliminary file backup system for surface analysis data using Secure Explorer.*

**Keywords** – *secret sharing, backup, surface analysis, X-ray photoelectron spectroscopy, common data processing system, International Organization for Standardization, Zip.*

---

### Introduction

#### 1. What is open innovation

In recent years, the global competition for innovation has intensified, and the levels being achieved are rapidly diversifying and advancing. Of course, new materials and technologies are needed, and it is virtually impossible for a company to secure all of these under the conventional system of self-sufficiency.

To fill the gap, companies should make much greater use of external ideas and technologies in their own business, while letting their unused ideas be used by other companies. Through the realization of open innovation, both sides became win-win [4].

#### 2. Using the cloud for information sharing

Cloud services are increasingly attracting attention because they reduce the complexity of server management and new services can be quickly created.

If you have an internet-based work environment, it can be accessed regardless of time or place, so work can be done outside of a company’s physical location.

Conventional file sharing was commonly done over e-mail and USB, but by placing files in the cloud, it is possible to easily share multiple files at the same time [5].

Since all files can be managed centrally on the cloud, information retrieval can be done immediately when necessary.

When utilizing a fee-based service, it can be used as a new storage destination because there are many items which can be stored without having to regard to a capacity limit.

When utilizing online storage, only the service fee will be charged, and the initial cost can be drastically reduced [6].

#### 3. Problems with the cloud

Most operations of a cloud service are carried out under the control of the cloud operator, and it is common for the operator to share the computer resources with other users in order to minimize operating costs. Concerns for information security, such as data protection and maintenance, must therefore be pointed out [5].

When utilizing services offered by other

companies, it is difficult to customize the service for ease of use since there are many limits set from the beginning.

If a user knows a login ID and password, this can be accessed from outside the company, so it is necessary to completely manage information accessed by each employee. Since it is said that about 80% of information leaks are from insiders, we must educate external people not to leak IDs and passwords.

Since it is beyond the control of the company, if an obstacle occurs on the service provider end, the company cannot take any measures and only wait for recovery [6].

#### **4. Use secret sharing**

Both individuals and organizations are the second-leading targets of ransomware, as cited by the Information-technology Promotion Agency's "Information Security 10 Major Threats 2017". Information is stored in three data files separately using secret sharing technology which can protect against potential ransomware, and when necessary, two of the dispersed files are combined to reproduce the information.

In this study, we will construct a compressed file backup system for surface analysis using the cloud in the age of open innovation.

### **Industry 4.0**

#### **1. Background surrounding this research**

Industry 4.0 is the name for the current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of Things, cloud computing [7 – 9] and cognitive computing.

Over the Internet of Things, cyber-physical systems communicate and cooperate with each other and with humans in real time, and via cloud computing, both internal and cross-organizational services are offered and used by the participants in the value chain [7].

To realize high speed communication of information, communication devices are indispensable, and the materials making up the devices are important.

#### **2. Materials Informatics**

Recent advances in computational methods and the exponential increase in computer processing have made it possible to computationally generate large databases of material properties.

Materials informatics is a field of study that applies the principles of informatics science and engineering to better understand the use, selection, development, and discovery of materials. (The concept of materials informatics is addressed by the *Materials Research Society*. For example, materials informatics is the theme of the December 2006 issue of the *MRS Bulletin*.)

Furthermore, in order to get precise and clean electronic materials, the measurement of them – for example, surface analysis - becomes essential.

#### **3. The feature of Secure Explorer**

Our "Secure Explorer" adopts AIST's library (AIST: National Institute of Advanced Industrial Science and Technology) which is based on one of ISO standards (ISO/IEC 19592-2: 2017), namely, "Computational Additive Secret Sharing Scheme".

The features of Secure Explorer can be regarded as follows.

- (a) High system reliability;
- (b) Quick processing of large amounts of data;
- (c) Easy access;
- (d) Information disclosure published in Windows.

One of the unresolved issues for the construction of information security is the establishment of a public data center for further security.

### **Construction of a file backup system for surface analysis data**

#### **1. The reason to take surface analysis data as an object of study**

The outermost part of a material, its surface, is an extremely sensitive part which bears the surface characteristics such as chemical activity, adhesion, wetness, electrical properties, optical properties, corrosion-resistance, friction, and biocompatibility of the material, and it is also the part that is prone to losing such characteristics by degradation and contamination of the environment, adhesion of process residues, etc. [10].

