Ahmet Ramazan AĞIRTAŞ
PhD, Cryptography

Skills

Low/Mid-level Military Management 18 yrs.

IT Management 10 years

Digital Signatures 9+ yrs.

Python 5+ yrs.

SageMath 5+ yrs.

Cryptographic Protocol Design 5+ yrs.

English

Turkish

Education

10/2015 - 02/2024

PhD, Cryptography

Middle East Technical University

Institute of Applied Mathematics

09/2004 - 06/2005

Digital Communication and Electronics

Hacettepe University

Electronics and Computer Engineering

09/1999 - 08/2003

BSc, System Engineering

Turkish Military Academy

System Eng. • *Electronic Eng.*

Work experience

Manager — **2/2024 - Now**
AYWARE Bilisim Çözümleri Ltd.Sti.

PoS Blockchains, DVT, liquid staking, multi-signatures, zero-knowledge proofs, Commitment schemes, Post-quantum cryptography, zkML, Agentic AI

Blockchain and Cryptography Researcher — **2/2022 - 2/2024**
Nethermind, Remote

PoS Blockchains, DVT, liquid staking, multi-signatures, zero-knowledge proofs, Commitment schemes, Post-quantum cryptography, zkML, Agentic AI

Cryptographer — **12/2021 - 2/2022**
Freelance

Basically, reading, understanding and analysing State-of-the-Art algortihms, and then modify them in order to improve their efficiency.

Quality Manager — **06/2018 - 12/2021**
Maintenance Command of Turkish Gendarmerie, ANKARA

In this position, I managed the construction process and implementation of quality system standards of ISO 9001:2015 in Maintenance Command of Turkish Gendarmerie which is responsible for maintaining the functionalities of special digital equipments, weapon systems, armoured vehicles of Turkish Gendarmerie.

Inspector — **06/2018 - 09/2017**
Inspection Directorate of the Turkish Gendarmerie General Command, ANKARA

In this position, I inspected the personnel using IT systems and weapon systems of Turkish Gendarmerie across the country, and prepared inspection reports for the HQ.

Communication Information Systems Unit Commander — **06/2017 - 09/2017**
Special Peace Command of Turkish Gendarmerie, ANKARA

I worked just 3 months in this special unit, and I was responsible for establishing and maintaining the digital communication, including wired/wireless communication, radio communication via APCO-25, satellite communication of 4 battallions.

Human Resources Manager — **08/2014 - 06/2017**
Personnel Directorate of the Turkish Gendarmerie General Command, ANKARA

In this position, I planned and managed the assignment of the officers of Turkish Gendarmerie. I also worked in close coordination with a team which was responsible for developing a software for automation of assignment process. I managed the process of quantization of the verbal characteristics of all personnel.

Communication and Information Systems Manager — **07/2011 - 07/2014**
Provincial Gendarmerie Command, BINGOL

In this position, I managed the communication and information systems of Gendarmerie General Command in Bingol province.

Interests

- Hiking
- Cellular Automata & Chaos
- Astronomy
- Classical Turkish Arts & Classical Music

Contact

Maltepe Mahallesi
Genclik Caddesi No:63/6
Cankaya Ankara TURKEY

+90 532 720 06 92

a.r.agirtas@gmail.com

LinkedIn

github.com/ahmetramazan

Communication and Information Systems Manager — 07/2009 - 07/2011
Regional Gendarmerie Command, KASTAMONU

In this position, I managed the communication and information systems of Gendarmerie General Command in 5 provinces (Zonguldak, Bartin, Karabuk, Kastamonu and Sinop).

Liaison Officer — 01/2007 - 08/2007
Turkish Battle Group, Regional Command Capital, ISAF, NATO, KABUL/AFGHANISTAN

In this position, I worked for International Security Assistance Force (NATO). My main duty was establishing the connection between Italian, French, Turkish Battle Groups and the Local Authority.

Training Company Commander — 07/2004 - 08/2009
Gendarmerie Training Battallion, Seferihisar IZMIR

In this position, I managed the basic training process of recruits, both military training and branch training. I had trained approximately a thousand candidate soldiers per year.

Courses and Certificates

- "Human Resource Management Course", Institute of Strategic Researches, Turkish Military Academy, 2014.
- "Radio Systems used in Joint Operations Course", NATO/National Joint Communication and Information Systems Training Center, 2012.
- "Operation and Security of Communication and Information Systems Course", CIS Training Center of Turkish Gendarmerie General Command, 2011.
- "Security of Joint Communication Course", NATO/National Joint CIS Training Center, 2009.
- "Network-based Constructions and System Planning Course", NATO / National Joint CIS Training Center, 2009.
- "NATO/National Joint Communication and Information Systems Course", NATO / National Joint CIS Training Center, 2008.
- "Digital Communication and Electronics Course", Hacettepe University, 2005.
- "Fundamental Course for Signal Officers", CIS Training Center of Turkish Army, 2003.

