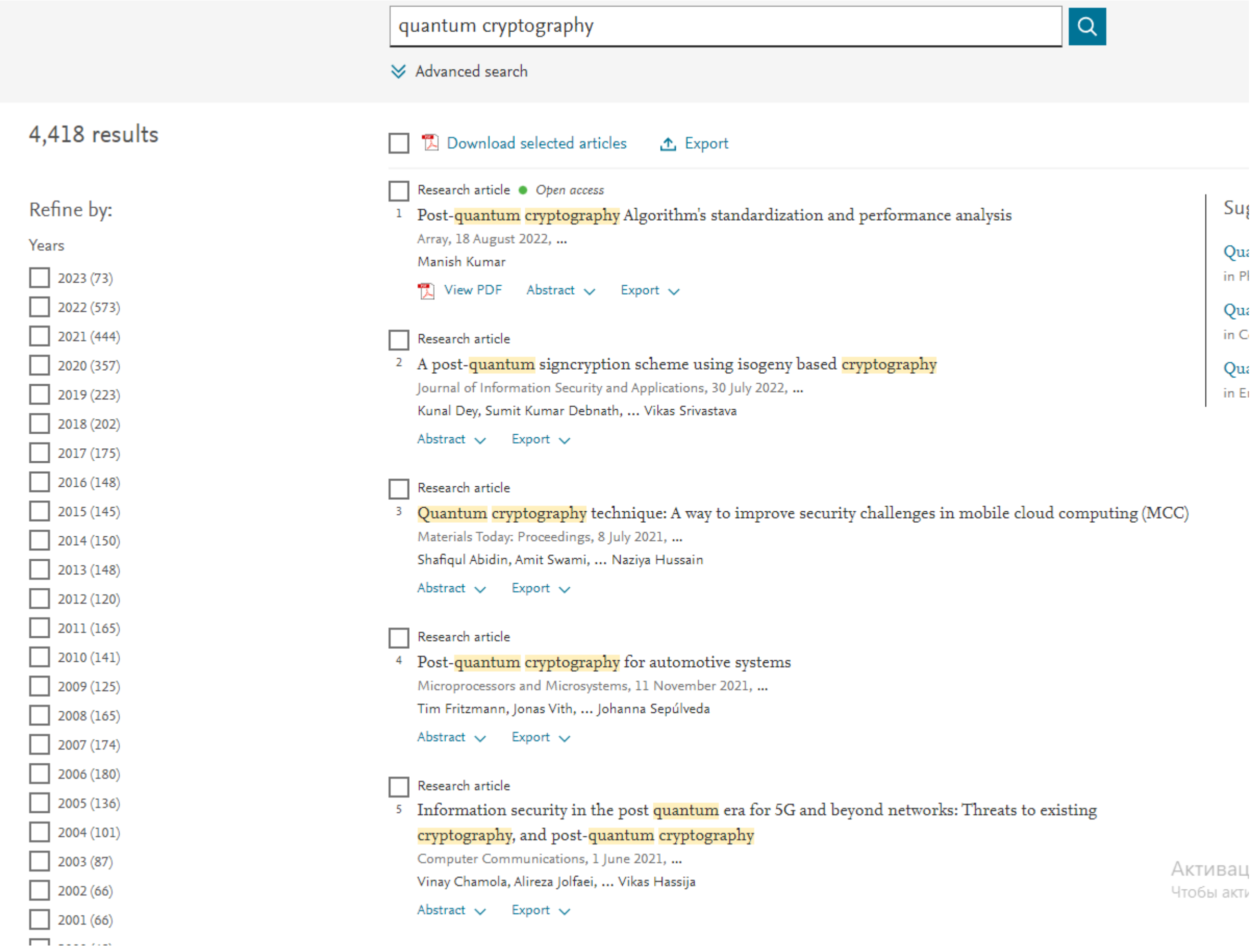
Тема: Квантовая криптография

Ключевые слова: quantum cryptography

Результат поиска:



quantum cryptography

Advanced search

4,418 results

Refine by:

Years

□ 2023 (73)
□ 2022 (573)
□ 2021 (444)
□ 2020 (357)
□ 2019 (223)
□ 2018 (202)
□ 2017 (175)
□ 2016 (148)
□ 2015 (145)
□ 2014 (150)
□ 2013 (148)
□ 2012 (120)
□ 2011 (165)
□ 2010 (141)
□ 2009 (125)
□ 2008 (165)
□ 2007 (174)
□ 2006 (180)
□ 2005 (136)
□ 2004 (101)
□ 2003 (87)
□ 2002 (66)
□ 2001 (66)

□ Download selected articles   Export

□ Research article ● *Open access*

1 Post-quantum cryptography Algorithm's standardization and performance analysis

Array, 18 August 2022, ...

