Rebuttal of overtaking VEST

(VEST P2.1)

Benjamin Gittins, Howard A. Landman
{b.gittins, h.landman}@synaptic-labs.com

Synaptic Laboratories Limited
www.vestciphers.com

March, 2007

Abstract. VEST is a set of four stream cipher families targeted to semiconductor applications. All VEST family members support efficient encryption, single pass authenticated encryption, and collision resistant hashing in the one low area module. VEST was submitted by Synaptic Laboratories to the ECRYPT NoE eSTREAM project in 2005. Recently, a single digit typographical error was identified in the VEST counter diffuser description[1]. Shortly afterwards Antoine Joux and Jean-René Reinhard [1] published collisions in the counter-diffuser based upon the erroneous description. By extending these collisions across the entire cipher state, they were able to explore various attack scenarios. We prove that the correction of the typographical error removes all the exploitable collisions in the counter diffuser during key and IV loading operations; thereby establishing that the Joux-Reinhard attacks are an artefact of the erroneous description. Complete test vectors are included.

1. Introduction

VEST is a set of four stream cipher families dedicated to hardware applications. VEST is a modern cipher design featuring many desirable properties not found in other ciphers. VEST ciphers support efficient encryption, embedded authentication and (keyed & unkeyed) collision-resistant hashing modes of operation with over 90% logic reuse between all modes of operation. VEST ciphers support keys twice the length of the security rating to protect against brute force and potential quantum computing attacks. Submitted by Synaptic Laboratories to the ECRYPT NoE eSTREAM project [2] and published in 2005, the VEST specifications contained a single digit typographic error that was recently discovered in the description of the VEST counter diffuser. The error, incorrectly substituting a 1 for 7, is sincerely regretted since the use of an erroneous VEST description can result in collisions in the counter diffuser. The correction must be applied.

A. Joux and J. Reinhard [1] explore the above collisions in the counter diffuser and describe a "long" IV attack, requiring $2^{22.24}$ IV set-ups on average, which can create a collision in the total cipher state. The ability to create collisions in the total cipher state results in forgeries in the (keyed & unkeyed) collision-resistant hashing mode and the ability to encrypt two messages with the same key-stream under different IV's. The paper then purports to break VEST when using keys equal in length to the security claims of the four cipher families.

[1] By Sean O'Neil, one of the co-authors of the original VEST specifications. See http://www.ecrypt.eu.org/stream/phorum/read.php?1,979

We acknowledge that collisions in the counter-diffuser, when implemented according to the erroneous description, could be exploited during (keyed and unkeyed) hashing mode of operation[2] and enable an attacker the ability to encrypt two messages with the same key-stream.

However, the success of the key recovery attack is contentious. A. Joux and J. Reinhard [1] claim that finding a collision using the IV attacks can reduce the complexity of an exhaustive key search by fifty-three bits. That is, where F is the length of the key, that the attack recovers the key used by the cipher using $2^{\max(F/2+4,F-53)}$ time and $2^{F/2-4}$ memory, resulting in the average number of keys to test is 2^{F-53}. The attack is clearly not successful when using keys of $2F$ in length as strongly recommended in section 3.3 of the VEST specifications. Professor D. J. Bernstein has performed an independent review of the attack. Quoting Bernstein's website [3]:

> They claim: "VEST should be considered as broken." I disagree. The stated attack is slower than a brute-force search on a machine of the same size. My current impression is that a refined attack, parallelizing the Joux-Reinhard attack and reducing its memory requirements, uses time approximately 2^(F/2+4) on a machine of size 2^(F/4); in particular, a 128-bit ProVEST key can be found in time comparable to a 100-bit brute-force search.

In any case, given the attack built upon the collision resulting from the uncorrected counter-diffuser wiring, we must establish that without the typographic error exploitable collisions are not present.

The remainder of our paper proceeds as follows: in section 2 of this paper, we recite the analysis describing the fault in the counter diffuser and perform a similar analysis on the counter diffuser with the correction. In section 3 we perform exhaustive simulations of key loading and IV loading to prove that controlled collisions cannot be introduced in the counter diffuser. In section 4 we clarify the minimal deviation of the correction in relation to the complete VEST specifications. Section 5 discusses naming conventions and we provide a summary of the paper in section 6. Complete source code for all exhaustive tests and the cipher test vectors are embedded as an attachment within this PDF.

