Refining Quantum Cryptography

Richard Hughes and Jane Nordholt

Science **333**, 1584 (2011);
DOI: 10.1126/science.1208527

M. tuberculosis (*4*). In the bacterium, prodrug activation is catalyzed by pyrazinamidase, an enzyme encoded by the *pncA* gene that converts the amide to pyrazinoic acid (POA), a weak carboxylic acid. Almost all PZA-resistant strains of *M. tuberculosis* have *pncA* mutations that reduce enzyme activity and abolish POA production (*5*). It has not been clear, however, why the loss of POA production confers resistance, or what target POA is acting against.

To clarify matters, Shi *et al*. used affinity chromatography and mass spectrometry to identify four proteins that were potential POA targets. Using a variety of methods, including genetic analysis of PZA-resistant mutants, the researchers identified the ribosomal protein S1 (RpsA) as a previously unrecognized target of POA. RpsA plays two important roles in ribosome function. When *M. tuberculosis* is living in conditions that enable it to reproduce exponentially, RpsA binds to upstream sequences of mRNA to ensure connectivity to the 30*S* ribosomal subunit and thus efficient translation. In contrast, when times are hard—during starvation, for instance—RpsA engages in trans-translation, which "spares" ribosomes by restarting those that "stalled" while in the process of decoding mRNA (*6*). In this case, RpsA's C terminus specifically binds to a transfer-messenger RNA (tmRNA), and a complex forms with SmpB (small protein B) and EF-Tu·GTP (elongation factor Tu containing guanosine triphosphate) (*7*). This complex restarts translation by switching to the tmRNA template from the mRNA template; protein synthesis then resumes by incorporation of an Ala residue (see the figure). This ribosome-sparing role appears to be critical to enabling dormant bacteria to survive stress.

To establish whether POA blocked classical translation, trans-translation, or both, Shi *et al*. used an elegant cell-free in vitro translation assay. They concluded that POA only inhibits trans-translation and that this inhibition strictly depended on wild-type *M. tuberculosis* RpsA. This finding has important ramifications for TB drug discovery, which in the past decade has had limited success using genome-inspired target-based screening to generate potential leads (*8*) and for finding new antimicrobial compounds. Pharmacological validation of a potential target is an important prerequisite for drug discovery (*9*), and few such targets are known in *M. tuberculosis* (*10*). Now, investigators can add the trans-translation apparatus to this short list and, in particular, the RpsA protein.

It is anticipated that the power of x-ray crystallography and structure-assisted drug design will be brought to bear on the RpsA-POA complex, as well as other components of the trans-translation system, as there is considerable room for improving the efficacy of PZA. The challenge will be finding a compound that has effects at nanomolar levels and can penetrate the mycobacterial cell. Overcoming this challenge, however, could have widespread and potentially profitable implications. It could lead to a drug that kills the latent form of TB, which afflicts much of the world's population. In addition, if pharmaceutical companies consider the TB market to be insufficiently lucrative to justify the R&D investment, they should not overlook the possibility that research in this area could lead to a new broad-spectrum antibiotic. Indeed, on the basis of genetic validation in *Helicobacter pylori*, a pathogen of the human stomach, researchers have already proposed that the trans-translation machinery is an excellent target for the development of novel antibacterials (*11*).

References

1. W. Shi *et al*., *Science* **333**, 1630 (2011); 10.1126/science.1208813.
2. V. Chorine, *C. R. Acad. Sci.* **220**, 150 (1945).
3. W. McDermott, R. Tompsett, *Am. Rev. Tuberc.* **70**, 748 (1954).
4. Y. Zhang, C. Vilcheze, W. R. Jacobs Jr., in *Tuberculosis and the Tubercle Bacillus*, S. T. Cole, K. D. Eisenach, D. N. McMurray, W. R. Jacobs Jr., Eds. (ASM Press, Washington, DC, 2005), pp. 115–140.
5. A. Scorpio, Y. Zhang, *Nat. Med.* **2**, 662 (1996).
6. K. C. Keiler, *Annu. Rev. Microbiol.* **62**, 133 (2008).
7. S. Barends, A. W. Karzai, R. T. Sauer, J. Wower, B. Kraal, *J. Mol. Biol.* **314**, 9 (2001).
8. A. Koul, E. Arnoult, N. Lounis, J. Guillemont, K. Andries, *Nature* **469**, 483 (2011).
9. C. Sala, R. C. Hartkoorn, *Future Microbiol.* **6**, 617 (2011).
10. G. Lamichhane, *Trends Mol. Med.* **17**, 25 (2011).
11. M. Thibonnier, J. M. Thiberge, H. De Reuse, *PLoS ONE* **3**, e3810 (2008).

10.1126/science.1212450

PHYSICS

Refining Quantum Cryptography

Richard Hughes and Jane Nordholt

Recent hacking efforts on quantum cryptography systems have resulted in new approaches for more secure communication networks.

