

Q5: Are we confident that quantum spin microscopy will work?

A5: QMOR reaches deeply into geometry, algebra, informatics, cryptography

• QMOR's emerging mathematical frontiers

public key distribution via private quantum model order reduction (QMOR)

QMOR's mathematical frontier touches upon deep mysteries: the most powerful formalisms of modern mathematics — geometric, algebraic, informatic, and cryptographic — are now being embraced by quantum system engineers.

MATHEMATICS AT THE INTERFACE OF CRYPTOGRAPHY, QUANTUM PHYSICS, AND ENGINEERING SIMULATIONS

We suppose that Alice is conducting a simulation which is MOR-compressible in Alice's basis, while Bob conducts a simulation that is MOR-compressible in Bob's basis. By taking turns at each simulation step, Alice and Bob can conduct a joint simulation, such that—as our numerical experiments have shown—the resulting trajectory is compressible in *both* bases.

Now Alice can deduce information about Bob's basis by studying the public trajectory (with the help of her private basis), and Bob can similarly learn about Alice's basis (with the help of his private basis), but Eve (having access to neither Alice's private basis nor Bob's private basis) cannot easily deduce either basis, even if she has complete access to the publicly shared quantum trajectory: this is the "hard" problem of quantum MOR cryptography.

Therefore, knowledge of the public quantum trajectory, combined with private knowledge of how it was created, suffices for Alice and Bob to compute a shared key. The security of this key depends on Eve's inability to solve a "hard" (yet natural) problem in theoretical physics, namely, to deduce the basis states of Alice's and Bob's joint simulation from the public trajectory.

Our pilot implementation of this key distribution method required no changes to our MOR code, and yet, the resulting scheme notably resembles—in its algebraic and projective aspects—a hybrid of elliptic curve cryptography with Ajtai-Dwork lattice cryptography [2].

