LECTURE NOTES

Hard Problems in Cryptography

Classical Assumptions and Post-Quantum Foundations

Factoring · Discrete Log · Lattices · Codes · Hash-Based · Isogenies

Ji, Yonghyeon

Classical hardness assumptions and post-quantum reductions

Hard Problems in Cryptography: Classical Assumptions and Post-Quantum Foundations

Ji, Yonghyeon

February 14, 2026

Contents

Hard Problem	Cryptosystems	Major Attacks	Complexity (Best Known)
Integer Factorization	RSA, Rabin	General Number Field Sieve (GNFS)	Sub-exponential (Classical) $L_n[1/3, \sqrt[3]{64/9}]$
		Quadratic Sieve (QS)	Sub-exponential (Classical) $L_n[1/2, 1]$
		Shor's Algorithm	Polynomial (Quantum) $O((\log N)^2)$
Discrete Logarithm (DLP) *(Finite Fields)*	Diffie-Hellman, DSA, ElGamal	Number Field Sieve (NFS)	Sub-exponential (Classical) $L_p[1/3, \sqrt[3]{64/9}]$
		Index Calculus	Sub-exponential (Classical) $L_p[1/2, \sqrt{2}]$
		Shor's Algorithm	Polynomial (Quantum) $O((\log N)^2)$
Elliptic Curve DLP (ECDLP)	ECDH, ECDSA, EdDSA	Pollard's Rho / Kangaroo	Exponential (Classical) $O(\sqrt{n})$
		MOV Attack (Supersingular curves only)	Reduces to Finite Field DLP $L_n[1/3, c]$
		Shor's Algorithm	Polynomial (Quantum) $O((\log n)^2)$
Lattice Problems (LWE, SIS, SVP, CVP)	Kyber (ML-KEM), Dilithium (ML-DSA), NTRU, FHE	Lattice Reduction (LLL, BKZ)	Exponential (Classical/Quantum) $2^{O(d)}$
		Sieve Algorithms	Exponential (Classical) $2^{O(d)}$
Code-Based (Syndrome Decoding)	McEliece, HQC, BIKE	Information Set Decoding (ISD) (e.g., Stern, Lee-Brickell)	Exponential (Classical/Quantum) $2^{O(n/\log n)}$
		Grover's Search	Quadratic Speedup only (Halves the exponent)
Isogeny Problems	SQISign, CSIDH *(SIKE is broken)*	Castryck-Decru Attack (Specific to SIDH/SIKE)	Polynomial (Classical) **Broken**
		Meet-in-the-Middle / Delfs-Galbraith	Exponential (Classical) $O(p^{1/4})$
		Kuperberg's Algorithm	Sub-exponential (Quantum) $L[1/2]$ (Commutative only)

Continued on next page

Hard Problem	**Cryptosystems**	**Major Attacks**	**Complexity (Best Known)**
Hash-Based (Collision / Preimage)	SPHINCS+, XMSS, LMS	Birthday Attack (Collision)	Exponential $O(2^{n/2})$
		Grover's Algorithm (Preimage)	Exponential (Quantum) $O(2^{n/2})$
Multivariate (MQ) (Solving Quadratic Systems)	UOV, MAYO *(Rainbow is broken)*	MinRank / Kipnis-Shamir	Exponential (Classical)
		XL Algorithm (Groebner Basis)	Exponential (generally)
		Beullens' Attack (Specific to Rainbow)	Polynomial (Classical) **Broken**

