http://www.icact.org/journal.asp

ICACT-TACT JOURNAL

Transactions on Advanced Communications Technology

Volume 8 Issue 5, September. 2019, ISSN: 2288-0003

Editor-in-Chief
Prof. Thomas Byeongnam YOON, PhD.

GIRI
Global IT Research Institute

Journal Editorial Board

■ Editor-in-Chief

Prof. Thomas Byeongnam YOON, PhD.
Founding Editor-in-Chief
ICACT Transactions on the Advanced Communications Technology (TACT)

■ Editors

Prof. Jun-Chul Chun, Kyonggi University, Korea
Dr. JongWon Kim, GIST (Gwangju Institute of Science & Technology), Korea
Dr. Xi Chen, State Grid Corparation of China, China
Prof. Arash Dana, Islamic Azad university , Central Tehran Branch, Iran
Dr. Pasquale Pace, University of Calabria - DEIS - Italy, Italy
Dr. Mitch Haspel, Stochastikos Solutions R&D, Israel
Prof. Shintaro Uno, Aichi University of Technology, Japan
Dr. Tony Tsang, Hong Kong Polytechnic UNiversity, Hong Kong
Prof. Kwang-Hoon Kim, Kyonggi University, Korea
Prof. Rosilah Hassan, Universiti Kebangsaan Malaysia(UKM), Malaysia
Dr. Sung Moon Shin, ETRI, Korea
Dr. Takahiro Matsumoto, Yamaguchi University, Japan
Dr. Christian Esteve Rothenberg, CPqD - R&D Center for. Telecommunications, Brazil
Prof. Lakshmi Prasad Saikia, Assam down town University, India
Prof. Moo Wan Kim, Tokyo University of Information Sciences, Japan
Prof. Yong-Hee Jeon, Catholic Univ. of Daegu, Korea
Dr. E.A.Mary Anita, Prathyusha Institute of Technology and Management, India
Dr. Chun-Hsin Wang, Chung Hua University, Taiwan
Prof. Wilaiporn Lee, King Mongkut's University of Technology North, Thailand
Dr. Zhi-Qiang Yao, XiangTan University, China
Prof. Bin Shen, Chongqing Univ. of Posts and Telecommunications (CQUPT), China
Prof. Vishal Bharti, Dronacharya College of Engineering, India
Dr. Marsono, Muhammad Nadzir , Universiti Teknologi Malaysia, Malaysia
Mr. Muhammad Yasir Malik, Samsung Electronics, Korea
Prof. Yeonseung Ryu, Myongji University, Korea
Dr. Kyuchang Kang, ETRI, Korea
Prof. Plamena Zlateva, BAS(Bulgarian Academy of Sciences), Bulgaria
Dr. Pasi Ojala, University of Oulu, Finland
Prof. CheonShik Kim, Sejong University, Korea
Dr. Anna bruno, University of Salento, Italy
Prof. Jesuk Ko, Gwangju University, Korea
Dr. Saba Mahmood, Air University Islamabad Pakistan, Pakistan
Prof. Zhiming Cai, Macao University of Science and Technology, Macau
Prof. Man Soo Han, Mokpo National Univ., Korea
Mr. Jose Gutierrez, Aalborg University, Denmark

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Dr. Youssef SAID, Tunisie Telecom, Tunisia
Dr. Noor Zaman, King Faisal University, Al Ahsa Hofuf, Saudi Arabia
Dr. Srinivas Mantha, SASTRA University, Thanjavur, India
Dr. Shahriar Mohammadi, KNTU University, Iran
Prof. Beonsku An, Hongik University, korea
Dr. Guanbo Zheng, University of Houston, USA
Prof. Sangho Choe, The Catholic University of Korea, korea
Dr. Gyanendra Prasad Joshi, Yeungnam University, korea
Dr. Tae-Gyu Lee, Korea Institue of Industrial Technology(KITECH), korea
Prof. Ilkyeun Ra, University of Colorado Denver, USA
Dr. Yong Sun, Beijing University of Posts and Telecommunications, China
Dr. Yulei Wu, Chinese Academy of Sciences, China
Mr. Anup Thapa, Chosun University, korea
Dr. Vo Nguyen Quoc Bao, Posts and Telecommunications Institute of Technology, Vietnam
Dr. Harish Kumar, Bhagwant institute of technology, India
Dr. Jin REN, North china university of technology, China
Dr. Joseph Kandath, Electronics & Commn Engg, India
Dr. Mohamed M. A. Moustafa, Arab Information Union (AIU), Egypt
Dr. Mostafa Zaman Chowdhury, Kookmin University, Korea
Prof. Francis C.M. Lau, Hong Kong Polytechnic University, Hong Kong
Prof. Ju Bin Song, Kyung Hee University, korea
Prof. KyungHi Chang, Inha University, Korea
Prof. Sherif Welsen Shaker, Kuang-Chi Institute of Advanced Technology, China
Prof. Seung-Hoon Hwang, Dongguk University, Korea
Prof. Dal-Hwan Yoon, Semyung University, korea
Prof. Chongyang ZHANG, Shanghai Jiao Tong University, China
Dr. H K Lau, The Open University of Hong Kong, Honh Kong
Prof. Ying-Ren Chien, Department of Electrical Engineering, National Ilan University, Taiwan
Prof. Mai Yi-Ting, Hsiuping University of Science and Technology, Taiwan
Dr. Sang-Hwan Ryu, Korea Railroad Research Institute, Korea
Dr. Yung-Chien Shih, MediaTek Inc., Taiwan
Dr. Kuan Hoong Poo, Multimedia University, Malaysia
Dr. Michael Leung, CEng MIET SMIEEE, Hong Kong
Dr. Abu sahman Bin mohd Supa'at, Universiti Teknologi Malaysia, Malaysia
Prof. Amit Kumar Garg, Deenbandhu Chhotu Ram University of Science & Technology, India
Dr. Jens Myrup Pedersen, Aalborg University, Denmark
Dr. Augustine Ikechi Ukaegbu, KAIST, Korea
Dr. Jamshid Sangirov, KAIST, Korea
Prof. Ahmed Dooguy KORA, Ecole Sup. Multinationale des Telecommunications, Senegal
Dr. Se-Jin Oh, Korea Astronomy & Space Science Institute, Korea
Dr. Rajendra Prasad Mahajan, RGPV Bhopal, India
Dr. Woo-Jin Byun, ETRI, Korea
Dr. Mohammed M. Kadhum, School of Computing, Goodwin Hall, Queen's University , Canada
Prof. Seong Gon Choi, Chungbuk National University, Korea
Prof. Yao-Chung Chang, National Taitung University, Taiwan
Dr. Abdallah Handoura, Engineering school of Gabes - Tunisia, Tunisia
Dr. Gopal Chandra Manna, BSNL, India

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Dr. Il Kwon Cho, National Information Society Agency, Korea
Prof. Jiann-Liang Chen, National Taiwan University of Science and Technology, Taiwan
Prof. Ruay-Shiung Chang, National Dong Hwa University, Taiwan
Dr. Vasaka Visoottiviseth, Mahidol University, Thailand
Prof. Dae-Ki Kang, Dongseo University, Korea
Dr. Yong-Sik Choi, Research Institute, IDLE co., ltd, Korea
Dr. Xuena Peng, Northeastern University, China
Dr. Ming-Shen Jian, National Formosa University, Taiwan
Dr. Soobin Lee, KAIST Institute for IT Convergence, Korea
Prof. Yongpan Liu, Tsinghua University, China
Prof. Chih-Lin HU, National Central University, Taiwan
Prof. Chen-Shie Ho, Oriental Institute of Technology, Taiwan
Dr. Hyoung-Jun Kim, ETRI, Korea
Prof. Bernard Cousin, IRISA/Universite de Rennes 1, France
Prof. Eun-young Lee, Dongduk Woman s University, Korea
Dr. Porkumaran K, NGP institute of technology India, India
Dr. Feng CHENG, Hasso Plattner Institute at University of Potsdam, Germany
Prof. El-Sayed M. El-Alfy, King Fahd University of Petroleum and Minerals, Saudi Arabia
Prof. Lin You, Hangzhou Dianzi Univ, China
Mr. Nicolai Kuntze, Fraunhofer Institute for Secure Information Technology, Germany
Dr. Min-Hong Yun, ETRI, Korea
Dr. Seong Joon Lee, Korea Electrotechnology Research Institute, korea
Dr. Kwihoon Kim, ETRI, Korea
Dr. Jin Woo HONG, Electronics and Telecommunications Research Inst., Korea
Dr. Heeseok Choi, KISTI(Korea Institute of Science and Technology Information), korea
Dr. Somkiat Kitjongthawonkul, Australian Catholic University, St Patrick's Campus, Australia
Dr. Dae Won Kim, ETRI, Korea
Dr. Ho-Jin CHOI, KAIST(Univ), Korea
Dr. Su-Cheng HAW, Multimedia University, Faculty of Information Technology, Malaysia
Dr. Myoung-Jin Kim, Soongsil University, Korea
Dr. Gyu Myoung Lee, Institut Mines-Telecom, Telecom SudParis, France
Dr. Dongkyun Kim, KISTI(Korea Institute of Science and Technology Information), Korea
Prof. Yoonhee Kim, Sookmyung Women s University, Korea
Prof. Li-Der Chou, National Central University, Taiwan
Prof. Young Woong Ko, Hallym University, Korea
Prof. Dimiter G. Velev, UNWE(University of National and World Economy), Bulgaria
Dr. Tadasuke Minagawa, Meiji University, Japan
Prof. Jun-Kyun Choi, KAIST (Univ.), Korea
Dr. Brownson ObaridoaObele, Hyundai Mobis Multimedia R&D Lab , Korea
Prof. Anisha Lal, VIT university, India
Dr. kyeong kang, University of technology sydney, faculty of engineering and IT , Australia
Prof. Chwen-Yea Lin, Tatung Institute of Commerce and Technology, Taiwan
Dr. Ting Peng, Chang'an University, China
Prof. ChaeSoo Kim, Donga University in Korea, Korea
Prof. kirankumar M. joshi, m.s.uni.of baroda, India
Dr. Chin-Feng Lin, National Taiwan Ocean University, Taiwan
Dr. Chang-shin Chung, TTA(Telecommunications Technology Association), Korea

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Dr. Che-Sheng Chiu, Chunghwa Telecom Laboratories, Taiwan
Dr. Chirawat Kotchasarn, RMUTT, Thailand
Dr. Fateme Khalili, K.N.Toosi. University of Technology, Iran
Dr. Izzeldin Ibrahim Mohamed Abdelaziz, Universiti Teknologi Malaysia , Malaysia
Dr. Kamrul Hasan Talukder, Khulna University, Bangladesh
Prof. HwaSung Kim, Kwangwoon University, Korea
Prof. Jongsub Moon, CIST, Korea University, Korea
Prof. Juinn-Horng Deng, Yuan Ze University, Taiwan
Dr. Yen-Wen Lin, National Taichung University, Taiwan
Prof. Junhui Zhao, Beijing Jiaotong University, China
Dr. JaeGwan Kim, SamsungThales co, Korea
Prof. Davar PISHVA, Ph.D., Asia Pacific University, Japan
Ms. Hela Mliki, National School of Engineers of Sfax, Tunisia
Prof. Amirmansour Nabavinejad, Ph.D., Sepahan Institute of Higher Education, Iran

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Editor Guide

■ Introduction for Editor or Reviewer

All the editor group members are to be assigned as a evaluator(editor or reviewer) to submitted journal papers at the discretion of the Editor-in-Chief. It will be informed by eMail with a Member Login ID and Password.

