

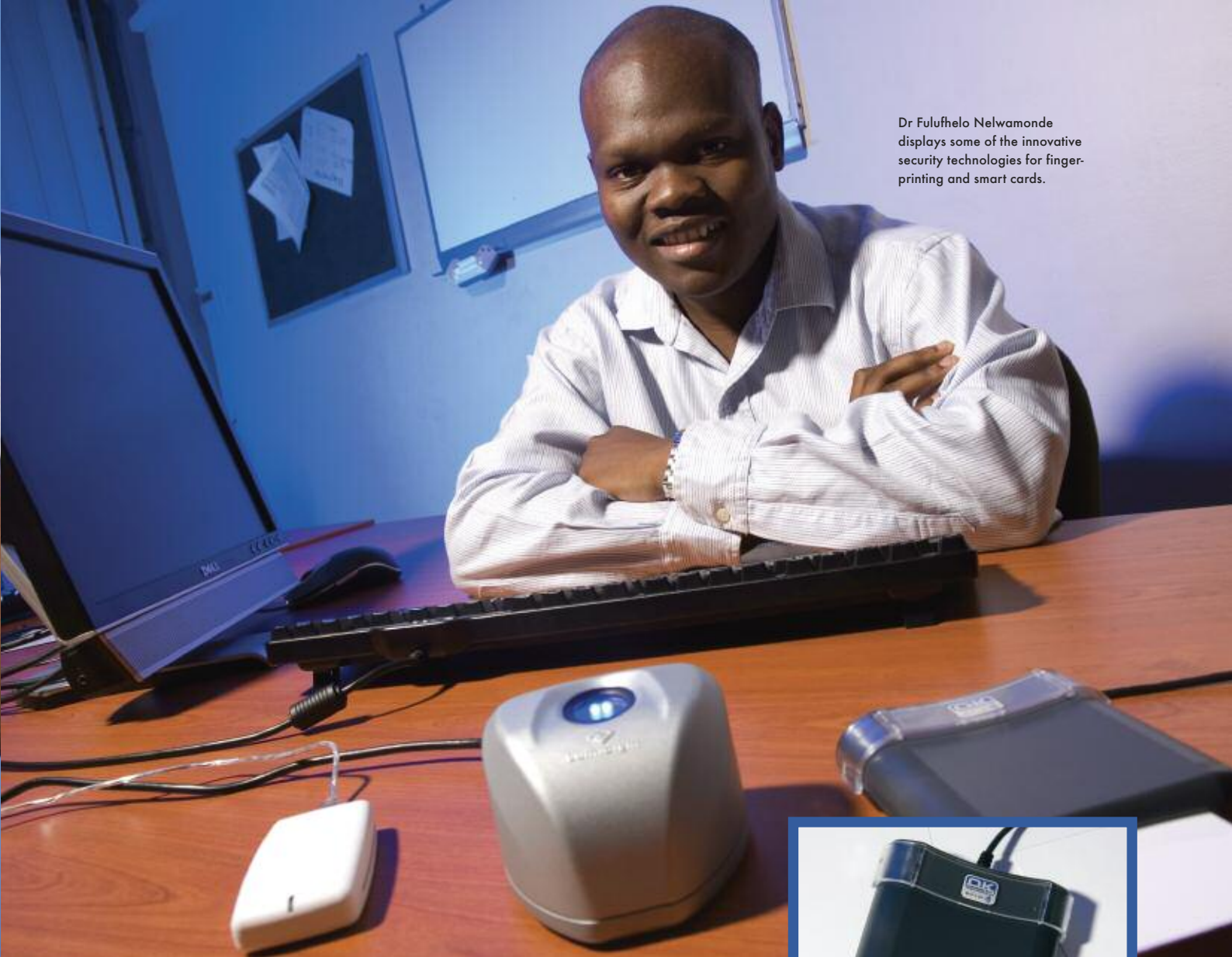


# Building a strong local information security competence

and reducing SA's dependency on  
imported information security solutions

BY DR FULUFHELO NELWAMONDO

South Africa, like many other countries, faces a number of challenges relating to information security. The CSIR engages vigorously in the research, development and implementation of information security technologies in support of national projects.



