⭯⌥^↑↪⇆▼↪↕⮌↳⇡⇱△⇣⌤⇉↻

The DNA-256 IP

& Product Suite

by Garth Wayne Haslam - Cryptographer & Technology Inventor / Architect

*A '**Pattern Transforming Intelligence**' named '**Quantum Abstractive Superdense Coding Obscurity**'*
Facilitates A Unique Future-Proof Crypto - Impenetrable by Classical & Quantum Computers...
Makes Data Storage & Data Transmission - Useless To Hackers & Eavesdroppers
Applicable to Most Industries & Government Services - And Enabler of Future Startup Companies

A growing number of interested parties have requested a document such as this - So here it is
This document merges / updates / replaces all previous documents and communications

What Makes DNA-256 Possible?

A 'Pattern Transforming Intelligence', that I named 'Quantum Abstractive Superdense Coding Obscurity'; - the shortest description possible. The complete proprietary composite technique, is encapsulated in the DNA-256 IP Trade Secrets. This technique is not the only proprietary technique, but the primary technique of everything that makes up the DNA-256 IP Trade Secrets. Without it, DNA-256 wouldn't have even been possible. This pioneering, extremely innovative technique, is expected to have multiple future applications, besides Impenetrable Cryptography. It's something I've enjoyed musing / thinking about, ever since it first came to me, in a eureka moment I will never forget...

In The Simplest Terms - What Is A Classical Computer?

- Your present Smartphone, Tablet, Netbook, Laptop, Desktop, Workstation, Server.
- Represents data, as groups of Digital Bits.
- Each Digital Bit, can be either a 0 or 1, but never both, and never anything else.
- Considers multiple potential states of data, one at a time, sequentially or randomly.

In The Simplest Terms - What Is A Quantum Computer?

- A totally different way of computing, that relies on the properties of Quantum Physics.
- Represents extreme abstractions of data, as groups of Quantum Bits (QuBits).
- Each QuBit, is indeterminately between 0 and 1 until read at the end of the calculation.
- Considers multiple potential states of data, in the same instant, ie. in abstraction.
- The more QuBits, the more simultaneous abstractions of abstractions of abstractions...

What Is The DNA-256 IP?

- A Futuristic Technology inspired by God's Creations of : DNA and the Laws of Quantum Physics...
- Future-Proof Encryption And Other Cryptographic Functions, That Generate :
    - Encryption that is Impenetrable / Unbreakable, by Classical & Quantum - Computers & Cryptanalysis, so therefore meets and even exceeds :
        - Post-Quantum Cryptography (PQC).
        - Classical & Quantum Secure Cryptography.
        - Classical & Quantum Safe Cryptography.
        - Classical & Quantum Resistant Cryptography.
        - Classical & Quantum Computer Proof Cryptography.
    - Decryption of the above.
    - Hashes, Digital Fingerprints, Digital Signatures, etc.
    - Quantum True Random Numbers, for creating : Files, Keys, Shared Secrets, Passwords, etc.

The DNA-256 IP is a portfolio of Intellectual Property (IP), invented, architected, implemented, and tested, by Garth Wayne Haslam, from 2012-2019. DNA-256 is a fully-functional cryptographic solution, that makes data impenetrable to cryptanalysis, whether using Classical Computing or Quantum Computing, and so, absolutely useless to hackers, eavesdroppers, tampering, etc, whether that data is in temporary or long-term storage, or is being transmitted locally, globally, or beyond. DNA-256 encrypts the data, and generates one or more keys for that encrypted data. As long as the key(s) are kept secret, the encrypted data remains impenetrable and useless to hackers, eavesdroppers, tampering, etc.

The number of keys generated by DNA-256, will depend on the required number of key-holders or vault-sites, where keys are held, and the number of keys required together / simultaneously, to unlock / decrypt the encrypted data. For example, in an Escrow scenario, there may be 9 key-holders or vault-sites, where keys are held, but you decided at the time of encryption, that keys from only 6 of them, would be required to unlock / decrypt at some future time, in case, up to 3 of the key-holders were unavailable, or up to 3 of the vault-sites were compromized, in the future. DNA-256 can accommodate any Escrow scenario. A copy of each encrypted file, should be held by all key-holders or vault-sites, in case of the unavailability of a key-holder or a compromized vault-site. Actually, the encrypted files can be stored or transmitted anywhere, without jeopardizing security, so long as they are available when required, and their matching keys are securely held by the required minimum of key-holders / vault-sites at all times. Escrow, is a means of permitting access to something of value, only when there is a required number or minimum number of, custodians authorizing such access, using their keys or signatures etc.

What Does The Product Suite Consist Of?

- The DNA-256 Chip : Available as a 64-pin or 100-pin QFN package Silicon Chip / ASIC, that has a real (not pseudo) Quantum True Random-Number-Generator (QRNG / TRNG / QTRNG), and the unique set of DNA-256 Cryptographic Primitives, Formulae, and Algorithms, locked inside. The 64-pin Chip's dimensions, are < 0.9x9x9mm. The Chip, is itself the smallest possible self-contained DNA-256 Device. It could be embedded directly onto or within, the PCBs of Smartphones, Tablets, Netbooks, Laptops, Desktops, Workstations, Servers, and any other OEM electronic device requiring its advanced cryptographic features.