Once logined the Website via the Member Login menu in left as a evaluator, you can find out the paper assigned to you. You can evaluate it there. All the results of the evaluation are supposed to be shown in the Author Homepage in the real time manner. You can also enter the Author Homepage assigned to you by the Paper ID and the author's eMail address shown in your Evaluation Webpage. In the Author Homepage, you can communicate each other efficiently under the peer review policy. Please don't miss it!

All the editor group members are supposed to be candidates of a part of the editorial board, depending on their contribution which comes from history of ICACT TACT as an active evaluator. Because the main contribution comes from sincere paper reviewing role.

■ Role of the Editor

The editor's primary responsibilities are to conduct the peer review process, and check the final camera-ready manuscripts for any technical, grammatical or typographical errors.

As a member of the editorial board of the publication, the editor is responsible for ensuring that the publication maintains the highest quality while adhering to the publication policies and procedures of the ICACT TACT(Transactions on the Advanced Communications Technology).

For each paper that the editor-in-chief gets assigned, the Secretariat of ICACT Journal will send the editor an eMail requesting the review process of the paper.

The editor is responsible to make a decision on an "accept", "reject", or "revision" to the Editor-in-Chief via the Evaluation Webpage that can be shown in the Author Homepage also.

■ Deadlines for Regular Review

Editor-in-Chief will assign a evalaution group(a Editor and 2 reviewers) in a week upon receiving a completed Journal paper submission. Evaluators are given 2 weeks to review the paper. Editors are given a week to submit a recommendation to the Editor-in-Chief via the evaluation Webpage, once all or enough of the reviews have come in. In revision case, authors have a maximum of a month to submit their revised manuscripts. The deadlines for the regular review process are as follows:

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Evalution Procedure	Deadline
Selection of Evaluation Group	1 week
Review processing	2 weeks
Editor's recommendation	1 week
Final Decision Noticing	1 week

■ Making Decisions on Manuscript

Editor will make a decision on the disposition of the manuscript, based on remarks of the reviewers. The editor's recommendation must be well justified and explained in detail. In cases where the revision is requested, these should be clearly indicated and explained. The editor must then promptly convey this decision to the author. The author may contact the editor if instructions regarding amendments to the manuscript are unclear. All these actions could be done via the evaluation system in this Website. The guidelines of decisions for publication are as follows:

Decision	Description
Accept	An accept decision means that an editor is accepting the paper with no further modifications. The paper will not be seen again by the editor or by the reviewers.
Reject	The manuscript is not suitable for the ICACT TACT publication.
Revision	The paper is conditionally accepted with some requirements. A revision means that the paper should go back to the original reviewers for a second round of reviews. We strongly discourage editors from making a decision based on their own review of the manuscript if a revision had been previously required.

■ Role of the Reviewer

Reviewer Webpage:

Once logined the Member Login menu in left, you can find out papers assigned to you. You can also login the Author Homepage assigned to you with the paper ID and author's eMail address. In there you can communicate each other via a Communication Channel Box.

Quick Review Required:

You are given 2 weeks for the first round of review and 1 week for the second round of review. You must agree that time is so important for the rapidly changing IT technologies and applications trend. Please respect the deadline. Authors undoubtedly appreciate your quick review.

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Anonymity:

Do not identify yourself or your organization within the review text.

Review:

Reviewer will perform the paper review based on the main criteria provided below. Please provide detailed public comments for each criterion, also available to the author.

- How this manuscript advances this field of research and/or contributes something new to the literature?
- Relevance of this manuscript to the readers of TACT?
- Is the manuscript technically sound?
- Is the paper clearly written and well organized?
- Are all figures and tables appropriately provided and are their resolution good quality?
- Does the introduction state the objectives of the manuscript encouraging the reader to read on?
- Are the references relevant and complete?

Supply missing references:

Please supply any information that you think will be useful to the author in revision for enhancing quality of the paperor for convincing him/her of the mistakes.

Review Comments:

If you find any already known results related to the manuscript, please give references to earlier papers which contain these or similar results. If the reasoning is incorrect or ambiguous, please indicate specifically where and why. If you would like to suggest that the paper be rewritten, give specific suggestions regarding which parts of the paper should be deleted, added or modified, and please indicate how.

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Journal Procedure

Dear Author,

- **You can see all your paper information & progress.**

- **Step 1. Journal Full Paper Submission**

Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Journal Paper/CRF Template

- **Step 2. Full Paper Review**

Using the evaluation system in the ICACT Website, the editor, reviewer and author can communicate each other for the good quality publication. It may take about 1 month.

- **Step 3. Acceptance Notification**

It officially informs acceptance, revision, or reject of submitted full paper after the full paper review process.

Status	Action
Acceptance	Go to next Step.
Revision	Re-submit Full Paper within 1 month after Revision Notification.
Reject	Drop everything.

- **Step 4. Payment Registration**

So far it's free of charge in case of the journal promotion paper from the registered ICACT conference paper! But you have to regist it, because you need your Journal Paper Registration ID for submission of the final CRF manuscripts in the next step's process. Once you get your Registration ID, send it to Secretariat@icact.org for further process.

- **Step 5. Camera Ready Form (CRF) Manuscripts Submission**

After you have received the confirmation notice from secretariat of ICACT, and then you are allowed to submit the final CRF manuscripts in PDF file form, the full paper and the Copyright Transfer Agreement. Journal Paper Template, Copyright Form Template, BioAbstract Template,

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Journal Submission Guide

All the Out-Standing ICACT conference papers have been invited to this "ICACT Transactions on the Advanced Communications Technology" Journal, and also welcome all the authors whose conference paper has been accepted by the ICACT Technical Program Committee, if you could extend new contents at least 30% more than pure content of your conference paper. Journal paper must be followed to ensure full compliance with the IEEE Journal Template Form attached on this page.

➢ How to submit your Journal paper and check the progress?

Step 1. Submit	Using the Submit button, submit your journal paper through ICACT Website, then you will get new paper ID of your journal, and send your journal Paper ID to the Secretariat@icact.org for the review and editorial processing. Once you got your Journal paper ID, never submit again! Using the Update button, you can change any information of journal paper related or upload new full journal paper.
Step 2. Confirm	Secretariat is supposed to confirm all the necessary conditions of your journal paper to make it ready to review. In case of promotion from the conference paper to Journal paper, send us all the .DOC(or Latex) files of your ICACT conference paper and journal paper to evaluate the difference of the pure contents in between at least 30% more to avoid the self replication violation under scrutiny. The pure content does not include any reference list, acknowledgement, Appendix and author biography information.
Step 3. Review	Upon completing the confirmation, it gets started the review process thru the Editor & Reviewer Guideline. Whenever you visit the Author Homepage, you can check the progress status of your paper there from start to end like this, " Confirm OK! -> Gets started the review process -> ...", in the Review Status column. Please don't miss it!

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Volume. 8 Issue. 5

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Comprehending Taiwan ATM Heist: From Cyber-attack Phases to Investigation Processes

Da-Yu KAO

Department of Information Management, Central Police University, Taoyuan 333, Taiwan

dayukao@gmail.com

***Abstract*—Cybercriminals increasingly use sophisticated tools and advanced methods to attack bank systems. Cyber black markets for hacking tools or services are gaining widespread attention as more advanced persistent threat attacks are relevant to such markets. The recent cyber-attacks on banks or financial institutions have increased the technical expertise of cybercriminals. This study reviews ATM threats and highlights the cybercrime investigation of ATM heist. An incident investigation strategy from ISO/IEC 27043:2015 is proposed to embed cyber-attack phases and detect ATM heist. It demonstrates how this strategy can provide investigators with exceptional abilities to interpret evidence. By integrating an effective cybercrime investigation strategy, investigators can minimize the cost of collecting evidence in a forensically sound manner.**

Keyword—Cybercrime, ATM Threats, Bank Malware, Criminal Group, ISO/IEC 27043: 2015, Cybercrime Investigation, Malware Family

I. INTRODUCTION

A. Cybercrime Threats on Sophisticated ICT environment

The Internet has become an integral part of our society, and it enriches our lives in countless ways. Information and communications technologies (ICTs) are the integration of telecommunications, computers, and software, which enable users to access information. As the computer systems of the new ICT environment get more sophisticated than before, so do the criminals. ICTs have facilitated not only the methods in which crimes are committed but also the methods in which criminals interact in committing them.

1) Exploitable Vulnerabilities to Computer System

Zero-day vulnerabilities are exploitable weaknesses that a software vendor is not aware of and for which no patch has been created. However, half-days are also prevalent in the black market where the software creator may know of the weaknesses. A patch may be available, but few users are aware of and implementing those patches [18]. That is where the danger lies. People are the greatest threat to a computer system [8]. More exceptional care has to be paid to the individuals' authorization to access sensitive data in the computer system since this can reduce the number of attack incidents.

2) *Increasing Expertise of Cybercriminals*

The Internet has come to represent both attractive and available for finding victims. The data breach of hacking activities becomes prevalent. The sophistication of cybercriminals and their advantageous positions as attackers will target the transactions for a data breach, and innovate in ways to infiltrate computer systems [12].

3) *Undetected Cybercrimes on Malware Attacks*

Cyberspace consists of interrelated and interdependent ICT devices. That includes the Internet, telecommunications networks, and computer systems [4]. As ICT continues to change and evolve, some cybercrimes remain undetected. Cybercriminals increasingly use sophisticated tools and advanced methods to distribute a wide range of malicious attacks [6]. Cybercrimes require the advanced hacking capability to target financial services, and the global economy requires a proactive and coordinated response.

B. Financial Technology

Financial Technology (FinTech) refers to the use of software and digital platforms to deliver money exchange services to consumers and make it easier than ever to make transactions between two entities [21]. While much cybercrime is committed by individuals acting alone, a significant amount of criminal groups have tended to vary significantly in their criminal activities. Cybercrimes are developing exponentially and threating our FinTech. To fight against the unlimited growth of Automated Teller Machine (ATM) security threats, a sound knowledge of the problem and perpetrators can contribute to preventing cybercrimes.

1) Advantages

a) The Traditional Need for Strict Security Controls

Banks use many electronic systems for the operation of their

Manuscript received Jan. 1, 2019. This work was a follow-up of the invited journal to the accepted & presented paper of the 21st Conference on Advanced Communication Technology (ICACT2019), and this research was partially sponsored by the Executive Yuan of the Republic of China under the Grants Forward-looking Infrastructure Development Program (Digital Infrastructure-Information Security Project-109).

Da-Yu Kao is with the Department of Information Management, Central Police University, Taoyuan 333, Taiwan (Corresponding Author phone: +886-3-328-2321; fax: +886-3-328-5189; e-mail: dayukao@gmail.com).

