Stream ciphers and eSTREAM

Thomas Johansson
Lund University
Motivation

- The most used stream cipher constructions (A5, RC4, E0, ...) all have serious weaknesses.
- There is a belief that we can have stream ciphers that outperform AES in some aspects.
- A previous attempt to produce good stream cipher candidates (NESSIE) failed.
Background

• eSTREAM – an evaluation project to come up with a portfolio of new and promising stream ciphers.
• Similar projects: AES competition, NESSIE, ...
• eSTREAM was decided to be more research oriented, e.g., allowing designers to modify.
Background

• Evaluating committee of roughly 10 ECRYPT representatives headed by Matt Robshaw (head of STVL lab).

• Project outline
  – Prestudy
  – Call for primitives
  – Evaluation in several phases
Timeline

Oct 2004  
SASC - *The State of the Art of Stream Ciphers.*
Discussion leads to the ECRYPT Call for Primitives

Nov 2004  
Call for Primitives

April 2005  
The deadline

May 2005  
SKEW - *Symmetric Key Encryption Workshop.*
Most eSTREAM submissions are presented here.

June 2005  
The eSTREAM website is launched.

Feb 2006  
SASC 2006: *Stream Ciphers Revisited.*

Feb 2006  
The end of phase I.

Jan 2007  
SASC 2007 workshop.

Feb 2007  
The end of phase II.

Feb 2008  
SASC 2008 workshop.

April 2008  
The end of phase III. The eSTREAM Portfolio is announced.
The call for primitives

• PROFILE 1.
  – Stream ciphers for software applications with high throughput requirements.

• PROFILE 2.
  – Stream ciphers for hardware applications with restricted resources such as limited storage, gate count, or power consumption.

• Optionally also an associated authentication method.
## Submissions – profile 1

<table>
<thead>
<tr>
<th>Phase 3</th>
<th>Phase 2</th>
<th>Phase 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>CryptMT</td>
<td>ABC</td>
<td>F-FCSR</td>
</tr>
<tr>
<td>Dragon</td>
<td>DICING</td>
<td>Fubuki</td>
</tr>
<tr>
<td>HC</td>
<td>Phelix</td>
<td>Frogbit</td>
</tr>
<tr>
<td>LEX</td>
<td>Polar Bear</td>
<td>Hermes</td>
</tr>
<tr>
<td>NLS</td>
<td>Py</td>
<td>MAG</td>
</tr>
<tr>
<td>Rabbit</td>
<td></td>
<td>Mir-1</td>
</tr>
<tr>
<td>Salsa20</td>
<td></td>
<td>Pomaranch</td>
</tr>
<tr>
<td>SOSEMANUK</td>
<td></td>
<td>SSS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TRBDK3 YAEA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yamb</td>
</tr>
</tbody>
</table>

23 submissions
## Submissions – profile 2

<table>
<thead>
<tr>
<th>Phase 3</th>
<th>Phase 2</th>
<th>Phase 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECIM</td>
<td>Achterbahn</td>
<td>MAG</td>
</tr>
<tr>
<td>Edon80</td>
<td>Hermes</td>
<td>Sfinks</td>
</tr>
<tr>
<td>F-FCSR</td>
<td>LEX</td>
<td>SSS</td>
</tr>
<tr>
<td>Grain</td>
<td>NLS</td>
<td>TRBDK3 YAEA</td>
</tr>
<tr>
<td>MICKEY</td>
<td>Phelix</td>
<td>Yamb</td>
</tr>
<tr>
<td>Moustique</td>
<td>Polar Bear</td>
<td></td>
</tr>
<tr>
<td>Pomaranch</td>
<td>Rabbit</td>
<td></td>
</tr>
<tr>
<td>Trivium</td>
<td>Salsa20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TSC-3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VEST</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Zk-Crypt</td>
<td></td>
</tr>
</tbody>
</table>

25 submissions
The eSTREAM portfolio

<table>
<thead>
<tr>
<th>Profile 1 (SW)</th>
<th>Profile 2 (HW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HC-128</td>
<td>F-FCSR-H v2</td>
</tr>
<tr>
<td>Rabbit</td>
<td>Grain v1</td>
</tr>
<tr>
<td>Salsa20/12</td>
<td>MICKEY v2</td>
</tr>
<tr>
<td>SOSEMANUK</td>
<td>Trivium</td>
</tr>
</tbody>
</table>
A stream cipher

- The PRKG stretches the $k$ bit key to some arbitrarily long sequence

\[ Z = z_1, z_2, z_3, \ldots \]

(keystream, running key)
Profile 1

• Software-oriented designs
  – A key length of 128.
  – An IV length of at least one of 64 or 128 bits.
  – ( An authentication tag length of 32-128 bits.)