- The DNA-256 Device : A robust, epoxy-filled, waterproof anodized-aluminum enclosure, containing a Printed Circuit Board (PCB) with the above silicon chip fitted. The device has a single USB connector, to facilitate connection to a computer or computing device, either directly or via one or more USB hubs.
- The DNA-256 Dongle : A miniature version of the DNA-256 Device, the size of a USB Memory-Stick or Thumb-Drive.
- The DNA-256 Click-Board : A miniature version of the DNA-256 Device, the size of a typical Click-Board. A wide variety of Microprocessor & Microcontroller & FPGA Development Boards, have one or more sockets especially for plugging in a huge array of Click-Boards. A Development Board with two or more Click-Board sockets, could combine one or more DNA-256 Click-Boards, along with one or more other Click-Boards. Other Click-Boards on the market include : various types of serial and parallel interfaces, eg. USB, Fiber Optic, IrDA, RS485; various types of display, eg. LED matrix, TFT; various types of radio link, eg. RFID, NFC, 3G, Wi-Fi, LoRa; various types of sensors; various types of switch, keyboard, potentiometer; various types of non-volatile memory; etc. So for example, DNA-256 could be combined with NFC and 3G, to easily produce a device that could read RFIDs and Smart-Cards, impenetrably encrypt their codes, and transmit these securely via 3G UDP / TCP, to a matching receiving device elsewhere in the world. Later as time and funds permit, the circuitry from this combined solution, could be merged into a miniaturized single PCB solution, where instead of using the DNA-256 Click-Board(s), DNA-256 Chip(s) would be used instead.
- The DNA-256 System :
    - A customer specified enclosure -
    - A 19" 1U or 2U enclosure, or an entire 19" Rack Cabinet of such -

  - Containing a number of DNA-256 Devices or Dongles, and USB Hub(s), and having a single external USB connector (per group of up to 127), for connection to a computer or computing device, eg. a workstation or server, maybe interfacing it to an entire local area, wide area, or global, network, depending on requirements.

- 3rd-Party Distributable USB Device-Drivers : A software interface between the DNA-256 Device's USB interface, and the DNA-256 Commands App; available for various computer operating systems, including Microsoft Windows 10 64-Bit.
- The DNA-256 Commands App : An App for Microsoft Windows 10 64-Bit, that provides an API of DNA-256 Commands, that can be called :
    - Directly from the command-line like DOS / UNIX commands.
    - From script / batch files.
    - From customized console apps.
    - From customized graphical user interface (GUI) apps.

As many copies of the App, as you wish, and your Microsoft Windows 10 64-Bit computing system will support, can be run simultaneously in parallel. The Apps will automatically negotiate access to the installed pool of DNA-256 Devices, and generate Log Files.

- Sample Script / Batch Files : To demonstrate how easy it is to use one or more DNA-256 Devices simultaneously on the same computer.
- A Sample Console App : To demonstrate how easy it is to use one or more DNA-256 Devices simultaneously on the same computer.
- A GUI App : To demonstrate how vastly different :
    - DNA-256 encrypted data is, vs, non-encrypted data.
    - One DNA-256 encryption is, vs, another of the same non-encrypted data.
    - One DNA-256 generated key is, vs, another.

  In each case, the difference will be approximately 50% (the absolute optimum). A 100% difference, would be very bad, as it would be a pure-inversion of all bits.

- There are also some domain names, appropriate to the technology.

What Commands Does The DNA-256 Commands App Provide?

- Generate Quantum Random (Truly Random) : files, keys, public / private keys, shared secrets, passwords, etc.
- Generate Hash, Digital Fingerprint, Digital Signature, of : files, zip files, keys, public / private keys, shared secrets, passwords, etc.
- Encrypt / Decrypt with asymmetric keys (Public / Private keys).
- Encrypt / Decrypt with symmetric keys.
- Compare, Convert, Verify, Analyze : files, keys, public / private keys, shared secrets, passwords, etc.
- Multiple Actions, in parallel, or sequentially.
- Commands wait for the next available DNA-256 Device, so, many DNA-256 Command Apps running in parallel, will automatically share the entire pool of installed DNA-256 Devices.
- Display Help Info.

How Would An OEM Add The Chip or Multiple Chips To A Product's PCB?

- Provide the chip with a 3.3V supply.
- The chip is internally clocked, so no external clocks are required.
- Add some surface-mount decoupling capacitors.
- Connect the chip's Tx pad and Rx pad, to the Product's microprocessor, microcontroller, FPGA, etc. The Tx and Rx signals are 3.3V UART compatible. Chips with alternative interface types, can be custom made if required.
- Same again for any other DNA-256 Chips.

How Would An OEM Product Access The Chip or Multiple Chips On A Product's PCB?

Whereas the present DNA-256 Commands App is a 64-Bit App to run under Microsoft Windows 10 64-Bit, and uses freely re-distributable USB Device-Drivers to interface the App to the Chip via a USB connection; if say a manufacturer of Android Smartphones, wanted to add the Chip to their next generation Smartphones, the following would be required :

- Purchase a license to the Chip Programming File, and then program Chips.
- Incorporate the Chip and some decoupling capacitors, onto each Smartphone's PCB.
- Purchase a license to the App's Source Code, and then port it from its Microsoft Windows compatibility, to Android compatibility (small changes), and convert the USB Device-Driver calls to direct UART calls.

What Do I Mean By 'Impenetrable'?

DNA-256 is so named, because in addition to being inspired by Quantum Physics and related mathematics, the amazing properties and possibilities of DNA played a large part too. Also, the symmetric and public key size, is 256-bits. This key size, gives 2^{256} combinations, which is approximately :

115792089237316195423570985008690000000000000000000000000000000000000000000000 combinations!!!

That's a huge number in comparison to anything, eg. the number of atoms in the universe... But it's the same number of key combinations, that some other cryptographic algorithms have, eg. AES-256. Where DNA-256 gets its strength in comparison to other cryptographic algorithms, is that DNA-256 doesn't have the accidental or deliberate, mathematical weaknesses or short-cuts, and back-doors, that make others susceptible to various types of cryptanalysis attacks.

A Quantum True Random-Number-Generator, and a unique set of DNA-256 Cryptographic Primitives, Formulae, and Algorithms, locked inside a Silicon Chip / Application Specific Integrated Circuit (ASIC), work together in secret, as a 'Pattern Transforming Intelligence', to generate encryption of data, that appears to be a sequence of completely random numbers, with no apparent way-in or starting point for decryption.

With DNA-256, the key is the ONLY way-in, so without it, there is no way-in. For example, DNA-256 Encryption is like, converting the data into a randomized formula, then separating the formula into numbers and mathematical symbols, with all the numbers going into a file called 'encryption', and the mathematical symbols going into a file called 'key'. Obviously, the key is the ONLY way-in.

Some other cryptographic algorithms, produce encryption where a cryptanalysis attack, can actually work out most if not all, of the key that was used, similar to using simultaneous equations to work out unknowns.

