

BLEEDING EDGE: NANOTECHNOLOGICAL APPLICATIONS IN QUANTUM CRYPTOGRAPHY

CSC

Kelly Koenig
CSC
kkoenig3@csc.com

CSC Grants

December 2008

ABSTRACT

Background K. Koenig discusses her work on a subject that many are keen to understand but few talk about: provable, guaranteed and “future-proof” online security through today’s quantum nanotechnology solutions. Due to recently witnessed events that quantum scientists call “the biggest event breakthrough of the year,” much excitement has converged around this subject. In this day of large-scale, expensive public online security breaches, companies spend much attention addressing both reputation and competitive advantage. K. Koenig’s paper discusses today’s nanotechnological offerings that move beyond classical computational security to provide proactive, future-proof security at the highest level using quantum physics. Today, the nanotechnology that provides unconditional security across public networks – being sold for years under the radar – is moving into its public debut. This paper provides the full breadth of research on this subject, discussing business implications, technologies and market impacts.

Results Long-term, quantitative research shows that a quantum network, already available in environments requiring guaranteed security, has been demonstrated in the worldwide, mainstream environment. Quantum networks offer dynamic, provable security for online data transmission through quantum nanotechnologies. Today’s technologies offer point-to-point solutions; tomorrow’s solutions provide dynamic offerings. MIT Technology Review and Newsweek magazine identified quantum cryptography in 2003 as one of the “ten technologies that will change the world.” Top companies are expending much effort to prepare for the propagation of a quantum network that’s expected to revolutionize the market (think Cisco, IBM, Hewlett Packard, Siemens, AT&T, Nokia, Nortel Networks, Verizon, Toshiba).

Conclusion Research has found the majority of adults have heard just a little or nothing about nanotechnology. However, a major industry forecasting firm found 2007’s nanotechnology goods in the global marketplace totaled \$147 billion. Specifically, quantum security solutions are expected to revolutionize online security, with many forecasts predicting exponential growth to reach \$200 million within a few years, and long term, \$1 billion annually. It is critical that such a low level of awareness be improved in order to stay on top of the economic wave, provide for increasingly sustainable solutions, and provide for the 1.15 billion people of the middle class world market expected by 2030.

CSC

BLEEDING EDGE

Nanotechnological Applications
in Quantum Cryptography
by K. Koenig

Abstract	4
Preface	5
Quantum Physics and the Rise of Nanotechnology	6
Shrinking Device Geometry: The Rapid Growth of Electronics	6
After Moore's Law: Connecting the Dots	10
Grasping the Importance of Nano	12
Thought Leadership in Emerging Markets	17
A Nanotechnological Application in Security: Quantum Cryptography	19
A Conditional Security Discussion	19
Shining a Light on Today's Classical Encryption Techniques	22
Quantum Cryptography: Unconditional Security in Quantum Principles	23
Challenges in Today's Quantum Cryptographical Methods	28
Economic Value of Quantum Cryptography	30
Conclusion	36
Acknowledgements	37
About the Author	38
Works Cited	39

Abstract

Background K. Koenig discusses her work on a subject that many are keen to understand but few talk about: provable, guaranteed and “future-proof” online security through today’s quantum nanotechnology solutions. Due to recently witnessed events that quantum scientists call “the biggest event breakthrough of the year,” much excitement has converged around this subject. In this day of large-scale, expensive public online security breaches, companies spend much attention addressing both reputation and competitive advantage. K. Koenig’s paper discusses today’s nanotechnological offerings that move beyond classical computational security to provide proactive, future-proof security at the highest level using quantum physics. Today, the nanotechnology that provides unconditional security across public networks – being sold for years under the radar – is moving into its public debut. This paper provides the full breadth of research on this subject, discussing business implications, technologies and market impacts.

Results Long-term, quantitative research shows that a quantum network, already available in environments requiring guaranteed security, has been demonstrated in the worldwide, mainstream environment. Quantum networks offer dynamic, provable security for online data transmission through quantum nanotechnologies. Today’s technologies offer point-to-point solutions; tomorrow’s solutions provide dynamic offerings. MIT Technology Review and Newsweek magazine identified quantum cryptography in 2003 as one of the “ten technologies that will change the world.” Top companies are expending much effort to prepare for the propagation of a quantum network that’s expected to revolutionize the market (think Cisco, IBM, Hewlett Packard, Siemens, AT&T, Nokia, Nortel Networks, Verizon, Toshiba).

Conclusion Research has found the majority of adults have heard just a little or nothing about nanotechnology. However, a major industry forecasting firm found 2007’s nanotechnology goods in the global marketplace totaled \$147 billion. Specifically, quantum security solutions are expected to revolutionize online security, with many forecasts predicting exponential growth to reach \$200 million within a few years, and long term, \$1 billion annually. It is critical that such a low level of awareness be improved in order to stay on top of the economic wave, provide for increasingly sustainable solutions, and provide for the 1.15 billion people of the middle class world market expected by 2030.

Key Words Nanotechnology, quantum cryptography, quantum networks, Quantum Key Distribution (QKD), information security; data confidentiality, long-term security; business applications, business effectiveness and competitiveness.

Preface

After the Leading Edge Forum announced the subject of my research grant, I received many reactions from colleagues. Primarily, their reaction was, “Quantum what?” Many went on to tell me that they had studied the subject in school, but the subject ended up being too complicated for them to understand, let alone enjoy.

I agree – the way science has been taught regularly taxed me as well, until I found brilliant teachers who rejected the overly complicated, exclusive method of teaching. I identified with Harvard physics professor Dr. Lisa Randall’s comment on understanding science books: “...I never felt sufficiently engaged or challenged. The tone often seemed condescending to readers, overly worshipful of scientists, or boring. I felt the authors mystified results or glorified the men who found them, rather than describing science itself and the process by which scientists made their connections. That was the part I actually wanted to know.”¹¹

Today, many scientists and technologists see the gap that results from such non-collaborative efforts. People are excited about the subject that intersects nanotechnology and quantum physics, and they enjoy reading about such science

subjects as the Large Hadron Collider. What usually gets in the way of people’s enthusiasm is the lack of effort to bridge the verbose scientific community with the public at large. Because this subject shouldn’t needlessly cause further confusion, discussions enclosed in this paper will take a cue from those who seek to be inclusive, not exclusive, in their communication style. Therefore, the intent of this work is to open discussion and broaden the cross-pollination of ideas to move us forward in our solutions technology. It is with this goal in mind that I’ve organized this discussion as follows: I’ve separated the sections so that readers may read individual sections as they choose, focusing on the business side, the technical side, or both.

Additionally, this work serves as a vehicle for staying on top of emergent technologies that collaborators face today and many of us are expected to deal with in the near future. Quantum cryptography is a technology that applies some of the most innovative and transformational technologies. Many dynamic groups are at the forefront of change in a variety of sectors that range from large, publicly-traded companies to exceptional start-ups. Understanding a deeper level of what this technology has to offer will only advance the value we can bring to the immediate future.

Quantum Physics and the Rise of Nanotechnology

Shrinking Device Geometry: The Rapid Growth of Electronics

“There is nothing new to be discovered in physics now. All that remains is more and more precise measurement.”

— Lord Kelvin’s famously incorrect statement, made at the beginning of the last century

A BRIEF HISTORY

For hundreds of years, people perceived light just as they saw it: as a wave. Scientists seemed to agree light travelled in a wave function, and therefore their conclusions on other behaviors were built (incorrectly) upon this assumption. However, in 1905 a publication by a then-unknown Einstein proposed that the way scientists perceived light was, in fact, wrong. Light was not a wave, lingering on through space; it is in fact a series of quanta – discrete particles with a distinct start and end. It turns out that what we thought were laws of physical behaviors were, at best, merely approximations.

Of course, such a groundbreaking idea was very different from the established consensus of light-as-wave. But, once Einstein’s thought leadership spread throughout the scientific community (and was confirmed by other leading scientists), scientists began to open their minds to the idea. As the idea caught fire within the scientific community, scientists performed follow-up experiments and found Einstein to be correct (or, at least, they couldn’t prove him wrong!).

Einstein’s theory was the precursor to what we know today as quantum physics. Quantum physics is a branch of science that deals with discrete, indivisible entities. The results of quantum physics are, undoubtedly, difficult to understand. Once understood, they can be even harder to accept. “The import of quantum mechanics was too radical for most scientists to immediately absorb,” says Dr. Lisa Randall.¹¹ Going from principles of exact properties to probabilistic concepts is hard to embrace, let alone live by and build technologies around. Even Einstein, after winning the Nobel Prize for his founding laws of quantum physics in light emissions, had a difficult time accepting the fact that quantum physics is based on probabilistic statistics rather than true mathematical determinism, saying, “Quantum mechanics is certainly imposing. But an inner voice tells me that it is not yet the real thing.”¹

But by the early 1920s, a structural shift was well on its way, prompting scientists to move down the path of how to wrap their brains around this new “quantum” physics idea. The range of theories began to fracture the scientific community in its proposals for how things really worked within quantum physics. After realizing that their breakthroughs could so easily crumble the classical foundations of physics, Einstein and his predecessor, Max Planck, both backtracked on their theories. They understood that a crumbling foundation wouldn’t help their cause to find the truth about quantum light behavior; instead, they decided that the two theories should co-exist while they gradually led people to see the truth, laying the groundwork for a productive revolution.

Many still have a hard time coming to terms with quantum physics’ evolution in today’s world.

As a result, old and incorrect theories are still taught today, even though they are wrong. “In high school physics, we learned Newton’s laws and calculated the behavior of interesting (if somewhat contrived) systems,” said Dr. Lisa Randall. “I remember my outrage when our teacher, Mr. Baumel, informed us that the gravitational theory we had just learned was wrong. Why teach us a theory that we know to be incorrect?”¹¹ Many of physics’ classical teachings contain incorrect foundations, yet we haven’t confirmed many quantum theories that built the Standard Model of particle physics. Which teaching approach do we take?

THE RAPID GROWTH OF ELECTRONICS

The advent of quantum components has lent itself to increasingly smaller technologies. As computational growth continues, we certainly see the positive impacts – constant increase in capacity, productivity and effectiveness of computers; increased confidence and invention in the high-tech market; and continued confidence in the technology sector. Over the years, markets have been adopting information technology and software, and targeting new technologies. New technologies offer solutions that are faster, smaller, cheaper and lower power. We can do more with less.

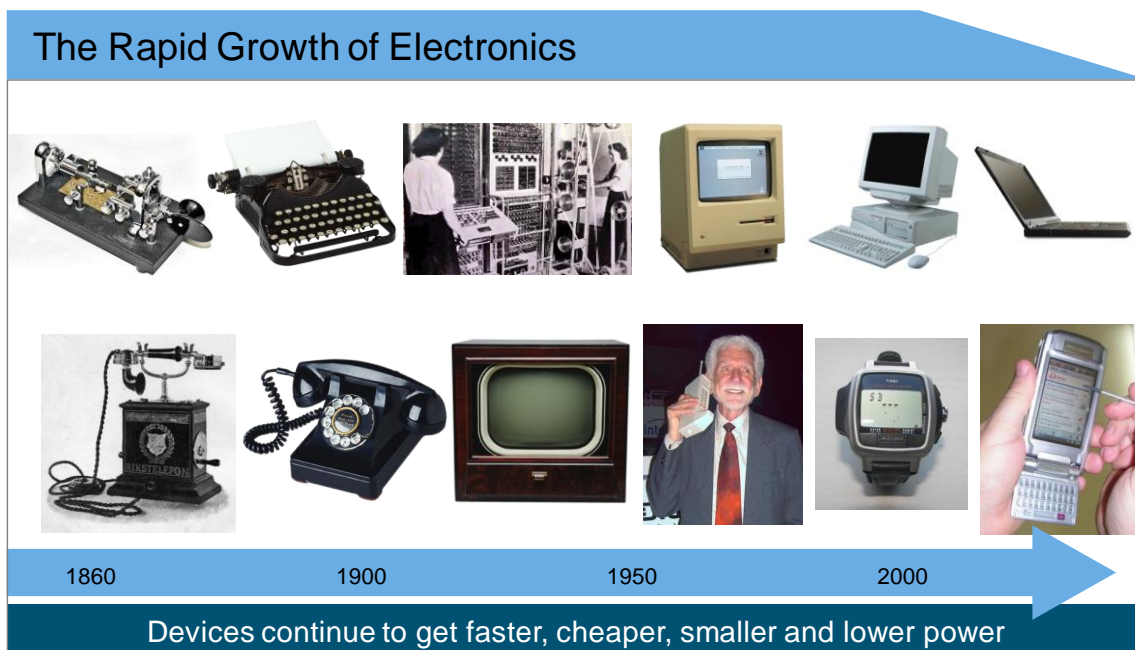


Figure 1. The Rapid Growth of Electronics illustrates temporal advancements in electronics.

