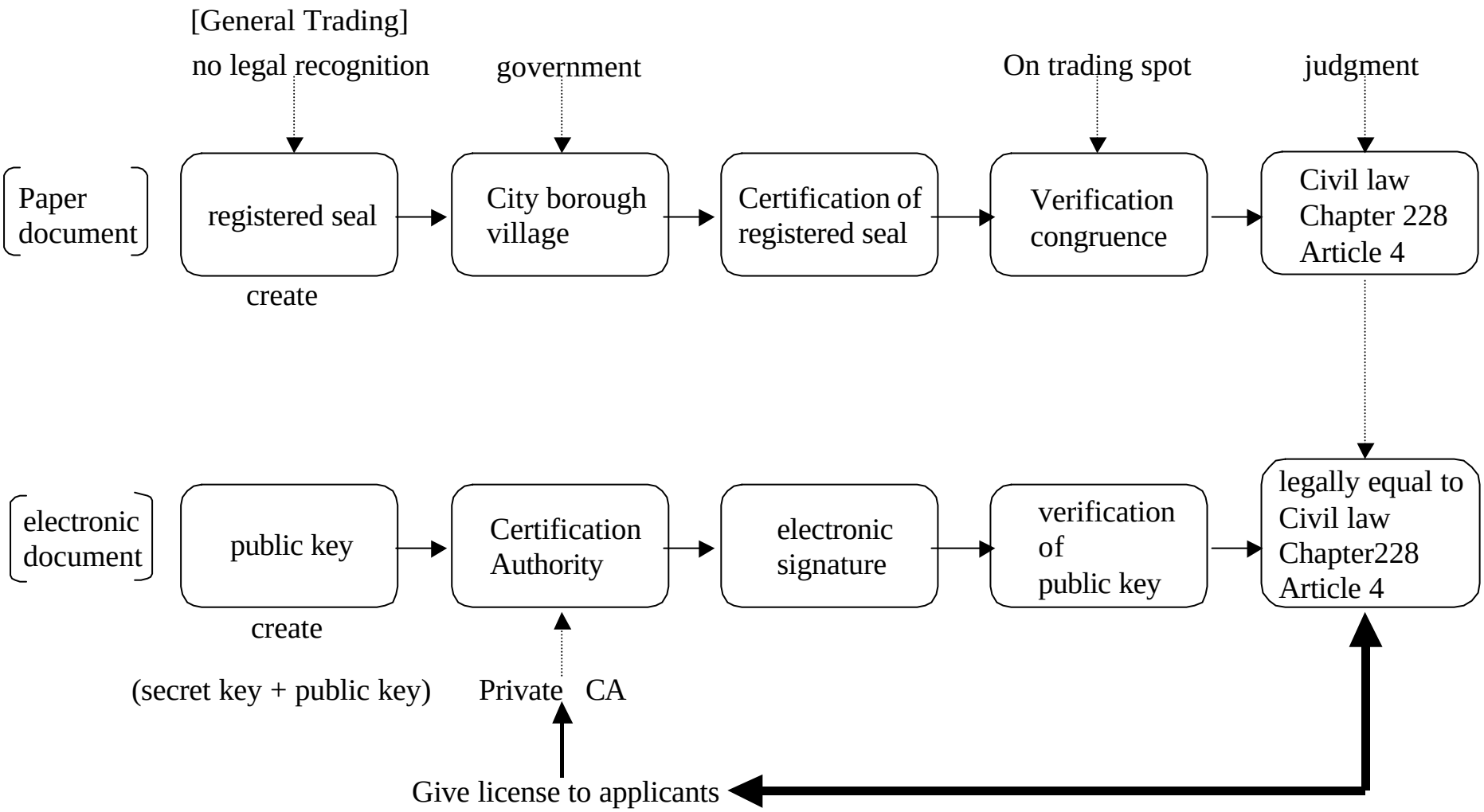



Fig.5 Lawful authorization to electronic signature and certification

