ॐ भूर्भुवस्व तत् सवितूर्वरेण्यम् भर्गो देवस्य धीमहि धियो यो न प्रचोदयात्

VEST

A multi-purpose cryptographic primitive with integrated family keying support providing encryption, keyed message authentication and collision resistant hashing, targeted to semi-conductor applications

A Presentation on VEST Hardware Performance, Chip Area Measurements, Power Consumption Estimates

and

Benchmarking in relation to AES, SHA-256 and SHA-512

Benjamin Gittins, Howard Landman, Sean O'Neil, Ron Kelson

14th November 2005

Introduction

The ECRYPT/eSTREAM organisers have required all submissions to be benchmarked against the Advanced Encryption Standard (AES) and where applicable, a secure trusted authentication mechanism. The goal is stated to be to identify those eSTREAM submissions that offer an advance over AES efficiency in any one or more benchmark dimensions.

In this paper, we respond to the eSTREAM requirement and offer a wide-sweeping multi-dimensional analysis and comparison between VEST and the hardware implementations of the AES, AES-HMAC and SHA-2 primitives.

This analysis clearly establishes VEST superiority over the AES, HMAC and SHA-2 primitives generally while direct comparisons between VEST and several of the best AES HMAC and SHA-2 implementations illustrates VEST superiority measuring in the hundreds of percent on several design dimensions or axis.

Table of Contents

In Part One of this document we present some explanatory background discussion on VEST design and how we have approached the task of benchmarking VEST variants in relation to AES and SHA-2. Many of the issues we touch upon are well understood by semi-conductor design and synthesis engineers, but since the greater proportion of the readers are cryptographers skilled in software design, we consider it necessary and helpful to discuss these issues. One such issue is the constraints imposed on a cipher implementation by power-budgets and thermal issues.

In Part Two we tabulate various FPGA figures to assist in the independent assessment of the performance, power consumption and area efficiency of the VEST ciphers in each of its three modes of operation, namely stream cipher, authenticated encryption (MAC) *and* collision resistant [keyed and un-keyed] hashing modes. For FPGA comparison purposes, we have compiled data on forty-eight (48) AES and SHA-2 FPGA implementations. For power consumption comparison purposes we were obliged to perform explorative FPGA power analysis on sixteen (16) of the FPGA cipher instances.

In Part Three we tabulate performance figures to assist in ASIC benchmarking. For ASIC comparison purposes, we have compiled data on forty-three (43) AES and SHA-2 ASIC implementations. Exact figures are not available for some of the aspects of the VEST implementations in ASIC, and although we anticipate excellent performance scaling when VEST is targeted to ASIC geometries, we prefer to adopt a conservative approach in this document until concrete figures can be presented.

In Part Four we briefly discuss the latest developments in VEST ciphers software performance in relation to AES.

In Part Five we acknowledge the work of Tim Good, Mohammed Benaissa [33] who claim to implement the smallest and fastest known FPGA AES implementations. We offer comparisons between these two implementations and other relevant AES implementations in relation to VEST.

In Part Six we offer comparisons of the fastest and register-only SHA-2 implementations with VEST-8 and VEST-32.

In Part Seven we perform a review of specific hardware applications for VEST ciphers.

In Part Eight we offer our final conclusions and references.

In Appendix A we provide technical material concerning FPGA analysis.

In Appendix B we provide technical material concerning ASIC analysis.

Front Matter

This document represents a significant body of research based upon an extensive survey of academic and commercially published cipher implementations. Large segments of the information in this document have been compiled from a diverse selection of public sources. We have included in the body of the document and in the appendices a significant amount of detail describing how our results were obtained. Although our main purpose has been to provide a comparison with VEST, we have been careful to tabulate all the comparative data on the AES and SHA implementations separately to compose a derivative base-line survey paper. We are unaware of any survey of AES and SHA implementations approaching this level of detail. Although the focus of this original document is to compare VEST with AES and SHA, this comparative survey does not extend to compare every feature of these primitives. For example, some AES implementations like the Helion Tech ciphers include support circuitry for several modes of operation whereas many other implementations do not. We have not surveyed additional features or functionality. Comparison between VEST and the smallest and the fastest AES and SHA FPGA implementations can be found in Part Five of this document.

Preparation of this document has not been a straightforward task. Most publications do not provide technical data on all the important dimensions of hardware implementations. Estimating, measuring or calculating the missing data has entailed a great deal of effort and time. When inevitably faced with incomplete information for many of the leading AES and SHA implementations, we are forced to extrapolate some aspects of this survey, which inevitably introduced a potential small degree of error. Electronic correspondence with some cipher authors surveyed in this paper has resulted in additional statistics not previously published, which has improved the quality of some of our original estimations.

The information in this document represents our current best effort and we welcome and encourage any feedback concerning errors, omissions or other relevant information that may assist in clarifying or enhancing accurate performance comparison. Overall, this document represents several months of intense work and we acknowledge the wider support of our team in Synaptic's and CB Capital Management SA. We hope that the extent and thoroughness of the AES HMAC and SHA survey demonstrates our collective commitment to promoting and advancing the ECRYPT process.

PART 1
PRELIMINARY

1.1 On benchmarking the eSTREAM hardware cipher primitives

The ECRYPT coordinators have requested that all submissions to the eSTREAM competition offer a minimum-security level of 80-bit, and are benchmarked in relation to the AES. In this paper, we present our comparison of the VEST eSTREAM submission with an extensive selection of the best independent hardware implementations of the AES, AES-HMAC and SHA-2 we could find.

It is important to bear in mind the 80-bit minimum-security level when considering authenticated encryption systems. Many implementations employing AES only offer 64-bit secure hash or MAC, which results in systems that fall well below the 80-bit requirement. By comparison, VEST offers encryption, hash and MAC functionality with security of all modes of operation ranging from 80-bit to 256-bit.

Concerning the selection of the AES as the benchmark cipher, we understand that this decision has not been taken in isolation and that there has been no suggestion from the global cryptographic community that there is a better standard than the AES against which to benchmark the eSTREAM submissions. However, benchmarking hardware implementations against the AES standard is a non-trivial request.

When comparing the many existing implementations with each other and with VEST, it is important to consider what we call the four complimentary dimensions of a cipher design before reaching any conclusions about one cipher's performance in relation to another. These four dimensions are:

1. Robustness and security margins engineered into a design
2. The logic and RAM resource utilisation
3. Power consumption
4. Overall performance claims

We consider this multi-dimensional analysis essential because often hardware cipher designers sacrifice efficiency in one or more dimensions to win efficiency in the other/s. The most common fault in new hardware cipher designs is sacrifice of robustness and inbuilt conservative margins to win that exceptional circuit area or power efficiency.

A cursory exploration of the robustness or security margins of such designs soon introduces serious uncertainty as to the confidence level that can be attributed to the security rating. Breaks quickly follow. Sometimes the authors recognise and acknowledge the reduction in security in their design, subsequently lowering their security claims or offering a chain of incremental repairs, but all too often the end-result is the same. Sacrificing robustness and traditional conservative margins can never be a reasonable trade-off for suspiciously high efficiency in other dimensions. The question of **sufficient** security margins was subject of much discussion during the entire NIST AES selection process, with Rijndael (the AES finalist), having the smallest [51] security margin of all the NIST round-2 candidates, with prominent cryptographers such as Lars Knudsen arguing [52] for a safety factor of at **least two** (2.0). At time of publishing, the best attack on the 10-round 128-bit secure AES [59] is seven (7) rounds, giving a security factor of approximately 1.4. Another example of this type of a cipher outside the eSTREAM is the Japanese cipher VSC whose exceptional hardware performance was obtained at the expense of its security [69], [70].

Regardless of the security margins that exist, these can be readily compromised in certain high-risk (low-area, low-speed) hardware implementations by not implementing protective methods that may be required to protect certain cipher designs against devastating side-channel [53] attacks. The paper [53] describes a side-channel attack that can determine an entire 128-bit AES key in as little as 40 measurements!

The level of cryptographic work performed to maintain a security level correlates strongly with power consumption. Ciphers that exhibit exceptionally low power characteristics per bit of ciphertext output may be achieving this without sufficient consideration of security implications. Another method of achieving attractive performance figures is by placing unrealistic burdens on hardware resources. Such burdens are frequently ignored and unaddressed in cipher designs or implementations. Frequently the bandwidth performance of the fastest ciphers require power consumption and circuit area demands that are prohibitive, thus also severely limiting the range of possible real-world cipher applications.

It is one of the objectives of ECRYPT / eSTREAM to identify new designs that deliver security with efficiency across all dimensions of the design.

We suggest the following as necessary elements in a reasonable benchmarking that will clarify relative efficiency across all dimensions for Category II eSTREAM submissions.

1.1.a) Designs must be professionally implemented on a broad range of different hardware. This achieves tighter bounds when comparing implementations on equivalent platforms to demonstrate their suitability when mapped to a wide range of platforms.

1.1.b) Designs must outline active and side-channel attacks that appear to be most relevant to a cipher implementation. Designs must include preliminary information on what steps must be taken to thwart such attacks and how this will affect circuit area, power consumption and static timing.

1.1.c) FPGA implementations must include detailed information concerning Logic usage, Register usage, SRAM module usage, Total SRAM usage in Kilobits and static timing. Detailed metrics significantly aid independent analysis, reducing opportunity for error.

1.1.d) FPGA implementations must include extensive information concerning power consumption issues such as power consumed per MHz (pW-S), power consumed to achieve maximum clock speed, total theoretical MHz/Bandwidth achievable at 85°C junction temperature. For FPGA designs, the thermal characteristics, power budget, chip-family and chip-grade should be normalised against one of the many architectures found in our survey.

1.1.e) ASIC implementations should include reliable area measurements using an ASIC VLSI CAD tool. The Free (GPL) Alliance VLSI CAD system [39] accepts VHDL and can perform synthesis and routing on small sub-4K ASIC gate segments of a design.

1.1.f) Accurate static-timing and power-consumption figures for ASIC designs for all Category II submissions will probably require co-ordination through the eSTREAM process as, based on our preliminary investigations, it appears that the professional ASIC tools are rather expensive to license.

1.1.g) In our opinion it is not enough for the authors of a submission to simply claim a certain level of security for their design and then to select from the spectrum of AES implementations the one with the same security rating as their benchmark implementation. If a submission claims an equal security rating to a particular AES benchmark (e.g., 128-bit), then it is reasonable for the readers to expect the submission authors to present their case for how and to what level the robustness and conservative elements have been built into their design. Such information is necessary to assist the readers to more readily accept at the face value the security rating claimed by the author/s, which leads to acceptance of the comparison results derived from that particular AES benchmark implementation selected by the submission authors.

We endeavour to address all the above points in this paper.

We hope that our AES, HMAC and SHA-2 survey and the multi-dimensional benchmarking in this document will assist other Category II submissions in achieving similar levels of detail to support both their own claims and also the external analysis of their submissions.

1.2 The number and range of benchmarks provided

This paper compiles the circuit area, static-timing and performance figures of sixty-eight (68) AES, fifteen (15) SHA-256, six (6) SHA-512 and two (2) DES implementations on FPGA or ASIC for comparison with 5 implementations of each of the four root families of VEST ciphers on Xilinx and Altera platforms that are most commonly found in the AES and SHA FPGA implementation publications.

In selecting the benchmark ciphers and hash functions we have chosen the ninety one (91) best performing hardware implementations from an extensive search of well over one hundred and fifty (150) implementations. We are not aware of any better performing or more efficient hardware implementations of the AES, DES or SHA-256 than those selected as benchmarks in this survey.

The publications for these implementations are most often incomplete, lacking important details such as register usage and/or power consumption figures. We have measured the power requirements of fourteen (14) AES and two (2) SHA implementations on Xilinx platforms by the power estimation tools. The process is discussed in more detail in section 1.4.

The breadth and variety of statistics compiled in this survey enable VEST implementations to be selectively compared with other ciphers in a meaningful way. In many cases, extremely accurate hardware comparisons can be made concerning area, power usage and performance in relation to a particular cipher implementation.

1.3 On benchmarking encryption

For the purposes of responding to the eSTREAM request to compare our Category II submission VEST in relation to the AES in counter mode, we have used the points listed in 1.1.a through 1.1.e and 1.1.g as a guide. Issues concerning ASIC static timing and power remain unresolved.

Our selection of AES and SHA implementations covers a broad range of design variations including:

- Low area, low bandwidth designs, and
- High area, high bandwidth designs

- Iterated architectures (frequent feedback), and
- Fully unrolled pipelined architectures (zero feedback)

- Designs where part of the logic is executed using precomputed SRAM operations, and
- Designs where no precomputed tables of SRAM are used

- Designs with precomputed key/round material, and
- Designs with runtime generation of key/round material with the data to be encoded

- Designs supporting dynamic selection of variable key sizes, and
- Designs supporting a singular fixed key size

- Designs supporting generic block-cipher encryption / decryption, and
- Designs supporting full-duplex encryption and decryption paths

- Designs supporting only ECB / CTR modes of operation
- A wide range of target hardware chipsets and architectures
- A broad range of power consumption objectives

The alternatives listed above imply fundamentally different design objectives, and the resulting perfectly legitimate variations between designs make fair comparison a difficult task.

Assessing the general or specific suitability of a cipher implementation requires a combination of extensive cryptographic and hardware design expertise and application of the domain-specific knowledge, which is generally beyond capability of a single expert, most likely requiring independent evaluations by expert teams.

1.4 On static timing and power requirements

We have taken particular care in ensuring availability of VEST preliminary static-timing results the four root families of VEST ciphers on the Xilinx platforms that are most commonly found in the AES and SHA FPGA implementation publications. This should enable the reader to compare VEST ciphers in relation to published or unpublished static-timing results for other ciphers to establish a clear comparison for any given criterion.

The static timing results for VEST ciphers are *as reported* by the FPGA Synthesis tools. The Xilinx and Altera static timing results do not appear to take into consideration thermal or power requirements.

Unfortunately, cipher power budget is an important real-world limitation of cipher implementations that requires careful attention. For example, a cipher design may appear to be a performance leader because it appears to offer excellent speed on paper, but if it demands more power than many FGPA chipsets or designs can reasonably accommodate, then its range of leadership will be seriously restricted.

Therefore we have taken the unusual (and time consuming) step of performing explorative power analysis on the reported circuit area and clock speeds of several prominent hardware cipher implementations. Using power estimation tools for the Xilinx chipsets, we have independently measured the power consumption of sixteen (16) third party AES and SHA FPGA cipher implementations to compare them with VEST. Of course, estimation of power requirements of third party cipher implementations with only incomplete information concerning the design architecture, routing congestion, slice and memory requirements will inevitably introduce error. Consequently, where no figures were available, we have conservatively underestimated the register usage of third party designs. We have also consistently selected a uniform lower routing congestion level for the benchmark ciphers than the level that we have applied to the VEST ciphers. In both cases, this weighs the results in favour of the AES and SHA-2 ciphers. For example, in every instance we measure VEST with heavy routing congestion but always measure the benchmarking ciphers with medium routing congestion. This alone results in a ~10% disadvantage to VEST ciphers in the comparison results and is done to establish that we have reasonably endeavoured to be conservative in our process and to protect the objectivity of our power consumption measurements.

This paper publishes sufficient information for the reader to be able to measure the power requirements of any cipher in this survey using the free online tools provided by Xilinx [46] independently. Table 2.12 provides performance figures actually achievable within reasonable FPGA power limitations. These figures often can be seen to be far less than the theoretical performance achievable (and advertised) if power considerations are ignored.

In recent electronic correspondences with Helion Tech just prior to publication, Graeme Durant raised questions regarding the quality of our results achieved with the Xilinx static power tool. Graeme describes how Helion Tech have experienced up to +/–100% error between actual power measurements and those based on transistor simulation power estimates with Xpower, which seem to correlate with statements made by Altera [72]. Obviously, the Xilinx static power analysis tools are inherently prone to greater margins of error than dynamic power analysis using Xpower.

With this in mind, our current measurements remain objective within the limitations of the process employed. The most accurate power analysis would require gate level simulation between designs using the Altera PowerPlay II architecture that claims an accuracy level of +/–20% biased towards over-estimation [72], and this level of detailed power analysis is beyond the scope of this paper.

