Curriculum Vitae & Resume
Garth Wayne Haslam

IP-Owner / Inventor / Architect of the World's Only ~ Algorithm and ASIC / Chip for Impenetrable and Unbreakable Post-Quantum End-to-End Encryption (E2EE) ~ Quantum Cryptography & Quantum / True Random-Number-Generator Combination

Updated - 2017-09-05

Location: Nr. Liverpool, England, UK Will Consider Relocation Worldwide

LinkedIn: https://uk.linkedin.com/pub/garth-wayne-haslam/90/607/ab1

Cover Note

Garth-Wayne is willing to take on additional assignments, for external project-contracts / positions worldwide, to build-up funding to further his own internal venture described below. He will consider external project-contracts / positions involving the type of experiences discussed throughout this CV, especially Quantum related, but also for ground-breaking, state-of-the-art product R&D. Both temporary and permanent can be considered. Please connect and contact him, initially via LinkedIn.

Present Focus

Garth-Wayne, a former Silicon Valley Innovator with more than 33-years of international technology expertise; is the Inventor / Architect of DNA-256 Encryption (inspired by genetics), encapsulated with a Quantum / True Random-Number-Generator into an ASIC / chip, now available globally to OEMs, governments, organizations, and individuals, as a range of Impenetrable and Unbreakable Post-Quantum End-to-End Encryption (E2EE) products.

AES-256 and other previously trusted encryption algorithms, have vulnerabilities as confirmed by the NSA, NIST and ETSI, especially when faced with a suitably configured Quantum Computer (and yes they do exist).

DNA-256 solves these vulnerabilities in an impenetrable future-proofed way, and has absolutely no back-doors or mathematical weaknesses, proven by years of analysis. 256-bit keys, are intelligently generated, by a unique Quantum-Randomized Fusion of the entire information.

Each time encryption is performed, even on the same data / information, the newly generated key will differ vastly from any previous key, also 50% of the bits in the encryption, will be 0|1, differ from any previous encryption (Cipher-Text) and the original data (Plain-Text), thus achieving non-compressible maximum entropy, looking just like truly-random files!

These and other unique features, make the encryption impenetrable and unbreakable by eavesdroppers, hackers, and cryptanalysis techniques, even using Super / Quantum Computers.

A self-contained device, based on the IC, can encrypt and decrypt data of ANY format on a USB memory-stick plugged into it. A USB Command and Control Interface has been provided, to make it easy to interface the chips / devices with supervisory computers and software systems, for automated processing.

Chips, USB Devices, and Din-Rail / Rack-Mount Units, can be ordered, for Impenetrable Data Storage / Communications, for QKD, VPN, Cloud, Computers, Smartphones, Vehicles, Aircraft, IoT, SCADA, Satellites... Any Escrow scenario can be added. Enquiries are welcome.

Work & Education History

2005 – Present: Freelance Consultant, Systems Architect & Analyst, Contractor.

Required relocation around the United Kingdom & Europe.

- MANSION CONTROL (and an in-stealth-mode start-up company awaiting funding) – Research, Brainstorming, Mathematics, Cryptography, Cryptanalysis, Simulation, and Modelling, in C / C++ for architectural exploration and performance optimization. R&D of a unique cryptographic primitive with quantum-like properties, inspired by genetics, and based on it – an encryption-algorithm / streaming-bit-processing-pipeline, named DNA-256.

  It has no back-doors or mathematical weaknesses / shortcuts, and completely resists parallel computing attack techniques, so is exponentially stronger than present algorithms (like AES-256 etc), and will withstand cryptanalysis and brute-force attacks by any computer, super-computer, or quantum-computer, or network of these, present and future, thus is even better than the Post-Quantum performance hoped for by the NSA, NIST, and ETSI. Assuming that a network of quantum computers knew and understood the enigma of the unique algorithm, and could try a different 256-bit key through the decryption algorithm, every 1-micro-second (1us), or at the rate of 1-million keys per second, then collectively it would take them (at the precise rate of 365.2422 days per year), a mind-boggling 3.6693 e+63 years (nearly, the number 4 followed by 63 zeros, in years), to guarantee a successful brute-force decryption of a single file or zipped folder.

