

Lili Tang 唐雳雳

Beijing, China tanglili@iie.ac.cn

ORCID Institution GitHub Blog Resume

SHORT BIO

I am a Ph.D. student in cybersecurity at the University of Chinese Academy of Sciences (**UCAS**), advised by Prof. Xiaorui Gong. I received my B.E. degree in information security from the University of Science and Technology of China (**USTC**) in 2022. Prior to 2026, I was actively involved in CTF competitions with the NeSE team, focusing on cryptography and blockchain.

My doctoral research focuses on applied cryptography, particularly the Generalized Birthday Problem and its cryptanalytic applications. Now I am focusing on **LLM post-training** and exploring the intersection of **AI and cryptography**. **I will graduate in June 2027 and am open to opportunities.**

RESEARCH INTERESTS

Large Language Models (LLM)

LLM post-training (SFT & RL). Advancing and benchmarking frontier models in cryptography and cybersecurity.

Cryptography + AI

Automated cryptanalysis and vulnerability discovery using LLM agents. Currently learning Lean 4 and formal verification for cryptography.

News

July, 2026 — I expect to complete my Ph.D. in **June 2027**. I'm looking for postdoctoral or other research positions in **LLM post-training, cryptography and AI, or cybersecurity**. If you find my research areas matching any opportunity, please feel free to contact me via email.

November, 2026 — We released our automated cryptanalysis results found by a MiniMax internal model. See our technical reports in **MiniMax Research**.

July, 2026 — Our joint work on using LLM agents to discover vulnerabilities in cryptographic libraries will be presented at the **Black Hat USA 2026 Briefings**. See the **talk page** for details.

Experience

Education

Ph.D. Candidate in Cybersecurity — Aug. 2022 – Ongoing
University of Chinese Academy of Sciences — Beijing, China
Straight-to-PhD. Major in Cybersecurity.

B.Eng. in Information Security — Aug. 2018 – Jul. 2022
University of Science and Technology of China — Hefei, China

Intern

Research Intern
MiniMax
Aug. 2026 – Present
Beijing, China

Post-training of MiniMax cyber models. Automated Cryptanalysis & AI for Security.

Post-Quantum Research Intern, Ant Research
Ant Group
Jul. 2026 – Aug. 2026
Beijing, China

Conducted security analysis of ML-DSA (Dilithium) and its implementation bugs.

Research Intern, Tencent Xuanwu Lab
Tencent Technology
Oct. 2025 – Mar. 2026
Beijing, China

Automated discovery of cryptography vulnerabilities using LLM agents.

Publications & Presentations

On the Regularity of the Generalized Birthday Problem

Crypto 2026

Lili Tang, Yao Sun, and Xiaorui Gong

The 46th International Cryptology Conference

> *TL;DR: We study structural regularity in the Generalized Birthday Problem and its impact on practical schemes including incremental hashing and Equihash. The main contribution of this work is the complexity analysis of regular and non-regular GBP, with important implications for the k-XOR and k-SUM problems.*

EPRINT CODE CCF-A CORE-A*

Memory Optimizations of Wagner's Algorithm with Applications to Equihash

CHES 2026

Lili Tang, Rui Ding, Yao Sun, and Xiaorui Gong

IACR Transactions on Cryptographic Hardware and Embedded Systems, 2026 (2)

> *TL;DR: We propose a new list-item-reduction framework that reduces the memory complexity of Wagner's algorithm from $2nN$ to nN bits, thereby weakening the ASIC resistance of Equihash. This optimization has important implications for the efficient implementation of Wagner-style algorithms.*

EPRINT CODE CCF-B CORE-A

k-Tree Revisited: Memory-Time Cost of Preimage Attack on Incremental Hashes

FSE 2027

Rui Ding*, **Lili Tang***, Shaomin Chen, and Xiaorui Gong * *Equal Contribution*

IACR Transactions on Symmetric Cryptology, 2026 (3)

> *TL;DR: We extend post-retrieval to Wagner's k-tree algorithm, reducing peak memory from exponential in k to $O(k^2\ell N)$ with only linear time overhead. Applied to preimage attacks on incremental hashes, this trade-off can substantially reduce their memory–time cost.*

EPRINT CODE CCF-B CORE-B

A Counterexample to Tokareva's Conjecture on Sums of Two Bent Functions

Preprint

Yansong Feng, Hao Jiang, Guancheng Li, Tianyi Li, and **Lili Tang**

arXiv

> *TL;DR: We disprove Tokareva's conjecture that every Boolean function on $\mathbb{F}_2^n$ of algebraic degree at most $n/2$ can be written as a sum of two bent functions, constructing explicit counterexamples for all even $n \geq 8$ via large-scale automated reasoning with LLM agents.*

ARXIV

Two-Bit Lifting for Ternary SIS: Polynomial-Time Collision Attacks on LtHash

Preprint

Rui Ding, Xiaorui Gong, Hao Jiang, and **Lili Tang**

IACR ePrint

> *TL;DR: We introduce two-bit lifting for ternary SIS, reducing the query complexity of polynomial-time LtHash collision attacks while preserving ternary coefficients. For LtHash16, the attack uses about 2^{81} hash queries.*

EPRINT

Talks & Presentations

Breaking the Unbreakable: Dismantling the Myth of Trusted Cryptographic Libraries

Black Hat USA

Guannan Wang, **Lili Tang**, and Guancheng Li *Speakers*

Black Hat USA 2026 Briefings · Aug 1-6, 2026 · Las Vegas · On Demand

LINK SLIDE

Capture The Flag (CTF)

CTF Team



NeSE Team
Institute of Information Engineering, UCAS
Crypto & Blockchain.

Mar. 2022 – Ongoing
Beijing, China
nese.team ↗



Nebula Team
USTC
Crypto & Reverse Engineering.

Oct. 2021 – Mar. 2022
Hefei, China
nebuu.la ↗

Selected Awards

2025 — **Crypto CTF 2025** — 2nd Place
NeSE's crypto team: tl2cents (me), deebato, and Threonine.
Captain · All Kill

2025 — **N1CTF 2025** — 1st Place
With NeSE

2025 — **0CTF 2025** — 2nd Place
With NeSE

2024 — **NSU-Crypto Olympiad 2024** — 2nd Place
Team: Lili Tang, Chenyu Li, and Hao Jiang
Silver Medal · Crypto · Olympiad

2024 — **CyberSecurityRumble Quals 2024** — 3rd Place
With NeSE · Top Contributor

2024 — **DEF CON CTF Qualifier 2024** — 9th Place
First independent team from mainland China to qualify for DEFCON Finals.
With NeSE

> **More about CTF**
>
> I was one of NeSE's top two contributors from 2022 to 2025. Over the same period, NeSE consistently ranked in **CTFtime**'s global top 10 teams (3rd in 2022, 7th in 2023, 8th in 2024, and 5th in 2025). See more awards at **nese.team** and related writeups on **my blog**. I also enjoy solving challenges on **CryptoHack** and completed all of them in July 2024, **ranking 24th** globally at the time.