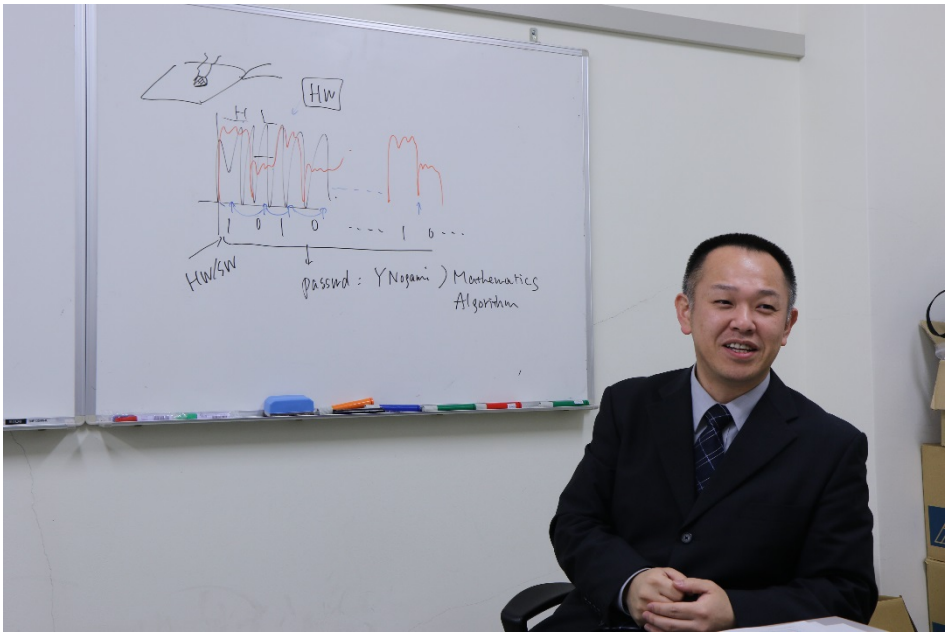
OKAYAMA UNIVERSITY e-Bulletin



Vol. 15, July 2016

Contents

News

Feature

Research Highlight

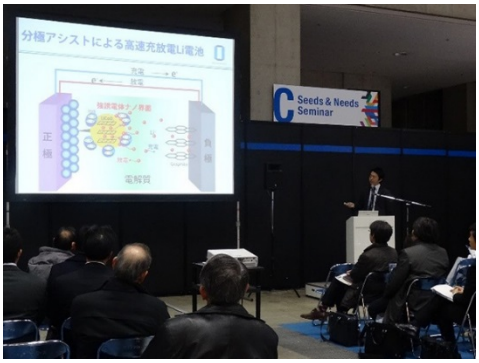
Topics

Okayama Travelogue

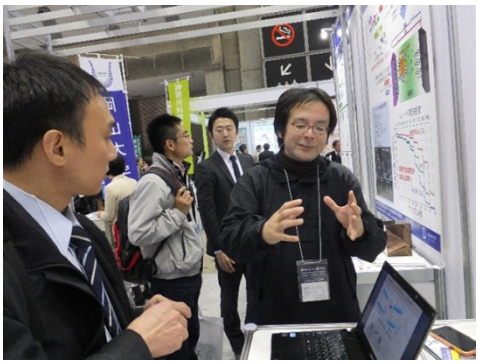
■ News

Okayama University participates in “nano tech 2016”: world’s largest exhibition of nanotechnology

Okayama University participated in “nano tech 2016 – the 15th International Nanotechnology Exhibition and Conference,” the world’s largest exhibition on nanotechnology held at Tokyo Big Sight , 27 to 29 January 2016.



Representatives from Okayama University displayed four posters and gave the following four oral presentations about science and technology



1. Yuta Nishina, Associate Professor, Research Core for Interdisciplinary Sciences
Title: Preparation and application of wood-derived nanocarbons (WNCs)

2. Takashi Teranishi, Assistant Professor, Department of Applied Chemistry, Graduate School of Natural Science and Technology
Title: Secondary battery with nano-ferroelectrics polarization assisted ultrahigh rate capability

3. Jun Kano, Associate Professor, Department of Applied Chemistry, Graduate School of Natural Science and Technology
Title: Catalyst designed by ferroelectric compounds

4. Toshihiko Kiwa, Associate Professor, Department of Medical Bioengineering, Graduate School of Natural Science and Technology
Title: Imaging of chemical reactions using a terahertz chemical microscopy

■ News

OKAYAMA UNIVERSITY Summer School 2016 Apply now !