2. Formal analysis of the collision and correction in the linear counter diffuser

2.1 Description of the counter diffuser and its properties

[2] The Joux-Reinhard paper incorrectly describes the message digest of the (keyed or unkeyed) collision resistant hash as a MAC. This leads the reader to believe that the authenticated encryption mode of operation in VEST has been compromised. No such analysis on the AE mode of operation was performed and the security of the VEST AE MAC remains unchallenged.

In section 2.2 of the Joux-Reinhard attack [1] a description of the VEST linear counter diffuser with the typographic error is as follows:

> The linear counter diffuser is a 10-bit value used to disturb the core accumulator. Every cycle, the linear counter diffuser is updated linearly with the 16-bit output from the counter. As in [*the vest specifications*] we note d^r_j the value at step *r* of bit *j* of the linear counter diffuser. We note
>
> $$D^{(r)} = \begin{pmatrix} d^r_0 \\ d^r_0 \\ \vdots \\ d^r_9 \end{pmatrix} \quad C^{(r)} = \begin{pmatrix} c^r_0\ 1 \\ c^r_0\ 1 \\ \vdots \\ c^r_9\ 1 \end{pmatrix}.$$
>
> The linear counter diffuser update function can be written as:
>
> $$D^{(r+1)} = A \cdot D^{(r)} \oplus M \cdot C^{(r)} \oplus B,$$
>
> With
>
> $$A = \begin{bmatrix} 0100000000 \\ 0010000000 \\ 0001000000 \\ 0000100000 \\ 0000010000 \\ 0000001000 \\ 0000000100 \\ 0000000010 \\ 1000000000 \\ 0000000001 \end{bmatrix} \quad M = \begin{bmatrix} 0100110000010100 \\ 1010001010000010 \\ 0001100100100001 \\ 1001010001001000 \\ 0100101000001001 \\ 1000000101000110 \\ 0100000010010011 \\ 0010011000101000 \\ 1001000111000000 \\ 0000000010101101 \end{bmatrix} \quad B = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$
>
> Matrix M having more columns than rows has a non zero kernel, generated by vectors:
>
> **(1,0,0,0,1,1,1,1,0,0,0,0,0,0,0,0)^T,**
> (1,1,1,1,0,1,1,0,1,1,1,0,0,0,0,0)^T,
> (0,1,1,0,0,0,1,0,1,0,0,1,0,0,0,0)^T,
> (0,1,0,1,1,0,1,0,1,0,0,0,1,0,0,0)^T,
> (1,1,0,1,1,0,0,0,0,0,0,0,0,0,1,0)^T,
> (0,1,0,1,0,0,0,0,0,1,0,0,0,1,0,1)^T
>
> .

The Joux-Reinhard attacks [1] exploit a property in the first kernel vector in the table above (highlighted in bold) where none of the last eight registers is used. A linear expansion of the lower eight counter bits to nine-bits in the faulty counter diffuser results in 128 distinct collisions. The ability to readily choose from a wide range of collisions during the hashing mode of VEST is the prerequisite from which all the proposed attacks are derived.

2.2 Description of the correct counter diffuser

A single digit typographic error exists in the wiring selection in the VEST specifications. The input $c_1{}^r{}_1$ of $d^{r+1}{}_6$ of the counter diffuser should be $c_7{}^r{}_1$. The counter diffuser in section 2.2 of the VEST specifications should have read as:

$$
\begin{aligned}
d^{r+1}{}_0 &= d^r{}_1 + c_1{}^r{}_1 + c_4{}^r{}_1 + c_5{}^r{}_1 + c_{11}{}^r{}_1 + c_{13}{}^r{}_1 + 1;\\
d^{r+1}{}_1 &= d^r{}_2 + c_0{}^r{}_1 + c_2{}^r{}_1 + c_6{}^r{}_1 + c_8{}^r{}_1 + c_{14}{}^r{}_1;\\
d^{r+1}{}_2 &= d^r{}_3 + c_3{}^r{}_1 + c_4{}^r{}_1 + c_7{}^r{}_1 + c_{10}{}^r{}_1 + c_{15}{}^r{}_1;\\
d^{r+1}{}_3 &= d^r{}_4 + c_0{}^r{}_1 + c_3{}^r{}_1 + c_5{}^r{}_1 + c_9{}^r{}_1 + c_{12}{}^r{}_1;\\
d^{r+1}{}_4 &= d^r{}_5 + c_1{}^r{}_1 + c_4{}^r{}_1 + c_6{}^r{}_1 + c_{12}{}^r{}_1 + c_{15}{}^r{}_1 + 1;\\
d^{r+1}{}_5 &= d^r{}_6 + c_0{}^r{}_1 + c_7{}^r{}_1 + c_9{}^r{}_1 + c_{13}{}^r{}_1 + c_{14}{}^r{}_1;\\
d^{r+1}{}_6 &= d^r{}_7 + \mathbf{c_7{}^r{}_1} + c_8{}^r{}_1 + c_{11}{}^r{}_1 + c_{14}{}^r{}_1 + c_{15}{}^r{}_1;\\
d^{r+1}{}_7 &= d^r{}_8 + c_2{}^r{}_1 + c_5{}^r{}_1 + c_6{}^r{}_1 + c_{10}{}^r{}_1 + c_{12}{}^r{}_1 + 1;\\
d^{r+1}{}_8 &= d^r{}_0 + c_0{}^r{}_1 + c_3{}^r{}_1 + c_7{}^r{}_1 + c_8{}^r{}_1 + c_9{}^r{}_1 + 1;\\
d^{r+1}{}_9 &= d^r{}_9 + c_8{}^r{}_1 + c_{10}{}^r{}_1 + c_{12}{}^r{}_1 + c_{13}{}^r{}_1 + c_{15}{}^r{}_1 + 1;
\end{aligned}
$$