  Each encrypted, file or zipped folder, gets its own unique 256-bit key, so a brute-force attack would have to be re-started afresh, for each. From a practical point of view, this level of performance is considered as, Impenetrable and Unbreakable End-To-End Encryption (E2EE), even exceeding the requirements for Post-Quantum / Quantum-Resistant / Quantum-Secure / Quantum-Safe – Encryption.

  DNA-256 has been coded in portable C / C++ for modelling, simulation, and analysis purposes. A Graphical User Interface (GUI), has also been produced, which provides, binary image processing and display, for easy observation

and differential-analysis of bit-patterns and randomness / entropy, during testing, verification and validation.

DNA-256 has future applications in: Quantum Key Distribution (QKD); Software and Hardware Authentication; Licence Verification / Validation; Access Control; Data Shredding; Anti-Counterfeiting; Anti-Tampering; Hard-Disk Encryption; Cyber Security; IoT Security; Data Security; Internet, Intranet, Wireless, RF, IR, Satellite, Cable, and Fibre – Telecommunications Absolute Privacy; Cloud Security; LAN / WAN Network Security; Secure Banking; ID Authentication; Secure Aerospace and Automotive Telemetry; Encryption / Cryptographic Engines or Co-Processors; Encryption Dongles for Smartphones, Netbooks, Laptops, Workstations, Servers...

As the owner / inventor / architect of the intellectual property (IP), Garth-Wayne plans to sell / licence it, but meanwhile continue to produce and add further features to, a range of products based on it; and is currently marketing these to governmental and commercial organizations, through his 1200+ 1st level LinkedIn contacts network, mostly made up of: experts in Quantum Physics and Data / Network Security, and, organizations and government personnel worldwide, requiring impenetrable solutions.

- MANSION CONTROL – R&D of an integrated self-healing mesh-networked Building Automation, Energy Management, Security and SCADA System (BMS / BEMS), for a number of confidential clients.

- MANSION CONTROL – R&D, build, installation, and maintenance, of computer systems, public address systems (PA), sound and music systems, home and building automation, and security systems, for a number of confidential clients.

- INFINITRONIX – R&D of a C / C++ software suite for a mesh-networked Data Center Energy Management & Monitoring System (EMS), for a number of confidential clients.

- INFINITRONIX – R&D of a C / C++ software suite to mesh-network all assigned: government, borough council, stadium, shopping centre, underground, airport, road and rail transportation links, public buildings, and street – full-feature camera resources, around the entire city of London, for a number of confidential clients.

  The solution implemented the TeleVision Network Protocol (TVNP3), to create a city-wide Command, Control, Communications, Computing, and Intelligence (C3i / C4i) system. The distributed C4i solution, already has capacity to handle 65535 control-room sites, each site managing up to 65535 cameras, so in total, more than 4-billion cameras – so obviously capable of covering an entire country, if required.

  Each camera's resources can be individually monitored and controlled, and includes: pan, tilt, zoom, focus, iris, visible-illumination, infrared-illumination, siren, speaker, wiper, washer, heater, auxiliary sensor / device inputs and

outputs, etc. Implementation and testing required modelling and simulation on a large scale, in C / C++, to perfect the intelligent algorithms for: audio and video switching / routing, via chains of matrixes and trunk-lines, to government and intelligence agency monitors and recorders, across control rooms around the city; and control routing, network building, and network self-healing...

- AIRBUS (AN EADS GROUP COMPANY) – R&D of a multitude of C / C++ applications, modules, libraries, and routines, for the modelling, simulation, and analysis, of existing and proposed avionics and aerospace functionalities, most being integrated into the permanent continuous-testing, test rigs for the AIRBUS range of aircraft, eg. A330, A340, A350, A380...

- SUN MICROSYSTEMS (NOW PART OF ORACLE) – R&D of a multitude of C / C++ applications, modules, libraries, and routines, for the analysis of existing and proposed Solaris operating system functionalities.

- KAUST (Saudi Arabian University) – Remote review of all technical documents for the proposed, integrated campus-wide automation, communications, and security system (ICAS).

2004 – 2005: Professor & Foreign Expert. 2-Year Assignment.

Required relocation to Quanzhou, Fujian Province, P. R. China.