> [Note : For the following explanation of why this would be a futile exercise, please note that there are some extremely large numbers referred to, and so a scientific notation is used for most of these, eg. (1.1579208923731619542357098500869e+77) means, 115792089237316195423570985008690000000000000000000000000000000000000000000000.0 where, the 'e+77' means that the decimal point needs moved '77' places to the right, adding 0s as required, in order to do so.]

But with DNA-256, the only type of attack that would 'eventually' succeed, is a Brute-Force attack, where every key combination is tried one-by-one, until successful. **HOWEVER, even with a network of suitably configured Quantum Computers, all kitted out with millions of DNA-256 Devices; there are many reasons why such an attack, would take such a vast amount of time, as to be practically impossible.** Eg. If the combined cryptanalysis resources, on average, could process a DNA-256 encrypted file, through the DNA-256 decryption algorithm (in-chip), in a single microsecond, then to try every key combination, it would take :

- (1.1579208923731619542357098500869e+77) microseconds =
- (1.1579208923731619542357098500869e+71) seconds =
- (1.9298681539552699237261830834781e+69) minutes =
- (3.2164469232587832062103051391302e+67) hours =
- (1.3401862180244930025876271413043e+66) days =
- (3.6692298919219520946957621938515e+63) years.

On average, only 50% of the key combinations would need to be tried, but that would still take approximately :

- 1834614945960976047347881096925700000000000000000000000000000000 YEARS.

And that's just to crack a SINGLE FILE!!! To crack the next file, would be the same all over again...

Also :

- The DNA-256 Chip's built-in Quantum True Random-Number-Generator, results in two or more separate encryptions of the same file, being approximately 50% different from each other. The generated keys will similarly differ by approximately 50% too. In each case, the difference will be approximately 50% (the absolute optimum). A 100% difference, would be very bad, as it would be a pure-inversion of all bits.
- A 'Pattern Transforming Intelligence', built into the algorithms within the chip, will result in the encryption of files larger than a certain size, being slightly smaller after encryption and key generation. The size difference cannot be predicted, thus adding another level of security.
- Some of the cryptographic primitives making up the algorithms locked inside the chip, are purely 'countermeasures', to protect against various types of advanced cryptanalysis attacks.

That's why DNA-256 Encryption is Impenetrable / Unbreakable, without having the key for that specific encryption.

Who Else Has Verified The Impenetrability Of DNA-256 Encryption?

- During testing of the DNA-256 Algorithms, sample encrypted files were made available via a website, and hundreds of copies were downloaded. Since then, there has been a stream of requests for these files, which have been sent directly to them. The only feedback from the people and organizations who have a copy of these files, is that the files are totally random with no way-in to even begin cryptanalysis. Some people believe these sample encryptions are just files generated by a Random-Number-Generator. Without them purchasing a DNA-

256 Device or two, to generate their own sample encrypted files, and use the same or second Device to decrypt them back to their non-encrypted format; it is difficult to convince these people that the sample encrypted files, are genuinely sample encryptions of real Data / Audio / Video files.

- Government Intelligence Agencies were contacted, and asked if they would be able to try to crack the sample encryptions. Those that took the request seriously, replied that they or their testing contacts, would have to charge for the service, and it might get expensive due to certain requirements that would need to be put in place. Also, they said that they would need the inner workings of the full IP to be disclosed to them. I wasn't able to take up their offer, due to costs, and because Trade Secrets would have to be disclosed.
- An Ethical Hacking / Penetration Testing Magazine, was offered the sample encrypted files as a competition challenge, for their next magazine issue, but after a long delay, declined the offer without providing any reason.
- There were some in the global cryptographic community, who were quite upset that they had not been consulted or involved during development of the IP.
- Quantum Computer experts and students, have been offered the opportunity to attempt to crack the sample encrypted files, but have turned down the opportunity.

Why Does Encryption Now Need To Be Quantum Computer Proof?

Quantum Computers can be simulated to a certain extent using Classical Computers. And real Quantum Computers are already available remotely via the Internet, eg. D-WAVE. Though Quantum Computers exist, and are improving exponentially, they do not yet have sufficient reliable QuBits, to be a useful tool for cracking encryption. However, they soon will, if present progress continues. And the encryption cracking algorithms that they will use, already exist, and are being improved in readiness even now, for when Quantum Computers have sufficient reliable QuBits.

As encrypted data is frequently copied and stored, by hackers of stored data, and eavesdroppers of transmitted data, for future cryptanalysis attacks when time and / or technology permits; it's very important that, the more important the encrypted data is or will be, then the sooner it should be re-encrypted to an encryption that's Future-Proof, ie. DNA-256.

Is The World Ready For Impenetrable Encryption?

All of the successful hacks of confidential data / information around the world, even at the highest levels, where you would expect security to be extreme; prove that the world needs Impenetrable Encryption for certain types of data / information. What use is encryption when it's not Impenetrable, especially if you require that encrypted data / information to remain secret / confidential, despite advances in hacking technologies and Quantum Computers?

What Size & Format Of Data Can DNA-256 Encrypt?

- Any Size.
- Any Format.
- Data, Audio, Video...

Can DNA-256 Encrypt / Decrypt - Streams of Data / Streaming Data?

- Yes, there is a mode for that.
- Some DNA-256 Commands, allow a chain of such commands to 'Pipe' one command's output, to the next command's input..., and for the first command to take its input from a file / device, and the last command to give its output to a file / device...

Why Doesn't This Document Use Cryptographic Terms Such As 'Plain Text' and 'Cipher Text'?

- Not all interested parties understand such terms, so appreciate the easiest read possible.
- Some interested parties are purely financial investors, who will involve technical people later.

Is DNA-256 Actually Classed As Encryption?