Manish Kumar

View PDF   Abstract   Export

□ Research article

2 A post-quantum signcryption scheme using isogeny based cryptography

Journal of Information Security and Applications, 30 July 2022, ...

Kunal Dey, Sumit Kumar Debnath, ... Vikas Srivastava

Abstract   Export

□ Research article

3 Quantum cryptography technique: A way to improve security challenges in mobile cloud computing (MCC)

Materials Today: Proceedings, 8 July 2021, ...

Shafiqul Abidin, Amit Swami, ... Naziya Hussain

Abstract   Export

□ Research article

4 Post-quantum cryptography for automotive systems

Microprocessors and Microsystems, 11 November 2021, ...

Tim Fritzmann, Jonas Vith, ... Johanna Sepúlveda

Abstract   Export

□ Research article

5 Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography

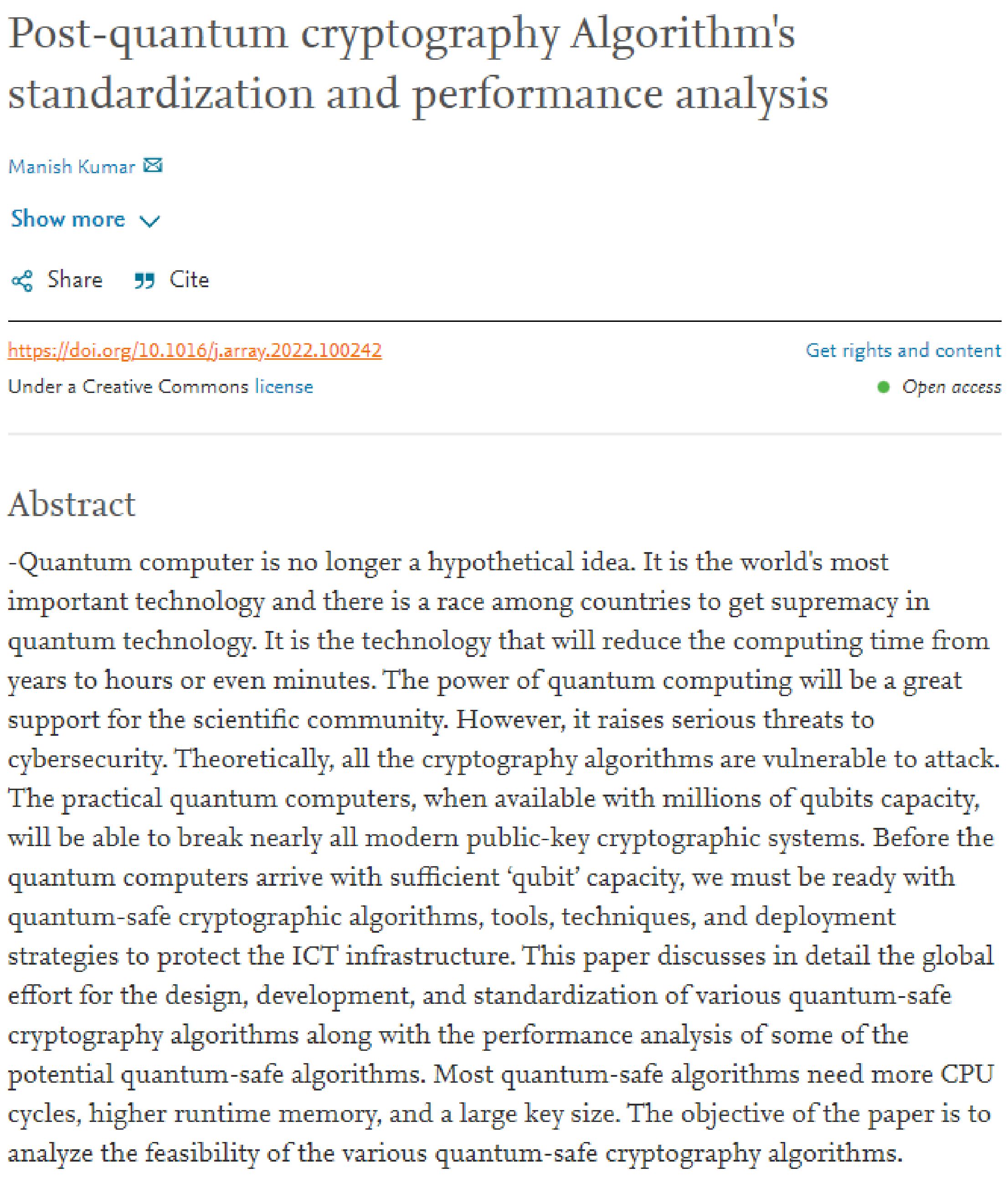
Computer Communications, 1 June 2021, ...

