ॐ भूर्भुवस्व तत् सवितूर्वरेण्यम् भर्गो देवस्य धीमहि धियो यो न प्रचोदयात्

Authenticated Encryption Mode of VEST Ciphers

28 October 2005

Sean O'Neil, Benjamin Gittins
CB Capital Management S.A.

Abstract: This paper demonstrates operation of the authenticated encryption mode in VEST ciphers. All VEST ciphers operating in the authenticated encryption mode with infinite error propagation provide keyed message authentication at the same speed as their keystream generation, with negligible overhead and maintaining their security ratings.

1. Introduction

Hardware stream ciphers were designed in the past mostly for encryption of highly unstable radio and POTS transmissions that introduced large numbers of errors and where error correction codes were an absolute necessity. Such ciphers had to apply their keystream to the plaintext linearly to eliminate error propagation to other bits allowing for faster recovery. Error propagation is a natural occurrence in all non-linear operations and if applied to the plaintext continuously without special techniques restricting it, error propagation tends to remain unlimited due to the non-linear feedback spreading errors throughout the cipher state incrementally. Although self-synchronising ciphers are an ingenious creation of that time allowing the code-maker to apply keystream to the plaintext non-linearly while limiting error propagation, infinite error propagation is essential for message or packet authentication.

Unlike thirty-forty years ago, encryption without authentication has very little or no use in communication security: protocols lacking secure authentication end up inevitably attacked and broken. Although modern block and stream ciphers may show acceptable software and hardware performance, their security and their performance [especially in hardware] are often significantly impaired by the authentication modules. To help rectify this deficit, VEST ciphers [1] offer two different methods to provide data authentication: a collision-resistant hash (described in the VEST cipher specification [1]), and the native authenticated encryption mode described below.

In the authenticated encryption mode, VEST ciphers [1] receive additional M bits of ciphertext as feedback into the core accumulator. Strongly unforgeable ciphertext authentication (encrypt-then-MAC) is chosen to ensure indistinguishability and non-malleability under both chosen ciphertext and chosen plaintext attacks against it, as well as integrity of both ciphertext and plaintext [2].

As in hashing mode, VEST ciphers produce H bits of MAC in H/M rounds after a final sealing stage. Although we do not recommend using MACs produced by VEST ciphers as collision-resistant hash values, they are sufficient for fast message authentication provided with negligible additional circuit area or power consumption overhead.

VEST cipher operation in authenticated encryption mode has infinite error propagation, although its operation is different from the mode of operation described in the US Patent 6,912,284 [3] that mistakenly authenticates plaintext merely combined with a weak LFSR counter output, thus only allowing the "encrypt and MAC" and "MAC then encrypt" methods. The former is proven insecure against all attacks only ensuring integrity of the plaintext and the latter only provides extra indistinguishability under chosen plaintext attacks [2]. In contrast to that, in the authenticated encryption mode of VEST ciphers, the plaintext is first linearly combined with the keystream produced by the output combiner of the cipher, and the resulting ciphertext value is

fed back into the core accumulator concatenated with the pseudo-random counter value, thus implementing the only secure "encrypt then MAC" authenticated encryption method.

At the time of publication of this paper, only VEST-8 is available with its core accumulator adapted to support authenticated encryption mode. VEST ciphers of all other sizes adapted to support authenticated encryption mode will be formally published in the updated Round-2 eSTREAM submission along with other minor security and performance related improvements and are available from the authors on request. No major structural changes are anticipated.

2. Authenticated Encryption

In addition to the parameters and variables listed in [1], the following parameters and variables are used in the authenticated encryption mode of the VEST ciphers:

e^j – bit j of the encrypted data (ciphertext)
u^j – bit j of the unencrypted data (plaintext)

2.1 Structure

In the authenticated encryption mode, VEST ciphers operate with the only structural difference being the ciphertext feedback into the core accumulator as shown below:

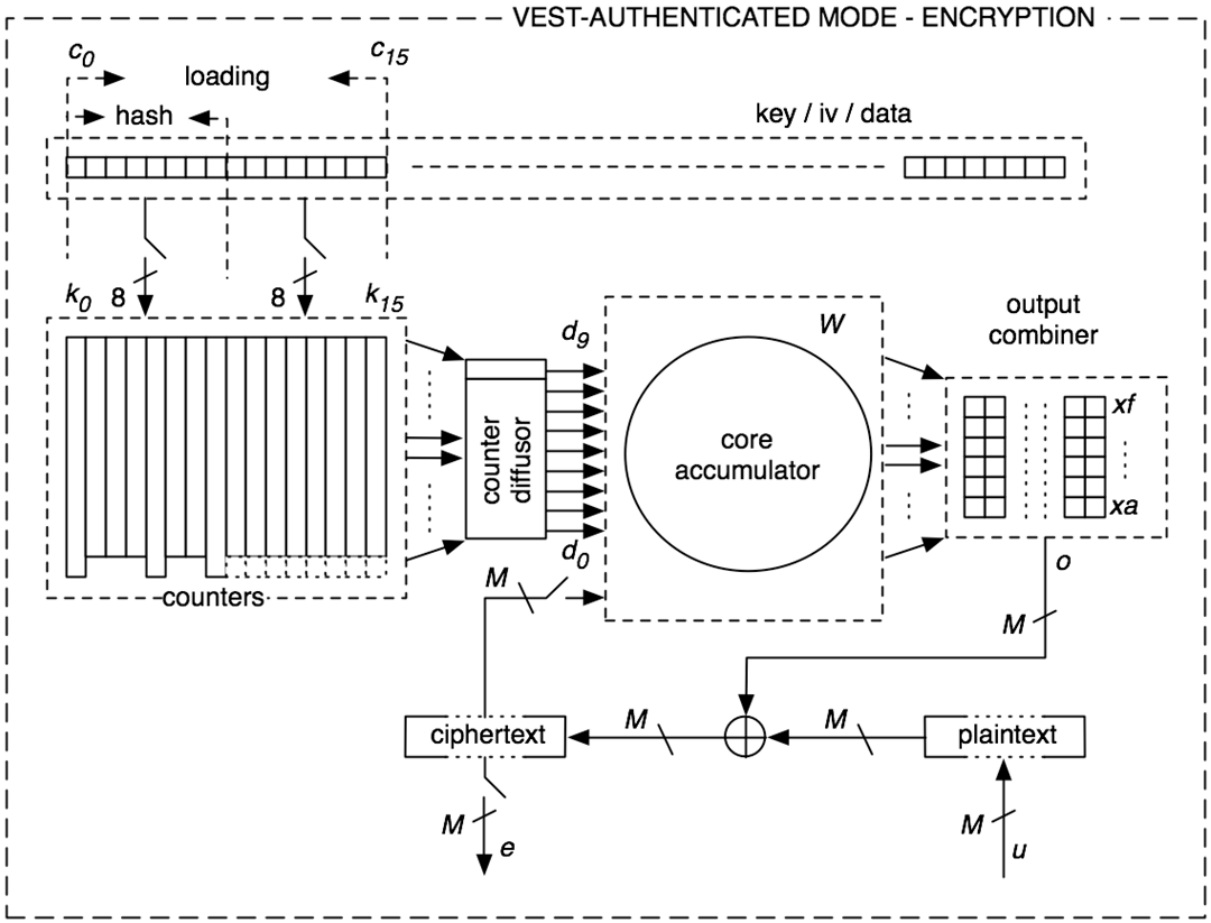

Fig 1. VEST structure in AE mode, encryption

Note: Parallel feedback of the core accumulator output produced in the previous round into bits 10 to M+9 of the core accumulator as shown above maintains its bijective operation.

