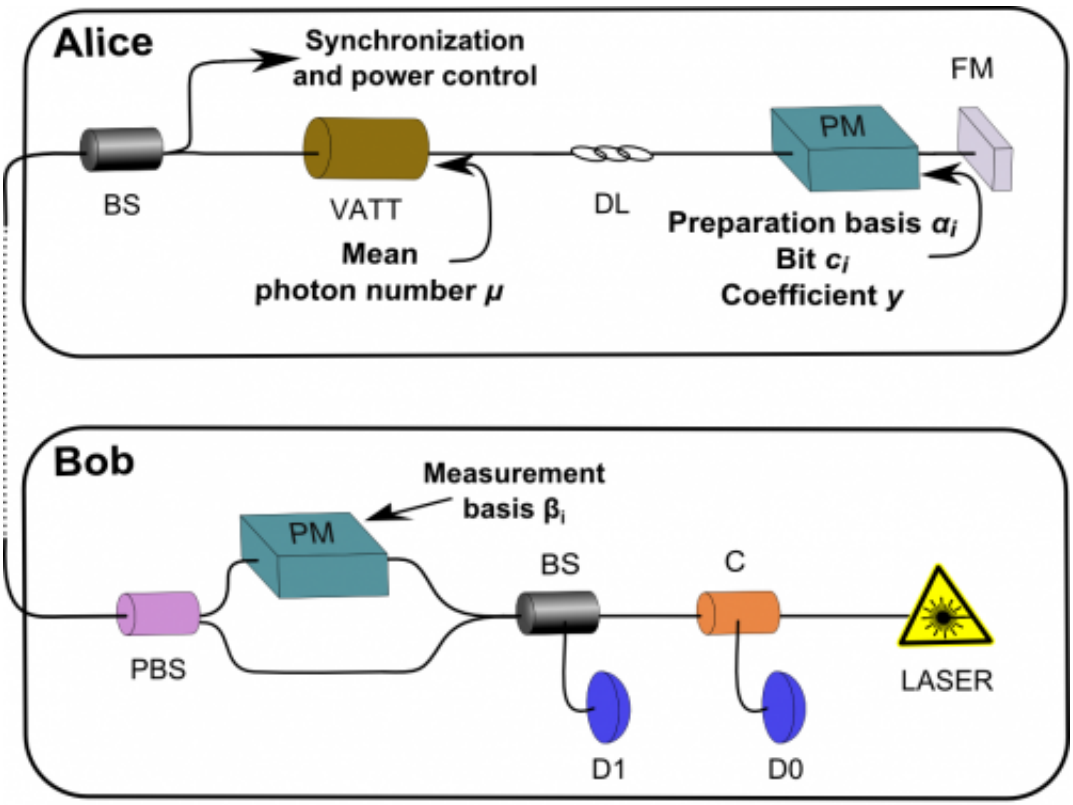
Heads or tails: Experimental quantum coin flipping cryptography performs better than classical protocols

May 26 2014, by Stuart Mason Dambrot



Experimental setup of the plug-and-play Clavis2 system. This type of interferometric setup does not necessitate continuous polarization control and alignment, and therefore guarantees excellent system stability for quantum communications. Courtesy: Anna Pappa, LTCI, CNRS—Télécom ParisTech

(Phys.org) —Cryptography – the practice and study of techniques for secure communication in the presence of third parties, referred to as *adversaries* – has a long and varied history. In ancient Greece, for example, the Spartan military may have used the so-called *scytale* transposition cipher to encrypt and decrypt messages. Steganography (hiding the existence of a message) was also first developed at that time as, according to Herodotus, a message tattooed on a slave's shaved head and then hidden under regrown hair – and is still in use in the form of invisible ink, microdots, and digital watermarks. That said, applying complexity cryptography to quantum communication is and will continue to be essential – and while quantum cryptographic primitives are in principle more secure than classical protocols, demonstrating this in a practical system has proven difficult.

Recently, however, scientists at Laboratory for Communication and Processing of Information (LTCI), Paris – a joint research lab between Centre National de la Recherche Scientifique (CNRS) and Télécom ParisTech – have experimentally implemented a quantum coin flipping protocol that performs better than any classical system over a distance suitable for deployment in metropolitan area optical networks. Based on an enhanced commercial quantum key distribution (QKD) device, the approach is nearly perfectly secure against bounded adversaries – a feature the researchers state make it a practical toolbox for designing secure quantum communications systems.

