



ToDiQT

Towards Device-Independent Quantum Technologies



Consortium: Gláucia Murta (Coordinator), Jean-Daniel Bancal, Peter Brown, Felix Huber, Stefano Pironio, Ramona Wolf

CERTIFYING QUANTUM TECHNOLOGIES

The challenge

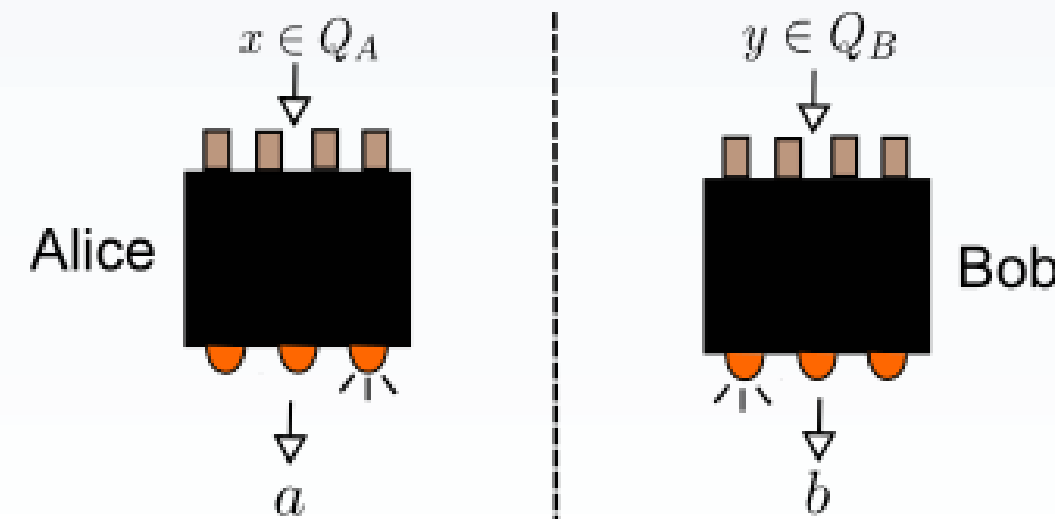
Quantum technologies promise transformative applications in communication and computing, but their guarantees often depend on trusting detailed device models.

Noise, drifts, model mismatch, malicious devices

Loss of security and reliability

Device-independence

Device-independent certification treats devices as black boxes and uses only observed input-output statistics