1. Program Description

Students will examine the key obstacles to integrating East Asian countries into a tightly-knit community. Under the guidance of a multinational team of academics, students will examine issues of identity, colonial settlement, and contemporary politics in the East Asian context.

They will consider both the possibilities and dangers of increased cooperation, and come to understand the preconditions for forming a more systematic regional community. Utilizing Charles Taylor's concept of "social imaginary," this course will be an exercise in imagining an East Asian Community that will enjoy a widely shared sense of legitimacy among the peoples of the region.

2. Time/Date

Aug. 3 - Aug. 12, 2016

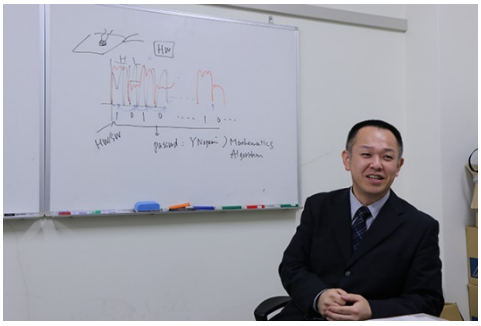
3. Okayama University Summer School 2016 Lecturers

Naomi Hosoda
Assistant professor at the Graduate School of Asian and African Area Studies, Kyoto University
Dong Kwang Kim
Professor at the Institute of Global Human Resource Development at Okayama University
Peodair Leihy
Administrator, strategist and researcher in the Academic Division, Universidad de Valparaíso, Chile
Simon Thornley

■ Feature

Okadai is Japan's leading university in IoT security

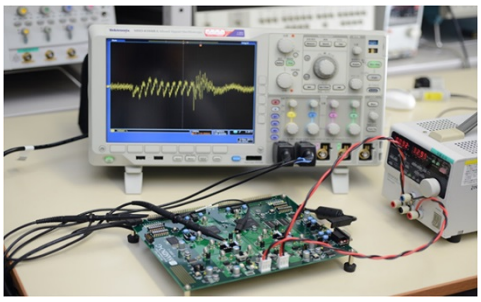
Yasuyuki Nogami, Associate Professor, Graduate School of Natural Science and Technology, Okayama University.



Associate Professor Yasuyuki Nogami, Graduate School of Natural Science and Technology, Okayama University

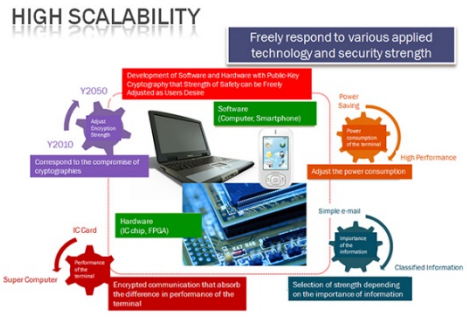
Advances in cybersecurity technology are important to meet the challenges of ensuring the safety and social acceptably of the proliferation of technology based cloud computing and internet of things (IoT).

Researchers at Okayama University are playing a central role in the development public-key internet security systems for data transmission. cybersecurity in particularly, RSA cryptography and elliptic curve cryptography for digital authentication of users and devices.



Hardware implementation of advanced cryptography and its security evaluation from the viewpoint of side channel information: On SASEBO, that is an security evaluation FPGA board, various pairing-based cryptographies are implemented on the board.

"Okayama University is Japan's top academic institute in research on cybersecurity," says Yasuyuki Nogami, head of the Okayama University Security Research Group. "In 2015 our cybersecurity group received the highest number of so-called 'Kakken' competitive research grants from Ministry of Education, Culture, Sports, Science and Technology (MEXT)."



Professor Nogami's trained as a mathematician and has a doctorate in 'finite field theory' and the construction of so-called extension fields from additive and multiplicative perspectives. After joining Okayama University Nogami concluded that it was "difficult to eat with mathematics" and decided to apply his mathematical skills to developing advanced cryptography. "My expertise in discrete mathematics is proving to be invaluable for cryptography," says Nogami. "Furthermore, I decided to set up the Okayama University Security Group to expand this area of research." The Group consists of 16 members with backgrounds in pure sciences, engineering, and medicine.