Researcher Anna Pappa discussed the paper she and her co-authors published in *Nature Communications* with *Phys.org* – beginning with the challenge of addressing the historical difficulty of demonstrating the known information-theoretic security advantages of quantum versions of coin flipping and other primitives (basic cryptographic algorithms used to construct more complicated cryptographic tools) relative to classical protocols in a practical communication scenario. "Quantum cryptography is a relatively new field that emerged after Bennett and

Brassard's groundbreaking paper in1984[1], which introduced the idea of using quantum mechanics to enhance classical cryptographic protocols like key distribution and coin flipping," Pappa tells *Phys.org*, adding that the main difference between classical and quantum computing is that in the latter, information is contained in the physical properties of the exchanged messages.

"This provides a strong advantage but also hinders straightforward applications of quantum protocols," Pappa point out. "Historically, many protocols that were in theory secure were completely broken in practice, because of limitations in current technology. For example," she illustrates, "previous coin flipping protocols necessitated a single-photon source or an entangled source in order to be secure – but the first is not currently available, while the second cannot be easily deployed for long-distance communications since entanglement is very fragile, and cannot be maintained for long periods of time due to quantum memory limitations. In our research, while we are exploiting the effects of superposition in quantum mechanics, we do not use entangled states – and this is what makes our implementation easily implementable with standard photonic sources."

Another important factor, she notes, is that coin flipping is a protocol used when participants do not trust each other, which makes correcting transmission errors more difficult. At the same time, trusted setting protocols like quantum key distribution (QKD) have in recent years achieved security for distances of more than 100 kilometers. This is due to the fact that measuring a quantum system disturbs that system, and any third party trying to gain knowledge of the key can therefore be detected by the two communicating users.

The researchers also faced the challenge of experimentally implementing a quantum coin flipping protocol that performs strictly better than classically possible over a distance suitable for communication over

metropolitan area optical networks. "The Clavis2 platform that we used was developed by IdQuantique, a company based in Geneva, Switzerland that works closely with researchers worldwide in order to test and verify their systems," Pappa recalls. "There were many challenges that we faced during the implementation of our coin flipping protocol using a commercial plug-and-play system originally designed to perform key distribution between two parties (commonly referred to as Alice and Bob) who trust each other and want to establish a common secret key.

Reconstructed ancient Greek scytale, an early cipher device. Courtesy: Wikimedia Commons

"In quantum coin flipping," Pappa explains, "the players do not trust each other, since both want to win the coin flip, so they try to cheat by numerous ways – for example, by increasing the average photons contained in the pulses, or by declaring that they lost some message when they do not like the result of the protocol. Furthermore, they could

try to exploit the physical properties of the system, like an asymmetry in the creation of the different quantum states used, or in the detection of the different states. We therefore needed to account for all imperfections of the system and come up with detailed security proofs in order to show the quantum advantage of our implementation."

Relatedly, the scientists sought to provide combined quantum coin flipping protocols that were almost perfectly secure against bounded adversaries. "We wanted to find a way to provide security against an adversary of unknown abilities, so we used two schemes that are secure against adversaries of limited power – that is, noisy storage and computationally bounded – and enhanced them with our protocol." To do this, they we analyzed the bounded protocols and found the exact step where an unbounded adversary would be able to perfectly cheat, and then strengthened that step using our protocol."

"A problem that we faced," Pappa tells Phys.org, "was that, since the players do not trust each other, they cannot perform error-correction and other procedures that necessitate collaboration between the parties, therefore limiting the tolerance to errors. We therefore needed to make some changes to the system in order to observe a quantum advantage for a considerable channel length. For example," Pappa explains, "the detectors on Bob's side had to be replaced because they had low detection efficiencies and high dark counts, and we could not observe any quantum advantage for any channel length. By substituting them with better quality detectors, we managed to experimentally demonstrate a quantum advantage for a channel distance of 15km. In addition," she continues, "photon source attenuation was very high. This meant that essential Clavis2 procedures could not be executed, requiring significant reprogramming." Finally, Pappa notes, in order for the players to decide on the protocol parameters, the scientists had to perform detailed careful system analyses to identify system component losses and errors in order to, for example, estimate how many times they need to run the protocol

and how much attenuation needs to be applied.

