XISEN TIAN

Monterey, CA | xisentian.github.io

xisen.tian1[at]nps.edu

Insightful, articulate, and adaptable Naval Engineering Duty Officer with research expertise in cryptography, operational experience in information warfare, and program management skills. Multidisciplinary collaborative researcher working with security experts around the world on secure messaging and post quantum cryptography.

EXPERIENCE

SPACE SYSTEMS PROGRAM MANAGER

U.S. Navy

2020 – 2022

Assistant program manager for 30-member team supporting two space programs valued at $1B+ and managed 41 cyber security assets across three Major Systems Acquisitions.

CRYPTOLOGIC WARFARE OFFICER

U.S. Navy

2015 – 2020

Deployed onboard USS CARL VINSON as Information Operations Watch Officer. Led 9-member team analyzing cyber-attacks against DOD Information Networks.

SUMMER RESEARCH INTERN

Portland State University & Various National Laboratories

2010 – 2014

Published research in organic photovoltaics at Portland State University. Researched datamining and Android security at Lawrence Livermore and Sandia National Laboratories, resp.

EDUCATION

PHD COMPUTER SCIENCE

Naval Postgraduate School | Monterey, CA

DEC 2025 (EXPECTED)

- Published research in areas of secure messaging, space network security, and post-quantum cryptography
- Authored standards adopted by the Internet Engineering Task Force

M.S. ELECTRICAL ENGINEERING

Naval Postgraduate School | Monterey, CA

2018 – 2020

- Conducted classified vulnerability analysis of a shipboard radar using machine learning techniques
- Awarded John Wozencraft Award for Outstanding Research in Electrical and Computer Engineering

B.S. (DUAL) COMP SCI & IT

U.S. Naval Academy | Annapolis, MD

2011 – 2015

- Published research in areas of natural language processing and parallel computation

SKILLS

- Defense Acquisition
- Computational cryptographic analysis
- Datamining, machine learning, network analysis

- Programming: Python, C, C++, Rust, Go
- Writing & Presenting: LaTeX, Markdown, HTML/CSS
- Public speaking

SELECTED PUBLICATIONS

NOTE: Publications in cryptography, as is in theoretical computer science and mathematics, list authors in alphabetical order to emphasize author equality in contribution

Dowling, B., Hale, B., <u>Tian, X.</u>, & Wimalasiri, B. (2025). Key Establishment in the Space Environment. *Arxiv*
> We propose to use continuous key agreement protocol for key establishment in popular space communications protocols over pre-shared keys and session based paradigms.

Dowling, B., Hale, B., <u>Tian, X.</u>, & Wimalasiri, B. (2025). Cryptography is Rocket Science: Analysis of BPSec. *IACR Communications in Cryptology*, *1*(4)
> We provide the first formal analysis of BPSec, a delay tolerant network security protocol standardized by the Internet Engineering Task Force and adopted by NASA and ESA that is used in deep space communications.

Joël A., Hale, B., Mularczyk, M., & <u>Tian, X</u>. (2025). *Flexible Hybrid PQ MLS Combiner*. Retrieved from Internet Engineering Task Force website: https://datatracker.ietf.org/doc/draft-ietf-mls-combiner/00/
> We provide an efficient combiner protocol for the Messaging Layer Security protocol to utilize post quantum (PQ) security without paying the PQ price each time messages are sent. Accompanying white paper in progress.

Fondevik, E. M., Hale, B., & <u>Tian, X</u>. (2023). Guardianship in Group Key Exchange for Limited Environments. *Cryptology ePrint Archive*
> We address how devices operating in limited environments (e.g. receive-only modes) can heal from compromises in secure group communications.

<u>Tian, X</u>. (2020). Commercial Radar Vulnerability Assessment. *Naval Postgraduate School Master's Thesis*. [CUI Classified Publication – available upon request]
> I reverse engineer a commercial radar and use a generative adversarial network to spoof radar imagery

Chambers, N., Bowen, V., Genco, E., <u>Tian, X</u>., Young, E., Harihara, G., & Yang, E. (2015, September). Identifying political sentiment between nation states with social media. In *Proceedings of the 2015 conference on empirical methods in natural language processing* (pp. 65-75)
> We describe an approach to large-scale modeling of sentiment analysis for the social sciences to model relations between nation states.

Khochtali, M., Roche, D. S., & <u>Tian, X</u>. (2015, July). Parallel sparse interpolation using small primes. In *Proceedings of the 2015 International Workshop on Parallel Symbolic Computation* (pp. 70-77)
> We present a parallel algorithm for sparse interpolation that uses small primes to reduce the number of operations required to interpolate a polynomial.

**References available upon request