This survey neither compiles published power requirements nor attempts to estimate the power requirements of third-party ASIC designs. The many options available for power reduction in ASIC design, including choice of process, voltage reduction, high-Vt transistors, multi-Vdd, power gating, substrate biasing, clock gating, register clustering, etc. make this impractical.

1.5 Benchmarking authenticated encryption (MAC functionality)

The eSTREAM organisers have requested that all submissions that include a message authentication mechanism be benchmarked in relation to a suitable industry respected message authentication code.

VEST offers two mechanisms to implement message authentication:

1) VEST can be implemented as a separate MAC module, sequentially to a keystream generation module implementing any stream cipher, including VEST. This type of implementation may be useful when a standards-based cipher is required to be used for encryption.

2) The high-performance authenticated encryption mode of VEST ciphers [42] operating at the same speed as the keystream generation, offers the same range of security levels and will be recommended as the preferred mode of operation in Round 2, therefore we have chosen to benchmark the VEST native authenticated encryption mode in this document.

We have chosen not to include the recent parallelisable MAC implementations (universal hash) based on the Carter-Wegman design [43] in our survey. Universal hash images typically employ a **weak** accumulator mechanism and rely **entirely** upon the security of the companion block cipher or stream cipher. MAC codes generated by universal hashes are also not ideal in respect to certain classes of attacks [44]. The performance of universal hash functions is limited by the companion block cipher or stream cipher. A detailed analysis on the security properties or hardware performance of the many recently proposed universal hashing schemes is outside the scope of this paper, in no small part due to the large number of recent schemes that have been broken.

The most widely accepted MAC techniques are the keyed HMAC constructions. HMAC can be implemented using a keyed block cipher (128-bit blocks or wider) or an unkeyed collision-resistant hash function. Therefore, we have compiled a separate table of AES implementations running in feedback mode required for AES-HMAC constructions.

1.6 Benchmarking collision-resistant hash functionality

All VEST ciphers offer high-performance collision-resistant hash functionality.

It is well known that collision-resistant hash functions must satisfy the most aggressive security constraints of any symmetric keyed or unkeyed cryptographic primitive. When selecting a hash function benchmark, we looked for a widely accepted secure collision-resistant hash and chose to focus on the modern SHA-256 and SHA-512 primitives.

1.7 Benchmarking complete systems providing both encryption and authentication

VEST employs an authenticated encryption mode similar in principle to the method used by the software stream cipher Phelix [40], a Category I submission to the eSTREAM by Doug Whiting, Bruce Schneier, Stefan Lucks, and Frédéric Muller.

Generally, when we consider traditional authenticated encryption using general-purpose block ciphers and hash functions, the encryption and message authentication must be performed using two independent cryptographic operations on the message.

In this document, we have found it necessary to benchmark the performance and efficiency of the three functions individually:

1. Counter mode of operation (CTR) / Electronic Codebook (ECB)
2. Feedback mode of operation (required for HMAC-AES)
3. Collision-resistant hashing using SHA-2

This enables the reader to compare the efficiency of different AES and SHA-2 combinations in relation to VEST to suit their own analysis objectives.

1.8 Benchmarking ASIC implementations

We have compiled a broad range of static timing and area requirements for AES and SHA-2 cipher implementations in ASIC. In order to estimate gate count and circuit area, we have performed explorative analysis and synthesis using Alliance EDA [39] tools and production standard-cell libraries. While a complete survey of static-timing and power requirements for VEST ciphers is in development, readers may choose to extrapolate from our extensive FPGA synthesis and static timing results presented in this paper. In isolated cases, we have performed conservative static-timing extrapolations ourselves based on FPGA static-timing results for speculative comparison with ASIC implementations.

The general superiority of VEST across several important benchmarking dimensions in relation to the entire broad range of different leading AES and SHA designs in FPGA we have surveyed in this document strongly supports the view that VEST will be a clear leader in ASIC. This view is reinforced by the fact that the VEST FPGA design achieves its efficiency without leveraging the dedicated high-performance addition, DSP or SRAM modules available on the FPGA chips.

1.9 Benchmarking cipher complexity and security

VEST ciphers are secure cryptographic primitives that can be directly compared with [also considered being secure] AES and SHA-2 cryptographic primitives.

The reader is expected to know that a vast number of stream ciphers have been overly optimistic in reducing the complexity of the cipher design to achieve low gate counts and increase the perceived efficiency of the cipher. We refer the reader to the cryptanalysis of SFINKS for one such example of an overly optimistic design [41].

However, the accusation of obtaining increased efficiency through oversimplification cannot be brought against VEST. By comparison, all VEST ciphers are robust cryptographic designs with large internal states updated by a strong non-linear substitution-permutation network with minimal possible redundancy, with strong non-linear counters to ensure a sufficiently long guaranteed minimal period length, with a conservative number of rounds executed before releasing their first output or their hash values, and releasing only a small portion of their internal state as output on every round.

VEST delivers unrivalled efficiency in terms of speed, demanded circuit area and power consumption for such a conservative and robust cryptographic design. As such, VEST is considered a preferable choice for deployment in proprietary cryptographic applications in hardware.

To elaborate further on this subject, we quote:

> "*… In the design of block ciphers, Lars Knudsen (and others) have for a long time promoted the following: see how many rounds we need to make it secure, then double it (or even multiply by 4). We believe that stream ciphers should also be designed with such a comfortable security margin.*"
>
> – Nicolas T. Courtois, "Cryptanalysis of Sfinks" [41].

Designers of VEST followed the same approach by utilising only strong non-linear feedback, multiplying the secure number of sealing rounds by eight (8) and keeping the state/output proportions at more than 16:1 plus compensation for the information leaked by the output. Extensive analysis has proven such overkill to be unnecessary suggesting that the number of sealing rounds can be safely reduced by half, which is to be expected in the Round 2 VEST submission.

1.10 Cursory analysis concerning active and side-channel attacks

The VEST design avoids several of the worst properties that are routinely exploited in side-channel attacks:

- VEST does not use key or data-dependent branching operations
- VEST does not use key or data-dependent arithmetic operations
- VEST does not use key or data-dependent word-based rotation operations
- VEST does not use unbalanced non-linear Boolean functions

The VEST design includes several highly desirable properties:

- VEST employs shallow and near-uniform logic depth for all cryptographic operations
- VEST employs massive parallelism updating almost the entire secret state on every clock cycle
- VEST round function operates with almost identical behavioural characteristics during keying, sealing, compression and expansion operations
- VEST ciphers are more power-efficient per bit of ciphertext output than AES or SHA, reducing the signal emissions to ciphertext output ratio
- The entire cipher state is updated concurrently with a pseudo-random substitution-permutation network with a very high diffusion rate resulting in any glitch attack uncontrollably influencing large portions of the secret internal state.

We consider that the points raised above demonstrate that the features inherent in the VEST design prevents to a large extent the possible success of side-channel and invasive attacks. Therefore VEST currently does not include the exhaustive defences against this style of attack that other more exposed designs must have. By way of comparison between VEST and the AES, it is important to note that most AES hardware implementation publications we surveyed simply ignore these attacks in their publications even if their designs are particularly exposed to these attacks. We discuss this further below.

Additional hardware implementation techniques that may be employed to improve further any cipher's protection against side-channel attacks include partially randomised clocks, detached power supplies [45], asynchronous self-timing implementations and other well-known techniques.

The VEST authors welcome feedback in relation to any aspect of the design including the potential for side channel and invasive attacks.

PART 2
FPGA PERFORMANCE

2.1 Readings

All static timing results are based on the synthesis and static timing of the primary accumulator core, the largest and slowest component in the cipher design; consequently, these figures represent the upper bound on the cipher performance. Static timing estimates are expected to approximate tightly the upper bound for low-area implementations in otherwise optimal place-and-route conditions. We intend to present static-timing results on complete cipher implementations in the future.

Different implementations, such as low-area, or supporting fast rekeying, will naturally result in different routing congestion overhead in the accumulator and in different area overheads for the finite-state machines. The mapping of different implementations to different FPGA architectures may result in modest performance variation based on macro-cell functionality of a specific FPGA target. It is worthy to mention that variation in FGPA chip grade can result in up to 25% difference in performance between otherwise equivalent implementations.

It is generally recognised as best practice to select a cipher with static timing modestly faster than required otherwise, to ensure robust operation under higher ambient temperatures and to reduce the time and cost required to achieve total static-timing sign off on chip designs. VEST is particularly helpful in this regard.

Analysis concerning the surveyed results can be found in Part Five.

2.2 Results of VEST static timing based on synthesis for encryption and collision-resistant hashing operations on FPGA

Author	Product (Security)	Device	Stages	~Slices	FF	K bits SRAM	MHz	ENC Gbps	Hash Gbps
Sean O'Neil	VEST-4 (~80)	XC3S50-5	1	~170	~256	0	175	~0.7	~1.4
Sean O'Neil	VEST-4 (~80)	XC2V40-5	1	~170	~256	0	225	~0.9	~1.8
Sean O'Neil	VEST-4 (~80)	XC4VLX15-11	1	~170	~256	0	325	~1.3	~2.6
Sean O'Neil	VEST-4 (~80)	XC2VP2-7	1	~170	~256	0	375	~1.5	~3.0
Sean O'Neil	VEST-8 (~128)	XC3S200-5	1	~366	~384	0	175	~1.4	~1.4
Sean O'Neil	VEST-8 (~128)	XC2V80-5	1	~366	~384	0	225	~1.8	~1.8
Sean O'Neil	VEST-8 (~128)	XC4VLX25-11	1	~366	~384	0	312	~2.5	~2.5
Sean O'Neil	VEST-8 (~128)	XC2VP2-7	1	~366	~384	0	350	~2.8	~2.8
Sean O'Neil	VEST-16 (~160)	XC3S1000-5	1	~555	~512	0	175	~2.8	~1.4
Sean O'Neil	VEST-16 (~160)	XC2V250-5	1	~555	~512	0	175	~2.8	~1.4
Sean O'Neil	VEST-16 (~160)	XC4VLX25-11	1	~555	~512	0	300	~4.8	~2.4
Sean O'Neil	VEST-16 (~160)	XC2VP2-7	1	~555	~512	0	318	~5.1	~2.5
Sean O'Neil	VEST-32 (~256)	XC3S1000-5	1	~954	~768	0	146	~4.7	~1.1
Sean O'Neil	VEST-32 (~256)	XC2V250-5	1	~954	~768	0	150	~4.8	~1.2
Sean O'Neil	VEST-32 (~256)	XC4VLX25-11	1	~954	~768	0	243	~7.8	~1.9
Sean O'Neil	VEST-32 (~256)	XC2VP2-7	1	~954	~768	0	265	~8.5	~2.1

[Table 2.1] Static timing results reported for Xilinx chips

Author	Product (Security)	Device	Stages	ALUT	FF	K bits SRAM	MHz	ENC Gbps	Hash Gbps
Sean O'Neil	VEST-4 (~80)	EP2S15F484C3	1	~125	256	0	500	~2.0	~4.0
Sean O'Neil	VEST-8 (~128)	EP2S15F484C3	1	~253	384	0	500	~4.0	~4.0
Sean O'Neil	VEST-16 (~160)	EP2S15F484C3	1	~381	512	0	500	~8.0	~4.0
Sean O'Neil	VEST-32 (~256)	EP2S15F484C3	1	~653	768	0	462	~14.8	~3.7

[Table 2.2] Static timing results reported for Altera Stratix-II

Author	Product (Security)	Device	Stages	ALUT	FF	K bits SRAM	MHz	ENC Gbps	Hash Gbps
Sean O'Neil	VEST-4 (~80)	EP2S15F484C3	1	~125	256	0	725	~2.9	~5.8
Sean O'Neil	VEST-8 (~128)	EP2S15F484C3	1	~253	384	0	625	~5.0	~5.0
Sean O'Neil	VEST-16 (~160)	EP2S15F484C3	1	~381	512	0	581	~9.3	~4.6
Sean O'Neil	VEST-32 (~256)	EP2S15F484C3	1	~653	768	0	462	~14.8	~3.7

[Table 2.3] Projected static timing results for Altera Stratix-II with unbound clock

2.3 The Performance of VEST authenticated encryption mode (MAC) on FPGA

VEST ciphers offer two different methods to provide data authentication: as a separate collision-resistant hash, and the authenticated encryption mode of operation [42].

All VEST ciphers will assume authenticated encryption as their default mode of operation. In applications that require MAC operation, the circuit area and power consumption requirements of the circuit implementing authenticated encryption mode do not significantly increase over what would have been required for achieving encryption alone. Advantageously the security of the MAC generated using the single-pass authentication mode matches the encryption security rating.

The authenticated encryption mode effectively results in roughly halving the circuit area and roughly halving the power requirements of the VEST authenticated encryption implementation comprising a VEST cipher module inline with a VEST hashing module.

The benefits of the authenticated encryption mode in VEST ciphers are even more significant when we consider that the power consumption of a single VEST module is roughly 1.5 to 3.2 times less than the power consumption of some well-known AES implementations performing encryption alone.

When comparing VEST single-pass authenticated encryption mode to AES-HMAC, VEST is always superior across several important benchmarking dimensions.

2.4 Survey of AES-ECB Static Performance

2.4.1 Survey of 128-bit secure AES FPGA implementations

Author	Product	F()	Device	Sec	Mode	Data Stages	Data Bus	SRAM K bits upper bound	SRAM 16 kbits	Slices	Logic with RAM normalised as slices*	Clock	ECB Mbps**
Tim Good, et al [35]	3LUT	E/D	XC2S15-6	128	128	CPU	8	4.4	0.25 (4 kbit)	124	~~*264*~~	67	2
Helion Tech [38]	Tiny AES	E/D	XC4VLX25-11	ALL	128	(i) 615	8	32	2	164	~~*1164*~~	215	44
IP Cores [31]	Ultra Compact	E	XC2VP2-7	128	128	(i) 160	8	0	0	240	~~*240*~~	***130	104
P Chodowiece [36]	Compact	E/D	XC2S30-6	128	128	(i) 44	32	9.6	0	222	~~*522*~~	60	174
G. Rouvroy [37]		E/D	XC3S50-4	128	128	(i) 44	32	34	0	163	~~*1,231*~~	71	208
Algotronix [32]	AES Core Enc	E	XCV250-5	128	128	(i) 44	32	64	4	791	~~*2,791*~~	93	270
North Pole Eng [6]	Compact E/D	E/D	XC2Vxxx-5	ALL	128	(i) 45	32	160	10	864	~~*5,864*~~	117	335
Helion Tech [7]	Standard Enc	E	XC3S200-5	128	128	(i) 48	32	48	3	251	~~*1751*~~	151	402
CAST [33]	*AES_E Core*		*XC2VP2-7*	*128*	*128*	*(i) 44*	*32*	*32*	*2*	*133*	~~*(1,133)*~~	*200*	580
	AES_KEY	*(estimated on asic figures)*						*?*	*?*	*133*	~~*(133)*~~	*<200*	
	TOTAL							~32	~2	~266	~~*1,266*~~	200	
Helion Tech [7]	Standard Enc	E	XC4VLX25-11	128	128	(i) 48	32	48	3	240	~~*1,740*~~	252	672
Asics.ws [20]	128-Encrypt	E	XS2V200-6 (1026-r)	128	128	(i) 12	128	0	0	1748	~~*1,748*~~	101	1077
Helion Tech [7]	Fast Enc	E	XC3Sxx-5	128	128	(i) 11	128	160	10	447	~~*5,447*~~	133	1547
CAST [33]	*AES_E Core*		*XC2VP2-7*	*128*	*128*	*(i) 11*	*128*	128	*8*	*416*	~~*(4,416)*~~	*160*	1856
	AES_KEY	*(estimated on asic figures)*						?	?	416	~~*(416)*~~	<160	
	TOTAL							~128	~8	~832	~~*4,832*~~	160	
Helion Tech [7]	Fast Enc	E	XC2Vxxxx-6	128	128	(i) 11	128	160	10	447	~~*5,447*~~	166	1931
Helion Tech [7]	Fast Enc	E	XC4VLX25-11	128	128	(i) 11	128	160	10	447	~~*5,447*~~	219	2548
North Pole Eng [8]	Fast E/D Slow-Rekey	E/D	XC2Vxxx-5	ALL	192	(u) 44	128	1440	90	3880	~~*6,692*~~	100	~~12800~~
North Pole Eng [8]	Ultrafast E Dynamic-Rekey	E/D	XC2Vxxx-5	ALL	192	(u) 44	128	2560	160	5840	~~*10,840*~~	100	~~12800~~
Järvinen...[6]	SIG-AES-E	E	XC2V2000-5	128	128	(u) 44	128	0	0	10,750	~~*10,750*~~	139.1	~~17800~~
Alireza Hodjat, [3]	7 stages / round	E	XC2VP20-7	128	128	(u) 46	128	1,344	84	6,400	~~*48,400*~~	157.1	~~20110~~
Alireza Hodjat, [3]	4 stages / round	E	XC2VP20-7	128	128	(u) 41	128	0	0	12,450	~~*12,450*~~	168.3	~~21540~~
Alireza Hodjat, [3]	4 stages / round	E	XC2VP20-7	128	128	(u) 31	128	1,344	84	5,177	~~*47,177*~~	168.3	~~21540~~
Alireza Hodjat, [3]	7 stages / round	E	XC2VP20-7	128	128	(u) 71	128	0	0	9,446	~~*9,446*~~	169.1	~~21640~~
Tim Good… [35]	3LUT	E/D	XCV2000E-8	128	128	(u) 70	128	0	0	16,693	~~*16,693*~~	184.8	~~23654~~
Tim Good… [35]	3LUT	E/D	XC3S2000-5	128	128	(u) 70	128	0	0	17,425	~~*17,425*~~	196.1	~~25107~~

[Table 2.4] Claimed area and published static timing of third party AES-128 cipher implementations running in ECB mode

* The paper [35] describes a method of normalising SRAM as slices using a ratio of 32-bits of SRAM per slice. A cursory analysis of the Alireza Hodjat [3] designs highlights the **high-margin of error in this technique** when only the number of memory banks is known, as opposed to the actual amount of memory required. We do not recommend attempting to normalise SRAM to slices based on published figures.
** Struck out bandwidth performance figures indicate claimed performance speeds that cannot be attained under reasonable thermal commercial conditions.
*** Updated performance figures based on electronic correspondences with Dmitri Varsanofiev of IP Cores.

