Colloquium Syllabus: Hard Problems in Cryptography

[Insert Colloquium / Study Group Name]

[Insert Dates / Term]

Colloquium Information

Colloquium:	**[Insert Colloquium / Study Group Name]**
Dates:	**[Insert Dates / Term]**
Meeting:	**[Insert Day/Time/Location or Zoom link]**
Organizer:	**[Insert Your Name]**
Contact:	**[Insert Email / Contact]**
Audience:	Masters/advanced undergrad; PhD welcome
Duration:	10 weeks (adjustable)
Format:	1 talk + 1 discussion session per week
Shared Notes/Repo:	**[Insert shared notes repo link (e.g., Overleaf/GitHub/Drive)]**

Purpose and Scope

This colloquium is a structured study group on the *hard computational problems* that underpin classical and post-quantum cryptography. The goal is to develop: (i) precise mathematical understanding of the problem statements and reductions, (ii) a working map of best-known classical and quantum attacks, and (iii) the ability to read research papers and standards documents critically.

The emphasis is on **conceptual mastery and communication**: each week one participant presents a topic, and the group collectively works through proof sketches, toy instances, and attack-selection reasoning.

Learning Goals

By the end of the colloquium, participants should be able to:

1. State formal definitions of major cryptographic hard problems (search/decision/distinguishing forms).
2. Explain the relationship between cryptosystems and assumptions (what is proved, what is conjectured).
3. Describe the main attack families and why they work (smoothness, meet-in-the-middle, lattice reduction, Groebner bases, etc.).

4. Do "security back-of-the-envelope" estimates using asymptotic/heuristic models.
5. Present a paper or survey section clearly, including assumptions, limitations, and open questions.

Prerequisites (Lightweight)

Participants should be comfortable with:

- Modular arithmetic; basic group/field concepts (cyclic groups, generators).
- Linear algebra (rank, nullspace, solving linear systems).
- Proof writing (clear quantifiers; reduction-style arguments).
- Helpful: probability (birthday bound intuition), computational complexity vocabulary.

A short "preliminaries handout" will be shared in the repo for those who need a refresh.

Structure of a Typical Week

Before the meeting (asynchronous, 60–120 minutes)

- **Assigned reading** (10–25 pages): survey section or textbook notes.
- **Presenter prep**: 25–35 minute talk with 3 deliverables:
  1. Formal problem definition(s) + at least one reduction or equivalent formulation.
  2. Attack taxonomy + one representative attack explained at "mechanism" level.
  3. A "parameter intuition" slide: what knob controls hardness?
- **All participants**: submit 1–2 questions in the repo (issue/discussion thread) before the session.

During the meeting (90 minutes recommended)

1. **Talk (30–40 min)** by the assigned presenter.
2. **Clarifying Q&A (10 min)**: definitions and notation only.
3. **Board session (30–40 min)**: work through 1–2 problems or a proof sketch together.
4. **Research discussion (10 min)**: what is known, what's open, what assumptions are fragile?

After the meeting (optional, 30 minutes)

- Presenter posts slides/notes + a short summary (half page).
- Group finalizes a "glossary" entry for key terms introduced that week.

Participation Norms and Roles

Roles

- **Presenter (rotating):** leads the talk; posts notes and 2 practice problems.
- **Discussant (rotating):** prepares 5–8 minutes of critique/questions; highlights potential pitfalls or alternative viewpoints.
- **Scribe (rotating):** maintains a clean set of notes and a list of unresolved questions.

Norms

- Prefer precise statements: specify distributions, quantifiers, and model assumptions.
- Ask "mechanism" questions: *why* does an attack work, not just its name.
- Be explicit about heuristics vs theorems (e.g., NFS complexity is heuristic; generic-group bounds are theorems).
- Keep the room inclusive: ask clarifying questions early; avoid gatekeeping jargon.

Assessment (Optional for a Study Group)

If you want light structure without "grades," use:

- **Completion badges:** 1 badge per talk presented + 1 per discussant role.
- **Portfolio:** each participant contributes 2 pages of notes during the term.
- **Mini-project (optional):** reproduce a toy attack (e.g., BSGS, Prange ISD, toy LLL) and write a 2–3 page report.

Core Reading Suggestions

- Boneh–Shoup, *A Graduate Course in Applied Cryptography* (widely used, clear).
- Katz–Lindell, *Introduction to Modern Cryptography* (formal games/assumptions).
- Topic notes: Cohen (factoring), Washington (EC), Micciancio–Goldwasser (lattices), MacWilliams–Sloane (codes), Cox–Little–O'Shea (Gröbner/MQ).

Schedule (10-week template; adjust as needed)

Wk	Theme	Colloquium Targets	Presenter Deliverables
0	Preliminaries	Security parameter; negligible; search/decision/distinguish; L-notation; birthday heuristic; group/field review	1-page notation sheet
1	Integer Factorization	Factoring vs $\varphi(N)$ vs order-finding; ECM/QS/GNFS overview; Shor concept	Reduction + one sieve mechanism
2	DLP in Finite Fields	DLP/CDH/DDH; BSGS/Pollard; Pohlig–Hellman; index calculus / NFS-DL	Worked BSGS example + PH outline
3	ECDLP	Why generic $\tilde{O}(\sqrt{n})$; Pollard ρ; MOV/Frey–Rück pitfalls; curve selection	Attack comparison: FF-DLP vs ECDLP
4	Lattices I	Lattices, duals, Minkowski; SVP/CVP; LLL/BKZ concepts	Derive dual lattice + Minkowski (2D)
5	Lattices II (LWE/SIS)	SIS/LWE definitions; primal/dual/hybrid/BKW attacks; parameter intuition	"attack selection" decision tree
6	Code-based Crypto	Syndrome decoding; McEliece; ISD (Prange → BJMM); structural attacks	Derive Prange probability + toy SD
7	Isogenies	Isogeny definition; graphs/path-finding; CSIDH-style actions; protocol-specific breaks; quantum hidden shift	Graph model + MITM heuristic
8	Multivariate (MQ)	MQ definition; Gröbner (F4/F5); XL/hybrid; MinRank/rank attacks; pitfalls	Worked MQ toy + attack taxonomy
9	Hash	CR/SPR/OW games; birthday bound proof; Merkle–Damgård length extension; HMAC; quantum Grover	Prove birthday bound + length extension demo
10	Synthesis / Projects	Compare classical vs quantum across families; security-level mapping; open problems	2-page reflective memo per participant

Presenter Template (Copy/Paste)

Each presenter should submit a short document (2–4 pages or 6–10 slides) containing:

1. **Formal definition(s)** (inputs, outputs, distributions).
2. **One reduction or equivalence** (oracle reduction or explicit transformation).
3. **Attack taxonomy** with 2–3 named attacks *and* one explained mechanistically.
4. **Complexity summary** (best-known asymptotics; note heuristic vs theorem).
5. **Two practice problems** (one computation/toy; one reasoning/reduction).

Code of Conduct (Short)

We aim for a respectful, collaborative environment. Critique ideas, not people. If conflict arises, contact the organizer privately and we will resolve it promptly.