Dr Fulufhelo Nelwamondo displays some of the innovative security technologies for finger-printing and smart cards.

IN AN EFFORT TO SECURE INFORMATION, South Africa has tended to rely on security solutions from other countries. While this may seem like a viable solution, safeguarding our national information and infrastructure using already-available technologies raises a number of questions. How well do we know or understand the technology that we are importing? How much permission are we given to control it? Clearly, blindly importing technologies to safeguard our critical infrastructure makes us very vulnerable.

Think of importing iris scanners from other continents. While it seems a simple task to procure, we are not sure that the models used in the development of such technology fit the people of this country. Can the same features be extracted from South Africans as were the case for people whose features were used in the development of the algorithms? To address these and other challenges, South Africa needs to strengthen its technological compe-

tence in information security. Information security is about the protection of confidentiality, integrity and the infrastructure that stores/holds such critical information. The CSIR's work in this field is also aimed at ensuring that the government has adequate technology solutions, as well as the required strategic independence. To achieve this, the CSIR is completing projects on identity authentication systems.

In this study, understanding the dynamics of South Africans in relation to a particular biometric feature, is key. Identity authentication through the use of smart cards and biometrics is the primary skill required. Of equal importance for strategic independence, are skills in data mining, network security, cryptography, as well as signal and image processing.

**Enquiries:**  
Dr Fulufhelo Nelwamondo  
fnelwamondo@csir.co.za



Angela Dudley and Dr Stef Roux

# Twisted light used in information security systems

BY ANGELA DUDLEY, DR STEF ROUX AND DR ANDREW FORBES

**CSIR researchers use 'twisted' light to study new quantum-based information security systems.**

**"The idea is to make it too difficult for your adversary to solve the riddle of what the key is."**

## Understanding light

To understand the structure of 'twisted' light, it is useful to start with an ordinary light beam with zero twist, namely a plane wave. Imagine that one could freeze the plane wave and that one could then visualise the result as a collection of adjacent one-dimensional waves, consisting of troughs and crests. If the crests of all these waves were connected, they would form a surface that looks like an infinite flat plane. In fact, consecutive crests will form consecutive planar surfaces that are parallel to each other and all these surfaces would be perpendicular to the direction in which the light was propagating. These surfaces are known as wavefronts and they are separated from each other by a distance of one wavelength.

The wavefronts of twisted light no longer look like those of ordinary light but instead combine into a corkscrew-shaped wavefront. Following the same argument as before, if we connect the crests of all the adjacent waves to form the surfaces that define the wavefronts, we find that they have a helical (corkscrew) shape.

If we 'unfreeze' the beam and watch the movement of the wavefronts, we will see that they rotate around the central beam axis. Near the centre of the beam, the wavefronts are twisted to such an extent that they define a singularity, causing the intensity of the light in the centre of the beam to vanish. This dark spot produces the visual distinction between twisted and ordinary light. When ordinary laser light is focused it appears as a bright point. On the other hand, this is not what happens with twisted light. A focused twisted light beam produces a ring of light with a dark centre. The size of the dark centre depends on the number of twisted wavefronts present in the light beam.

Another major difference is that the light in a twisted light beam does not propagate directly forward, parallel to the beam axis as in an ordinary light beam, but tends to move sideways in opposite directions on opposite sides of the beam. The net result is that the twisted light beam carries orbital angular momentum (OAM).

Light can be produced with any number of twists. The increased number of twists also implies that the sideways movement of the light increases, which in turn produces an increase in OAM. The OAM in a twisted light beam is therefore proportional to the number of twists. If one now considers the quantum nature of light one would discover that each photon in a twisted light beam carries a precise quantum of OAM, which is also proportional to the amount of twist in the light beam.