2.4.2 Survey of 192-bit secure AES FPGA implementations

Author	Product	F()	Device	Sec	Mode	Data Stages	Data Bus	Slices	SRAM Kbits	16k SRAM	Clock	ECB Mbps
North Pole Engineering [8]	Compact E/D	E/D	XC2Vxxx-5	ALL	192	(i) 53	32	864	160	10	117	283
North Pole Engineering [8]	Fast E/D Slow-Rekey	E/D	XC2Vxxx-5	ALL	192	(u) 44	128	3880	1440	90	100	~~12800~~
North Pole Engineering [8]	Ultrafast E Dynamic-Rekey	E/D	XC2Vxxx-5	ALL	192	(u) 44	128	5840	2560	160	100	~~12800~~

[Table 2.5] Claimed area and published static timing of third party AES-192 cipher implementations running in ECB mode

2.4.3 Survey of 256-bit secure AES FPGA implementations

Author	Product	F()	Device	Sec	Mode	Data Stages	Data Bus	Slices	SRAM Kbits	16k SRAM	Clock	ECB Mbps
North Pole Engineering [8]	Compact E/D	E/D	XC2Vxxx-5	ALL	256	(i) 61	32	864	160	10	117	246
Helion Tech [7]	Fast Enc	E	XC4VLX25-11	256	256	(i) 15	128	581	160	10	219	1868.8
North Pole Engineering [8]	Fast E/D Slow-Rekey	E/D	XC2Vxxx-5	ALL	256	(u) 44	128	3880	1440	90	100	~~12800~~
North Pole Engineering [8]	Ultrafast E Dynamic-Rekey	E/D	XC2Vxxx-5	ALL	256	(u) 44	128	5840	2560	160	100	~~12800~~

[Table 2.6] Claimed area and published static timing of third party AES-256 cipher implementations running in ECB mode

2.5 Survey of AES-FEEDBACK Static Performance

Author	Product	F()	Device	Sec	Mode	Data Stages	Data Bus	Slices	SRAM Kbits	16k SRAM	Clock	Hash Mbps
Tim Good… [35]	3LUT	E/D	XC2S15-6	128	128	CPU	8	124	4.4	8	0	67
P Chodowiece [36]	Compact	E/D	XC2S30-6	128	128	(i) 44	32	222	9.6	12	0	60
G. Rouvroy [37]		E/D	XC3S50-4	128	128	(i) 44	32	163	768	48	**0**	71
IP Cores [31]	Ultra Compact	E	XC2VP2-7	128	~~128~~	(i) 160	8	240	0	0	130	104
Algotronix [32]	AES Core Enc	E	XCV250-5	128	~~128~~	(i) 44	32	791	64	4	93	270
North Pole Engineering [8]	Fast E/D Slow-Rekey	E/D	XC2Vxxx-5	ALL	~~128~~	(u) 44	128	3880	1,440	90	100	~~291~~
North Pole Engineering [8]	Ultrafast E Dynamic-Rekey	E/D	XC2Vxxx-5	ALL	~~128~~	(u) 44	128	5840	2,560	160	100	~~291~~
Alireza Hodjat, [5]	7 stages / round	E	XC2VP20-7	128	~~128~~	(u) 71	128	9,446	0	0	169.1	~~304~~
North Pole Engineering [8]	Compact E/D	E/D	XC2Vxxx-5	ALL	~~128~~	(i) 45	32	864	160	10	117	335
Helion Tech [7]	Standard Enc	E	XC3Sxx-5	128	~~128~~	(i) 48	32	251	48	3	151	402
Kimmo U. Järvinen...[6]	SIG-AES-E	E	XC2V2000-5	128	~~128~~	(u) 44	128	10,750	0	0	139.1	~~405~~
Alireza Hodjat, [5]	7 stages / round	E	XC2VP20-7	128	~~128~~	(u) 46	128	6,400	1,344	84	157.1	~~437~~
Alireza Hodjat, [5]	4 stages / round	E	XC2VP20-7	128	~~128~~	(u) 41	128	12,450	0	0	168.3	~~525~~
CAST [33]	*AES_E Core*		*XC2VP2-7*	*128*	~~*128*~~	*(i) 44*	*32*	*133*	*32*	*2*	*200*	580
	AES_KEY	*(estimated on asic figures)*						*~133*	*?*	*?*	*<200*	
	TOTAL							~266	~32	~2	200	
Helion Tech [7]	Standard Enc	E	XC4VLX25-11	128	128	(i) 48	32	240	48	3	252	672
Alireza Hodjat, [4]	4 stages / round	E	XC2VP20-7	128	~~128~~	(u) 31	128	5,177	1,344	84	168.3	~~695~~
Asics.ws [20]	128-Encrypt	E	XS2V200-6 (1026-r)	128	~~128~~	(i) 12	128	1748	0	0	101	1077
Helion Tech [7]	Fast Enc	E	XC3Sxx-5	128	~~128~~	(i) 11	128	447	160	10	133	1547
CAST [33]	*AES_E Core*		*XC2VP2-7*	*128*	~~*128*~~	*(i) 11*	*128*	*416*	*128*	*8*	*160.0*	1856
	AES_KEY	*(estimated on asic figures)*						*~416*	*?*	*?*	*<160.0*	
	TOTAL							~832	~128	~8	160.0	
Helion Tech [7]	Fast Enc	E	XC2Vxxxx-5	128	~~128~~	(i) 11	128	447	160	10	166	1931
Helion Tech [7]	Fast Enc	E	XC4Vxxxx-11	128	~~128~~	(i) 11	128	447	160	10	219	2548

[Table 2.6] Claimed area and measured static timing of third party AES-128 cipher implementations running feedback mode of operation with a fixed key

* The security of AES HMAC is limited to 64-bit.
* Performance figures for AES running in 192-bit and 256-bit key modes are slower than 128-bit key results.
* Not all cipher instances are suitable for performing hashing mode of operations that require the per-block rekeying.

2.6 Survey of SHA-256 Static Performance

Author	Product	Device	Clock	Slices	DFF	16 kbit SRAM	SHA-256 Mbps
Helion Tech [50]	SHA-1, SHA-224, SHA-256 and MD5 Hashing, Tiny with HMAC	XC4VFX12-11	175	526	?	1	29
Norbert Pramstaller…[10]	SHA-256	XC2Sxxx-?	84	964	**?**	**?**	196
CAST [11]	SHA-256	XC2V1000-6	56	980	?	1	441
CAST [11]	SHA-256	XC31000-5	62	980	?	1	488
N. Sklavos, et al. [12]	SHA-256/384/512	XCV200PQ240-6	74	~2384	?	2	582
Helion Tech [9]	SHA-256	XC3Sxxx-5	82	814	?	1	636
N. Sklavos, et al. [49]	SHA-256	XCV200PQ240-6	85	~1060	?	1	653
CAST [11]	SHA-256	XC2VP7-7	85	955	?	1	669
CAST [11]	SHA-256	XC4VLX25-11	96	945	?	1	756
Helion Tech [9]	SHA-256	XC2VPxx-7	126	815	?	1	977
Helion Tech [9]	SHA-256	XC4VLXxxx-11	140	834	?	1	1086

[Table 2.7] Claimed area and published static timing of third party SHA-256 implementations

Caveat: When comparing VEST keyed hashing performance in relation to HMAC-like hashing algorithms, it is important to keep in mind the 32 sealing rounds required by VEST ciphers. The VEST 32 sealing rounds represent a significant overhead for small messages. We expect to reduce that overhead in our Round 2 submission.

Caveat: HMAC-SHA-256 requires an overhead of three full SHA-256 invocations, an increase of 192 bytes to the length of the message in processing time, which represents a significant overhead for small messages.

2.7 Survey of SHA-512 Static Performance

Author	Product	Device	Clock	Slices	DFF	SRAM modules	Mbps
Francis Crowe [13]	Iterated SHA-512	XCV2000E-?	32	1996	?	?	414
N. Sklavos, et al. [49]	SHA-512	XCV200PQ240-6	75	~2237	?	? 2	474
N. Sklavos, et al. [12]	SHA-256/384/512	XCV200PQ240-6	74	~2384	?	? 2	467
Francis Crowe [13]	Unrolled-2	XCV2000E-?	20	2383	?	? 4	516
Francis Crowe [13]	Unrolled-4	XCV2000E-?	10	3506	?	? 8	533
Tim Grembowski… [14]	SHA-512	XCV1000-6	55	~3400	?	2	616

[Table 2.8] Claimed area and static timing of third party SHA-512 implementations

* SHA-512 implementations are notorious for poorly documenting required SRAM and DFF usage.

Caveat: When comparing VEST keyed hashing performance in relation to HMAC-like hashing algorithms, it is important to keep in mind the 32 sealing rounds required by VEST ciphers. The VEST 32 sealing rounds represent a significant overhead for small messages. We expect to reduce that overhead in our Round 2 submission.

Caveat: HMAC-SHA-512 requires an overhead of three full SHA-512 invocations, an increase of 384 bytes to the length of the message in processing time, which represents a significant overhead for small messages.

2.8 Results of Power analysis of VEST on Stratix-II FPGA

Upper Bound Bandwidth	pW-S	Budget	1.23 W	2.45 W
VEST-4 (pins + counters + acc)	0.49	**Megabit/s**	5788	15748
VEST-8 (pins + counters + acc)	1.10	**Megabit/s**	5744	14024
VEST-16 (36 pins + counters + acc)	1.85	**Megabit/s**	6720	16672
VEST-32 (68 pins + counters + acc)	3.59	**Megabit/s**	7040	17184

[Table 2.9] Maximum total bandwidth achievable limited by power budget

The above table shows measured upper bounds of the total achievable bandwidth given a power budget of 1.23 W and 2.45 W respectively on a Stratix-II chip maintaining a junction temperature of 85°C. Power budget includes the FPGA device quiescent power overhead.

2.9 Results of Power analysis of VEST on Xilinx FPGA

VEST	PINS	CLB SLICES	FF	Select RAM	Routing
VEST-4	12	170	256	0	Heavy*
VEST -8	20	366	384	0	Heavy*
VEST -16	36	555	512	0	Heavy*
VEST -32	68	954	768	0	Heavy*

[Table 2.10] Inputs supplied to the Xilinx power measurement tool

*Approximately 10% more power hungry than medium routing for VEST designs.

Commercial Ambient: 55°**C**, ThetaJA = 12.8°**C**/W

Cipher	Mode	Device	<1.23 W MHz	< 1.23 W Mbps	pW-S (J=85)	Quiet (J=85)	Actual mW	<2.45 W MHz	<2.45 W Mbps
VEST-4 (~80)	Encrypt (~80)	XC3S50-5	2900*	11600	0.36	31	2342	6450*	25800
VEST-4 (~80)	Encrypt (~80)	XC2V40-5	660	2640	1.32	333	2376	1550	6200
VEST-4 (~80)	Encrypt (~80)	XC4VLX15-11	960	3840	0.95	360	2374	2120	8480
VEST-4 (~80)	Encrypt (~80)	XC2VP2-7	600	2400	0.93	918	2366	1550	6200
VEST-8 (~128)	Encrypt (~128)	XC3S200-5	1620*	12960	0.73	31	2362	3200*	25600
VEST-8 (~128)	Encrypt (~128)	XC2V80-5	320	2560	2.68	338	2433	780	6240
VEST-8 (~128)	Encrypt (~128)	XC4VLX25-11	658*	5264	0.83	360	2352	2400*	19200
VEST-8 (~128)	Encrypt (~128)	XC2VP2-7	282	2256	1.92	918	2360	750	6000
VEST-16 (~160)	Encrypt (~160)	XC3S1000-5	1020	16320	1.19	31	2347	1950	31200
VEST-16 (~160)	Encrypt (~160)	XC2V250-5	210	3360	4.16	342	2421	500	8000
VEST-16 (~160)	Encrypt (~160)	XC4VLX25-11	505	8080	1.82	360	2367	1100	17600
VEST-16 (~160)	Encrypt (~160)	XC2VP2-7	274	4384	2.06	918	2340	687	10992
VEST-32 (~256)	Encrypt (~256)	XC3S1000-5	605	19360	1.99	31	2365	1170	37440
VEST-32 (~256)	Encrypt (~256)	XC2V250-5	120	3840	7.23	342	2405	285	9120
VEST-32 (~256)	Encrypt (~256)	XC4VLX25-11	360	11520	2.82	360	2368	710	22720
VEST-32 (~256)	Encrypt (~256)	XC2VP2-7	110	3520	5.72	918	2361	282	9024

[Table 2.11] Power measurement results for VEST ciphers on Xilinx chipsets

* A small margin of error is anticipated in favour of the performance of VEST-4 and VEST-8 power requirements when the aggregate clock speed exceeds the aggregate clock synchronisation resources.