- DNA-256 is much more than encryption. Each DNA-256 Chip or DNA-256 Device, is a Hardware Security Module (HSM), containing many Cryptographic Capabilities.
- Used in its slower but impenetrable mode, DNA-256 uses its inherent 'Pattern Transforming Intelligence', to not only encrypt, but generate a key (or Escrow keys), that absolutely must be present for future decryption, as the correct key(s) are the ONLY way-in. Each Escrow key is just as futile to attempt to Brute-Force, as a single key.
- Some people believe that encryption is ONLY when :
  - Data is converted to an encrypted form by means of a key.
    Whereas in DNA-256's impenetrable mode :
  - Data is converted to an encrypted form, plus a key (or Escrow keys) are generated.
- DNA-256's various Encryption modes, can use an input key (Shared Secret / Public Key / Private Key), but can also generate an output key or keys.
- DNA-256 is unique, being made up of many Countermeasures & Cryptographic Primitives, uniquely configured; several of which, are unique / novel too, so don't exist anywhere else and so cannot be found in Encryption Textbooks.

What Else Does DNA-256 Incorporate?

- Turns the Chip's Hardware Random-Number-Generator into a Quantum True Random-Number-Generator. Though not a pseudo Random-Number-Generator, but a real Random-Number-Generator, DNA-256 has special properties that removes even the slightest possibility of bias in the randomization.
- Sophisticated Countermeasures, to block attempts to discover the DNA-256 Algorithm or its component Cryptographic Primitives...

How Can Others Test DNA-256?

- Request free sample encrypted files, for you to analyze to your heart's content.
- Purchase one or more DNA-256 Devices, for you to create your own encryptions, analyze them, and then decrypt. Of course, in addition to being an evaluation device, it's also a fully functioning practical tool for real-world cryptographic applications.

- Quantum Computer experts and academia, may wish to use their organization's Quantum Computer or a remotely accessible one, to analyze or perform cryptanalysis on sample encrypted files.

What Other Applications Will DNA-256 Improve Or Facilitate?

- Absolute Privacy of data stored in the Cloud anywhere.
- Access Management.
- Aircraft Remote-Control / Telemetry - Anti-Hijacking.
- Anti-Cloning.
- Anti-Counterfeit.
- Anti-Hijacking.
- Anti-Identity-Theft.
- Anti-Piracy.
- Anti-Tamper.
- Assets Management.
- Blockchains.
- Cryptocurrencies.
- Cryptocurrency Mining Work.
- Crypto-Currency Wallets.
- Data Center - Mass-Encryption / Mass-Decryption - Engine / Processor.
- Data Compression.
- Data Shredding.
- Decrypting After Downloading From The Cloud.
- Distributed Data Vaults.
- Distributed Key Systems.
- Drone Remote-Control / Telemetry - Anti-Hijacking.
- DVD / Blu-Ray Encryption.
- Encrypted Live Streaming.
- Encrypted Messaging Apps.
- Encrypting Before Uploading To The Cloud.
- Encryption of 'Originating Source & Final Destination' fields, of data packets, between network nodes. Eg. Nodes on the network that are DNA-256 compatible (contain DNA-256 in some form), could temporarily decrypt the Final Destination field, while securely inside the DNA-256 compatible node, to determine the best neighbouring node to forward the anonymous data packet on to...
- Fintech.
- Hard-Disk Encryption.
- Helping organizations meet or exceed the General Data Protection Regulations (GDPR).
- ID Authentication.
- Immutable Data.
- Impenetrable Vehicle Immobilization Systems.
- Implantable Cardio Defibrillator (ICD) Remote-Control / Telemetry - Anti-Hijacking.
- IP & Data Escrow.

- IP Protection.
- Key Management.
- Layered Security - Allowing Documentation etc, to unveil portions of a Document etc, according to the Security Clearance of the Person / System accessing it.
- Licensing Dongles.
- Licensing Management.
- Logistics / Shipments Tracking.
- Making ID-Enabled Firearms Unhackable.
- Merged with Mesh Networking IP, an Impenetrable Multi-Node Virtual Private Network (VPN), could be constructed, for absolutely private transactions of any type of data, between multiple parties.
- Password Management.
- Pay Per View TV.
- Product Authentication.
- Reducing / Eliminating the DC-Offset in VOIP / Data Transmission Signals.
- RFID / NFC Systems.
- Robot Remote-Control / Telemetry - Anti-Hijacking.
- Secure Access Control.
- Secure Access, Storage & Transmission of ID Info : Fingerprints, Facial Recognition, Voice Recognition, Retina & Iris Recognition, Passwords...
- Secure Aircraft Telemetry Links.
- Secure Backups.
- Secure Data Acquisition.
- Secure Database Sharing & Access.
- Secure Electricity Grids.
- Secure Email.
- Secure Inter-Vault Communications.
- Secure Intra-Vault Communications.
- Secure Mesh Communications.
- Secure Mesh Networks.
- Secure Mobile Networks.
- Secure Radio / Microwave / Laser Links.
- Secure Radio Modems.
- Secure Remote Control.
- Secure Remote Metering.
- Secure Remote System Access & Control.
- Secure Satellite Command & Control.
- Secure Satellite Links.
- Secure Solar Farms.
- Secure Spacecraft Telemetry Links.
- Secure Tank Farms (Gas / Oil / Water).

- Secure Transponders / RFIDs / NFC - Where the required trigger and / or response, is different every time (random but with intelligence), so eliminating cloning, spoofing, fakes, imposters...
- Secure Vehicle Telemetry Links.
- Secure Voice / Video Calls.
- Secure VPNs.
- Secure Wind Farms.
- Securing Artificial Intelligence (AI).
- Securing Autonomous Vehicle Intercommunications.
- Securing Backup Distribution.
- Securing DNA / Gene / Genetics / Bio-Tech Databases & IP.
- Securing Formula-One Racing Car to Pit Communications & Telemetry.
- Securing Gas / Oil / Water Infrastructures.
- Securing Machine Learning.
- Securing Medical Equipment.
- Securing Medical Records.
- Securing Remote Surveillance.
- Securing Telecommunications Infrastructures.
- Securing The Internet of Things (IOT).
- Securing Traffic Control Systems.
- Securing Undersea Cable Links Against Eavesdropping.
- Site To Site - Mass-Encryption / Mass-Decryption - Engine / Processor.
- So as to send some Data from one point on the planet to another, without that Data being able to be eavesdropped, and its route being able to be tracked, DNA-256 can be used in a very special way to simultaneously accomplish both.
- SSD Encryption.
- Subscription TV.
- Supplier Authentication.
- Tamper-Resistance.
- The ideal encryption solution to combine with Quantum Key Distribution (QKD).
- Vehicle Remote-Control / Telemetry - Anti-Hijacking.

