

Fig.5 Lawful authorization to electronic signature and certification

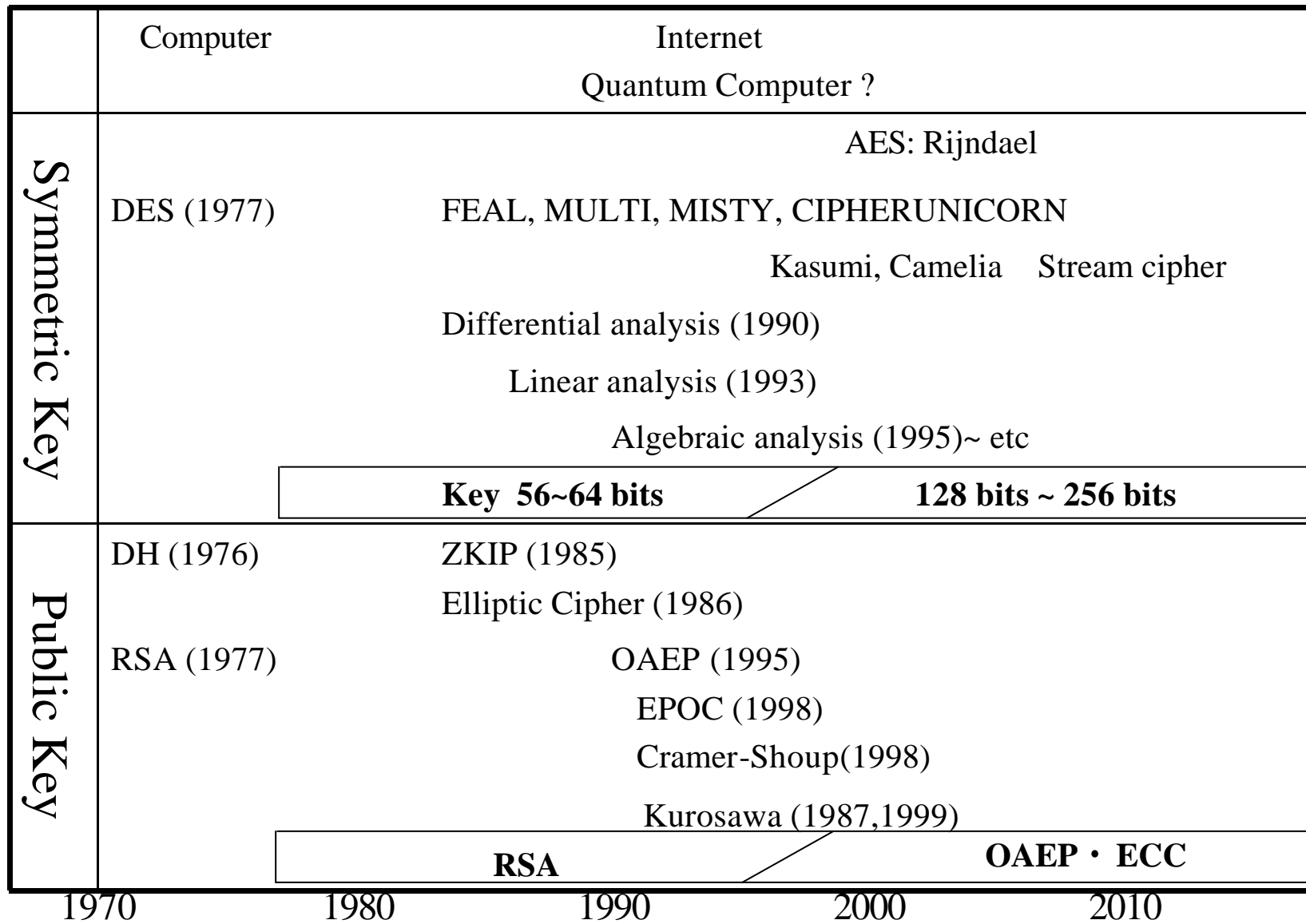


Fig.6 Development of Cryptosystems

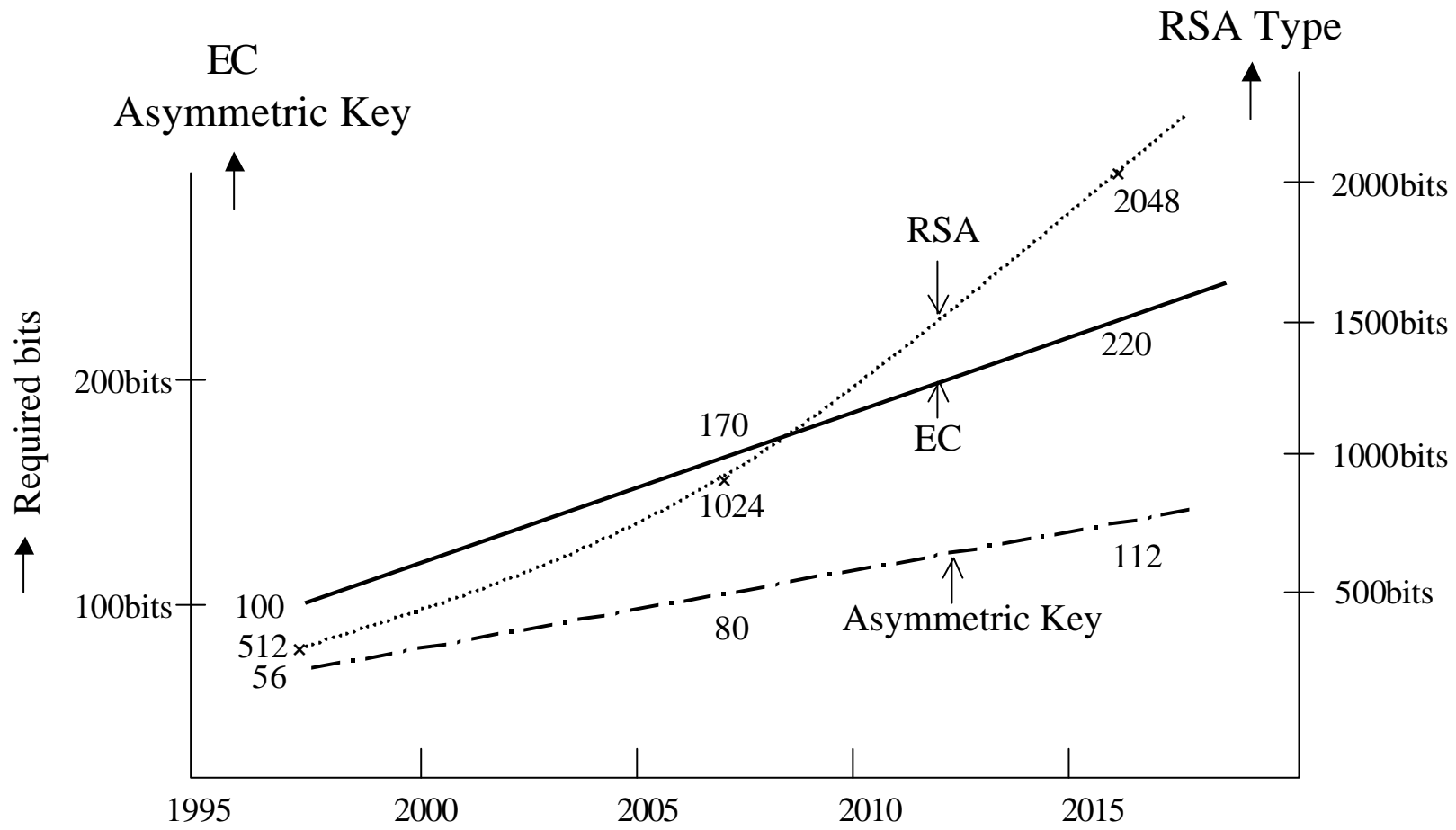


Fig.7 Comparison of Required Bits of Key Length

1978	RSA		$N=pq$						
1979	Rabin	}	$N=pq$	OK	CCA	NO	(Chosen Cipher Attack)		
1980	Williams								
1987	Kurosawa								
	et al								
1985	ElGamal	IND		DDH					
1986•7	EC-ElGamal								
1990	Schnorr								
1994	DSA (FIPS186)								
	EC-DSA								
1984	Goldwasser-Micali	IND							
		IND-CCA		NO					
		(IND: indistinguishability of encryption)							
1990	Naor / Yung	IND-CCA							
		Practicality		NO					
1991	Dolev / Dwork / Naor	NM							
		(non-malleability)							
1993	Bellare / Rogaway								
1995	OAEP								
1998	Okamoto-Uhiyama								
		EPOC		IND-CCA		$N=p^2 q$			
1998	Cramer/ Shoup	IND-CCA2		DDH					
1999	Kurosawa	CPA / IND-CCA2	$N=pq$						
2000									