2.10 Results of Power analysis of AES-ECB on Xilinx FPGA

Commercial Ambient: 55°**C**, ThetaJA = 12.8°**C**/W, Total Power = 2.45W ~ Junction 85°**C**

Author	**Product**	**F()**	**Device**	**Sec**	**Mode**	**MHz**	**Mbps**	**Pow mW**	**J°C**	**pW-S**	**J=85 Quiet**	**J=85 Power mW**	**MHz**	**Mbps**
Alireza Hodjat, et al [3]	7 stages per round AES-128	E	XC2VP20-7	128	128	169.1	21600	9167	**72**	25.1	918	2300	55	7040
North Pole Engineering [8]	AES Compact Encrypt / Decrypt	E/D	XC2V250-5	128	128	117	335	799	65	3.92	342	2402	525	1493
North Pole Engineering [8]	AES Ultrafast Encryptor	E	XC2V8000-5	128	128	100	12800	3301	**97**	39.5	400	2314	49	6208
North Pole Engineering [8]	Fast E/D Slow-Rekey	E/D	XC2V250-5 (normalised)	ALL	128	100	12800	2954	**93**	26.0	342	2376	78	9984
North Pole Engineering [8]	Ultrafast E Dynamic-Rekey	E/D	XC2V250-5 (normalised)	ALL	128	100	12800	4094	**107**	37.4	342	2326	53	6784
Helion Tech [7]	AES Standard Encryptor	E	XC3S15-5	128	128	151	402	110	56	0.38	31	2316	6000	16000
Helion Tech [7]	AES Fast Encryptor	E	XC3SXX-5	128	128	133	1547	179	57	0.94	31	2376	2500	29090
Helion Tech [7]	AES Fast Encryptor	E	XC2V250-5	128	128	146	1699	751	64	2.76	342	2362	730	8494
Helion Tech [7]	AES Fast Encryptor	E	XC4Vxxxx-11	128	128	219	2548	643	63	1.56	360	2313	1250	14545
IP Cores [31]	8 bit Ultra Compact Encrypt	E	XC2V250-5	128	128	?	?	?	?	0.95	342	2345	2090	1672
IP Cores [31]	Ultra Compact (?80 reg)	E	XC2VP2-7	128	128	130	104	754	65	0.80	687	2338	2050	1640
Asics.ws [20]	128-Encrypt	E	XCS2V200-6 **	128	128	101	1077	?	?	?	?	?	?	?
Asics.ws [20]	128-Encrypt	E	XC2V250-5 (normalise)	128	128	?	?	?	?	6.94	342	2356	290	3093
Tim Good, et al [35]	3LUT (17425 CLB, 5000 DFF)	E/D	XC3S2000-5	128	128	196.1	25107	3521	**100**	17.8	31	2313	128	16384
Helion Tech [7]	Fast Enc	E	XC4Vxxxx-11	128	128	219	2548	643	63	1.5	360	2314	1280	14894
Tim Good, et al [35]	TINY (124 slice / 280 select LUT)	E/D	XC2VP2-7	128	128	?	?	?	?	0.907	687	2321	1800	60

[Table 2.12] Power consumption measurement results for electronic codebook mode of operation

** The VirtexE online power worksheet does not support thermal controls.
*** It is important to note that there are only a small number of SRAM modules on FPGA chips.

It is difficult to predict the design decisions employed in block cipher implementations supporting both encryption and decryption in regard to minimisation of power-consumption accurately. A cursory review of open-source DES [27] and AES [46] and [47] implementations clearly indicates that a multiplexer is used to select the output between encoding and inverse encoding operations resulting in concurrent transistor activity for both the encryption and decryption circuits.

It is natural for a cipher implementation to mask off one or some of the paths almost halving the power overhead. In fully unrolled cipher implementations, supporting encryption and decryption operations in one pipeline, advanced masking techniques may reduce power consumption if the consecutive pipeline operations are of the same class.

We are not aware of designs employing these techniques or advertising power-efficiency of any specific implementations. Increasing power-efficiency will always result in an increase in circuit area, and potentially an increase in critical-path depth.

It is difficult to predict the likely power-consumption of block ciphers that employ decoupled key-expansion modules. Block-ciphers performing hashing operations will result in frequent per block rekeying, where as encoding of long chunks of data will result in sparse rekeying. Where the area figures include an authentication module, the power consumption approximates the upper bound, assuming frequent key expansion.

2.11 Results of Power analysis of SHA on Xilinx FPGA

Commercial Ambient: 55°**C**, ThetaJA = 12.8°**C**/W, Total Power = 2.45W ~ Junction 85°**C**

Author	**Product**	**F()**	**Device**	**Sec**	**Mode**	**Slice**	**Reg**	**16k bit SRAM**	**Stages**	**pW-S**	**J=85 Quiet**	**J=85 Power mW**	**MHz**	**Mbps**
N. Sklavos, et al. [12]	SHA-256	H	XC2V250-5 (normalise)	128	128	1060	1651	0	65	4.45	342	2344	450	3545
Helion Tech [9]	SHA-256	H	XC4VLX25-11	128	128	834	? (256)	1	66	1.52	360	2346	1300	10085
N. Sklavos, et al. [12]	SHA-512	H	XC2V250-5 (normalise)	256	256	2237	3739	0	81	8.81	342	2338	215	1359
Francis Crowe [13]	Unrolled-4	H	XCV250-5 (normalize)	256	256	3506	? (292)	? (8 dual port)	20	15.3	342	2409	135	7195*

[Table 2.13] Power consumption measurement results for SHA-2

* The number of registers is loosely estimated based on 1/3 the logic CLB per round, divided by 4 because the loop has been unrolled 4 times.

PART 3
ASIC PERFORMANCE

3.1 Survey of VEST Static circuit area requirements

Author	Product	Encryption Security	MAC Security	Hash Security	K Gates min	Memory Kilobit
Sean O'Neil	VEST-4	80	80	80	5	0
Sean O'Neil	VEST-8	128	128	128	9	0
Sean O'Neil	VEST-16	160	160	160	13	0
Sean O'Neil	VEST-32	256	256	256	22	0

[Table 3.1] Estimated ASIC area requirements and claimed security

All Round 2 VEST ciphers will assume authenticated encryption as their default mode of operation.

We leave it to the reader at this stage to consult hardware design and synthesis experts independently to extrapolate expected ASIC performance and comment on the suitability of VEST for specific custom projects using our extensive FPGA synthesis, static timing and power results on both Xilinx and Altera platforms. A general industry rule of thumb is a 2 to 4 times performance improvement from a FGPA to an ASIC design targeted to the same geometry. We anticipate good scaling, in part because VEST does not leverage high-performance ASIC macro-cells found in FPGA designs such as SRAM or DSP modules.

3.2 Cursory survey of DES Static Performance

Author	Instance	F()	Geo	Sec	Mode	Data Stages	Enc Bus	~ K Gates	~ K Bits	MHz	Speed Mbit/s
Asics.ws [27]	3DES	E/D	0.18	168	168	(i) 48	64	5.5	0	160	200
Asics.ws [27]	3DES	E/D	0.18	168	168	(u) 48	64	55.0	0	300	19200

[Table 3.2] DES static timing and area requirements

The above two cipher instances, from our cursory searching, appear to be roughly the smallest and fastest cipher implementations of DES respectively.

3.3 Survey of AES-ECB Static Performance

3.3.1 Survey of 128-bit secure AES ASIC implementations

Author	**Instance**	**F()**	**Geo**	**Sec**	**Mode**	**Data Stages**	**Enc Bus**	**~ K Gates**	**~ K Bits**	**MHz**	**Speed Mbit/s**
Elliptic Semi. [27]	Tiny AES Core	E/D	?	ALL	128	(i) 262	?	8	0	(?) 81	(Claimed) 40
IP Cores [31]	Ultra Compact Enc	E	0.18	128	128	(i) 160	8	3	0	80	64
			***0.13**							150	**120**
Helion Tech [7]	Standard Enc	E	0.18	ALL	128	(i) 48	32	11	0	200	533
North Pole Eng. [8]	Compact	E/D	0.25	ALL	128	(i) 45	32	3	160	278	790
Cadence [19]	AES-128	E/D	?	128	128	(i) 42	32	36	0	260	792
CAST [34]	AES-Enc+Key	E/D	0.18	128	128	(i) 44	32	11	0	384	1117
Cadence [19]	AES-HP	E/D	?	ALL	128	(i) 12	128	64	0	200	2133
Helion Tech [7]	Fast Enc and Dec Full Duplex E/D	E/D	0.18	128	128	(i) 11	128	57	0	200	2327
Asics.ws [20]	128-Encrypt	E	0.18	128	128	(i) 12	128	38	0	265	2827
Helion Tech [7]	Fast Enc	E	0.18	128	128	(i) 11	128	27	0	**250	2909
CAST [34]	AES-Enc+Key	E/D	0.18	128	128	(i) 11	128	38	0	250	2909
Alireza Hodjat [22]	Feedback (86 mW)	E/D	0.18	128	128	(i) 11	128	73	0	295	3430
Sumio Morioko [57]	Twisted-BDD + Basic	D	***0.13**	128	128	(i) 10	128	62	0	699	**8900**
Sumio Morioko [57]	Twisted-BDD + TBox	D	***0.13**	128	128	(i) 10	128	282	0	885	**11300**
Sumio Morioko [57]	Twisted-BDD + TBox	E	***0.13**	128	128	(i) 10	128	168	0	909	**11600**
Alireza Hodjat [23]	Multi-Round	E	0.18	128	128	(u) 11	128	116	0	245	15700
Alireza Hodjat [23]	Multi-Round	E	0.18	128	128	(u) 11	128	225	0	362	23100
Alireza Hodjat [23]	Outer-Round	E	0.18	128	128	(u) 11	128	211	0	246	31500
Asics.ws [21]	Data-Path + key	E/D	0.18	128	128	(u) 12	128	395	0	266	34000
Alireza Hodjat [23]	Outer-Round	E	0.18	128	128	(u) 11	128	372	0	377	48200
Alireza Hodjat [23]	Inner/Outer-Round	E	0.18	128	128	(u) 41	128	313	0	467	59700
Alireza Hodjat [23]	Inner/Outer-Round	E	0.18	128	128	(u) 41	128	473	0	606	77600

[Table 3.3] AES-128 static timing and area requirements for electronic codebook mode

* 0.13 geometries may achieve a full 2x clock-speed gain over 0.18 geometries.
** Helion Tech claims that speeds approaching 300 MHz are possible with some EDA toolsets and standard cell libraries. They requested we surveyed the cipher at 250 MHz as this is a realistic expectation for most toolsets.

3.3.2 Survey of 192-bit secure AES ASIC implementations

Author	Instance	F()	Geo	Sec	Mode	Data Stages	Enc Bus	~ K Gates	~ K Bits	MHz	Speed Mbit/s
Elliptic Semi. [28]	Tiny AES Core	E/D	?	ALL	192	(i) 312	?	8	0	81	33
Helion Tech [7]	Standard Enc	E	0.18	ALL	192	(i) 56	32	11	0	200	457
Cadence [19]	AES-192	E/D	?	ALL	192	(i) 50	32	42	0	260	665
North Pole Eng. [8]	Compact	E/D	0.25	ALL	192	(i) 53	32	3	160	278	671
Cadence [19]	AES-HP	E/D	?	ALL	192	(i) 14	128	64	0	200	1828
Northpole Eng. [8]	Fast (813 Mbps feedback)	E/D	0.25	ALL	192	? (u) 44	128	15	1440	285	36000
Northpole Eng. [8]	Ultra Fast	E/D	0.25	ALL	192	? (u) 44	128	26	2560	323	41300

[Table 3.4] AES-192 static timing and area requirements for electronic codebook mode

3.3.3 Survey of 256-bit secure AES ASIC implementations

Author	Instance	F()	Geo	Sec	Mode	Data Stages	Enc Bus	~ K Gates	~ K Bits	MHz	Speed Mbit/s
Elliptic Semi. [28]	Tiny AES Core	E/D	?	ALL	256	(i) 362	?	8	0	81	29
Helion Tech [7]	Standard Enc	E	0.18	ALL	256	(i) 64	32	11	0	200	400
Cadence [19]	AES-256	E/D	?	ALL	256	(i) 58	32	40	0	260	574
North Pole Eng. [8]	Compact	E/D	0.25	ALL	256	(i) 61	32	3	160	278	583
Cadence [19]	AES-HP	E/D	?	ALL	256	(i) 16	128	64	0	200	1600
Helion Tech [7]	Fast Enc and Dec Full Duplex E/D	E/D	0.18	256	256	(i) 15	128	60	0	200	1706
Helion Tech [7]	Fast Enc	E	0.18	ALL	256	(i) 15 (claimed)	128	31	0	200	1706 (1828)
Asics.ws [21]	Data-Path + key	E/D	0.18	256	256	(u) 16	128	889	0	266	34000
Northpole Eng. [8]	Fast (813 Mbps feedback)	E/D	0.25	ALL	256	? (u) 44	128	15	1440	285	36000
Northpole Eng. [8]	Ultra Fast	E/D	0.25	ALL	256	? (u) 44	128	26	2560	323	41300

[Table 3.5] AES-256 static timing and area requirements for electronic codebook mode

3.4 Survey of AES-FEEDBACK Static Performance in ASIC

Author	Instance	F()	Geo	Sec	Mode	Data Stages	Enc Bus	~ K Gates	~ K Bits	MHz	Hash Mbit/s
Elliptic Semi. [28]	Tiny AES Core	E/D	?	ALL	~~128~~	262	?	8	0	(?) 81	(claimed) 40
IP Cores [31]	Ultra Compact Enc	E	0.18	128	~~128~~	160	8	3	0	80	64
			***0.13**							150	**120**
Helion Tech [7]	Standard Enc	E	0.18	ALL	~~128~~	(i) 48	32	11	0	200	533
North Pole Eng. [8]	Compact	E/D	0.25	ALL	~~128~~	(i) 45	32	3	160	278	790
Cadence [19]	AES-128	E/D	?	128	~~128~~	(i) 42	32	36	0	260	792
Northpole Eng. [8]	Fast (813Mbps)	E/D	0.25	ALL	~~128~~	(u) 44	128	15	1440	285	818
Northpole Eng. [8]	Ultra Fast	E/D	0.25	ALL	~~128~~	(u) 44	128	26	2560	323	939
CAST [34]	AES-Enc+Key	E/D	0.18	128	~~128~~	(i) 44	32	11	0	384	1117
Alireza Hodjat [23]	Multi-Round	E	0.18	128	~~128~~	(u) 11	128	116	0	245	1427
Alireza Hodjat [23]	Inner/Outer-Round	E	0.18	128	~~128~~	(u) 41	128	313	0	467	1456
Helion Tech [7]	Fast Enc	E	0.18	256	~~128~~	(i) 15 (claimed)	128	31	0	200	1706 (1828)
Alireza Hodjat [23]	Inner/Outer-Round	E	0.18	128	~~128~~	(u) 41	128	473	0	606	1893
Alireza Hodjat [23]	Multi-Round	E	0.18	128	~~128~~	(u) 11	128	225	0	362	2100
Cadence [19]	AES-HP	E/D	?	ALL	~~128~~	(i) 12	128	64	0	200	2133
Helion Tech [7]	Fast Enc and Dec Full Duplex E/D	E/D	0.18	128	~~128~~	(i) 11	128	57	0	200	2327
Helion Tech [7]	Fast Enc	E	0.18	128	~~128~~	(i) 11	128	27	0	200	2327
Asics.ws [20]	128-Encrypt	E	0.18	128	~~128~~	(i) 12	128	38	0	265	2827
Asics.ws [21]	Data-Path + key	E/D	0.18	128	~~128~~	(u) 12	128	395	0	266	2833
Alireza Hodjat [23]	Outer-Round	E	0.18	128	~~128~~	(u) 11	128	211	0	246	2864
CAST [35]	AES-Enc+Key	E/D	0.18	128	~~128~~	(i) 11	128	38	0	250	2909
Alireza Hodjat [22]	Feedback (86 mW)	E/D	0.18	128	~~128~~	(i) 11	128	73	0	295	3430
Alireza Hodjat [23]	Outer-Round	E	0.18	128	~~128~~	(u) 11	128	372	0	377	4381
Sumio Morioko [57]	Twisted-BDD + Basic	D	***0.13**	128	128	(i) 10	128	62	0	699	**8900**
Sumio Morioko [57]	Twisted-BDD + TBox	D	***0.13**	128	128	(i) 10	128	282	0	885	**11300**
Sumio Morioko [57]	Twisted-BDD + TBox	E	***0.13**	128	128	(i) 10	128	168	0	909	**11600**

[Table 3.6] AES-128 static timing and area requirements for feedback mode of operations with a fixed key

* 0.13 geometries may achieve a full 2x clock-speed gain over 0.18 geometries.

3.5 Survey of SHA-256 Static performance

Author	Instance	Technology	Security Claimed	Clock Speed	Gates Minimum	Memory Kilobit	Speed Megabit/s
Cadence [24]	SHA-256	0.18 CMOS	128	133	~21 k	0 kb	~971
Helion Tech [9]	SHA-256	0.18 CMOS	128	150	~23 k	0 kb	~1163
Helion Tech [9]	SHA-256	0.18 CMOS	128	253	~26 k	0 kb	~1963
SafeXcell IP [25]	EIP-57c	0.13 CMOS	128	162	~23 k	0 kb	~2000
SafeXcell IP [25]	EIP-57cl	0.13 CMOS	128	250	~31 k	0 kb	~2600

[Table 3.7] SHA-256 static timing and area requirements

3.6 Survey of SHA-512 Static performance

We could not find any ASIC performance figures for SHA-512 implementations.