Ongoing Blockchain Projects

Completed Blockchain Projects

- **Allowing validators to provide client information privately—a project by Nethermind Research and Nethermind Core (EF Research Grant)**
  TL;DR
  "In this work, we analyzed various approaches for validators to report their client diversity data. Among these, we highlight the reporting of validator data on the graffiti field of Ethereum blocks and the gossiping of this data through a dedicated GossipSub channel on the P2P network. We also considered the sample sizes required to achieve a statistically significant approximation to the client diversity distribution. This led to the recommendations of 9.6k and 38k validators for a confidence

level of 95% and tolerated errors of 1% and 0.5%, respectively. We identified two main techniques that can be used to imbue these data-sharing methods with privacy. The first method utilizes nullifiers to allow validators to submit anonymous reports as long as they can prove in zero-knowledge that they belong to a secret sample. For this method, a sufficiently motivated attacker may theoretically compromise the method's privacy via P2P monitoring and heuristics—a weakness shared by the Ethereum network itself that could be used for more harmful ends. We discussed possible mitigation strategies leveraging specialized routing protocols (such as Dandelion), although a full analysis is beyond the scope of the research and is proposed as future work. The second technique is inspired by private voting schemes; it uses homomorphic encryption coupled with a low-cost blockchain to gather encrypted votes. Putting the above findings together, we presented three different methods for client diversity data collection. Different trade-offs were found, involving complexity and introducing a trusted committee to mitigate P2P tracking concerns. Each of the three methods was then assessed with respect to various features such as privacy guarantees, trust assumptions, and complexity, among others."
Proposal and deliverable

- **Obol Distributed Validator Technology (DVT) v2**

  Deliverable 1 (TL;DR)
  "In this report, we propose a distributed key generation (DKG) method for Obol clusters, which provides public verification and has a reasonably low cost of on-chain verification. More precisely, we propose operators to perform a VSS (Feldman's VSS) using a one-layer recursive SNARK (Groth16) composition. Then, an aggregator (one of the operators) submits a succinct wrapper SNARK that attests to the validity of a fair DKG to a verifier smart contract."
  Research report 1

  Deliverable 2 (TL;DR)
  "In this report, we propose to use a Groth16 proof composition method (see below). An aggregator (one of the operators) generates a succinct wrapper SNARK that attests to the validity of a fair key refresh, and submits a commitment to the proof of a fair key refresh to a smart contract. If there are no whistleblower complaints about the proof for some time, the cluster starts using the fresh keys. If a whistleblower sends a fraud proof (see below) to the smart contract regarding what the aggregator submitted, the smart contract verifies the fraud proof and approves or declines the key refresh."
  Research report 2

- **A proposal for partnering with Nethermind to design a mechanism for a good validator set maintenance**
  The proposal
  TL;DR
  "In this systematization of knowledge, we examine the current innovations and approaches to the field of decentralized identity (also self-sovereign identity), as well as its relevant foundations."
  The deliverable

- **Using Shamir's secret sharing to share mnemonics**
  TL;DR
  "In this project we implement a modified version of Shamir's secret sharing scheme (SSS) in order to share a secret phrase, called mnemonics, in a secure way. In the following we give the notation that we use, then we give the definition of Shamir's secret sharing scheme and our modified scheme. We describe how we generate shares and reconstruct the secret. Then we give a basic usage information and the format of a share file. Finally, we give a few comments on design rationale."
  The post
  The code

Blog posts

- **Threshold Signature Schemes** by Ahmet Ramazan Agirtas, Jorge Arce-Garro, Yevgeny Zaytman and Jelilat Anofiu.
  Medium post
- **BLS Signatures & Withdrawals** by Ahmet Ramazan Agirtas, Aikaterini-Panagiota Stouka and Isaac Villalobos Gutiérrez.
  Medium post

Publications under review

- Ağırtaş, A.R.; Yayla, O.; *"Lattice-based Accountable Subgroup Multi-signature Scheme."* (Under review)
- Ağırtaş, A.R.; Yayla, O.; *"Pairing-based Accountable Subgroup Multi-signatures with Verifiable Group Setup"*, Cryptology ePrint Archive, Report 2022/018, 2022. ePrint (Under review)

Publications

- Ağırtaş, A.R., Yayla, O. (2025). Compartment-Based and Hierarchical Threshold Delegated Verifiable Accountable Subgroup Multi-signatures. In: Dąbrowski, A., Pieprzyk, J., Pomykała, J. (eds) Number-Theoretic Methods in Cryptology. NuTMiC 2024. Lecture Notes in Computer Science, vol 14966. Springer, Cham. Link
- Ağırtaş, A.R.; Özer, A.B.; Saygı, Z.; Yayla, O.; "Distributed Verifiable Random Function with Compact Proof," 8th International Symposium on Cyber Security, Cryptology, and Machine Learning, CSCML 2024 , vol.15349 LNCS, Be'er-Sheva, Israel, pp.119-134, 2024. Link
- Ağırtaş, A.R.; Gökçe, N.Y.; Yayla, O. *"Locally Verifiable Signature Schemes: A Study of Aggregate and Multi-signatures"*, 2024. Paper presented at SecITC2024: 17th International Conference on Information Technology and Communications Security. (accepted to be published in Proceedings, LNCS) Available in ePrint.
- Ağırtaş, A.R.; Yayla, O.; *Delegated Verifiable Accountable Subgroup Multi-signatures*. Paper presented at the ALCOCRYPT 2023: Algebraic and Combinatorial Methods for Coding and Cryptography, February 20-24, 2023, CIRM, Luminy, France.
- Mahmutoglu, T.B., Ağırtaş, A.R., *"An example in the context of science journalism: Aziz Sancar, before and after the Nobel Prize in the press of Turkey and the USA"*, International Symposium on Knowledge Production and Science Policies in Turkey, 2018.

Patents

- "Quantum-resistant, lattice-based Accountable Subgroup Multi-signature Scheme", 2022/014511.
  (Inventors: A.R. Ağırtaş, O. Yayla, Current Assignee: Middle East Technical University)
- "Pairing-based Accountable Subgroup Multi-signature Schemes", 2021/022220.
  (Inventors: A.R. Ağırtaş, O. Yayla, Current Assignee: Middle East Technical University)

Ankara, 21st March 2025

Ahmet Ramazan AĞIRTAŞ