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

economic environment. Traditionally, they use strict security controls overall operational and transaction-related procedures. In terms of segregation of duties, all systems administration must have dual login controls, rare network protocols, and multiple serial firewalls for internal banking communications [3]. However, banks generally choose an open system due to friendly user-interface, convenient process, or insufficient budget. That raises severe concerns on ATM protection. Several measures can be adopted by banks to detect, prevent, and minimize the cybercrime damage on the Internet.

b) Online ATMs for Convenient Payment Activities

Once computers or ATMs connect to the insecure Internet, no one can guarantee their security. Online ATMs have gained increasing popularity all over the world, as they provide convenience to the public in managing their banking accounts and payment activities [21]. The vulnerability of a complicated, fragmented ATM system relies on many providers to get customers to cash on demand. Due to the growth of FinTech, some ATM services have offered convenient payment solutions to facilitate online internal examination.

2) Disadvantages

a) The Lack of Cybersecurity Awareness

Exploits take advantage of weaknesses or vulnerabilities in software. A vulnerability run malicious code onto compromised computers. Malware can further infect other internal computers without users' knowledge [14]. Financial ATMs to internet-connected industrials should not be built using commercial operating systems for safety concerns. The lack of cybersecurity awareness may enhance the vulnerability of individuals and organizations. The threat of cybercrime impedes the development of information technology. It could contribute to the weakening of a nation's economic security.

b) Unauthorized Access of Internal ATM Details

How can the criminal group obtain the internal ATM information? Internal IP Address, computer name, and device name should be challenging to match them. As far as ICT governance is concerned, this kind of data is limited to internal vital persons. The main threat arising is the possibility of unauthorized access and use of bank card/ATM information by a fraudster [3]. Once malware is in place, buyers can rent them to deliver a variety of attacks. Active crime groups have recognized the benefits of the Internet [21]. A bank system should have the boundary of a closed system for safety concerns [10]. A closed system has no external interactions and is an isolated system that exchanges neither matter nor information with its environment. No interactions can take the form of information or material transfers into or out of the system boundary.

3) Proper Security Measures

Banks may implement several organized policies to protect against computer security threats. Moreover, banks need to provide information security training to staff, increase their awareness of the Internet dangers, and create effective practices to prevent its happening [22]. The following security measures for banks are recommended both to the cashpoints and the environment they are placed in, with sufficient lighting and cameras monitoring all activity [14].

- Review the physical security of all ATMs
- Consider investing in quality security solutions.
- Replace all locks and master keys on the upper hood of the ATMs
- Ditch the defaults provided by the manufacturer.
- Install an alarm and ensure it is in good working order.
- Change the default BIOS password.
- Ensure the machines have up-to-date antivirus protection.

The literature reviews of organized cybercrime activities and ATM threats are discussed in Section 2. Section 3 describes specific questions and behavioral attributes in Taiwan ATM Heist. An incident investigation strategy from ISO/IEC 27043:2015 is proposed to embed cyber-attack phases and detect ATM heist in Section 4. Our conclusions are given in Section 5.

II. LITERATURE REVIEWS

A. Organized Cybercrime Activities

Cybercrime has grown tremendously over the past decade as public administration and private service gained a more fabulous online presence than before. The increasing risk of cyber-attack is driven by continuously changing technology, vulnerabilities, and advanced persistent threats. An ongoing chronology of serious data breaches raises awareness about cybercrime issues [16]. A review is a necessary step in the continued growth of a multi-faceted lens on cyber-attack or investigation process. The cybercrime investigation discipline intersects several fields, including computer science, criminology, and management. Cybercrime is a rapidly growing phenomenon that requires a proactive and coordinated response. The convenience for a user has become another advantage for criminals [14]. The diversity of organized cybercriminal exploits by state and non-state actors alike. Criminal offenders or nation-states have entailed a diverse set of organized activities. The following activities in Table I describe some organized cybercrime activities in recent years [7, 8].

1) Cross-broader Hackers in Organized Crime Groups

Geographical boundaries have become trivial as cyber-attacks are theoretically able to carry out from anywhere in the world. The cyber exploitations can occur outside of the reach of local Law Enforcement Agencies (LEAs)[4]. The Carberp malware source code was leaked and enhanced to create new threat products for sale to the underground fraud community [14]. The future damage cannot be limited or controlled. The do-it-yourself malware toolkit sold by the group has been used to make unauthorized banking transactions.

2) Malware Black Market for Hackers

The arrests or takedowns in cyber-attacks often lead to public

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

media coverage. Even if a group or individual gets taken down, the vast majority of criminals do not be arrested [9]. The black market of the organized group is on the increase and often connected with crime groups or nation-states. The hackers in online black markets or dark web grow smarter as they learn from LEAs' investigative techniques. Cybercrime vendors sold access to a wide selection of malware or compromised zombies from any country. Price tags for remote desktop-based access run no more than a few dollars. The criminal group could buy access to bank employee computers that were already compromised by massively distributed opportunistic malware [14]. The international reach of LEAs has some difficulties, and the development of bank malware continued. Cybercriminals would like to hide in any particular jurisdiction and avoid prosecution. They can make use of the lucrative malware black market, raise funds for their activities, and gather intelligence on possible targets [2].

3) The Need for Profiling Hackers

Investigating hackers is a time-consuming effort. The Internet offers a degree of anonymity which affords organized crime groups the ability to recruit cross-broader hackers. The hacker forums offer criminals a wide variety of malware for low prices to assist them in criminal activities. The topic of identifying a practical framework of cybercrime investigation is a challenging one. No current set of profiling cybercriminals exists. In this regard, the emergence of a useful cybercrime investigation framework may rely on the experiences of cybercrime investigation pioneers.

TABLE I
ORGANIZED CYBERCRIME ACTIVITIES

Year	Group Name	Actor	Behavior Type	Activity
1993~2001	DrinkOrDie (DoD)	Non-state	An international group of copyright pirates	Illegally reproduced and distributed software, games, and movies over the Internet.
1996~1998	The Wonderland Club		A members-only group	Exchanged illicit images of children.
2003~	Anonymous		A decentralized group of activist and hacktivist entities.	Focus on website defacements, distributed denial of service attacks, and prominent symbols
2006~2008	Dark Market		A forum for the exchange of stolen credit card and banking details, and malicious software.	Take advantage of the criminal opportunities presented by the advent of electronic banking and the increasing use of credit and debit cards.
2006~2010	PLA Unit 61398	State	A large-scale program of industrial espionage	Acquire a massive volume of data from a wide variety of industries in English-speaking countries.
	Shady RAT		An ongoing series of cyber-attacks	Hit at least 71 organizations
	Aurora		A series of cyber-attacks	Aim at dozens of other organizations
	GhostNet		A cyber espionage operation	Operate from commercial Internet accounts in China.
2007~2013	PRISM		A systematic harvesting program of digital information by the US National Security Agency (NSA).	Capture and store a wide range of Internet data on the following prominent IT companies: Microsoft, Google, Yahoo!, Facebook, Pal Talk, YouTube, Skype, AOL, and Apple.
2009~	Lazarus, Guardians of Peace, or Whois Team		Compromised several banks and Fintech companies.	Be famous for Operation Troy, Ten Days of Rain, Sony breach, Operation Blockbuster, WannaCry, cryptocurrency attacks
2010~	Operation Olympic Games		A collaboration between the US National Security Agency and its Israeli counterpart, Unit 8200.	Disrupt the Iranian nuclear enrichment program.
	Stuxnet		A malicious computer worm is believed to be a jointly built American-Israeli cyberweapon.	Involve the clandestine insertion of a complex and sophisticated set of software into communications and control systems at the Natanz nuclear facility.
2010~2012	Ukrainian Zeus	Non-state	Software engineers in Eastern Europe	Gain access to the computers of individuals employed in a variety of small businesses, municipalities, and non-government organizations in the United States.
2016~	MoneyTaker		Stole millions from U.S. & Russian Banks	Target Banks, financial institutions, and legal firms in the United States, UK, and Russia.

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

B. The Shadowy Criminal Group on ATM Threats

Cyber threats are still profitable for cybercrime groups and sponsored groups, who may attack bank systems for financial profits or political reasons. Cyber risks and their follow-up losses are becoming increasingly international across the world [7]. Cybercrime investigation of these cyber threats through hacker tools, techniques, and procedures is critical for LEAs to protect users and reduce fraud risk.

Some of the most notable malware families are ZeuS (its successor Carberp) and Carberp (its successor Carbanak). The criminal's pragmatic approach starts a new chapter in the cybercrime ecosystem [14]. In this era of increasing cyber-attacks, many different malware families are programmed, especially for the majority of internet banking fraud through malware. Bank heists are attracting large-scale hackers with its unlimited borders, as cybercrime against financial banks turns out to be an increasingly convenient way to withdraw big money. This study focused on the Carberp malware, and it showed there was a grey area between APT and malware. There are a variety of shadowy criminal groups that focus on banks and payment providers. The shadowy criminal group members began actively taking an interest in retail organizations or bank payment systems. Hackers hacked up to $1 billion from more than 100 banks in 30 countries. ATM hacking is becoming a new trend for an organized cybercrime group. There are a particular tutorial, tricks, and techniques online about ATM devices hacking like Diebold, Defcon, or Wincor Nixdorf [14, 19]. It is not easy to cheat an ATM computer. If cybercrime targets financial services, it requires advanced hacking capability. Profit or money is always an initial motivation for criminals, who have targeted ATMs to withdraw cash even without the need for a card.

An organized group of criminals from Russia and Ukraine has broken into internal networks at dozens of commercial banks and installed malware that allowed the group to drain bank ATMs of cash. The ATM malware family in Latin America, Europe, and Asia are identified as 'Carberp,' 'Qadars,' 'Ploutus,' 'Tyupkin,' 'Anunak,' or 'Carbanak' during the period from 2009 to 2015 in Table II [19]. This malware has evolved and has added functionality beyond banking credential theft. The details of each malware are somewhat different. The stealthy APT methods used by the attackers in these heists would work across a broad range of commercial banks one by one. This group specializes in hacking into banks directly and then working out ingenious ways to funnel cash directly from the financial institution itself. Since 2009, researchers have warned that hackers were developing malicious software for ATMs [14]. The online banking malware of the Carberp program is reported to have impacted hundreds of financial institutions around the world since 2009. In addition to its malicious capabilities, the Carberp malware family uses a combination of evasion techniques from the Zeus malware, and the invisible persistence feature from other viruses, worms, Trojans, or botnets. Hackers can resort to open source codes to achieve their goals [13, 19]. Since 2012 several ATM heists of this type were reportedly carried out in Russia, Europe, and the USA. It appeared to be attacked by organized crime gangs, and the compromised ATMs were reprogrammed to dispense cash using malware. Ìn 2015, an international organized crime ring had stolen up to US$1 billion from more than 100 banks in 30 nations [19]. Hackers may exploit security flaws in specific ATMs, and cause the compromised machines to spew a flurry of bills on stage. Table III illustrates the behavioral comparison of the ATM malware family. These three cases were all arrested by LEAs.