Selection of ongoing projects on advanced cryptography and its applications

Algorithms and hardware for 'secure cryptoprocessor' with adjustable security levels

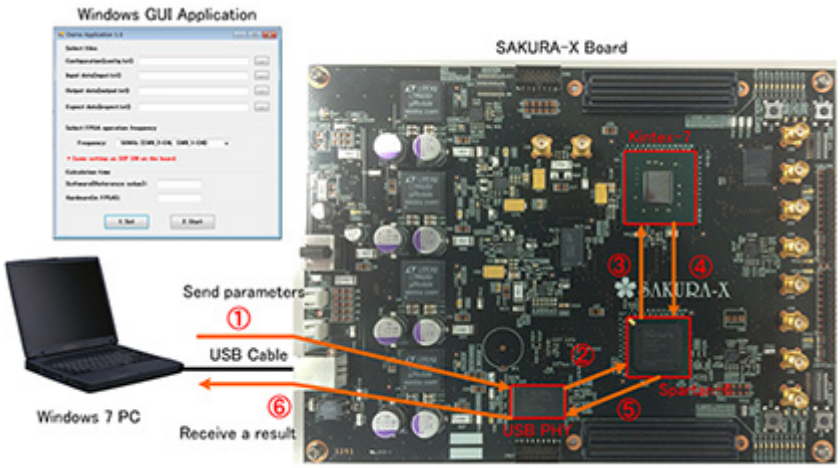
Professor Nogami and colleagues are developing an innovative 'secure cryptoprocessor chip' that can be programmed to match specific security levels—for example, high for protecting national secrets and not so high for protecting an online vending machine selling soft drinks. More specifically, the secure key length of RSA cryptography increases from 512, 1024, 2048, to 3072 bits, and accordingly, it is necessary to upgrade both the hardware and arithmetic architecture of cryptoprocessors to handle the increases in bit size.

The secure cryptoprocessor chip' being developed by the Okayama group is the world's first 'adjustable security level secure cryptoprocessor' offering variable security levels without requiring changes in the hardware. The Okayama University secure cryptoprocessor chip supports a wide range of recent cryptographic protocols including elliptic curve and paring-based cryptography. The secure cryptoprocessor can respond to security strengths between 256 to 5120 bits with elliptic curve and pairing-based cryptography. Notably, cryptoprocessor device is small in size and has a practical calculation efficiency.

This scalability of the chip is supported by the original idea of the Okayama group called cyclic vector multiplication algorithm (CVMA) that is used for vector multiplication but with the ability for wide ranging scalability for security parameters. The chip expected to find many applications including ubiquitous terminals and IoT devices.

Publication

Yasuyuki Nogami, et al, FPGA Implementation of Various Elliptic Curve Pairings over Odd Characteristic Field with Non Super Singular Curves, IEICE Trans. E99-D, No. 4, 805-815, (2016).
DOI: 10.1587/transinf.2015ICP0018



The SCOPE project—extracting passwords from electromagnetic noise from devices

Professor Nogami and colleagues have devised a method to extract the secret password for accessing personal computers and other such devices by analyzing the electromagnetic noise (em-noise) emanating from peripheral cables connected to the devices. The Okayama Security Group are leaders in this area of research in Japan.

This research requires expertise in the development of hardware, software, and mathematical algorithms.

High security communications for control systems

The development of secure and safe methods for controlling autonomous automobiles, medical robots for surgery, GPS information, images from compact CCD cameras and related sensors.

International collaboration

Professor Nogami and his colleagues at the Okayama Security Group are collaborating with the following groups overseas as part of the Super Global University Program.

San Jose State University, USA (Big data and cybersecurity)
INRAI, France (encryption)
Université de Rennes 1 (cryptographic mathematics)
Pusan University (encryption hardware)

■ Research Highlight

World's first flexible security Secure Cryptoprocessor with adjustable security level

Information security technology is necessary for the Cloud and IoT era. Particularly, public key cryptography such as RSA cryptography and elliptic curve cryptography plays an important role since it enables digital authentications for users and devices. In addition, recent innovative secure applications such as ID-based cryptography and time release encryption need much more complicated cryptographies such as pairing-based cryptography. ID-based cryptography enables the use some ID of the user as the public key.

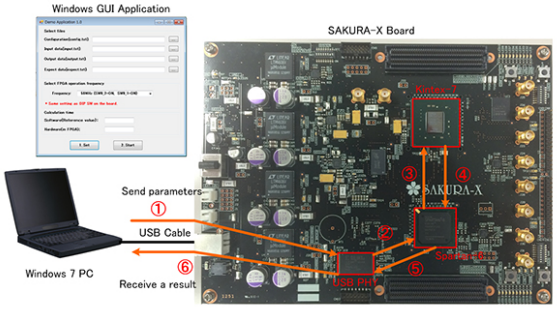


Figure 1: Secure Cryptoprocessor implemented on FPGA
This is the FPGA board on which the cryptoprocessor is embedded.
It is used for cryptographic simulations with changing security parameters flexibly.
The parameter settings are able to be controlled from the USB-connected PC.