Surface analysis is used not only for the development of new surfaces with high functionality and products, but also for helping materials with high functions properly exhibit their functionality.

Surface analysis methods have advanced as an essential technique for R&D and quality management of materials with new characteristics and features in many industrial and scientific research fields. Thus, surface analysis data is useful and of great significance.

## 2. The meaning of using XPS (X-ray Photoelectron Spectroscopy) for analyzing the surface of a material

In order to examine a solid surface, the surface must first be stimulated for signals to appear. Light, x-rays, and electrons are used for surface stimulation. The main types of surface analysis (Table 1) include XPS, TOF-SIMS (Time - of - Flight Secondary Ion Mass Spectrometry, where time-of-flight is proportional to the square root of the weight), and AES (Auger Electron Spectroscopy) [10].

**Table 1**

*Comparison of the possible different methods of selected area surface compositional analysis [11] (extract)*

Method	Information available	Spatial resolution	Advantages and disadvantages
X-ray photoelectron microscope (XPS)	Surface elemental composition and chemical state analysis	10um	Chemical shift information obtainable with a minimum of radiation damage. Image obtained by control of electron optics.
Scanning Auger microscope (SAM)	Surface elemental composition and some chemical state analysis via "fingerprinting"	30-500nm	Chemical state information is difficult to obtain although phase identification is possible from a multielement correlation diagram analysis.
Secondary ion imaging mass spectrometry (SIMS)	Surface elemental composition and isotope distribution	50nm	Excellent elemental sensitivity. Based on fragments, some chemical state information is possible although the interpretation can be difficult.

XPS is a technique in which x-rays are used to analyze the energy of photoelectrons generated by the photoelectric effect. It is characterized by its ability to analyze the elements constituting the sample surface, its composition, and chemical-bonding states. It can be used for the surface analysis of various materials regardless of whether they are organic or inorganic. Thus, this technique was used in this study.

## 3. COMPRO fit for the program to process XPS data

The Surface Analysis Society of Japan has been constructing the spectral data processing system named Common Data Processing System (COMPRO) under the VAMAS (Versailles Project on Advanced Materials and Standards) umbrella since 1989.

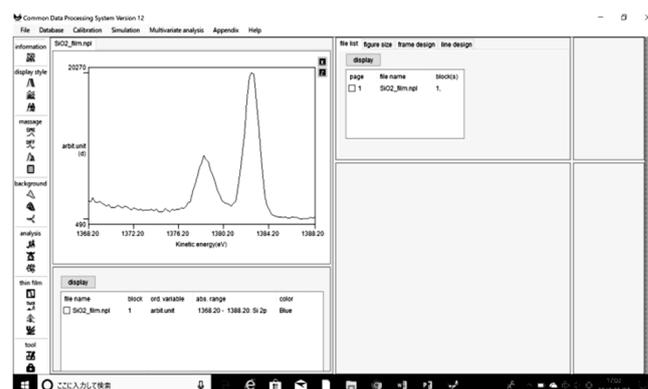
COMPRO has been designed as a program to convert an original spectral data file structure to ISO 14975 and 14976 formats, to assess the data processing procedures proposed by scientists, to calibrate energy and intensity scales according to ISO standards, to check a spectrum, and to build both spectra and correction factor databases [12].

## 4. Construction of a file backup system for COMPRO data

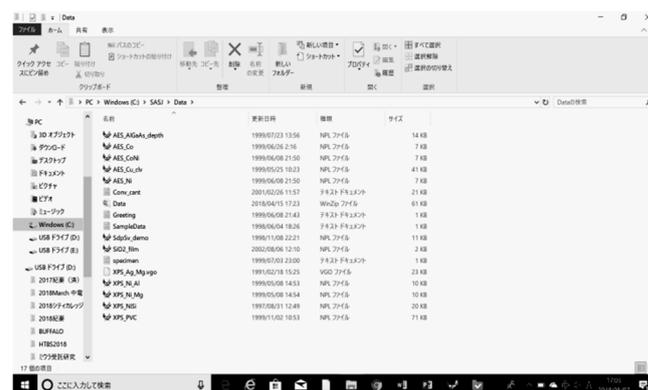
We attempted to construct a file backup system for the COMPRO data.

(1) The data of the surface of SiO<sub>2</sub> (Fig. 1) from the database of COMPRO on Windows has been added for convenience. This filename extension is ".npl".

We proceeded to carry out the secret sharing process and stored the divided files in three different parts for storage.