TABLE II
THE FUNCTIONAL COMPARISON OF ATM MALWARE FAMILY

Malware Family	Carberp	Qadars	Ploutus	Tyupkin	Anunak	Carbanak
Identified Companies	Federal Office for Information Security, BSI and Trend Micro	Symantec, Microsoft, and Sophos	Symantec, Microsoft, and SafenSoft	Symantec, Kaspersky	Group-IB and Fox-IT	Kaspersky
Finding Time	2009	May 2013	August 2013	March 2014	December 2014	2015
Victim Location	Russian	Netherlands, France, Canada, India, Australia, and Italy	Mexico	Eastern Europe, the U.S., India, China, Russia, Israel, France, and Malaysia.	Eastern Europe, the U.S.	Russia, the United States, Germany, China, and Ukraine

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

TABLE III
THE BEHAVIORAL ATTRIBUTE COMPARISON OF ATM MALWARE FAMILY

Category	Case	1	2	3
Who	An organized criminal group name	Carberp, Pawn Storm or APT28	Unlimited Operations	Russian Mafia
	Suspect numbers	8	8	19
	Arrest by	Russia	USA	Taiwan
	Arrested suspects name (from Newspaper)	Germes and Arashi (Alias)	Elvis Rafael Rodriguez, Emir Yasser Yeje, and Alberto Yusi Lajud-Peña	Andrejs Peregudovs, Mihail Colibaba, and Nikolay Penkov
What	USD theft in an ATM looting	$1 Billion	$45 Million	$2.6 Million (NT$83.27 Million)
When	From plan to ATM heist	2009 ~ February 2015	December 2012 and February 2013	July 2016
	Arrest date	March 2012	May 2013	July 2016
Where	ATM location	Moscow in Russia	New York in the USA (More than 24 countries)	Taipei City, New Taipei City, and Taichung in Taiwan
How	Money from	the financial institution	Prepaid Debit Accounts	the financial institution itself

III. SAMPLE CASE: TAIWAN ATM HEIST

In recent years there has been a tremendous increase in organized crimes. Banks in many countries are becoming new targets of several independent cybercrime groups. Traditional organization crimes have a hierarchical top-down command-and-control structure, but cybercrime groups tend to involve a loose network or even a peer-to-peer decentralized structure [1]. The group operated in closed cells, and the suspects did not know each other involved in the ATM heist [14]. These attacks rely upon both highly sophisticated hackers and criminal cells whose role is to withdraw the cash as quickly as possible. The crime chain is the series of steps cybercriminals go through to transform its ATM invasion into something of higher value. They make their output worth more than the sum of its inputs.

A. Specific Questions in Taiwan ATM Heist

The ATM transactions in the USA's Unlimited Operations require only general bank card information to effect payment, such as the bank card number, and PIN code [19]. However, Taiwan's Russian Mafia Group in July 2016 further compromises the ATM systems and criminals can withdraw money without any bank card information. The ATM heist of Taiwan First bank is based on a well-known Carberp malware family, which is available for sharing, sale or cooperation on such markets. Investigators seek to explore cyber-attacks. The arrest was made after police officers spent many sleepless nights watching surveillance videos and checking hotel registries in Taiwan. Putting relevant data all together becomes essential to support or refute a cybercrime. The questions go along the lines of whom, who, how, and why [13, 20, 23]. Without understanding these root causes, it would be difficult to use evidence from multiple independent sources, develop a strong association between a criminal and an event, and explore the incident under control.

1) Who Are Victims?

The ATM attack in Taiwan targeted the First Bank's network. The ATM heist occurred between July 9 and 10 2016, when members of ATM heist gangs stole over USD 2 million from 41 ATMs in Taipei, New Taipei and Taichung using malware to hack into the computer system [15]. The Wincor Nixdorf ATM framework was targeted. They use malicious software and defy the bank effort to strengthen the security controls of ATM fleets. That case has demonstrated that bank systems lack adequate security measures to stop cybercrimes.

2) Who Are Cybercriminals?

Three cybercriminals were arrested on July 17, 2016, and each was sentenced to prison terms of 12 years. The 19 escaped cybercriminals have been put on a wanted list, and a total of 22 cybercriminals from six countries were involved [15].

3) How Did Hackers Do?

The heist was committed without using cards, but the ATMs spat out bills. LEAs have identified some patterns to trigger withdrawals. As a result of access to internal bank networks, hackers also gained access to ATM systems, infected these computers with their specific malware, and launched the fraud command from London, UK. The dispensing of the cash could have been triggered by a mobile phone, a laptop, or a hacked private bank computer. The cybercriminals use Whatsapp and other Internet-based communication methods to communicate internally and with other criminal cells [15]. They used an old spying technique of dead drops and modern technology to move the stolen money around. A dead drop is a method of espionage tradecraft used to pass items or information without meeting each other directly. Another method of a live drop is used when two persons meet to exchange items or information.

4) Why Did this Attack Happen?

Organized criminals can rent hackers to conduct attacks or hire mediators to handle the sale of stolen information. Cybercrime as a service (CAAS) increases when the ATM malware is sold to the highest bidders. Criminals no longer need to rely on their knowledge, abilities, and abilities to carry out exploits, build threats, and launch attacks. This ATM malware is sold only to selected people. Most of the infections are from a different group and share the command and control (C&C) servers [13]. The profit attracts hackers by running vulnerable services. Cybercriminals try to maximize their

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

financial gain while minimizing their risk [2].

B. Behavioral Attributes of ATM Malware Family

In several historical data breaches, hackers have exploited security flaws in specific ATMs, and cause the compromised machines to spew a flurry of bills on stage. The behavioral comparison of the ATM malware family is listed in Table IV [13, 19]. Their local LEAs arrested these three cases. In March 2012, the 8-member arrest of Department K group in Moscow by the Russia Ministry of Internal Affairs (Министерство внутренних дел) was a great example of international collaboration between both private industry research and international law enforcement (see the case 1 in Table IV). A lack of awareness of cybersecurity may enhance the vulnerability in the public or private sectors. Their differences are likely due to the type of cybercrime victimization, the effectiveness of cybersecurity measures, or the extent of online banking services. Unlike the traditional forms of crime, cybercrimes can act without leaving a fingerprint for their actions. Not only the Internet but also commercial bank systems are facing increasing physical and virtual risks [17].

TABLE IV
THE BEHAVIORAL ATTRIBUTE COMPARISON OF ATM MALWARE FAMILY

Category		1	2	3
Case	An organized criminal group name	Carberp, Pawn Storm or APT28	Unlimited Operations	Russian Mafia
	Arrest by	Russia	USA	Taiwan
	Arrest date	March 2012	May 2013	July 2016
Physical	Criminals under arrest	V	V	V
	Shadowy criminal group	V	V	V
	Assistance from other countries' LEAs		V	
	On-premises to withdraw cash	V	V	V
Virtual	32-bit Windows ATM platforms	V	V	V
	Through the ATM's pin pad		V	
	No user account required	V	V	V
	On-Premises to install the malware		V	
	Avoiding detection	V	V	V

Note: 'V' means match.

1) Access Controls

The ATM operation is continuing to become more complex, challenging, and costly. Most ATMs are still running Windows XP, which is first released on October 2001. When Microsoft has ended support for Windows XP, most ATM manufacturers continued to use this version [19]. The old system often opens security holes for hackers. There will be a persistent increase in ATM robbery around the world. The access controls of ATM theft still leave much to be desired. They are networked devices that have many potential weaknesses if not carefully configured, updated, and physically secured. It is vital to improving the security controls within banks. Although security controls can never be perfect for implementing and expensive to deploy, it remains of critical importance for security measures to be continually managed, reviewed, and improved. Insufficient budget can never be used as the reason for not taking action [21]. The default setting for any users is no or limited access. If nothing has been correctly configured for an individual or the groups, users should not be able to access that resource. Banks should enforce strict access criteria, and pay more attention to limiting and monitoring the usage of administrator and other privileged accounts.

ATMs need remote access to communicate with bank data, so network attacks are also a possibility [14]. A trade-off between convenience and security lies in wireless communication over the public Internet or dedicated connections. If convenience increases, security must decrease. The availability of access to bank ATMs from internal network segments opens excellent opportunities for hackers. Security holes or mistakes of a system configuration in the internal bank network left sensitive databases exposed to hackers. The strategy should remove or limit the remote access for ATMs.

2) Physical Process

a) Criminals under Arrest

Three organized criminal groups were arrested in Russia, USA, and Taiwan. They were involved in large scale ATM jackpotting. Their methods of operation were similar to each other.

b) Shadowy Criminal Group

The group allegedly used a piece of malware, pilfered cash from ATMs, and made millions by infecting ATMs across the world.

c) Assistance from other Countries' LEAs

It is difficult for any country to expand its power to other countries. The cybercrime arrest needs assistance from other LEAs. Arrests often take years because the cybercriminals were located in countries where the local authorities would not arrest them.

d) On-Premises to Withdraw Cash

LEAs can theoretically catch criminals in the act with security cameras since they must be on-premises to withdraw cash. However, it is difficult to obtain relevant evidence and differentiate a criminal and a regular customer.

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

3) Virtual Process

a) 32-bit Windows ATM Platforms

ATM malware worked on ATMs that run Windows 32-bit operating systems.

b) Through the ATM's Pin Pad

With the help of ATM malware, cybercriminals were able to empty the infected ATM cash cassettes by issuing commands through the ATM's pin pad.

c) No User Account Required

The malware allows its operators to withdraw cash from ATMs without the requirement of any payment card.

d) On-Premises to Install the Malware

Cybercriminals started by unlocking an ATM's enclosure and infected the computer with a piece of malware. Days later, they returned to the computer and dispensed from the ATM without the need for user account verification.

e) Avoiding Detection

The ATM malware kept the exploit hidden most of the time and had several features that helped it avoid detection [13]:

- It was only active at specific times of the night on certain days of the week.
- ATM malware implements anti-debug and anti-emulation techniques
- The malware could disable the anti-virus system from the infected system.

IV. Comprehending Taiwan ATM Heist: from Cyber-attack Phases to Investigation Processes

A. Embedding Cyber-attack Phases into the ATM Heist Investigation

According to public reports surrounding the incident investigation of Taiwan ATM heist, criminals deleted traces of the cyber-attack to prevent from detecting irregularities in the ATM behavior. Some malware behaviors and file names have been identified from the cyber-attack phases [14, 15, 19, 24].

1) Reconnaissance and Footprinting

In this phase of reconnaissance and footprinting, criminals gather information about computer systems, reveal system vulnerabilities, and find ways to intrude into the cyberspace [18]. Most exploits are dependent on operating systems, applications, ports, or services. Hackers may perform reconnaissance for about 2 to 3 times to gather a big-picture view of a network or servers before they attempt an exploit. It identifies the IP addresses, open ports, running services, and operating systems in the target network [22, 24]. Footprinting identifies the operating system, service pack or patches of the target, gathers the maximum information about the computer system or a network, evaluates the security of any IT infrastructure, and determines the follow-up attack path. It is used to get detail information on a specific target. For example, if a server is listening on port 80, it is running the HTTP protocol and is very likely a web server. It is often used as part of a more significant reconnaissance attack. Increased access to the Internet has enabled cybercriminals to perform reconnaissance on their targets. Cnginfo.exe and cnginfo_new.exe can read the information inside the ATM in the phase of reconnaissance and footprinting.

