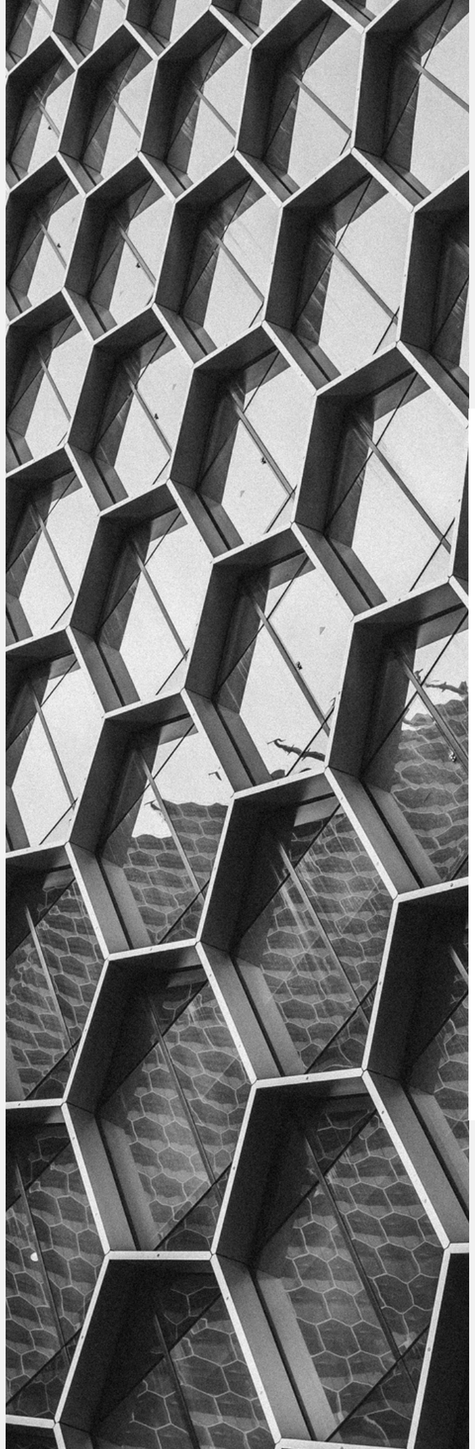
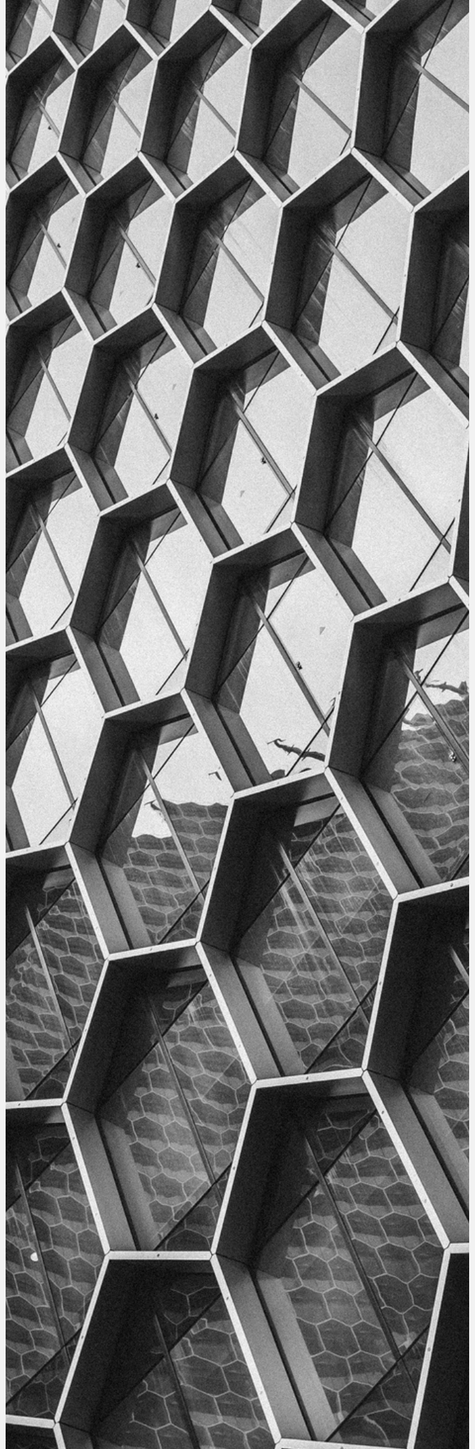


Funded by
the European Union

MILESTONES TO BE ACHIEVED IN 2024:

MILESTONE	WP	INSTIT.	DUE DATE	MEANS OF VERIFICATION
Organizing Schools	WP4	UNIPD	31 March 2024	All Schools held
Security analysis of practical quantum-interference based QKD	WP1	UVIGO	30 Nov 2024	Key rate analysis includes typical transmitter flaws
Formal model for KE is developed	WP1	TU/e	30 Nov 2024	The model for KE considers quantum adversaries
Analysis of quantum-enhanced MPC	WP1	SU	30 Nov 2024	Includes definition of hybrid MPC scheme
Quantum security definition of MHF	WP1	UvA	30 Nov 2024	The definition includes quantum adversaries
Design new quantum attacks against PQC cryptosystems	WP1	RUB	30 Nov 2024	The attacks improve the state of the art
Autonomous prototype for TF-QKD	WP2	UNIPD	30 Nov 2024	Continuous operation of TF-QKD prototype (>1hr

Milestones to be achieved in November 2024 are scientific!



Funded by
the European Union

MILESTONES TO BE ACHIEVED IN 2024:

Assessment of different network-compatible protocols	WP2	UVIGO	30 Nov 2024	Analysis includes devices present in the established network architecture
Design of an intermodal quantum communications interface	WP2	UNIPD	30 Nov 2024	It includes free-space and fibre-based QKD
Design quantum repeater protocols for packet-switched networks	WP2	UNIPD	30 Nov 2024	The protocols are compatible with packetswitched networking
Design of next-generation hybridisation methods for authentication and data integrity	WP2	UVIGO	30 Nov 2024	The methods use QRNG, PUFs, QKD and PQC
Security reductions for correctness error finding in FO KEMs	WP1	DTU	30 Nov 2024	The security reduction technique yields a security bound for FO KEMs
Design multi-user cryptographic schemes for quantum networks	WP2	UVIGO	30 Nov 2024	The schemes involve more than two users

Milestones to be achieved in November 2024 are scientific!