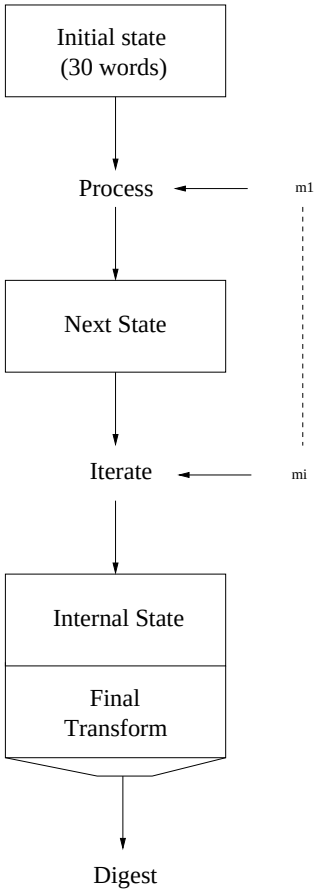
# Some improved attacks on Fugue-256

Praveen Gauravaram*
Joint work with
Lars R. Knudsen*, Nasour Bagheri**, Lei Wei***

MAT, DTU*, SRTTU, Iran** and NTU, Singapore***

FSE 2011, Rump session
14 February 2011

# F-256


Initial state
(30 words)
Process
m1
Next State
Iterate
mi
Internal State
Final
Transform
Digest