An essential consideration in designing a secure communications protocol is identifying and devising appropriate countermeasures against potential side-channel attacks – and Pappa points out that a positive aspect of using the Clavis2 platform is that, as mentioned, it is commercially available and can be tested by researchers worldwide. "Using a plug-and-play system makes our protocol potentially vulnerable to the specific types of attack on the particular system – for example, the famous blinding attack that was performed some years ago, which allowed an eavesdropper to break QKD protocol security, and it therefore could also break the security of our protocol as well. IdQuantique has installed an extra power meter in the Clavis2 system as a countermeasure for this attack – but of course, everything is secure until someone discovers a new attack…and then it isn't secure anymore!"

In addressing these challenges, Pappa says that their research work was very multidisciplinary, combining tools from quantum mechanics, engineering and programming. The scientists based their protocol on a previous loss-tolerant protocol that could not be straightforwardly implemented because it required entangled states – but this led to too much noise, and consequently to a very small communication distance. "We decided to abandon complete loss-tolerance and introduce a small honest abort probability – that is, a probability that two honest players cannot obtain a coin flip at the end of the protocol – allowing us to address more errors in the implementation and use a simple attenuated laser source," she explains. "The resulting quantum advantage can be estimated by comparing the relation between the quantum cheating probability and the honest abort with the classical bounds given by Hänggi and Wullschleger in 2011[2]. Moreover," she continues, "we analyzed adversaries that have almost absolute power – for example, total control of the communication channel, ability to have perfect equipment and knowledge of the other party's equipment – and we

provided detailed security proofs which included exhaustive analyses of all types of attacks on a theoretical level."

In their paper, the researchers state that their results offer a useful toolbox for future secure quantum communications. "I tend to believe that future telecommunication networks will comprise of quantum and classical agents of different capabilities, with classical or quantum small-scale computers delegating complex computations to powerful quantum servers. It is therefore important to provide cryptographic protocols that are secure against different types of adversaries – and this is what our combined protocols achieve." She illustrates that while the cheating probability limit of over 90% is very high, it is for an all-powerful adversary who has perfect equipment and controls everything except the other player's device. "This type of adversary is not very likely to exist in the foreseeable future," she says, "but even if it is built at some point, our quantum protocol will still provide better security than a classical protocol."

The paper also discusses possible new techniques to deal with the imperfections of the current implementation and the inherent limitations to the attainable communication distance. "Our protocol's communication distance was limited due to losses and errors in the different components of the system," Pappa explains, "but experimental researchers put continuous effort in improving all these components, which will also improve our protocol's performance. A straightforward way to increase the channel length is to use better detectors, with higher detection efficiencies and lower dark count rates." (The *dark count rate* is the average rate of registered counts without any incident light.)

The scientists also hope that their work is a step towards simplifying quantum protocols that achieve almost perfect security but, until now, require large-dimension entangled states. "With our work, we tried to bring more attention to quantum two-party protocols other than quantum

key distribution, and show that it is possible to achieve a level of security that is better than classically possible," Pappa tells Phys.org. "For example, there exists another version of coin flipping, called *weak coin flipping*, which can in theory achieve perfect information-theoretic security. However, while it's not easy to see how such a protocol could in practice be implemented – it requires a complex setup that is not possible with present-day technology – a simpler protocol for weak coin flipping would be a breakthrough in the quantum cryptography field."

Regarding the potential impact of their work, Pappa concludes, "We believe that we've provided a full security analysis for the distrustful model that can be used in future analyses of other two-party cryptographic protocols, and have also showed ways to combine quantum protocols in order to provide different layers of security which could be extended to other primitives beyond coin flipping."

Moving forward, Pappa is involved in an Entanglement Verification project studied in a cryptographic setting that she says could prove useful for distributed computing schemes and multiparty computations, and is also working on Bayesian Games (in which information about characteristics of the other players is incomplete) and how quantum information could provide higher gains and better points of equilibrium.

More information: Experimental plug and play quantum coin flipping, *Nature Communications* 5:3717, 24 April 2014, doi:10.1038/ncomms4717

Related:

[1]Quantum cryptography: Public key distribution and coin tossing (PDF), *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175-179*, 1984

[2]Tight bounds for classical and quantum coin flipping, arXiv:1009.4741v2 [quant-ph], 26 Apr 2011, doi:10.1007/978-3-642-19571-6_28