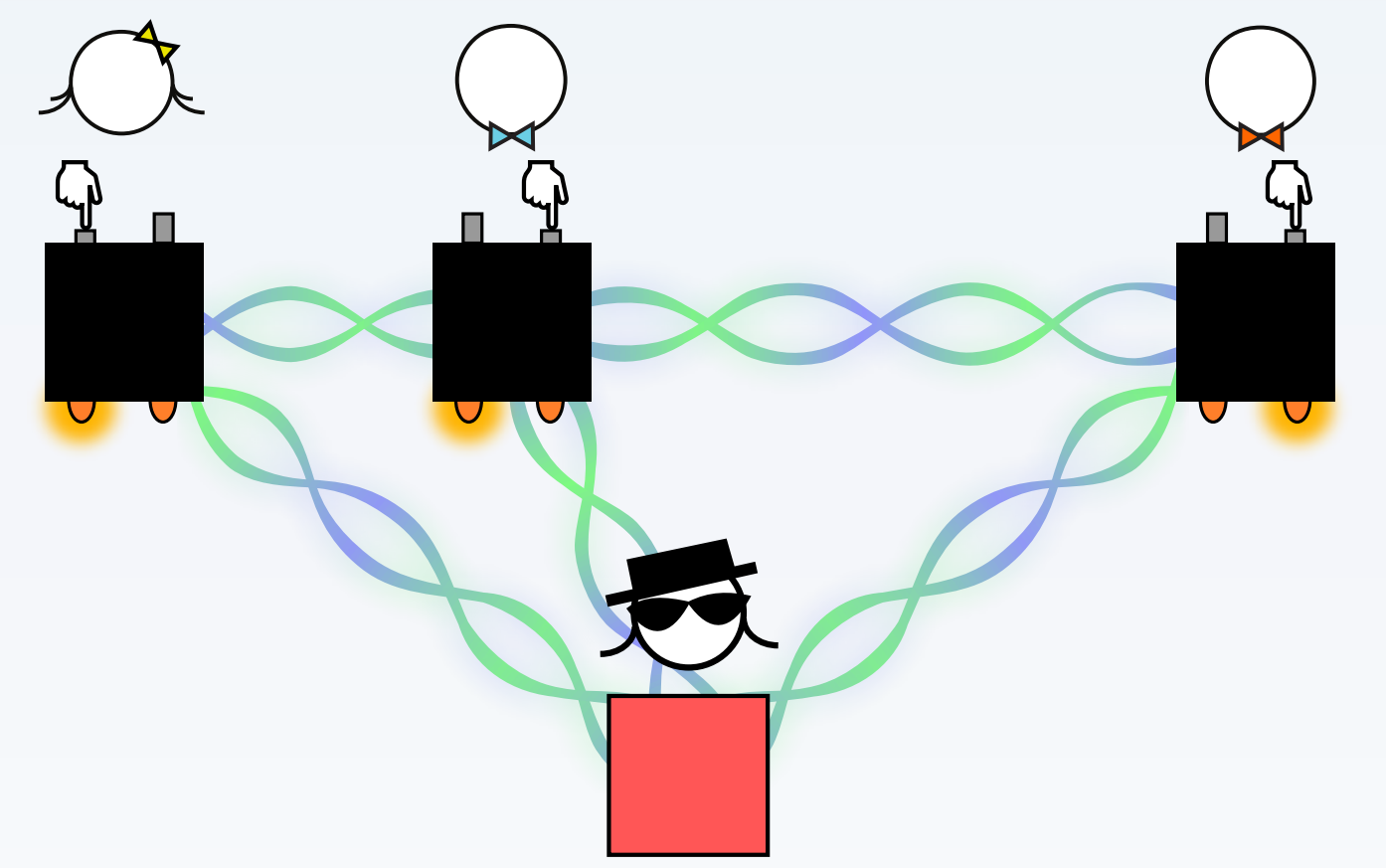


ToDiQT vision

Make device-independent certification practical for quantum communication and quantum computing.

The project develops tools and protocols that are robust to finite statistics, noise, imperfect devices and realistic implementation constraints.

CORE CONCEPT



Observed statistics: $p(ab \dots | xy \dots)$

Bell violation

Cryptographic security

NISQ verification

Fault-tolerant QC

Quantum nonlocality certifies properties of the state and measurement devices without relying on assumptions about their internal workings.

TARGETED BREAKTHROUGHS

From foundational certification to practical quantum technologies

1. **Practical DI certification tools** reducing experimental and computational costs.
2. **Robust DIQKD protocols** with improved finite-size thresholds.
3. **Hybrid DI cryptography** combining nonlocality, post-quantum cryptography and physical assumptions.
4. **DI certification of NISQ devices** through one-shot verification of MBQC resources and gates.
5. **Foundations for DI fault-tolerant computing** via verification of logical code states and operations.