Table 1: Comprehensive Summary of Hard Cryptographic Problems and Attacks

Hard Problem	Cryptosystems	Major Attacks	Complexity (best known)
Integer Factorization	RSA, Rabin	General Number Field Sieve (GNFS)	Sub-exponential (classical) $L_N\left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right]$
		Quadratic Sieve (QS)	Sub-exponential (classical) $L_N\left[\frac{1}{2}, 1\right]$
		ECM (small prime factors)	Heuristic $\approx \exp\left(\sqrt{2 \log p \log \log p}\right)$ for factor p
		Shor (quantum)	Polynomial in $\log N$ (quantum) $\text{poly}(\log N)$
Discrete Logarithm (DLP) *(finite fields)*	Diffie–Hellman, DSA, ElGamal	Number Field Sieve for DL (NFS-DL)	Sub-exponential (classical) $L_p\left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right]$
		Index Calculus (classical; group-dependent)	Sub-exponential (classical) typically $L_p\left[\frac{1}{2}, c\right]$
		Pohlig–Hellman (if $\lvert G\rvert$ smooth)	Polynomial in $\log p$ given smooth factorization of $\lvert G\rvert$
		Shor (quantum)	Polynomial in $\log p$ (quantum) $\text{poly}(\log p)$
Elliptic Curve DLP (ECDLP)	ECDH, ECDSA, EdDSA	Pollard ρ / Kangaroo (generic)	Exponential (classical) $\tilde{O}(\sqrt{n})$ group ops
		MOV / Frey–Rück (special curves only)	Reduces to finite-field DLP (curve-dependent)
		Shor (quantum)	Polynomial in $\log n$ (quantum) $\text{poly}(\log n)$
Lattice Problems (SVP, CVP, LWE, SIS)	Kyber (ML-KEM), Dilithium (ML-DSA), NTRU, FHE	BKZ/LLL basis reduction (core primitive)	Parameterized by dimension d: typically $2^{\Theta(d)}$ (classical)
		Enumeration (primal) / Dual attacks (LWE)	$2^{\Theta(d)}$ (classical), constants depend on BKZ blocksize

Continued on next page

Hard Problem	Cryptosystems	Major Attacks	Complexity (best known)
		Sieving for SVP (heuristic)	$\approx 2^{cd}$ with known $c < 1$ (classical heuristic)
		Quantum speedups (search/sieving subroutines)	No known Shor-like poly-time; typically improves constants/exponents in $2^{\Theta(d)}$
Code-Based (Syndrome Decoding)	McEliece, HQC, BIKE	Information Set Decoding (ISD) (Prange, Stern, Dumer, BJMM, ...)	Exponential (classical) $\approx 2^{\Theta(n)}$ (instance/params dependent)
		Structural attacks (if code not pseudorandom)	Often polynomial if exploitable structure exists
		Grover-type quantum speedups	Typically reduces brute-force layers (often "halves" exponents in idealized models)
Isogeny Problems	SQISign, CSIDH *(SIDH/SIKE broken)*	Castryck–Decru (SIDH/SIKE-specific)	Polynomial-time key recovery for those schemes **Broken (protocol-specific)**
		Meet-in-the-middle / Delfs–Galbraith (path finding)	Heuristic $\tilde{O}(p^{1/4})$ for supersingular path-finding variants
		Classical random-walk / graph search	Roughly $\tilde{O}(p^{1/2})$ in naive models
		Kuperberg-type (quantum; abelian hidden shift)	Sub-exponential (quantum) $\exp\left(O(\sqrt{\log p \, \log\log p})\right)$ (commutative settings)
Hash-Based (Collision / Preimage)	SPHINCS+, XMSS, LMS	Birthday attack (collisions)	$\Theta(2^{n/2})$ evaluations for n-bit outputs
		Generic preimage search	$\Theta(2^n)$ evaluations (classical)
		Grover (quantum preimage)	$\Theta(2^{n/2})$ quantum queries (idealized)

Continued on next page

Hard Problem	**Cryptosystems**	**Major Attacks**	**Complexity (best known)**
Multivariate (MQ) (Quadratic systems)	UOV, MAYO *(Rainbow broken)*	Gröbner basis (F4/F5), XL / relinearization	Exponential in n in general; governed by degree of regularity
		Hybrid attacks (guess variables + algebraic solve)	Exponential; trades time for memory / guessing
		MinRank / Kipnis–Shamir (scheme-structure dependent)	Often subexponential-to-exponential; can be polynomial for weak parameters
		Beullens-type attacks (Rainbow-specific)	Practical/polynomial-time breaks for Rainbow variants **Broken (protocol-specific)**

Table 2: Hard problems in cryptography: canonical systems, major attacks, and best-known asymptotic complexities (high-level).

1 Preliminaries

Security parameter and asymptotics

Security parameter. Cryptographic families are indexed by a security parameter $\lambda \in \mathbb{N}$. All objects (groups, moduli, dimensions, etc.) are efficiently generated from 1^λ. A function $\mu : \mathbb{N} \to \mathbb{R}_{\geq 0}$ is *negligible* if for every $c > 0$, there exists λ_0 such that for all $\lambda \geq \lambda_0$,

$$\mu(\lambda) < \lambda^{-c}.$$

An event happens with *non-negligible* probability if its probability is not negligible.