As DNA-256 is applicable to most industries, and many government services, all requiring Unhackable data / information security, the above list is just a generalization of potential applications, either for DNA-256 as it is, or merged with other technologies.

Depending on how DNA-256 Products / Systems are used in other products / systems, and whether they are added to existing products / systems, or products / systems are built around them, determines whether DNA-256 :

- Makes Data Unhackable.
- Makes Data Useless To Hackers.

Impenetrable Encryption aside, the DNA-256 Chip & App IP, maybe of interest to anyone who wants to put some other algorithm into a chip, and make it accessible via a USB interface and app, ie. as a co-processor or algorithm-processing-engine.

Is DNA-256 Patented Anywhere?

Though there are numerous patentable, unique, and novel, properties that together makeup DNA-256; ***patenting these, was not the best or most appropriate protection available***. Patenting makes IP publicly available, so would have reduced the potential security applications of DNA-256. A chip was required anyway, to provide a True Random-Number-Generator; so it was decided that DNA-256's unique set of Cryptographic Primitives, Formulae, and Algorithms, would be locked inside a Silicon Chip / Application Specific Integrated Circuit (ASIC), as 'Trade Secrets', to work together in secret. ***If the DNA-256 IP / Trade Secrets, are ever sold exclusively***, then the purchaser would have the right to apply for patents anywhere they wished, if they so desired. The DNA-256 Devices, are each a complete Hardware Security Module (HSM). The inner workings of HSMs, are best kept as Trade Secrets, rather than being patented.

How Has DNA-256 Been Funded?

- Self-Funding.
- Overdrafts.
- Gifts.
- Occasional External Projects / Contracts - In Parallel.

What Alternatives To DNA-256 Are Out There?

- Classical Encryption that is being broken by Classical Computers, certainly won't survive Quantum Computers.
- The NIST is currently evaluating entries to their Post Quantum Cryptography competition. Many entries have already been eliminated. Some entrants have submitted multiple potential solutions, rather than narrow these down to just one that they are sure will pass.

Has DNA-256 Been Submitted To The NIST Competition?

No. Why not?

- Full public disclosure of the DNA-256 IP (Trade Secrets) would be required.
- Monetization would be forever damaged.
- DNA-256's R&D and V&V costs from 2012-2019, would never be recouped.
- DNA-256 includes, but goes well beyond, Post Quantum Cryptography (PQC).

How Do Governments View Impenetrable Encryption?

The World is a big place in some ways and seems small in other ways. It is made up of many governments, each with their own views about encryption, and Impenetrable Encryption. Some like the idea and others don't. Some want a way-in especially for them, some don't, and some are still undecided. Some view the extremely popular AES-256, which was based on the winner of the last big cryptography competition, as practically impenetrable; but compared to DNA-256, it certainly isn't. Quantum Computers will be able to quickly crack AES-256 encryptions. Many encryption algorithms, once promoted by governments as very secure, have already been broken by even Classical Computers. Elliptic-Curve cryptography, was fairly recently promoted as the next generation of encryption, but has already been labelled as, 'Not Suitable For Future Designs'.

I contacted the UK government regarding their requirement, that encryption suppliers unlock customer-generated encryptions, when required to do so by court order. I explained that in the case of DNA-256 Encryption, it would be mathematically / technically impossible, for me to comply with such a potential court order. Their reply does not prohibit Impenetrable Encryption. The reasons for genuinely being unable to comply with such an unlock-order, are that with DNA-256 Encryption :

- There are NO back-doors.
- There are NO mathematical weaknesses or short-cuts.
- A Quantum True Random-Number-Generator is used.
- Generated Encryptions, even from the same original file, are never the same.
- Generated Encryptions, look and analyze as totally random with no way-in.
- Generated Keys, even from the same original file, are never the same.
- Generated Keys, look and analyze as totally random, so can't be predicted...
- Cryptanalysis is futile, as it won't reveal the original non-encrypted data, or key(s).
- Attempting to Brute-Force is futile, as the time and resources required, are practically infinite.
- It's Impenetrable / Unbreakable.
- Due to the unique properties of the DNA-256 Algorithms, Formulae, and Primitives, in combination with a built-in Quantum True Random-Number-Generator; even I as Inventor and Architect of DNA-256, have absolutely no way of knowing or discovering, the 256-bit key(s) generated each time.
- The DNA-256 Device and DNA-256 App, do not retain the generated encryptions and keys, and in fact, reset and exit respectively, on completion of each DNA-256 Command sequence.
- If the DNA-256 App(s) are executed from a RamDisk / RamDrive on the user's computing device, then the only place the generated key(s) will reside, until the user moves them, is in file(s) on the RamDisk / RamDrive. In fact, if the user (or their automated tools), don't relocate the generated key(s), following an encryption event, then upon a computer restart or shutdown, they will be lost forever, with no way for anyone to decrypt the encryption (which would also vanish if not relocated before a restart / shutdown).

Where Can DNA-256 : Chips, Dongles, Devices, Systems, Apps - Be Purchased?

DNA-256 Solutions have not yet been officially launched or marketed, and so are not yet available from distributors or manufacturers. However, they can all be purchased (POA) from myself (via Qi), for evaluation purposes; or for practical use, if you accept full responsibility for potential loss of data. Using a technology that generates Impenetrable Encryption, could easily result in permanent loss of access to your data, if you or your staff, etc, don't follow special procedures, or don't keep the key(s) safe and secure for EACH stored or transmitted file.

Are There Any Import / Export Restrictions?

- The chosen raw chips, have no Import / Export restrictions, except for a few embargoed countries. They are readily available throughout most of the world, which is one reason why this particular raw chip was chosen.
- After the raw chips have been programmed with the DNA-256 Chip Programming File, these chips become Cryptographic / Encryption ASICs. From that point on, Import / Export restrictions will start to apply in some additional countries; either being completely embargoed by some countries, or requiring a special license to Import / Export. You are advised to consult an Import / Export Lawyer if in doubt.