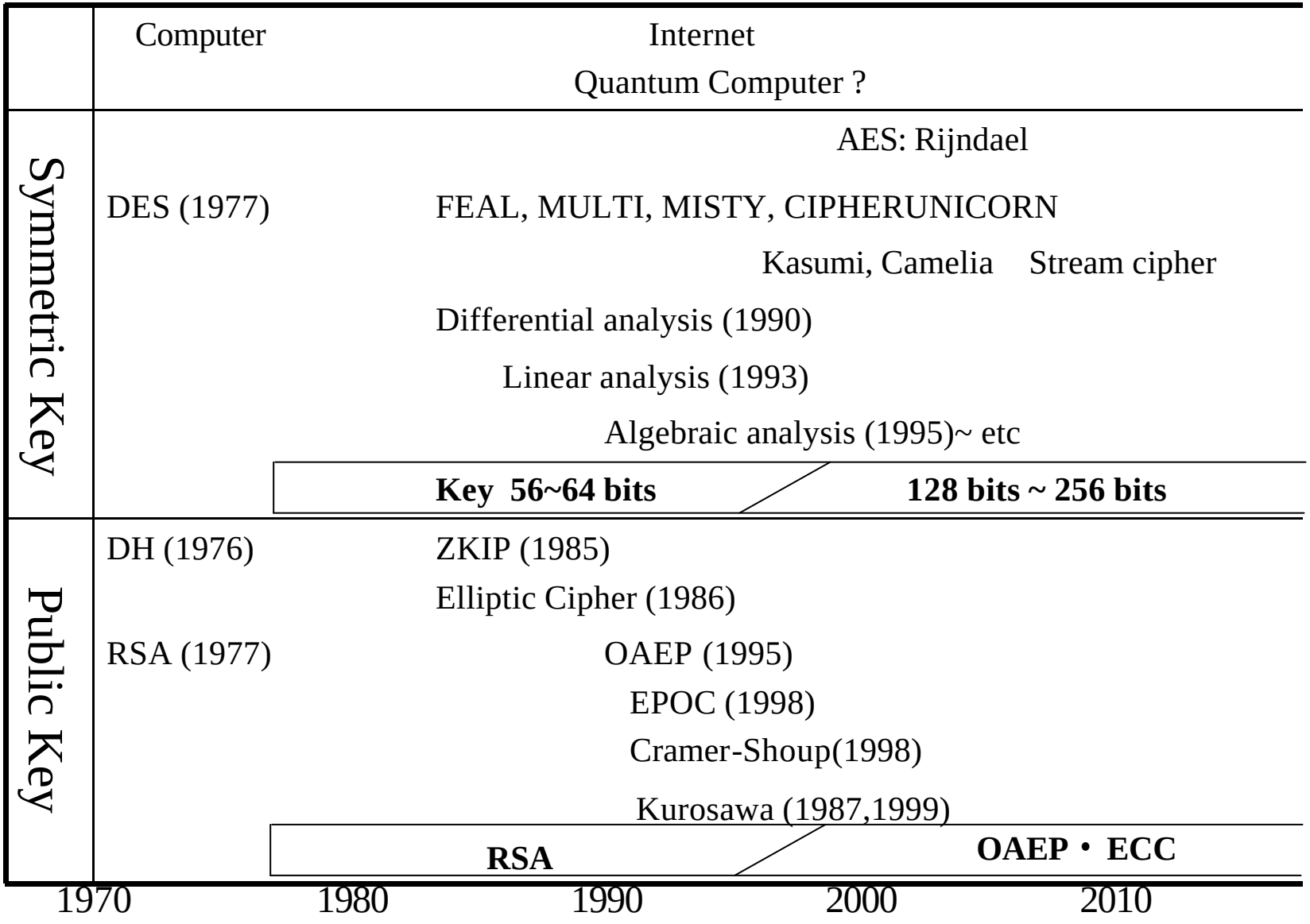



Fig.6 Development of Cryptosystems

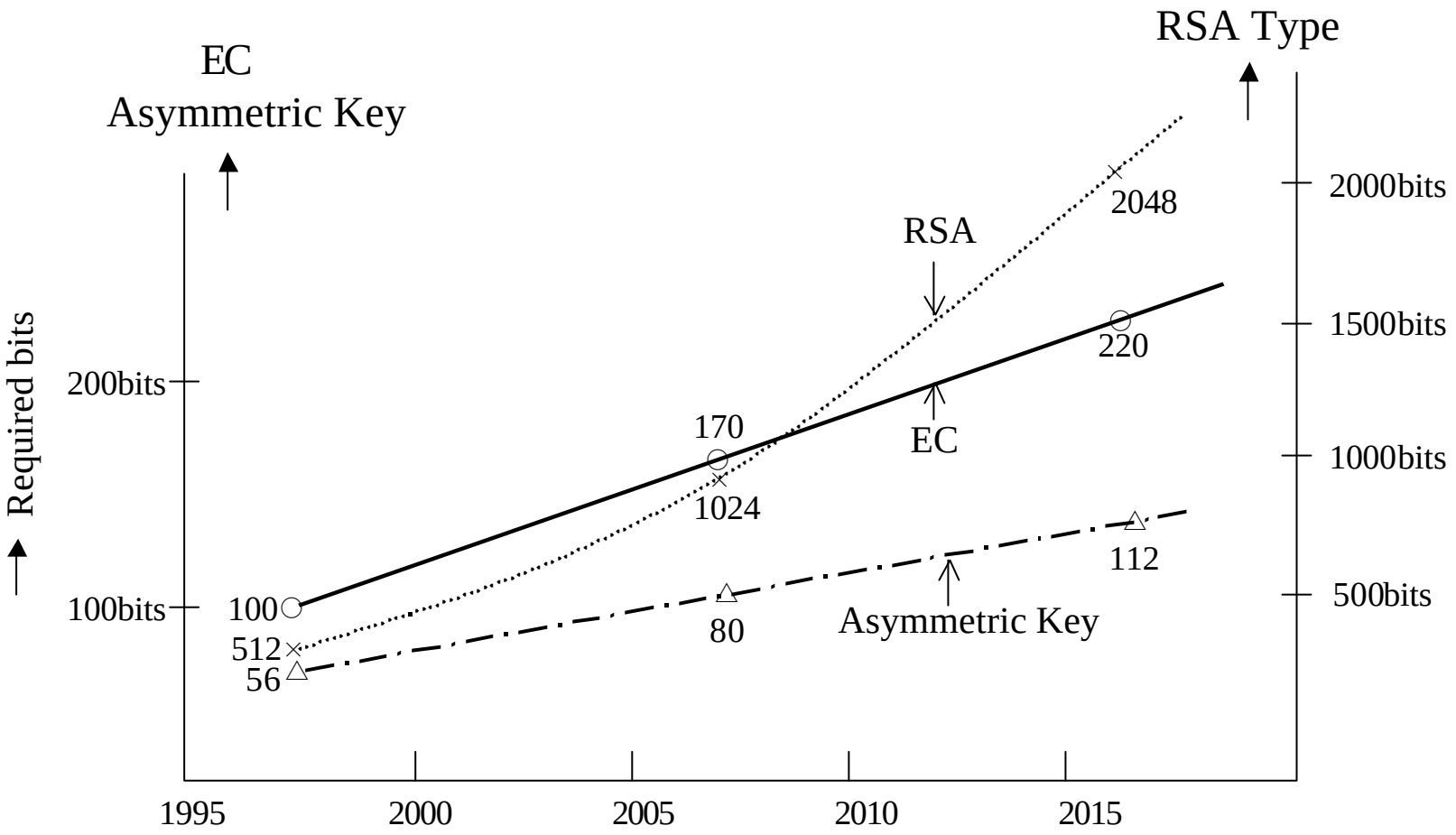



Fig.7 Comparison of Required Bits of Key Length