However, the truth is that a constant increase in capacity will eventually hit an upper bound in a relatively short period of time. Due to the combination of computational and thermal limits, we will no longer be in a position to follow the current linear increase in the transistor-to-chip ratio. Realizing this, nanotechnologists are researching other options so that we have alternatives by the time we hit such limits.

HITTING MOORE’S LIMITS

In April 1965, Gordon Moore jotted down his thoughts on how he viewed the silicon chip’s future. He devised a prolific concept that has held for the mainstay of the transistor (the

transistor makes up the computational power of an electronic device). Moore proposed that the number of transistors that can fit on a chip will double every 18 months. With Moore's Law, predicting computational capacity has been possible – we've been able to see the direction we're going and the speed at which we can reach our self-imposed goals. However, eventually the components on a chip will become so small that the atomic structure of the materials will be a limitation. Moore himself declared in a 2005 Techworld interview, "It can't continue forever...We have another 10 to 20 years before we reach a fundamental limit."

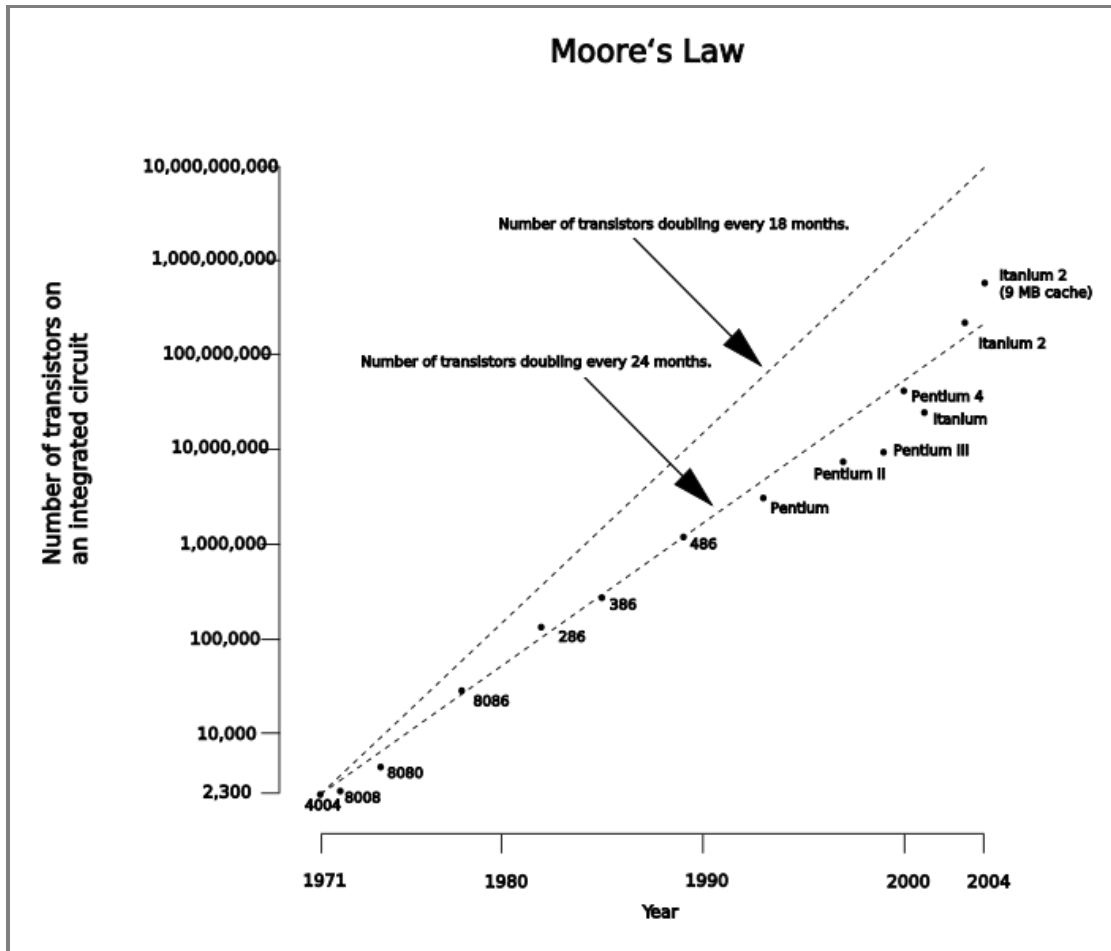


Figure 2. Graphical depiction of Moore's Law. Gordon Moore, one of three Intel founders, predicted an exponential growth in the number of transistors per chip. Moore's Law has been quite accurate over the past 45 years.

THERMAL LIMITS

In addition to atomic structural limits, physicists and computer scientists expect to breach other limits as well, reducing the timeframe of Moore's predictions. The predictions for future devices are not very promising. For example, as more and more transistors get squeezed on each chip, this reduces the space between each transistor. More and more transistors on each chip cause more heat to be emitted – to the point that we're hitting what's called Thermal Limits. This means that there are such a high number of transistors generating heat on a chip that, with today's construction, the chip cannot effectively handle the heat. Traditional cooling systems (used to cool anything from computers to

data centers) can no longer keep up with the heat generated by each generation of condensed computers.

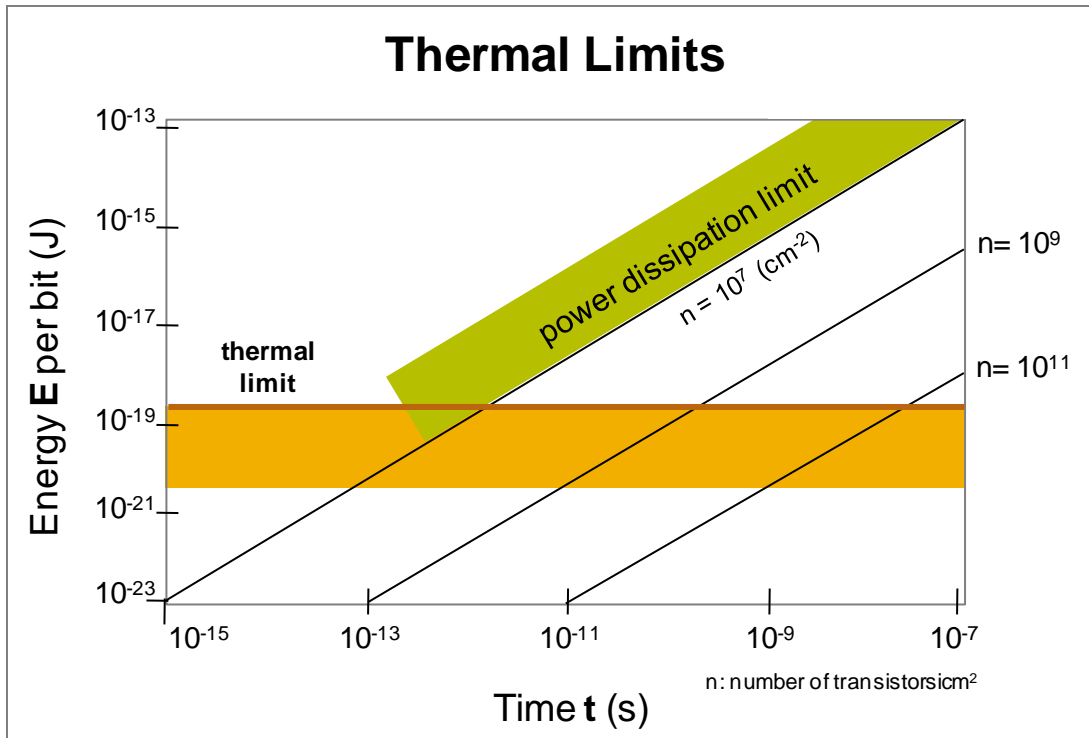


Figure 3. As (1) frequency and (2) number of transistors per cm^2 increase, the allowed operating region decreases.

POST-MOORE’S LAW

We’re hitting a true limit to the computing-power-versus-size conundrum. But today we’re in a position to look forward and preempt such issues before they become too large and cavernous to cross. Nanotechnologists are researching completely new technologies in order to provide alternatives by the time we hit such limits. Creating solutions using tried and true means is becoming more involved, complicated and expensive. Take miniaturization as an example: one can only shrink current technologies to a point until structural components hit a diseconomy of scale (i.e., where smaller means proportionally less power). This gives more incentive for emerging technologies to step in, and gives rise to the bottom-up nanotechnologies seen today (think sustainability and clean energy advancements). The costs to overcome these limitations are sometimes deemed too great today, but scientists have the foresight to work on such issues today in order to solve them for tomorrow.

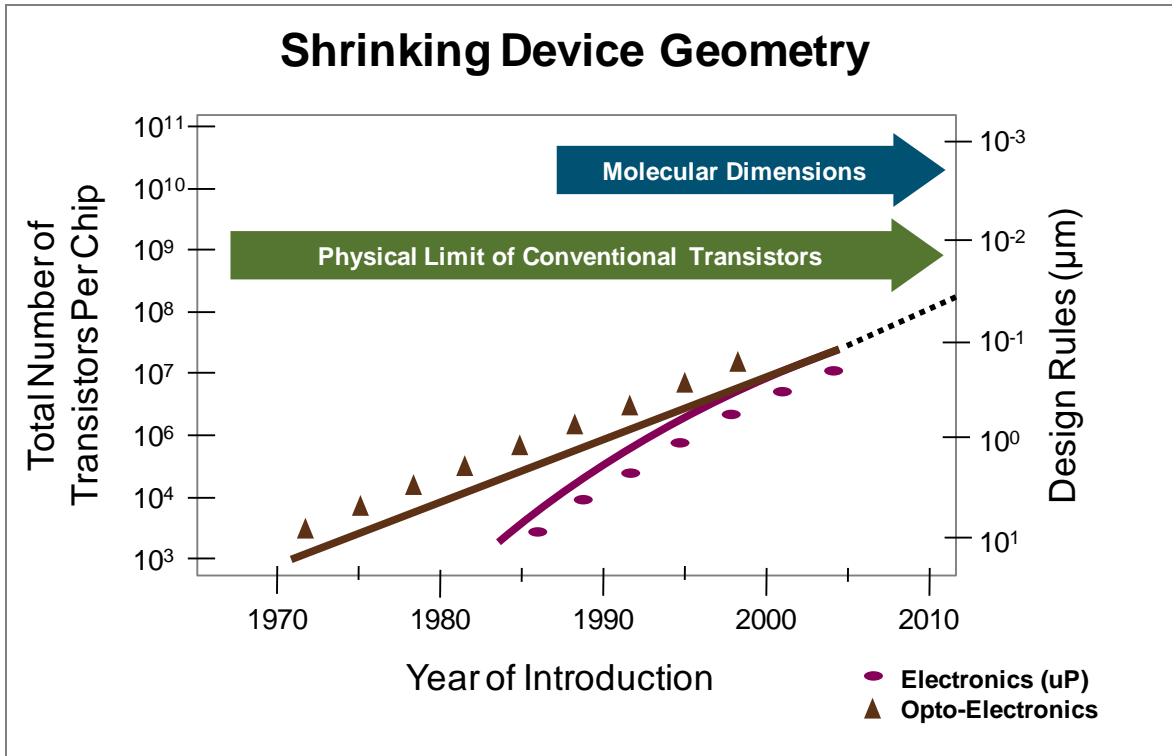


Figure 4. Timetable of the Requirements for Shrinking Device Geometry

After Moore’s Law: Connecting the Dots

“Anyone who is not shocked by quantum theory has not understood it.”

– Niels Bohr, arguably one of the most influential physicists on the subject of quantum mechanics, for which he won a Nobel Prize in 1922

CONNECTING THE DOTS

The subject of quantum physics is ubiquitous; it’s under every rock. Progress is regularly reported not only in scientific publications like the American Physics Society, but also in non-scientific publications like the Organization for Economic Co-Operation and Development (OECD), the Wall Street Journal and The Economist. The subject is even listed as a stabilized risk on the World Economic Forum. Nevertheless, when people hear the word quantum, their response is that it’s elusive, overly complicated, and something of the far-off future. Although we’ve proven inner workings of quantum physics and harnessed it into hundreds of market offerings, difficulty in considering and understanding

such physical properties still exists. After much forward movement on what we know to be true, we continue to fill in gaps of the theory on what is fact and what is, simply, incomplete.