How Am I Able To Make DNA-256 Devices, Without Having In-House Production Facilities?

- I presently buy one of a number of suitable Off-The-Shelf Chip Development Boards (PCBs).
- These boards, come fitted with at least the set of components that the DNA-256 Device requires. The other components, surplus to my requirements, are disabled.
- The boards, come fitted with one of the types of raw non-programmed chip, that the DNA-256 Chip IP is compatible with.
- By using a programming device, I am able to program the raw chip whilst on the PCB, with the DNA-256 Chip Programming File. This is called 'Fabless Chip Production'. Fabless, because I don't need to Fabricate the physical chips, as the raw chips come ready made, awaiting the customization that the DNA-256 Chip Programming File provides. Any attempt to modify the chip after this, requires a full erasure of its contents first. Protection mechanisms, inside the chip, prevent the DNA-256 IP from being read / viewed by chip hackers, for industrial espionage... For the super-paranoid, there are more expensive compatible chips, that the DNA-256 Chip IP could be ported to, that will automatically erase the entire IP, as soon as any chip tampering is detected...
- In-house equipment, allows me to drill enclosures, to fit connectors, mount the PCB, and fill the enclosure with epoxy to seal everything. The result is an extremely robust waterproof DNA-256 Device or Hardware Security Module (HSM).

What Would A Purchaser / Licensee Of The DNA-256 IP, Require To Go Into Production?

- For the DNA-256 Device :
    - They could order the required Off-The-Shelf parts, from say, RS Components, Digikey, Arrow, and other good international distributors.
    - They could in-house program the chip, on each Off-The-Shelf Chip Development Board.
    - They could in-house drill or laser-cut the enclosures, or else ask the enclosure manufacturer to provide them pre-drilled.
    - Fit the parts.
    - Fill the enclosure with epoxy.
    - Fit a label, or use the laser-cutter to etch a label design into the enclosure's surface.
- For the DNA-256 System :
    - It's the same as the above.

    - Then mount multiple DNA-256 Devices into a 19" 1U or 2U enclosure, along with one or more USB Hubs, as required...
- For the DNA-256 Dongle or Click-Board :
    - Their schematics have already been verified by trying out the required configurations on Off-The-Shelf Chip Development Boards.
    - Due to limited time and self-funding, PCB layouts for these, have not yet been produced, but are simple for someone who specializes in laying out PCB designs.
    - There are outsource PCB fabricators and assemblers, who will turn the schematics into finished products, in any quantities, quickly.
    - Regarding the Chip : As these boards are NOT Off-The-Shelf, but a custom design; the Chip for each board, can either be programmed with the DNA-256 Chip Programming File :
        - By the raw chip fabricator / manufacturer. But a strict NDA maybe required, to add legal and financial protection in case of an IP leak at the factory.
        - In-house after the chip has been soldered onto the board, if a special connector has been added to the PCB layout.
        - In-house before the chip has been soldered onto the board, if a special chip programming device and chip socket are used. Such chip programming equipment, can be obtained for programming a single chip at a time, or multiples simultaneously, depending on price.
        - For either of the above in-house options, a robot or robots, can be installed and setup, to accomplish the programming autonomously. It could be left running 24 / 7, securely locked inside a vault for example. If a robot or robots are used, they could also be configured to accomplish post-production testing at the same time, if required. It is the programming task, that requires a secure environment though, as a Machine Code version of the DNA-256 IP, is exposed whilst programming.

What Is The Cost Price vs Selling Price For These Products?

- Low Cost Price.
- High Selling Price.
- Excellent Profit Margin.
- The value is likely to ever-increase, as the need for Future-Proof Impenetrable Encryption increases; as threats to presently popular 'strong' encryption algorithms, ever-increase.
- What value would you put on 'Impenetrable'?

What Do I Want To Do With DNA-256?

Originally, the desire was to obtain government and investor funding, to create an employment-generating startup in the IOM; to manufacture, and, globally market and support, the growing product suite, which was initially based on a self-contained device that would encrypt files on an inserted USB memory-stick / thumb-drive. However, a lack of such funding, and now caring for my wife and I's health, and our developing interest in a world-wide Bible education and humanitarian work, would make the long-term running of a startup myself, unfeasible. So presently, the desire is to sell exclusive / shared IP rights or multiple non-exclusive IP licenses, so any of these options could now apply :

- IP Royalty Securitization. Eg. Silicon Valley Bank does this, and I hope to discover others.
- Assist IP Brokers, a purchaser, or licensees, to monetize the IP, by helping them to :
    - Crowd Funding the setup of startups, for the manufacture and support of the present product suite, and future products; resulting in a large number of employment opportunities being created.
    - Produce quantities of the DNA-256 Chips, now, in advance of future demand; as a store of future value (like tokens), as the need for Impenetrable Cryptography ever-increases.
    - Justify their investment, by helping them to have the information they require to develop a Business Plan, for their own Startup, or Branch of their existing organization / company.
    - Design and build Automated Test Equipment (ATE) or an Encryption As A Service (EaaS) System, for investor / customer Demonstrations, eg. For the annual CES in Las Vegas, and Hackathons, and other such events...
    - Manufacture and globally market the existing products.
    - Train staff, including Field Application Engineers (FAEs), to assist customers with applying DNA-256 products to their industry / markets...
    - Merge the DNA-256 products with other technologies, to create new products.
    - Design and build Automated Test Equipment (ATE), for post-production testing of products before shipment.
    - In the case of selling exclusive or shared IP rights - assist the purchaser with :
        - Merging the DNA-256 IP with other technologies, to create new products.
        - Applying for patents, if they so wish.
        - Selling / licensing the IP to their customer(s), if they so wish.
        - Writing Textbooks, if they so wish.
        - Writing & Developing Training Materials, if they so wish.

Will DNA-256 Need To Adapt As New Threats To Encryption Emerge, Such As, More Powerful Quantum Computers?

