ITU Journal
Future and evolving technologies

FREE I FAST I FOR ALL

The *ITU Journal on Future and Evolving Technologies (ITU J-FET)* is an international journal providing complete coverage of all communications and networking paradigms, free of charge for both readers and authors. The ITU Journal considers yet-to-be-published papers addressing fundamental and applied research. It shares new techniques and concepts, analyses and tutorials, as well as learning from experiments and physical and simulated testbeds. It also discusses the implications of the latest research results for policy and regulation, legal frameworks, the economy and society. This publication builds bridges between disciplines, connects theory with application, and stimulates international dialogue. Its interdisciplinary approach reflects ITU's comprehensive field of interest and explores the convergence of ICT with other disciplines. The ITU Journal welcomes submissions at any time, and on any topic within its scope.

Special issue on

Privacy and security challenges of generative AI

Call for papers

The use of Large Language Model (LLM) and Generative Pre-trained Transforms (GPT) technology based on Generative Artificial Intelligence (GAI) has become ubiquitous across various industries and societal domains due to their powerful capabilities in extracting, processing and expanding data, information, and knowledge. GAI can address the escalating demands of our digital life, encompassing cost, power, capacity, coverage, latency, efficiency, flexibility, compatibility, quality of experience and services.

However, as GAI application systems proliferate, privacy and security concerns have assumed an increasing pivotal role in their rapid development and massive deployment. Private and secure generative AI technology not only prevents unauthorized data and model parameters usage but also safeguards highly sensitive, proprietary, classified or private information during both training and inference phases. This adherence to security standards and privacy laws, such as the European GDPR rules or the US HIPPA rules, is crucial.

Fully Homomorphic Encryption (FHE) technology emerges as the most promising solution to address privacy and security concerns in GAI. Unlike GAI operating in plaintext formats, FHE based on GAI conducts all computations and operations in encrypted ciphertext formats. However, this comes with a substantial increase in implementation complexity on the order of 1,000 times compared to plaintext formats. Consequently, this imposes great limitations and challenges on processing architecture, memory access, computational capability, inference latency, data interfaces and bandwidths of hardware and silicon convergence for FHE-based GAI. Realizing secure and private GAI is a very challenging task and requires significant efforts from the related industry, research, and regulatory authorities for success.

This special issue aims to catalyze and steer the advancement of novel and improved systems to enable private and secure Generative AI, by fostering collaboration among scientists, engineers, broadcasters, manufacturers, software developers, and other related professionals.

The topics of interest for this special issue include, but are not limited to:

Suggested topics	
Algorithms, architectures and applications	• Encryption and decryption for private and secure GAI • Pipelining, parallel and distributed processing with co-design of algorithm and hardware • Ciphertexts-data driven programming platform and models • New computing architecture, memory access and data-interface • FHE based training and inference in GAI
Deployment, standardization and development	• Standardization, technical regulations and specifications for GAI • Secure multiple-party computation, differential privacy and federal learning • FHE based development libraries and open-source software
Information and signal processing	• Learning with noise, bootstrapping and programming bootstrapping • Private LLM with fine-tuning, transfer learning and lower-rank adaption • FHE based transforms and neural networks

Keywords
Fully homomorphic encryption (FHE), information security, data privacy, machine learning, neural networks, generative pre-trained transforms (GPT), large language model (LLM), generative artificial intelligence (GAI), learning and inference, fine-tuning, transfer learning, attention and query

Deadlines
Paper submission: 14 October 2024
Paper acceptance notification: 14 February 2025
Camera-ready paper submission: 14 April 2025

Paper submission
This special issue calls for original scientific papers. Submitted papers should not be under consideration for publication elsewhere. Submissions must be made electronically using ScholarOne Manuscripts, where templates and guidelines are also available.

Publication
Papers will be published in the ITU digital library.

Additional information
Please visit the ITU Journal website at https://www.itu.int/en/journal/j-fet/Pages/default.aspx. Inquiries should be addressed to Alessia Magliarditi at journal@itu.int.