2) Scanning or Enumeration

In this phase of scanning and enumeration, hackers gather in-depth information on the victims. Enumeration often occurs after scanning [17]. The more hackers know in advance, the fewer surprises they will have. They run scanning activities to infer vulnerabilities on the Internet. Once a computer is found vulnerable, they attempt to control or infect that computer based on the inferred vulnerability. Running a ping sweep or a network mapper can explore what systems are on the network. Running a vulnerability scanner can also determine which ports may be open on a particular system. Enumeration refers to actively connecting to a target system, and identifies usernames, computer names, network resources, shares, and services. It also refers to actively connecting to a target system to acquire this information. Once a vulnerability is identified, a cyber-attack is relatively easy to disguise. There is no clear evidence from criminals' scanning or enumeration. These activities can be found from the target's firewall log files. Auditing logs can be monitored to detect threatening incidents promptly. By monitoring logs of digital evidence, LEAs can look for the triggers or something suspicious.

3) Gaining Access

In the phase of gaining access, these attacks can access insecure access [18]. Hackers can gain access to the system, crack a password, and escalate privileges. The hackers initially compromised a vulnerable telephone recording computer used by the targeted bank in order to establish network access. Cngdisp.exe and cngdisp_new.exe potentially contain more robust capabilities than cngdisp.exe, executed the function of dispensing bills in the phase of gaining access.

4) Maintaining Access

Gaining access to a connection does not mean hackers can access everything. The objective of maintaining access is to ensure that hackers can have long-term access. Hackers used this network access to move laterally within the targeted bank's network and subsequently gained access to deliver software updates across the network. They use the update service to send malware to the target ATMs. The malware masqueraded as a software update. They utilized the remote commands to empty the cash-carrying cassettes in the infected ATMs. There was no action required at the ATM except the collection of the money.

5) Covering Tracks

In the final phase of covering tracks, hackers attempt to conceal their trails, manipulate the event logs, and avoid detection by the system administrator or LEAs. Log files contain information about every computer activity. Hackers may try their best in hiding or obscuring the applications they leave behind. That leads hackers into paying attention to log files. Covering tracks consists of removing or altering log files, hiding files with unclear attributes, or using tunneling

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

protocols to communicate with the information system [18]. Hackers need to evade detection, erase evidence of a compromised computer, and remove the portions of logs that can reveal their presence. A significant amount of malware deploys various anti-forensics tricks in an attempt to make the analysis more difficult. In the final phase of the cyber-attack, the criminals deleted (sdelete.exe) components of the malware employed in the ATM heist. Sdelete.exe and batch file cleanup.bat deleted the other programs in the phase of covering tracks [15].

B. Detecting ATM Heist Using ISO/IEC 27043:2015 Incident Investigation Processes Classes

The regulation of cyberspace law often lags behind technological development in cybercrime. Hackers will try their best to hide their identity and reduce their chances of detection across jurisdictional broader. A threat determines the risk, but for each risk, LEAs can determine the following countermeasures. The cybercrime investigation processes in ISO/IEC 27043:2015 are purposely designed at an abstract level for different types of cybercrimes [11]. In Table V, the cybercrime investigation processes in cyber-attack scenarios from LEAs' perspective can be further discussed and analyzed into the following processes classes: Readiness, Initialization, Acquisitive, Investigative, and Concurrent.

TABLE V
CYBERCRIME INVESTIGATION FROM ISO/IEC 27043:2015

Processes Class	People	Process/Activities	Technology
Readiness	System administrators	Pre-incident investigation/ plan and prepare	ICT Governance
Initialization	First responders	Cybercrime investigation/ respond	Live forensics
Acquisitive	Lab analysts	Physical investigation/ identify, collect, acquire, and preserve	Dead forensics
Investigative	LEAs	Event reconstruction/ understand, report and close	Digital forensic analysis
Concurrent	Obtaining Authorization Process, Documentation Process, Managing Information Flow Process, Preserving Chain of Custody Process, Preserving Digital Evidence Process, and Interaction with Physical Investigation Process		

1) Readiness Processes Class: Prepare the ICT Governance from System Administrators

The first class of readiness processes is prepared in advance for an investigation. Investigators can plan incident detection, identify potential digital evidence sources, analyze digital data, and explore the truth in a legally proper way. This class deals with pre-incident investigation processes and ensures that incident detection systems are in place [5]. Deploying a digital forensic readiness program can favorably impact LEAs by maximizing the potential of digital evidence and minimizing the time and costs of an investigation [11]. The investigators of data breaches can initiate some plans for taking the actions, reinforces a direct relationship between cybercrime investigation and fact-finding. Cybercrime prevention requires the participation of Internet users, the system administers, or enterprises to maintain personal or commercial data. The whole society should be encouraged to participate more fully and effectively in cybercrime prevention in order to provide for a harmonious online world [21]. A supplementary strategy is intended to achieve the goal of information security. This method can assist banks or LEAs in dealing with today's ever-increasing ATM heist.

2) Initialization Processes Class: Initiate the Live Forensics from First Responders

The second class of initialization processes deals with uncovering the potential digital evidence and searching for traces of digital evidence in a legal process. It includes incident detection, first response, and preparation [11]. The implementation of cybercrime investigation procedures includes the responsibilities for establishing a direction for its execution. The identification of appropriate best practices should develop a cybercrime investigation strategy, implement risk management, and meet the need for an investigation with acceptable efforts. There is an opportunity to actively collect potential evidence in the form of log files or network traffic records in a forensically sound manner. Live forensics primarily targets volatile data from a running system. Ignoring the volatile data of computer memory is impossible in collecting digital evidence. It can be the first step toward an incident response scenario. Live forensics can analyze volatile data, system running processes, cached processes, network connections, and opened ports without shutting down a system. Practitioners can directly make contact with the suspect and ask what has happened. Investigators can locate, extract, and analyze data from digital devices, which LEAs interpret to serve as legal evidence [16].

3) Acquisitive Processes Class: Perform the Dead Forensics from Lab Analysts

The third class of acquisitive processes deals with the physical investigation of a case where potential digital evidence is identified and handled. It includes identification, acquisition, transportation, and storage in potential digital evidence [11]. In dead forensics, practitioners can conveniently minimize system modification when working with a copy of a write-protected drive at laboratories. An examination of the computer is conducted systematically to ensure the admissibility of the evidence. The investigator should achieve continual improvement of the cybercrime investigation and take reactive activities based on the results of the case reviews or other relevant information. The investigation procedure will continue to evolve together with the requirement to incorporate new evidence and associated knowledge. LEAs have actively gathered evidence to support a legal defense [23].

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

4) Investigative Processes Class: Conduct the Digital Forensic Analysis from LEAs

The fourth and last class of investigative processes develops a likely sequence of events. It includes investigating the incident, analyzing the evidence, interpreting results from the analysis, and reporting on results of the digital evidence. Investigators can examine the pieces of evidence to measure performance against the determined objectives and report the results to the appropriate recipients for review. A singular strategy can not resolve the majority of cybercrime challenges. Technical minds alone cannot solve the issue of prosecuting cybercriminals. Given limited time and resources, it is essential to maximally leverage knowledge, capabilities, and investments in a range of public-private partnerships to improve foundations of trust and enhance agility and resilience.

5) Concurrent Processes Class: Take Place in Company with these Processes Classes

The following concurrent processes class takes place in company with the former processes classes [5, 11, 20].

a) Obtaining Authorization Process

Having authorization from the appropriate authorities makes sure that the appropriate countermeasures are ready to solve it.

b) Documentation Process

Investigators must maintain documentation of digital evidence from the beginning of the e-discovery process until the end.

c) Managing Information Flow Process

Information flow could describe the use of trusted PKI and time stamping to identify the exchange of digital evidence between each of the processes in the same investigation.

d) Preserving Chain of Custody Process

The documentation comprises the chain of custody form and records relating to the evidence analysis.

e) Preserving Digital Evidence Process

In order to preserve the integrity of the digital evidence, investigators should guarantee that the original evidence is not changed.

f) Interaction with Physical Investigation Process

There are some complex interactions with the physical investigation according to the digital investigator's needs and fast adaption to changing boundaries, scope, or investigation objectives. All of the complexities must be simplified to ensure an efficient investigation.

V. *CONCLUSIONS*

ICT innovations are not only set to bring enormous benefits to the general public, but also bring new technological risks to individuals and businesses. Cybercrimes have rapidly evolved for the dissemination of malware. Criminals increasingly use sophisticated tools and methods to commit their cybercrimes. Major information systems of modern society are under the burgeoning attack. Cybersecurity for banking or financial institutions becomes a vital business enabler to enhance customer confidence and bring in more business. It is vital to leverage investments in a range of societies to assure societal services. The ATM withdrawals happened so quickly that none of the commercial banks involved noticed in time to stop the perpetrators. ATM technologies are evolving fast and making payments more convenient. Organizations need a balance between security and functionality in information security. This study outlines a set of profiling cybercrime investigation that aims to identify digital pieces of evidence in the face of increased complexity and vulnerability in hacking activities. It is our sincere hope to bring the technical details to the attention of information security specialists and to minimize risks by preventing information security incidents. A small sacrifice inconvenience can be useful to prevent an attack on the ATM's door. ICT governance should be employed by banks to heist ATM money with more barriers.

REFERENCES

[1] Ablon, L., Libicki, M. C., and Golay, A. A. *Markets for Cybercrime Tools and Stolen Data Hackers' Bazaar*, Rand Corporation, pp. 3-28, 2014.

[2] Akhgar, B., Staniforth, A., and Bosco, F., *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Elsevier Publishing, pp. 88-90, 2014.

[3] Bates, A. and Hassan, W. U., "Can Data Provenance Put an End to the Data Breach? " *IEEE Security & Privacy*, Vol. 17, No. 4, pp. 88-93, July-Aug. 2019.

[4] Bernik, I., *Cybercrime and Cyberwarfare*, John Wiley & Sons Inc., pp. 1-57, 2014.

[5] Brooks, C. L., *CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide (1st Edition)*, McGraw-Hill Education, pp. 13-50, 2015.

[6] Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd Edition)*, Elsevier Inc., pp. 187-306, 2011.

[7] Coburn, A.W., Daffron, J., Smith, A., Bordeau, J., Leverett, É., Sweeney, S., and Harvey, T., "Cyber Risk Outlook 2018, " Centre for Risk Studies, University of Cambridge and Risk Management Solutions, Inc., pp. 2-25, 2018.

[8] Europol and European Cybercrime Center, "Internet Organised Crime Threat Assessment (IOCTA) 2018, " European Union Agency for Law Enforcement Cooperation, pp. 14-65, 2018.

[9] Graves, M. W., *Digital Archaeology: The Art and Science of Digital Forensics*, Addison-Wesley, pp. 91-110, 2014.

[10] Impagliazzo, J. and McGettrick, *A., Information Systems: What Every Business Student Needs to Know*, NW: Taylor & Francis Group, 2016.

[11] International Organization for Standardization (ISO), "ISO/IEC 27043:2015 Information Technology - Security Techniques - Incident Investigation Principles and Processes," ISO Office, 2015.

[12] Jewkes, Y, and Yar, M., *Handbook of Internet crime*, Willan Publishing, pp. 173-193, 2009.

[13] Kao, D. Y., "Exploring the Cybercrime Investigation Framework of ATM Heist from ISO/IEC 27043:2015, " IEEE ICACT 2017 (19th International Conference on Advanced Communications Technology), Pyeong Chaung, South Korea, 2017.