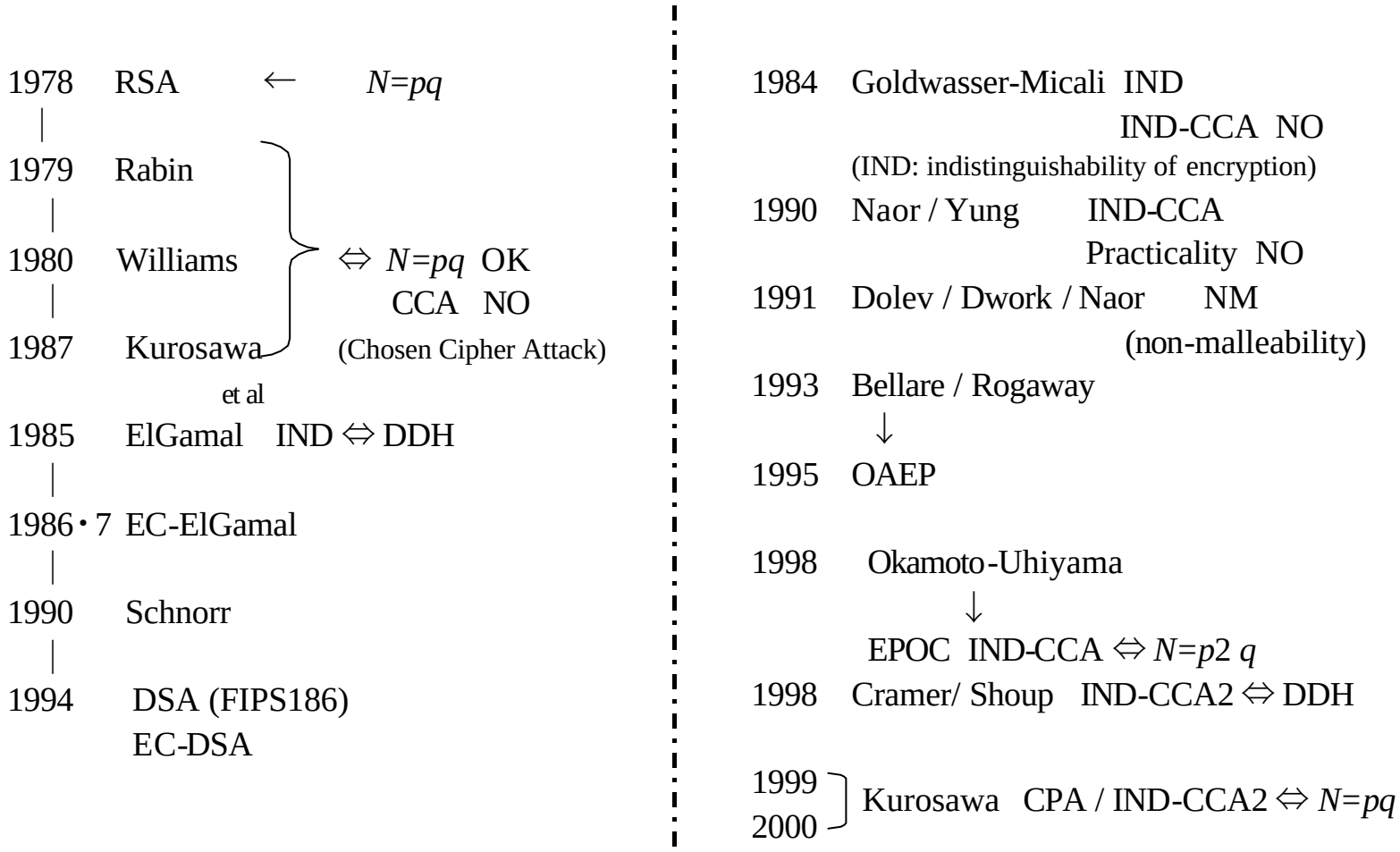



Fig.8 History of development of public key cryptosystems that enjoy practicality and provable security simultaneously against adaptive chosen ciphertext attack under standard intractability assumptions