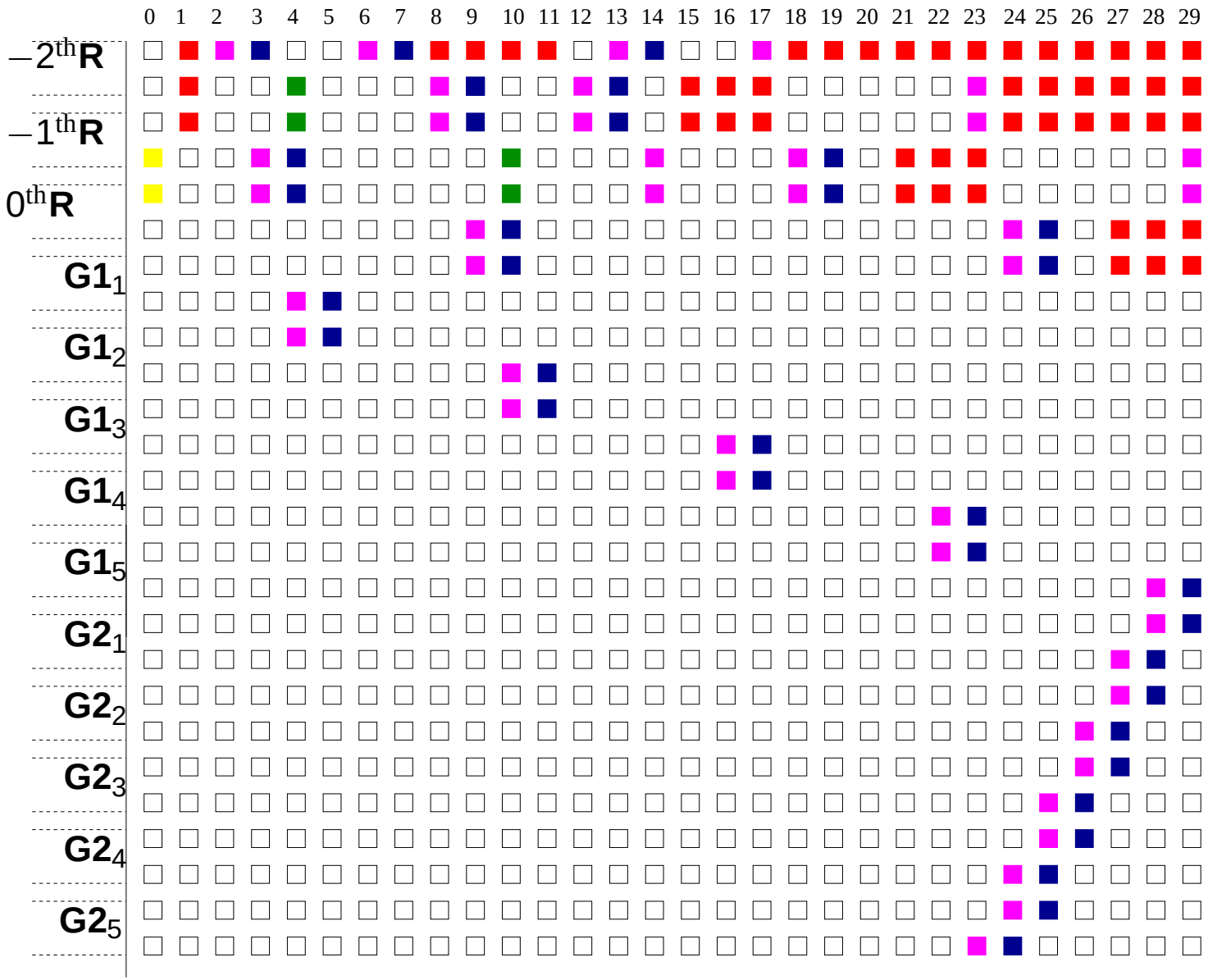
# F-256

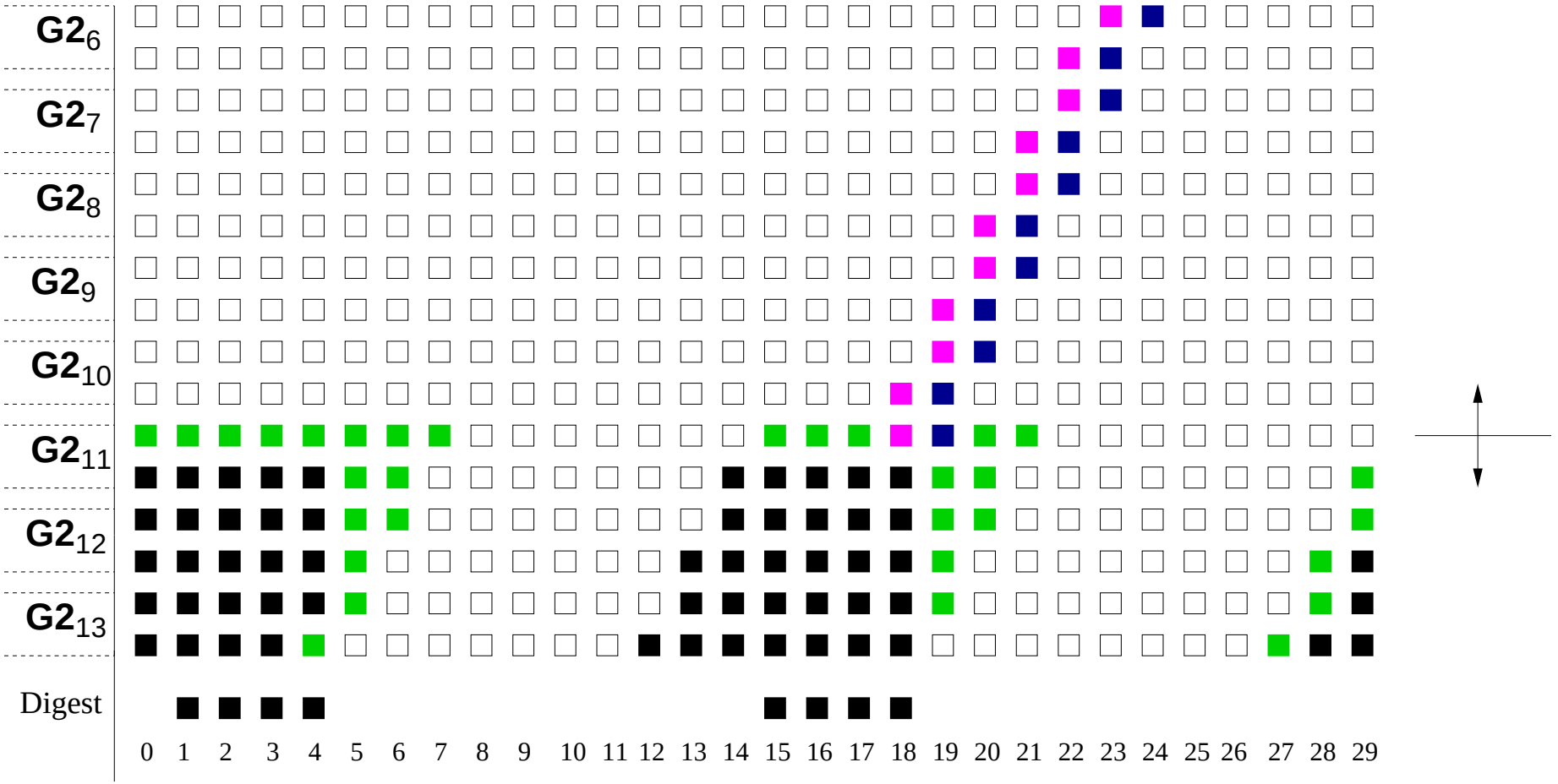
- *Initial state*: $S_{0\sim21} = 0$ and $S_{22\sim29} = IV$.
- *Padding:* Zero padding and length encoding of 64 bits.
- *Round transform* **R** consists of: TIX (I),ROR3, CMIX, SMIX, ROR3, CMIX, SMIX.
- *Final transform* **G** consists of 5 rounds of **G1** and 13 rounds of **G2**.
  - **G1**: ROR3, CMIX, SMIX, ROR3, CMIX, SMIX;
  - **G2**: $S_4 += S_0$, $S_{15} += S_0$, ROR15, SMIX; $S_4 += S_0$, $S_{16} += S_0$, ROR14, SMIX;
  - $S_4 += S_0$; $S_{15} += 0$.
- Collect the output words $S_{1\sim4}$ and $S_{15\sim18}$ as the digest.

