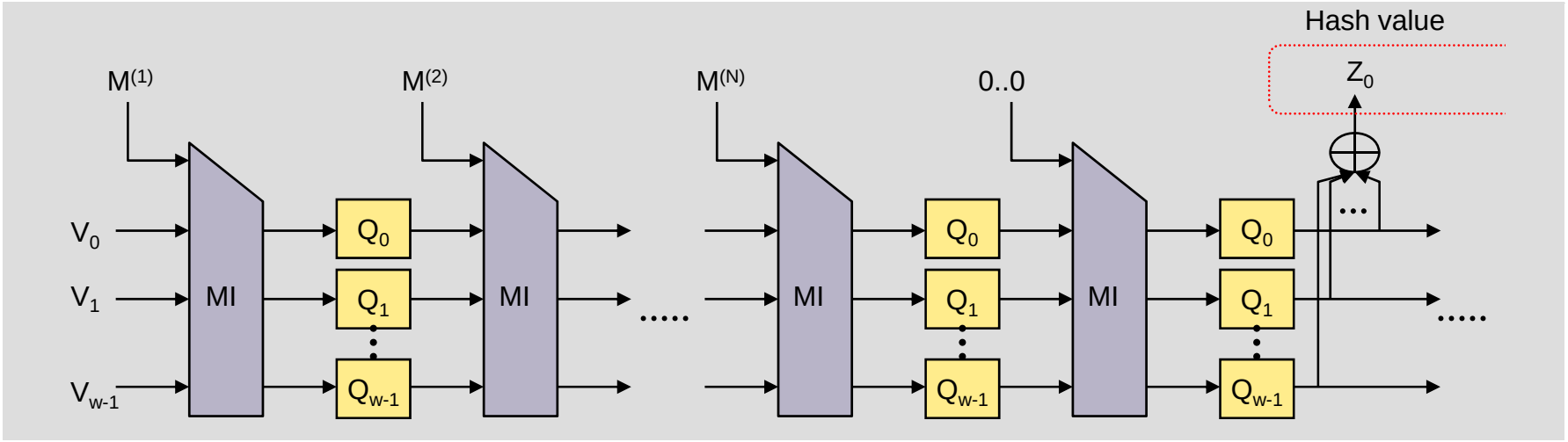
2009/1/21 Release

Development of a secure and high-speed next generation hash function

Sponge construction method resolves vulnerability in standard hash function “SHA-1”



Hitachi, Ltd. together with the Katholieke Universiteit Leuven have developed a secure and high-speed next generation hash function,*1 which will become a base in cryptography for providing information security. The hash function developed utilizes a sponge construction method whereby all the data is collectively safely compressed, and provides greater security than the current standard hash function “SHA-1”*2 as well as enabling high-speed processing within various products and systems such as PCs, mobile telephones and IC cards.

*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 Secure Hash Algorithm-1 (SHA-1): A hash function defined in the US Federal Information Processing Standard 180-2 and developed by the US National Institute of Standards and Technology (NIST), which generates a 160-bit long characteristic level. It is not only a US standard but also a for the Internet as well as ISO, etc.

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