## Twisted light in securing communication

The ability to increase the twist (and thereby the OAM) of a beam of light plays an important role in the applications of twisted light and particularly in secure quantum communication.

Consider a conventional form of communication such as using a flashlight to send a message. In this simple example one would modulate the beam by turning it on and off. This is referred to as binary information transfer, as only two possible choices or states exist. Similarly, Morse messages can only consist of 'dots' and 'dashes'. In more sophisticated (yet conventional non-quantum) communication schemes, more levels are used to increase the amount of information per pulse.

Note, however, that in all conventional schemes only one specific state can exist in any particular pulse. On the other hand, in



quantum communication an object ('pulse') can simultaneously have different states or 'levels'. One can think of this as different 'realities' that can exist simultaneously. This combination of different realities is called a quantum state. The benefit is that quantum communication allows a certain economy in conveying the information. The objects that carry the information in quantum communication would have the ability to exist in particular quantum states. One would for instance use photons (the quantum particles of light), rather than pulses of light, like those one would produce with a flashlight.

In quantum communication systems the information has, until recently, been encoded in the spin states of photons, which are restricted to only two states (clockwise and anticlockwise), leaving us at the same point as in the flashlight example. The OAM of photons offers an infinite number of possible states, which can be adjusted simply by changing the number of twists in the beam. This opens the way to a 'twisted' alphabet: simply set a photon in a single helix (single twist) beam of light to represent the letter 'A,' a double helix for the letter 'B,' up until 26 helices for the letter 'Z.' What is remarkable here, is that because OAM is carried down to the single photon level, one can encode this alphabet at the quantum level.

When two photons are used in the system, it is possible to 'entangle' their quantum states in such a way that in each reality there is a fixed relationship between the states of the two photons. Altogether the alternative realities allow all the possible states for each photon, but in every one of the realities the state of one photon dictates the state of the other photon. When a property of one of the photons is measured, all but one of the realities would vanish, leaving only one reality, thus fixing the states of both photons. One of the photons would also be destroyed during the measurement.

## Enter quantum cryptography

The property of quantum entanglement allows quantum cryptography to become viable. For two photons that are entangled, only two parties are allowed to take part in the communication process. Any additional eavesdropper would destroy one of the photons and cause all but one of the realities to vanish. This would then be noticed by the legitimate parties and inform them of the existence of the eavesdropper.

In the case of twisted photons, the entanglement is in the OAM states, and offers fundamentally secure communication over an insecure communication channel independent of the adversary's technological advantage. This differs from classical cryptography at the most fundamental level: it is physical laws, rather than computational complexity that provide the security basis of quantum information science. Classical cryptography systems exploit mathematical complexities and computational inefficiencies to distribute encryption keys. The idea is to make it too difficult for your adversary to solve the riddle of what the key is. The security provided by these classical techniques, however, is bound by advancements in mathematics and computing power.

Quantum cryptography using twisted light, physically encodes the encryption key within the OAM states of the photons – an application of quantum physics rather than a man-made algorithm. So there is no possibility of cracking this code unless quantum physics as a theory is wrong. If an eavesdropper should try to intercept the message, the quantum states change, modifying the cryptographic key and thereby alerting the legitimate parties involved. Thus, quantum systems for secure information are considered the technology of the future, and twisted light may just be the enabling technology to make it happen.



Dr Andrew Forbes

## Creating secure information systems

Research is currently underway to exploit these quantum properties to create secure information systems. Our team is working with laboratory-based quantum optics experiments: creating and manipulating photons that carry OAM. In particular the group is studying how the entanglement of OAM photons decreases due to unwanted interactions with their environment (for example, the atmosphere), and possible means to overcome these limitations. The group recently started a three-year programme to investigate long distance quantum communication through free-space, for secure information transfer. The hope is to perform world-leading demonstrations of this technology in the near future, heralding South Africa's arrival in the quantum world.

Enquiries:  
Dr Andrew Forbes  
aforbes@csir.co.za