

WAIFI 2022 Program at a glance

(All date/times are in Beijing time, please change the time zone in your local time)

(You can directly click on the dates to go to the relevant ZOOM links)

29th Aug (Monday)	30th Aug (Tuesday)	31st Aug (Wednesday)	1st Sept (Thursday)	2nd Sept (Friday)
3:00 PM - 3:20 PM Opening Remarks				
3:20 PM - 3:30 PM Coffee	3:20 PM - 3:30 PM Coffee	3:20 PM - 3:30 PM Coffee	3:20 PM - 3:30 PM Coffee	3:20 PM - 3:30 PM Coffee
3:30 PM - 4:30 PM Keynote Speech 1 Speaker: Lilya Budaghyan		3:30 PM - 4:30 PM Keynote Speech 2 Speaker: Cunsheng Ding	3:30 PM - 4:30 PM Keynote Speech 3 Speaker: Sylvain Duquesne	
4:30 PM - 4:40 PM Coffee	4:30 PM - 4:40 PM Coffee	4:30 PM - 4:40 PM Coffee	4:30 PM - 4:40 PM Coffee	4:30 PM - 4:40 PM Coffee
4:40 PM - 6:00 PM Session 1 (4 Papers)	4:40 PM - 6:00 PM Session 2 (4 Papers)	4:40 PM - 6:00 PM Session 3 (4 Papers)	4:40 PM - 6:00 PM Session 4 (4 Papers)	4:40 PM - 6:00 PM Session 5 (3 Papers)
6:00 PM - 6:30 PM Coffee	6:00 PM - 6:30 PM Coffee	6:00 PM - 6:30 PM Coffee	6:00 PM - 6:30 PM Coffee	6:00 PM - 6:30 PM Coffee

WAIFI 2022 Invited Talks

(All times are in Beijing date/time, please change the time zone in your local time)

Keynote 1:

Speaker: **Lilya Budaghyan** (University of Bergen, Norway)

Title of the talk: **Polynomial expansion of APN functions**

Session Chair: Alev Topuzoglu (Sabancı University, Turkey)

Date & Time: **29th August 2022, 3:30 PM - 4:30 PM**

Keynote 2:

Speaker: **Cunsheng Ding** (The Hong Kong University of Science and Technology, Hong Kong)

Title of the talk: **Two families of constacyclic codes**

Session Chair: Zhengchun Zhou (Southwest Jiaotong University, China)

Date & Time: **31st August 2022, 3:30 PM - 4:30 PM**

Keynote 3:

Speaker: **Sylvain Duquesne** (University of Rennes 1, France)

Title of the talk: **Finite field arithmetic in large characteristic for classical and post-quantum cryptography**

Session Chair: Çetin Kaya Koç (University of California, Santa Barbara, USA)

Date & Time: **1st September 2022, 3:30 PM - 4:30 PM**

WAIFI 2022 Paper Presentation Sessions

(All times are in Beijing date/time, please change the time zone in your local time)

Session 1: Polynomials & Bent Functions 29 August 2022, 4:40 PM - 6:00 PM	
Session Chair: <u>Xiwang Cao</u> (Nanjing University of Aeronautics and Astronautics, China)	
Sl. No.	Paper details
1	<i>Title: New classes of bent functions via the switching method</i> <i>Authors: Xi Xie, Bing Chen, Nian Li and Xiangyong Zeng</i>
2	<i>Title: On a conjecture on irreducible polynomials over finite fields with restricted coefficients</i> <i>Authors: Andrea Ferraguti and Giacomo Micheli</i>
3	<i>Title: On two applications of polynomials x^k-cx-d over finite fields and more</i> <i>Authors: Canberk Irimagzi and Ferruh Ozbudak</i>
4	<i>Title: Polynomial Constructions of Chudnovsky-type algorithms for multiplication in finite fields with linear bilinear complexity</i> <i>Authors: Bastien Pacifico, Stephane Ballet and Alexis Bonnet</i>

Session 2: Coding Theory 30 August 2022, 4:40 PM - 6:00 PM	
Session Chair: <u>Ferruh Ozbudak</u> (Middle East Technical University, Ankara, Turkey)	
Sl. No.	Paper details
1	<i>Title: PIR codes from combinatorial structures</i> <i>Authors: Massimo Giulietti, Arianna Sabatini and Marco Timpanella</i>
2	<i>Title: Optimal possibly nonlinear 3-PIR codes of small size</i> <i>Authors: Henk D.L. Hollmann and Urmaz Luhaäär</i>
3	<i>Title: Near MDS codes with dimension 4 and their application in locally recoverable codes</i> <i>Authors: Ziling Heng and Xiaoru Li</i>

4	<p><i>Title: The Projective General Linear Group $PGL(2, 5m)$ and Linear Codes of Length $5m+1$</i></p> <p><i>Authors: Yue Zhao, Chunming Tang and Yanfeng Qi</i></p>
---	---

