Cryptography

Research Center

The foundaton
of information
security

tii.ae

Inspiring
innovation
for tomorrow

Theoretical knowledge, engineering knowhow

The Cryptography Research Center (CRC) at the Technology Innovation Institute (TII) is one of the few centres of its kind to bring together theoretical and applied cryptographers in a highly innovative environment.

Today, our researchers design the building blocks of advanced cryptographic and cryptanalytic mechanisms that enable advanced data privacy, integrity, confidentiality and non-repudiation.

Working on multiple research streams in the fundamental and applied domains, we research new cryptographic primitives covering design, analysis and implementation, as well as the development of security protocols.

Expertise in depth

Taking a leading position in cryptography, regionally and globally, we have built an international team of cryptography experts from top-tier academic institutions and research bodies with strong ties to renowned international cryptographers.

Our in-depth technical expertise encompasses fundamental classical and post-quantum cryptography research, applied cryptography engineering as well as research on theoretical and practical cryptanalytic techniques, applying the latest machine learning to enhance our defenses against cryptographic attacks.

Tackling key questions

We address the world's most pressing cryptographic questions. Our work covers post-quantum cryptography, lightweight cryptography, cloud encryption schemes, secure protocols, quantum cryptographic technologies and cryptanalysis.

Our core research areas

CRC works on multiple research areas in fundamental as well as applied science disciplines.

Cryptography in the era of quantum computers

Our research team focuses on developing cryptographic schemes to protect data, systems and network communications against the threat of quantum computers. Public-key cryptography based on RSA or ECC will be insecure once a sufficiently powerful quantum computer is built and is able to run Shor's and Grover's algorithms. For this reason, post-quantum cryptography (PQC) has emerged as a practical solution to make communications and systems quantum-resistant.

Our work is open and conducted in collaboration with academic partners, with the goal of designing and implementing robust and tested post-quantum cryptosystems in both software and hardware environments.

Our research domains include:
- Code-based post-quantum cryptography
- Hash-based post-quantum cryptography
- Lattice-based post-quantum cryptography
- Quantum key distribution protocols

Cryptography for the Internet Of Things and cyber-physical systems

Embedded systems including, Internet of Things (IoT) and cyber-physical systems (CPS), are proliferating across multiple domains, including mission-critical systems, such as nuclear power plants, smart cities and smart healthcare. However, vulnerabilities in the design and implementation of IoT and CPS devices are coupled with an absence of standard cryptographic primitives and network protocols.

As a consequence, lightweight cryptography has become a pivotal area, and focuses on designing and securely implementing cryptographic primitives suitable for all sorts of IoT and CPS scenarios.

At CRC, collaborative work is ongoing to design and implement robust and tested lightweight cryptosystems in software as well as hardware.

Our research domains include:
- Lightweight symmetric cryptographic primitives
- Quantum-resistant schemes for resource-constrained devices

Cryptography for the Cloud

Cloud computing has undergone significant growth in the last decade, offering myriad applications, some of which generate privacy and confidentiality challenges, even when the connection between users and cloud providers is secure.

However, the traditional use of cryptography is not the ideal solution for confidential computing and security preservation within the cloud environment.

At TII, we are working to design and implement robust and tested cloud encryption schemes. Our work on multi-party computation (MPC) and fully homomorphic encryption (FHE) solutions offer advanced security guarantees in the cloud environment. MPC and FHE are next-generation algorithms for cloud data encryption that enable decentralization and fragmentation of key storage, and smart computations on encrypted data, respectively.

Our research domains include:
- Multi-party computation
- Fully homomorphic encryption
- Key management systems for cloud environments

Cryptographic protocols

The TII team focuses on multiple areas, from foundational primitives to the design, analysis, implementation and testing, and developing security proofs for cryptographic protocols.

Cryptographic protocols have evolved significantly, adapting to the needs of recently developed applications. These provide several security properties at once, and end up as complex compositions of cryptographic primitives and schemes. The detailed study of these protocols is of the utmost importance, given that some of them are deployed on a large scale.

In addition, some of today's commonly used protocols are not quantum-resistant. As a consequence, hybrid protocols (combining PQC schemes and traditional RSA or ECC) have emerged as a practical solution.

Our research domains include:
- Cryptographic protocols
- Hybrid key establishment protocols
- Hybrid digital signature protocols

Our core research areas

CRC works on multiple research areas in fundamental as well as applied science disciplines.

Cryptography engineering

In cryptography, it is important not only to design secure systems, but also to implement them so they can be integrated and deployed in a secure and modular way. A secure implementation of cryptographic libraries in both software and hardware is pivotal, as they need to comply with performance requirements without jeopardizing security properties.

More recently, software-hardware co-designs have come into play and offer valuable trade-offs for engineers. All these constructions need to be thoroughly tested in multiple scenarios, including a wide variety of side-channel attacks and fault injections.

Our research domains include:

- Secure implementations optimized for different architectures and platforms
- Side-channel analysis and countermeasures implementation

Cryptanalysis

Cryptanalysis focuses on analyzing cryptographic constructions to identify weaknesses in their design and implementation, which are then exploited in order to derive keys or plaintexts.

Cryptanalysis has also paved the way for the development of criteria for the security evaluation of cryptographic primitives.

CRC is invested in research in two major cryptanalytic domains.

- Theoretical cryptanalysis attacks
- Cryptanalytic attacks against implementations

Our goal is to design and implement new and modular cryptanalytic frameworks in both software and hardware implementations. In addition, we are also building a comprehensive cryptanalysis library aimed at gathering different cryptanalysis techniques and tools under a common framework.