• Superior to the AES in at least one significant aspect.
  – Fast encryption of long sequences (cycles/byte).
  – Fast reinitialization (encryption of packet data)
### Profile 1 - Performance

<table>
<thead>
<tr>
<th>Primitive</th>
<th>Profile</th>
<th>Key</th>
<th>IV</th>
<th>Stream</th>
<th>40 bytes</th>
<th>1500 bytes</th>
<th>Key setup</th>
<th>IV setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>COPY</td>
<td>B</td>
<td>80</td>
<td>80</td>
<td>0.50</td>
<td>3.02</td>
<td>0.60</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>HC-128</td>
<td>128</td>
<td>128</td>
<td>128</td>
<td>3.52</td>
<td>767.72</td>
<td>23.83</td>
<td>60</td>
<td>30367</td>
</tr>
<tr>
<td>Rabbit</td>
<td>128</td>
<td>64</td>
<td>64</td>
<td>3.94</td>
<td>22.69</td>
<td>4.46</td>
<td>548</td>
<td>454</td>
</tr>
<tr>
<td>SNOW-2.0</td>
<td>B</td>
<td>128</td>
<td>128</td>
<td>4.74</td>
<td>28.63</td>
<td>5.37</td>
<td>76</td>
<td>745</td>
</tr>
<tr>
<td>SOSEMANUK</td>
<td>128</td>
<td>64</td>
<td>64</td>
<td>5.60</td>
<td>36.02</td>
<td>8.60</td>
<td>1185</td>
<td>840</td>
</tr>
<tr>
<td>Salsa20/12</td>
<td>128</td>
<td>64</td>
<td>64</td>
<td>7.43</td>
<td>22.07</td>
<td>7.83</td>
<td>43</td>
<td>32</td>
</tr>
<tr>
<td>AES - CRT</td>
<td>A</td>
<td>128</td>
<td>128</td>
<td>15.97</td>
<td>22.73</td>
<td>16.11</td>
<td>168</td>
<td>33</td>
</tr>
</tbody>
</table>

eSTREAM internal performance figures: Pentium M
Profile 2

- Hardware-oriented designs with restricted resources such as limited storage, gate count, or power consumption.
  - A key length of 80 bits.
  - An IV length of at least one of 32 or 64 bits.
  - (An authentication tag length of 32-64 bits.)
- Superior to the AES in at least one significant aspect.
  - Smaller hardware fingerprint, low power consumption, …
## Profile 2 - Performance

