論 文 内 容 の 要 旨

Over the past decade, chaos theory has been purely studied for academic as a fascinating mathematical phenomenon, until latterly a new research aspect has emerged. As a result of many years of research and study, chaos has now been considered beneficial to actual applications especially in communication and cryptography. Regarding to the increasing interest on chaos, a circuit which offer chaotic behavior such a chaotic oscillator circuit has become a subject of increasingly and extensively research and study and led to an introduction of many new design chaotic oscillator circuits.

Beside the increasing interest in research on chaotic oscillator, a major part of cryptography such a true random bit generator has also recently attracted a lot of research attention due to the increasingly demand on security and privacy. Typically, the true random bit generator is utilized in confidential key generation, however it can also be used in some computational algorithm. Although the dynamics of chaotic systems is deterministic, the highly sensitivity to change of initial condition and aperiodic characteristic of the chaotic system still make chaotic oscillator suitable for the use as a randomness source of true random bit generator.

This dissertation mainly aims to develop new chaotic oscillators as well as research and investigation on new chaotic maps and their chaotic dynamic. The circuit structures of the oscillators are expected to be simple and compact, yet proper chaotic dynamics such a robustness are also expected. The design strategy for the chaotic oscillator is the development of circuit regarding the exiting chaotic maps and the new propose chaotic maps. Hence, the implementation of application regarding chaotic oscillators such a true random bit generator is also develop as a practical example. Through the literature reviews, a hypothesis can be defined that the chaotic oscillator circuit can be built by using a nonlinear circuit with the specific transfer characteristic such as approximate V-shape or N-shape. The first approach of designing chaotic oscillators is regarding the hypothesis by using V-shape characteristic and S-shape (sigmoid) characteristic. The second design approach is regarding a new sigmoidal chaotic map. The research on the proposed chaotic map, which based on S-shape functions, shows the feasibility of offering robust chaotic behavior. The third approach is also regarding to a new chaotic map which based on parabola curve function. This chaotic oscillator circuit is designed based on a circuit realization method.

As mentioned, the first approach presents two CMOS based discrete-time chaotic oscillators and its

application for random bit generator (RBG). The first design method of chaotic oscillator was given by the use of 3 transistors to construct chaotic map circuit in order to achieve a V-shape characteristic (inverse tent map). Simulation of the chaotic oscillator is described and examined in terms of bifurcation diagram and transient waveform to show that it has a desirable output and suitability for a true random bit generator (TRBG). The TRBG is designed using chaotic oscillator as random signal generator which also known as entropy source and randomness of output signal can be increased by a dual oscillator sampling method and a XOR operation. The second design method of chaotic oscillator is based on a chaotic map with reverse sigmoid characteristic. Then, a hybrid random number generator (HRNG) based on a combination of discrete-time chaotic oscillator and a linear feedback shift register (LFSR) is presented. A random signal is produced by the chaotic oscillator and then, to increases the randomness; the signal is combined with LFSR signal through XOR gate. The resulting output from both RBG are evaluated using the NIST SP800-22 test suite.

The second approach is interested regarding a 1-D sigmoidal chaotic map, which has never been distinctly investigated. A generic form of the sigmoidal chaotic map with three terms, i.e., $x_{n+1} = \mp AfNL(Bx_n) \pm Cx_n \pm D$, where A, B, C, and D are real constants is introduced. The unification of modified sigmoid and hyperbolic tangent (tanh) functions reveals the existence of a "unified sigmoidal chaotic map" generically fulfilling the three terms, with robust chaos partially appearing in some parameter ranges. A simplified generic form, i.e., $x_{n+1} = \mp fNL(Bx_n) \pm Cx_n$, through various S-shaped functions, has recently led to the possibility of linearization using (i) hardtanh and (ii) signum functions. This study finds a linearized sigmoidal chaotic map that potentially offers robust chaos over an entire range of parameters. Chaos dynamics are described in terms of chaotic waveforms, histogram, cobweb plots, fixed point, Jacobian, and a bifurcation structure diagram based on Lyapunov exponents. Hence, the chaotic oscillator based the linearized sigmoidal chaotic map is shown as well as a true random bit generator based on the proposed chaotic oscillator is demonstrated as a practical example. The resulting output of the random bit generator is evaluated using the NIST SP800-22 test suite and TestU01.

The third approach is interested in designing a discrete-time chaotic oscillator circuit with reference to the research and study regarding a parabola chaotic map. As the proposed generic form of chaotic map with three terms which introduced in the Chapter 3, a new chaotic map based on nonlinear function with parabola curve transfer characteristic is proposed. A simplified parabola chaotic map is based on various parabola curve functions which led to the linearized parabola chaotic map using Absolute Value function. The linearized chaotic map can of offer a robust chaos over the entire range of parameter. Chaos dynamics were described in terms of fixed point, Jacobian, chaotic waveforms, cobweb plots, bifurcation diagram, and Lyapunov

exponents. A discrete-time chaotic oscillator circuit based on the proposed parabola chaotic map is presented. Simulation results of the circuit such a bifurcation diagram and chaotic waveforms are presented in order to investigate the chaotic dynamic of the circuit which also revealed that the proposed chaotic oscillator can offer robust chaos nearly the entire range of parameter.

This dissertation has proposed many chaotic oscillator implementation using a simple structure and few number of components. The research and study on two new chaotic maps are also presented. Simulation results show the feasibility and compatibility for application based on all the proposed chaotic oscillators. The true random bit generators based on each proposed chaotic oscillators were presented with the statistical evaluation.