(All date/times are in Beijing time, please change the time zone in your local time)

<p>Session 3: Cryptography & Coding Theory 31 August 2022, 4:40 PM - 6:00 PM</p>	
<p>Session Chair: <u>Qi Wang</u> (Southern University of Science and Technology, China)</p>	
Sl. No.	Paper details
1	<p><i>Title: New Versions of Miller-loop Secured against Side-Channel Attacks</i></p> <p><i>Authors: Nadia El Mrabet, Fouotsa Emmanuel, Loubna Ghammam and Nicolas Méloni</i></p>
2	<p><i>Title: Private Information Retrieval Schemes Using Cyclic Codes</i></p> <p><i>Authors: Seyma Bodur, Edgar Martinez-Moro and Diego Ruano</i></p>
3	<p><i>Title: Explicit Non-Malleable Codes from Bipartite Graphs</i></p> <p><i>Authors: Shohei Satake, Yujie Gu and Kouichi Sakurai</i></p>
4	<p><i>Title: Two classes of optimal few-weight codes over $\mathbb{F}_q + u\mathbb{F}_q$</i></p> <p><i>Authors: Zhao Hu, Bing Chen, Nian Li and Xiangyong Zeng</i></p>

<p>Session 4: Finite Fields 1 September 2022, 4:40 PM - 6:00 PM</p>	
<p>Session Chair: <u>Nian Li</u> (Hubei University, China)</p>	
Sl. No.	Paper details
1	<p><i>Title: Fast enumeration of superspecial hyperelliptic curves of genus four with automorphism group V_4</i></p> <p><i>Authors: Ryo Ohashi, Momonari Kudo and Shushi Harashita</i></p>
2	<p><i>Title: A Class of Power Mappings with Low Boomerang Uniformity</i></p> <p><i>Authors: Haode Yan, Ziyang Zhang and Zhengchun Zhou</i></p>

3	<i>Title: Algebraic Relation of Three MinRank Algebraic Modelings</i> <i>Authors: Hao Guo and Jintai Ding</i>
4	<i>Title: Reduction-free Multiplication for Finite Fields and Polynomial Rings</i> <i>Authors: Cetin Koc, S. C. Oliva Madrigal, Gokay Saldamli, Chen Li, Yue Geng, Tian Jing and Zhongfong Wang</i>

(All dates/times are in Beijing time, please change the time zone in your local time)

Session 5: Sequences 2 September 2022, 4:40 PM - 6:00 PM	
Session Chair: <u>Avik R. Adhikary</u> (Southwest Jiaotong University, China)	
Sl. No.	Paper details
1	<i>Title: Correlation measure of binary sequence families with trace representation</i> <i>Authors: Domingo Gomez-Perez, Andrew Tirkel and Ana I. Gomez</i>
2	<i>Title: On the 2-adic complexity of cyclotomic binary sequences with period p^2 and $2p^2$</i> <i>Authors: Fuqing Sun, Qin Yue and Xia Li</i>
3	<i>Title: Linear complexity of generalized cyclotomic sequences with period $p^n q^m$</i> <i>Authors: Vladimir Edemskiy and Chenhuang Wu</i>

WAIFI 2022 ZOOM Links

(All times are in Beijing date/time, please change the time zone in your local time)

Day	Date	ZOOM Links
1	29th Aug 2022	https://univ-paris8.zoom.us/j/96798428766?pwd=NzBEZkxHZHBSMFIwcVFvNmFKakwvUT09 MEETING ID: 967 9842 8766 PASSCODE: 951298
2	30th Aug 2022	https://univ-paris8.zoom.us/j/95932353354?pwd=NVdVbkZvdTFXV0JHbXgxVmwyMldrdz09 MEETING ID: 959 3235 3354 PASSCODE: 348357
3	31st Aug 2022	https://univ-paris8.zoom.us/j/95716796181?pwd=anNHVFZaK05iY296ZCtraWZGZWdYQT09 MEETING ID: 957 1679 6181 PASSCODE: 521396
4	1st Sept 2022	https://univ-paris8.zoom.us/j/98388691182?pwd=SVFvWG1oUXFyeWlUalprc0dRdm9Rdz09 MEETING ID: 983 8869 1182 PASSCODE: 290417
5	2nd Sept 2022	https://univ-paris8.zoom.us/j/94522393952?pwd=SW52OG4zQ1dvZGZ6TGkvbFlDTGM2QT09 MEETING ID: 945 2239 3952 PASSCODE: 971567

Notes:

1. For us to know who you are, please change your ZOOM name to your name in English (First name + Surname).

2. Please contact Dr. Avik Adhikary by WhatsApp (+91 7759084499) or WeChat (Avik_adhikary) in case of problems in ZOOM connections. You can also contact Prof. Haode Yan in WeChat (math_yhd) for the same.
3. Please be online 15 minutes before your presentation and report to your respective session chairs via ZOOM chat for smooth conduct of the sessions.