1067-94-740 **Hiroyuki Okazaki*** (okazaki@cs.shinshu-u.ac.jp), Shinshu University, Graduate School of Science and Technology, 4-17-1 Wakasato, Nagano, Nagano 380-8553, and **Yasunari Shidama** and **Yuichi Futa**. *Formal Definition of Probability and Probabilistic Function on Finite and Discrete Sample Space for Proving Security of Cryptographic Systems Using Mizar.*

In recent studies, many researchers have attempted to verify the security of cryptographic systems using computer-assisted proof tools. For example, Certicrypt and Cryptoverif are well-known frameworks in this context. However, these proof tools are insufficient for proving the security of some cryptographic systems, because the tools specialize in the game-based proof method. Thus, in this study, we attempt to formalize essential elements of cryptology, number theory,computational complexity, and probability etc. We then also encode them in Mizar system. In this report, we briefly introduce the importance of which probability and probabilistic functions in cryptology. Further, we present our formal definition of probability and probabilistic function on a finite and discrete sample space in Mizar. (Received September 14, 2010)