Our research domains include:

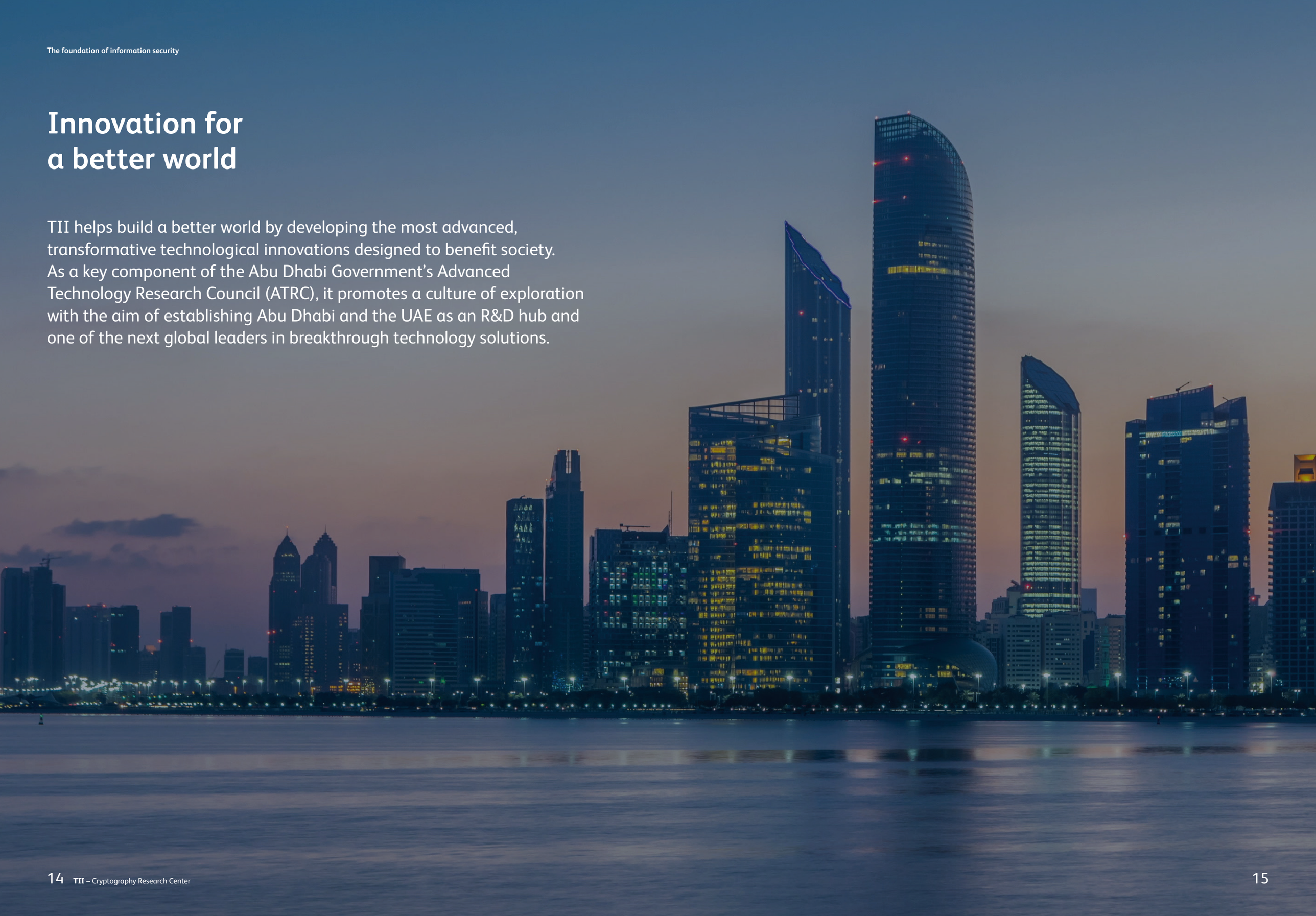
- Theoretical cryptanalysis of symmetric primitives and post-quantum cryptography schemes
- Cryptanalytic attacks against cryptographic implementations
- Leveraging machine learning to design new cryptanalytic techniques

Future challenges, practical solutions

We have assembled a team of passionate professionals from across the global cryptography community and from different areas of expertise to investigate the current and future challenges of the digital society, and to respond to them with practical solutions.

Innovation for a better world

TII helps build a better world by developing the most advanced, transformative technological innovations designed to benefit society. As a key component of the Abu Dhabi Government's Advanced Technology Research Council (ATRC), it promotes a culture of exploration with the aim of establishing Abu Dhabi and the UAE as an R&D hub and one of the next global leaders in breakthrough technology solutions.



Ahead of the curve, beyond tomorrow

Our Visiting Scholars Programme provides distinguished researchers at master's and doctorate levels valuable opportunities for professional development, networking and acquiring industry experience. All of our fellows conduct research on specialized topics, with options for both short-term and long-term stays. They collaborate with our experts, present talks at national and international conferences, and host public workshops in their areas of expertise and research.

We also provide exceptional opportunities for post-graduate students to spend two to three years working with our leading principal investigators. During this time, they can also collaborate with local and international academic institutions. In addition, we offer a number of year-long internships opportunities for both graduate and undergraduate students.

CRC collaborates with leading research institutions in the UAE and around the world to conduct advanced research in areas of strategic importance.

Cryptography Research Center

Technology Innovation Institute LLC
P.O. Box 9639
Abu Dhabi, UAE

tii.ae/cryptography