On the other hand, the performance of computers improves dramatically year by year, and their level of security to prevent eavesdroppers should become higher accordingly. However, it is not easy to seamlessly adjust the security level of devices because public key cryptographies are basically based on some difficult and complicated mathematic problems. As an example, the secure key length of RSA cryptography increases 512, 1024, 2048, and then 3072 bits. Accordingly, cryptoprocessors need to be upgraded together with their arithmetic architectures.

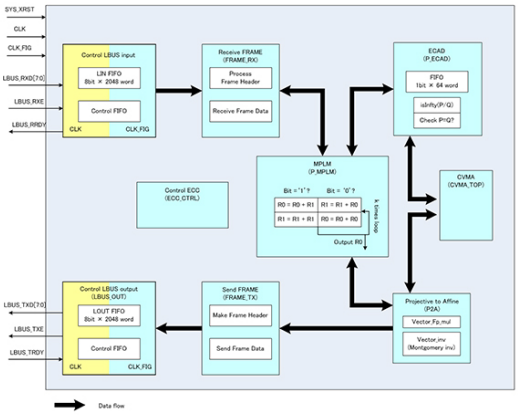


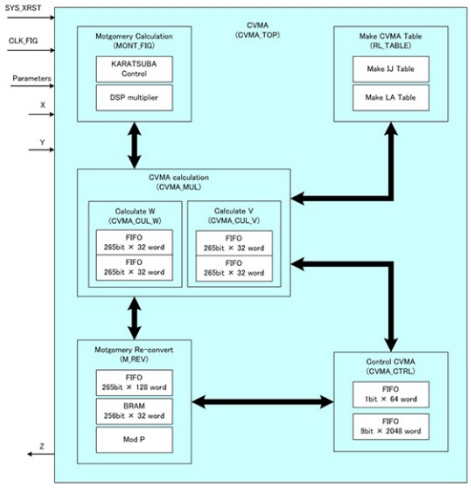
Figure 2: Calculation architecture
In the Kintex-7 on the board shown in Fig.1, the cryptoprocessor is embedded.
This figure shows the details of the calculation architecture.
It consists of several parts such as elliptic curve cryptography, Montgomery powering ladder,
vector multiplication (CVMA : cyclic vector multiplication algorithm), and pairing.
It flexibly accepts many kinds of parameter settings.

Now, Yasuyuki Nogami and colleagues at Okayama University and Tokyo Electron Device Ltd, supported by Japan Science and Technology Agency (JST) have developed a secure cryptoprocessor that is able to flexibly adjust the level of security without upgrading the device itself. The Okayama University secure cryptoprocessor device supports several kinds of recent cryptographies such as elliptic curve and paring-based cryptography.

The secure cryptoprocessor devices can respond to the requirements of a wide range of security strengths in between 256 to 5120 bits with elliptic curve and pairing-based cryptography. In addition, the secure cryptoprocessor device has a small circuit area size and practical calculation efficiency.

This is the world's first Secure Cryptoprocessor that can change the scale of security levels flexibly without requiring changes in the hardware. This scalability is supported by the original idea of the Okayama group called cyclic vector multiplication algorithm (CVMA). It is mainly used for vector multiplication but it enables wide scalability for security parameters.

It is expected to be mounted into a wide range of ubiquitous terminals and IoT devices because the circuit scale is extremely compact with efficient calculation power.



This figure shows the architecture of cyclic vector multiplication algorithm. It uses Montgomery representation for efficient multi-precision arithmetic. The cryptoprocessor supports many kinds of parameter settings for which CVMA plays an important role. That is, since CVMA is able to accept many parameter settings, then accordingly elliptic curve and pairing cryptographies on CVMA is also able to support a wide range of security parameters.

Reference:

Authors: Yasuyuki Nogami, Hiroto Kagotani, and Kengo Iokibe, Okayama University, Hiroyuki Miyatake and Takashi Narita, Tokyo Electron Device LTD.

Title of original paper: FPGA Implementation of Various Elliptic Curve Pairings over Odd Characteristic Field with Non Super Singular Curves.