Vinay Chamola, Alireza Jolfaei, ... Vikas Hassija

Abstract   Export

Статьи

1. **Post-quantum cryptography Algorithm's standardization and performance analysis**



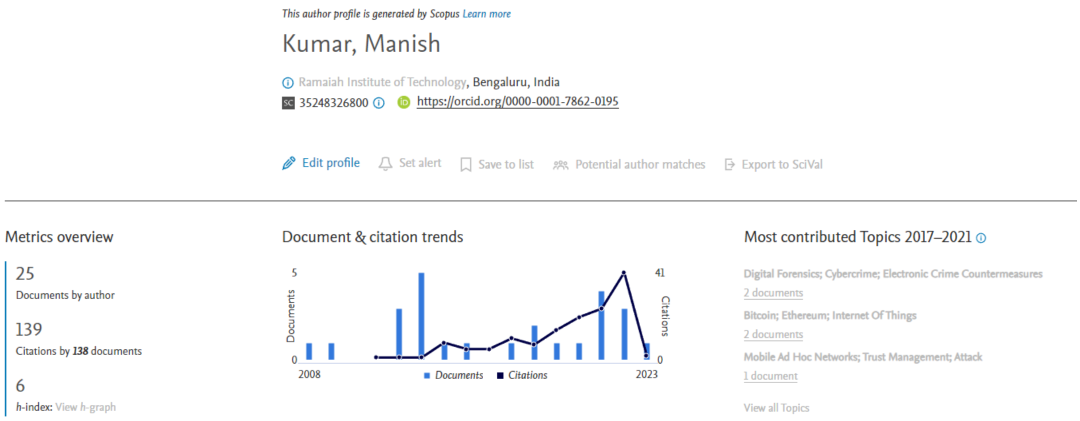
Post-quantum cryptography Algorithm's standardization and performance analysis

Manish Kumar ✉

https://doi.org/10.1016/j.array.2022.100242

Abstract

-Quantum computer is no longer a hypothetical idea. It is the world's most important technology and there is a race among countries to get supremacy in quantum technology. It is the technology that will reduce the computing time from years to hours or even minutes. The power of quantum computing will be a great support for the scientific community. However, it raises serious threats to cybersecurity. Theoretically, all the cryptography algorithms are vulnerable to attack. The practical quantum computers, when available with millions of qubits capacity, will be able to break nearly all modern public-key cryptographic systems. Before the quantum computers arrive with sufficient 'qubit' capacity, we must be ready with quantum-safe cryptographic algorithms, tools, techniques, and deployment strategies to protect the ICT infrastructure. This paper discusses in detail the global effort for the design, development, and standardization of various quantum-safe cryptography algorithms along with the performance analysis of some of the potential quantum-safe algorithms. Most quantum-safe algorithms need more CPU cycles, higher runtime memory, and a large key size. The objective of the paper is to analyze the feasibility of the various quantum-safe cryptography algorithms.



