**Using this task**

It is recommended that the class is divided up into up to six teams (with a minimum of two people per team). Teams each research one practical use for QKD, and then put together a presentation bid for funding. The areas covered are:

* bank-to-bank transfers
* retail transactions
* election voting systems
* satellites (communications, GPS etc)
* military uses
* home computers

**Research stage**

There are stimulus sheets for each usage, which also make the presentation’s expectations clear.

For each QKD usage, there are also optional additional information sections with links to further information, and some ideas that may be worth exploring. Depending on the confidence of the groups, this additional information could be given out at the start, after 30 minutes, on request, or held back.

**Bid Delivery**

Once students have prepared their talks they deliver them in front of a panel. Ideally this will be a panel of teachers, but it could also be other students from this group, or from another group. Instructions that the panel can be given are also in this document.

Students are told they can use PowerPoints of up to 4 slides, with a maximum of 60 words to help get their point across.

**Equipment needed:**

* Printouts of this document.
* Computer with access to Internet and PowerPoint.
* £10,000,000 of fake money to give to the winning team. The Game of Life has enough money, or you can make your own.

**Research Council instructions**

You have **£10,000,000** research funding that you wish to allocate to the **four bids** that are most convincingly argued. Each group will talk for four minutes each, and then have two minutes for questions from you and other teams.

**Decide how you split this money up.**

You may wish to give £7,000,000 to one team and £1,000,000 to the three runners up, or you may do a more democratic split.

The six teams will be arguing that they need money to research one of the following uses of Quantum Key Distribution (QKD):

* bank-to-bank
* retail transactions
* election voting systems
* satellites (communications, GPS etc)
* military uses
* home computers

**Decide exactly how you are going to assess the bids that are received.**

They have been given the following considerations.

* Will this project be easy to implement? (i.e. connecting two computers together is much easier than connecting tens of thousands)
* What is the value of fraud and risks that can occur from poor security in this market?
* Are there currently problems with security for this market?

**Additional information**

As well as being experts at how QKD works, you also need to be aware of some of the proposed applications of QKD and those limitations. There is a lot of information online, but a comprehensive description is given in chapter 9 of Sheila Coburne’s report, Quantum Key Distribution Protocols and Applications, from Royal Holloway, University of London.

https://www.ma.rhul.ac.uk/static/techrep/2011/RHUL-MA-2011-05.pdf

These are the three companies that have QKD systems at the time of writing:

* http://www.idquantique.com
* http://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information-Group/Quantum-Key-Distribution/Toshiba-QKD-system/
* http://www.magiqtech.com/Products.html

**Bank-to-bank transfers**

Your team is interested in developing practical uses for Quantum Key Distribution (QKD) in bank-to-bank communications and money transfers (and between other financial institutions such as stockbrokers).

You have one hour to prepare a bid for funding into research for using QKD for bank-to-bank transfers.

This is slightly different from most other teams that will be bidding, because bank-to-bank transfers using QKD have actually been used in real life, although they are not used on a large scale. A demonstration system was setup in Vienna in 2004 and a bank transfer was completed using a key sent by QKD.

**Preparing the bid**

Things that all teams will be asked to consider are the following.

* Will this project be easy to implement? (i.e. connecting two computers together is much easier than connecting tens of thousands)
* What is the value of fraud and risks that can occur from poor security in this market?
* Are there currently problems with security for this market?

**Delivering the bid**

The bid that you put together will be delivered by your whole team, in a similar way to someone pitching on Dragons’ Den. You may create a PowerPoint if you wish, however it must have a maximum of 4 slides and 60 words in total. Your bid will be four minutes long, and you should be prepared to answer questions for two minutes afterwards.

**If you finish early**

The other teams will be delivering on the following topics:

* retail transactions
* election voting systems
* satellites (communications, GPS etc.)
* military uses
* home computers

If you finish early you can think about questions that you could ask them.

**Retail transactions**

Your team is interested in developing practical uses for QKD when using your bank-card (or mobile phone) in cash machines and in shops.

You have one hour to prepare a bid for funding into research for using Quantum Key Distribution (QKD) for retail transactions.

You may want to start by investigating the types of fraud used currently, and what suggestions QKD advocates are making to protect these transactions.

**Preparing the bid**

Things that all teams will be asked to consider are the following.

* Will this project be easy to implement? (i.e. connecting two computers together is much easier than connecting tens of thousands)
* What is the value of fraud and risks that can occur from poor security in this market?
* Are there currently problems with security for this market?

**Delivering the bid**

The bid that you put together will be delivered by your whole team, in a similar way to someone pitching on Dragons’ Den. You may create a PowerPoint if you wish, however it must have a maximum of 4 slides and 60 words in total. Your bid will be four minutes long, and you should be prepared to answer questions for two minutes afterwards.

**If you finish early**

The other teams will be delivering on the following topics:

* bank-to-bank transfers
* election voting systems
* satellites (communications, GPS etc)
* military uses
* home computers

If you finish early you can think about questions that you could ask them.

**Election voting systems**

Your team is interested in developing practical uses for QKD in electoral voting systems.

