Despite quantum's gains, standard computers still rule

January 3 2014, by Richard Ingham, Laurent Banguet

View of the National Security Agency (NSA) in the Washington suburb of Fort Meade, Maryland, 25 January 2006

Quantum computing is getting the headlines these days, with buzz among scientists of giga-powered number-crunching and unbreakable encryption.

The US National Security Agency (NSA) is reportedly advancing

towards a quantum computer that could crack almost any conventional algorithm.

The NSA plans were leaked by contractor Edward Snowden and reported by The Washington Post on Thursday.

Details of its work remain sketchy, though. And the agency is only one of many players, both public and corporate, in a field that must overcome many hurdles before it can dethrone standard computing.

Conventional computers work by processing binary code—an information currency that exists in one of two states, either zero or 1.

Quantum computers, though, break free of the two-state constraints.

They harness the principle of quantum mechanics, when strange things occur through the state of an atom's spin, something called angular momentum.

In a quantum state, the atom goes into a condition called superposition. It can hold the value of zero or 1 or both values at the same time.

This juggling trick holds out the possibility of parallel processing on a massive scale.

An algorithm that a conventional supercomputer might take years to break could be cracked by so-called qubits, or quantum bits, in a fraction of the time.

"The special properties of qubits will allow quantum computers to work on millions of computations at once," says IBM. "For example, a single 250-qubit state contains more bits of information than there are atoms in the Universe."

Daunting engineering obstacles have to be overcome, though. In order to achieve the fragile quantum state, a cloud of atoms has to be cooled to near-absolute zero and controlled by pulses of laser.

Changes in temperature, electromagnetic waves and minute defects in material can all wreck the sought-after superposition that fuels the qubit.

Scaling up these computers from hugely expensive, highly protective labs represents "an enormous practical challenge," the Nobel jury said in 2012, when it awarded that year's physics prize for fundamental work on the quantum state.

Quantum's other big plus is a phenomenon called entanglement.

Particles created in a quantum state behave like psychic twins.

Even if they are far apart, a disturbance to one particle affects the other, a phenomenon that Einstein once called "spooky action at a distance."

Thus if a message sent in a quantum state is intercepted en route, the entanglement is destroyed—and alarm bells ring that someone is eavesdropping.

Achieving quantum cryptography

Entanglement is the big goal of quantum cryptography.

It holds out the possibility of creating a unique, one-time code shared only by sender and recipient that would be almost impossible to decrypt by an outsider. Better still, the message could not even be touched during transmission.

Even without entanglement, though, the quantum state can be useful in

cryptography, said Philippe Grangier, a specialist in quantum optics at France's National Centre for Scientific Research (CNRS).

His team has done tests that sends a standard-encrypted message, along with a quantum-encrypted key, in squirts of light down a fibre-optic cable.

Once received, the key is then used to decode the message.

The technique uses the quantum signature in the key as a burglar alarm, Grangier said in a phone interview.

"Just the slightest interception of the data will reduce the size of the quantum key when it gets to the recipient, and the spy gets detected," said Grangier.

"The more the spy perseveres, the smaller the key becomes. Eventually, the connection is cut."

Their greatest length for transmission has been through a cable 80 kilometres (50 miles) long—a distance that is useful for local communications but still way too short for transcontinental use or more.

Going beyond this distance lies the conundrum of how to amplify a weakening light signal down a cable so that the data is repeated but does not lose its quantum state through interference.

Other techniques aim at overcoming the "repeater" problem by line of sight laser transmission, in theory to satellites in near-Earth orbit.

Citation: Despite quantum's gains, standard computers still rule (2014, January 3) retrieved 25