Efficient algorithms and PPT adversaries. A *probabilistic polynomial-time* (PPT) algorithm $\mathcal{A}$ is a randomized algorithm running in time $\mathrm{poly}(\lambda)$ on inputs generated at security level λ. Probabilities are taken over the internal randomness of $\mathcal{A}$ and over all random choices made by experiment distributions.

Basic algebraic structures

Rings and fields. $\mathbb{Z}$ denotes the integers. For $q \geq 2$,

$$\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$$

is the ring of integers modulo q. If $q = p$ is prime, then $\mathbb{Z}_p \cong \mathbb{F}_p$ is a field. For a finite field $\mathbb{F}_q$ (with $q = p^r$), $\mathbb{F}_q^\times := \mathbb{F}_q \setminus \{0\}$ denotes its multiplicative group.

Groups. A (finite) group is a pair $(G, \circ)$ with associative operation, identity element e, and inverses for all elements. A group is *cyclic* if $G = \langle g \rangle$ for some $g \in G$. If $|G| = n$, then exponents are interpreted modulo n:

$$g^x := \underbrace{g \circ \cdots \circ g}_{x \text{ times}} \quad \text{and} \quad g^{x+n} = g^x.$$

Homomorphisms. A map $\varphi : G \to H$ between groups is a homomorphism if $\varphi(x \circ_G y) = \varphi(x) \circ_H \varphi(y)$. Its kernel is $\ker(\varphi) = \{x \in G : \varphi(x) = e_H\}$.

Probability and sampling notation

Uniform sampling. For a finite set S, the notation $x \xleftarrow{\$} S$ means x is sampled uniformly from S. More generally, $x \leftarrow \mathcal{D}$ means x is sampled from distribution $\mathcal{D}$.

Advantage in a distinguishing task. For distributions $\mathcal{D}_0, \mathcal{D}_1$ on a common sample space and a (randomized) distinguisher $\mathcal{A}$ outputting a bit, define

$$\mathrm{Adv}_{\mathcal{A}}(\mathcal{D}_0, \mathcal{D}_1) := \left| \Pr_{x \leftarrow \mathcal{D}_0}[\mathcal{A}(x) = 1] - \Pr_{x \leftarrow \mathcal{D}_1}[\mathcal{A}(x) = 1] \right|.$$

A distinguishing advantage is *negligible* if it is negligible in λ.

Bitstrings and encodings

Bitstrings. $\{0,1\}^*$ is the set of all finite bitstrings; $\{0,1\}^n$ denotes bitstrings of length n. Concrete mathematical objects (integers, group elements, matrices) are assumed to have fixed, efficient encodings as bitstrings, so they can be given to algorithms.

Integers and arithmetic

Divisibility and gcd. For $a, b \in \mathbb{Z}$, $a \mid b$ means $\exists k \in \mathbb{Z}$ with $b = ak$. The greatest common divisor is $\gcd(a, b)$.

RSA-type moduli. A common distribution for factorization hardness is

$$N = pq$$

where p, q are distinct random primes of prescribed bit-length.

Linear algebra over finite fields

Vector spaces. For a finite field $\mathbb{F}_q$, $\mathbb{F}_q^n$ is an n-dimensional vector space. Matrices $A \in \mathbb{F}_q^{m \times n}$ act on vectors by multiplication.

Inner product modulo q. For $a, s \in \mathbb{Z}_q^n$,

$$\langle a, s \rangle := \sum_{i=1}^{n} a_i s_i \pmod{q}.$$

Normed spaces and geometry of numbers

Euclidean norm. For $x \in \mathbb{R}^n$,

$$\|x\|_2 := \sqrt{\sum_{i=1}^{n} x_i^2}.$$

(Other norms, e.g. $\|\cdot\|_\infty$, may be used depending on the lattice problem.)

Distance to a set. For $t \in \mathbb{R}^n$ and $S \subseteq \mathbb{R}^n$,

$$\operatorname{dist}(t, S) := \inf_{x \in S} \|t - x\|.$$

Lattices (basic definitions used later)

Lattice and basis. A full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ is

$$\mathcal{L}(B) = \{Bz : z \in \mathbb{Z}^n\}$$

for an invertible matrix $B \in \mathbb{R}^{n \times n}$ whose columns form a basis.