- TAFE NSW SOUTH WESTERN SYDNEY INSTITUTE BRANCH AT QNU-CHINA – Preparation and delivery of Bachelor's degree courses. Supervision and assessment of examinations. Student guidance and counselling.

1999 – 2003: Technical Specialist – Authorized by the United States Government.

Required relocation to Silicon Valley & Orange County, California.

- CAMERON HEALTH (STARTUP – NOW PART OF BOSTON SCIENTIFIC) – Reported directly to the EVP of Research & Development. R&D of a multitude of C / C++ applications, modules, libraries, and routines, for the modelling, simulation, and analysis of existing and proposed, algorithms for identifying heart arrhythmias, calculating heart therapies, antenna designs, bespoke wireless communications protocols, FPGA and CPLD and System-on-Chip (SoC) and ASIC logic. The handheld controller for the ICD, was based on an Intel StrongARM SA-1110 processor (ARM V4 with coprocessor 15 architectural enhancements). Boston Scientific bought the company and its IP for a deal worth USD $1.3-billion.

- DISPENSESOURCE (STARTUP – NOW PART OF MARGINPOINT) – Reported directly to the EVP of Research & Development. Setup the company's electronics assembly and SMT rework lab. R&D of a Motherboard and Power Supply & Communications board, based on an Intel StrongARM SA-1110 processor (ARM V4 with coprocessor 15 architectural enhancements), and its companion GPIO, communications, and graphics display coprocessor, the Intel SA-1111. Surface-mount PCB circuit schematics, component positioning,

multi-layer route planning, supervision, and final edits. PCB assembly planning and supervision and inspection. Board bring-up using an ICE, and developing TCL-like test scripts to drive the ICE, and test board components. R&D of Assembly Language and C / C++ drivers for the boards and external peripherals. Required bespoke CPLD logic design to memory-map a multitude of on-board chips and tune signal timings. Ports included, multiple UART based RS-485 and RS-422 and RS-232, TFT color display, TFT backlight, TFT touch-screen, stereo audio, mouse, keyboard, Wiegand, Ethernet... The company achieved Deloitte's Orange County Technology Fast 50 ranking of Fastest-Growing Companies.

- TELENETWORK V2D (STARTUP) – Reported directly to the company's founder and President. Setup the company's electronics assembly and SMT rework lab. R&D of a multitude of C / C++ applications, modules, libraries, and routines, for the modelling, simulation, and analysis of proposed ground-breaking telecommunications speed enhancement technologies. R&D of test systems, based on Triscend A7 System-on-Chip (SoC) incorporating an ARM7 (ARM V4 based) processor and an FPGA. Required bespoke FPGA logic design to create communications sub-systems and tune signal timings.

- NOHAU (STARTUP) – Reported directly to the company's founder and President. R&D of In-Circuit-Emulators (ICE) for a number of microprocessor types. Required extensive modifications to existing FPGA and CPLD logic, to affect memory-mappings and signal timings. Garth-Wayne worked closely with a number of semiconductor manufacturers to test and improve flash memory and CAN bus communications.

1999 – 1999: BSCS - Education and Experience Evaluation for the United States Government – Department of Justice (DoJ) H1B Visa.

- Qualifications and experience were collectively evaluated as being greater than the minimum requirement of a Bachelor of Science (BSc) degree in Computer Science (BSCS), by the FOUNDATION FOR INTERNATIONAL SERVICES, a United States Government approved evaluation organization. Subsequent evaluations by an on-line university, have resulted in education and experience being awarded the equivalent of:
  - Master of Science (MSc) in Electronics Eng. & Communications.
  - Doctor of Science (DSc [PhD]) in Computer & Electronics Eng. Technology.

1993 – 1999: Freelance Consultant, Systems Architect & Analyst, Contractor.

- AIRBUS & BAE SYSTEMS & GKN – R&D of a multitude of C / C++ applications, modules, libraries, and routines, for the modelling, simulation, and analysis, of existing and proposed avionics and aerospace functionalities, most being integrated into the permanent continuous-testing, test rigs for the AIRBUS range of aircraft. Highly complex mathematics were developed, to model and simulate such things as, fuel movement, at changing temperatures and aircraft attitudes and wing displacements, and the vectored forces, on structures and mechanical components, during all modes of takeoff, flight, landing, breaking, steering... Certain simulations, were fed into a very large

number of digital and analogue hardware outputs, to drive the inputs of multiple avionics units, to persuade the avionics to behave as though installed on an actual aircraft. Code was also developed to enable the test rigs to command and control and monitor the avionics via their ARINC buses.