Journal, volume, pages and year: IEICE Trans. E99-D, No. 4, 805-815, (2016).

Digital Object Identifier (DOI): 10.1587/transinf.2015ICP0018

Journal website: http://search.ieice.org/bin/summary.php?id=e99-d_4_805

Affiliations: Graduate School of Natural Science and Technology, Okayama University.

Department website: http://www.gnst.okayama-u.ac.jp/index_e.html

■ Research Highlight

Traceability for Multimedia Content: Protection against Pirated Copies

Digital Fingerprinting is a technique to identify users of illegal copies of multimedia content. It secretly inserts each user's identity information into the content before sale. If an illegal copy is discovered, the illegal user(s) can be identified by the appropriate extraction of embedded information from the copy.

If a coalition of users compares their uniquely fingerprinted copies, they will find the differences, and hence they will be able to delete/modify the embedded information. In conventional systems, their algorithms for inserting/detecting the identities should be secret so that they cannot directly modify the information. However, if the system is standardized, the specifications of the algorithms must be disclosed in public except for a secret key.

Now, Minoru Kuribayashi at Okayama University has developed a simple method to enhance the security of conventional schemes.

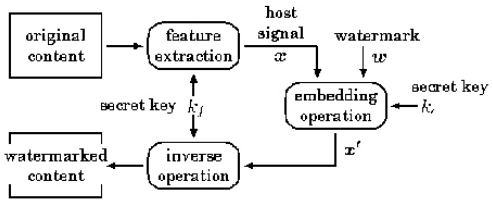


Figure 1: Framework of the fingerprinting scheme.
There are two main operations: one is feature extraction and the other is the embedding operation. Even if a secret key is used for feature extraction, a coalition of users will easily determine the selected host signal. The security problem in the feature extraction is solved in the proposed method by introducing a simple obfuscation method.

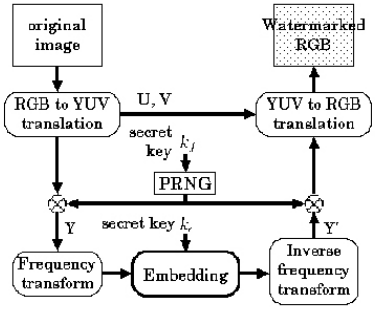


Figure 2: Flowchart of the proposed method.
Before selecting the feature points of an original image, a pseudo-random number is multiplied to the luminance components to obfuscate the elements selected for embedding fingerprint signals.

For a coalition of users, several pirated copies are produced using standard images based on the consideration of possible attack scenarios, and the traceability from the pirated copies is evaluated through computer simulations.

The proposed scheme ensures the secrecy of the inserted fingerprint signal even if all algorithms except for the secret key are disclosed. Without the secret key, it is difficult for a coalition of users to effectively delete/reduce the inserted signals as fingerprints. What they can do is to globally degrade the given fingerprinted copies to produce a pirated version.

It is expected that the proposed method can be applied for the prevention of illegal distribution of multimedia content, which stimulates the industry of content distribution services via Internet.

Reference:

Authors: Minoru Kuribayashi.
Title of original paper: Simple countermeasure to non-linear collusion attacks targeted for spread-spectrum fingerprinting scheme.
Journal, volume, pages and year: IEICE Trans. E99-D, No.1, 50-59, (2016).
Digital Object Identifier (DOI): 10.1587/transinf.2015MUP0005
Journal website: http://search.ieice.org/bin/summary.php?id=e99-d_1_50
Affiliations: Graduate School of Natural Science and Technology, Okayama University.
Department website: http://www.eng.okayama-u.ac.jp/eng_elec/html/

■ Topics: Okayama Travelogue

Yumeji Art Museum

The exhibits at the Yumeji Art Museum Okayama, celebrate the artistic genius of painter, illustrator, poet, and writer Yumeji Takehisa, born in Okayama in 1884, and famous for his drawings of women during the Taisho era (1912-1926).

The women depicted in the drawings—'Yumeji bijin-ga'—are distinctive in that they have slim bodies, large eyes, and drawn in typical Japanese scenes such as a fireworks festival and rising moon.

Since opening in 1966 the museum has welcomed many visitors—both local and overseas—and the award of a Michelin Guide Star in 2007 underscores the importance and popularity of the approximately 3000 exhibits on display in the refined surroundings that are a mixture of Japanese and Western designs.

Further information
http://yumeji-art-museum.com/07_index-e.html

Tatsuta hime

Douji