This author profile is generated by Scopus *Learn more*

Kumar, Manish

ⓘ Ramaiah Institute of Technology, Bengaluru, India

35248326800 ⓘ https://orcid.org/0000-0001-7862-0195

Edit profile Set alert Save to list Potential author matches Export to SciVal

Metrics overview

25
Documents by author

139
Citations by ***138*** documents

6
h-index: View *h*-graph

Document & citation trends

Most contributed Topics 2017–2021 ⓘ

Digital Forensics; Cybercrime; Electronic Crime Countermeasures
2 documents

Bitcoin; Ethereum; Internet Of Things
2 documents

Mobile Ad Hoc Networks; Trust Management; Attack
1 document

View all Topics

2. Post-quantum cryptography Algorithm's standardization and performance analysis

Special Section on Quantum Information Processing

Quantum Cryptography for Internet of Things Security a

Alekha Parimal Bhatt 1 ✉, Anand Sharma 1 👤 ✉

Show more ∨

Share Cite

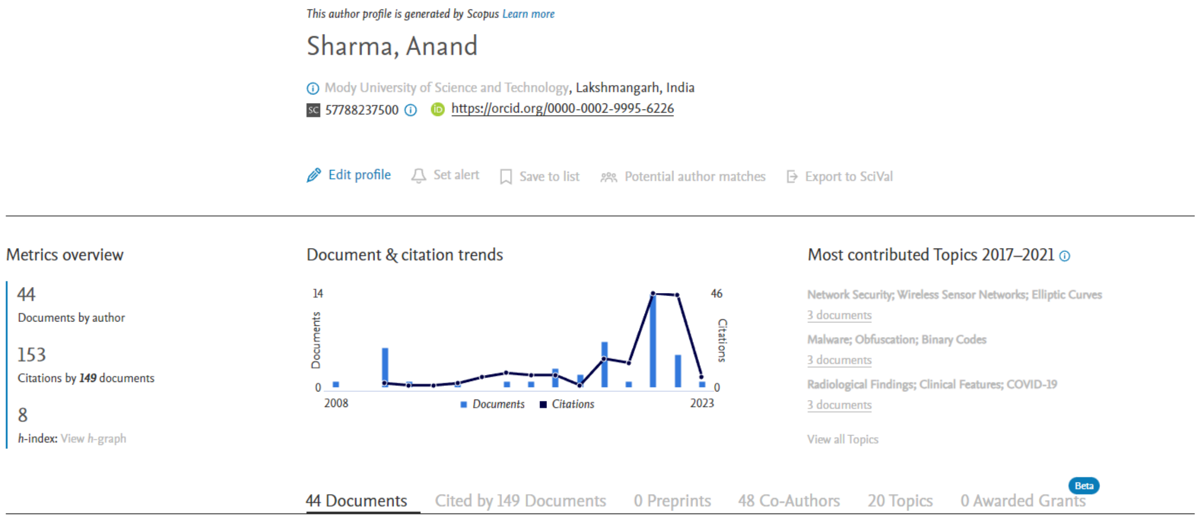
https://doi.org/10.11989/JEST.1674-862X.90523016

Get rights and content

● *Open access*

Abstract

Internet of things (IoT) is a developing technology with a lot of scope in the future. It can ease various different tasks for us. On one hand, IoT is useful for us, on the other hand, it has many serious security threats, like data breaches, side-channel attacks, and virus and data authentication. Classical cryptographic algorithms, like the Rivest-Shamir-Adleman (RSA) algorithm, work well under the classical computers. But the technology is slowly shifting towards quantum computing, which has immense processing power and is more than enough to break the current cryptographic algorithms easily. So it is required that we have to design quantum cryptographic algorithms to prevent our systems from security breaches even before quantum computers come in the market for commercial uses. IoT will also be one of the disciplines, which needs to be secured to prevent any malicious activities. In this paper, we review the common security threats in IoT and the presently available solutions with their drawbacks. Then quantum cryptography is introduced with some of its variations. And finally, the analysis has been carried out in terms of the pros and cons of implementing quantum cryptography for IoT security.