This section will reflect on several key concepts that make nanotechnology the \$147 billion worldwide market it is today.¹⁰ To understand this discussion, one must understand not only the innerworkings of quantum physics, but also its evolutionary path. Although this discussion follows a rough historical outline, the real purpose is to introduce the main concepts necessary to understand today's nanotechnological implications. It will provide the basic concepts in quantum physics that give rise to today's nanotechnologies, particularly this paper's subject of quantum cryptography.

CLASSICAL PHYSICS: AN INCOMPLETE THEORY

Classical physics has been viewed in the scientific community as an all-encompassing theory, as the explanation of how every particle behaves. For example (and for purposes directly related to this discussion), the theory explains that things are stationary unless force is applied to them. They have no internal energy; they simply exist as atoms.

However, objects at the very small level do not behave in a way that classical physics can explain. This is probably why quantum physics has garnered its reputation for elusively complicated workings: The theory that we've proven over and over again – that we thought sufficiently explained the motion of objects for hundreds of years, which seemed to envelop atomical behaviors elegantly – appears to be *wrong*. You can imagine that once this foundational theory was proven wrong, it opened up Pandora's Box.

To explain these strange behaviors that happen at an extremely small scale, scientists created the new branch of theory called quantum physics. For example, we often think of light as a wave that streams by, but in fact light is made up of energized quantum particles. This idea was suggested in 1900 by German physicist Max Planck, who proposed that light's delivery happened in quantized units.

Quantum physics, as counterintuitive as it is, explains why a single atom placed inside a 6-inch concrete box-shaped block is small enough to tunnel through to the outside of the box, or why a stationary particle can roll up an incline without prompting. Quantum physics also explains why nano-scale particles seem to gain increased inertial energy when placed into increasingly confining environments – again, quite contrary to classical physics.

Although we have proven theories of classical physics to be wrong, we still cannot really explain some intricacies of how they are wrong. Once we get down to the sub-atomic scale, these particles behave with unpredictable, entangled behaviors. Despite this, though, nano-scale applications have become sophisticated to the point where we understand their behaviors on multiple levels.

Grasping the Importance of Nano

In September 2008, a groundbreaking poll found that three in four adults have heard just a little or nothing about nanotechnology. Nearly half of adults say they have heard nothing at all about it – quite unsettling when major industry forecasters found 2007’s nanotechnological goods totaled \$147 billion for the global marketplace.¹⁰

NANOTECHNOLOGY IS EVERYWHERE

“Nano” means a size of 10^{-9} , or a billionth of a meter. A nanometer (nm) is generally defined as smaller than the size of a human cell. In the case of quantum cryptography, it refers to the subatomic sized photon(s) carrying provably secure data across fiber optic wire (for details, see *A Nanotechnological Application in Security: Quantum Cryptography*). Such a nano-size object can travel to a wider variety of places than a larger object, such as into the body to deliver more targeted treatment. The nano object has another property that its larger components lack: once we get down to objects of nano-size scale, quantum effects become significant. This is when we see the “spooky action at a distance,” as Einstein so cleverly put it.¹

The chemical, electronic and optical nano-size properties may be very different from the same component on a larger scale. They behave differently, often in unpredictable ways. Take carbon nanotubes (CNTs) as an example. Hollow cylinders of carbon comprising the thickness of an atom, CNTs have long been touted as one of the strongest (100 times stronger than steel) yet lightest man-made materials. They’re used in everything from security (“stronger than Kevlar”²⁴) to sports (a CNT-reinforced bike won the 2006 Tour de France²⁶) Consideration of a CNT-reinforced bridge is under way for the Messina Bridge, which joins Sicily to mainland Italy. The resulting suspension bridge is expected to be 3 times longer than the current limit, and constructed at a reduced cost.²⁵

To further illustrate the omnipresence that nanotechnology has in our everyday lives, note the Nanotechnology Consumer Products Inventory. This inventory of nanotechnology-based consumer products contains over 800 products, produced by 420 companies, located in 21 countries. These are all nanotechnologies widely available to the public. As a result of nanotechnology’s multitude of applications, 3-4 new nanotechnology consumer products are released to the public each week.⁸

Applications have grown tremendously over the years into mainstream products – think Intel’s Core 2 Duo that utilizes a 45 nm process to create its incredibly efficient microprocessors, or Motorola’s OLEDs (organic light emitting diodes), which use nanostructured polymer films to create flexible display screens far more clear and energy efficient than conventional liquid crystal displays. (The market for OLED displays is expected to grow from \$112 million in 2002 to \$3.1 billion by 2007.) In 2006 research indicated that governments, corporations and venture capitalists worldwide spent \$12.4 billion on nanotechnology research and development – up almost 30 percent from 2005. By 2014, that

The Nanotechnology Consumer Products Inventory is the first and only publicly accessible online inventory of nanotechnology consumer products (over 800).

[†] Refers to Floyd Landis’ BMC Pro Machine SLC 01. The frame weighed less than a kilogram (2.2 pounds). The entire bike weighed 14.74 lbs. It was one of the lightest frames in the race and roughly 20 percent lighter than the BMC frame ridden by the team the year before.

estimate increases with the expectation that \$2.6 trillion in manufactured goods will incorporate nanotechnology – or about 15 percent of total global output.[‡]

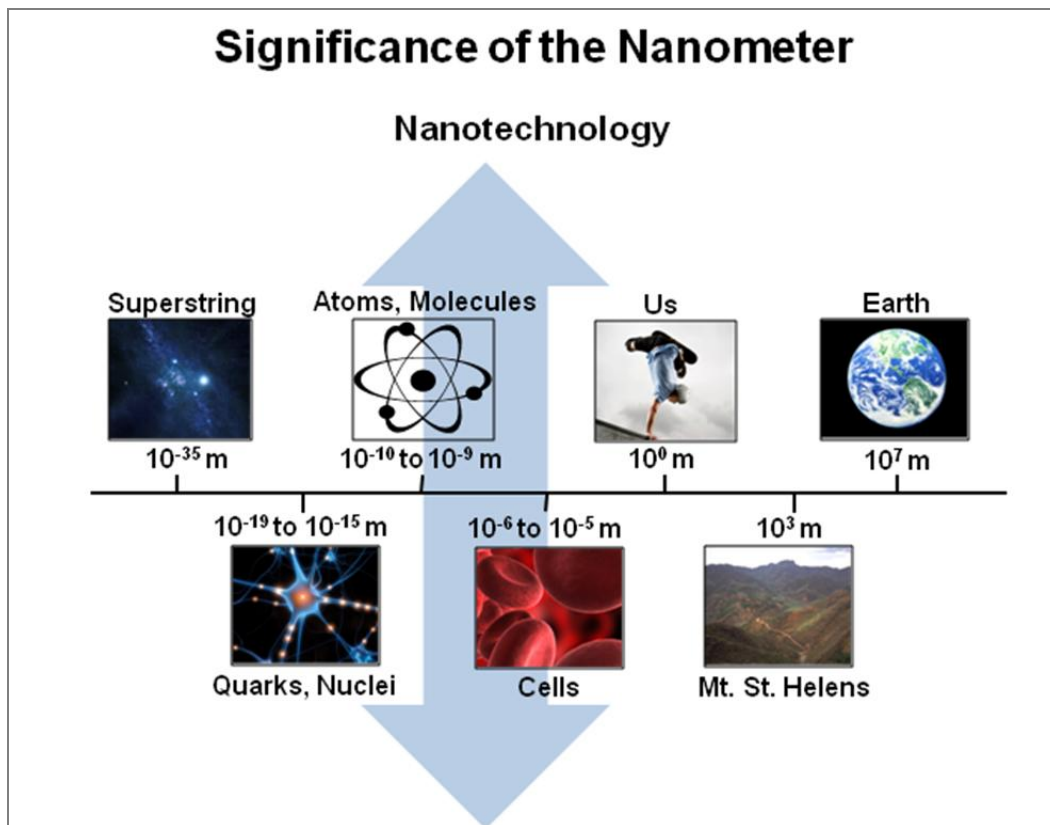


Figure 5. Nanometer and Its Significance. At 10^{-9} meters (one billionth of a meter), the nanometer (nm) is at the “interface” of dead and live material. Nanotechnology generally deals with dimensions of 1-100 nm.

"There are limits, if you think classically," said Seth Lloyd, a professor in MIT's Research Laboratory of Electronics and Department of Mechanical Engineering. But "...once you think quantum mechanically you can start to surpass those limits."⁷ For example, the subject of this paper, quantum cryptography, wasn't even a blip on the radar screen in the early 1970s. Yet today it flourishes as we master material properties. By shining a light on progress already made in the nanotechnological field, we lay the groundwork for the opportunity to understand how these applications will shape the future. For example, the National Science Foundation has estimated that 2 million workers will be needed to support nanotechnology industries worldwide within 15 years.

[‡] Lux Research

Table 1: Innovative Products Created as a Result of Nanotechnology²⁸

Market Products Resulting from Nanotechnology	
Sustainable Energy	<ul style="list-style-type: none"> • Solar cells — 7x more powerful than traditional models • Water filters — Low cost filters to provide clean, desalinized water • Rechargeable batteries — Last over 12x longer than conventional lithium batteries • Car batteries — Phoenix Motorcars' SUV drives 100 miles per hour for up to 130 miles on a rechargeable battery that recharges within 10 minutes
Medical	<ul style="list-style-type: none"> • Quantum dots — Provide direct-delivery cancer treatment; detect and treat diseases more effectively with fewer side effects; detect and identify harmful chemical or biological presence • Biochips — Detect cancers before symptoms arise; diagnose health issues at record pace
Technology	<ul style="list-style-type: none"> • Quantum cryptography — Provable, unconditional online encryption • Flash Memory — 16 gigabit (Gb), 51 nm flash chips (Samsung) • Processors — 45nm — 90 nm processors (AMD, Intel) • Video Display — Organic light emitting diodes (OLEDs) color video display. Result is higher-quality large flat panel displays that last longer, use less energy, and cost less (DuPont, Motorola, NanoHorizons, Samsung, Sony) • XBOX 360 — Contains an IBM 64-bit PowerPC core. 165 million transistors on a 90nm Silicon on Insulator (SOI)
Home	<ul style="list-style-type: none"> • Air Conditioners — With anti-bacterial filters, purifying filters, and silver nano evaporators (LG, Samsung) • Refrigerators, washing machines — With anti-bacterial effects, sterilization and nano-deodorizers (LG, Daewoo, Hitachi, Sharp, Samsung) • Paint — Stronger adhesion with anti-mildew properties (Behr), with anti-graffiti properties (Victor Castaño)

SUSTAINABILITY, BY NATURE

As the price of energy sources increases, the subject of sustainability has become increasingly popular and controversial. Researchers are scouting alternative energy sources with increased enthusiasm, and governments are making decisions on whether to fund small-town garage entrepreneurs or big businesses to find an energy solution. In either event, this shines a light on the many advantages of nanotechnology, bringing them to the forefront to serve as possible solutions to our changing models of energy processing and demand. As we explore the solutions to our world's energy needs, efficiency has become a hallmark of many nanotechnologies.

For example, quantum particles, known as quantum dots, are known to improve energy efficiencies. Quantum dots may extend the range of energy that can be absorbed and stored (and later converted into such energies as electric current). Since quantum dots are found to absorb more energy than classical conductors, they have been proven to emit more energy as well. For example, today's solar

cell applications using this nanotechnology result in a seven-fold increase in stored energy output. Speaking at 2008's Nanotechnology for Sustainable Energy conference, Professor Bengt Kasemo said, "If solar energy is harvested where it is most abundant, and distributed on a global net (easy to say – and a hard but not impossible task to do), it will be enough to replace a large fraction of today's fossil-based electricity generation." (Professor Kasemo is from Chalmers University of Technology and chairs the European Science Foundation (ESF), which hosted the conference.²⁷) Solar energy can be used to then generate electricity or hydrogen for engines. To come full circle in power generation, such a process can be used indirectly to generate electricity in conventional power stations.

Nanotechnology is, by nature, designed with energy efficiency in mind. For example, quantum cryptography isn't a solution that's recycled when the next model comes around; it's a technology that scientists agree is sustainable and future-proof. (for more information, see *A Nanotechnological Application in Security: Quantum Cryptography*.) And as the sustainability revolution expands, nanotechnology is seen at the forefront with its capacity to form cleaner and more efficient energy. The companies that figure out how to harness this energy while providing a smooth transition will win a large share of the world market.