PART 4
SOFTWARE PERFORMANCE

4.1 Software Performance

VEST ciphers were designed exclusively with hardware performance in mind.

Our original reference implementations of VEST ciphers submitted to eSTREAM currently perform at speeds between about 4000 and 6000 clocks per byte. We have updated our software performance figures based on a bit-sliced implementation of the VEST cipher. A 32-bit bitslice VEST implementation currently performs at speeds between 42 and 64 clocks per byte. Even though it may not be fast enough to compete with software-efficient designs such as the AES or RC4, VEST ciphers show tolerable software speeds comparable with the fastest known software implementations of the DES (45 clocks per byte) or IDEA (50 clocks per byte). We anticipate that 64-bit or 128-bit implementations utilising SIMD or GPU instruction sets can improve VEST software performance further.

Bitslice implementations of VEST ciphers are suitable for packet-based software interoperability with hardware devices such as server-side RFID and networking applications hosted on general-purpose processors.

Although we continue to improve the performance of VEST ciphers in software, neither its security nor its hardware performance will be sacrificed.

PART 5
SELECTIVE COMPARISON OF VARIOUS AES IMPLEMENTATIONS

5.1 Table Shorthand

- The bandwidth in Megabits per second for the cipher running at “10 MHz”
- “Static Megabits” per second is claimed top speed of cipher
- “Max Mbps” achievable with J=85 and a budget of <2.45W

5.2 General differences between VEST and AES ciphers
5.2.1 Target applications

The AES standard is a general-purpose block cipher that supports hardware acceleration. AES is designed to support encryption and message-authentication operations. AES is designed to operate efficiently for 8-bit smartcard processors and for 32-bit general-purpose processors.

The VEST ciphers are hardware-dedicated constructions that are intended for proprietary applications. VEST ciphers are intended to provide encryption, decryption, message authentication and collision-resistant hashing in one module. VEST is designed to provide these services in less circuit area and at reduced cost when implemented in hardware than the solutions based on general-purpose primitives such as the AES or SHA.

5.2.2 Performance in hardware

The ability to implement the AES round function in several different ways enables hardware implementations in the range of 2 megabit to 11600 megabit for iterated constructions, as well as slow low-area implementations. This flexibility is achieved by selecting operations that are reasonably efficient in both software and hardware architectures. AES was designed and selected with the intention of performing collision-resistant hashing with dedicated primitives. It follows that general-purpose software block ciphers lose resource efficiency to gain generality.

The VEST primitives are intended to achieve the desired security properties with the greatest resource efficiency in hardware. Each family of VEST ciphers has its own window of ideal bandwidth performance. VEST supports encryption, single-pass authenticated encryption and collision-resistant hashing to minimise overall implementation costs for proprietary hardware applications. It follows that to achieve this we sacrifice generality of application. For example, VEST is not intended to compete in speed with software ciphers designed to be efficient on 8-bit smart cards. VEST is intended to reside as a robust cryptographic co-processor and link-level service relieving the smartcard processor of the complex encryption and authentication operations.

5.2.3 Message authentication codes (MAC)

For the education of the lay reader, we wish to note that unlike the common usage of collision-resistant hashing, there exists a strong tendency in communication protocols to compromise on the strength of message authentication codes to improve the remaining performance indexes.

There exists more than one method to generate a MAC using the AES. The traditional HMAC-AES (now also known as CMAC [54]) generates MAC images with its security limited to 64-bit as a function operating on 128-bit blocks. The HMAC mode requires two complete passes of the AES block cipher to perform encryption and authentication.

The NIST process selected a single-pass CCM [55] mode of operation, a universal hashing scheme, for authentication and confidentiality. Concern over the suitability of this mode of operation was expressed to NIST [56] by M. Bellare, P. Barreto, T. Iwata, P. Rogaway and R. Wagner. We say no more about this mode of operation as it is falling out of favour.

The Galois/counter mode of operation (GCM), a single-pass universal-hashing scheme, for authentication and confidentiality has been proposed and adopted in some recent standards. HMAC codes generated by universal hashes are not ideal in respect to certain classes of attacks [44]. For completeness, we survey the only detailed implementation of GCM known to the authors. For AES to support GCM, an estimate 25% to 66% circuit area increase is estimated over an encryption-only cipher implementation. The GCM accumulator is not an independently secure operation without the assistance of the AES cipher.

As described elsewhere, VEST can operate in a single-pass authenticated encryption mode that exhibits several desirable properties:

- Message authentication operates at the same speed as encryption
- It requires negligible area and power consumption overhead
- The VEST accumulator is a cryptographically secure primitive in it's own right
- The MAC lengths range from 160-bit to 512-bit in length, offering 80-bit to 256-bit security respectively

VEST primitives offer no-compromise authentication services.
VEST authenticated encryption has a stronger security rating than the AES.

5.2.4 Area exploration of a GCM universal hash implementation in ASIC

Designs	Geometry	Gates	Bus Width	Clock rate (MHz)	Throughput (Mb/s)	Latency
Iterative AES	0.18	29,436	128	276	3530	10
Pipelined AES	0.18	287,184	128	282	36090	1
GHASH	0.18	78,974	128	271	34690	1
	Total	***395,594***				

It is not possible at this time to perform an extensive analysis of GCM hardware suitability without performing significant lab work, as detailed published information on hardware requirements of GCM is extremely limited. Specifically, we were only able to find one implementation [58] that clearly delineates individual module resource requirements. This implementation is architecturally optimised to achieve the near upper bounds for the GCM algorithm on ASIC 0.18 geometries.

The iterative AES module is used in the cipher to decouple the generation of key-dependent constant used in the GHASH operation. The pipelined AES module is dedicated to generating key-stream material. The GHASH module is the accumulator for the GCM algorithm. The heart of the accumulator is a 128-bit parallel GF(2^{128}) multiplication operation. The multiplication operation cannot be pipelined to improve performance.

Designs	Gates	Overhead Gates	Clock rate (MHz)	Throughput (Mb/s)	Mbps / KGate	Latency
GCM Decryption	446,108	50514	271	34690	77.7	11
GCM Encryption	463,328	67734	271	34690	74.9	12
GCM Enc or Dec	498,658	103064	271	34690	69.6	12

The three GCM Implementations, Encryption, Decryption and Enc/Dec modules incorporate the first three modules, namely the Iterative AES, Pipelined AES and GHASH. There appears to be a significant and non-trivial overhead that cannot be dismissed; we are unclear as to the function of this overhead.

We note the following additional properties of the implementation:
- The iterative AES module is approaching the upper bound performance on 0.18 geometries
- The pipelined AES implementation is carefully designed to match the performance of GHASH
- The GHASH module limits the maximum speed achievable by GCM systems.

Area Requirements:

The GHASH module implementing the addition, multiplication and MAC image collection is about a quarter of the size over-and-above the requirements for a fully unrolled pipelined implementation of the AES. This is a non-trivial increase in circuit area or power-consumption. When we compare a complete encryption-only GCM module with CTR-only encryption, we find a 1.6 times increase in the circuit area. As we have no other figures available for comparison, we estimate approximately 25% to 66% increase in circuit area over the encryption-only module to support GCM mode of operation.

5.2.5 Collision-resistant hashing

The AES standard has a fixed block length of 128-bits. The security of hash images generated using the AES is limited to 64-bit regardless of the key length. The Rijndael cipher specifications [71], a subset of which was subsequently standardised as the AES cipher, clearly stated that 128-bit block lengths are not suitable for collision-resistant hashing. In contrast, VEST collision-resistant hash functions are cryptographically strong primitives with their security ranging from 80-bit to 256-bit.

5.3 Comparison of VEST and AES implementations

5.3.1 Comparison of the smallest VEST and the smallest AES FPGA implementations

Author	Product	F()	Device	Sec	Mode	Slices	FF	SRAM kbit	10 MHz	Static Mbps	Max Mbps
Tim Good, et al [35]	TINY	E/D	XC2S15-6	128	128	124	?(41)	4.4	0.3	2.2	n/a
			XC2VP2-7			264		0	n/a	n/a	60
Sean O'Neil	VEST-4	E	XC2S15-6	80	80	170	254	0	40	570.6	n/a
			XC2VP2-7							1500	6200

The TINY cipher instance is the smallest AES implementation in respect to slice count in our survey. The TINY AES implementation publishes static timing and performance characteristics. Due to limitations with the Spartan II power analysis tool, we have implemented TINY with select RAM (the Spartan-II is unusual in its support of 4 kilobit SRAM modules as opposed to 16 kilobit SRAM modules) and simulated power consumption on the Virtex-II Pro. The normalised area requirements are based upon the actual memory requirements for the TINY implementation.

[+] VEST-4 is 55% smaller than the normalised CLB area requirements [35] for TINY
[+] VEST-4 is 259 times faster than TINY for encryption operations on the XC2S15-6 architecture
[+] VEST-4 achieves 133 times the output per clock cycle
[+] VEST-4 is 130 times more power efficient when implemented using only combinatorial logic!
[*] Tiny supports inverse block cipher operations, which increases the area requirements over an encryption-only solution
[*] TINY is a minimal AES implementation and does not include any control logic to support different modes of operation
[X] TINY is in the high-risk category for AES side-channel attacks and does not advertise any hardware security measures

5.3.2 Comparison of the smallest VEST and the smallest normalised FPGA AES implementations

Author	Product	F()	Device	Sec	Mode	Area	FF	SRAM	10 MHz	Static Mbps	Max Mbps
IP Cores [31]	8-bit ultra compact encrypt	E	XC2VP2-7	128		240	?	0	8	104	1640
			XC2V250-5		128	236	?			?	1672
			0.18 ASIC			3K	n/a			80	64
Sean O'Neil	VEST-4	E	XC2VP2-7	80	80	170 slices	254	0	40	1500	6200
			XC2V40-5							900	6200
			XCV200E-8 (0.18 ASIC)							751	n/a
			0.18 ASIC x2			5K	n/a			1502	n/a

When we compare the 8-bit ultra compact core implemented on an XC2VP2-7:

[+] VEST-4 requires ~30% less CLB slices
[+] VEST-4 is 3.7 times more power efficient
[+] VEST-4 offers encryption that is 14.4 times faster than 8-bit ultra compact core
[+] VEST-4 is at least 20 times more efficient per slice
[+] VEST-4 achieves 5 times the output per clock cycle
[–] VEST-4 offers 80-bit encryption security compared to 128-bit encryption
[*] Both the VEST-4 and AES1 [31] cipher are implemented using only combinatorial and sequential logic operations, resulting in improved accuracy when heuristically estimating ASIC performance from these designs
[*] The 8-bit ultra compact core is a minimal AES implementation, and does not include any control logic to support different modes of operation
[X] The 8-bit ultra compact core is in the high-risk category for AES side-channel attacks and does not advertise any hardware security measures

When we compare the 8-bit ultra compact core implemented on an ASIC 0.18 geometry against a conservative heuristic 2x clock-speed increase for VEST over its 0.18 geometry FPGA design:

[+] VEST-4 offers encryption that is >18.5 times faster than 8-bit ultra compact core
[+] VEST-4 is at least 11 times more efficient per gate
[–] VEST-4 requires 60% more ASIC gates (probably due to the large register requirements)

5.3.3 Comparison of the smallest normalised FPGA AES implementation and equivalent rated VEST

Author	Product	F()	Device	Sec	Mode	Area	FF	SRAM	10 MHz	Static Mbps	Max Mbps
IP Cores [31]	8-bit ultra compact encryption	E	XC2VP2-7	128	128	240	?	0	8	104	1640
			XC2V250-5			236	?			?	1672
			0.18 ASIC			3K	n/a			80	64
Sean O'Neil	VEST-8	E	XC2VP2-7	128	128	366 slices	384	0	80	2800	6000
			XC2V40-5							900	6200
			XCV200E-8 (0.18 ASIC)							1312	n/a
			0.18 ASIC x2			9K	n/a			2624	n/a

When we compare the 8-bit ultra compact core implemented on an XC2VP2-7:

[+] VEST-8 is 3.6 times more power efficient
[+] VEST-8 offers encryption that is 26.9 times faster
[+] VEST-8 is at least 20 times more efficient per slice
[+] VEST-8 achieves 10 times the output per clock cycle
[=] VEST-8 offers 128-bit secure encryption, as does AES1
[–] VEST-8 is ~55% larger than the 8-bit ultra compact encrypt core
[*] The 8-bit ultra compact core is a minimal AES implementation, and does not include any control logic to support different modes of operation
[X] The 8-bit ultra compact core is a high-risk category for AES side-channel attacks and does not advertise any hardware security measures

When we compare the 8-bit ultra compact core implemented on an ASIC 0.18 geometry against a conservative heuristic 2x clock-speed increase for VEST over its 0.18 geometry FPGA design:

[+] VEST-4 offers encryption that is >18.5 times faster
[+] VEST-4 is at least 11 times more efficient per gate
[–] VEST-4 requires 60% more ASIC gates (probably due to the large register requirements)

5.3.4 Comparison of the fastest VEST and the fastest FPGA AES ENCRYPT implementations

Author	Product	F()	Device	Sec	Mode	Slices	FF	SRAM kbit	10 MHz	Static Mbps	Max Mbps	pW-S (J=85)
Tim Good, et al [35]	3LUT	E/D	XC3S2000-5	128	128	17425	~5000	0	1280	~~25107~~	16384	17.8
Sean O'Neil	VEST-32	E	XC3S250-5	256	256	954	768	0	320	4700	37440	1.99

[+] VEST-32 is 2.2 times more power efficient overall than the encryption-only 3LUT-AES-128
[+] VEST-32 is 5.2 times more efficient per slice at generating output
[+] VEST-32 offers 256-bit strong encryption compared to only 128-bit encryption
[+] VEST-32 requires a minimum Spartan-3 chip size of “XCS200” to support the minimum number of slices, which is 4 sizes smaller than the “XC3S2000” chip minimally required for 3LUT-AES-128
[+] VEST-32 is 18 times smaller
[+] VEST-32 performs **authenticated** encryption 13 times faster for a single data stream than 3LUT-AES-128
[–] VEST-32 has a top speed (4.700 Mb/s) that is significantly slower than the 16,834 Mb/s achievable by the 3-LUT-AES in theory and only 3.4 times slower for encryption in production environments where thermal constraints are satisfied
[–] VEST-32 releases 4 times less output per clock cycle
[*] The VEST-32 and 3LUT-AES-128 ciphers [35] are implemented using only combinatorial and sequential logic operations, resulting in improved accuracy when heuristically estimating ASIC performance from these designs
[X] 3LUT-AES cannot achieve the static timing / bandwidth claimed, because it is reasonably argued to be unrealistic in most real-world applications by significantly exceeding the maximum Junction temperature of 85°C when operating with a commercial ambient temperature of 55°C and a ThetaJA of 12.8°C

It is clear that VEST-32 is significantly more area and power efficient than the fastest FPGA AES cipher implementation found in this survey, especially for performing **authenticated** encryption. It is reasonably agued than an encryption-only implementation of the 3LUT-AES-128 would improve static timing, reduce area and reduce power consumption requirements for ECB or counter mode of operation. Along the same line of reasoning, the area requirements would by necessity increase to support 256-bit key sizes in AES to match the VEST-32 security.