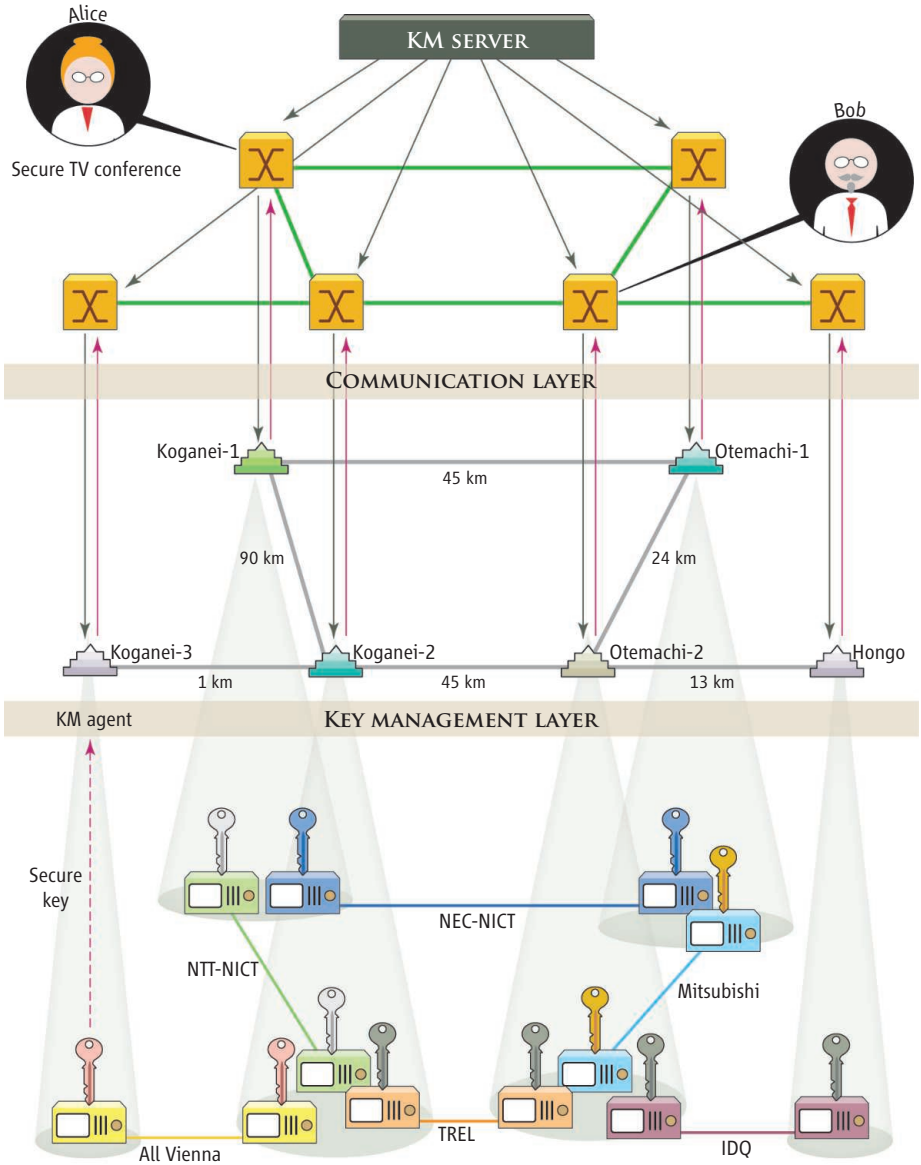
With its promise of security rooted in the laws of physics, quantum cryptography has seen tremendous growth as a worldwide research activity and the emergence of start-up commercial ventures since its invention 27 years ago. But in 2010, quantum hacking results (*1*, *2*) appeared to call into question the validity of the entire endeavor. Instead, the ensuing vigorous debate, combined with major network testbed results in Japan (*3*) and China (*4*, *5*), is defining a new, much brighter future for quantum cryptography research.

Los Alamos National Laboratory, Los Alamos, NM 87545, USA. E-mail: hughes@lanl.gov

Encryption enables users traditionally referred to as "Alice" and "Bob" to prevent eavesdropper "Eve" from learning the content of their communications. Authentication prevents Eve from impersonating either Alice or Bob, or substituting her own messages for theirs. Both confidentiality and authenticity are possible if Alice and Bob share secret random number sequences (unknown to Eve), known as cryptographic keys, used as parameters in their encryption and authentication algorithms. Communications security is thereby reduced to the problem of secret key distribution between Alice and Bob.