LOW POWER USAGE

Thanks to ever-shrinking technologies, today you can buy a laptop with a battery that lasts 19 hours. And thanks to nanotechnology, you can buy a zero emission SUV that runs over 100 miles per hour for up to 130 miles on a battery that recharges within 10 minutes.[§] The flip side of having nano solutions that require less energy to maintain is that they may require increasing levels of energy to produce in the first place. In other words, they're cheap to maintain and more expensive to buy. As nanotechnology becomes more prevalent as a research technology, however, the costs associated with bringing a product to market will decrease substantially.

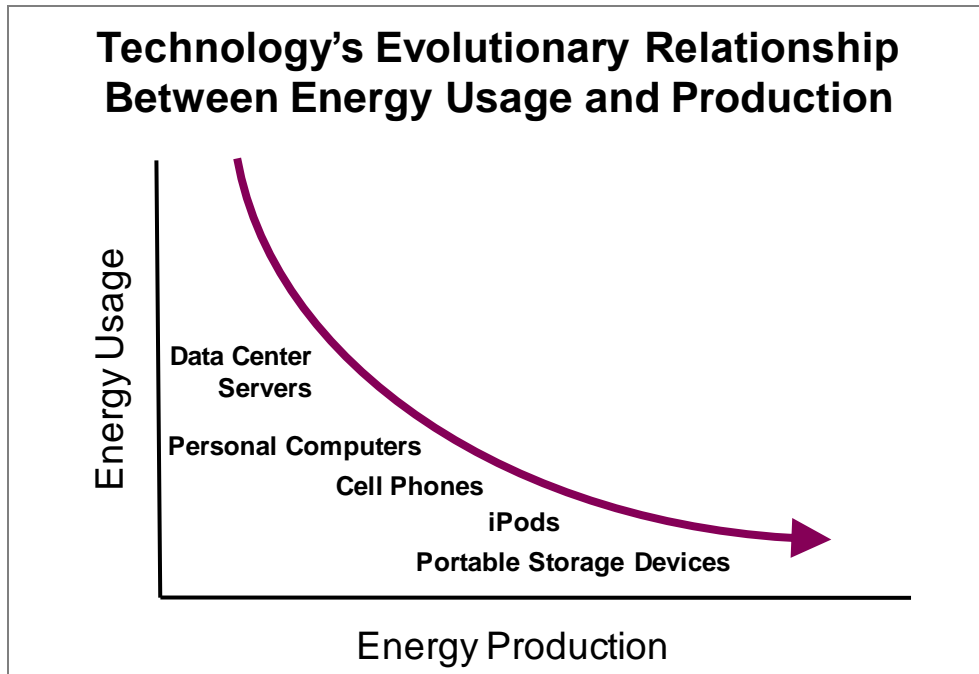


Figure 6. As technology advances provide for decreased product energy usage, they also suffer from increased energy required in production.

A NEW MARKET

Changing perceptions about nanotechnologies are causing consumer buying behavior to change quickly as well. One only need look at the commercials in the marketplace today to see the sustainability that businesses are now touting. Sustainable technology is here to stay. People who wouldn't think of buying a hybrid car before now consider it because it is touted as sustainable.

Not only are views changing, but new consumer demographics are emerging that are synonymous with the sustainability outlook. The World Bank estimates that the global middle class is likely to grow

[§] This quote refers to Phoenix Motorcars' Altair Nano 35 kWh lithium-ion battery packs for use in its all-electric sport utility trucks (SUTs) and sport utility vehicles (SUVs). Lithium-ion charging capabilities may be recharged without ion leakage.

from 430 million in 2000 to 1.15 billion in 2030. In order to obtain the benefits of an expanding middle class, markets must pay close attention to this ever-increasing population segment.

Thought Leadership in Emerging Markets

Now that we've built a basic understanding of quantum theory, we can understand how important and impactful this theory is in today's world. For a long time, such quantum theories were seen as frivolous ideas of the far-off future – if we could only grasp the applicable concepts, the things we could do on a quantum level would boggle the mind. Therefore, unless one regularly reads scientific journals or works within certain technological communities, one doesn't tend to be exposed to the advanced nanotechnological applications happening today. We see the conventional applications used in a multitude of ways, but rarely pay attention to the advancements because they're seen as niche solutions.

In the next few years, we'll witness subsequent students coming through the ranks of undergraduate and graduate school, rife with knowledge to work through problems that we've only heard referenced on Star Trek episodes. And this younger set will have the knowledge to advance and even accelerate the rate of growth to levels not anticipated even a decade ago. Understanding such an effect on the world is key to preparing for a stable and prosperous future.

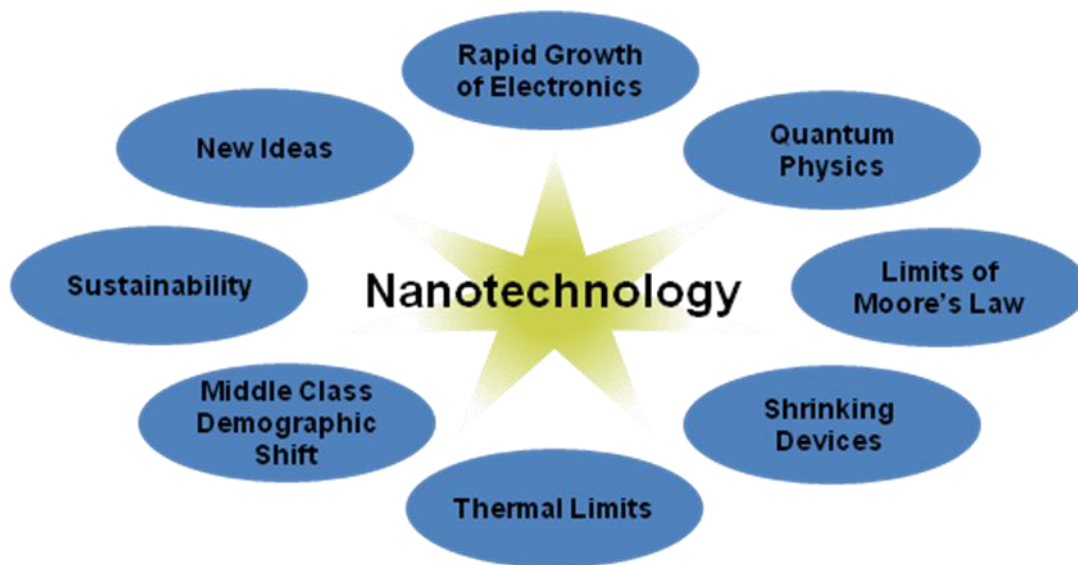


Figure 7. All of these aspects converge to create the emergence of nanotechnology.

BREAKTHROUGHS THROUGH COLLABORATION



Figure 8. Apollo 8.

Source: NASA

Breakthroughs often do not happen in isolation; they usually come encased within a movement at large, while people are collaborating (or even competing). They're often surrounded by, or working on top of, some great ideological movement or previous breakthrough. When goals are set within the scientific community, the community is quite resourceful in seeing them to fruition, especially with the right motivation. To illustrate the outstanding capacity of collaboration and vision, think about the first manned mission around the moon. The Apollo 8 mission didn't have a blueprint to follow. It was a mission imperative announced by an American president^{**} at a time of the Cold War, the arms race, and a period of fierce scientific competition in the space race. At the time, nothing like it had been created, and scientists literally had a blank slate from which to work toward getting a man into space. NASA didn't have a preconceived plan to disseminate to its engineers, but instead expected its engineers to produce their own. Unsure of how to accomplish such a monumental goal (but determined to be the first), the engineers were known to have gained tremendous advantage from the

psychological synergy that developed from their collaborative spirit to design the project. The average age of these engineers was 27.

To use a more current example, the European community recently celebrated the kickoff of the Large Hadron Collider. Much of its excitement is in the unknown. One of its many purposes is to explore whether we are right in our common theories of how the universe behaves – such as string theory and the Standard Model of particle physics. Located at CERN in Switzerland, the Large Hadron Collider is a culmination of over 20 years of work with over 10,000 scientists worldwide. However, many say that goals set today are not as set in stone as they once were. For example, the United States once exemplified rapid scientific advancements. But it has recently suffered from scientific budget cuts. For example, the Superconducting Super Collider, begun in Texas in 1991, would have employed more power than the Large Hadron Collider. But a change in government leadership meant its cancellation two years after its construction. Today, Europe spends almost twice as much as the U.S. on nanotechnology projects on the basis of what spreads scientific advancement: risk relevance of a project.^{††}

^{**} John F Kennedy, United States president, 1960-1963

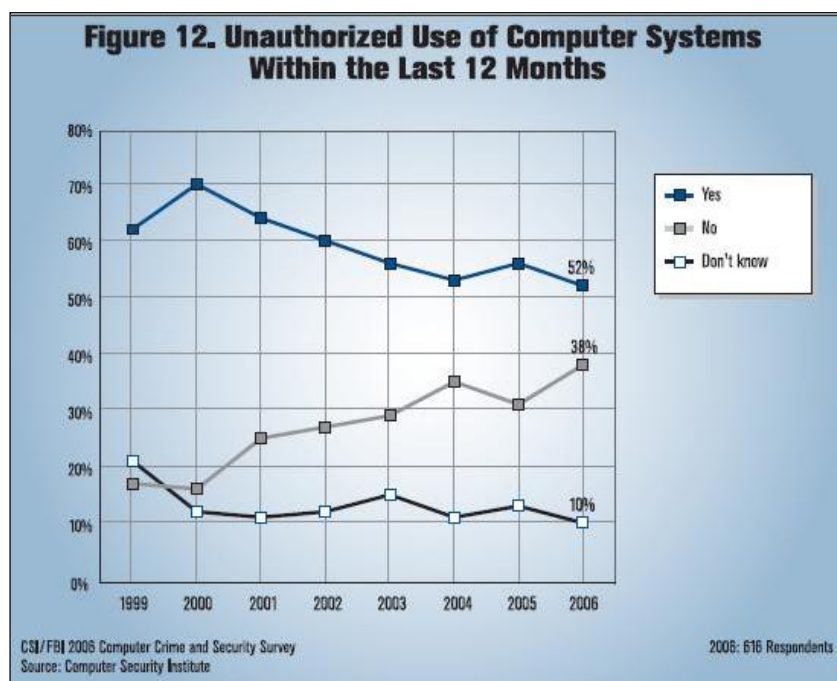
^{††} The Project on Emerging Nanotechnologies' (PEN) assessment of nanotechnology risk-relevant projects identified by the federal government's National Nanotechnology Initiative (NNI) for fiscal year 2006 reported \$13 million was invested in projects addressing possible risks. Within the same timeframe, PEN analysis found European countries invested nearly \$24 million in projects with similar aim.

A Nanotechnological Application in Security: Quantum Cryptography

This section delves deeper into quantum mechanics' application within nanotechnology. Specifically, this section continues to demonstrate quantum physics' achievements within the nanotechnological movement at large; discusses current security concerns, quantum cryptography's solutions to these concerns, and the economic market implications of this application. This section simplifies concepts where possible so they can be understood by a broad range of readers.

A Conditional Security Discussion

Malicious codes caused over \$28 billion in economic losses in 2003, and are estimated to have grown to over \$75 billion in 2007.⁶ Trends show that this number continues to grow over time. As a result, the need for security has intensified. In fact, full-time information security professionals are expected to rise approximately 14% per year worldwide, moving past 2.1 million in 2008.^{##}



But, malicious codes aren't the only culprit in security breaches. Eavesdropping via fiber tapping has become more and more prevalent over the years. A congressional panel, for instance, was recently reminded of an allegation that French intelligence had tapped in to Boeing's new 747-400 flight tests. The French are major partners with Boeing's primary competitor, the Airbus Industrie consortium.²⁹ Today, companies are victims of internal attacks with tools available on the open market and a trip to a telecom closet, where one can plug into company fiber infrastructure and pull down data.

Figure 9. CSI's resulting analysis of unauthorized use of computer systems within the last 12 months (1999-2006).

The CSI Computer Crime and Security Survey^{##}, arguably the

^{##} IDC Report

^{##} The Computer Security Institute (CSI) is a 33-year-old professional organization for information security professionals. The survey is arguably the most widely quoted computer security survey. Sectors with the largest number of responses came from the financial sector (20 percent), followed by consulting (11 percent), education (11 percent), information technology (10 percent) and manufacturing (8 percent).

longest-running average annual survey garnered from C-level officers and managers at the forefront of information security, reported that U.S. companies stated individual losses that more than doubled in 2007.^{***} Virus losses, the number one cause for seven straight years, fell to second place, with financial fraud now the leading cause of financial loss. The 2007 survey also indicated trend movement toward targeted attacks aimed directly at one target (as opposed to attacks on multiple random systems).

