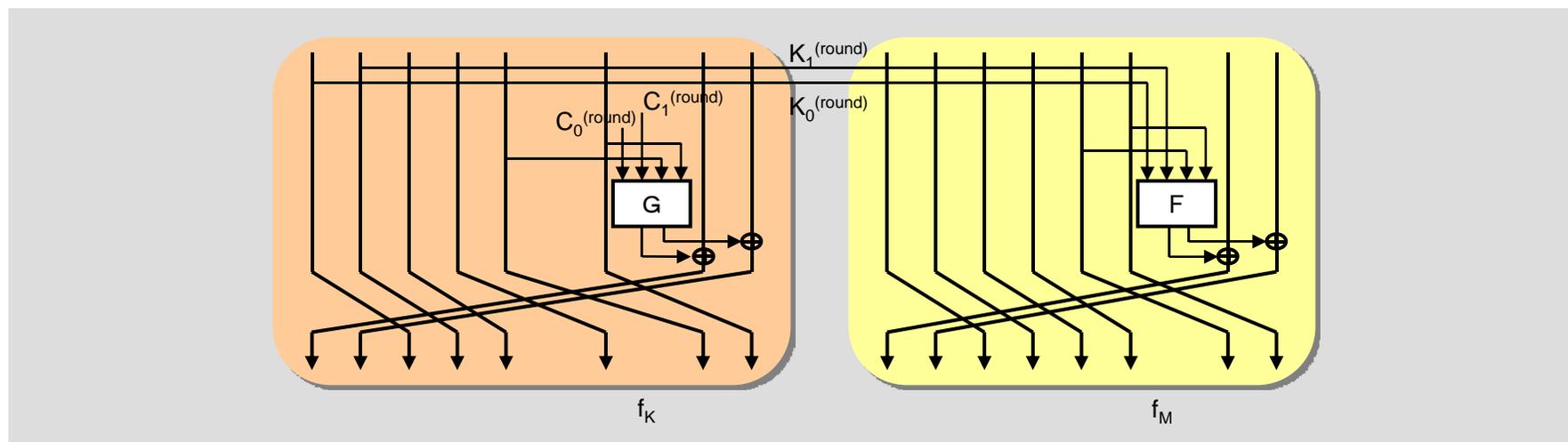2009/1/15 Release

Development of next-generation cryptography for secure information communication
Accepted as official candidate in the NICT competition for next-generation cryptography

Hitachi, Ltd. together with Kobe University, and Fukui University have co-developed an even more secure next-generation hash function,[1] "Lesamnta."[2] Further, "Lesamta" has been formally accepted as a candidate in the open international Cryptographic Hash Algorithm Competition held by the US National Institute of Standards and Technology (NIST), which holds an influential role in determining international cryptographic standards.

This research is a result of "Research & development on next-generation hash function (FY2007-2008)", commissioned by the National Institute of Communications Technology (NICT), Japan.

[1] Hash function: A function which generates a fixed-length output value for an arbitrary message input. It is required to meet various safety criteria such as difficulty in determining an input message which will provide the same output value.

[2] Lesamnta: A registered trademark of Hitachi, Ltd., in Japan.

Details of this hash function will be presented at the 2009 Symposium on Cryptography and Information Security (SCIS 2009), held from 20th - 23rd January 2009 in Otzu-shi, Shiga-ken, Japan.