List of Acronyms

Advanced Encryption Standard	AES
Bilinear Diffie-Hellman Problem	BDHP
Bilinear Paring	BP
Certificate Authority	CA
CA-based Public Key Cryptography	CA-PKC
Certificateless Digital Signature	CL-DS
Certificateless Public Key Cryptography	CL-PKC
Computational Diffie-Hellman Problem	CDHP
Data Encryption Standard	DES
Decisional Diffie-Hellman Problem	DDHP
Diffie-Hellman	DH
Digital Signature	DS
Elliptic Curve Cryptography	ECC
Elliptic Curve Discrete Logarithm Problem	ECDLP
Elliptic Curve Factorization Problem	ECFP
Elliptic Curve Scalar Point Multiplication	ECPM
Existential Unforgeability against Adaptive Chosen Message Attack	EUF-CMA
International Data Encryption Algorithm	IDEA
Identity-based Cryptosystem	IBC
Identity-based Encryption/Decryption	IBE
Identity-based Partially Blind Signature	ID-PBS
Identity-based Two-party Authenticated Key Agreement	ID-2PAKA
Key Generation Center	KGC
Key Off-set Attack	KOA

Key Replicating Attack	KRA
Key-compromise Impersonation	K-CI
Known Session-specific Temporary Information Attack	KSSTIA
Known-key Attack	K-KA
Map-to-point	MTP
Message Digest 5	MD5
Mutual Authentication	MA
No Key Control	NKC
Off-line Password Guessing Attack	OPGA
Parallel Guessing Attack	PGA
Password-based Authenticated Key Agreement	PAKA
Perfect Forward Security	PFS
Personal Digital Assistant	PDA
PKG Forward Security	PKG-FS
Private Key Generator	PKG
Public Key Cryptography	PKC
Public Key Infrastructure	PKI
Reflection Attack	RA
Ron's Code 4	RC4
Rivest-Shamir-Addleman	RSA
Secure Hash Algorithm	SHA
Self-certified Public Key Cryptography	SC-PKC
System Authority	SA
Two-party Authenticated Key Agreement	2PAKA
Unknown Key-share Attack	UKA
Weak Diffie-Hellman Problem	WDHP