The security of traditional key distribution methods is based on computationally intractable problems. Unfortunately, it has proven much more difficult to reliably estimate their future security than either the encryption or authentication algorithms that rely on those keys. And with knowledge of the key, a future adversary could break the encryption of past communications, introducing a retroactive vulnerability. The invention of quantum key distribution (QKD) by Charles Bennett of IBM and Gilles Brassard of the University of Montreal in 1984 provided a solution to this problem.

In QKD, Alice and Bob use single-photon (quantum) communications to establish shared secret keys whose security rests on



Secure conferencing. The six-node Tokyo QKD Network was demonstrated in October 2010. QKD systems from ID Quantique (IDQ), Mitsubishi, NEC, NICT, NTT, Toshiba Research (TREL), and a Vienna consortium (All Vienna) linked four metropolitan Tokyo sites over installed optical fiber. The systems interoperated through a Key Management (KM) Layer, which provided secure key material for video-conferencing, and a secure smartphone interface.

fundamental quantum principles. Whereas Eve will have better future algorithms and computers to attack conventional key distribution methods, the security of QKD is future proof: It can only be attacked with technology in existence at the time the photons are transmitted. Because Eve can never break the laws of physics, QKD has the potential to provide unconditional security.

QKD has been demonstrated across optical fiber paths of more than 200 km, and over multikilometer line-of-sight atmospheric paths, establishing the feasibility of satellite-to-ground quantum communications. Since 2003, small start-up companies have offered conventional encryption devices in which QKD supplies the keys. The cost, size, and point-to-point nature of these products has limited their commercial success, in spite of their asserted unconditional security. These assertions were greeted skeptically among applied cryptographers, and this opinion received dramatic confirmation with quantum hacking research results in 2010. These results exposed design weaknesses in commercial QKD products, which could in principle allow an adversary to compromise the keys. However, rather than revealing a fundamental problem with quantum cryptography, the quantum hacking results instead point to the brittle security of particular designs.

The design weakness at the root of the quantum hacking was that the classical devices used to prepare and measure the quantum states required for QKD were simply trusted to perform correctly. In the adversarial setting of cryptography this trust was misplaced, potentially allowing Eve to gain sufficient control over these devices to compromise the keys produced. Two clear research paths are now emerging.

A fundamental physics research path will seek to establish security even with untrusted devices. In the widely used "prepare and measure" form of QKD, Alice sends single-photon states to Bob. In 1991 Artur Ekert showed an equivalent approach in which Alice and Bob each receive one of a pair of photons from an entangled photon source. The security of QKD is then related to the Einstein-Podolsky-Rosen paradox where the act of eavesdropping introduces changes in the photons' quantum state. These changes would be apparent from a measurement of the quantum correlations between the photons. At present, establishing the trustworthiness through such correlations requires a "fair sampling" assumption to argue that the detected pairs are a fair sample of all the pairs. But in cryptography, Eve is not constrained to be fair. However, for system efficiencies above a given threshold, this assumption is not required, and the security of QKD could be established even if Alice and Bob use untrusted devices. With recent advances in very high efficiency single-photon detectors, the elusive goal of unconditional security using this device-independent QKD (*6*) appears to be within experimental reach.

A second, more applied research path accepts that unconditional security can be relaxed in favor of a "trust but verify" approach, which offers other, important value propositions. For example, QKD has forward security (future keys have no dependence on past ones), and has a much lighter computational footprint than conventional methods of key distribution. Once it is accepted that unconditional security need not be an essential requirement, additional quantum cryptographic protocols such as secure identification and secret sharing become possible. This opens up the possibility of new cryptosystems constructed from quantum and classical cryptographic ingredients.

Quantum cryptography is also well-aligned with the trend toward increasing capacity of optical fiber networks through

CREDIT: ADAPTED FROM NICT, JAPAN.

greater transparency. This raises the possibility that quantum cryptography could be incorporated into future networks to provide cybersecurity at the physical layer for new application areas such as the SmartGrid and data centers. Deployment of transparent network infrastructure is most advanced in the Asia-Pacific region, where the potential value of quantum cryptography has been recently demonstrated. For example, Japan's quantum cryptography testbed is a component of a national optical communications program and involves the research arms of several major Japanese corporations, which provide the commercial "heft" for successful future deployment (see the figure). Japan also plans to draw on its satellite optical communications capability to overcome the current metro-area range limitation of optical fiber quantum cryptography. With one or more space-based quantum communications nodes, geographically separated ground-based domains could be linked, even on a global scale. Japan has announced plans for a combined quantum and optical communications demonstration satellite for launch in 2013 (*7*), and China will launch its own experimental quantum communications satellite in 2016 (*8*).

Quantum cryptography research has been reinvigorated by quantum hackers. The fundamental connection between security and quantum mechanics is now more clearly defined. And with new clarity brought to its value proposition, quantum cryptography has a bright future within applied communications research as a physical-layer security technology for protecting the networks of the future.