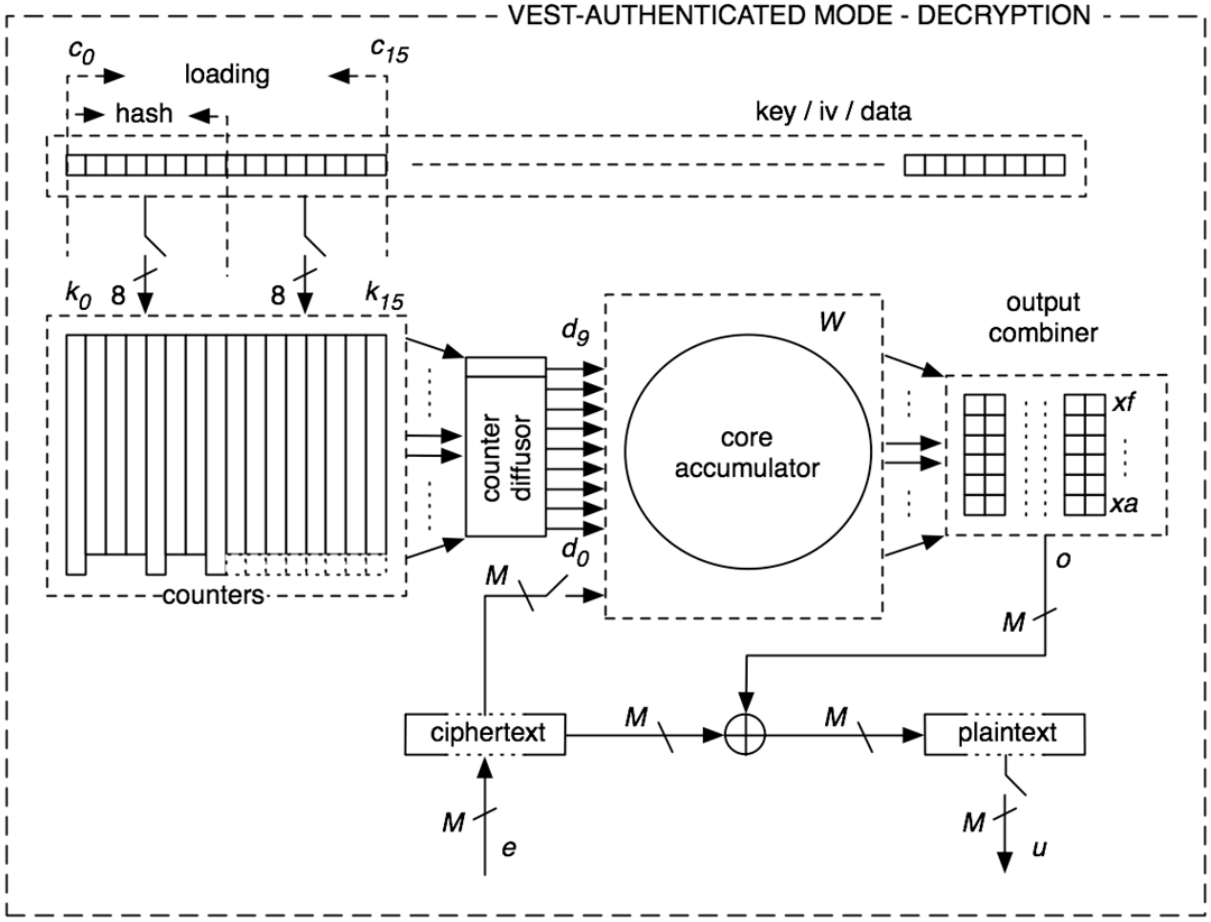

Fig 2. VEST structure in AE mode, decryption

2.2 Initialisation

The cipher is initialised according to the section 3.3.1 of [1], after which M bits of the "previous round ciphertext" e are set to 0 prior to encryption:

$$e^j = 0, -M \le j < 0.$$

Although authentication of associated data may be performed, the cipher is initialised with a key used for keystream generation, and therefore the keying process is sealed with the value 0x2B.

2.3 Operation

The authenticated encryption mode of operation of VEST ciphers can be summarised as follows:

[encryption]: $e^{(r-Ri)*M+j} = u^{(r-Ri)*M+j} + o^{(r-Ri)*M+j}, 0 \le j < M;$
[decryption]: $u^{(r-Ri)*M+j} = e^{(r-Ri)*M+j} + o^{(r-Ri)*M+j}, 0 \le j < M;$

