



SYNAPTIC
LABORATORIES LTD.

Ronald Kelson
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

Benjamin Gittins
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

Synaptic Laboratories Ltd.
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.pqs.io

Thursday, 1 January 2009

**Proprietary Technologies to create 50-to-100 year
including Post Quantum:**

- **Secure Communications Infrastructure**
- **Secure Collaboration Applications such as e-mail,
Instant Messaging, and VoIP**

The Problem Addressed

Public key infrastructures secure billions of transactions valued at trillions of dollars each year, for example in B2B and retail eCommerce. PKI also secures most banking credit and debit cards, Internet banking, eGovernment programs, health cards and ePassports. PKI is used in secure access control systems for access to critical infrastructures and programs.

The trend in the deployment of public key technologies has been to select smaller, faster key-lengths that provide modest short term security. Today, many years after their initial deployment, a very large number of security systems employing RSA or D&H key lengths of 1024 bit are in need of upgrading to defend against classical advances in computing power and cryptanalysis¹. Unfortunately all data and communications and certificates secured by superseded key lengths can be decrypted and all privacy and data integrity lost. This is a major problem since most PKI secured data and communications can be recorded and archived for later decryption.

Furthermore it is known that all globally deployed mainstream PKI fail catastrophically against attack by a large quantum computer capable of running Shor's quantum algorithm for approximately one second to a few minutes (depending on the clock-speed of the first quantum computer). It is impossible to upgrade existing PKI key-lengths to defend against the quantum computing threat. The arrival of a code breaking quantum computer will result in a complete global rip and replace scenario.

While there are some candidates, there is no trusted or widely accepted solution to these threats that is suitable for universal global applications such as eCommerce². Synaptic addresses this threat in an incrementally deployable non-disruptive solution using techniques widely accepted by the cryptographic community to offer security against classical and quantum computer attacks. That is, the security of our system can be reasoned from the security of components already trusted by the global cryptographic community.

Synaptic is developing a universal solution to manage these risks and threats and overcome the barriers such as mutual trust. Independent expert preliminary evaluation reports are available upon request.

More information on the problems we address can be found our website: <http://synaptic-labs.com>

In the following pages we outline the Unique Selling Points (USP's), and the potential high volume end-user applications.

¹ Florence Luy, Hendrik Lenstra, "[A mighty number falls](#)", 21 May 2007, [École Polytechnique Fédérale de Lausanne](#)

² Brian Snow, Former Technical Director of the US National Security Agency (NSA), Public Key Cryptography 30th Anniversary Conference, Dec 2006

Unique Selling Points

A **software solution** that employs hardware security modules such as low-end 8-bit smart cards to protect smart card, desktops and server communications. Often deployable on existing hardware, with no retooling required.

Post quantum secure to protect against the catastrophic failure of all mainstream PKI (RSA, ECC, D&H, etc) when large code breaking quantum computers arrive. Prof. Seth Lloyd of MIT, a coauthor of the Report by the Quantum Information Science and Technology Experts Panel of the U.S. Advanced Research and Development Activity³, states that “at current rates of progress, big, code-breaking quantum computers are at least a decade away”⁴. If we are to fully mitigate the risks anticipated by this projection than security systems requiring data privacy and integrity for at least 5 years with high assurance must be upgraded and deployed in the field with post quantum security status in less than 5 years.

A **layered defense** that wraps around existing PKI to satisfy existing standards and trust requirements while providing defense against known threats. Avoids the need to periodically upgrade low-margin PKI key lengths. Prevents decryption of recorded data and traffic as PKI attacks improve.

Migrate and/or replace existing PKI. Synaptic technologies can facilitate a incremental migration path, or an outright replacement of existing public key technologies.

More efficient than existing PKI. Synaptic authenticated key exchange operations require less CPU time and are faster than RSA & ECC for each additional key exchange.

Employs trusted well studied components. System can be built entirely from US NIST cryptographic primitives such as AES-256 and SHA-512. Key exchanges and next generation digital signatures are protocols based entirely on symmetric primitives and well studied (30+ years) cryptographic techniques.

Three solution variants to match the application. From highest-assurance small Group systems to Enterprise and Universal global system using techniques that can scale to supporting billions of users.

Suitable to upgrade Secure Socket Layer (SSL). The SSL protocol can be upgraded to support Synaptic key exchange technologies and integrated directly into open source and commercial applications without updating the operating system.

³ http://gist.lanl.gov/pdfs/qc_roadmap.pdf

⁴ http://www.technologyreview.com/printer_friendly_article.aspx?id=20590

Additional Unique Selling Points

- the Synaptic key exchange:
 - is NOT a new public key algorithm
 - combines known and well studied key exchange techniques in new secure ways
 - is a protocol based on standards based ciphers that facilitates fast take up as the fundamental design principles within the protocol are well known and studied
- the Digital signatures are based on Merkle tree technologies
 - have been known and studied for as long as RSA and D&H
 - both the Coronado Merkle Signature Scheme (CMSS) and Generalized Merkle Signature Scheme (GMSS) offer excellent performance
 - are known to offer long term (including post quantum) security when used with strong hash functions
- the complete Synaptic solution enables the first high assurance classical and post quantum secure digital signatures, key exchanges, messaging and VoIP for all size groups:
 - easily marketable as software, no manufacturing ramp ups or heavy capital costs
 - can be deployed and operational rapidly before large quantum computers are commercially available and before the deployment of the next PKI key length upgrades
- patent applications filed over all key technologies including underlying principles
- patent law foundation offers opportunity to deploy globally uniform solutions, removing the risks and cost of 'bridging' disparate systems

Potential High Volume End User Products

The Synaptic technologies can enhance existing open source applications used ubiquitously across the Internet with 50-to-100 year security (including post quantum security) to prevent against catastrophic security failures:

- secure e-Mail
- secure file transfers
- voice over IP
- secure instant messaging
- virtual private networks
- secure socket layer