*Fig. 1. COMPRO data of the surface of SiO<sub>2</sub>.*



*Fig. 2. COMPRO data of the surface of SiO<sub>2</sub>.*

(2) In aiming to restore the original data, we discovered that the restoration cannot be done using the software of COMPRO (Fig. 2).

(3) Returning to the starting point, we combined the files from COMPRO in ZIP file format (Fig. 3).

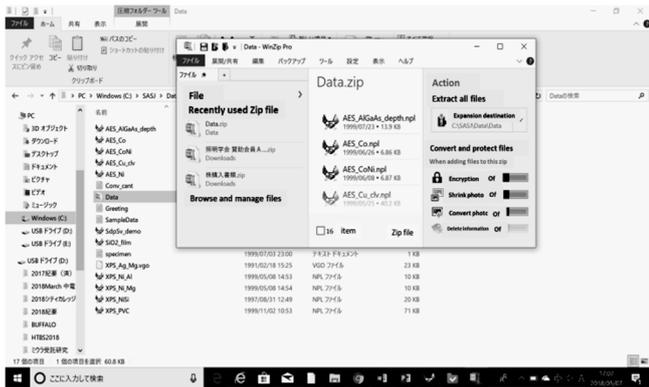


Fig. 3. The ZIP file using WinZip.

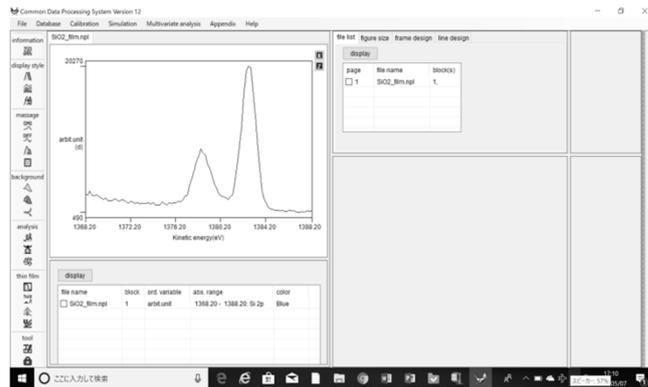


Fig. 6. The reconstruction COMPRO data.

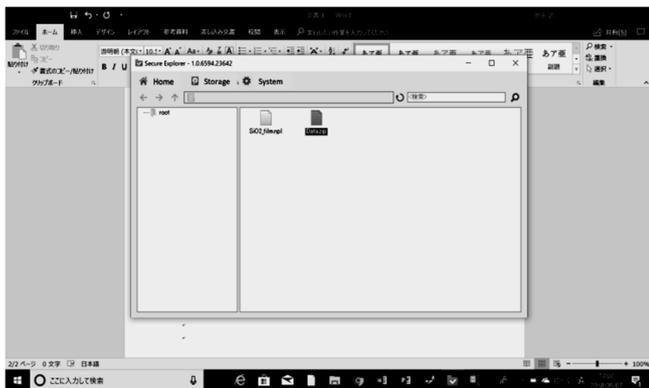


Fig. 4. The ZIP file using WinZip

Since a ZIP file is a “zipped” or compressed file, it takes up less hard drive space and takes less time to transfer to another computer. To store files as a ZIP file, we used a compression utility such as WinZip [13].

(4) When we combined all “.npl” files and compressed them using WinZip, we were able to perform the secret sharing process on the compressed file as intended (Fig. 4).

(5) After extracting the ZIP file using WinZip, we were able to access the “.npl” file and make use of the file using the software of COMPRO (Fig. 5 and Fig. 6).

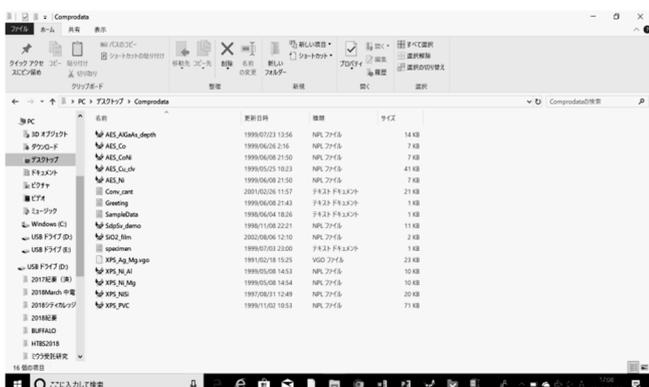


Fig. 5. The reconstruction COMPRO data.