The matrix M in the analysis by Joux-Reinhard is rewritten as:

$$
M' = \begin{bmatrix}
0100110000010100\\
1010001010000010\\
0001100100100001\\
1001010001001000\\
0100101000001001\\
1000000101000110\\
0000000110010011\\
0010011000101000\\
1001000111000000\\
0000000010101101
\end{bmatrix},
$$

having a null space generated by the following vectors:

$$
\begin{aligned}
&(0,1,1,1,1,0,0,1,1,1,\mathbf{1},0,0,0,0,0)^{\mathrm{T}},\\
&(1,1,1,0,1,1,0,1,0,0,0,\mathbf{1},0,0,0,0)^{\mathrm{T}},\\
&(1,1,0,1,0,1,0,1,1,0,0,0,\mathbf{1},0,0,0)^{\mathrm{T}},\\
&(1,0,1,0,1,0,1,1,1,1,0,0,0,\mathbf{1},0,0)^{\mathrm{T}},\\
&(0,1,0,1,0,1,1,1,0,0,0,0,0,0,\mathbf{1},0)^{\mathrm{T}},\\
&(0,1,1,1,0,1,0,0,1,0,0,0,0,0,0,\mathbf{1})^{\mathrm{T}}
\end{aligned}
$$

It is easy to see that no non-zero vector in this null space can possibly be all zeros in the last eight bits. It is not possible for an attacker to introduce a collision when loading data into the lower eight counters.

The corrected cipher test vectors are embedded as an attachment in this PDF and can be retrieved using recent versions of the Adobe "Acrobat Reader" application.

3. Controlled collisions are impossible with the corrected VEST specifications

In the VEST design, on every clock cycle, bit 1 of each of the 16 counters ($c_{0:1}$ to $c_{15:1}$) and the output of the ten diffuser bits (d_0 to d_9) are linearly combined and stored in the ten diffuser bits (d_0 to d_9). In section 3.1 it is conclusively shown that attacker controlled collisions cannot be introduced into the counter diffuser by performing exhaustive analysis of all possible inputs patterns for all possible states of the counter diffuser. In section 3.2 the correctness of this model is then validated by executing a bit-level accurate model of the front end of the VEST-4 cipher including the full 16 counters and counter-diffuser.

3.1 Testing hashing mode of operation

When VEST runs in hashing mode (also used to load the IV) the higher eight counters ($c_{0:8}$ to $c_{15:1}$) operate autonomously and the lower eight counters ($c_{0:1}$ to $c_{7:1}$) accept eight new bits of input every clock cycle.

When exhaustively testing the counter diffuser module eight new bits of input are loaded directly into bits $c_{0:1}$ to $c_{7:1}$. There are 2^8 states for the high eight counters and 2^{10} diffuser states. There are $2^{14.9}$ combinadics in the system of 2-combinations from the set of 2^8 possible inputs to the lower eight counters. Out tests search for collisions across the counter diffuser state for each of the $2^{14.9}$ combinadics for all of the 2^{18} states. Collisions were detected when using the faulty counter diffuser wirings. No collisions were found with the corrected counter diffuser wirings.

