Ahmet Ramazan AĞIRTAŞ
PhD Candidate (Cryptography)

Skills

Low/Mid-level Military Management 18 yrs.

IT Management 10 years

Cryptographic Protocol Design 8+ yrs.

Digital Signatures 8+ yrs.

C/C++/ C#, Python 5+ yrs.

SageMath 5+ yrs.

English

Turkish

Education

10/2015 - 10/2023

PhD Candidate, 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

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

Blockchain, digital signatures, polynomial commitments, zero-knowledge proofs.

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

- Running and 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.

Publications under review

- Agirtas, A.R., Yayla, O., *"Lattice-based Accountable Subgroup Multi-signature Scheme."* (Under review)
- Agirtas, A.R., Yayla, O., *"Compartment-based and Hierarchical Threshold Delegated Verifiable Accountable Subgroup Multi-signatures."*, Cryptology ePrint Archive, Report 2023/548, 2023. (https://eprint.iacr.org/2023/548)(Under review)
- Agirtas, A.R., Yayla, O., *"Pairing-based Accountable Subgroup Multi-signatures with Verifiable Group Setup"*, Cryptology ePrint Archive, Report 2022/018, 2022. (https://eprint.iacr.org/2022/018) (Under review)

Publications

- Ahmet Ramazan Ağırtaş and Oğuz Yayla, *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., Agirtas, 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.Agirtas, O.Yayla, Current Assignee: Middle East Technical University)
- "Pairing-based Accountable Subgroup Multi-signature Schemes", 2021/022220.

  (Inventors: A.R.Agirtas, O.Yayla, Current Assignee: Middle East Technical University)

Ankara, 11th October 2023

Ahmet Ramazan AĞIRTAŞ