[14] Kao, D. Y., "ATM Heist Threats: a Proposed ICT Governance Strategy," IEEE ICACT 2019 (21th International Conference on Advanced Communications Technology), Pyeong Chaung, South Korea, pp. 610 - 615, 2019.

[15] Law and Regulations Retrieving System, "Criminal Appeals No. 593/106 in Taiwan High Court," Judicial Yuan, May 18, 2017.

[16] Marcella, A. J., Menendez, D., *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes (2nd Edition)*, Auerbach Publications, pp. 1-26, 2008.

[17] Mehan, J. E., *Cyberterror, Cybercrime, and Cyberactivism: An In-Depth Guide to the Role of Security Standards in the Cybersecurity Environment (2nd Edition)*, IT Governance Publishing, pp. 25-58, 2014.

[18] Oriyano, S. P., *CEH v9: Certified Ethical Hacker Version 9 Study Guide (3rd Edition)*, John Wiley & Sons, Inc., pp. 1-222, 2016.

[19] Sancho, D., Huq, N., and Michenzi, M., "Cashing in on ATM Malware: A Comprehensive Look at Various Attack Types," Trend

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Micro Forward-Looking Threat Research (FTR) Team and Europol's European Cybercrime Centre (EC3), 2017.
[20] Shipley, T. G. and Bowker, A., *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Elsevier Inc., pp. 21-38, 2014.
[21] Smith, R. G., Cheung, R. C. C., and Lau, L. Y.C., *Cybercrime Risks and Responses Eastern and Western Perspectives*, Macmillan Publishers Limited, pp. 67-211, 2015.
[22] Spitzner, L., *Honeypots Tracking Hackers*, Addison-Wesley, pp. 8-20, 2002.
[23] Stephenson, P., *Official (ISC)²® Guide to the CCFP CBK*, Auerbach Publications, pp. 293-404, 2014.
[24] Walker, M., *CEH Certified Ethical Hacker All-in-One Exam Guide (2nd Edition)*, Graw-Hill Education, pp. 35-198, 2014.

Da-Yu Kao received the B.S. and M.S. degree in Information Management from Central Police University, Taiwan, in 1993 and 2001, the Ph.D. degrees in Crime Prevention and Correction from Central Police University, Taiwan, in 2009, respectively. From 1993 to 1996, he was with Taipei City Police Department, Taiwan, where he was an information technology police officer involved in the development of policing information systems. From 1996 to 2007, he was with Criminal Investigation Bureau, National Police Administration, Taiwan, where he was a detective and forensic police officer in cybercrime investigation and digital forensics. From 2007 to 2013, he was with Maritime Patrol Directorate General, Coast Guard Administration, Taiwan, where he was an information technology section chief in the department of information and communication. Since 2013, he has been with Central Police University, Taiwan, where he is currently an associate professor in the Department of Information Management. His research interests include cybercrime investigation, digital forensics, digital evidence, information management, criminal profiling, and cyber criminology.

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

A High-Performance Parallel Hardware Architecture of SHA-256 Hash in ASIC

Ruizhen Wu*, Xiaoyong Zhang**, Mingming Wang*, Lin Wang*

*Inspur Electronic Information Industry Co.,Ltd, Xi'an Shaanxi Province China

**Biren Technology Ltd, Shanghai China

wuruizhen@inspur.com, xyz8070@126.com, wangmingming02@inspur.com, wanglinlc@inspur.com

***Abstract*—The SHA-256 algorithm is used to ensure the integrity and authenticity of data in order to achieve a good security thus is playing an important role in various applications, such as e-transactions and bitcoins. The SHA-256 computation capacity is a main research direction of Hashing Algorithm. In order to improve the computation capacity of hardware, the proposed design first uses pipeline principle and circuitry of timing prediction to find a most efficient architecture for implementation. Then it is optimized with hash function and hardware characteristics to give a high-performance hardware architecture of SHA-256 hash. Three pipelines are used to replace the critical path in the round functions which can shorten the timing path, and divide the computation chain into independent steps. Multi-computation of SHA-256 is working in parallel pipelines, indicating that the computation capacity can be 3 times of that with standard SHA-256 implementation. The proposed SHA-256 hardware architecture has been implemented and synthesized with Intel 14nm technology. Simulation and synthesis results show the proposed SHA-256 hashing throughput can be improved by 3 times with 50.7% power reduction, at an area cost of 2.9 times compared to that of the standard implementation.**

***Keyword*—Application specific integrated circuits, Cryptography, High-speed integrated circuits, Low-power electronics**

I. INTRODUCTION

SECURE hashing algorithm is used to ensure the data integrity and authenticity while being stored and transferred. Hash functions take input data of arbitrary length and convert them into some fixed data, called hash value or message digest. The SHA-256 of hashing algorithm is playing an important role in various applications. Almost all e-transactions, high-throughput designs of security schemes are needed. Bitcoin is a new and popular use of SHA-256, as the POW ("Proof of Work" [1]) mentions in the Bitcoin protocol: the POW requests a huge number of SHA-256 computations to find a proper 32-bit number to satisfy the protocol requirement. The first finder is awarded by bitcoin, which means the computation capacity of SHA-256 is the key factor to get awarded, therefor the main research direction.

The SHA-256 hash architecture acts more and more important nowadays thus several improved designs are proposed. To embed a security engine in a RFID tag, two compact SHA-256 implementation are presented, a low area design and a low power design [2]. To achieve the improvement several adder cycles and adder selectors were added in the round computation which made it very suitable for power-area balanced applications.

One application of ideas and techniques from functional languages to the model-driven design and synthesis of hardware artifacts for SHA-256 was proposed in [3]. The co-design of hardware and software not just made the SHA-256 algorithm easier to implement, but also gave a more effective way to optimize the performance of SHA-256 from software to hardware based on designer's need.

However the most challenging request of SHA-256 is high processing speed and low power in hardware. An optimized pipelined architecture of SHA-256 hash function has been implemented in [4] which used custom data path that enforces the reuse of modules based on which novel processor architecture was implemented. Reference [5] proposed a SHA-256 unfolding design based on reconfigurable hardware modules. The complex linear computing of SHA-256 was reconfigured by newly added computation modules. Reference [6] implemented SHA-256 architecture based on operation rescheduling to minimize the critical path delay. Reference [7] proposed a more effective hardware to control the SHA-256 computation, which was using the finite state machine (FSM).

The purpose of this paper is to provide a high

Manuscript received Jan. 10, 2019. This work is a follow-up of the invited journal to the accepted & presented paper of the 21th International Conference on Advanced Communication Technology (ICACT2019), and Grant ID is ICACT-20190011.

Ruizhen Wu is with the Inspur Electronic Information Industry Co.,Ltd, Xi'an, Shaanxi 710071 China. (Phone: +86 15909206044; e-mail: wuruizhen@inspur.com).

Xiaoyong Zhang is with the Biren Technology Ltd, Shanghai 201210 China. (E-mail: xyz8070@126.com).

Mingming Wang is with the Inspur Electronic Information Industry Co., Ltd, Xi'an, Shaanxi 710071 China. (E-mail: wangmingming02@inspur.com).

Lin Wang is with the Inspur Electronic Information Industry Co.,Ltd, Xi'an, Shaanxi 710071 China. (E-mail: wanglinlc@inspur.com).

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

performance parallel computation hardware architecture in ASIC of SHA-256 hash. The organization of this paper is: Section 2 describes the classic SHA-256 algorithm; Section 3 uses the pipeline principle and circuitry timing prediction to find the most efficient pipeline architecture for SHA-256. Section 4 presents the proposed SHA-256 parallel computation hardware architecture with 3 pipelines. The implementation results and comparison with other designs are in Section 5. The last section provides the conclusions.

II. SHA-256 ALGORITHM

This section describes the function of SHA-256 hash. A detailed description of the SHA-256 hashing algorithm can be found in the official NIST standard [8]. The SHA-256 computation can be divided into 2 steps. The first step is to pre-process the original messages. It involves message padding and expanding the message for the round computation. The padding means appending bits according to some rules until the total length is integer of 512-bit. Afterwards every 512-bit will be expanded to 64*32 bit for SHA-256 round computation.

Here we use "t" to indicate the number of transformation rounds.

When 0≤t≤15: $W_t = input\ message$

When 16≤t≤63:

$$W_t = \sigma_1^{\{256\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{256\}}(W_{t-15}) + W_{t-16} \quad (1)$$

The first 16 W_t are input messages. And after that the others are from iterative operation. In equation (1) the σ is calculated by:

$$\sigma_0^{\{256\}}(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x) \quad (2)$$

$$\sigma_1^{\{256\}}(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x) \quad (3)$$

In (2) and (3), the $ROTR^n(x)$ means a right rotation of x by n bits, and $SHR^n(x)$ means shift right of x by n bits.

The whole SHA-256 computation is showed in Fig. 1.

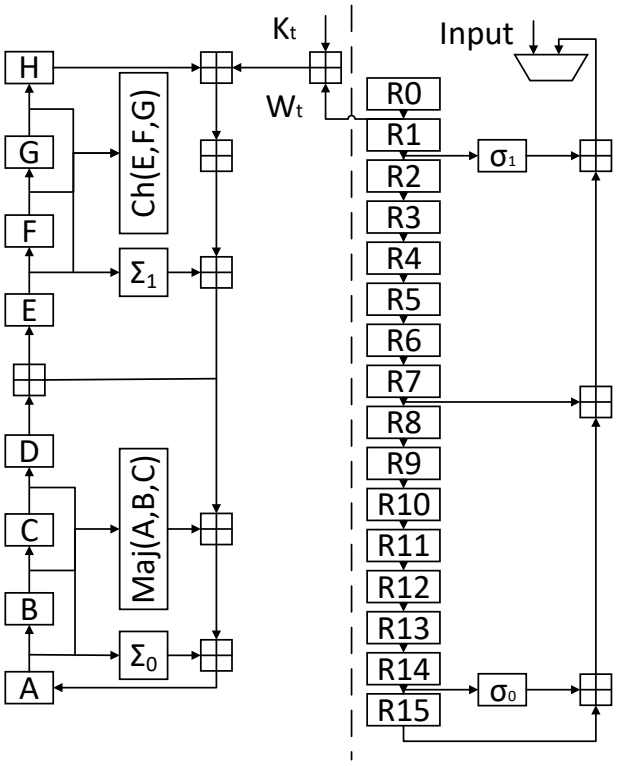

Fig. 1. SHA-256 hashing algorithm

The second step is called round computation shown in left part of dotted line in Fig. 1 is to obtain the "a"~ "h", which can be calculated by:

$$T_1 = h + \sum_1^{\{256\}}(e) + ch(e,f,g) + K_1^{\{256\}} + W_1 \quad (4)$$

$$T_2 = \sum_0^{\{256\}}(a) + Maj(a,b,c) \quad (5)$$

$$h = g \quad (6)$$

$$g = f \quad (7)$$

$$f = e \quad (8)$$

$$e = d + T_1 \quad (9)$$

$$d = c \quad (10)$$

$$c = b \quad (11)$$

$$b = a \quad (12)$$

$$a = T_1 + T_2 \quad (13)$$

The first round of a, b, c, d, e, f, g and h are assigned by the initial value of SHA-256 definition. The K_t is a constant in 32-bit and 64 values overall. And the four function computations are showed in (14)-(17):

$$Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge y) \quad (14)$$

$$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \quad (15)$$

$$\sum_0^{\{256\}}(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x) \quad (16)$$

$$\sum_1^{\{256\}}(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x) \quad (17)$$

The $\oplus$ represent bitwise XOR operation, the $\wedge$ represent bitwise AND operation and the $\neg$ bitwise complement operation.