This author profile is generated by Scopus *Learn more*

Sharma, Anand

Mody University of Science and Technology, Lakshmangarh, India

57788237500 https://orcid.org/0000-0002-9995-6226

Edit profile Set alert Save to list Potential author matches Export to SciVal

Metrics overview

44
Documents by author

153
Citations by *149* documents

8
h-index: View *h*-graph

Document & citation trends

Most contributed Topics 2017–2021

Network Security; Wireless Sensor Networks; Elliptic Curves
3 documents

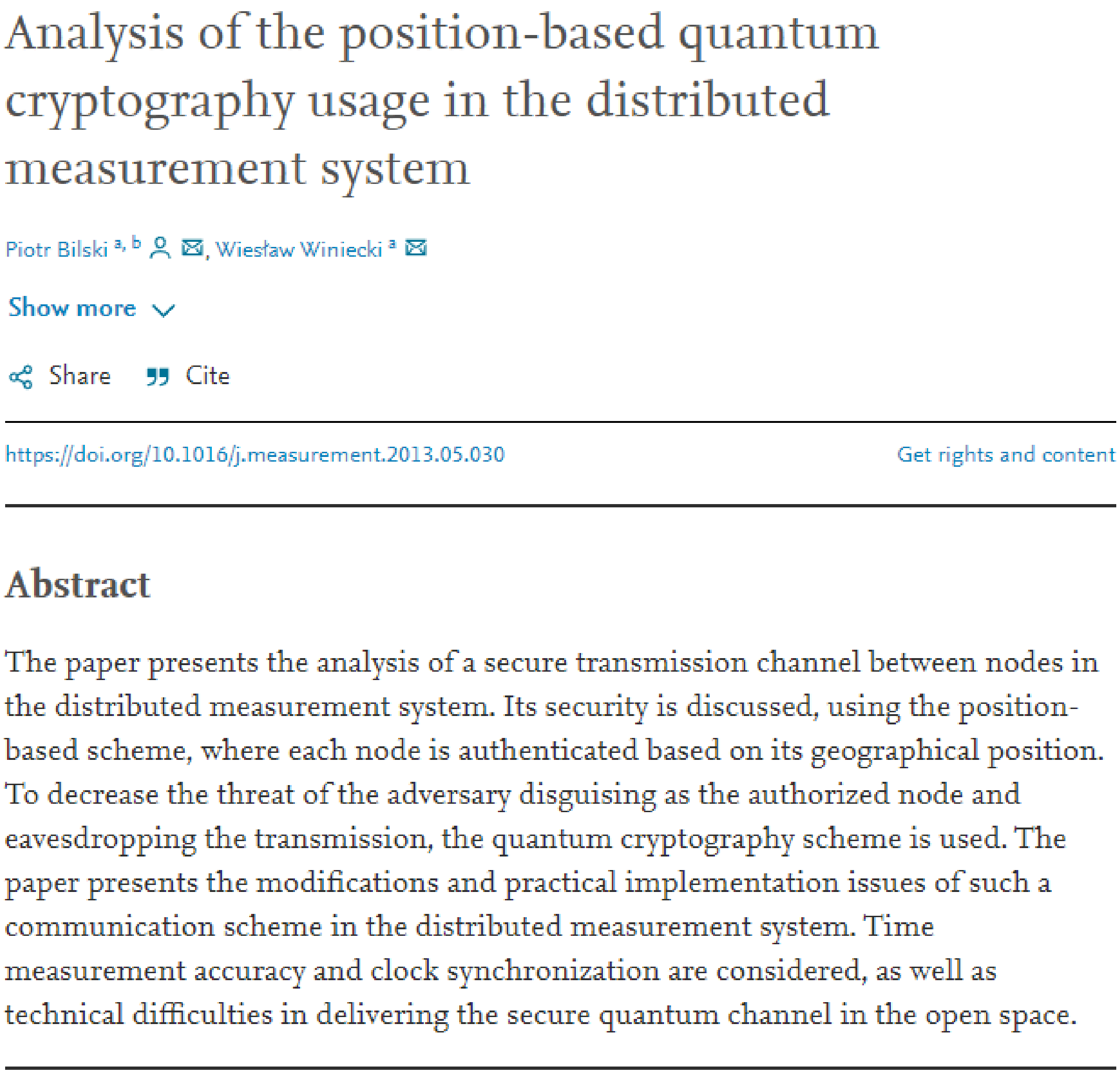
Malware; Obfuscation; Binary Codes
3 documents

