

Number theory based public-key cryptography

Paul Dumais, Halloween 2002

Public-key cryptosystem	Underlying presumably hard problem	Randomized encryption?	Secure against chosen-ciphertext attacks?	Semantically secure (assuming that the problem is hard) ?
RSA	RSA	No	No	No
Rabin	SQROOT	No	No	No
Blum-Goldwasser	SQROOT	Yes	No	Yes
Goldwasser-Micali	QR	Yes	No	Yes
El-Gamal	DH	Yes	No	No