The key(s) are the ONLY way-in for decryption, and attempting to Brute-Force is futile, as keys are generated in an unpredictable, randomized way; so even exponentially more powerful Quantum Computers, will still find DNA-256 Encryptions to be Impenetrable.

What Could Owner(s) Do With The DNA-256 IP, Besides Produce The Present Product Suite?

The DNA-256 Chip is a Microprocessor-oriented ASIC, so its Source Code has been written in the C / C++ Programming Language, then compiled, and then assembled, into a Machine Code - Chip Programming File. Under an appropriate IP transfer, share, or licensing agreement(s), the purchaser(s) would have the options to :

- Move certain DNA-256 Chip functionality into the DNA-256 Commands App (also C / C++ Programming Language based), to benefit from super-fast multi-core processors on state-of-the-art servers, workstations, and gaming laptops... However, the Quantum True Random-

Number-Generator will still need to be Chip-based, and the Computing System(s) will have a much greater need to be caged, or other security precautions implemented, as the entire DNA-256 Encryption IP will no longer be entirely locked inside the Chip as Trade Secrets.

- Add custom functions into the existing Chip, to add further capabilities, perhaps for bespoke customer applications.
- Produce custom boards, such as PCIe or larger, that could be populated with up to hundreds of DNA-256 Chips, arranged as a matrix of chips on each side... There's a Real-Time Operating System available, that can be installed UNDER Microsoft Windows, that would be ideal, for enabling Windows Apps to access a vast array of chips, simultaneously, without requiring a USB interface to each. I have experience of designing and implementing such boards (and device-drivers, firmware and software), even purpose designed motherboards and communications boards for Silicon Valley startups.
- Produce ever-faster Chips, by increasing their execution speed, by :
    - Increasing the efficiency of the existing C / C++ code, by converting time-critical functions to :
        - More efficient code.
        - Macros.
        - In-line Assembly Language.
        - Etc.
    - Porting the Chip IP to future, faster ASICs.
    - Porting the Chip IP to multi-processor / multi-core (physical or virtual) ASICs.
- Convert / Port the Chip IP from C / C++ to System C, VHDL, etc :
    - The Chip IP, contains both combinational and sequential logic and codes, synchronized in such a way, that attempting to attain substantially greater parallelism, of each encryption / decryption process, would be futile.
    - What can be accomplished though, is :
        - Creating a number of virtual-processors, to each handle separate encryption / decryption processes.
        - Moving certain functionality, from virtual processor(s) into faster Logic-oriented implementations.

What Value Do You Put On the DNA-256 IP?

- Chip's Source Code.
- Chip's Programming File (Source Code Compiled & Assembled into Machine Code).
- Command App's Source Code.
- Command App's Executable File (Source Code Compiled & Assembled into Machine Code).
- TBD for all of the above, depending on whether selling exclusive rights or multiple non-exclusive licenses...

Will I Do Video / Phone Calls?

I do Linked-In messaging, emails, and in-person meetings with seriously interested persons / organizations.

Will I Sign NDAs Or Similar?

- No NDA is required to receive a copy of this document for example.
- No NDA is required to receive sample encrypted files for your own cryptanalysis or black-box testing.
- If interested parties wish to discuss how they see DNA-256 working with their technologies or products, I prefer them to discuss this in such a way that they are not disclosing something confidential about their own technologies or products.
- I will occasionally consider signing certain Mutual NDAs, for special circumstances only.
- For previous projects, I've signed NDAs, Mutual NDAs, and many times, the UK Official Secrets Act. ***I do not design and implement solutions exclusively for military purposes.***

How Much Will I Disclose About DNA-256 Under A Mutual NDA?

- There is little difference between what I can disclose, inside or outside of an NDA.
- What I can disclose, has mostly already been disclosed in this and previous documents, with any further disclosures likely be added to this document as an update.

How Much Will I Disclose About DNA-256 Under An IP Purchase Or License Agreement?

- The IP Purchaser or Licensee, should assure themselves of the suitability of DNA-256, prior to any agreement, by conducting their own cryptanalysis and black-box testing of :
  - Free, sample encrypted files.
  - Purchased, DNA-256 Devices & DNA-256 Apps.
- Once the purchase or licensing transaction has been agreed and executed, the agreed parts of the DNA-256 IP, will be disclosed to that party, in the manner agreed. The IP is in two forms :
  - Source Code in C / C++ Programming Language.
  - Programming / Executable File (Source Code Compiled & Assembled into Machine Code).

About The Author And Inventor

- Can be contacted in writing, via :
  - Email : ConsultantArchitect@Yahoo.CA
  - Web Form : QuantumImpenetrable.COM
  - Linked-In - Connection requests welcome.
- Age : Early 50's.
- Professional Experience : 35 years.
- World-Wide Relocation : Yes, with my wife and her assistance dog.
- Multiple Qualifications, previously approved for USA Speciality Work Visas (H1B).
- Eligible to apply for a USA NAFTA Work Visa (TN), in advance or on day of entry.
- Health Issues : M.E. continuously since 1987, resulting in cyclic relapses of it and its complications. ***I therefore accomplish my greatest achievements; working mostly from a home office, though that has been in many places around the world; and a private company office.*** My greatest creative eureka moments, have been whilst walking on

beaches with my wife and her assistance dog, snorkelling, or, swimming in warm, clean sea, or a pool, or, soaking in a Jacuzzi or hot-spring; day or night!

