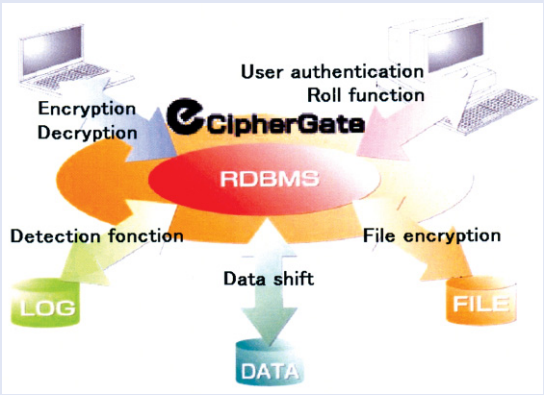
Patent No. 3030341

Device and Method for Outputting Random Vectors and Recording Medium

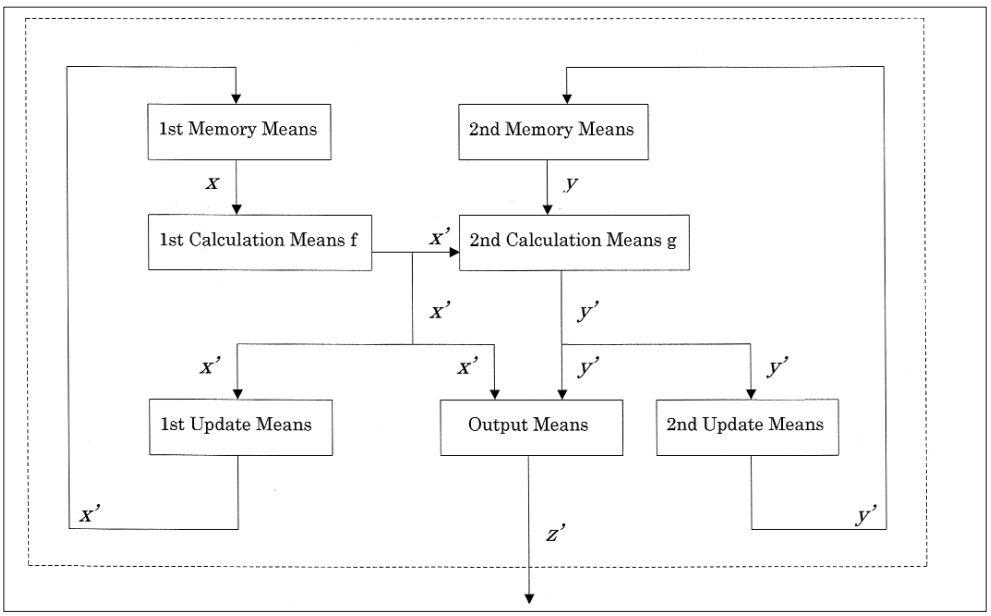
Invented by: UMENO Ken



(Photo of eCipherGate)

Overview of Technology

Most conventional methods for generating random number sequences use a preset one-dimensional recurrence formula. However, these conventional methods cannot respond to the growing needs of recent applications that require not only the generation of a single random number sequence but also the simultaneous generation of several independent sequences. It was therefore necessary to develop a completely new type of random number sequence generator, one that could generate a random vector series with components that are statistically independent random number sequences. In particular, this new type of generator is required for applications that simultaneously encrypt large-volume data such as moving pictures. This invention allows the generation of high-bandwidth random number sequences that can respond to the demands of network broadband technologies. The flowchart in Fig.1 shows the process of random vector series generation using the present invention. This invention is the first to provide the basic technology for the generation of random vector series in arbitrary dimensions, and can be applied to image encryption, multi-dimensional database encryption, the Monte Carlo method, scrambling code generation for multicarrier CDMA, and initial key generation for public key cryptosystems.



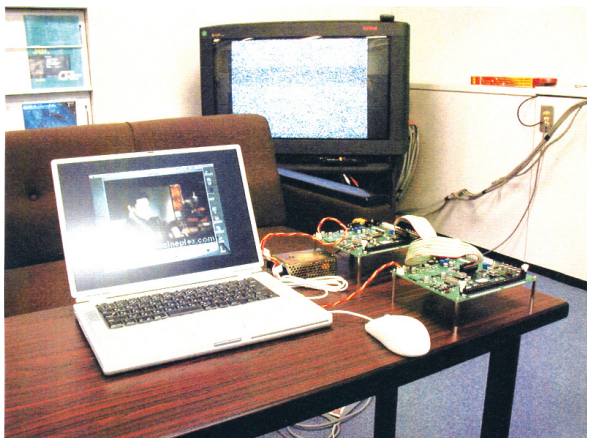
Commercialization by the Researchers Themselves

This patent provides the basic architecture for a new encryption algorithm called the "Vector Stream Cipher," which is being developed as part of the "R&D for a Chaotic Cipher Chip" under the CRL's "Pre-venture Program." This program, launched last fiscal year, is designed to support the promotion of new businesses by allowing researchers to capitalize on the results of their research. Researchers can thus dedicate their time and efforts to the sort of prototype development and validation experiments required to launch new businesses, all within the context of their regular duties at CRL. The development of the Vector Stream Cipher chip was also carried out under this program. Construction is now complete of a prototype of the chaotic cipher chip (a circuit-reprogrammable LSI chip) using the Field Programming Gate Array (FPGA). This prototype chip allows real-time encryption and decryption of movies (such as those in video signal format) at the extremely high processing rate of 1 Gbps. For this purpose, a generation algorithm for random vector series similar to that shown in Fig. 1 can be easily parallelized and is suitable for pipeline processing. The Vector Stream Cipher chip can therefore significantly speed up processing operations.

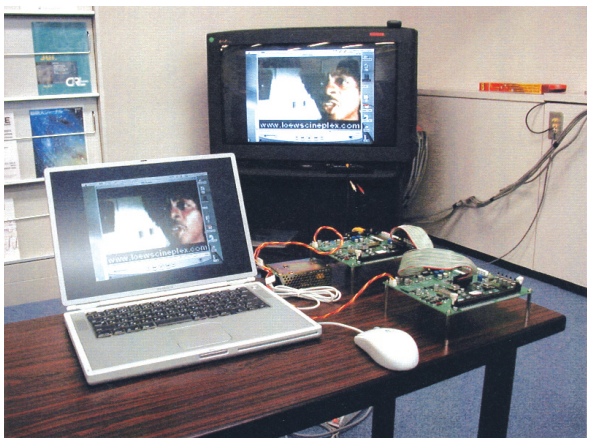
Currently, a one-million-gate FPGA chip has achieved an encryption speed of 25 Gbps, which is the faster record in the world.

Technology Transfer to Venture Businesses

In May 2000, a license contract was entered into between the CRL and Japan Information Technology Co., Ltd., which developed the eCipherGate, the first software to perform automatic column content encryption using the vector stream encryption technology of the present patent. In the spring of 2002, eCipherGate was released in Japan. In the first half of fiscal 2002, six products have been delivered through five sales subsidiaries (including Itochu Techno-Science Corporation) and one of these products has been used for encryption of R&D data at major pharmaceutical companies. In the future, this patent should prove useful in strengthening the security of today's backbone systems by providing partial encryption technologies for databases such as the Basic Resident Register Network as well as for financial and medical databases.



Encrypted Video Signals on TV



Decrypted Video Signals on TV

Video Signal Encryption by Chaotic Cipher Chip

Patents Obtained by CRL may be used for a fee. Please contact CRL Intellectual Property Group for information on patent licensing and technical data.