Not surprisingly, we see that when CSI asked, “What do you think will be the most critical computer security issue(s) your organization will face over the next two years,” the top rated concern was data protection. Part of the reason behind the high concern is that economic loss adds up quickly. For example, Forrester Research estimates losses from security breaches are \$90-\$305 per record.⁵

^{***} Losses went from \$168,000 in 2006 to \$350,424 in 2007.

Table 2: A sampling of worldwide company data loss³⁰

Company	Loss	Year	Description of Breach
TJ Maxx	\$118 M	2007	45.7 million records of personally identifiable information
Boeing	\$5-15 B	2004 - 2006	382,000 current and former employees' information
Fidelity National Information Services	N/A	2007	8.5 million records of personal data
Nordea (Sweden's largest bank by value)	\$1.1 M	2007	250 accounts affected
Marks and Spencer (U.K. Retailer)	£1.5 M	2007	26,000 UK employees' names, addresses, national insurance number and pension plan information, estimated at £59 per record
London Stock Exchange	N/A	2007	Attackers created a disruption that halted alerts system of 14,000 private investors for more than 48 hours
Ernst and Young	N/A	2006	243,000 Hotels.com customers
T-Mobile	N/A	2006	Data of 17 million customers
HM Revenue and Customs (U.K.)	N/A	2007	Loss of 25 million personal records
Veteran Affairs Data Security (U.S.)	N/A	2006	Over 26.5 million veterans and their families. Data included names, social security numbers, and dates of birth.

Today's cryptography solutions rely upon computational difficulty (like factorization or transposition) to send information. The issue is that this information is transmitted with the knowledge that someone – anyone – could be eavesdropping. What happens when the information being sent is priceless, or could result in insurmountable loss should it be intercepted?

WHO IS AT THE MOST RISK?

Firms for which data is sensitive are the most at risk for losses: financial institutions, insurance companies, national security entities, corporations' intellectual property units, trading institutions, and any storage area network that may hold such information. "The volume and type of sensitive

information being transmitted over data networks continues to grow at a remarkable pace,” said Prem Kumar, professor of electrical engineering and computer science at the McCormick School of Engineering and Applied Science. “New cryptographic methods are needed to continue ensuring that the privacy and safety of each user’s information is secure.”¹⁸ Clearly, the larger the security risks, the more effort firms are willing to put into securing their networks.

Shining a Light on Today’s Classical Encryption Techniques

THE KEY DISTRIBUTION PROBLEM

In classical cryptography there exists an unbreakable code. Called a “one-time pad,” the encrypted code must be equal in length to the message text itself. In order to encrypt a message with this unbreakable code, each communicating party must share the secret sequence of random numbers, known as the key, and use this “one-time pad” only once.

Distribution of the key usually involves an exchange using non-secure means. For example, often keys are distributed by physical distribution or download over an insecure network. Called the “Key Distribution Problem,” this method leaves today’s security techniques incomplete. Since often there is no practical way to distribute these keys securely, most of today’s cryptographic protocols rely on public key distribution and the assumed computational difficulty of breaking the protocol instead. In order to securely distribute the key, one would need a means by which to distribute the key to each party without chance of it being exposed to outside parties.

THE KEY REFRESH PROBLEM

In analysis, we come across another gap: to provide security, we need to refresh the key, as described above (the “one-time pad”), for each message. Most systems rarely refresh their cryptographic keys, and usually do so less than once per year. Should a key be compromised between a key refresh, information transmitted over the communication link is vulnerable to eavesdroppers.

THE MATHEMATICAL COMPUTATION PROBLEM

As computing power continues to increase dramatically, new code-breaking algorithms are developed, but as quantum computing nears reality, today’s secrets will become vulnerable. Today’s messages that are secret may be compromised tomorrow. Additionally, the subject of the encrypted key itself poses a problem: classical encryption algorithms aren’t altogether impervious to cracking, and with the advent of parallel computing and quantum computing (which easily equals the computation power of hundreds of thousands of regular computers), complex codes have been broken in realistic time frames. Although seen as the best solution for its time, in the end classical cryptographic solutions fail the test of time.

Quantum Cryptography: Unconditional Security in Quantum Principles

Now that we've laid the groundwork of quantum physics, its basic properties and behaviors, and its role within nanotechnology, we may now move on to a specific application: quantum cryptography. (As explained in the preface, it is not necessary to read the previous sections in order to jump right into this section.)

Ultimately, there are many methods used to perform quantum cryptography, all of which have their associated advantages and disadvantages depending upon the application. As discussed in the preface, the scope of this paper is to provide clarity to the discussion and simplify concepts where possible. Therefore, we bypass discussion of each individual protocol offered on the market today, and instead delve into the foundations of the nanotechnology itself.

Quantum Cryptography is not Quantum Computing

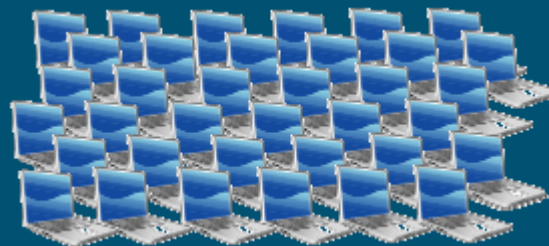
While it harnesses the quantum mechanical properties of physics, quantum computing is a very different technology than quantum cryptography. Quantum computing leverages the individual Qbit to provide computing speeds and capacities that far exceed today's classical computers.

How does it work? Where a classical computer's memory is made of bits that hold either a 1 or a 0, a quantum computer uses Qbits to hold a 1, a 0, or both a 1 *and* a 0 simultaneously. Therefore, it provides for 2^n (n =number of Qbits) states at one time. Not only does a quantum computer provide the ability to hold massively more data in memory, but it also processes exponentially faster than today's classical computers. In many cases, problem solving occurs millions of times faster than what we've seen with classical computers.

Conventional Computer with 64 bit Architecture
Computes using *one* of the 2^{64} possible numbers at a given time (assume single core)



Quantum Computer with 64 Qbit Architecture
Computes using *all* of the 2^{64} possible numbers at a given time, equaling 2^{64} or 18,446,744,073,709,551,616 conventional computers working in parallel



When will we see quantum computers in the mainstream market? Companies such as D-Wave Systems have been providing quantum computers for its clientele since February 2007.

The advent of quantum computing has put classical cryptography on notice: The extreme speeds of quantum computing have already broken classical cryptographic algorithms in seconds, rendering them useless against those who intend to capture and decrypt data. Earlier this year, associate scientists at both the University of Science and Technology of China and The University of Queensland in Australia developed a photonic quantum computer that can quickly crack the widely used RSA code—an undertaking that would take hundreds of years on even today's supercomputers.³¹ The ability to more quickly break traditional encryption is just one more reason companies are investing in quantum cryptography. Quantum cryptography works *with* traditional encryption protocols to provide an additional layer of unbreakable encryption.

QUANTUM CRYPTOGRAPHY AT 50,000 FEET

Quantum cryptography, invented in 1984 by Charles Bennett and Gilles Brassard and based on earlier position papers by Stephen Wiesner, exploits the basic properties of quantum physics to provide unconditional security. It not only makes it difficult for someone to eavesdrop on the signal, it simply doesn't allow eavesdropping to happen in the first place.

So, what is it about the quantum effects of this unique cryptography technique that provides unconditional security? First, consider a light beam: it is composed of a quantized stream of photons (a photon is an elementary particle of light), yet it behaves as both a wave and a particle. This wave-particle duality^{†††} theory explains why light behaves in a more wavelike manner when in relatively larger quantities, yet behaves as particle-like when discerned in a very small quantity. Generally, individual particles of light exhibit quantum behaviors when we get down to their individual photons.

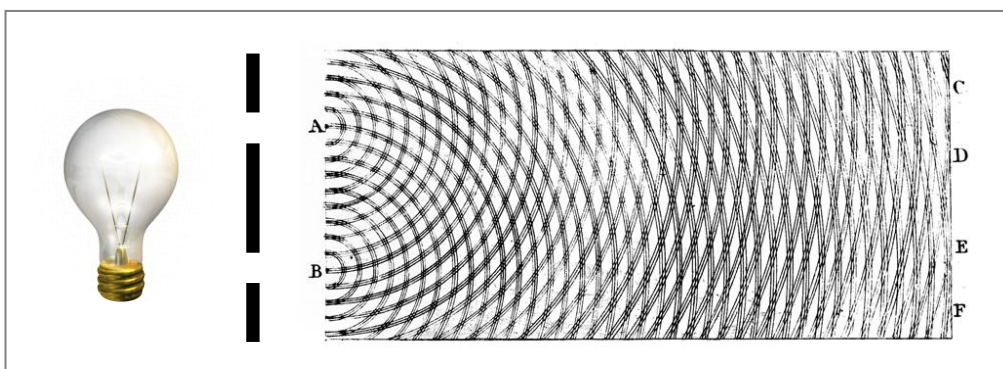


Figure 6. An experiment illustrates the wave-particle duality of light. Light is sent through a screen with two slits. The light source is directed toward and probably travels through only the two slits. However, after light passes through the slits and is absorbed, it exhibits the well-known, classical wave pattern with which we are familiar.

It is only when the light beam is reduced to its individual photons that its quantum effects can be exploited. Intriguingly, when we reduce a light beam down to one stream of photons, the quantum behaviors get truly interesting: We find that we cannot even observe the photon stream without leaving indelible traces. In fact, in attempting to measure or observe the photon stream, the observer cannot avoid changing stream composition, and thus is always detected.^{†††} This concept lays the groundwork for quantum cryptography: Any attempt to contact, copy, observe or eavesdrop is instantaneously detected.^{§§§¹⁴}

^{†††} For a more detailed explanation, see: <http://www.youtube.com/watch?v=DfPeprQ7oGc>

^{†††} Today's public offerings may detect the type of eavesdropping happening to your network. Whether an eavesdropping attempt or a full-scale attack, the administrator is notified and then determines whether or not to halt transmission. This situation can lead to quite complex discussions and is beyond scope of this publication.

^{§§§} These concepts were discovered by Werner Heisenberg, a favorite and highly-referenced pioneer of quantum mechanics. Heisenberg developed the Uncertainty Principle: that one cannot measure certain pairs of quantities (i.e., both velocity and location).

Now let's use an example of a quantum encryption technique: The sender, Alice, transmits a stream of classical bits and encodes them into a sequence of random quantum states of light (photons). The bits are randomly selected from four types and are sent over the quantum channel. The receiver, Bob, randomly selects an appropriate measurement device to survey the bit stream, leading him to share some classical data correlated with Alice's bit stream. The classical channel is then used to test these correlations. If the correlations are high enough, then this signals that no significant eavesdropping has occurred. As a result of a "clear channel," a perfectly secure symmetric key can be distilled from Alice and Bob's correlated data. After the key is distilled, secure data transmission may begin. However, should a threshold of errors be introduced into the signal, key generation stops and the process starts again from the beginning.