References

1. L. Lydersen *et al.*, *Nat. Photonics* **4**, 686 (2010).
2. F. Xu, B. Qi, H.-K. Lo, *N. J. Phys.* **12**, 113026 (2010).
3. M. Sasaki *et al.*, *Opt. Exp.* **19**, 10387 (2011).
4. T.-Y. Chen *et al.*, *Opt. Exp.* **18**, 27217 (2010).
5. S. Wang *et al.*, *Opt. Lett.* **35**, 2454 (2010).
6. S. Pironio *et al.*, *N. J. Phys.* **11**, 045021 (2009).
7. H. Takenaka *et al.*, *Proc. IEEE* ICSOS 10.1109/ICSOS.2011.5783653 (2011).
8. H. Xin, *Science* **332**, 904 (2011).

10.1126/science.1208527

GEOCHEMISTRY

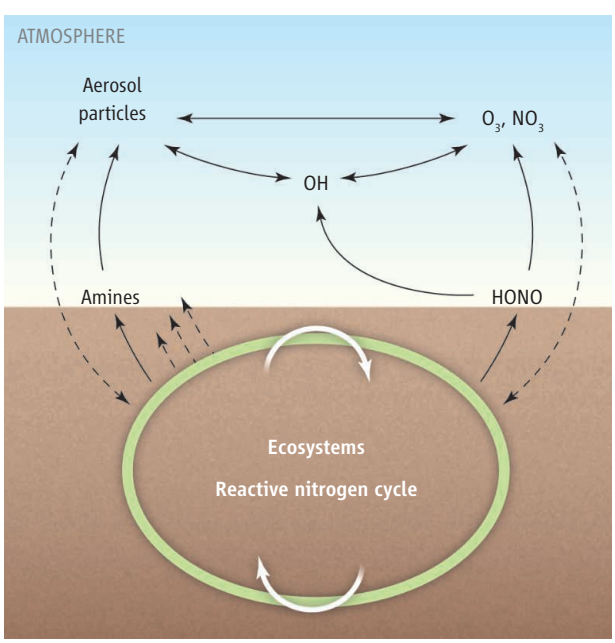
Soil Nitrites Influence Atmospheric Chemistry

Soil nitrite is a source of nitrous acid emissions that contribute to hydroxyl radical production.

Markku Kulmala and Tuukka Petäjä

Public discussion of climate change typically revolves around greenhouse gases, aerosol particles, and the role of human actions (*1*–*3*), but it is just beginning to reflect an awareness of the important role played by the global nitrogen cycle (*4*). It has been difficult, however, to disentangle the nitrogen cycle's role in climate change owing to its complex interactions with other biogeochemical cycles, including the carbon and sulfur cycles (*5*), and with factors such as soil, vegetation, and water. These interactions can lead to unexpected, nonlinear responses in the Earth system as a whole. On page 1616 of this issue, Su *et al.* (*6*) illuminate one poorly understood set of interactions, showing that nitrite in soil can produce nitrous acid (HONO) emissions that are a source of hydroxyl (OH) radicals in the atmosphere. The finding helps identify one source of "missing" atmospheric HONO, and highlights how HONO emissions could rise with increasing temperatures and nitrogen fertilizer use.

Reactive nitrogen compounds, including synthetic fertilizers, are key to sustaining soil fertility and global food production. During the last century, humans have increased the amount of reactive nitrogen involved in the global nitrogen cycle (*4*). In ecosystems, nitrogen compounds circulate within an almost closed loop (*7*). Studies have suggested that the photolysis of HONO, one component of the nitrogen cycle, is a major source of OH in the lower atmosphere. OH, in turn, plays a role in creating and removing atmospheric gases (*8*) and acting as a precursor for aerosols, particles that contribute to pollution and climate change. Known sources of HONO, however, were poorly understood and did not account for observed levels in the atmosphere (*6*, *9*). For example, measurements taken on a mountain top in Hohenpeissenberg, Germany, suggested that ~30% of OH formation was attributable to unknown HONO sources (*10*). Recently, researchers have suggested that microbe-produced nitrite in soil (*6*) and on leaf surfaces (*9*) could be the missing sources.



Soil-atmosphere connections. Microbial activity in the soil and processes in the ecosystem (bottom) connect the nitrogen cycle (green) to atmospheric reactions (blue) involved in atmospheric chemistry and aerosol dynamics. Microbe-produced nitrite in soil feeds HONO emissions, which contribute to the creation of atmospheric OH. Amines contribute to aerosol formation. HONO and amine emissions from soil could increase as global temperatures rise and nitrogen fertilizer use increases, in turn affecting global climate. White arrows indicate reactive nitrogen cycle in the soil ecosystem.

Department of Physics, University of Helsinki, Gustaf Hällströmin katu 2a, P.O. Box 64, FI-00014 Helsinki, Finland. E-mail: markku.kulmala@helsinki.fi