You have one hour to prepare a bid for funding into research for using Quantum Key Distribution (QKD) for electoral voting systems.

This is slightly different from most other teams that will be bidding, because QKD was used in the Geneva 2007 elections, and so has therefore been demonstrated successfully in principle. It was comparatively easy to do in Geneva, because it is a fairly small city – there will clearly be many more problems that will need to be researched and overcome if this is to be rolled out across the UK, for example.

**Preparing the bid**

Things that all teams will be asked to consider are the following.

* Will this project be easy to implement? (i.e. connecting two computers together is much easier than connecting tens of thousands)
* What is the value of fraud and risks that can occur from poor security in this market?
* Are there currently problems with security for this market?

**Delivering the bid**

The bid that you put together will be delivered by your whole team, in a similar way to someone pitching on Dragons’ Den. You may create a PowerPoint if you wish, however it must have a maximum of 4 slides and 60 words in total. Your bid will be four minutes long, and you should be prepared to answer questions for two minutes afterwards.

**If you finish early**

The other teams will be delivering on the following topics:

* bank-to-bank transfers
* retail transactions
* satellites (communications, GPS etc)
* military uses
* home computers

If you finish early you can think about questions that you could ask them.

**Military uses**

Your team is interested in developing practical uses for QKD in military situations.

You have one hour to prepare a bid for funding into research for using Quantum Key Distribution (QKD) for military uses.

The extent to which government agencies are investigating QKD is kept relatively quiet, but the benefits to having secure military communications should be obvious to most.

**Preparing the bid**

Things that all teams will be asked to consider are the following.

* Will this project be easy to implement? (i.e. connecting two computers together is much easier than connecting tens of thousands)
* What is the value of fraud and risks that can occur from poor security in this market?
* Are there currently problems with security for this market?

**Delivering the bid**

The bid that you put together will be delivered by your whole team, in a similar way to someone pitching on Dragons’ Den. You may create a PowerPoint if you wish, however it must have a maximum of 4 slides and 60 words in total. Your bid will be four minutes long, and you should be prepared to answer questions for two minutes afterwards.

**If you finish early**

The other teams will be delivering on the following topics:

* bank-to-bank transfers
* retail transactions
* election voting systems
* satellites (communications, GPS etc)
* home computers

If you finish early you can think about questions that you could ask them.

**Satellites (communications, GPS etc)**

Your team is interested in developing practical uses for QKD between ground based systems and satellites.

You have one hour to prepare a bid for funding into research for using Quantum Key Distribution (QKD) with satellites.

Many times we are using satellites but are not aware that we are doing so, and a huge number of systems on earth rely on GPS for navigation or to provide time that is accurate to 40ns. It is rumoured that spy agencies try to eavesdrop on satellites by placing spy satellites right next to them. What would happen if GPS was hacked? Can we develop systems so that future satellites are guaranteed to be secure?

**Preparing the bid**

Things that all teams will be asked to consider are the following.

* Will this project be easy to implement? (i.e. connecting two computers together is much easier than connecting tens of thousands)
* What is the value of fraud and risks that can occur from poor security in this market?
* Are there currently problems with security for this market?

**Delivering the bid**

The bid that you put together will be delivered by your whole team, in a similar way to someone pitching on Dragons’ Den. You may create a PowerPoint if you wish, however it must have a maximum of 4 slides and 60 words in total. Your bid will be four minutes long, and you should be prepared to answer questions for two minutes afterwards.

**If you finish early**

The other teams will be delivering on the following topics:

* bank-to-bank transfers
* retail transactions
* election voting systems
* military uses
* home computers

If you finish early you can think about questions that you could ask them.

**Home computers**

Your team is interested in developing practical uses for QKD to connect computers over the Internet.

You have one hour to prepare a bid for funding into research for using Quantum Key Distribution (QKD) for home computers.

Millions of people are victim of some form of identity theft each year. Could we connect computers to one another through the Internet using QKD systems so that they are guaranteed to be unhackable?

**Preparing the bid**

Things that all teams will be asked to consider are the following.

* Will this project be easy to implement? (i.e. connecting two computers together is much easier than connecting tens of thousands)
* What is the value of fraud and risks that can occur from poor security in this market?
* Are there currently problems with security for this market?

**Delivering the bid**

The bid that you put together will be delivered by your whole team, in a similar way to someone pitching on Dragons’ Den. You may create a PowerPoint if you wish, however it must have a maximum of 4 slides and 60 words in total. Your bid will be four minutes long, and you should be prepared to answer questions for two minutes afterwards.

**If you finish early**

The other teams will be delivering on the following topics:

* bank-to-bank transfers
* retail transactions
* election voting systems
* satellites (communications, GPS, etc)
* military uses

If you finish early you can think about questions that you could ask them.

**Bank-to-bank transfers – additional information**

Everybody has seen images of the stock exchanges where bankers trade billions of dollars each day. This is a huge amount of money, but is actually dwarfed by the currency exchange markets, where the total amount traded may be $4,000,000,000,000 (four trillion dollars) per day. The potential benefits to hacking into these systems are huge.

The first demonstration system was setup in 2004, but only really as a showcase. A small number of Swiss banks now use them regularly.