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Each round of (6)-(13) can generate 8 hash values, they were showed in the right part of Fig. 1 and calculated by:

$$H_0^{(i)} = a + H_0^{(i-1)} \quad (18)$$

$$H_1^{(i)} = b + H_1^{(i-1)} \quad (19)$$

$$H_2^{(i)} = c + H_2^{(i-1)} \quad (20)$$

$$H_3^{(i)} = d + H_3^{(i-1)} \quad (21)$$

$$H_4^{(i)} = e + H_4^{(i-1)} \quad (22)$$

$$H_5^{(i)} = f + H_5^{(i-1)} \quad (23)$$

$$H_6^{(i)} = g + H_6^{(i-1)} \quad (24)$$

$$H_7^{(i)} = h + H_7^{(i-1)} \quad (25)$$

The final output is obtained by the 64th round hash value as below:

$$output = H_0 \,\|\, H_1 \,\|\, H_2 \,\|\, H_3 \,\|\, H_4 \,\|\, H_5 \,\|\, H_6 \,\|\, H_7 \quad (26)$$

III. PIPELINE ARCHITECTURE

It is clear from [4]-[7] that to achieve high processing speed and low power in hardware the pipeline architecture is a good choice of implementation which has gained a lot of interests. From hardware design perspective the pipeline architecture can work in various forms as long as the algorithm calculation units can be divided to satisfy the pipeline architecture needs.

So to find a most efficient pipeline architecture for high processing speed and low power in hardware we need to consider the change of delay and area cost in SHA-256 hardware architecture.

A. State-of-art Pipeline principle

The pipeline architecture's core concept is to use FFs (Flip-Flops) to divide the serial working flow and rebuild it into a parallel working flow. So the timing model based on the hardware function requirement have to be built first to find out the most efficient hardware architecture solution. From [9-15] we used the state-of-art pipeline method to consider the relationship between delays and timing combinations with a piecewise linear model. Consider the serial working flow's path delay is "D" and area is "G". And the parallel working flow's one stage pipeline path delay is "S" and area is "L". Then the relationship between the serial working flow and parallel working flow can be described as Fig. 2 showed.

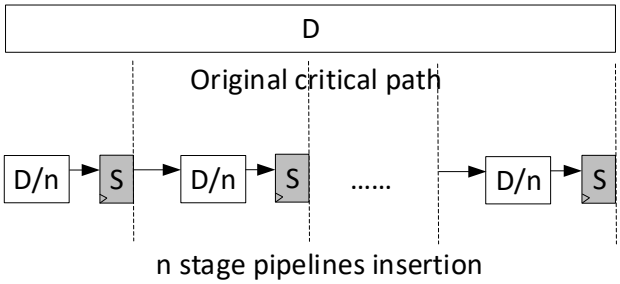

Fig. 2. N stage pipeline insertion into a critical path

The serial working flow can be described as an original critical path which can insert n stage pipelines to work as a parallel working flow. So the new path delay with n stage pipelines inserted is:

$$D' = \frac{D}{n} + S \quad (27)$$

The new area with n stage pipelines inserted can be described as:

$$G' = G + n \times L \quad (28)$$

To give a most efficient pipeline architecture means to find an optimum solution which can have the smallest frequency per area. And that equals to the same question of finding out the smallest area cost for maximum achievable frequency. Considering the maximum achievable frequency can be described as "1/D" so the area cost is:

$$Cost = G \times D \quad (29)$$

Which means the n stage pipelines cost can use (27)-(29) to summarize as:

$$\begin{aligned} Cost' &= G' \times D' \\ &= (G + n \times L) \times \left(\frac{D}{n} + S\right) \\ &= \frac{G \times D}{n} + G \times S + L \times D + L \times S \times n \end{aligned} \quad (30)$$

B. Update the pipeline principle

Evolve the theory and model of III.A with II's SHA-256 algorithm to update the pipeline architecture, the N stage pipelines insertion of Fig. 2 can be described as:

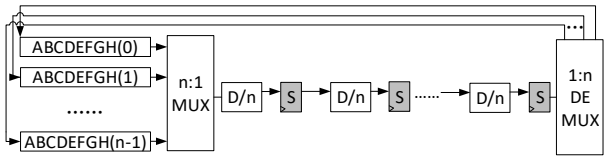

Fig. 3. N stage pipeline insertion with SHA-256

From Fig. 3 it is clear to see that besides the (30) considering FFs' cost there are additional cost needed for MUX and DEMUX's input and output. So for A~H's calculation each pipeline insertion needs an extra 8 registers to temporarily store values of A~H for MUX and DEMUX. No matter how many pipelines are inserted the hardware architecture only needs a pair of MUX and DEMUX. Taking Intel 14nm technology devices' parameter for reference to calculate the area cost with (28), the area of (28) can be updated to:

$$\begin{aligned} G'' &= G' + 8 \times n \times L + 2 \times (n-1) L_{m\&d} \\ &= G + 7.5 \times L + 9.5 \times n \times L \end{aligned} \quad (31)$$

The $L_{m\&d}$ is the area cost of MUX and DEMUX, which is almost 0.25L of (28). The 8*n*L represents the extra 8 registers area cost for n pipelines insertion.

Do the same calculation to find the delay relationship of MUX and DEMUX with (28) to update the (27):

$$D'' = \frac{D}{n} + (0.46 \times \log_2(n) + 1) \times S \quad (32)$$

The 0.46 here is because in STA report it can find that

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

one AND gate's delay is almost 0.46 time of a FF's delay. Use (31) and (32) to update the cost equation as shown in (30):

$$\begin{aligned} Cost'' &= G'' \times D'' \\ &= (G + 7.5 \times L + 9.5 \times n \times L) \\ &\quad \times \left(\frac{D}{n} + (1 + 0.46 \times \log_2(n)) \times S \right) \\ &= (G + 7.5 \times L) \times \frac{D}{n} + 9.5 \times L \times (D + S \times n) \\ &\quad + (G + 7.5 \times L) \times 0.46 \times \log_2(n) \\ &\quad + 4.37 \times L \times S \times n \times \log_2(n) \end{aligned} \tag{33}$$

In (33) only the "n" is a variable, the others are all decided by the technology lib used which can be considered as fixed values here. So the optimum solution means to find out the minimum value of (33).

With the actual technology lib's parameters. the fixed values of (33) can be calculated as:

$$G = 11.2579 \mu m^2 \tag{34}$$

$$D = 1712.57 ps \tag{35}$$

$$L = 0.67 \mu m^2 \tag{36}$$

$$S = 131.71 ps \tag{37}$$

Calculating the (33) with (34)-(37), the relationship curve of cost'' with different n is showed in Fig. 4.

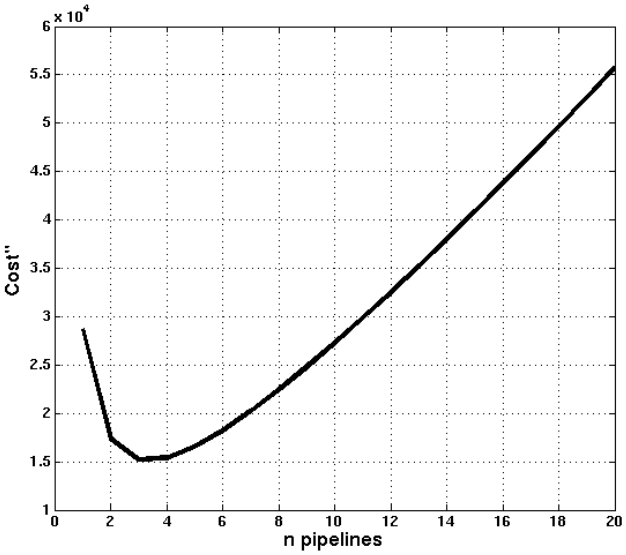

Fig. 4. Relationship curve of cost'' with different n

According to Fig. 4 it is clear to see that when n=3 the cost gets the minimum value which means the most efficient pipeline architecture for SHA-256 calculation with Intel 14nm technology lib is 3 pipelined architecture.

IV. Proposed Design

To realize the 3 pipeline architecture of SHA-256 we need to divide the SHA-256 calculation into 3 parallel working flow in an efficient way. From the SHA-256 hashing algorithm we can see what limits the computation speed most is (4)-(17). In fact the (1)-(3) can be done quite earlier but has to wait a very long time for (4)-(17) to finish a round of whole SHA-256 computation. The proposed design is to optimize the (4)-(17) in order to get a better performance in 3 steps.

A. Critical Path Analysis

To analyze the critical path of SHA-256 we unfold the computation steps, which are showed in Fig. 5.

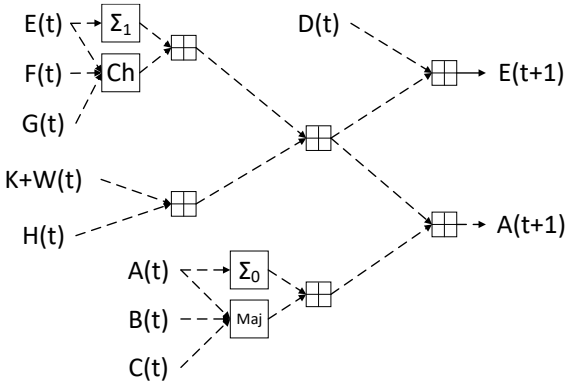

Fig. 5. Critical path

The symbols in Fig. 5 are same as Fig. 1, and the "+" represents the addition modulo 232. As known the most problematic characteristic of SHA-256 is the addition modulo 232, which slows down the speed heavily versus the other calculation steps [16]. Based on this fact, we find the most critical path in SHA-256 round calculation. As Fig. 5 shows, the most critical path is showed in dotted line, which means from calculation e(t) to obtain a(t+1) in each round is the longest path worth optimizing (same as other long path with 3 "+" calculations).

B. Break Critical Path

To optimize the SHA-256 computation it needs to break the critical path into shorter paths thus make it possible for the whole computation chain to work at a higher frequency. For this need, we consider each addition modulo 232 calculation as one basic unit of SHA-256 calculation in each round. To separate all calculations we insert FFs to each minimum unit.

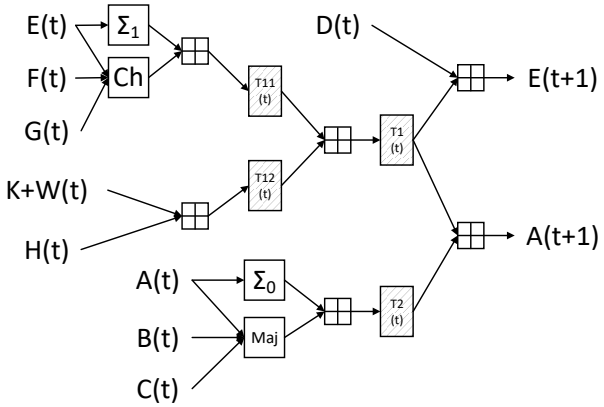

Fig. 6. FFs insertion

As Fig. 6 shows, we insert 4 32-bits FFs (The grey rectangles) in each round of SHA-256 to separate all basic units. With the insertion, there is only one addition modulo 232 calculation between each two FFs. And the T1 (t) and T2 (t) mean the FFs for T1 and T2 calculation as

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

what equation (4) and (5) show, n means the round number of whole SHA-256 computation. T11 (t) and T12 (t) are intermediate results for T1, "t" the same as before.