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

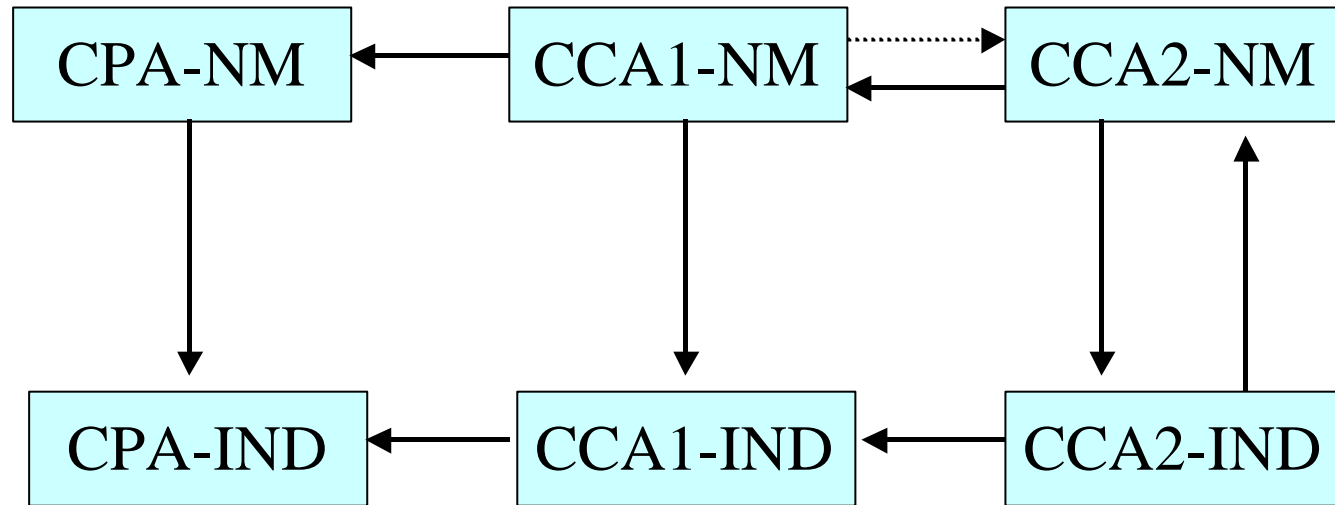


Fig.9 Security Level

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