5.3.5 Comparison of the fastest VEST and the fastest FPGA AES-FEEDBACK implementations

Author	Product	F()	Device	Sec	Mode	Slices	FF	SRAM kbit	10 MHz	Static Mbps	Max Mbps	pW-S (J=85)
Helion Tech [7]	Fast-Enc	E	XC4Vxxxx-11	128	128	447 (5625)	?	180 (0)	116	2548	14894	1.5
Sean O'Neil	VEST-32	E	XC4VLX25-11	256	256	954	768	0	320	7800	22720	2.82

[+] VEST-32 has a top encryption speed that is 3 times faster than Fast-Enc
[+] VEST-32 achieves 2.7 times output per clock than Fast-Enc
[+] VEST-32 is at least 50% more power efficient*
[+] VEST-32 offers 256-bit strong encryption compared to only 128-bit encryption
[+] VEST-32 offers 256-bit authenticated encryption that is 2.7 times faster than a 64-bit MAC by Fast-Enc

* Fast-Enc extensively employs the use of SRAM modules that are particularly efficient in FPGA when compared with combinatorial logic s-boxes implemented in configurable logic blocks. Fast-Enc product includes real-time hardware key-expansion.

5.4 Conservative comparison of ASIC VEST-32 and an equivalently sized ASIC AES implementation

Author	Product	F()	Device	Geometry	Sec	Mode	Rounds	Area	K gates	SRAM kbit	10 MHz	MHz	Static Mb/s
Helion Tech [7]	Fast Enc	E	ASIC	0.18	128	128	11	n/a	27	0	116	250	2909
					n/a	*256*	*15*	*n/a*	*n/a*	*0*	*85*	*250*	*~2133*
Sean O'Neil	VEST-32	E	Virtex-E XCV200e-7	0.18	256	256	1	954 CLB 768 FF	n/a	0	320	102	3264
			ASIC					n/a	~22	0	320	102	3264
			ASIC x2									204	6528

[*] VEST-32 figures are based on the conservative 2x speedup estimate over FPGA implementation
[+] VEST-32 on the low-cost Spartan-IIE based on a 0.18 ASIC geometry is 1.3 times faster than the standard-cell ASIC hardware implementation of AES-128
[+] VEST-32 is 2.6 times faster than the ASIC hardware implementation of AES-128 in less circuit area
[+] Based on the characteristics of the Helion-tech FPGA implementations, we can estimate the throughput of an AES-256 as 2133 Megabit/s
[+] VEST-32 in FPGA is 1.5 times faster than the estimated performance of AES-256
[+] Based on the immediately preceding assumptions, VEST-32 with a 2x speed-up in ASIC is 3.0 times faster
[+] VEST-32 offers 256-bit encryption security compared to AES 128-bit
[+] VEST-32 authenticated encryption mode in ASIC is conservatively estimated have a top speed of 2.6 to 3.0 times faster than this implementation of encryption-only AES

PART 6
SELECTIVE COMPARISON IN RELATION TO SHA-2 IMPLEMENTATIONS

6.1 Comparison of VEST-8 in relation to the fastest SHA-256 in FPGA

Author	Product	F()	Device	Sec	Rounds	Slices/ DFF	K gates	SRAM 16 kbit	10 MHz	MHz	Static Mb/s	Max Mb/s
Helion Tech [8]	SHA-256	H	XC4VLX25-11	128	66	834/? (256)	16	1	77.5	140	1,086	10,085
Sean O'Neil	VEST-8	H	XC4VLX25-11	128	1	366 / 348	0	0	80	312	2,500	19,200

[+] VEST-8 requires 2.2 less CLB slices and no SRAM
[+] VEST-8 is 1.9 times more power efficient
[+] VEST-8 is 2.3 times faster than HELION-SHA-256
[+] VEST-8 is 5.2 times more efficient per CLB slice
[=] VEST-8 offers 128-bit collision resistant hash
[+] VEST-8 encryption is 4.6 times faster than HELION-SHA-256 in a counter-mode of operation

6.2 Comparison of VEST-32 in relation to SHA-512 in FPGA

Author	Product	F()	Device	Sec	Rounds	Slices/ DFF	K gates	SRAM 4 kbit	10 MHz	MHz	Static Mb/s	Max Mb/s
Francis Crowe [13]	Unrolled-4	H	XCV2000E-?	256	20	3506/? (292)	? 32	? 8	533	10	533	n/a
			XCV250-5 (normalize)							n/a	n/a	7195*
Sean O'Neil	VEST-32	H	XCV200E-7	256	1	964 / 768	0	0	80	109	872	n/a
			XCV250-5							150	1200	8000

* Our EDA workflow does not support the legacy Virtex architecture. The second fastest implementation was selected for comparison. Due to limitations with the Virtex-E power analysis tool, we have estimated the power consumption of UNROLLED-4 implementation using the Virtex-II architecture. The power figures are hard to calculate as the number of registers is not disclosed in the paper; consequently we have estimated the number of registers as 1/3 the logic CLB, divided by 4 because the loop has been unrolled 4 times between registers. To complicate analysis further, the number of SRAM modules is not clearly disclosed in the paper. The critical-path depth of the above circuit is the deepest surveyed in this paper; consequently, it is possible that the dynamic power consumption will vary significantly from our static-timing estimates for this circuit.

[+] VEST-32 requires 3.6 less CLB slices and no SRAM
[+] VEST-32 is 2.2 times faster
[+] VEST-32 is 5.9 times more efficient per CLB slice
[+] VEST-32 is estimated to be 10% more power efficient than this implementation
[=] VEST-32 offers 256-bit collision resistant hash
[+] VEST-32 encryption is 18 times faster than UNROLLED-4 in a counter-mode of operation
[+] VEST-32 offers 256-bit authenticated encryption support at full encryption speeds

PART 7
APPLICATIONS

7.1 Low power applications in FPGA

Low power applications require precise detailed power analysis of each module implemented on the chip. In order to achieve greater accuracy in power consumption estimates, dynamic gate-level simulation of the circuit must be performed. Such extensive dynamic power analysis is beyond the scope of this paper. We believe that the static power analysis alone is an objective method allowing us to compare relative efficiency of different FPGA designs with an acceptable degree of accuracy, and also static power analysis effectively measures the base-line power efficiency of FPGA cipher implementations, or in other words the amount of hardware resources required to generate each bit of ciphertext output.

According to our power analysis, VEST ciphers are consistently more power-efficient than all the FPGA AES implementations chosen for this survey from fundamentally different application categories. This natural power efficiency of VEST ciphers is an inherent property and is not owed to some clever implementation techniques: VEST ciphers simply perform more work for the same amount of consumed energy.

A significant portion of power consumption in many circuits is attributed to intermediate transistor transitions before a circuit stabilises between clock cycles. The ability of FPGA design to control this influence is limited for the following reasons:

1. Logic of FPGA implementations must be mapped to the look-up-table modules of the design, limiting variation in power consumption between cipher implementations
2. Glitch minimisation techniques available in FPGA are very crude, hence it is not possible to reduce the intermediate transitions within a single LUT module
3. LUT modules have a significant fixed number of transistors in their implementation that cannot be reduced
4. A single input toggle to a LUT performing an S-Box (or its equivalent) will result in a 50% toggle rate on its output on average
5. We estimate that over 80% of the combinatorial logic of most cipher implementations surveyed in this paper is allocated to manipulating pseudo-random data sources
6. The best method to reduce power in FPGA designs is using SRAM to implement table look-up operations
7. We were unable to identify any papers discussing FPGA-based low-power optimisations for S-Box or cipher design using synchronous designs

FPGA static power analysis tools are unable to catch this dynamic behaviour in their estimations. VEST ciphers have a shorter critical path depth and lower fan-in for each non-linear bit of updated state than the AES implementations, which suggests that VEST will be the least vulnerable to glitch overheads of all the cipher implementations surveyed here. Glitch masking in FPGA can be best performed by limiting the logic depth of Boolean functions in order to limit the avalanche of transitions that flow forward from a single-bit state change. VEST ciphers have a logic depth of only two (2) LUT elements in Xilinx, which is probably the best glitch minimisation that could be reasonably anticipated in FPGA architectures. The clocked logic masking in VEST is achieved in principle by using registers, and does not impede on the cryptographic work performed by the LUT elements.

Further power (and security) improvement in FPGA may be achieved by using asynchronous logic techniques [61], [62], [63].

7.2 Low power applications in ASIC

We believe that the power efficiency superiority of VEST ciphers in FPGA designs will also translate to its superiority ASIC designs. We acknowledge the work of [60] that illustrates that the power-consumption of ASIC implementations can range by up to a factor of three between the cheapest and most power hungry AES S-Box tables depending on the strategy used to implement the AES S-Box operations. (It is questionable if any of the particularly inefficient techniques surveyed are likely to be found in real-world designs).

It is reasonable to believe that a naive VEST ASIC implementation will achieve significant power reductions through optimised mapping to specific standard-cell libraries, choice of process, voltage reduction, high-Vt transistors, multi-Vdd, power gating, substrate biasing, clock gating, register clustering, etc. Ideally, low power, high-security ASIC implementations of VEST will be implemented with asynchronous logic techniques.

The power-efficient characteristics of VEST primitives will be a significant consideration in all hardware designs.

7.3 Minimal resource applications

As the size of AES and SHA implementations decrease, the power-to-cipher-text output increases as a function of increased logic overhead of a highly iterated cipher design. VEST root families are purpose-built constructions targeted explicitly for a particular area / security / bandwidth bracket. Consequently, the low-area VEST-4 and VEST-8 implementations are extremely tight constructions with minimal implementation overheads.

Both VEST-4 and VEST-8 are roughly 3.5 times more power efficient than minimal area encryption-only AES-128 solutions in FPGA and 7 times more power efficient when encryption combined with message authentication. We believe that VEST primitives should be exceptionally interesting to applications seeking the minimal encryption overheads.

VEST-4 and VEST-8 ciphers offer several other advantages:

- 4-bit and 8-bit bus per-clock bus widths simplifying hardware implementations
- Cryptographic support in applications with extremely tight power budgets
- Significantly higher per-module encryption bandwidth
    - Consequently reducing the total area costs in many applications
- Collision-resistant hashing suitable for digital signatures and authentication purposes that is significantly more area and power efficient than SHA-2 or similar hash functions
- Inherently stronger protection against side-channel and glitch attacks
- Authenticated encryption at the same security level, speed, area and power consumption as encryption alone

7.4 Identity Authentication systems such as RFID

It is widely felt by the cryptographic community that 160 bits is the absolute minimal hash length suitable for medium-term authentication services and 256-bit hash length is a minimum for general use and longer-term security.

The full SHA-1 hash claiming 80-bit security was reduced by a recent attack [64] to being at most 69-bit secure. According to Bruce Schneier, this attack is “just on the far edge of feasibility with current technology” [65].

AES offers maximum 64 bits of security for collision-resistant hashing, which does not provide sufficient security with modern computational capabilities, even for short-term commercial applications. It makes AES not suitable as a general-purpose cryptographic hash function.

For RFID systems and other designs, this clearly raises the question of what is a suitable low-area hash function. The smallest ASIC implementation of SHA-256 occupies 21K ASIC gates. An ASIC implementation of SHA-512 would require a minimum of 40K ASIC gates. This is clearly not suitable for a very broad range of low-area applications such as inexpensive RFID devices.

VEST-4 can operate as an 80-bit secure collision-resistant hash function occupying approximately 5K ASIC gates.
VEST-8 can operate as a 128-bit secure collision-resistant hash function occupying approximately 9K ASIC gates.

The security level provided by the VEST-4 and VEST-8 ciphers and their low area allows them to cover the broadest range of low-cost applications providing medium-term and long-term security services.

Side Note: The recent paper [66] explores possible techniques that may improve resistance of MD-X and SHA-1 primitives against the pre-image attacks, although effectiveness of such techniques requires further analysis. VEST ciphers do not appear to be vulnerable to this broad class of attacks due to significant architectural differences that include in-built non-linear message expansion rendering techniques described in [66] unnecessary for VEST ciphers executed in hashing mode.

7.5 Chip-To-Chip High Assurance Systems

With the increased awareness of side-channel attacks, timing attacks, and attacks against the host-processing environment in general the protection of chip-to-chip communications in commercial applications is becoming increasingly important. The use of general-purpose software primitives has generally been considered prohibitive for this purpose. The low area, low power and low-latency characteristics of VEST present new opportunities for protection of inter-chip communications.

The authenticated encryption mode of operation of VEST ciphers is ideally suited for packet-based bus protocols with modest inter-packet gaps between packets.

For applications sensitive to real-time latencies, privacy may be sufficient in its own right for streaming data services. In these applications the authenticated mode of operation of VEST provides integrity operations required to ensure the correct operation of the system as a whole. For instance, HDTV requires privacy only for the audio-video data stream and both privacy and integrity services for the access control. A single VEST module allows achieving both goals seamlessly in

these applications.

For applications requiring the most robust operation, the VEST authentication can provide 256-bit secure message authentication combined with performance exceeding that of the AES or any SHA family member.

It is our vision that VEST ciphers would initiate the development of a new generation of high-assurance systems that could not be achieved previously using general-purpose software primitives. Deployed in public infrastructure and mission-critical systems, high-assurance systems incorporating VEST primitives would incrementally improve the robustness of complex products and other associated technologies in the face of natural or malicious interference.

PART 8
CONCLUSIONS

8.1 Foreword

Having performed the most extensive survey of AES and SHA implementations of its kind, we believe that the conclusions of this survey map closely to the actualities of the academic and commercial domains. For specific performance-point comparisons, please review section 6. Given the scope and breadth of the survey and the sometimes very large differences noted in area, performance, etc., we feel justified in making the following broad sweeping claims without limiting them to any particular application or specific problem domain.

8.2 Conclusions for FPGA

8.2.1 Encryption/decryption

- VEST ciphers are more power efficient than all the measured AES implementations
- VEST ciphers perform authenticated encryption for any given bandwidth generally around two (2) to four (4) times more power efficiently than all the measured AES implementations performing encryption only
- VEST ciphers require less CLB and SRAM resources to perform authenticated encryption for any given bandwidth than all the measured AES implementations, most of which are encryption-only
- VEST-16 and VEST-32 ciphers are ~1.8 to ~3.4x faster respectively than the fastest measured iterated AES implementation
- VEST ciphers do not utilise SRAM look-up-table operations, freeing up precious FPGA resources

8.2.2 Message Authentication

- All VEST ciphers offer stronger authenticated message security than is offered by the AES standard
- The single pass authenticated encryption mode of VEST primitives is achieved with negligible overhead
- VEST ciphers achieve any given bandwidth generally around four (4) to eight (8) times more power efficiently than all the measured AES implementations performing two-pass authenticated encryption (HMAC)
- VEST-8 performs in authenticated encryption mode at roughly the same speed as the fastest AES feedback mode of operation with significantly less power, CLB and SRAM resources
- Authenticated encryption mode of the VEST-16 and VEST-32 ciphers is ~1.8 to ~3.4x faster respectively than the fastest measured iterated AES implementation while utilising less chip resources than the AES and enabling new high-bandwidth high-security applications

8.2.3 Collision-resistant hashing

- The AES standard is not suitable for use as a collision-resistant hash
- VEST-4 offers the smallest collision-resistant hash function known to the authors at the time of publication
- VEST-8 offers 128-bit secure collision-resistant hashing about 2.3 times faster than SHA-256 with less than half the CLB and not requiring SRAM
- VEST-32 offers 256-bit secure collision-resistant hashing about 1.5 times faster than SHA-512 with less than half to a third CLB and not requiring SRAM
- VEST ciphers are more power efficient than all surveyed SHA implementations

8.2.4 Multi-function design

- VEST ciphers offer area efficient, power efficient, high-performance, high-security encryption, authenticated encryption and collision resistant [keyed and unkeyed] hash performance in a singular module
- AES ciphers cannot perform collision resistant hashing
- VEST ciphers achieve faster encryption, authenticated encryption and collision resistant hashing than can be achieved through Counter mode, HMAC mode and Hashing mode of operation respectively for the SHA-2 family of hash functions
- VEST ciphers offer significantly faster encryption and dramatically faster authenticated encryption in a single module in less area and with less power than can be achieved with a single SHA-2 module

8.3 Conclusion ASIC

- VEST ciphers appear to offer exceptional performance, with a surveyed FPGA implementation of VEST-32 offering 256-bit authenticated encryption outperforming an ASIC dedicated AES cipher implementation on the same 0.18 geometry by 1.3 times

- VEST ciphers appear to offer extremely compact constructions in standard-cell implementations in respect to their projected performance from FPGA designs
- The performance advantages in FPGA are reasonably believed to translate to excellent characteristics when implemented in ASIC flows

8.4 Family Keying

During the research for our extensive survey of published academic and commercial ciphers we did not identify a single stream cipher or block cipher that implements family-keying as a standard feature. We note that the TWOFISH cipher by Bruce Schneier proposes a method of family keying in the specifications but we are unaware of any software or hardware implementations of this feature at the time of publication.