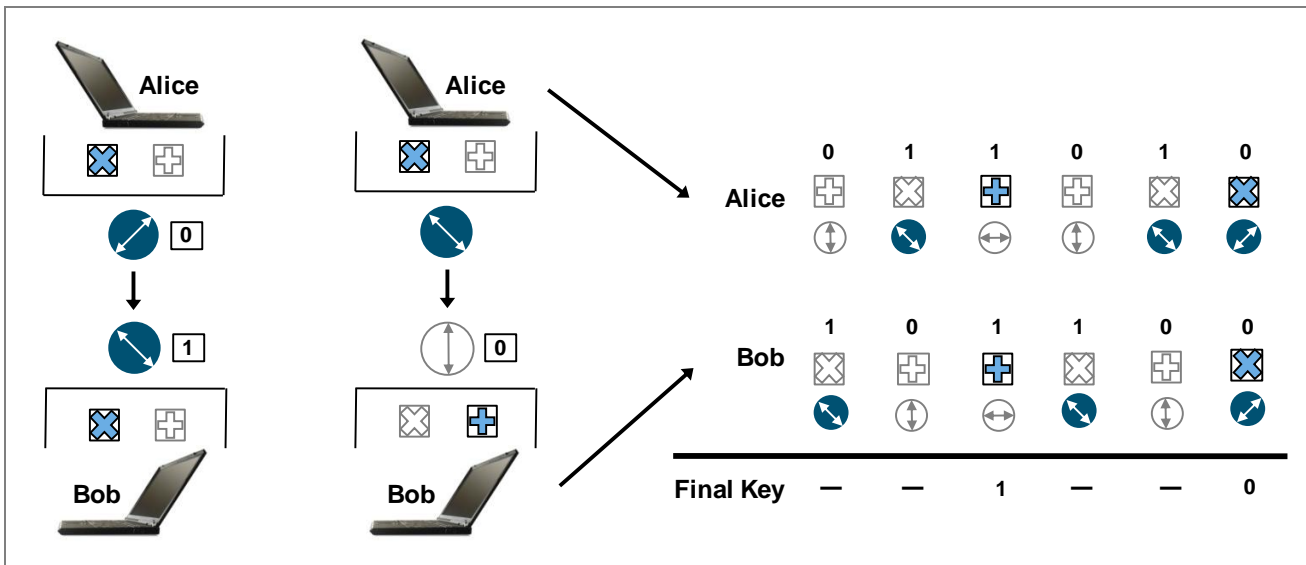
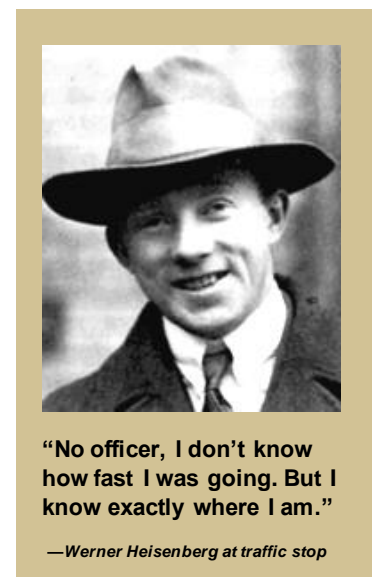


Figure 11. Illustration of a Quantum Cryptography Protocol Creating a Secure Key. This figure shows a quantum cryptography protocol, BB84, creating a secure key

BASIC PRINCIPLES OF QUANTUM CRYPTOGRAPHY

Ultimately, quantum cryptography's provable security is based upon no technological assumptions. The security offered lies simply in the principles of physics. Two frameworks, in fact, guide the basic workings of the unconditional security: the Heisenberg Uncertainty Principle and the no cloning theorem.

The Heisenberg Uncertainty Principle states that measuring certain pairs of quantities is impossible. In the case that applies to quantum cryptography, the laws of physics are such that one cannot measure a stream of quantum photons, else the stream will change upon measurement and negate chances that the second measurement will be accurate.



For example, an attempt in measuring both the location of a quantum particle and its velocity would be impossible. The first attempt at measuring the location would be accurate, but the act of measuring would change the particle and cause measurement of the particle's velocity to be inaccurate. This is a distinct physical property of quantum physics, called the Effect of Measurement: quantum particles (in this case, photons) carry a certain state up until they are "seen" or measured. Upon measurement, their state unequivocally and detectably changes. At best, only approximations of location and velocity can be made.

The no cloning theorem states that an exact copy of a quantum-size particle cannot be made. Attempts at reproduction would not result in a copy of the original's true state. This theorem is key with respect to quantum cryptography. It means that an eavesdropper could not copy any part of the photon stream between sender and receiver – not even one photon. It also means that any attempt at reproducing a key would result in irreversible errors in a photon stream, which would then cut key transmission.

Quantum Key Distribution's Security Lies in These Frameworks:

Heisenberg Uncertainty Principle

Measurement of certain pairs of quantities is impossible (for example, location and velocity).

No Cloning Theorem

Attempt at creating an identical copy of a photon (whose quantum state is unknown) is impossible.

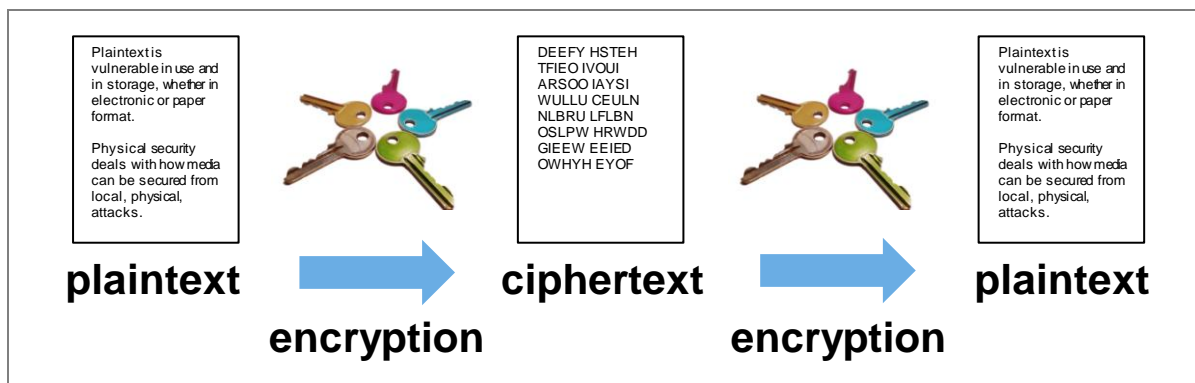
The Heisenberg Uncertainty Principle and the no cloning theorem work together to provide the guaranteed security of quantum cryptography: Should an eavesdropper try to capture part of the transmission (even a fraction of the transmission), eavesdropping is detected. Should the eavesdropper try to work around this roadblock by copying a photon stream along its pathway, copying changes the state of the photon. This change in state not only means that the eavesdropper captures inaccurate misinformation, but also that the eavesdropper's attempt at copy is detected.

SECURE KEY EXCHANGE

Traditional key distribution relies on humans to disseminate a secure key. A distribution method that relies on humans is exposed to such risks as involuntary key disclosure: the key could be revealed through internal intelligence or even under conditions of coercion. In contrast, quantum cryptography uses quantum key distribution (QKD), an automated key distribution, to provide automation that doesn't require human interaction. The key is automatically generated and sent without human interaction.

Additionally, another feature of the key comes into play: key length, crucial to the security factor, is totally flexible in the case of QKD. Recall that a key in equal length to the message provides maximum security, but is often unrealistically slow in the case of classical cryptography due to the time taken to generate the long key length for each message. The advantage of QKD is that the time needed for key generation is not affected by exponential increases as it is for longer asymmetrical

keys.



SECURE KEY REFRESH

QKD provides for a regular key change, reducing risk of key retrieval even further. QKD uses true random number generation that provides real random keys associated with physics-based number generation. It essentially bypasses the need for pseudo-random number algorithms used in classical encryption, which rely on mathematical formulae to produce a list of numbers that appear random. The result of a true random number generator is a sequence of random numbers statistically independent of the others. This process can repeat itself hundreds of times a second.

The revolutionary feature of QKD is that it is inherently secure. The distributed key cannot be acquired by an eavesdropper without the sender and recipient's knowledge. The provable security of QKD lies in the reality that a key may be transmitted with guaranteed security. Encoding the key on a photon stream guarantees that any eavesdropper will be detected; the eavesdropper cannot observe, copy, or in any way reproduce any part of the photon stream without detection.

EAVESDROPPING DETECTION

Now that the technology is over 20 years old, many companies have taken their own approach and offer their own spin on the technology. Many methods involve something more complex than simply an “on” or “off” switch in response to eavesdropping. Such a method uses the key to manipulate the photon stream, creating a type of quantum noise that’s integrated with the key's pattern. To an eavesdropper, the data sent contains too much "noise" to properly eavesdrop. The recipient with the key has the pattern and can receive the signal with much less noise, allowing him to read the encoded message. Should an eavesdropper be detected, there are any number of ways communication can be handled with today’s offerings. Some company offerings have devised a way to notify the communicating parties, allowing them to confirm next actions. Other company offerings simply cut transmission entirely and produce a new secure key for transmission.

Recognize that QKD is not meant to replace existing encryption technologies. The fundamental component in secure transmission is that the key is communicated between parties under a guaranteed secure line. It is used in *combination* with such technologies as Secure Socket Layer and Public Key Infrastructure to provide secure data transmission. It can be used with any encryption algorithm to encrypt and decrypt a message, which is transmitted over a standard communication

channel. As a result, when QKD works with these technologies, they deliver an unbreakable barrier of message security.

Challenges in Today's Quantum Cryptographical Methods

EVOLUTION

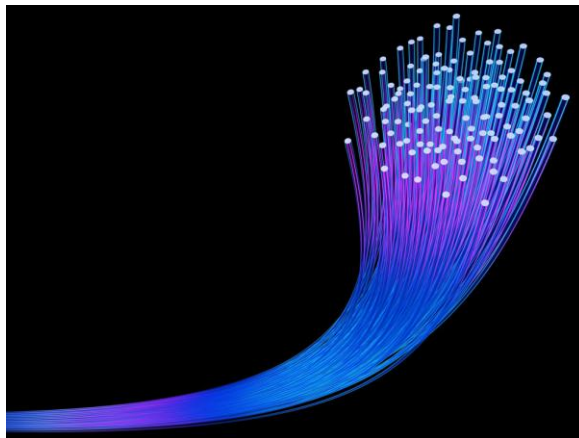
Immediately after quantum cryptography moved from a research discovery to an applied science with a public offering, security architects uncovered the business and technological implications of this business solution. In this section, we'll reflect on the challenges this technology faces as applied to market demands. Many challenges have since been overcome; some remain long-term challenges that, by nature, must be overcome with the proliferation of corporate adoption. The discussions below include approaches taken to ensure a true competitive advantage that lasts beyond the novelty period found in so many high-tech offerings on the market today.

THE DISTANCE BARRIER

From the first laboratory demonstrations over 30 centimeters of air to the latest fiber-based systems operating over 140 kilometers, QKD has certainly come a long way in the last two decades. Current systems offered by U.S. companies to the public provide 140 kilometers before security denigrates. However, recall that any attempt to measure, observe, or copy the photon stream leaves traces in the signal, and therefore a repeater installed at each hop would destroy the signal's viability. So, a solution to this distance barrier has been worked out in the form of hops. A company that offers quantum cryptography solutions, MagiQ Technologies, currently plans to build a quantum network spanning New York and Washington, D.C. Involving 7 hops between the two cities; each hop incorporates a tamper-proof black box that regenerates the key to the next hop.

THE USABILITY BARRIER

Although quantum cryptography is a new technology, it is surprisingly easy to integrate. Generally, the physical offering itself consists of a black box the size of a PC. The box uses current fiber infrastructure and requires as much energy as a personal computer. Current quantum cryptography boxes can be plugged in and ready to go in as little as 20 minutes. The boxes require virtually zero maintenance or human interference, as they are self-healing. In fact, the only particular problem of selling technology based on quantum physics is that clients often know little about quantum physics. They therefore must be briefed on how their black boxes work for them.



BANDWIDTH ISSUES

In the past, firms have been hesitant to adopt quantum cryptography because of the low speeds available at the time. However, over the years, quantum cryptographic data rates have increased from dial-up speeds of 56 kbps to 3 GigE (gigabit Ethernet, or 3 GigE/s). As a result, a number of



high-profile firms in Cambridge, Boston, Washington, D.C. and Switzerland have built quantum networks that include full quantum-encrypted streaming video, VoIP and open air.**** Current quantum networks offer multiple users to be connected with redirection routes possible when direct paths are slow or blocked.

HOW LONG WILL IT LAST?

So are there any showstoppers to this innovation in security? One school of thought is that the advancement of quantum physics could bring development of a quantum

computer (or similarly, parallel computing) that would “break” the security provided by quantum cryptography. In other words, the security provided by the laws of physics is safe today because physicists simply haven’t found a way to measure the photon stream with delicate enough instruments to avoid collapsing the stream. One day, therefore, we might just invent such instruments that would put quantum cryptography’s protection in jeopardy.

However, quantum scientists agree that a way around quantum cryptography simply doesn’t exist. Quantum computers may bring the computing power of hundreds of thousands of computers into one system; however, they cannot defy the laws of physics. Advancements couldn’t break quantum encryption because there are no technological assumptions inherent in quantum cryptography.

MARKET DEMAND

As the market for QKD develops, we can expect equipment prices to drop significantly. Within 3-5 years QKD will expand beyond the mainstay solutions applied to financial, government and military networks, to networks serving smaller companies. For example, a company in the UK has a personal system in the works; the company intends to provide cost-effective quantum security to the individual. The days when products from the quantum information industry serve every household may be sooner than you think.