# Practical structural pseudo differentiator for F-256

- Uses a new probability 1 differential from $\mathbf{G2}_{11}$ till the first round of the **R** transform.
  1. Forwards from $\mathbf{G2}_{11}$
  2. Backwards from $\mathbf{G2}_{11}$
- Two pairs of *initial states* with a structure at input produce the same digest difference in $2^{33}$ calls to F-256.
- Additional couple of pairs of *initial states* that produce identical digest difference can be found for a similar complexity by using the freedom in the state at $\mathbf{G2}_{11}$.
- Demonstrates *weak* state diffusion in F-256 (including padding).

# Differential path




G2$_6$
G2$_7$
G2$_8$
G2$_9$
G2$_{10}$
G2$_{11}$
G2$_{12}$
G2$_{13}$
Digest
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29

# Example

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $S_i$ | 00000000 | 60384cec | c88579f6 | ef3384a7 | 1122cf88 | 699f49c9 | 061dd5c7 | d0ec2932 |
| $S_i^*$ | 00000000 | 1b4b4b3b | c88579ff | bf715080 | 1122cf88 | 699f49c9 | 061dd5ce | 80aefd15 |
| $\delta S_i$ | 00000000 | 7b7307d7 | 00000009 | 5042d427 | 00000000 | 00000000 | 00000009 | 5042d427 |
| $i$ | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| $S_i$ | 490b3310 | e9515c99 | 0f318596 | 5d5cf9cb | 8b3ed0d8 | f24df5be | 0e882d53 | a04d1f33 |
| $S_i^*$ | bab9bb1a | 3f0e6e44 | 3060b6a1 | 952343d8 | 8b3ed0d8 | f24df5b7 | 5ecaf974 | a04d1f33 |
| $\delta S_i$ | f3b2880a | d65f32dd | 3f513337 | c87fba13 | 00000000 | 00000009 | 5042d427 | 00000000 |
| $i$ | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| $S_i$ | 55c282ac | 7dac1e94 | 8128362d | 9bfb7773 | e027a681 | 26b47a29 | 31432623 | 1d8fd2d0 |
| $S_i^*$ | 55c282ac | 7dac1e9d | c653bcab | 8fcd7448 | c8a9b641 | 4e4ee6a6 | 6c9e69b9 | b5612464 |
| $\delta S_i$ | 00000000 | 00000009 | 477b8a86 | 1436033b | 288e10c0 | 68fa9c8f | 5ddd4f9a | a8eef6b4 |
| $i$ | 24 | 25 | 26 | 27 | 28 | 29 | | |
| $S_i$ | e6beba51 | f632b2d6 | 6a9e272e | 48be89d7 | 415cc7c3 | d0913503 | | |
| $S_i^*$ | 9dcdbd86 | 4d01224b | 4e845d7d | c0be7791 | 6ba488f9 | 651ff74e | | |
| $\delta S_i$ | 7b7307d7 | bb33909d | 241a7a53 | 8800fe46 | 2af84f3a | b58ec24d | | |
| $S_i$ | 00000000 | dfc0c8dc | 9f377939 | 79a8eedf | a1494d9a | 7c7ec219 | 57ba13ef | 419425ff |
| $S_i^*$ | 00000000 | a384d860 | 9f377930 | 29ea3af8 | a1494d9a | 7c7ec219 | 57ba13e6 | 11d6f1d8 |
| $\delta S_i$ | 00000000 | 7c4410bc | 00000009 | 5042d427 | 00000000 | 00000000 | 00000009 | 5042d427 |
| $S_i$ | 92a4950a | ef401399 | 24a6b3da | 885f29bd | d2ad82df | d4a1c996 | 61e5f82c | f5df2e9c |
| $S_i^*$ | 97a2714e | df695c53 | dc179321 | e45d6bef | d2ad82df | d4a1c99f | 31a72c0b | f5df2e9c |
| $\delta S_i$ | 0506e444 | 30294fca | f8b120fb | 6c024252 | 00000000 | 00000009 | 5042d427 | 00000000 |
| $S_i$ | 6c43db27 | a3d7bba2 | ff80e3c3 | e6e9d43f | 7545d720 | 9ef2661d | f366637c | 2643cd41 |
| $S_i^*$ | 6c43db27 | a3d7bbab | b85bdda6 | 8ee38551 | b8356608 | f0253cc4 | 7cfb5757 | 5a907f38 |
| $\delta S_i$ | 00000000 | 00000009 | 47db3e65 | 680a516e | cd70b128 | 6ed75ad9 | 8f9d342b | 7cd3b279 |
| $S_i$ | b2a6c9a6 | 23253798 | 8cdb1796 | cd9ed766 | d6336037 | 251d81be | | |
| $S_i^*$ | cee2d91a | 3acd494c | 42729eb7 | 3e270858 | 8160fad6 | bb1c154c | | |
| $\delta S_i$ | 7c4410bc | 19e87ed4 | cea98921 | f3b9df3e | 57539ae1 | 9e0194f2 | | |

| $H_1$ | $H_1^*$ | $\delta H_1$ | $H_2$ | $H_2^*$ | $\delta H_2$ |
|---|---|---|---|---|---|
| c7d79278 | 1110cc99 | d6c75ee1 | c7d79278 | 1110cc99 | d6c75ee1 |
| 5bf7c4c7 | 0c8414e5 | 5773d022 | 5bf7c4c7 | 0c8414e5 | 5773d022 |
| 89887088 | a2001d55 | 2b886ddd | 89887088 | a2001d55 | 2b886ddd |
| d766450d | e3e3bdcf | 3485f8c2 | d766450d | e3e3bdcf | 3485f8c2 |
| 9832fbba | 8aeada67 | 12d821dd | 9832fbba | 8aeada67 | 12d821dd |
| 1af7391d | df11a14c | c5e69851 | 1af7391d | df11a14c | c5e69851 |
| b81725a5 | ab74f777 | 1363d2d2 | b81725a5 | ab74f777 | 1363d2d2 |
| c073bb41 | 4d788f18 | 8d0b3459 | c073bb41 | 4d788f18 | 8d0b3459 |

Digests and their difference for the pair of pseudo initial states presented before. The digests for the first pair are $(H_1, H_1^*)$ and those for the second pair are $(H_2, H_2^*)$. The message word $m^{-2}$ for the first pair of states are 452*e*0*fed* and *b*69*c*87*e*7 respectively and the message word $m^{-2}$ for the second pair of states are 3*e*38*f*1*d*5 and 3*b*3*e*1591 respectively.

# Other improved attacks on F-256

1. Structural pseudo differentiator also results in pseudo collisions for no additional cost (generic attack: $2^{65}$ due to length padding).
2. MIM preimage attack is improved to $2^{416}$ time and space from $2^{480}$ (designers' claim).
3. Integral distinguisher for the 16.5 rounds of the final transform (previous: 5.5 rounds by Aumasson and Phan).

Thank you!!