8.5 Forward Looking

The Round-2 VEST submission to the eSTREAM is reasonably projected to improve the power efficiency of cipher implementations, reduce latencies and include a number of other general improvements strengthening the design.

8.6 Acknowledgments

Benjamin Gittins is the principle author of this paper. Howard Landman advised concerning and authored parts of the text relating to the power calculations and thermal issues for FPGA. Landman also performed an independent search for 150 highest-performing general-purpose cipher implementations that was partially incorporated in this document. Sean O'Neil was responsible for ensuring the correctness of cryptographic claims and significantly improving overall clarity of the text for the technical community. Ron Kelson is responsible for ensuring the document satisfied all due-process requirements and for significantly improving the overall clarity of this text for its wider audience.

The authors of this paper would like to thank Helion Technology for supplying detailed technical data-sheets on their range of excellent AES and SHA implementations in FGPA, and for independently reviewing a draft version of this paper.

8.7 References

[1] R.B Lee et al, "Efficient permutation instructions for fast software cryptography". IEEE Micro, 21(6):56-69, December 2001.

[2] Z. Shi et al., "Arbitrary bit permutations in one or two cycles" in the Proceedings of the 15th International Conference on Application-Specific Systems, Architectures and Processors, pages 237-247, June 2003.

[3] Alireza Hodjat, Ingrid Verbauwhede, "Minimum Area Cost for a 30 to 70 Gbits/s AES Processor", Proceedings of IEEE computer Society Annual Symposium on VLSI, Pages: 83-88, February 2004 (ASIC).

[4] Alireza Hodjat, Ingrid Verbauwhede, "Speed-area trade-off for 10 to 100 Gbits/s throughput AES processor", IEEE Proceedings of The Thrity-Seventh Asilomar Conference on Signals, Systems & Computers, Volume: 2 , Pages: 2147 - 2150, November 2003 (ASIC).

[5] Alireza Hodjat, Ingrid Verbauwhede, "A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA", IEEE Symposium on Field-Programmable Custom Computing Machines, April 2004.

[6] Kimmo U. Järvinen, Matti Tommiska, Jorma Skyttä, "A fully pipelined memoryless 17.8 Gbps AES-128 encryptor", FPGA 2003, Proceedings of the ACM/SIGDA International Symposium on Field Programmable Gate Arrays, February 23-25, 2003, Monterey, CA, USA. ACM, 2003.

[7] "AES Core for FGPA and ASIC", Helion Technology, http://www.heliontech.com/core2.htm

[8] "AES Core", North Pole Engineering. http://www.northpoleengineering.com/aescore.htm

[9] "SHA-256 Core for FGPA and ASIC", Helion Technology, http://www.heliontech.com/core6.htm

[10] Norbert Pramstaller and Manfred Aigner, "A Universal and Efficient SHA-256 Implementation for FPGAs". In Proceedings of Austrochip 2004, pp.89-93, ISBN 3-200-00211-5, Villach, Austria, October 8th 2004.

[11] "256-bit SHA Cryptoprocessor Core", CAST, May 2005. http://www.cast-inc.com/cores/sha-256/cast_sha-256-x.pdf

[12] N. Sklavos, O. Koufopavlou, “Implementation of the SHA-2 Hash Family Standard”, The Journal of Supercomputing, 31, 227–248, 2005.

http://www.vlsi.ee.upatras.gr/~sklavos/Papers/Papers05/Kluwer05_Super_SHA2.pdf

[13] Francis Crowe, “Single-Chip FPGA Implementation of a 128-bit Cryptosystem", slide show presentation, Department of Electrical & Electronic Engineering, University College Cork, IRELAND

[14] Grembowski, T., Lien, R., Gaj, K., Nguyen, N., Bellows, P., Flidr, J., Lehman, T., and Schott, B. 2002. “Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512”. In Proceedings of the 5th international Conference on information Security (September 30 - October 02, 2002). A. H. Chan and V. D. Gligor, Eds. Lecture Notes In Computer Science, vol. 2433. Springer-Verlag, London, 75-89.

[15] “Digital Low Power Standard Cell Library for MOSIS TSMC CMOS 0.25 Process. Deep Sub-Micron Technology”, Tanner Consulting and Engineering Services, 1999.

http://www.mosis.org/cell-libraries/scn025-std-cells/mtsmd025dl.pdf

[16] Application Note 110, “Gate counting methodology for APEX 20K Devices”, Altera, August 1999. http://www.altera.com/literature/an/an110.pdf

[17] “SXLIB: A Portable CMOS Standard Cell Library”, ASIM/LIP6/UPMC laboratory, October 1999.

http://www-asim.lip6.fr/cgi-bin/czo/man2html?sxlib+5

[18] Mathew Kwan, “Reducing the Gate Count of Bitslice DES”, Cryptology ePrint Archive: Report 2000/051, August 2000, http://eprint.iacr.org/2000/051

[19] “AES Cores: Technical Data Sheet”, Cadence, July 2003, http://www.cadence.com/datasheets/AES_DataSheet.pdf

[20] “(Free) AES IP Core”, Asics.ws, Feburary 2004, http://www.opencores.org/projects/aes_core

[21] “Enhanced AES IP Core”, Asics.ws, July 2004, http://www.asics.ws/doc/aes_brief.pdf

[22] Alireza Hodjat, “An over 3 Gbits/s AES coprocessor in feedback and non-feedback modes of operation”, http://www.ee.ucla.edu/~ahodjat/AES/aes_modes.html

[23] Alireza Hodjat, Ingrid Verbauwhede, “Speed-area trade-off for 10 to 100 Gbits/s throughput AES processor”, 2003 IEEE Asilomar Conference on Signals, Systems, and Computers, November 2003. http://www.ee.ucla.edu/~ahodjat/AES/asilomar_paper_alireza.pdf

[24] “Hashing Algorithm Generator SHA-256: Technical Data Sheet”, Cadence, June 2003, http://www.cadence.com/datasheets/SHA256_Datasheet.pdf

[25] “SafeXcel IP: MD5/SHA-1/SHA-256 Accelerators”, Safenet, 2004, http://www.safenet-inc.com/Library/3/SafeXcel_MD5_SHA1_SHA-256_Accelerators.pdf

[26] Eli Biham, “A Fast New DES Implementation in Software”, proceedings of Fast Software Encryption - Fourth International Workshop, Haifa, Israel, Springer Verlag, pp. 260-272, 1997.

[27] “(Free) DES / Triple DES IP Core”, Asics.ws, July 2004, http://www.opencores.org/projects/des

[28] “CLP-11; Tiny AES Core; Preliminary Data Sheet”, Elliptic Semiconductor, 2004, http://www.ellipticsemi.com/CLP-11_40623.pdf

[29] Xilinx, San Jose, California, USA, “A simple method of estimating power in XC40000X1/EX/E FPGAs”, Application Brief XBRF 014 v1.0, 2002. http://direct.xilinx.com/bvdocs/appnotes/xbrf014.pdf

[30] Quartus II Handbook Version 5.0, “Section III. Power Estimation & Analysis”, Altera, May 2005, http://www.altera.com/literature/hb/qts/qts_qii5v3_03.pdf

[31] “Ultra-Compact Advanced Encryption Standard Core”, IP Cores Inc, April 2005. http://www.ipcores.com/AES1.pdf

[32] “Advanced Encryption Standard (AES) Core”, Algotronix, November 2004. http://www.algotronix.com/content/AES%20Core%20Complete.pdf

[33] “AES; Advanced Encryption Standard Core - Xilinx”, CAST, September 2005. http://www.cast-inc.com/cores/aes/cast_aes-x.pdf

[34] “AES: Advanced Encryption Standard Core – ASIC”, CAST, August 2005. http://www.cast-inc.com/cores/aes_e/cast_aes_e.pdf

[35] Tim Good, Mohammed Benaissa, “AES on FPGA: from the fastest to the smallest”, Proceedings of CHES 2005, pp. 427-440, LNCS 3659, Springer, 2005

[36] P. Chodowiec, K. Gaj, “Very Compact FPGA Implementation of the AES Algorithm”, Cryptographic Hardware and Embedded Systems (CHES 2003), LNCS Vol. 2779, pp. 319 – 333, Springer-Verlag, October 2003

[37] G. Rouvroy, F. X. Standaert, J. J. Quisquater, J. D. Legat, “Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications”, Proceedings of the international conference on Information Technology: Coding and Computing 2004 (ITCC 2004), pp. 583 – 587, Vol. 2, April 2004

[38] “Tiny AES Encryption and Decryption Cores”, Helion Technology, July 27, 2005.

[39] Université Pierre et Marie Curie, “Alliance, A free VLSI cad system”, http://www-asim.lip6.fr/recherche/alliance/

[40] Doug Whiting, Bruce Schneier, Stefan Lucks, and Frédéric Muller, “Phelix, Fast Encryption and Authentication in a Single Cryptographic Primitive”, submitted to eSTREAM 2005-04-29. http://www.ecrypt.eu.org/stream/ciphers/phelix/phelix.pdf

[41] Nicolas T. Courtois, “Cryptanalysis of Sfinks”, Report 2005/243, Cryptology ePrint Archive, 24 July, 2005. http://eprint.iacr.org/2005/243.pdf

[42] Sean O’Neil, Benjamin Gittins, "Authenticated Encryption Mode of VEST Ciphers", 28 October 2005

[43] M. Wegman and L. Carter. New hash functions and their use in authentication and set equality. Journal of Computer and System Sciences, 22:265279, 1981.

[44] David A. McGrew and Scott R. Fluhrer, "Multiple forgery attacks against Message Authentication Codes", Crypto EPRINT 2005/161, 31 May 2005. http://eprint.iacr.org/2005/161.pdf

[45] Adi Shamir, "Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies", Ç.K. Koç and C. Paar (ed.), Cryptographic Hardware and Embedded Systems - CHES 2000, Springer-Verlag, 2000 , LNCS , 1965 , 71-77

[46] Hemanth Satyanarayana, “AES-128 Crypto Core”, OpenCores http://www.opencores.com/projects.cgi/web/aes_crypto_core/overview

[47] Javier Castillo Villar, “AES-128/192”, OpenCores http://www.opencores.com/projects.cgi/web/systemcaes/overview

[48] Xilinx, “Xilinx: Power Consumption Tools”, http://www.xilinx.com/products/design_resources/design_tool/grouping/power_tools.htm

[49] N. Sklavos, and O. Koufopavlou, "On the Hardware Implementations of the SHA-2 (256, 384, 512) Hash Functions", proceedings of IEEE International Symposium on Circuits & Systems (ISCAS'03), Vol. V, pp. 153-156, Thailand, May 25-28, 2003 http://www.vlsi.ee.upatras.gr/~sklavos/Papers/Papers03/ISCAS03_SHA-2.pdf

[50] Helion Technology, “SHA-1, SHA-224, SHA-256 and MD5 Hashing, Tiny with HMAC”, July 14, 2005.

[51] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno, M. Stay, The Twofish Team's Final Comments on AES Selection, May 15, 2000. http://www.schneier.com/paper-twofish-final.pdf

[52] National Institute of Standards and Technology, “Status Report on the First Round of the Development of the Advanced Encryption Standard,” Aug 1999.

[53] Kai Schramm, Gregor Leander, Patrick Felke, Christof Paar, "A Collision-Attack on AES: Combining Side Channel- and Differential-Attack", CHES 2004, page 163-175. http://www.crypto.rub.de/imperia/md/content/texte/publications/conferences/aes_collisions.pdf

[54] Morris Dworkin, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication", NIST Special Publication 800-38B, May 2005, http://csrc.nist.gov/CryptoToolkit/modes/800-38_Series_Publications/SP800-38B.pdf

[55] Morris Dworkin, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", NIST Special Publications 800-38C, May 2004, http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf

[56] “NIST Responses to Public Comments on Draft SP 800-38C”, NIST, May 7, 2004 http://csrc.nist.gov/CryptoToolkit/modes/comments/800-38_Series-Drafts/RMAC/NIST_responses.pdf

[57] Sumio Morioka, Akashi Satoh. "A 10 Gbps Full-AES Crypto Design with a Twisted-BDD S-Box Architecture," iccd, p. 98, 2002 IEEE International Conference on Computer Design (ICCD'02), 2002.

[58] Bo Yang, Sambit Mishra, Ramesh Karri, "High Speed Architecture for Galois/Counter Mode of Operation (GCM)", http://eprint.iacr.org/2005/146.pdf

[59] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Mike Stay, David Wagner, and Doug Whiting, Improved Cryptanalysis of Rijndael, Fast Software Encryption, 2000 pp213–23. http://www.schneier.com/paper-rijndael.html

[60] Morioka S, Satoh A. “An Optimized S-Box Circuit Architecture for Low Power AES Design” in proc. of CHES 2002 pp. 172-186. http://ece.gmu.edu/crypto/ches02/talks_files/Satoh.pdf

[61] Asynchronous Circuit and System Design Group, “Desynchronization: an easy approach to Asynchronous design” http://www.ics.forth.gr/carv/async/demo/desynchronization/desynchronization.html

[62] Sklavos N and Koufopavlou O, "Asynchronous Low Power VLSI Implementation of the International Data Encryption Algorithm", proc. of 8th IEEE International Conference on Electronics, Circuits and Systems (ICECS'01) (Malta 2-5 September 2001) Vol. III pp. 1425-1428.

[63] Pui-Lam Siu, Chiou-Sing Choy, Butas J, Chan C F, "A Low Power Asynchronous DES" in proc. of 2001 Circuits and Systems Symposium (ISCAS 2001) 538-541 vol. 4, 347.

[64] X. Wang and Y.L. Yin and H. Yu. Finding Collisions in the full SHA-1. To appear in Advances in Cryptology – Crypto’05.

[65] B. Schneier, “Cryptanalysis of SHA-1”, http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html

[66] Michael Szydlo and Yiqun Lisa Yin, Collision-Resistant usage of MD5 and SHA-Message Preprocessing, Crypto EPRINT 2005/248, 18 Oct 2005. http://eprint.iacr.org/2005/248.pdf

[67] I. Damgård. A Design Principle for Hash Functions, In Advances in Cryptology – Crypto’89, Springer-Verlag, 1990.

[68] R. Merkle. One Way hash Functions and DES, In Advances in Cryptology –Crypto’89, Springer-Verlag, 1990.

[69] Y. Tsunoo et at, “Distinguishing Attack with Chosen Initialisation Vector Against VSC128”, ECRYPT - The State of the Art of Stream ciphers, October 2004.

[70] S. O’Neil, “Vector Stream Cipher instant key recovery”, Synaptic Labs, September 2004.

[71] Daemen, and Rijmen, V.: AES proposal: Rijndael. http://carc.nist.gov/encryption/aes/rijndael/Rijndael.pdf

[72] Altera, "Stratix II vs. Virtex-4 Power Comparison & Estimation Accuracy", August 2005, ver. 1.0, http://www.altera.co.jp/literature/wp/wp_s2v4_pwr_acc.pdf

APPENDIX A
FPGA MEASUREMENTS

A.1 Measuring the area usage of a static implementation of VEST

For the purpose of illustration, we measure the area requirements for the primary components of a low-area static implementation of VEST. It is reasonably required that the state of the cipher can be rapidly reset to a zero state. The finite state machine and key / IV storage are not included in these figures.