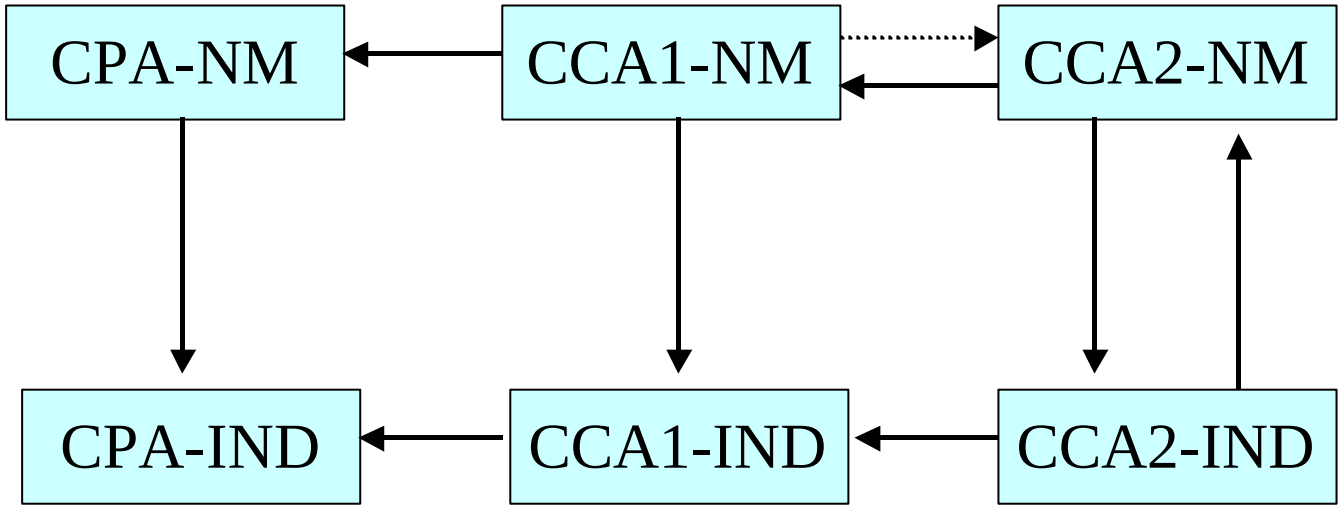



Fig.9 Security Level

| Mathematical Problem | | Encryption / Signature | Encryption only | Signature only |
|---|---|---|---|---|
| FP | $N = pq$<br>$N = p^2q$ | RSA<br>Rabin<br>Kurosawa | OAEP<br>EPOC | ESIGN<br>TDH-ESIGN<br>PSS |
| DLP | $y = g^x \bmod p$<br>$x = ?$ | | ElGamal<br>Cramaer-Shoup | ElGamal<br>DSA<br>R-ElGmal |
| | $Q = mp$<br>$m = ?$ | | EC-ElGmal<br>EC-Cramer-Shoup） | EC-ElGmal<br>EC-DSA<br>EC-R-ElGmal |

Revised and Translated from Discussion Paper No.98-J-28 (p8) of IMES (Institute for Monetary and Economic studies Bank of Japan by Une and Okamoto (in Japanese).

