AI-Driven Cryptography Research Roadmap

Deliverables, Milestones, Required Tools, and Expected Outcomes

✅ PHASE 1 — Foundation & Infrastructure (Months 1–6)

Goal: build the technical backbone to evaluate and attack crypto systems using AI

1. Neural Distinguisher Lab

Deliverables

- Dataset generator: produce ciphertext under random keys & reduced rounds
- PyTorch/TensorFlow training pipeline: CNN/ResNet classifiers
- Baseline distinguishers for standard ciphers:
  - SPECK32/64
  - PRESENT
  - GIFT
  - SKINNY
- Internal benchmark report: accuracy vs rounds

Outcome

- A working system that can "score" strength of symmetric primitives

Tools

- Python, PyTorch, GPU (even a single 3090/4090 is fine)
- Gohr's repo as template

2. S-Box & Round-Function Search System (Prototype)

Deliverables

- Genetic algorithm to generate S-box candidates
- Neural model to predict differential uniformity / nonlinearity
- Ranking system for candidate S-boxes

Outcome

- Automatic rejection of bad S-boxes without full brute-force evaluation

Tools

- Python, PyTorch, Gurobi (or open-source MILP solvers)

3. Stream Cipher Forensics Pipeline (Ciphertext Only)

Deliverables

- Rolling hash duplicate block detection
- FFT / autocorrelation engine for periodicity detection
- Bit extraction + Berlekamp–Massey implementation

Outcome

- Detect repeated keystream, PRNG collapse, XOR-cipher key length
- Publish internal report on IoT or malware traffic samples

Tools

- Python + numpy/scipy
- XORTool baseline comparison

Expected Publications (Phase 1)

- "Evaluation of Neural Distinguishers for Lightweight Ciphers"
- "Ciphertext-Only Detection of Stream Cipher Weakness Using FFT-Correlation"

✅ PHASE 2 — Advanced AI Cryptanalysis (Months 6–18)

Goal: produce publishable attacks and evaluation frameworks

4. Neural Distinguishers → Key Recovery

Deliverables

- Train distinguishers on reduced-round cipher
- Implement guided subkey search (neural-scored beam search)
- Compare attack complexity vs state-of-the-art

Outcome

- Demonstrate a practical key-recovery improvement on at least one lightweight cipher
- This is a real academic publication target (ToSC/CHES)

5. Full "Neural Evaluation Suite" for Symmetric Primitives

Deliverables

- API/CLI to input any candidate cipher
- Automatically:
  - generate datasets
  - train distinguishers
  - measure diffusion and avalanche

- run differential/linear estimators
- produce PDF or LaTeX security report

Outcome

- A reusable tool for researchers and designers
- Potentially adopted by external teams

Tools

- PyTorch, MILP/SAT, Python CLI, LaTeX generation

6. Side-Channel Deep Learning Engine

Deliverables

- Load ASCAD + ChipWhisperer datasets
- Train CNN and Transformer models for AES key byte recovery
- Rank leakage strength (traces required)
- Compare masked vs unmasked implementations

Outcome

- Practical evaluation system for hardware and embedded crypto

Tools

- PyTorch, ChipWhisperer board, ASCAD data

Expected Publications (Phase 2)

- Neural key-recovery on reduced-round cipher
- Deep-learning SCA effectiveness on masked implementations
- Open-source “Neural Evaluation Suite”

✅ PHASE 3 — Cryptographic Engineering & Audit Tools (Months 18–36)

Goal: build practical tools for real-world cryptographic security evaluation

7. AI-Assisted Cryptographic Code Auditor

Deliverables

- Static analysis detecting misuse:
  - ECB usage
  - nonce reuse
  - RNG misuse

    - missing tag verification
    - predictable IVs
- LLM or ML-ranked warnings
- Integration with CodeQL or Semgrep

Outcome

- Developer-friendly report: where and how crypto is misused

8. ML-Guided Fuzzing for Protocols

Deliverables

- RL-enhanced TLS or AEAD fuzzer
- Mutators guided by classifier confidence or branch coverage
- Discovery of error cases: padding oracle, tag bypass, handshake failures

Outcome

- Practical bugs found in open-source crypto libraries
- Publishable vulnerability reports + CVEs possible

9. Stream Cipher Classifier

Deliverables

- Train model to classify encrypted traffic as:
    - AES-CTR
    - ChaCha20
    - RC4
    - LFSR
    - weak XOR
- Detect keystream reuse from live traffic

Outcome

- Forensics / malware / IoT analysis tool

Expected Publications (Phase 3)

- “ML-Guided Detection of Keystream Reuse in IoT Traffic”
- “AI Auditor for Cryptographic API Misuse in Modern Codebases”
- “Reinforcement-Learning Fuzzing of TLS Handshake Implementations”

✅ PHASE 4 — Consolidation Into a Unified Platform (Years 3–5)

Goal: create a flagship deliverable with long-term value

10. AI Cryptographic Security Evaluation Platform

Deliverables

- Integrates:
  - Neural distinguishers
  - S-box/round-function search
  - Stream cipher forensics
  - Deep learning SCA
  - Code auditing
  - ML fuzzing
- Web dashboard and API
- Automatic PDF security assessment

Outcome

- Industrial-grade evaluation tool
- Usable by researchers, vendors, and auditors
- Potential for commercial licensing

✅ Required Resources (Minimal & Realistic)

- 1–3 GPUs (consumer: RTX 3090/4090 or A100 if available)
- Python, PyTorch, SciPy, MILP solver
- ChipWhisperer Lite (~$300) for side-channel evaluation
- Open-source datasets (ASCAD, public ciphers, IoT traces)

No quantum computers, huge clusters, or proprietary software needed.

✅ Expected Output & Value

Academic / Scientific Value

- Multiple CHES/ToSC/ESORICS/NDSS-level publications
- Open benchmarks and datasets
- Public tools that other researchers adopt

Industry Value

- Automated vulnerability detection for real crypto systems

- Hardware and IoT vendor evaluation
- Pentesting and forensics enhancement

Long-Term Vision

- Becoming a reference lab for AI-assisted cryptography testing

✅ Summary (One Paragraph)

This roadmap turns AI from a curiosity into a practical cryptographic weapon: a system that designs ciphers smarter, validates them faster, detects flaws earlier, breaks weak implementations, and audits real systems at scale. Every step yields measurable output: tools, datasets, evaluations, publications, vulnerabilities, and ultimately a unified platform capable of fully automated cryptographic security assessment. The approach is realistic, resource-efficient, and aligns with the research frontier where industry and academia are moving.