- MARCONI COMMUNICATIONS – R&D of a multitude of C / C++ applications, modules, libraries, and routines, for the modelling, simulation, and analysis of proposed: CCTV, Supervisory Control & Data Acquisition (SCADA), Passenger Information Display (PID), Packet-Radio, Signalling, Private Automatic Branch Exchange (PABX), Public Address (PA), Emergency Call-Point, and SDH Backbone, functionalities. These were later integrated, to become the Integrated Communications & Control Systems (ICCS), as drivers, algorithms, and sub-systems, for the Hong Kong Airport & Rail-Link, TFL London Underground Metro & Tube Stations, and the ALCATEL / CENTRO Midland Metro & Stations.

- GEC PLESSEY TELECOMMUNICATIONS (GPT) and STRATEGIC COMMUNICATIONS SYSTEMS – Same as immediately above.

- POLICE FRAUD SQUAD & CROWN PROSECUTION SERVICE – Micro-processor based technology, investigations, forensics, and expert witness reports.

- VARITY LUCAS AEROSPACE (NOW ROLLS-ROYCE) – R&D of C / C++ and electronics / computing systems and sub-systems, to condense a 19” rack-based locomotive test rig, into a robust, highly-portable unit / equipment, automated test equipment (ATE), able to be transported quickly by aircraft to an emergency locomotive-breakdown anywhere in the US; for in-the-field calibration / tuning and fault-diagnostics, of the multiple engines, and their EMUs & ECUs, harnesses, controls and communications.

- VEBA OIL OPERATIONS (RAS LANUF) & AMEC – Remote assistance in the design of a multi-PC replacement, of an old main-frame computer based SCADA system, for tank-farm control and monitoring at the oil terminal.

- WALLACE R&D – R&D of Assembly Language and electronics / micro-computing systems, to provide automotive manufacturers with RFID / NFC based, vehicle security and immobilization systems. Required extensive simulation to perfect the Manchester-Code (bi-phase-level) based communications protocols, used for wireless RFID and fibre-optic links.

- SMARTKEY SECURITY SYSTEMS – Same as immediately above.

- MANSION CONTROL – R&D of a SCADA system. Demos for funding.

1990 – 1993: Manager of Department of Technicians.

- MEARNS ACADEMY & ABERDEENSHIRE COUNCIL (LOCAL GOVERNMENT) – Assigned to look after and grow a team of technicians covering all departments within an academy. An especially enjoyable task that Garth-Wayne handled autonomously, was the building of a NOAA & Meteosat

weather satellite receiver, and then writing software in BASIC, to simultaneously simulate the orbits of multiple satellites, to predict the exact time and position on the horizon, that each satellite would appear, so as to provide a printed schedule of predictions. These predictions proved to be completely accurate in practice, and could have been used for automatic antenna-guidance (satellite tracking) if funds had permitted.

1985 – 1989: Freelance Consultant, Systems Architect & Analyst, Contractor.

- INVERNESS ITEC – Preparation and delivery of City & Guilds courses. Supervision and assessment of examinations and in-house R&D for external clients such as the IMPERIAL WAR MUSEUM...

- HIGHLAND REGIONAL COUNCIL (LOCAL GOVERNMENT) – R&D of bespoke solutions, and maintenance, of equipment used in education, health-care, and admin...

- HASALARM SECURITY ELECTRONICS – R&D of bespoke solutions, build, installation, and maintenance, of computer systems, control and monitoring systems (SCADA), electrical systems, health-care equipment, public address systems (PA), sound and music systems, home and building automation, and security systems.

1984 – 1985: Industrial Systems Research & Development Engineer.