Radiological Findings; Clinical Features; COVID-19
3 documents

View all Topics

44 Documents Cited by 149 Documents 0 Preprints 48 Co-Authors 20 Topics 0 Awarded Grants Beta

3. Analysis of the position-based quantum cryptography usage in the distributed measurement system



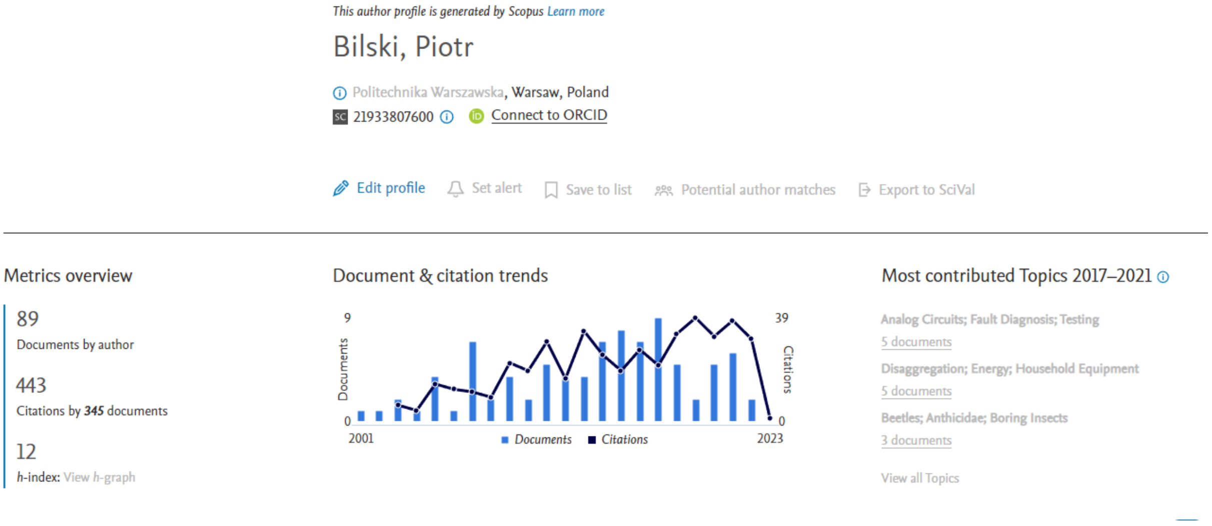
Analysis of the position-based quantum cryptography usage in the distributed measurement system

Piotr Bilski [a], [b], Wiesław Winiecki [a]

https://doi.org/10.1016/j.measurement.2013.05.030

Abstract

The paper presents the analysis of a secure transmission channel between nodes in the distributed measurement system. Its security is discussed, using the position-based scheme, where each node is authenticated based on its geographical position. To decrease the threat of the adversary disguising as the authorized node and eavesdropping the transmission, the quantum cryptography scheme is used. The paper presents the modifications and practical implementation issues of such a communication scheme in the distributed measurement system. Time measurement accuracy and clock synchronization are considered, as well as technical difficulties in delivering the secure quantum channel in the open space.



This author profile is generated by Scopus *Learn more*

Bilski, Piotr

Politechnika Warszawska, Warsaw, Poland

21933807600 Connect to ORCID

Metrics overview

89
Documents by author

443
Citations by **345** documents

12
h-index: View *h*-graph

Document & citation trends

Most contributed Topics 2017–2021

Analog Circuits; Fault Diagnosis; Testing
5 documents

Disaggregation; Energy; Household Equipment
5 documents

Beetles; Anthicidae; Boring Insects
3 documents

View all Topics

Вывод

Проанализировав поиск англоязычных и русскоязычных статей на тему, квантовая криптография можно сделать вывод что англоязычных статей больше. Видно, что данная тема начала своё развитее с 1999 года и стремительно развивается до сих пор, большее количество статей вышло в 2022 году.