Because the long path is broken , we can run almost 3 times faster than before, but each round will take 3 cycles now.

C. Reschedule With Parallel Pipeline

In standard SHA-256 computation, variable "A" to "H" are calculated one after another. But most of them are just a bit shifting operation which is much easier compared to addition modulo 232 calculation. Consequently, we reschedule the SHA-256 computation based on step B's basic units with parallel pipeline.

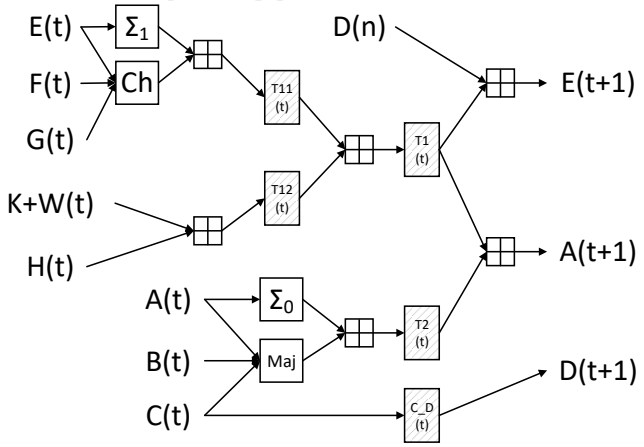

Fig. 7. Variable update

As Fig. 7 showed, to achieve parallel computation, a key intermediate FF "C_D" is added, to preserve C and update D later. With this rescheduling the SHA-256 is separated into 3 individual steps to update "A"~"H", in subsequent 3 cycles. The functional diagram in sequence is showed in Fig. 8.

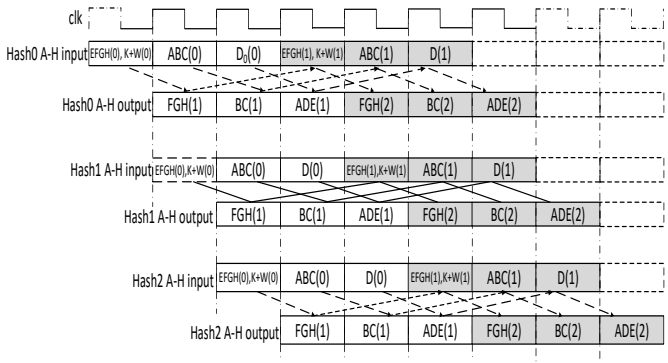

Fig. 8. Rescheduled parallel pipeline SHA-256

As the Fig. 8 shows, with parallel pipelines three SHA-256 hashes can be calculated at the same time. The hardware architecture is showed in Fig. 9.

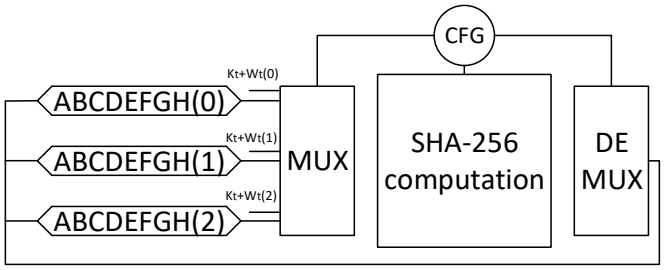

Fig. 9. Parallel computation SHA-256 hardware architecture

The proposed architecture gains 3 times performance with a 3 times higher clock frequency, compared to the standard architecture.

V. Result And Discussion

The proposed high performance parallel computation of SHA-256 is successfully implemented in Verilog. The hardware architecture is fully verified at RTL level and synthesized with Intel 14nm technology lib. The comparison results are showed below:

TABLE I
HARDWARE COMPARISON RESULTS

	Clock(ps)	Area(μm2)	Power(mW)
Standard	1959	4916.7	3.3794
Proposed	653	14272.6	6.855

The proposed high performance parallel computation hardware architecture of SHA-256 is 3 times faster than the standard architecture as we expected.

The area cost to achieve this improvement is 2.90 times compare to standard SHA-256, which is because there are reused function modules to save area.

The power of proposed parallel SHA-256 is just 2.03 times of standard SHA-256 to have same 3 times output. That's because the sequential logic consumes much bigger power than the combinational logic, and the proposed architecture can exactly save much sequential logic.

VI. Conclusions

The parallel hardware architecture is the best solution to achieve high processing speed and low power consumption in hardware. This paper first builds the speed and area model with SHA-256 algorithm and technology lib to find the most efficient pipeline architecture is 3 pipeline stages for SHA-256 realization. Then it is dividing and updating the architecture with SHA-256 calculation unfolding by FFs to give a high performance hardware architecture for parallel computation in AISC. The design is synthesized with Intel 14nm technology and the comparison results demonstrated the improvement of 3 times computation speed with 50.7% power consumption, at a cost of only 2.9 times area.

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

REFERENCES

[1] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] X. Cao and M. O'Neill, "Application-oriented SHA-256 hardware design for low-cost RFID," in *Proc. IEEE International Symposium on Circuits and Systems*, Seoul, 2012, pp. 1412-1415.

[3] W. L. Harrison, A. M. Procter and G. Allwein, "Model-driven design & synthesis of the SHA-256 cryptographic hash function in rewire," in *Proc. IEEE International Symposium on Rapid System Prototyping (RSP)*, Pittsburgh, 2016, pp. 1-7.

[4] M. Padhi and R. Chaudhari, "An optimized pipelined architecture of SHA-256 hash function," in *Proc. IEEE 7th International Symposium on Embedded Computing and System Design (ISED*), Durgapur, 2017, pp. 1-4.

[5] S. Suhaili and T. Watanabe, "Design of high-throughput SHA-256 hash function based on FPGA," in *Proc. IEEE 6th International Conference on Electrical Engineering and Informatics (ICEEI*), Langkawi, 2017, pp. 1-6.

[6] I. Algredo-Badillo, C. Feregrino-Uribe, R. Cumplido and M Morales-Sandoval, "FPGA-based implementation alternatives for the inner loop of the Secure Hash Algorithm SHA-256," *Microprocessors & Microsystems*, vol. 37, pp. 750-757, Jun. 2013.

[7] H. Mestiri, F. Kahri, B. Bouallegue, and M. Machhout, "Efficient FPGA Hardware Implementation of Secure Hash Function SHA-2," *International Journal of Computer Network and Information Security*, vol. 7, pp. 9-15, Dec. 2014.

[8] *Secure Hash Standard (SHS), N. I. of Standards and Technology,* FIBS PUB 180-4, 2012.

[9] G. L. Zhang, B. Li, and U. Schlichtmann, "PieceTimer: a holistic timing analysis framework considering setup/hold time interdependency using a piecewise model," in *Proc. 2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD),* Austin, 2016, pp. 1-8.

[10] G. L. Zhang, B. Li, Y. Shi, J. Hu, and U. Schlichtmann, "EffiTest2: Efficient Delay Test and Prediction for Post-Silicon Clock Skew Configuration Under Process Variations," *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. 38, pp. 705-718, Apr. 2019.

[11] G. L. Zhang, B. Li, J. Hu, Y. Shi, and U. Schlichtmann, "Design-Phase Buffer Allocation for Post-Silicon Clock Binning by Iterative Learning," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, pp. 392 – 405, Feb. 2018.

[12] G. L. Zhang, B. Li, M. Hashimoto, and U. Schlichtmann, "Virtualsync: timing optimization by synchronizing logic waves with sequential and combinational components as delay units," in *Proc. 2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC),* San Francisco, 2018, pp. 1-6.

[13] G. L. Zhang, B. Li, B. Yu, D. Z. Pan, and U. Schlichtmann, "TimingCamouflage: Improving circuit security against counterfeiting by unconventional timing," in *Proc. 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE),* Dresden, 2018, pp. 91-96.

[14] G. L. Zhang, B. Li, and U. Schlichtmann, "Timing with Virtual Signal Synchronization for Circuit Performance and Netlist Security," in *Proc. 2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI*), Hong Kong, 2018, pp. 715 – 718.

[15] Y. Yao, *SuperScalar RISC Processor Design*. Bei Jing: Tsinghua University Press, 2014, ch. 1.

[16] L. Dadda, M. Macchetti and J. Owen, "The design of a high speed ASIC unit for the hash function SHA-256 (384, 512)," in *Proc. Design, Automation and Test in Europe Conference and Exhibition*, Paris, 2004, pp. 70-75.

Ruizhen, Wu was born in China, Jan 1st 1986. PhD. The PhD was earned in School of Microelectronics of XIDIAN University, Shaanxi Province, China, in 2014. The major field of study is Asynchronous Circuits design, 5G CODEC and AI.

He has worked in Hangzhou, Zhejiang Province, China, since 2014, in the 2012 communication lab of Huawei at first, then Intel iCDG, and Inspur Electronic Information Industry Co.,Ltd now

Xiaoyong, Zhang was born in China, Nov 5th 1980. Bachelor. The first bachelor degree was earned in automation, in School of Marine Science and Technology, Northwestern Polytechnical University, Shaanxi Province, China, in 2003, and the second bachelor degree was earned in electronic science and technology, in Institute of Microelectronics, Tsinghua University, Beijing City, China, in 2005.

He has worked in Xi'an, Shaanxi Province, China, since 2005, in the wireless department for Infineon Technology at first, and now Biren technology. His current job is SoC HW design manager

Mingming, Wang was born in China, Oct 1st 1986. Master. The Master degree was earned in Computer Application Technology in Xi'an University of posts & Telecommunications, Shaanxi Province, China, in 2011, and the bachelor degree was earned in electronic science and technology, in Xi'an University of posts & Telecommunications, Shaanxi Province, China in 2008.

He has worked in Inspur Electronic Information Industry Co.,Ltd since 2019.

Lin, Wang was born in China, Dec. 1st. 1971. Master of Sci. The master degree was earned in Dept. of Electrical Engineering, Fudan University, Shanghai, China, in 1998. His majority is microelectronics and physics on semiconductor and semiconductor device.

He worked in Shanghai Nortel Semiconductor and Broadcom, focusing on communication chip development after his graduation.

He is now the Director of SoC R&D in Inspur Electronic Information Industry Co.,Ltd.

Copyright ⓒ 2019 GiRI (Global IT Research Institute)

Volume 8 Issue 5, September. 2019, ISSN: 2288-0003

ICACT-TACT JOURNAL

GIRI
Global IT Research Institute

1713 Obelisk, 216 Seohyunno, Bundang-gu, Sungnam Kyunggi-do, Republic of Korea 13591
Business Licence Number : 220-82-07506, Contact: tact@icact.org Tel: +82-70-4146-4991