## Conclusions

This study made it possible to devise a compressed file backup system for surface analysis using the cloud in the age of open innovation.

We compressed COMPRO data using WinZip and transferred the compressed file using a secret sharing method. After decompressing the compressed file, the secret sharing process has been achieved in restoring the original file. In other words, we established a compressed file backup system for surface analysis data using secret sharing technique by adding a ZIP file compression process when using COMPRO software.

Knowledge discovery in databases or data mining provides a unique tool in integrating scientific information and theory for materials discovery.

We believe that our preliminary file backup system can contribute to further developments in the study of materials informatics.

## REFERENCES

- [1] Shamir, A. How to share a secret, Communications of the ACM, Vol. 22, No. 11, 1979, pp.612-613.
- [2] Blakley, G. R. Safeguarding cryptographic keys. Proc. Of the National Computer Conference, Vol. 48, 1979, pp.313-317.
- [3] Tanaka, T. Construction of a preliminary educational system for file backup system using secret sharing technique. ELEKTROTECHNICA & ELEKTRONIKA, to be published.
- [4] Matsuno, M. MINISTRY OF EDUCATION, CULTURE, SPORTS, SCIENCE AND TECHNOLOGY – JAPAN : Science and technology white paper.
- [5] Information Media Center, Hiroshima University: Hiroshima University cloud service usage guidelines.
- [6] <https://boxil.jp/mag/a3414/#3414-9>
- [7] Hermann, Pentek, Otto, 2016: Design Principles for Industrie 4.0 Scenarios (<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=>

true&query=industrie%204.0%20design%20principles),  
accessed on 4 May 2016.

[8] Kagermann, H., W. Wahlster, J. Helbig, eds., 2013: Recommendations for implementing the strategic initiative Industrie 4.0: Final report of the Industrie 4.0 Working Group, 2013.

[9] Lasi, H., HG. Kemper, P. Fettke, Th. Feld, M. Hoffmann: Industry 4.0 In: Business & Information Systems Engineering, Vol. 4 (6), pp. 239-242.

[10] <https://www.ulvac-phi.com/en/surface.analysis/analysis/>

[11] O'Connor, D. J., B. A. Sexton, R. St. C. Smart. Surface Analysis Methods Materials Science, ISBN 987-3-642-07458-5 Springer-Verlag Berlin Heidelberg 1992, 2003, Table 1.7, pp.34.

[12] <http://www.sasj.jp/COMPRO/>

[13] . <http://www.winzip.com/win/jp/prodpagewz.html>

---

**Mr. Nobuharu Okamitsu** Doctoral student, Major in Intelligent Structure and Functional Science, Graduate School of Science and Technology, Hiroshima Institute of Technology, 2-1-1, Miyake, Saeki-ku, Hiroshima, 731-5193, Japan.

Tel. +81-82-921-3121 e-mail: [n.okamitsu@nifty.com](mailto:n.okamitsu@nifty.com)

**Mr. Tomonori Tabe** – Department of Electronics and Computer Engineering, Faculty of Engineering, Hiroshima Institute of Technology, 2-1-1, Miyake, Saeki-ku, Hiroshima, 731-5193, Japan.

**Mr. Ryota Matsuda** – Department of Electronics and Computer Engineering, Faculty of Engineering, Hiroshima Institute of Technology, 2-1-1, Miyake, Saeki-ku, Hiroshima, 731-5193, Japan.

**Mr. Noriyuki Yamada** – Innovation Firm Co.,Ltd, Taiyo Building 3F, 1-12-4, Iwamoto-cho, Chiyoda-ku, Tokyo 101-0032, Japan.

Tel. +81-3-5823-4398

e-mail: [noriyuki.yamada@innov-firm.co.jp](mailto:noriyuki.yamada@innov-firm.co.jp)

**Mr. Toyoharu Takemoto** – MIURA CORPORATION, 3-9, Minamisendahigashi, Naka-ku, Hiroshima 730-0054, Japan

Tel. +81-82-246-1155

**Prof. Dr. Takeshi Tanaka** – Department of Electronics and Computer Engineering, Faculty of Engineering, Hiroshima Institute of Technology, 2-1-1, Miyake, Saeki-ku, Hiroshima, 731-5193, Japan.

Tel. +81-82-921-3121

e-mail: [tanaka@cc.it-hiroshima.ac.jp](mailto:tanaka@cc.it-hiroshima.ac.jp)