**** *Quantum networks often use AES, the classical encryption method used in conjunction with quantum cryptography*

Table 3: Quantum Key Distribution Attributes

QKD Features	Why Companies Invest in QKD
<ul style="list-style-type: none"> • Uncompromisingly secure key distribution • Faster key refresh rate (than traditional approaches) • Truly random key generation • Unconditional eavesdropping protection • Proactive intrusion detection • Lower total cost of ownership • Future proof security • Speedy set-up, with virtually zero maintenance 	<ul style="list-style-type: none"> • Ensure safety of intellectual property. • Secure strategic information. • Capture an effective return on investment. • Protect data from leakage to the public. • Remove human risk. • Avoid information technology misuse; simplify processes to avoid error. • Guarantee business continuity. • Avoid reputational damage and client relationship. • Gain competitive advantage.

THE STANDARDS BARRIER

“The quantum science for cryptography and key distribution is essentially solved, and it is a great result,” explains Christian Monyk, coordinator of the SECOQC project and head of the quantum-technologies unit at the Austrian Research Centers. “Getting a system to work across a network is much more difficult. You have to deal with different protocols and network architectures, develop new nodes and new interfaces with the quantum devices to get it to a large-scale, long distance, real-world application.”²² In October 2008, SECOQC gave a live demonstration of just that – a quantum network that handles different schemes afforded by quantum cryptography manufacturers who’ve branched out to create new a new set of standards.

Economic Value of Quantum Cryptography

Many companies had been searching for a way to achieve the level of security required for such sensitive data without drastically changing their infrastructure. After quantum cryptography came to fruition, it was an “aha” moment. Once the concept of quantum cryptography moved past the research university and evolved into real-world applications, institutions and start-ups alike popped up to take advantage of the new technology that guaranteed security in data transmission. With a number of quantum cryptography products on the market since 2001, the quantum information industry has *arrived*. However, the subject is often misunderstood and misquoted. The aim of this section is to lend clarity to the business ventures, successes and advancements.



BUSINESS CASES

For certain industries, secure data transmission is critical to the success of the business. Loss of financial data, confidential customer records, and intellectual property not only involves loss due to clean-up, but also loss of collaborator confidence. Like intelligence and national security entities, quantum cryptography companies tend to fly under the radar, primarily on behalf of client preference. Client companies would neither like to advertise their security efforts nor shine a light on any perceived weaknesses they've had in the past.

Industries such as government, financial services, insurance, corporate and trading companies stand to gain the most from a technology that offers such heightened levels of security. Andrew Hammond, a vice president of quantum cryptography firm MagiQ Technologies, tells the story of a public financial institution that intercepted an eavesdropper trying to obtain the firm's encrypted earnings a few days before the earnings announcement. The company sought quantum cryptography as a solution after finding the source of the breach: a tap with a probe on the CFO's e-mail traffic. Looking forward, forecasters project that quantum cryptography will move past high-end core institutions to adoption by mid-cap financial institutions and control-based corporations within five years.

Financial Services

In 2004, the world's first bank transfer using quantum cryptography was successfully performed; Vienna's mayor supported the new technology with the transmission of an important check from him to an Austrian bank. The check required unconditional security in its transmission, laying the groundwork for the advancements that were to come.²¹ Financial services firms have been early adopters of this technology. They've expressed urgency in the provision of quantum cryptography in order to gain competitive advantage and produce efficiencies between collaborators.

Of course, insurance companies require a high degree of security in their data holdings and transmission as well. Dr. Hannes Huebel of Vienna University, who operates one of the nodes connected to a quantum network in Europe, gave the following example to illustrate the importance of security, saying, "We are constantly in touch with insurance companies and banks, and they say it's nearly better that they lose €10 million than if the system is down for two hours, because that might be more damaging...So that's what we have to prove, that we have a reliable system that delivers quantum keys for several weeks without interruption..."²⁰

Government

Clearly, the government sector has expressed intense concern over security. National security is of the utmost importance to governments around the world. Think of the secure transmission of national security information, intelligence and election results. For example, the Swiss company ID Quantique provided quantum encryption technology for the Swiss canton (state) of Geneva to transmit ballot results to the capitol in its October 2007 national election. Chancellor Hensler provided background on the choice of quantum cryptography for its elections, saying, "Information is the raw material of the State, which it uses to create added value. Whether in the context of a political decision, a police investigation or hospital care, the State is both a regulator of information exchange and a provider of information-based services."³⁸

Lottery and Gaming

Quantum cryptography companies also offer commercially available products that provide true random number generation. (Not surprisingly, the product is called the random number generator.) This device bypasses pseudo-random number algorithms, which rely on classical computers, to provide real random keys associated with physics-based number generation.

RESEARCH AND ACADEMIC ENDEAVORS

“Real breakthroughs are not found because you want to develop some new technology, but because you are curious and want to find out how the world is.”

– Anton Zeilinger, Vienna University

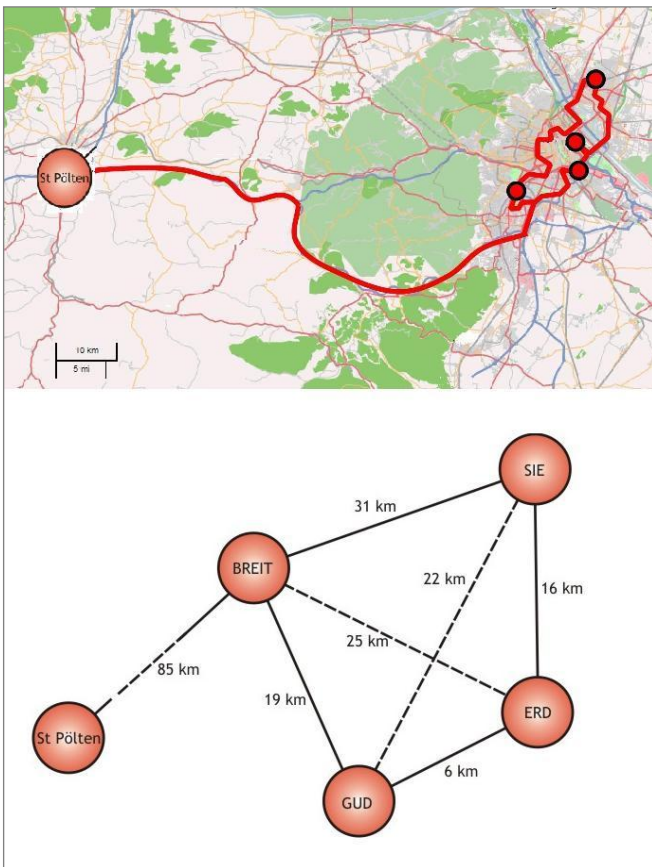


Figure 7. SECOQC's quantum network.
Courtesy of SECOQC.

The concept of quantum cryptography was proven in research labs, born out of scientific research from academic universities. Now that we've advanced quantum cryptography out of the lab and into public offerings, researchers are going back to the drawing board to see what continued advancements they can make. This section discusses worldwide efforts and funding to advance quantum cryptography.

On October 23, 2003, BBN Technologies used QKD to set up a quantum network that linked its site with Harvard and Boston Universities. Generating a 5 MHz pulse rate (0.1 mean photons per pulse), BBN provided a pioneering application that operated the world's first QKD network. The network employs 24-hour quantum cryptography, offering security over telecommunications fiber for conventional Internet traffic, including streaming video. A plan has recently been completed to expand the network through the metropolitan area to test its strength by effecting increasingly sophisticated attacks. The United States Department of Defense (DoD) is funding numerous quantum cryptography experiments as part of a \$20.6 million quantum information initiative at the Defense Advanced Research Projects Agency (DARPA). Last year DARPA also gave BBN a

nearly \$3.5 million increment of a \$14 million contract with a contingency for military applications of quantum information science (BBN operates DARPA's Quantum Network).

Today, research groups have built upon the pioneering frameworks to build systems with increasing sophistication. For example, new models are currently under development by the Secure Communication based on Quantum Cryptography (SECOQC) consortium^{††††}. SECOQC is a collaboration of academic and industrial QKD researchers, classical cryptographers, telecoms engineers, et al. Its goal is to develop protocols required to sufficiently move quantum cryptography technology into its larger-picture goal: standards for a quantum network. The €11 million research program incorporates 41 partners from 12 European countries, with the intent to create standards for storage and management of keys within a meshed network. SECOQC conducted a live demonstration of its quantum network, which concluded on October 10, 2008. The first live demonstration of a dynamic quantum network supporting a large number of users across heterogeneous QKD systems; the demonstration connected five company sites of Siemens Austria in Vienna and the neighboring capital of Lower Austria, St. Poelten. Noteworthy in this demonstration is that if one quantum link breaks down, the connections can be re-routed via other nodes so that any two users on the network can retain a secure, continuous connection.

SECOQC's strategy is to create long-range advancements to provide European citizens and companies with a standardized technology that holds fast against the threats predicted of future interception technologies. This project is expected to create the most significant advantages in the quantum security arena and the European economy. The European community sees this as such a breakthrough that the European Telecommunications Standards Institute (ETSI) announced the creation of an Industry Specification Group to start standardization efforts for quantum cryptography.

THE QUANTUM NETWORK

The quantum network offers obvious advantages. Due to the nature of quantum physics, most solutions offered today focus on point-to-point connections between only one concurrent sender and one receiver. Although these solutions are suitable for some applications, they cannot address all scenarios requiring secure communication. A quantum network offers the flexibility of today's online network; in addition, longer distances can be bridged and dynamic paths between communicating parties can be navigated. For example, the quantum network provides for more than two parties to simultaneously receive keys. Such developments keep the future open for corporations to fully integrate their QKD solutions into the quantum network.

How many years are we away from an online quantum network? In reality, it depends upon the commercial offerings that exist in the future, and how quickly companies pick up the technology to build commercial offerings. Today, quantum cryptography companies cater to firms for whom absolute security is a must. But as classical encryption continues to unravel, companies are expected to increasingly adopting quantum cryptography to ensure their information is securely transmitted over a public network.

Worldwide, both public and private entities are expected to fund well over \$50 million for quantum cryptography initiatives in the next few years. Included in this funding are not only the United States and Europe but also China, which announced its first successful quantum cryptography network in early 2007. Andrew Hammond provides insight on the market for QKD systems, saying that it will

^{††††} *European components of Ernst & Young and Hewlett Packard are partners in this venture, as well as Siemens, Nokia Siemens Networks, ID Quantique and SmartQuantum.*

reach \$200 million within a few years, just a step on the long-term forecast of \$1 billion annually”¹⁹

In fact, the subject of quantum physics as applied to information technology has become so fruitful that advancements in program studies are being made. For example, the Massachusetts Institute of Technology’s (MIT) new graduate training program, called Interdisciplinary Quantum Information Science and Engineering (iQuISE), will seek to nurture a new generation of students to become tomorrow’s quantum information scientists and engineers.

But it’s not only academic institutions whose efforts are advancing quantum technologies. Companies such as Cisco, IBM, Hewlett-Packard, Siemens, AT&T, Nokia, Nortel Networks, Verizon, Toshiba, NEC, SAIC, Fujitsu and Nippon Telegraph & Telephone (NTT) are all said to be conducting their own research on quantum information technologies. As a result, the solutions to the quantum cryptography product are getting smaller and smaller: Siemens IT Solutions and Services, Austrian Research Centers (ARC) and Graz University of Technology have collaborated to develop the first quantum cryptography chip for commercial use. The chip will be ready for series production within two years.

THE COST CONVERSATION

Ask a company why they would consider investing in quantum cryptography and, quite simply, they will tell you it’s because the information they want to transmit is invaluable. If the information they need to transmit fell into the wrong hands, it would be disastrous. For example, TJ Maxx was the victim of loss of an estimated 45.7 million customer records. This resulted in a second quarter announcement that the company had to absorb a \$118 million charge related to the massive security breach.²³ In addition, many companies find that risk for informational leakage often comes from

within the organization, and installing an automatic quantum cryptography system negates the risk of internal espionage.

Companies have notoriously had a hard time calculating the return on technological investments. Typically known as the cost conversation, many companies continue to struggle with quantifying business justifications. Over the years, the majority of companies use return on investment (ROI) to justify security investments in economic terms,¹¹ however, they often concede that many of their quantifications are merely rough estimates.