Would setting up QKD routes between banks, stock-brokers and other financial organisations make transactions significantly more secure? Are QKD systems capable of handling a high volume of data and at the speeds required?

Potential things to think about, and research, include:

* total amount of money traded on stock exchange
* size of currency exchange market
* number of financial institutions, and their geographic spread, in a city like London

*Press release from first ever bank-to-bank QKD transfer*

http://www.secoqc.net/downloads/pressrelease/Banktransfer\_english.pdf

**Retail transactions – additional information**

Think about how we currently use and protect our bank-card details. Many people use them daily in unknown shops, restaurants and online, and cards are very susceptible to having their details cloned. What often happens is that card details are copied and then used for online purchase. This is called Card Not Present Fraud (CNP), which is a widespread problem. Could we equip our bank-cards, or phones, with a QKD system so that when we use them at cash machines a QKD link is used to upload a list of guaranteed secure one-time codes onto the device? These could then be used to encrypt future transactions, at less secure locations; because they are only used once, it will not matter if they are copied.

Potential things to think about, and research, include:

* card cloning value
* CNP fraud
* amount spent online

*Two articles that describe QKD in mobile phones*

http://physicsworld.com/cws/article/news/2013/sep/02/quantum-cryptography-is-coming-to-mobile-phones

http://www.theguardian.com/technology/2008/oct/09/news.hitechcrime

**Election voting systems – additional information**

This was first used on a small scale in Geneva, 2007, and has been used again in some later Swiss elections. Although these systems may be used fairly infrequently, the importance of having secret (and unalterable) balloting seems to be fundamental to a democratic society.

Potential things to think about, and research, include:

* who would have an interest in subverting election results?
* what communication would be encrypted (i.e. between which parties)?
* what are the ramifications if traffic is altered?
* is electoral fraud common?

*Three articles that describe QKD in elections*

http://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election.html#.VSevBFy2TCE

http://www.scientificamerican.com/article/swiss-test-quantum-cryptography/

http://digitaldisruption.com/4-real-world-uses-quantum-cryptography

**Military uses – additional information**

It is relatively easy to see how QKD could be configured between stationary, fixed locations, but many military communications need to take place between objects that are moving, or at least mobile. There are therefore a lot of additional challenges that the military will have to overcome to use QKD as a matter of course. Opposing military forces may well have access to very strong computing power, which could be used to decrypt classical communications. If QKD was used then it would guarantee that the messages could not be decrypted by the enemy.

We can also think about how encryption techniques have been used in previous wars, and how cracking these have affected the wars’ outcomes.

Potential things to think about, and research, include:

* how the military currently communicates
* what would be the risks of information leak
* are there ways that the military communicate in peacetime that needs to be secure?

*A research paper that talks about the uses of QKD in a military context*

http://www.researchgate.net/publication/228838596\_A\_New\_Paradigm\_for\_Secure\_Military\_Communications\_Quantum\_Information\_Processing

*Battelle, an American company linked to homeland security, spends $6.5bn on research annually. They have installed a QKD system to connect their factory to their headquarters*

http://fortune.com/2013/10/14/unbreakable-encryption-comes-to-the-u-s/

http://www.battelle.org/our-work/national-security/cyber-innovations/quantum-key-distribution

**Satellites (communications, GPS etc) – additional information**

There are several problems that QKD systems have when used with satellites.

* Satellites that have geostationary orbits are usually a long distance away from where they are used.
* Satellites that are in other orbits are constantly moving, so transmitters/receivers would need to track them.

However, all satellites have very predictable orbits, and they are used for all manner of important uses.

Potential things to think about, and research, include:

* the number of systems that rely on GPS
* distances that can be reached by sending a signal via a satellite
* range of current QKD

*Quantum signal sent from aircraft*

http://physicsworld.com/cws/article/news/2013/apr/05/quantum-signal-sent-from-aircraft

*When will quantum communications blast off?*

http://blog.physicsworld.com/2013/04/09/when-will-quantum-communications-blast-off/

*Other links*

http://mappingignorance.org/2013/05/06/satellite-based-quantum-cryptography/

http://spectrum.ieee.org/aerospace/satellites/commercial-quantum-cryptography-satellites-coming

**Home computers – additional information**

If computers could be connected securely over the Internet, so that no important messages or transactions could be eavesdropped, then all of our transactions, files, messages and e-mails could be secure. Whilst there are many benefits, the difficulties in reaching home users are very large, because of the number of home networks, and wide geographical reach that would have to be covered.

Potential things to think about, and research, include:

* size of online fraud and problems with identify theft
* the distances from house to computer network
* would government agencies want people to have QKD at home?
* can we use QKD over existing networks?

*Quantum signal sent along busy telecoms optical fibre*

http://physicsworld.com/cws/article/news/2012/nov/20/toshiba-sends-quantum-keys-long-distances-on-busy-fibres

*Quantum encryption speed record*

http://physicsworld.com/cws/article/news/2008/oct/09/quantum-encryption-sets-speed-record

*Multiple users on the same line*

http://physicsworld.com/cws/article/news/2013/sep/05/quantum-cryptography-reaches-out-to-multiple-users