Cryptographic Key Generation from PUF Data Using Efficient Fuzzy Extractors

Hyunho Kang*, Yohei Hori**, Toshihiro Katashita**, Manabu Hagiwara***, Keiichi Iwamura*

**Dept. of Electrical Engineering, Tokyo University of Science,*
6-3-1 Niijuku, Katsushika-ku, Tokyo 125-8585, Japan
***Research Institute for Secure Systems (RISEC),*
National Institute of Advanced Industrial Science and Technology (AIST),
Central 2, 1-1-1 Umezono, Tsukuba, Ibaraki 305-8568, Japan
**** Dept. of Mathematics and Informatics, Faculty of Science, Chiba University,*
1-33 Yayoi-cho, Inage, Chiba 263-0022, Japan
kang@ee.kagu.tus.ac.jp, {hori, t-katashita}@aist.go.jp, hagiwara@math.s.chiba-u.ac.jp, iwamura@ee.kagu.tus.ac.jp

***Abstract*—Physical unclonable functions (PUFs) and biometrics are inherently noisy. When used in practice as cryptographic key generators, they need to be combined with an extraction technique to derive reliable bit strings (i.e., cryptographic key). An approach based on an error correcting code was proposed by Dodis et al. and is known as a fuzzy extractor. However, this method appears to be difficult for non-specialists to implement. In our recent study, we reported the results of some example implementations using PUF data and presented a detailed implementation diagram. In this paper, we describe a more efficient implementation method by replacing the hash function output with the syndrome from the BCH code. The experimental results show that the Hamming distance between two keys vary according to the key size and information-theoretic security has been achieved.**

***Keyword*—Fuzzy Extractor, Arbiter PUF, Physical Unclonable Functions**

Hyunho Kang is currently Assistant Professor in the Department of Electrical Engineering at Tokyo University of Science, Japan, from April 2013. He received his Ph.D from the University of Electro-Communications, Tokyo, in 2008. From 2008 to August 2010, he was a Researcher/Assistant Professor of the Chuo University, Tokyo, where he was part of team that developed Biometric Security technologies. From Sep. 2010 to March 2013, he was AIST Postdoctoral Researcher of the National Institute of Advanced Industrial Science and Technology (AIST), Japan, where his research work has been mainly focused on the evaluation of a Physical Unclonable Functions. His main interests are in digital watermarking, biometric security and Physical Unclonable Functions.

Yohei Hori received his BE, ME, and PhD degrees from the University of Tsukuba, Ibaraki, Japan, in 1999, 2001, and 2004, respectively. After receiving his PhD, he spent five years as a postdoctoral researcher at the National Institute of Advanced Industrial Science and Technology (AIST). He moved to Chuo University as a research scientist in 2008, before returning to AIST in 2010 as a researcher. His current research interests include partially reconfigurable systems, side-channel analysis, fault analysis, and physically unclonable functions. He is a member of IEEE, IEEE-CS, IEICE and IPSJ.

Toshihiro Katashita completed the doctoral program of the Graduate School of Systems and Information Engineering, University of Tsukuba, in 2006, whereupon he joined AIST as a fixed-term researcher. In 2008, he became a tenure-track researcher at AIST. He is involved in research projects on high-performance computation circuit design and hardware security. He is engaged in the development of cryptographic hardware and software as well as side channel attack experiments.

Manabu Hagiwara received the B.E. degree in mathematics from Chiba University in 1997, and the M.E. and Ph.D. degrees in mathematical science from the University of Tokyo in 1999 and 2002, respectively. From 2002 to 2005 he was a postdoctoral fellow at IIS, the University of Tokyo. From 2005 to 2012 he was a research scientist of National Institute of Advanced Industrial Science and Technology (AIST). Currently, he is an associate professor in Department of Mathematics and Informatics, Faculty of Science, Chiba University, and is a visiting associate professor of Center for Research and Development Initiative, Chuo University. His current research interests include industrial mathematics, coding theory, and combinatorics.

Keiichi Iwamura was born in Kyushu, Japan in 1958. He received the B.E. and M.E. degrees in information engineering from Kyushu University in 1980 and 1982, respectively. In 1982, he joined Canon Inc., Japan. In 1994, he received his Ph.D. degree from the University of Tokyo, Japan. He is currently Professor in the Department of Electrical Engineering at Tokyo University of Science, Japan. His main interests are in coding theory, parallel processing, information security and digital watermarking. He is a member of IEEE and IEICE. He served as the Chair of the society of Information Hiding and its Criteria for evaluation. He was elected a Fellow of IPSJ.