When asked the inevitable question on how customers can realize ROI for their investment, most quantum cryptography companies respond that they may realize ROI where absolute security is required. For example, let’s

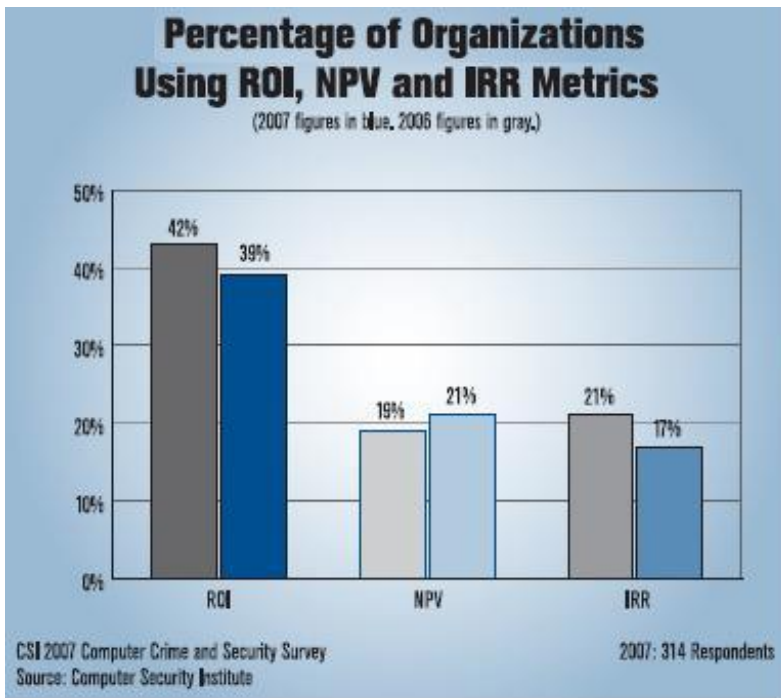


Figure 8. CSI’s percentage of organizations using different types of security investment rationalizations.

say that your company requires absolute security for each message, but cannot afford the manual transmission of one distinct key for each message. QKD resolves this issue with automatic key production (remember, each key is automatically generated to be truly distinct). Each key is transmitted using a system, so not only does it bypass the chance of human tampering but it also removes human error in transmission. The cost of a quantum cryptography box ranges from \$100,000-\$120,000 (between two point-to-point users). Such high security comes with a high price, which can be justifiable after considering repercussions of data loss.

Conclusion

After considering the physical limits of today's technology and the energy needs we face today, we're witnessing products coming to market that have already begun to exploit the potential of nanotechnology. However, the full potential that can be expected from advanced research investment in nanotechnology has not yet reached the market – it has only begun to scratch the surface.

A nanotechnological solution such as quantum cryptography is a leading force in a strong wave of nanotechnologies based on completely new properties relatively unacknowledged by the mainstream. Quantum cryptography is a powerful solution to today's security issues. It has already proven to be a successful and in-demand security solution, and it represents an enormous potential for market capture. It's an innovation that promises to revolutionize the entire IT industry over the next two decades.

Learning the principles behind quantum cryptography provides value for the next generation of nanotechnologies coming through the pipeline. It is important to educate and engage people of all backgrounds, both business and technical, in order to open a dialogue for future collaborations. Such collaborations ensure that the benefits of nanotechnology will be realized.

Acknowledgements

A special thanks to...

- Andy Hammond, Vice President of MagiQ Technologies, for providing his valuable knowledge of quantum cryptography.
- Professor Mohseni, PhD, award-winning professor of at Northwestern's Department of Engineering and Computer Sciences – a special thanks for providing availability of Northwestern's Nanotechnology Laboratory and its researchers.
- Lesley Meade Hamming, PhD, Program Director of NanoBusiness Alliance, for opening discussions with top business leaders.
- Jim Petrassi, GBS Chicago Technology Director, for discussing my LEF ideas and encouraging my work.
- Bill Lunz, GBS Principal, for providing his well-known vision and eloquence.
- Sharon Whitaker, GBS Principal, for offering her unconditional support, providing a positive influence and direction.

About the Author

K. Koenig is a consultant with CSC's Global Business Solutions. She has extensive experience in business architecture, risk mitigation and process improvement solutions. Aligning technological solutions with business needs, she has created revenue-based and utilization models adopted by firms worldwide. K. Koenig is also a regular contributor to CSC's internal newsletter, Breakaway.

K. Koenig has a master's degree from Northwestern University (joint program with Kellogg School of Management and McCormick School of Engineering and Applied Science). Founder of the program's advisory board, she is regularly requested to speak at the University on subjects such as innovation management and thought leadership.

Contact Information

KKoenig3@csc.com

KellyLKoenig@gmail.com

Mobile: 312-315-8825

Works Cited

- 1 Isaacson, Walter. 2007. Einstein: His Life and Universe. New York : Simon and Shuster, 2007. ISBN-13:978-0-7432-6473, ISBN-10:0-7432-6473-8.
- 2 2007. 2007 CSI Computer Crime and Security Survey. 2007.
- 3 2003. 2004 CSI/FBI Computer Crime and Security Survey. 2003.
- 4 Koenig, Kelly. 2008. Quantum Dots for an Energy Efficient World. 2008.
- 5 2007. s.l. : Forrester Research, 2007.
- 6 MxLogix. [Online] <http://www.mxlogic.com/PDFs/IndustryStats.2.28.04.pdf>.
- 7 Chandler, David. 2008. Turning 'funky' quantum mysteries into computing reality. MIT News. [Online] February 16, 2008. <http://web.mit.edu/newsoffice/2008/aaas-quantum-0216.html>.
- 8 2008. Nanotechnology Consumer Products Are in Your Mouth and On Your Face, Project on Emerging Nanotechnologies. (PEN). [Online] April 24, 2008.
- 9 Friedman, Discussion with David Gergen and Thomas. Free Market Society. s.l. : PBS NewsHour.
- 10 Peter D. Hart Research Associates, Inc. 2008. Awareness Of And Attitudes Toward Nanotechnology And Synthetic Biology, A Report Of Findings Based On A National Survey Among Adults Conducted On Behalf Of: Project On Emerging Nanotechnologies The Woodrow Wilson International Center For Scholars. 2008.
- 11 Randall, Lisa. 2006. Warped Passages Unravelling the Mysteries of the Universe's Hidden Dimensions. New York : HarperCollins, 2006. ISBN-13: 978-0-06-053109-6, ISBN-10: 0-06-053109-6.
- 12 Pais, Abraham. 1982. Subtle Is the Lord: The Science and Life of Albert Einstein. Philadelphia : The American Philological Association, 1982.
- 13 Holton, Geralk. 1988. Thematic Origins of Scientific Thought. Cambridge : Harvard University Press, 1988.
- 14 Heisenberg, Werner. 1971. Physics and Beyond: Encounters and Conversations, Translated by Arnold Pomerans. New York : Harper and Row, 1971.
- 15 NSF awards \$3M to MIT for a pioneering graduate training program in quantum information science. Research Laboratory of Electronics at MIT. [Online]
- 16 2006. QandA: Seth Lloyd. s.l. : Technology Review, 2006.
- 17 Lloyd, Seth. 2006. Programming the Universe: A Quantum Computer Scientist Takes on the Cosmos. s.l. : Knopf Publishing Group, 2006.
- 18 New Data Encryption System Highly Resilient Against Eavesdropping. Fellman, Megan. 2006. 2006.

- 19 SECOQC BUSINESS WHITE PAPER QUANTUM CRYPTOGRAPHY: An Innovation in the Domain of Secure Information Transmission Editing author: S. Ghernaouti-Hélie Contributing. Editing Author: S. Ghernaouti-Hélie Contributing Authors: S. Ghernaouti-Hélie, I. Tashi, Länger, Th. and Monyk, C. 2008. 2008.
- 20 Pease, Roland. 2008. Unbreakable Encryption Revealed. BBC News, BBC Radio Science Unit.
- 21 Republique et Canton de Geneve, Chancellerie d'Etat. Service communication et information. Press release of Geneva State Chancellery. Geneva is counting on Quantum Cryptography as it counts its Vote. 2007.
- 22 Beating the codebreakers with quantum cryptography. ICT Results. April 2008.
- 23 Hackers Break Into TJX's Bottom Line. Forbes Magazine. August 2008.
- 24 Rincon, Paul. 2008. Super Strong Body Armour in Sight. BBC News. 23 October 2007. <http://news.bbc.co.uk/2/hi/science/nature/7038686.stm>
- 25 Carbon nanotubes extend superbridge design. 30 May 2008. <http://nanotechweb.org/cws/article/tech/34424>
- 26 Carbon nanotubes enter Tour de France. 7 July 2006. http://news.cnet.com/Carbon-nanotubes-enter-Tour-de-France/2100-11395_3-6091347.html
- 27 How Nanotechnology Can Help Wean World off Fossil Fuels. 9 October 2008. <http://www.nano.org.uk/news/oct2008/latest1630.htm>
- 28 <http://www.nanotechproject.org/>.
- 29 Elbirt, A.J. Information warfare: are you at risk? Volume 22, Issue4. Winter 2003-2004.
- 30 TJ Maxx: 23 — Hackers Break Into TJX's Bottom Line. Forbes Magazine. August 2008.

Boeing: Carr, Jim. Former Boeing employee charged in data theft. July 2007. Secure Computing, Magazine for Security Professionals.

Fidelity National Information Services: Jewell, Mark. Reports of data breaches reached new heights in 2007. USA Today. 31 December 2007. http://www.usatoday.com/tech/news/computersecurity/2007-12-30-data_n.htm

Nordea: Russian gangs suspected of Swedish bank fraud. The Local: Sweden's News in English. 19 January 2007. <http://www.thelocal.se/6140/20070119/>

Marks and Spencer: MandS admits to losing data belonging to 26,000 staff. January 2008. Secure Computing, Magazine for Security Professionals.

London Stock Exchange: London Stock Exchange Cyber Attack. Computing.Co.Uk. 20 June 2007. <http://www.computing.co.uk/computing/news/2192455/london-stock-exchange-hacking>

London Stock Exchange: London Stock Exchange Cyber Attack. Computing.Co.Uk. 20 June 2007. <http://www.computing.co.uk/computing/news/2192455/london-stock-exchange-hacking>

Ernst and Young: Hotels.com credit card numbers stolen. CNN Money.com.
http://money.cnn.com/2006/06/02/news/companies/hotels.com_theft/index.htm

T-Mobile: T-Mobile loses 17 million customer details. Nichols, Shaun. 9 October 2008. iTnews
<http://www.itnews.com.au/News/86365,tmobile-loses-17-million-customer-details.aspx>

HMRC: New data procedures at HMRC. Parliametary reporter. Computing.Co.Uk. 30 November 2007. <http://www.computing.co.uk/computing/news/2204790/procedures-hmrc>

Veteran Affairs Data Security: All veterans at risk of ID theft after data heist. Sullivan, Bob. 22 May 2006. MSNBC.com. <http://www.msnbc.msn.com/id/12916803/>

- 31 Reid, Tim. 2008. Encryption: Quantum Code-Breaker.
<http://www.nature.com/nchina/2008/080611/full/nchina.2008.136.html>

Disclaimer

The information, views and opinions expressed in this paper constitute solely the author's views and opinions and do not represent in any way CSC's official corporate views and opinions. The author has made every attempt to ensure that the information contained in this paper has been obtained from reliable sources. CSC is not responsible for any errors or omissions or for the results obtained from the use of this information. All information in this paper is provided "as is," with no guarantee by CSC of completeness, accuracy, timeliness or the results obtained from the use of this information, and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability and fitness for a particular purpose.

In no event will CSC, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information in this paper or for any consequential, special or similar damages, even if advised of the possibility of such damages.

CSC

2021 Spring Road
Suite 200
Oak Brook, IL 60523
+1.630.574.0100

Worldwide CSC Headquarters

The Americas

3170 Fairview Park Drive
Falls Church, Virginia 22042
United States
+1.703.876.1000

Europe, Middle East, Africa

Royal Pavilion
Wellesley Road
Aldershot, Hampshire GU11 1PZ
United Kingdom
+44(0)1252.534000

Australia

26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61(0)29034.3000

Asia

139 Cecil Street
#06-00 Cecil House
Singapore 069539
Republic of Singapore
+65.6221.9095

About CSC

The mission of CSC is to be a global leader in providing technology enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients, and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC is vendor-independent, delivering solutions that best meet each client's unique requirements.

For more than 45 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol "CSC."

© 2008 Computer Sciences Corporation. All rights reserved.

