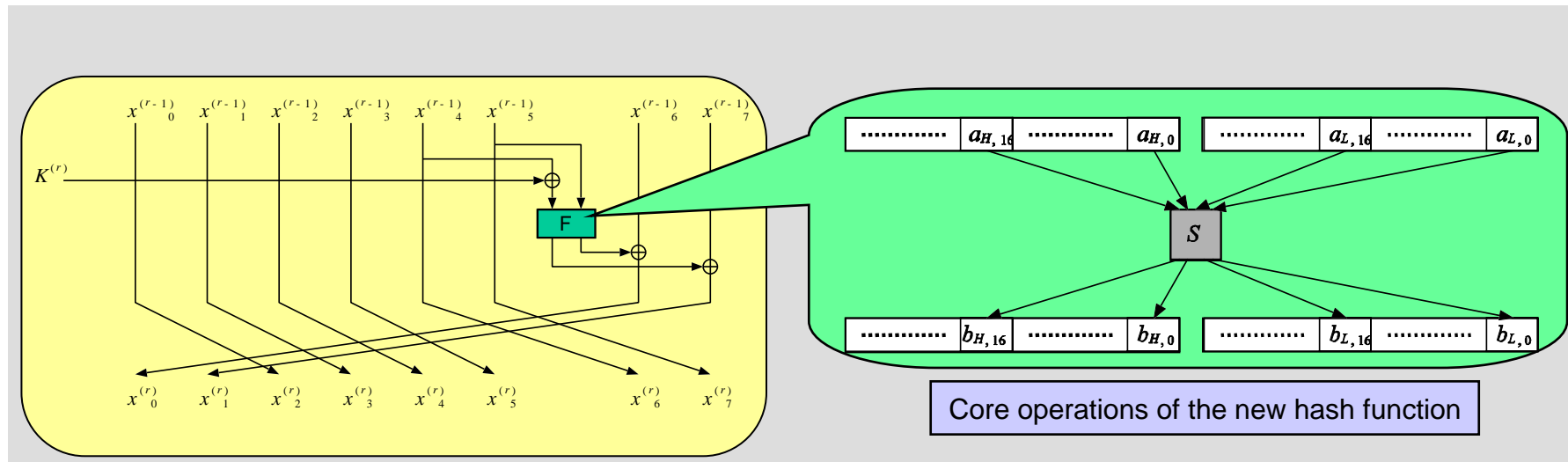


2007/1/22 Release

## Development of a light weight hash function for RFID tags

- Opening the way for authentication systems optimized for information security in compact electronic devices -



The National Institute of Information and Communications Technology (NICT; President: Dr. NAGAO Makoto) and Hitachi, Ltd., have succeeded in the development of a light weight hash function which can be embedded in compact electronic devices such as RFID tags. A hash function is an algorithm used in authentication of communication data or users (including devices). Conventionally, as a hash function requires a large amount of memory for processing, it was considered difficult to apply it to compact electronic devices. The hash function developed, uses a simple algorithm repeatedly, allowing the size of the circuit involved in the calculation to be small enough for it to be integrated within a compact electronic device. As a result, it will become possible to employ hash functions in a wide range of applications such as authentication of RFID tags or credit cards, and thus increase their security. This research was supported by National Institute of Information and Communications Technology (NICT), Japan