AICTE Training and Learning (ATAL) Academy
Sponsored
Five Day Faculty Development Program (FDP)
on
The Impact of Quantum Computing on Cryptography and Blockchain Technology
13-17 September 2021
Organised by
Department of Mathematics
GITAM, Hyderabad

About GITAM
GITAM (Gandhi Institute of Technology and Management) is a Deemed to be University, established under section 3 of UGC Act, 1956, in the year 1980 in Visakhapatnam with off-campuses at Hyderabad and Bengaluru. The University offers 128 programs at U.G., P.G. and Doctoral levels with a faculty strength of about 2,000. GITAM has been accredited by NAAC with A+ Grade. Ministry of HRD recognized GITAM as Category ‘1’ University and granted Graded Autonomy. GITAM has also been recognized by AICTE and UGC as a Research University and accorded 12 B status.

About GITAM Hyderabad
GITAM Hyderabad is set up on about 200 acres of land at Rudraram Village, Patancheru Mandal, Hyderabad. GITAM Hyderabad comprises of seven schools, viz., School of Technology, Business School, School of Sciences, School of Pharmacy, School of Architecture, Kautilya School of Public Policy and School of Humanities and Social Sciences.
About Department of Mathematics

The department of mathematics was established during the academic year 2009 as part of B.Tech/B.Sc/MBA/M.Tech programme. The department has 22 faculty members with doctorate degree. Research is the major strength of the department with a sharp focus on thrust areas such as Fluid Dynamics, Bio-fluid Dynamics, Mathematical Modeling, Functional Analysis, Operations Research, Algebra and Statistics. The faculty members are actively involved in research and have published more than 400 research papers, also successfully completed one UGC Major Research Project.

About ATAL Academy

AICTE Training and Learning (ATAL) Programme is an initiative by AICTE which aims at empowering faculty to achieve goals of Higher Education such as access, equity and quality. This programme is designed to fulfill the need to train the young generation in skill sector and having faculty & technicians to be trained in their respective disciplines. It was felt that training with latest tools and technologies is vital to keeping an institute competitive and more productive. Training is required for increasing the knowledge and skills of students to make them more employable to acquire global competencies.

About the FDP

In communication era, digital security and privacy are important to every individuals and organizations. Cryptography plays a crucial role to provide security services such as confidentiality, authenticity, data integrity, availability and non-repudiation and has wide range of applications in network security, cyber security, internet security, banking security, data security, communication security, and blockchain technology etc. The well-known applications of blockchain technology are digital wallet, smart contracts, cryptocurrency, bitcoin and Ethereum etc.

Cryptosystem has been classified into symmetric key cryptosystem and asymmetric key cryptosystem. There are many significant cryptographic algorithms such as secret key encryptions, public key encryptions, hash functions, message authentication codes, digital signatures, fully homomorphic encryptions, multiparty computations, secret sharing, authentication schemes for various functionalities. Most of the public key cryptographic algorithms rely on computational hard problems such as number theoretic problems: the Integer factorization problem, discrete logarithmic problem and elliptic curve discrete logarithmic problem. However, the cryptosystems based on these problems are vulnerable to quantum attacks due to Shor's algorithm.

Quantum computing is an efficient computational device which works on based on photon and performs computational tasks exponentially faster than digital computers. Due to computational efficiency of quantum computer, most of the existing cryptographic algorithms will affect, including symmetric cryptographic algorithms due to Grover's algorithm. Subsequently, this will impact security issues of cyber security, blockchain technology, e-mail security, banking security, network security, etc. Thus, one should choose either post-quantum cryptographic algorithms or quantum cryptographic algorithms those will work on quantum computer in near future. This faculty development programme will cover a wide range of cryptographic algorithms which include post-quantum algorithms and application to blockchain technology, including hands on programming on sage, python, magma etc.

Eligibility for Participants

The faculty members from AICTE approved institutions in engineering and sciences, research scholars and industry are eligible to apply.

Registration Procedure

Seats are limited to 200 and the participants shall be selected for the workshop on first come first serve basis. There is no registration fee for attending the FDP. Interested candidates are requested to sign up through this portal on or before 6th September 2021. (https://atalacademy.aicte-india.org/signup)

Then you need to register with FDP No.: 1614929160 “The Impact of Quantum Computing on Cryptography and Blockchain Technology”.

Test and Certificate

A test will be conducted by coordinator at the end of the program. A certificate will be issued to only those participants who have attended the program with minimum 80% attendance and scored minimum 60% marks in the test.
# Proposed Topics (Tentative)
- Basic Principle of Information Security
- Hash Functions
- Public key encryption schemes
- Basic of Quantum Computing
- Shor’s algorithm
- Post-quantum digital signature schemes
- Smart Contract, Bitcoin and Ethereum
- Symmetric key encryption schemes
- Message Authentication Code
- Digital signature schemes
- Grover’s algorithm
- NIST’s Post-Quantum Standardization Process
- Blockchain Technology
- Post-quantum encryption schemes and Post-Quantum Key Encapsulation Mechanism

## Chief Patron
**Sri. M. Sri Bharat**
President, GITAM

## Patrons
<table>
<thead>
<tr>
<th>Dr. Virander Singh Chauhan</th>
<th>Prof. K. Siva Rama Krishna</th>
<th>Prof. D. Gunasekaran</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chancellor, GITAM</td>
<td>Vice-Chancellor, GITAM</td>
<td>Registrar, GITAM</td>
</tr>
</tbody>
</table>

## Co-Patrons
| Prof. N. Siva Prasad     | Prof. N. Seetharamaiah    |
| Pro-Vice Chancellor      | Principal, School of Technology |
| GITAM - Hyderabad        | GITAM - Hyderabad         |

| Prof. G. A. Rama Rao     | Prof. K. Maruthi Prasad   |
| Principal, School of Science | HoD, Mathematics     |
| GITAM - Hyderabad        | GITAM - Hyderabad        |

## Coordinator
**Dr. P. Narasimha Swamy**
Asst. Prof., Dept. of Mathematics
GITAM - Hyderabad

## Co-Coordinator
**Dr. Siva Reddy Sheri**
Assoc. Prof., Dept. of Mathematics
GITAM - Hyderabad

## For more information
Dr. P. Narasimha Swamy - 99485 25133 and Dr. Siva Reddy Sheri - 77025 39113
GITAM-Hyderabad, Rudraram, Patancheru Mandal, Sangareddy District–502 329, Telangana State, India.
E-mail: npasham@gitam.edu / ssheri@gitam.edu

[https://atalacademy.aicte-india.org/signup](https://atalacademy.aicte-india.org/signup)

**In order to complete the registration on the ATAL FDP portal, please follow the below steps:**
1. Visit: [https://atalacademy.aicte-india.org/signup](https://atalacademy.aicte-india.org/signup)
2. Register as a Participant → Fill your details (General Details & Profile)
3. Go to Workshop: State → Telangana → Month → September → Thrust Areas
4. Select Title: The Impact of Quantum Computing on Cryptography and Blockchain Technology (or Application Number: 1614929160) → Click on +

**Application Number:** 1614929160  **Workshop ID:** 2247  **S. No.:** 1222