- LC AUTOMATION – R&D of industrial safety, control, automation, and SCADA systems. Required electrical and electronics design, and; modelling, simulation, and analysis, in Assembly Language, BASIC, PL / M, and C; which later became part of a range of products. An optics laboratory was setup, and Garth-Wayne created graphics drivers for the electro-optic parts. He was an early pioneer of Programmable Array Logic (PAL), the predecessor of CPLD and FPGA chips. Built Register-Transfer-Level (RTL) verification models in BASIC and C code. He worked closely with the US semiconductor manufacturers of PAL chips and laser diodes and charge-coupled-device (CCD) 'camera' chips, to test and improve them. On day one, he solved a problem that had been costing the company dearly, for some years due to no solution having worked. Products ranged from a six-color-process (black, cyan, magenta, yellow, orange, and green) plastic-film printing press, carpet weaving machine, IR-beam safety guards, robotics, SCADA, industrial machine control systems, positioning systems, motor and driver protection systems, servos...

1982 – 1984: College & Polytechnic / University Education.

- WR TUSON COLLEGE (NOW PRESTON'S COLLEGE) – BTEC National Diploma in Electrical & Electronics Engineering (Dip. EEE). Achieved 4 distinctions in Mathematics (100%) & Micro-Electronics.
- PRESTON POLYTECHNIC (NOW UNIVERITY OF CENTRAL LANCASHIRE).

1981 – 1984: Computer Systems & Software Sales Assistant.

- SUMITA ELECTRONICS and SUMITA BUSINESS MACHINES – During weekends and holidays from high school and college, Garth-Wayne helped a computer and software supplier with sales at their shop-fronted store. He also designed and built equipment, to allow the immediate selection of games and software packages on EPROMs, for quick-change demos.

Operating Systems Experience

- Windows 10 (64-bit & 32-bit), 8.1, 8, 7, CE (on ARM), XP, NT, 98, 95, 3.11...
- VenturCom / IntervalZero RTX Hard RTOS for Windows.
- WindRiver VxWorks RTOS.
- MS-DOS all versions (added his own real-time extension for multitasking).
- Solaris UNIX (twice briefly).
- Centos Linux (briefly).
- Also Bare-Metal Coding where no OS was used.

Telecommunications & Bus Protocols Experience

- Ethernet, IP, TCP, UDP...
- UART, RS232, RS422, RS485...
- Modbus, CAN...
- USB Host, Device, OTG...
- HDLC, SDLC.
- ATM, Frame Relay...
- Arinc...
- I2C, SPI...
- Numerous proprietary protocols at all stack levels.

Additional Information

- Nationality: British (EU) & Canadian (North America).
- Able to live and work in the US, upon renewal of H-1B, else a new TN visa.
- United States patentee.
- Yourdon Object Oriented – software and systems design methodology.
- Extensive C / C++ programming experience, in solving especially complex problems in numerous industries, has concentrated on using C / C++ in a way that more closely translates, to efficient and more practical Assembly Language or Logic, as much of the simulation, modelling, and analysis code, has found its way into the end product too, and so, had to be as efficient in both size and speed, as possible. Frequently uses structures for efficiency, classes and multi-threading when necessary, and tend to avoid the more academically-interesting features in favour of more practical, efficient, and easily verifiable code.
- Some experience with editing VHDL and Verilog code, and Register-Transfer-Level (RTL) verification.
- Proficient in MS Visual Studio, Visual C++, Visio, Office, Word, Excel, PowerPoint...
- Many projects have required the R&D of software or hardware signal conditioning, to filter and process inputs, or generate special signal outputs.

- Good organizational, project planning, documentation, reporting, communications, and accounting skills.
- Able to handle tasks autonomously or in a team, according to how each task will be more efficiently performed.
- Electronics, drawing, machining, metalwork, woodwork, and chemistry, started as hobbies from the age of 6.
- Mathematics, trigonometry and geometry, computing and software, started as hobbies from the age of 11, though frequently helped his dad from the age of 6, with a variety of tasks on mainframe banking computers that his dad was responsible for installing, maintaining, and improving.
- Comfortable translating between, and using both, fixed-point (integer that is scaled by a specific factor determined by the type / range) and floating-point (sign bit, the exponent field, and the significand or mantissa) arithmetic, as used in microcontrollers, microprocessors, and computing.
- Particularly good at solving complex mathematical and logic puzzles, hence his professional interest in cryptography, cryptanalysis, and image processing.
- Qualifications and evaluations, work examples and many written references, are all available to be viewed and discussed during interviews.