Determinant / covolume. $\det(\mathcal{L}) := |\det(B)|$ is independent of the chosen basis and equals the volume of a fundamental parallelepiped.

Successive minima. The first successive minimum is

$$\lambda_1(\mathcal{L}) := \min\{\|x\|_2 : x \in \mathcal{L} \setminus \{0\}\}.$$

Coding theory preliminaries

Hamming weight and distance. For $x \in \mathbb{F}_q^n$,

$$w_H(x) = |\{i : x_i \neq 0\}|, \qquad d_H(x,y) = w_H(x-y).$$

Linear codes. A linear $[n,k]_q$ code is a k-dimensional subspace $C \subseteq \mathbb{F}_q^n$. Generator and parity-check descriptions are equivalent:

$$C = \{uG : u \in \mathbb{F}_q^k\} \quad \text{and} \quad C = \{c \in \mathbb{F}_q^n : Hc^\top = 0\}.$$

Elliptic curves and finite-field preliminaries

Finite fields and extensions. For prime p, $\mathbb{F}_{p^2}$ is the degree-2 extension of $\mathbb{F}_p$. Elliptic curves in isogeny-based cryptography are often defined over $\mathbb{F}_{p^2}$.

Elliptic curves (minimal facts). An elliptic curve $E/\mathbb{F}_q$ is a smooth projective genus-one curve with a chosen base point, whose $\mathbb{F}_q$-rational points $E(\mathbb{F}_q)$ form a finite abelian group.

Morphisms and degree. A nonconstant rational map between curves has an associated (algebraic) degree. An *isogeny* is a morphism $E_1 \to E_2$ that is also a group homomorphism.

Hash-function preliminaries

Function families. A hash is typically modeled as a family $\{H_\lambda\}$ where each

$$H_\lambda : \{0,1\}^* \to \{0,1\}^{n(\lambda)}$$

is efficiently computable.

Search vs. decision vs. distinguishing. Many hardness notions can be expressed as:

- *Search*: output a witness (e.g. a factor, a discrete log, an error vector).
- *Decision*: decide existence of a witness.
- *Distinguishing*: tell apart two distributions (e.g. LWE vs. uniform).

2 Integer Factorization Problem (IFP)

Search problem (Factorization). Given an odd composite integer $N \in \mathbb{Z}_{\geq 2}$ (often $N = pq$ with distinct primes p, q), output a nontrivial factor d such that

$$1 < d < N \quad \text{and} \quad d \mid N.$$

Equivalently, output the prime factorization of N.

Hardness assumption (RSA distribution). Let $\mathcal{D}_\lambda$ output $N = pq$ where p, q are random λ-bit primes. The assumption states: no PPT algorithm factors $N \leftarrow \mathcal{D}_\lambda$ with non-negligible probability in λ.

Standard attacks (classical).

- **Trial division / Pollard** $p - 1$: effective when $p - 1$ is smooth.
- **Pollard** ρ: heuristic $O(\sqrt{p})$ time to find a factor p.
- **ECM (Elliptic Curve Method)**: best for finding relatively small prime factors.
- **QS (Quadratic Sieve)**: subexponential; good for moderate sizes.
- **GNFS (General Number Field Sieve)**: asymptotically fastest for general N.
- **SNFS (Special NFS)**: faster than GNFS when N has special form.
- **Implementation/key-gen weaknesses**: shared primes, partial key leakage, smoothness, side-channels.

Quantum attack. **Shor's algorithm** factors in time polynomial in $\log N$ on a fault-tolerant quantum computer.

3 Discrete Logarithm Problem (DLP)

Setting. Let G be a finite cyclic group (written multiplicatively) of order n, with generator $g \in G$.

Search DLP. Given g and $h \in G$, find $x \in \mathbb{Z}_n$ such that

$$g^x = h.$$

The solution is unique modulo n and is denoted $x = \log_g(h)$.

Hardness assumption. For a family $\{G_\lambda\}$, no PPT algorithm recovers x from $(g, h = g^x)$ with non-negligible probability over random g (generator) and random x.

Standard attacks (classical).

- **Generic attacks** (all groups): baby-step/giant-step; Pollard ρ in $\tilde{O}(\sqrt{n})$ time.
- **Pohlig–Hellman**: reduces DLP to prime-power factors of n; devastating if n is smooth.
- **Index calculus** (finite fields): subexponential; includes **NFS-DL** variants.
- **Special-curve pitfalls** (elliptic curves): MOV/Frey–Rück reductions for pairing-friendly/special curves.
- **Side-channel/implementation**: timing, power, fault attacks against exponentiation/scalar multiplication.