These results are confirmed using three bit-level accurate instances of the counters and counter diffuser of the VEST-4 cipher. The first instance is called the reference instance and the second instance is called the chaser instance; the third instance is called the explorative chaser instance and is frequently reinitialised with a copy of the current chaser instance. The reference and chaser instances are initialised with all ones according to the VEST specifications. The reference engine is supplied a random eight bit input and records 10-bits of output. An iterative search process now begins: the reference instance is again supplied a random eight bit input and records 10-bits of output. For all possible 2^8 inputs, explorative chaser instances are initialised from the chaser instance and supplied a distinct eight bit value and generate 20-bits of output. A collision occurs when the output of two explorative chaser instances matches the last 20-bit bits of output of the reference instance. A decision is made on which of the eight-bit inputs resulting in a collision to follow. The chaser module is cycled once with the chosen input and the resulting 10-bit output is recorded. The search process is repeated an arbitrarily large number of times. Collisions were detected when using the faulty counter diffuser wirings. No collisions were found with the corrected counter diffuser wirings.

3.2 Testing key loading mode of operation

When VEST runs in keying mode, the sixteen counters behave as a simple sixteen bit wide shift register, loading one new bit of key material every clock cycle.

When exhaustively testing the counter diffuser module, the sixteen counter bits ($c_{0:1}$ to $c_{15:1}$) are mapped as a simple shift register. A new key bit is loaded into the least significant bit $c_{0:1}$ and the most significant bit $c_{15:1}$ is discarded. There are a total of 2^{16} counter states, for each of these states there are only two possible state transitions. There are a total of 2^{10} counter diffuser states. Our tests search for collisions across the counter diffuser state when loading the two possible inputs for each of the 2^{26} states. No collisions were found in the faulty or corrected counter diffuser wirings.

These results are confirmed by exhaustively loading all keys of *n*-bit in length into a bit-level accurate model of the counters and counter diffuser of the VEST-4 cipher and searching for identical counter diffuser outputs also resulting in identical state. All key lengths up to and including twenty bits were tested. Probabilistic testing of key lengths up to and including thirty-two bits has also been performed. No collisions were found in the faulty or corrected counter diffuser wirings.

3.3 Summary of exhaustive analysis

It is impossible to introduce controlled collisions in the counter-diffuser during key-loading or IV-loading operations with the typographic error removed. These results are confirmed by executing exhaustive tests on the bit-level accurate front-end models of the VEST-4 cipher. The Joux-Reinhard attacks are clearly an artefact of a single digit typographic error in the wiring choices in the VEST cipher specifications.

The source code for the four exhaustive tests is embedded as an attachment in this PDF and can be retrieved using recent versions of the Adobe "Acrobat Reader" application.

4. Minimal deviation from published VEST specifications

In the VEST specifications and source code, one wire out of 8300+ wires was incorrectly assigned. The correct wire has now been assigned. No changes are made to the fundamental structure or operation of the cipher.

5. Nomenclature

We propose that:

> the VEST specification submitted to Phase 2 of the eSTREAM project (a.k.a. "VEST P2") be called "VEST P2.0";

and the VEST specification with the correction of the typographical error be called “VEST P2.1.

7. Summary

There was a single digit typographical error in the wiring selections in the VEST specifications that came through into VEST P2.0. As Joux and Reinhard have shown, VEST can be attacked if it is implemented with that erroneous wiring selection.

The error has been corrected. We have illustrated that the corrected construction remains injective in respect of inputs to the lower eight counters and studied its behavior during keying and hashing modes of operation. Results obtained from exhaustive analysis of all possible inputs to the corrected counter diffuser when performing key and IV loading protocols prove that collisions are not present in the corrected counter diffuser during these operations.

We conclude that this correction renders all the attacks suggested by Joux-Reinhard impossible and that, with the wiring correction applied, VEST security remains uncompromised in all modes of operation. This is true even if key lengths equal to the claimed security parameter of each cipher are used.

Clearly, the fundamental structure and operation of VEST remains unchanged, as does the authors’ original strong recommendation published in the VEST specifications that key lengths should be at least double the claimed security parameter.

The authors would like to thank Antoine Joux and Jean-René Reinhard for studying the VEST cipher and publishing their analysis and Sean O’Neil for pointing out the correction of the typographic error in the wiring selection in the VEST specifications.

References

[1] A. Joux, J. Reinhard, “Overtaking VEST’, SASC 2007, http://www.ecrypt.eu.org/stream/papersdir/2007/021.pdf

[2] ECRYPT NoE eSTREAM, http://www.ecrypt.eu.org/stream

[3] D. J. Bernstein, “Attacks”, http://cr.yp.to/streamciphers/attacks.html

[4] S. O’Neil, B. Gittins, H. Landman, “VEST Ciphers (eStream Phase 2)”, http://www.ecrypt.eu.org/stream/p2ciphers/vest/vest_p2.pdf