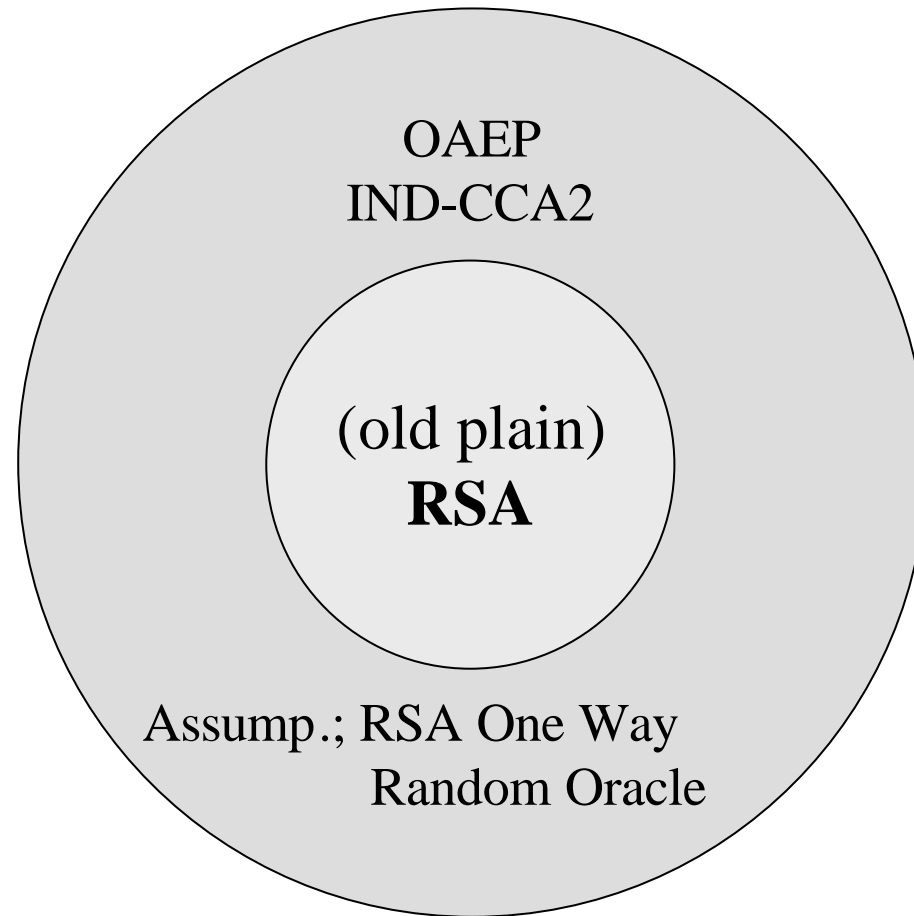


Fig.11 From RSA to OAEP

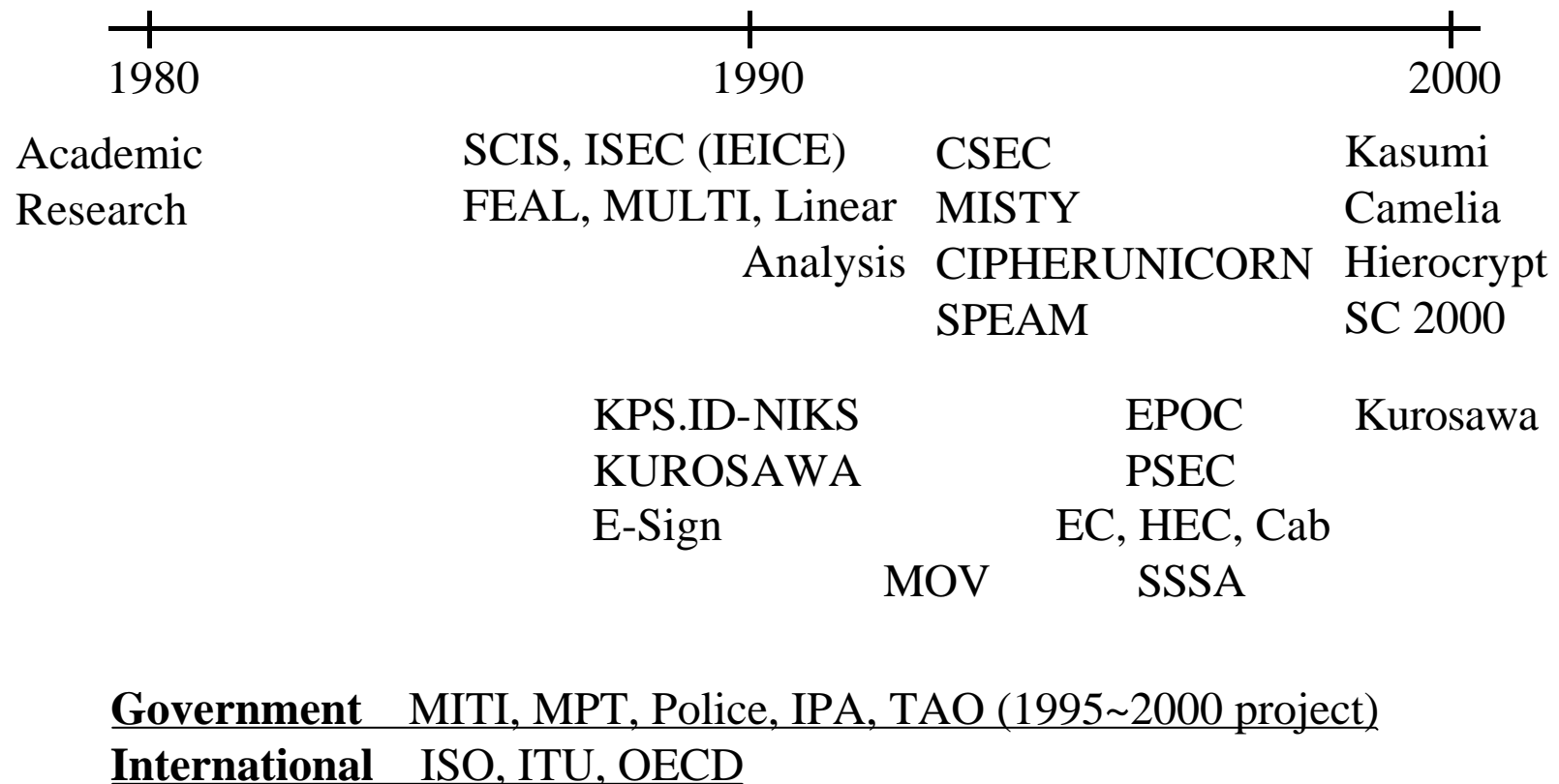


Fig.12 Activity in Japan