- Countries Lived & Worked In : United Kingdom, European Union, United States, China.
- Citizenships : Canada, United Kingdom, European Union.
- Co-Inventor / Co-Patentee of a US Patent related to ever-increasing telecommunications speeds.
- 100% Owner & CTO... of Quantum Impenetrable / Qi (Cryptography & Technology R&D).
- 100% Owner of the entire DNA-256 IP.
- Father's Related Influence :
  - Former Radio & Codes Officer in the Navy.
  - Became an international expert in Bubble-Memory as it was first starting to be used.
  - Former Mainframe Computer Manager for Unisys, Sperry, Burroughs.
  - Took me, at age 6 onwards, to see the Mainframe Computers, and taught me how to diagnose and repair their faults.
  - Gave me, access to numerous Mainframe Computer manuals.
  - Gave me, at age 6, a University-Level Philips Electronics Kit.
  - Gave me, various pieces of computer equipment, as they were replaced.
  - Bought me, my first scientific calculator, at a young age.
  - Bought me, my first computer, at a young age.
  - Taught me, Boolean Algebra and Combinational & Sequential Digital Logic.
  - Provided me, with his Technical College course notes.
  - Was always enthusiastic to see my many inventions as a child and adult.
- Key Skills :
  - Cryptography.
  - Cryptanalysis.
  - Cryptology.
  - Data Science.
  - Computer Science.
  - Information Technology.
  - Object-Oriented Analysis (OOA), Design (OOD), Programming (OOP).
  - Research, Architecture, Engineering, Integration, Testing, Analysis, Troubleshooting, of :
    - Pioneering New Technologies.
    - Ciphers & Codes.
    - Countermeasures.
    - Systems.
    - Electrical.
    - Electronics (Digital, Analog, Mixed Signal).
    - Micro Electronics.
    - ASICs.
    - Microprocessors.
    - Microcontrollers.
    - Programmable Logic.
    - Schematics & Printed Circuit Boards (PCBs).

    - Computing Systems, Devices & Components.
    - Automated Test Equipment (ATE).
    - Automated Diagnostics Equipment.
    - Automatic Calibration Equipment.
    - Hardware.
    - Firmware.
    - Software.
    - Real-Time.
    - Embedded.
    - Telecommunications.
    - Telemetry.
    - Infrastructures.
    - Virtual Private Networks.
    - Electronic Security.
    - Mechanical Security.
    - Cyber Security.
    - Robotics.
    - Machines.
    - Avionics.
    - Mechatronics.
    - Meditronics.
    - Automation.
    - Protocols.
    - Mathematics.
    - Algorithms.
    - Machining.
    - Audio & Video.
    - Financial.
    - Administrative.
    - Scheduling.
    - Satellite Tracking.
    - Databases Shared In Real-Time.
    - Data Processing.
  - Teaching at College & University Level :
    - Mathematics.
    - Electronics.
    - Computing.
    - Software Development.
    - PCB Design & Production.
    - English Literature & Language (TEFL).
    - Project Management.
    - E-Commerce.
    - Business.
  - Microsoft Windows (all versions).
  - Microsoft Visual Studio.

  - Microsoft Visual C / C++.
  - Microsoft Visio.
  - Microsoft Office.
  - Microchip MPLAB...
  - OrCAD.
  - DesignSpark PCB.
  - ASIC Development Systems (from various vendors).
  - Soldering...
  - Oscilloscopes...
  - In-Circuit-Emulators...
- Previously, Designed & Implemented Bespoke / Proprietary Systems For :
  - Government.
  - UK National CCTV Network - The self-healing TVNP CCTV Network Software.
  - British Aerospace - contracted to customer.
  - GKN - contracted to customer.
  - TeleNetwork V2D - Achieving ever-increasing telecommunications speeds.
  - Ras Lanuf Oil Terminal - Design of a replacement SCADA system for their Tank Farm...
  - Imperial War Museum - Systems for automated exhibits.
  - KAUST - Design review of the Campus' Integrated Security, Automation & Communications System.
  - Computer Futures - various contracts.
  - Airbus A330, A340, etc - Automated Landing Gear, Fuel Systems & Avionics V&V.
  - GE Locomotive - GELFTE (Automated Test / Diagnostics / Calibration Equipment miniaturized from a 19" Rack Cabinet, to an In-The-Field Ruggedized-Briefcase).
  - Grampian Regional Council - Technology Design & Maintenance.
  - Highland Regional Council - Technology Design & Maintenance.
  - Mearns Academy - Equipment Design & Maintenance and Dept / Team Management.
  - ADT - Security & Electronics.
  - Hong Kong Airport - Integrated CCTV, Security, Control, Automation & Communications.
  - Virgin Media - Multiple Data Center - HVAC Energy Saving, Energy Management Systems (EMS), and Server - Temperature Mapping & Automatic-Regulation...
  - Midland Metro - Integrated CCTV, Security, Control, Automation & Communications.
  - London Underground - Integrated CCTV Network.
  - Cameron Health (now part of Boston Scientific) - Implantable Cardio Defibrillator (ICD).
  - GEC Plessey Telecommunications (GPT) - Integrated CCTV, Security, Control, Automation & Communications.
  - Marconi - Integrated CCTV, Security, Control, Automation & Communications.
  - Lucas Aerospace - ATE for Locomotive Engine & Engine Management Systems.
  - DispenseSource / Nexiant (now MarginPoint) - Automated-Restocking ID-Access-Controlled Vending Machines & Vaults, and their bespoke Computers - Mother

Boards & Communications Boards... Included special control panels with TFT display...

- Smart-Key Security Systems - RFID / NFC Vehicle Immobilization Systems.
- Infinitronix - TVNP for National CCTV Network, and other Bespoke Systems.
- Mansion Control - Bespoke : SCADA, Building Management Systems (BMS), Energy Management Systems (EMS), Security Systems, Automation Systems; Mesh Networking IP that Automatically Builds a Self-Healing Multi-Node Virtual Private Network (VPN) for Linking IOT, Devices, Sensors...
- Hasalarm Security Electronics - Bespoke Systems.
- Haslam Software & Hardware Consultancy - Bespoke Systems.
- LC Automation - Bespoke Robotics, Machines & Safety Systems.
- Nordson - Bespoke Robotics.
- DAGE - Bespoke Robotics.
- Nohau - In-Circuit Emulators.
- Sumita Electronics - Computer Systems.
- Sumita Business Machines - Computer Systems.
- Many others who wish to remain confidential.

- Previously, Provided Technology Forensics & Expert Witness Reports To :
  - UK Police - Fraud Squad.
  - HM Crown Prosecution Service (CPS).
- Previously, Taught At :
  - Quanzhou Normal University (QNU) - Fujian Province, China, opposite Taiwan.
  - Information Technology Education Centre (ITEC) - Inverness, Scotland.
  - Highland Regional Council - Inverness, Scotland.
  - Private Tuition.