Quantum attack. **Shor's algorithm** solves DLP in abelian groups in polynomial time (in $\log n$).

4 Lattices (SVP/CVP and LWE)

3.1 Lattices

Definition (lattice). A full-rank lattice $\mathcal{L} \subset \mathbb{R}^n$ is a discrete subgroup: given linearly independent $b_1, \ldots, b_n \in \mathbb{R}^n$,

$$\mathcal{L} = \mathcal{L}(B) = \left\{ \sum_{i=1}^{n} z_i b_i : z_i \in \mathbb{Z} \right\}, \quad B = [b_1 | \cdots | b_n].$$

Define the first successive minimum

$$\lambda_1(\mathcal{L}) = \min\{\|v\|_2 : v \in \mathcal{L} \setminus \{0\}\}.$$

3.2 SVP and CVP

SVP (Shortest Vector Problem). Given a basis B of $\mathcal{L}$, find $v \in \mathcal{L} \setminus \{0\}$ such that $\|v\|_2 = \lambda_1(\mathcal{L})$.

γ-SVP (Approximate SVP). Given B and $\gamma \geq 1$, find $v \in \mathcal{L} \setminus \{0\}$ with

$$\|v\|_2 \leq \gamma \cdot \lambda_1(\mathcal{L}).$$

CVP (Closest Vector Problem). Given B and a target $t \in \mathbb{R}^n$, find $v \in \mathcal{L}$ minimizing $\|t - v\|_2$.

3.3 LWE (Learning With Errors)

Decision-LWE. Fix $n, q \geq 2$ and an error distribution χ over $\mathbb{Z}_q$. Given m samples $(a_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, distinguish:

$$\begin{aligned} \text{(LWE)} \quad & a_i \xleftarrow{\$} \mathbb{Z}_q^n,\ s \xleftarrow{\$} \mathbb{Z}_q^n,\ e_i \xleftarrow{\$} \chi,\ b_i = \langle a_i, s \rangle + e_i \pmod{q}; \\ \text{(Uniform)} \quad & (a_i, b_i) \xleftarrow{\$} \mathbb{Z}_q^n \times \mathbb{Z}_q. \end{aligned}$$

The *search* version asks to recover s.

Standard attacks (classical).

- **LLL/BKZ reduction** as the main engine (produces short/near-short vectors).
- **Primal attacks** (embedding to SVP/CVP) + enumeration/sieving.
- **Dual attacks** (find short dual vectors to distinguish LWE from uniform).
- **Hybrid attacks** (guess part of secret + lattice reduction).
- **BKW / combinatorial** attacks (parameter-dependent).
- **Algebraic attacks** in certain regimes (e.g. over-defined systems).

Quantum note. No known Shor-like polynomial-time algorithm for general lattice problems; quantum speedups mainly affect search/sieving constants/exponents.

5 Codes (Syndrome Decoding / Min Distance)

Linear code. A linear $[n, k]_q$ code is a k-dimensional subspace $C \subseteq \mathbb{F}_q^n$. A parity-check matrix $H \in \mathbb{F}_q^{(n-k)\times n}$ satisfies

$$C = \{c \in \mathbb{F}_q^n : Hc^\top = 0\}.$$

Hamming weight: $w_H(x) = |\{i : x_i \neq 0\}|$.

Syndrome Decoding (SD) — search form. Given $H \in \mathbb{F}_q^{(n-k)\times n}$, syndrome $s \in \mathbb{F}_q^{(n-k)}$, and bound t, find $e \in \mathbb{F}_q^n$ such that

$$He^\top = s \quad \text{and} \quad w_H(e) \leq t.$$

Minimum Distance Problem (MDP) — decision form. Given a linear code C and integer t, decide whether

$$\exists\, c \in C \setminus \{0\} \text{ with } w_H(c) \leq t.$$

Standard attacks (classical).

- **Information Set Decoding (ISD)** family: Prange, Stern, Dumer, BJMM-style improvements.
- **Structural attacks**: if the public code is not pseudorandom (hidden algebraic structure, rank defects, etc.).
- **Side-channel/implementation**: leakage from decoding routines or masking failures.

Quantum note. Grover-type search can improve brute-force components; quantum ISD analyses give model-dependent exponent reductions.

