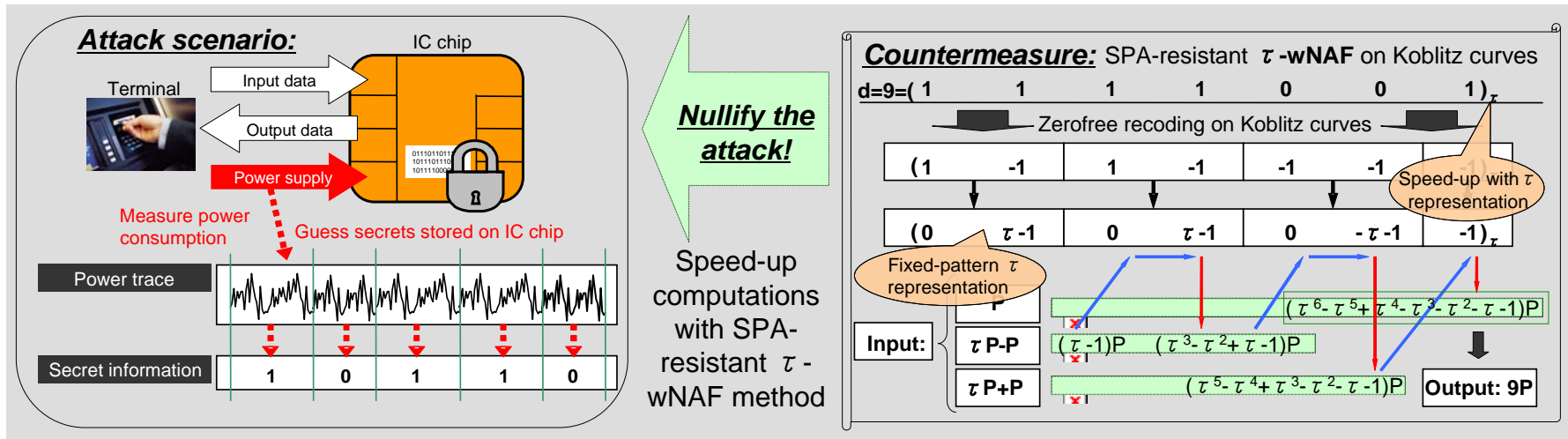


2005/7/4 Release

Development of embedded cryptographic technology for a compact microprocessor

- Facilitating the application of elliptic curve cryptosystems in IC cards and USB memory devices -



The Systems Development Laboratory of Hitachi, Ltd. has developed next-generation public key encryption technology which can operate without a dedicated cryptographic coprocessor, for compact microprocessors used in mobile devices and IC cards. This technology uses Koblitz curves in the frame of elliptic curve cryptosystems, used in digital signatures, and a highly secure Hitachi original tamper-resistant technology, the width-w Non-Adjacent Form (wNAF), accommodated for Koblitz curves. Compared to the RSA cryptosystem, this technology can operate without a dedicated coprocessor or loss of speed, and provide an equivalent level of security. Using this technology, it is possible to achieve a high integrity authentication system with a realistic processing speed using commonly available low-priced IC chips, and thus may be used in the replacement of magnetic strip credit cards with IC chip cards as a countermeasure for counterfeit magnetic card, or in a USB authentication chip, to be inserted in to a PC, as a preventive measure against Internet crimes. As this technology provides a reasonable level of protection against the menace of IC card skimming, expected to become a growing problem in the ubiquitous information society, Hitachi has assessed it as digital signature technology which can be achieved at a low cost, and plans to make it available as an encryption code library for compact microprocessors or as a cryptographic chip.