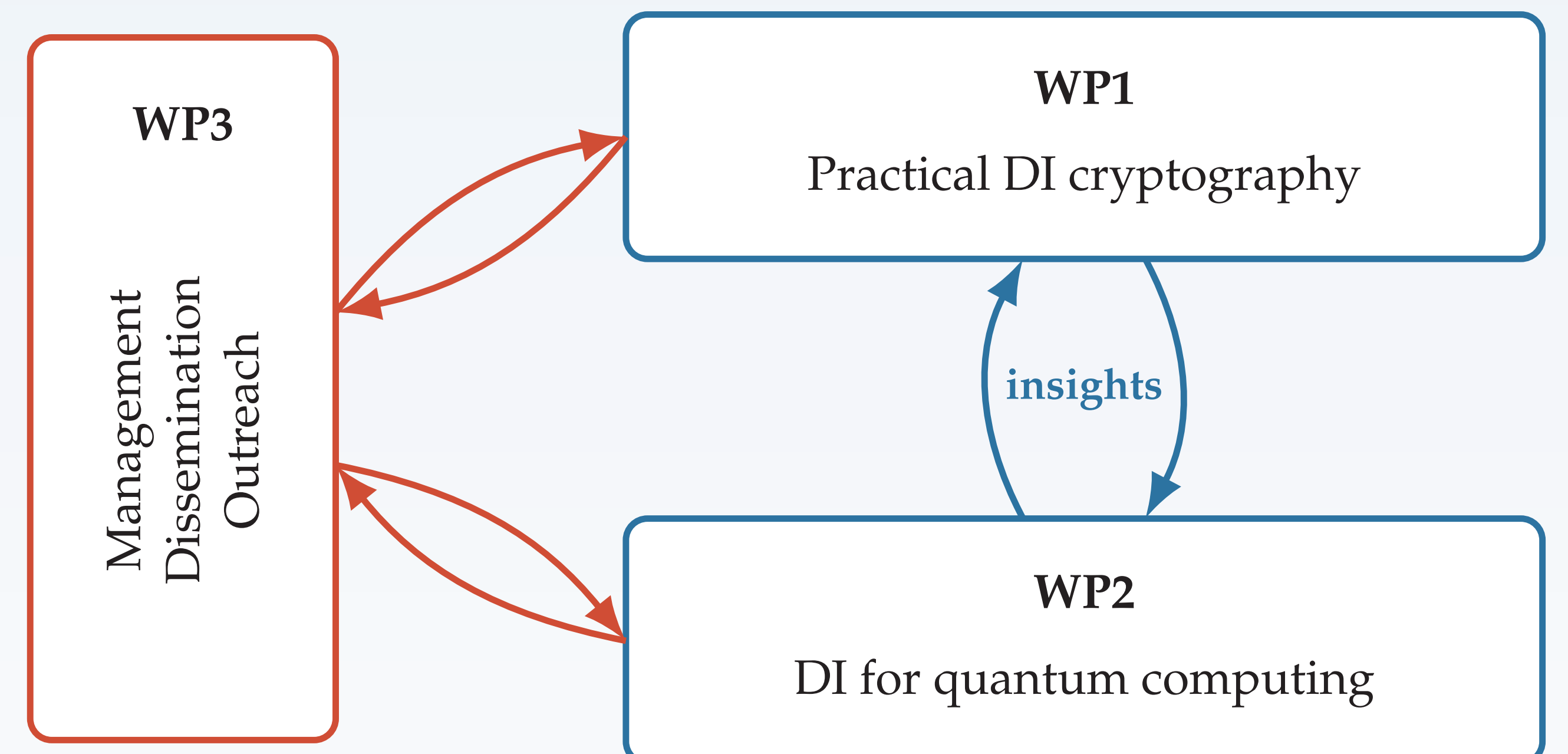
SCIENTIFIC AMBITION AND NOVELTY

Current device-independent protocols are limited by finite-size effects, experimental imperfections and high resource requirements. ToDiQT addresses these limitations by developing certification methods designed for realistic quantum technologies.

- **Beyond standard Bell tests:** routed Bell scenarios, semi-DI techniques and high-dimensional correlations.
- **Beyond asymptotic certification:** one-shot methods for finite-resource quantum computation and verification.
- **Beyond purely information-theoretic models:** hybrid DI protocols using post-quantum and physical constraints while aiming for strong long-term guarantees.
- **Beyond cryptography alone:** a unified device-independent roadmap for communication and computation.

ToDiQT bridges abstract device-independent theory and near-term quantum hardware.

PROJECT STRUCTURE



- **WP1:** Develop practical DI and semi-DI protocols for realistic communication scenarios, exploring new scenarios such as routed Bell tests and computational and physical constraints.
- **WP2:** Extend DI certification to quantum computing, targeting verification of quantum computing resources and certification of quantum advantage.
- **WP3:** Coordinate the consortium, support knowledge transfer between cryptography and computing, and maximize scientific impact.

WP1 and WP2 run in parallel: continuous knowledge exchange strengthens both cryptography and computing. WP1 methods will inform WP2 certification tools, while WP2 insights will inspire refinements in WP1 protocols.

CONSORTIUM

Complementary expertise across device-independent certification, cryptography, quantum computing and optimization methods.

DI certification
self-testing

Cryptography
security proofs,
finite-size analysis

Computation
MBQC, QEC,
logical states

Optimization
SDP, symmetry
reductions

6 PIs • 6 Institutions • 4 EU Countries



TAKE-HOME MESSAGE

Device-independence provides the strongest certification paradigm for quantum technologies.

ToDiQT develops the theoretical and computational tools needed to make device-independent cryptography and quantum-computing certification practical, robust and scalable.