



The 10th Anniversary of two related events;

- **The launch of the Advanced Encryption Standard**
- **Helion Technology unveils its first silicon IP**

On the 26th November 2001, a new standard for commercial encryption was ratified by the National Institute of Standards and Technology in the US. At that time, the “Advanced Encryption Standard” (AES) was only something that those with a particular interest in data security would have known or cared about. Ten years down the line, and AES is something even the man in the street is aware of. Our everyday WiFi connections proudly state that they are secured by AES, and our online banking systems boast AES 256-bit security. The world has changed a great deal over those ten years, and in hindsight AES turned out to be a very timely standard.

In parallel, Helion Technology Limited - now a leading provider of encryption and lossless data compression IP - was in the process of launching the world’s first AES core for use in FPGA and ASIC. Back then Helion had been a design house for nine years, and this was its initial foray into the world of intellectual property licensing.

Being ahead of the curve was exciting for Helion, but perhaps a little ahead of the market. It was only a year or two later, when major standards like 802.11 WLAN (later WiFi) adopted AES for its security, that the decision to develop and license crypto IP proved to have been the right one. Two years in, Helion was still one of the few companies able to offer a comprehensive AES solution, and was therefore well placed to accelerate its IP business on the back of emerging standards. Today Helion is a pure IP licensing company offering a broad portfolio of cores that enable its customers to add security and lossless compression to their chip designs. AES is still a major part of its business however, with a wide range of application specific solutions on offer, covering the diverse range of applications now routinely using data security.

So what of AES ten years down the line? It is clearly very widely deployed, but is it still the best option? And what about Helion Technology as a company? Has it been able to keep pace with its customer’s requirements and build a solid business from licensing its intellectual property?

In other parts of the tech world, ten years is a huge timespan. Over that period, we’ve seen leading edge chip geometries shrink from 130nm to 28nm, and transistor counts in our PC processors rise by almost a factor of 30x. However the ten year old AES standard is still the encryption algorithm of choice, considered to be sufficiently secure and with nothing anticipated in the pipeline to replace it. Before being ratified in 2001 it had been selected from a field of fifteen contenders, via an extremely rigorous five year process of competitive analysis and peer review, to ensure that the chosen algorithm was appropriate and would have a long lifespan. Its predecessor, the Data Encryption Standard (DES) was used for thirty years in various forms before it was in need of replacement, and the intent was similar for AES.

So what determines the lifespan of an encryption algorithm? The strength of any encryption is said to diminish over the years, as available computational power continually increases, thus making brute-force attacks faster and therefore more practical. If an algorithm is cracked, then clearly it can become obsolete overnight, but assuming this doesn’t happen, then an unstoppable erosion process based on Moore’s Law is what ages a particular encryption scheme. NIST suggest that AES, even with its shorter 128-bit key option, will be secure for at least another twenty years – and longer for the 256-bit key version. There are differing opinions in the industry as to exactly how long this will be, but the end is not thought to be in sight for a while yet. Not many major tech standards can

claim a multi-decade lifespan, but then having to update your encryption is not something you want to be doing on a frequent basis – especially on legacy equipment out in the field - due to the sheer size of the task!

Where encryption used to be the preserve of military and government users, it is now a part of our daily digital life. It is used routinely to secure transactions over the internet, to keep our stored data safe from unauthorised access, and to protect our wireless communications – now all everyday tasks. Commercial applications have solidly embraced encryption since AES, so Helion have worked tirelessly to put together appropriate solutions to address the challenges faced by its customers – military, government and commercial. As well as offering the first AES encryption engines, Helion has been first to market with customised solutions for use in the various wireless standards (e.g. AES-CCM for WiFi and WiMax), specific solutions optimised for securing data stored on tape or disk (e.g. AES-XTS), as well as special low area/power solutions for lower-rate applications, and cores offering many gigabits per second of throughput, for high rate networking (e.g. AES-GCM).

This ability to supply the right solutions, alongside an early realisation that the customer experience is of paramount importance in an IP business, has enabled Helion to work with some of the world's top companies on many exciting projects. One particularly proud moment was when a Helion core was chosen to take part in an experiment on board the International Space Station! In the military sector, Helion currently supply crypto IP to nine of the top ten prime contractors (by revenue) in the world. Helion also work with numerous companies supplying government security equipment in the UK, US and EU. From simple beginnings, ten years of hard work by Helion has enabled a very extensive customer base to be built, placing its future on very solid foundations.

Helion also bring something extra special to the table, brought over from its days as a design services provider. Back then it seemed that FPGAs were never quite fast enough, or never quite large enough for the most advanced applications being implemented at the time. Helion became expert at extracting the most out of FPGA technology, by careful low level design, and optimising separately for each type of FPGA target, plus various proprietary design techniques developed over many years. This philosophy is firmly in the DNA of Helion today, and even though FPGA technology has moved forwards hugely over recent years, the advantages of having a solution designed specifically for the target – and not relying purely on synthesis - is still very clear. When applied to both ASIC and FPGA designs, it means that Helion IP is usually the fastest and/or smallest solution using the lowest amount of power, by some margin - all important requirements for today's applications. This approach has earned critical acclaim from both customers and strategic partners, and is demonstrated admirably by Helion being an accredited IP partner with Actel and Lattice; and one of only four "Premier" level partners chosen by Xilinx, and the only security IP provider to have achieved this highest level of membership.

What about the future? Well for now AES is still very much the encryption algorithm of choice for any new commercial applications where strong and dependable security is required. Applications are continually demanding more speed or lower power – and sometimes both – hence a challenge always remains for companies like Helion to keep pace with what its customers are looking for. For the foreseeable future at least, if a commercial product says it is secured by AES, then you can be certain that it is employing the best current encryption algorithm for the job.

Copyright © Helion Technology Limited 2011

<http://www.heliontech.com>

Disclaimer. This publication is provided "as is" without warranty of any kind either expressed or implied. Helion Technology Limited believes that the information published in this document is true and accurate, but assumes no responsibility for errors or omissions. Helion Technology Limited shall not be liable in the event of incidental or consequential damages arising from the use of information supplied in this publication.