Cipher	Counter	Diffusor	Cipher Accumulator
VEST-4	163	10	83
VEST-8	163	10	211
VEST-16	171	10	331
VEST-32	171	10	587

[Table A.1] Distribution of internal state bits in VEST ciphers

A.2 4-to-1 look-up table architectures

Function	Instances	4-to-1	Slices	Total Slices
Counter: Bits	163			Floating *
Counter: 6-to-1 NL	16	3	1.5	24
Counter: Linear Input	16	1	0.5	8
Diffuser: Bits	10			
Diffuser: 6-to-1 XOR	10	2	1.0	10
Accumulator: Bits	83			
Accumulator: 6-to-1 NL	83	3	1.5	124
Combiner: 6-to-1 XOR	4	2	1.0	4
Encryption/decryption or Hash Total				***170***
Accumulator: Bits	96			
Accumulator: 6-to-1 NL	96	3	1.5	144
Combiner: 6-to-1 XOR	4	2	1.0	4
MAC Total				***148***

[Table A.2] Xilinx / Altera 4-to-1 tally

* The 163 bits of counter state can be register packed, exploiting the unused registers in the cipher and surrounding circuit areas

A.3 Altera 7-to-1 adaptable look up table architectures

Function	Instances	4-to-1	6-to-1	Total ALUT
Counter: Bits	163			Floating *
Counter: 6-to-1 NL	16		1	16
Counter: Linear Input	16	1	0.5	8
Diffuser: Bits	10			
Diffuser: 6-to-1 XOR	10		1	10
Accumulator: Bits	83			
Accumulator: 6-to-1 NL	83		1	83
Combiner: 6-to-1 XOR	4		1	4
Encryption/decryption or Hash Total				***121***
Accumulator: Bits	96			
Accumulator: 6-to-1 NL	96		1	96
Combiner: 6-to-1 XOR	4		1	4
MAC Total				***100***

[Table A.3] Stratix-II 6-to-1 tally

* The 163 bits of the counter state can be register packed to exploit the unused registers in the cipher logic and surrounding circuit areas. Each ALUT has two registers, of which one is used by 6-to-1 feedback functions. Most FPGA designs have an abundance of free registers, normally employing 2 to 3 ALUT for each register

A.4 Power Analysis of VEST on Stratix-II FPGA

Altera PowerPlay power analysis of synthesised VEST modules on the 3.3V Altera Stratix-II FPGA (EP2S15F484C3) at 85°**C** junction temperature with input pins, combinatorial logic and registers set at 50% duty cycle:

HDL description	**MHz**	**1**	**250**	**500**
1 register, (clock, d, q)	**mW**	522.64	532.44	542.28
VEST-4 cipher accumulator core (regional clock, d[9:0], q)	**mW**	523.95	603.94	684.94
VEST-8 cipher accumulator core (regional clock, d[9:0], q)	**mW**	524.57	713.84	904.12
VEST-16 cipher accumulator core (regional clock, d[9:0], q)	**mW**	525.28	817.21	1110.31
VEST-32 cipher accumulator core (regional clock, d[9:0], q)	**mW**	527.74	1081.44	1637.37

[Table A.4] PowerPlay results on synthesised modules

There is a large static power overhead in the Stratix-II FPGA amounting to 523 mW (the projected difference between 1 MHz and 0 MHz for the 1-register circuit is about 0.04 mW.) This static overhead is nearly independent of frequency and circuit size, but is strongly dependent on temperature, which would be expected for sub-threshold or gate leakage currents.

Thus, to a good approximation, there is no extra static power associated with implementing VEST-32 on the FPGA (at most a few mW). Almost all the power related to the VEST-32 circuitry is dynamic.

The power as a function of frequency (including data points not shown above) is perfectly linear. “Dynamic power increases linearly with the toggle rate as the capacitive load is charged more frequently for the logic and routing. The QuartusII models assume full rail-to-rail switching. For high toggle rates, especially on circuit output I/O pins, the circuit can transition before fully charging downstream capacitance. The result is a slightly conservative prediction of power by the QuartusII PowerPlay Power Analyzer.” [30]

By performing additional synthesis and power calculations we proceed to estimate the power requirements of the individual modules to estimate the lower-bound power requirements of a not-quite complete cipher instance. Our normalised power figures introduce a small margin of error:

Normalised power requirements	**MHz**	**1**	**250**	**500**
Approximate FPGA static consumption	**mW**	520.96	521.72	520.94
1 pin at 50% duty cycle	**mW**	0.56	5.36	10.67
VEST-4 cipher accumulator core (regional clock, no pins)	**mW**	< 1	23.26	46.61
VEST-8 cipher accumulator core (regional clock, no pins)	**mW**	< 1	133.16	265.79
VEST-16 cipher accumulator core (regional clock, no pins)	**mW**	< 1	236.58	471.98
VEST-32 cipher accumulator core (regional clock, no pins)	**mW**	< 1	500.76	999.06
16 Boolean functions for counters	**mW**	<1	4.50	8.98
181 registers for counters	**mW**	<1	30.09	60.10

[Table A.5] Measured power consumption of accumulators and module parts

Estimated lower bound power	**pW-S**	**MHz**	**250**	**500**
VEST-4 (counters + acc)	0.23	**mW**	57.85	115.67
VEST-8 (counters + acc)	0.67	**mW**	167.75	334.85
VEST-16 (counters + acc)	1.08	**mW**	271.17	541.04
VEST-32 (counters + acc)	2.14	**mW**	535.35	1068.12
VEST-4 (12 pins + counters + acc)	0.49	**mW**	122.17	243.71
VEST-8 (20 pins + counters + acc)	1.10	**mW**	274.95	548.25
VEST-16 (36 pins + counters + acc)	1.85	**mW**	464.13	925.16
VEST-32 (68 pins + counters + acc)	3.59	**mW**	899.83	1793.68

[Table A.6] Measured power consumption of counters, accumulator and pins

The above table illustrates the estimated lower-bound power consumption of a stand-alone cipher, and the cipher with LVTTL pins. The power consumption of the pins is a significant portion of the power consumption in all ciphers. Please note also that the cipher power estimates are indicative only, and do not include the FSM or linear components of the cipher at this time.

On a roughly complete VEST-32 cipher with 4 control pins, 32 data inputs and 32 data outputs, the slope is 3.59 pW/Hz or 3.59 pW-S, which gives the dynamic power expended to release one 32-bit word of cipher bits. Thus the dynamic power to run at a rate of N bits per second is (N/32)*3.59 pW. For example, 1 Gbps would require running at 31.25 MHz and use about 112.18 mW.

Since the (uncooled) package for this FPGA has a thermal resistance of 12.24**°C**/W, to stay within the 85**°C** temperature limit even at commercial max ambient of 55**°C** requires a total power dissipation of no more than (85-55)/12.24 = 2.45 W. At extended max ambient of 70**°C**, total power would be limited to 1.23 W.

If the total power budget of the FPGA chip was allocated to the VEST ciphers + static power overhead, the maximum number of clock-cycles available to the VEST ciphers is:

Upper Bound Clock Speed	**pW-S**	**Budget**	**1.23 W**	**2.45 W**
VEST-4 (pins + counters + acc)	0.49	**MHz**	1447	3937
VEST-8 (pins + counters + acc)	1.10	**MHz**	718	1753
VEST-16 (36 pins + counters + acc)	1.85	**MHz**	420	1042
VEST-32 (68 pins + counters + acc)	3.59	**MHz**	220	537

[Table A.7] Upper bound total clock budget for ciphers

Based on the above table, a complete VEST-32 cipher instance running on an uncooled Stratix-II FPGA at extended max ambient of 70**°C** has an upper bound of 220 MHz, ~7 gigabit/s. Alternatively under the same constraints it is possible to select two (2) independent VEST-32 instances at 110 MHz, still achieving a displacement of ~7 gigabits.

Upper Bound Bandwidth	**pW-S**	**Budget**	**1.23 W**	**2.45 W**
VEST-4 (pins + counters + acc)	0.49	**Megabit/s**	5788	15748
VEST-8 (pins + counters + acc)	1.10	**Megabit/s**	5744	14024
VEST-16 (36 pins + counters + acc)	1.85	**Megabit/s**	6720	16672
VEST-32 (68 pins + counters + acc)	3.59	**Megabit/s**	7040	17184

[Table A.8] Upper bound total bandwidth budget for ciphers

The above analysis highlights that it is important to calculate maximum clock-speed / bandwidth in relation to static-timing constraints, but also in relation to power budget.

A.5 Xilinx FPGA Power Analysis
A.5.1 On estimating the power consumption

To perform a comparison of VEST, AES and SHA implementations, we have used the Xilinx Web Power Tools to estimate the power requirements of cipher implementations.

The estimation of third party cipher implementations is particularly difficult as only partial information concerning the design operation is available. In particular, most independent applications do not document the register usage of cipher implementations.

We have biased all power figures **against** VEST ciphers by selecting the routing density as high on VEST designs, and medium on all other cipher implementations. Additionally we have strongly under-estimated the number of registers required for other cipher implementations where no figures are available.

A.5.2 Method

We have normalised the thermal characteristics of all compiled figures. The ThetaJA (Junction to Ambient) @ 0 LFM (Linear Feet per Minute) of Xilinx devices varies based upon the package. For the Virtex-4 chipset alone this value varies from 4.1 to 20.8°**C** / W. For sanity purposes, we normalise the ThetaJA at 12.8°**C** / W for all measurements. The absolute maximum junction temperature on the Virtex 2, Virtex 2 Pro and Virtex 4 is 125°**C** at 2.2V and <100°**C** at 3.3V. The absolute maximum temperature for the Spartan-II is 125°**C** at 3.3V (unless there is a typographic error in the documentation). Again, for normalisation purposes we ensure the Junction Temperature remains at 85°**C**.

Based upon the normalised metrics listed above, the total available power for 55°**C** and the extended 70°**C** are 2.45W and 1.23W respectively as per the power calculations for the Stratix-II devices.

When measuring the power characteristics of the ciphers, the estimates include Delayed Locked Loop circuitry set to the aggregate circuit clock speed. The average toggle rate of all logic and pin-data is set to 50%. Output load was set at 0pF. Output enable set 100% of time. The rate of input and output pin operation was carefully selected to match the expected bandwidth of the circuit simulated. Memories where required were selected as 9-bit read operations with 100% enable. (Power consumption for larger memory accesses do not differ significantly) Where available, process type was selected as worst-case.

The pW-S figures do not include the device quiescent power of an empty design with a junction temperature of 85°**C**.

APPENDIX B
ASIC MEASUREMENTS

B.1 Measuring the gate requirements for logic implemented in standard cell designs

We approximate our lower bound gate estimations using the "Digital Low Power Standard Cell library for MOSIS TSMC CMOS 0.25 Process" as a guide [15]. The MOSIS library counts gates as the number of transistors and does not take into account area usage. This matches the technique used by the Alliance EDA toolset for transistor reporting.

Gate Count	Function	Reference
0.250	Transistor	A Transistor
0.500	Inverter	MOSIS – mTSMd025DL – INV
1.000	2 input NAND	MOSIS – mTSMd025DL – NAND2
7.000	D-type FF (Simple)	MOSIS – mTSMd025DL – DFF_s
8.500	D-type FF (ACLR)	MOSIS – mTSMd025DL – DFFC_s
8.000	D-type FF (PRE)	MOSIS – mTSMd025DL – DFFP_s
9.500	D-type FF (ACLR/PRE)	MOSIS – mTSMd025DL – DFFP_s
8.000	D-type FF (CLR/PR/CLK EN)	Altera Apex 20 Flip Flop Gate estimate [14]
6.000	*D-type FF (Marketing gates)*	*Frequently cited optimistic gate estimates for FF*
3.000	2-to-1 Multiplexer	MOSIS – mTSMd025DL – MUX2
2.750	2-input XNOR gate	MOSIS – mTSMd025DL – XNOR2
2.750	2-input XOR gate	MOSIS – mTSMd025DL – XOR2
0.125	1 bit of ROM	Naïve Estimate
0.250	1 bit of 1-T RAM	Naïve Estimate RAM
1.500	1 bit of 6-T RAM	Naïve Estimate SRAM

[Table B.1] MOSIS gate metrics

Cipher	Counter	Diffusor	Cipher Accumulator	MAC Feedback
VEST-4	163	10	83	4
VEST-8	163	10	211	8
VEST-16	171	10	331	16
VEST-32	171	10	587	32

[Table B.2] Distribution of cipher-state

B.2 Estimates for dynamic 5-to-1 look-up tables with XOR

In some applications, it may be desirable to support dynamic family keying in hardware while maintaining high throughput of the cipher. We estimate the gate count required to implement the logic for each feedback function. We employ a simple shift register architecture chaining the 2^5 states of each Boolean function.

Function	Instances	Cell Name	Gates	Total Gates
32 LUT Values	32x	MOSIS-DFF_s	7.0	224.0
32-to-1 Multiplexer	31x	MOSIS-MUX2	3.0	93.0
2-to-1 Exclusive OR	1x	MOSIS-XOR2	3.0	3.0
				320.0

[Table B.2] MOSIS gate count estimates for dynamic family keying, per accumulator bit

B.3 Area requirements for static 5-to-1 look-up tables based on synthesis

We used the Alliance CAD System 5.0 to explore the transistor count on five of the 5-to-1 non-linear Boolean functions with a linear combiner found throughout the VEST cipher designs. The standard Alliance SXLIB [17] standard cell library was used, and the optimisations for all tools set for low area. The complete design flow including the Boolean Minimisation (BOOM), Binding and Optimising on Gates (BOOG), Local Optimisation on Nets (LOON), Placer for Standard Cells (OCP), Nero router, and Net-list extractor (COUGAR) were used to ensure realistic transistor counts. A small selection of functions has been arbitrarily selected for preliminary analysis:

Function	*S*	*J*	*B*	*G*	*P*	*W*	*T*	*M*	*O*	*R*
0x64A73A96	102	118	118	118	118	118	96	118	118	118
0xDA46704F	102	124	102	80	92	82	82	82	92	100
0x4790CDB6	98	138	96	96	96	98	88	98	96	96
0x631BCA96	118	152	100	108	100	100	110	106	100	110
0xA1FE2385	102	130	96	94	96	88	88	90	96	96
Average	*104.4*	*132*	*102.4*	*99.2*	*100.4*	*97.2*	*92.8*	*98.8*	*100.4*	*104*

[Table B.3] Transistor counts of some of the VEST feedback functions

Excluding the persistently worst-case optimisation '*j*', the overall average optimisation achieves a transistor count of 100, roughly 25 gates to implement the combinatorial logic of each 6-to-1 operation.

With simple search techniques using standard ASIC tools, we can expect to save roughly three (3) gates on each Boolean function implementation. Exhaustive exploration techniques [18] targeting a standard-cell library should result in further improvements.

The analysis above is oriented towards a minimum-area implementation. A high-speed implementation would have higher area due to buffering, gate resizing, and logic restructuring, but the amount of this increase would depend on the performance goals and the tools and libraries used.

B.4 Measuring the area usage of a static implementation of VEST-4

For the purpose of illustration, we measure the area requirements for the primary components of a low-area static implementation of VEST-4. It is reasonably required that the state of the cipher can be rapidly reset to zero. The finite state machine and key / IV storage are not included in these figures.

Function	Instances	Cell Name	Gates	Total Gates
Counter: Bits	163x	MOSIS-DFFC_s	8.500	1385.500
Counter: 6-to-1 NL	16x	Alliance Average	25.000	400.000
Counter: Linear Input	16x	MOSIS-XOR2	3.000	48.000
Diffuser: Bits	10x	MOSIS-DFFC_s	8.500	85.000
Diffuser: 6-to-1 XOR	10x	6 x MOSIS-XOR2	18.000	160.000
Accumulator: Bits	83x	MOSIS-DFFC_s	8.500	705.500
Accumulator: 6-to-1 NL	83x	Alliance Average	25.000	2075.000
Combiner: 6-to-1 XOR	4x	6 x MOSIS-XOR2	18.000	72.000
	(83+16)x	Avg - Optimised	3.000	-297.00
Optimised Non-linear				***4633.50***

[Table B.4] Gate count of the counter, diffusor, accumulator and linear combiner for VEST-4

Based on these figures, using conservative standard-cell library gate counts and preliminary synthesis results, our circuit is slightly larger than our original target goal and estimation of ~4K gates for the VEST-4 cipher in our original specification.

We have updated all the VEST area estimates based on our current research.

B.5 Estimating the ASIC performance of VEST ciphers

Currently a complete synthesis and static timing has not been performed on the VEST ciphers on an ASIC EDA toolset. (The Alliance toolset does not include a static timing analyser).

Analysis comparing FGPA and ASIC designs can be found in section 5.