Fig.10　Public Key Cryptosystem

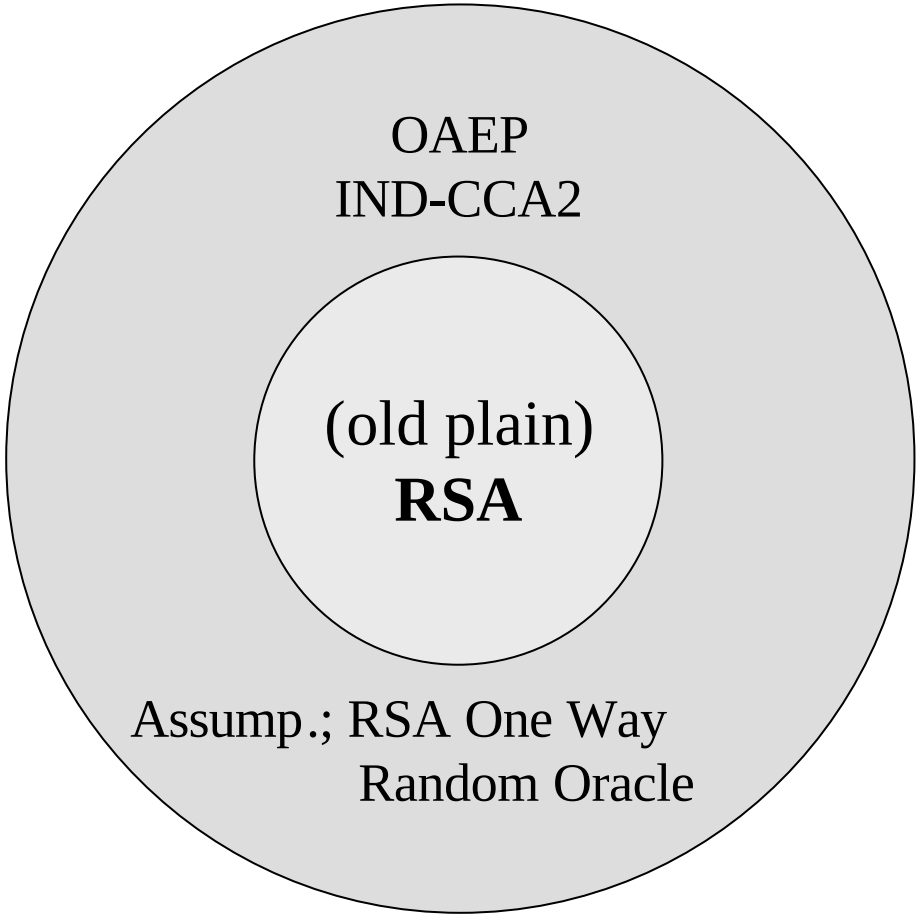
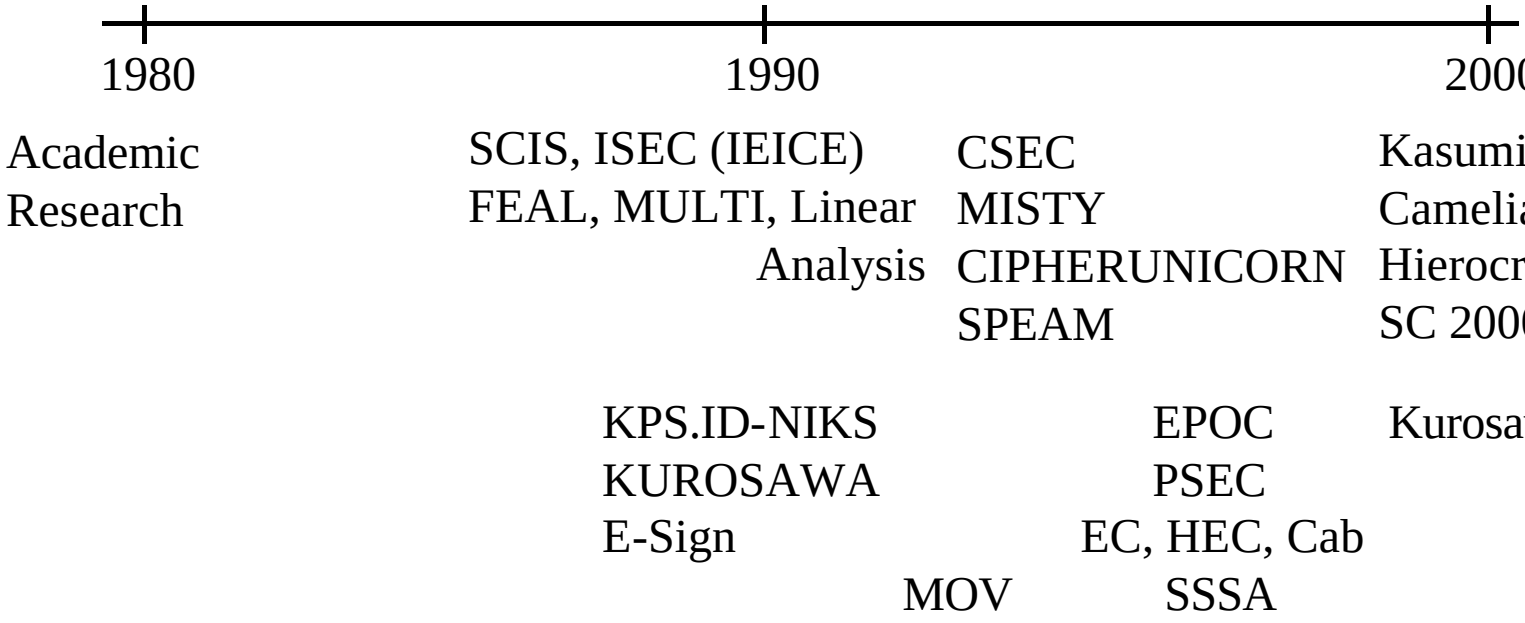



Fig.11 From RSA to OAEP




**Government** MITI, MPT, Police, IPA, TAO (1995~2000 project)
**International** ISO, ITU, OECD

Fig.12 Activity in Japan