$c_i^{r+1}{}_0 = g_i\,(c_i^r{}_0, c_i^r{}_1, c_i^r{}_2, c_i^r{}_6, c_i^r{}_7) + c_i^r{}_{B[i]-1},$
$c_i^{r+1}{}_j = c_i^r{}_{j-1}, 1 \le j < B_i, 0 \le i < 16;$
$x^{r+1}{}_{pj[5]} = f_j\,(x^r{}_0, x^r{}_1, x^r{}_2, x^r{}_3, x^r{}_4) + d^r{}_j, 0 \le \mathrm{j} < 5;$
$x^{r+1}{}_{pj[5]} = f_j\,(x^r{}_{pj[0]}, x^r{}_{pj[1]}, x^r{}_{pj[2]}, x^r{}_{pj[3]}, x^r{}_{pj[4]}) + x^r{}_j + d^r{}_j, 5 \le \mathrm{j} < 10;$
$x^{r+1}{}_{pj[5]} = f_j\,(x^r{}_{pj[0]}, x^r{}_{pj[1]}, x^r{}_{pj[2]}, x^r{}_{pj[3]}, x^r{}_{pj[4]}) + x^r{}_j + e^{(r-Ri-1)*M+j-10}, 10 \le j < 10+M;$
$x^{r+1}{}_{pj[5]} = f_j\,(x^r{}_{pj[0]}, x^r{}_{pj[1]}, x^r{}_{pj[2]}, x^r{}_{pj[3]}, x^r{}_{pj[4]}) + x^r{}_j, 10+M \le j < W;$
$o^{(r-Ri)*M+j} = x^r{}_{xaj} + x^r{}_{xbj} + x^r{}_{xcj} + x^r{}_{xdj} + x^r{}_{xej} + x^r{}_{xfj}, 0 \le j < M;$
$Ri \le r < Ri + L/M.$

Note: Even if the output feedback module is implemented in the cipher, it is enabled only in the authenticated encryption mode and only during the encryption/decryption: the "previous round ciphertext" bits (*e*) are not used as feedback (or just assumed to be 0) in any other stages or modes of operation described in [1], including the following sealing stage.

2.4 Finalising the MAC

The cipher is sealed according to the section 3.4.3, after which the *H*-bit MAC value of desired size is returned as described in the section 3.4.4 of [1].

3. Security

All VEST ciphers should maintain their respective security ratings when executed in the authenticated encryption mode.

4. Performance

The additional feedback bits are read directly from the ciphertext registers; consequently, all the accumulator feedback functions can still be implemented as 6-to-1 functions maintaining near-uniform performance distribution in the accumulator. VEST modules dedicated to authenticated encryption or decryption should maintain full speed in all FPGA and ASIC architectures. VEST modules that support dynamic selection between authenticated encryption, decryption and other modes of operation should maintain full speed in most Altera 4-to-1 LUT architectures, Altera Adaptive LUT architectures and ASIC environments. Xilinx FPGA maximum clock speed may reduce slightly due to a possible increase in critical path logic depth by one LUT element.

The native authenticated encryption mode effectively halves the cipher power budget required to achieve both message encryption and the generation of message authentication codes in both FPGA and ASIC. Native authenticated encryption mode of VEST-8 is more than twice as fast as the fastest surveyed HMAC-SHA-256 [4] with the same security rating in under half the circuit area on Xilinx FPGA. Native authenticated encryption mode of VEST-16 is more than 1.5 times faster than the fastest HMAC-AES [4] implementation on Xilinx FPGA in similar CLB slice usage but without the use of 10 instances of the 16-kilobit SRAM.

5. Circuit Area

In FPGA, the register count and logic area increases by approximately *M* to 2*M* 4-to-1 LUTs to accommodate the independent feedback [and output] logic paths.

In ASIC, the total circuit area will increase only very slightly, if at all: the circuit area increase is counteracted by the reduction in circuit area occupied by the *M* accumulator feedback functions that are now reduced from 5-to-1 down to 4-to-1 with two linear inputs instead of one.

6. References

[1] S. O'Neil, B. Gittins, H. Landman, VEST Hardware-Dedicated Stream Ciphers, eSTREAM, June 2005.

[2] M. Bellare, C. Namprempre, Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm, ASIACRYPT, September 2000.

[3] T.E. Palmatier, US Patent 6,912,284, NSA, June 1983.

[4] B. Gittins, H. Landman, S. O'Neil, A presentation on VEST hardware performance, October 2005.