6 Isogenies (Supersingular Isogeny Problems)

Elliptic curve over a finite field. Over $\mathbb{F}_q$ (characteristic $\neq 2, 3$), an elliptic curve can be given by

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q, \quad \Delta \neq 0,$$

and $E(\mathbb{F}_q)$ is a finite abelian group.

Isogeny. An isogeny $\varphi : E_1 \to E_2$ over $\mathbb{F}_q$ is a nonconstant morphism defined over $\mathbb{F}_q$ that is also a group homomorphism. Its kernel is finite; $\deg(\varphi)$ is its morphism degree.

Supersingular Isogeny Problem (one common search form). Work over $\mathbb{F}_{p^2}$. Given supersingular elliptic curves $E, E'/\mathbb{F}_{p^2}$, find an explicit isogeny

$$\varphi : E \to E'$$

of prescribed smooth degree (often ℓ^r for small prime ℓ), represented so φ is evaluable.

Standard attacks (classical).

- **Isogeny-graph path search**: treat curves as vertices, ℓ-isogenies as edges.
- **Meet-in-the-middle** / bidirectional search to find paths faster than naive random walk.
- **Protocol-specific cryptanalysis**: some isogeny protocols have been broken (do not assume all are secure).

Quantum note. Known quantum algorithms can improve generic path-finding exponents in isogeny graphs; no known general polynomial-time algorithm.

7 Multivariable (Multivariate Quadratic, MQ)

Setting (systems of polynomial equations). Let $\mathbb{F}_q$ be a finite field. Let $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ be polynomials.

MQ (Multivariate Quadratic) — search problem. Given m quadratic polynomials

$$f_i(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n], \quad \deg(f_i) \leq 2,$$

find a solution $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ such that

$$f_i(x) = 0 \quad \text{for all } i = 1, \ldots, m.$$

(Decision variant: decide whether such an x exists.)

Standard attacks (classical).

- **Gröbner basis** methods: F4/F5; complexity driven by degree of regularity and sparsity.
- **XL / variants** (eXtended Linearization) and relinearization methods.
- **Hybrid attacks**: guess some variables to reduce to smaller systems, then algebraic solve.
- **Rank attacks / MinRank** reductions for structured schemes (oil-vinegar-type, etc.).
- **Linearization traps**: if parameters make the system overdetermined/easy.

Quantum note. Grover can speed up variable-guessing layers; algebraic-solving quantum speedups are limited and highly model/instance-dependent.

8 Hash functions (Formal notions and Generic bounds)

Hash family. A hash family $\{H_\lambda\}$ is a set of efficiently computable functions

$$H_\lambda : \{0,1\}^* \to \{0,1\}^{n(\lambda)}.$$

Collision resistance (CR). $\{H_\lambda\}$ is collision resistant if for every PPT adversary $\mathcal{A}$,

$$\Pr\left[(x, x') \leftarrow \mathcal{A}(1^\lambda) : x \neq x' \ \wedge \ H_\lambda(x) = H_\lambda(x')\right]$$

is negligible in λ.

Second-preimage resistance (SPR). For every PPT $\mathcal{A}$,

$$\Pr\left[x \leftarrow \mathcal{D};\ x' \leftarrow \mathcal{A}(1^\lambda, x) : x' \neq x \ \wedge \ H_\lambda(x') = H_\lambda(x)\right]$$

is negligible (for a specified distribution $\mathcal{D}$ over inputs).

Preimage resistance (one-wayness, OW). For every PPT $\mathcal{A}$,

$$\Pr\left[y \leftarrow \{0,1\}^{n(\lambda)};\ x \leftarrow \mathcal{A}(1^\lambda, y) : H_\lambda(x) = y\right]$$

is negligible.

Standard attacks.

- **Generic bounds**: collisions in about $2^{n/2}$ evaluations (birthday paradox), preimages in about 2^n evaluations.
- **Design-specific cryptanalysis**: differential/boomerang-style attacks; rotational/symmetry attacks; etc.
- **Chosen-prefix collisions** (for weakened designs).
- **Length extension**: for Merkle–Damgård hashes if misused as $H(k\|m)$; use HMAC to avoid.

Quantum attacks. **Grover** gives preimages in about $2^{n/2}$ quantum queries. (Quantum collision-finding can also improve over the classical birthday bound in some models.)