Table 4. Derived metrics operating at 100kHz clock (low-end RFID/WSN applications)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Grain80</td>
<td>0.100</td>
<td>3.29</td>
<td>32.96</td>
<td>67,908</td>
<td>0.0149</td>
<td>221</td>
<td>3,210</td>
<td>70.99</td>
</tr>
<tr>
<td>Grain80x4</td>
<td>0.400</td>
<td>4.47</td>
<td>11.19</td>
<td>21,747</td>
<td>0.0480</td>
<td>97</td>
<td>810</td>
<td>31.54</td>
</tr>
<tr>
<td>Grain80x8</td>
<td>0.800</td>
<td>6.09</td>
<td>7.61</td>
<td>14,198</td>
<td>0.0704</td>
<td>86</td>
<td>410</td>
<td>28.38</td>
</tr>
<tr>
<td>Grain80x16</td>
<td>1.600</td>
<td>9.33</td>
<td>5.83</td>
<td>10,493</td>
<td>0.0953</td>
<td>97</td>
<td>210</td>
<td>32.89</td>
</tr>
<tr>
<td>Trivium</td>
<td>0.100</td>
<td>5.54</td>
<td>55.36</td>
<td>133,747</td>
<td>0.0075</td>
<td>740</td>
<td>13,140</td>
<td>972.87</td>
</tr>
<tr>
<td>Triviumx2</td>
<td>0.200</td>
<td>5.74</td>
<td>28.71</td>
<td>68,092</td>
<td>0.0147</td>
<td>391</td>
<td>6,600</td>
<td>516.14</td>
</tr>
<tr>
<td>Triviumx4</td>
<td>0.400</td>
<td>14.89</td>
<td>35,081</td>
<td>0.0285</td>
<td>209</td>
<td>3,320</td>
<td>277.22</td>
<td>19.77</td>
</tr>
<tr>
<td>Triviumx8</td>
<td>0.800</td>
<td>8.82</td>
<td>19,12/</td>
<td>0.0523</td>
<td>135</td>
<td>1,680</td>
<td>181.35</td>
<td>11.85</td>
</tr>
<tr>
<td>Triviumx16</td>
<td>1.600</td>
<td>4.84</td>
<td>10,259</td>
<td>0.0975</td>
<td>76</td>
<td>880</td>
<td>104.88</td>
<td>6.39</td>
</tr>
<tr>
<td>Triviumx32</td>
<td>3.200</td>
<td>3.20</td>
<td>6,135</td>
<td>0.1630</td>
<td>62</td>
<td>450</td>
<td>90.56</td>
<td>4.61</td>
</tr>
<tr>
<td>Triviumx64</td>
<td>6.400</td>
<td>2.23</td>
<td>3,986</td>
<td>0.2509</td>
<td>57</td>
<td>240</td>
<td>87.82</td>
<td>3.43</td>
</tr>
<tr>
<td>F-FCSR-H</td>
<td>0.800</td>
<td>10.58</td>
<td>13.23</td>
<td>30,847</td>
<td>0.0324</td>
<td>326</td>
<td>2,250</td>
<td>587.75</td>
</tr>
<tr>
<td>F-FCSR-16</td>
<td>1.600</td>
<td>18.29</td>
<td>11.43</td>
<td>26,153</td>
<td>0.0382</td>
<td>478</td>
<td>3,060</td>
<td>2357.93</td>
</tr>
<tr>
<td>Grain120</td>
<td>0.100</td>
<td>4.34</td>
<td>42.48</td>
<td>96,250</td>
<td>0.0104</td>
<td>418</td>
<td>5,120</td>
<td>214.70</td>
</tr>
<tr>
<td>Grain128x4</td>
<td>0.400</td>
<td>5.80</td>
<td>14.00</td>
<td>27,588</td>
<td>0.0382</td>
<td>154</td>
<td>1,290</td>
<td>79.74</td>
</tr>
<tr>
<td>Grain128x8</td>
<td>0.800</td>
<td>6.90</td>
<td>8.62</td>
<td>16,127</td>
<td>0.0620</td>
<td>111</td>
<td>650</td>
<td>57.86</td>
</tr>
<tr>
<td>Grain128x16</td>
<td>1.600</td>
<td>9.36</td>
<td>5.85</td>
<td>10,333</td>
<td>0.0968</td>
<td>96</td>
<td>330</td>
<td>51.06</td>
</tr>
<tr>
<td>Grain128x32</td>
<td>3.200</td>
<td>14.77</td>
<td>4.61</td>
<td>7,480</td>
<td>0.1337</td>
<td>110</td>
<td>170</td>
<td>60.12</td>
</tr>
<tr>
<td>Mickey128</td>
<td>0.100</td>
<td>11.17</td>
<td>111.69</td>
<td>261,204</td>
<td>0.0038</td>
<td>291</td>
<td>4,170</td>
<td>1216.84</td>
</tr>
<tr>
<td>Mickey2(80)</td>
<td>0.100</td>
<td>7.10</td>
<td>71.98</td>
<td>165,249</td>
<td>0.0081</td>
<td>1,174</td>
<td>2,610</td>
<td>366.58</td>
</tr>
<tr>
<td>Pomaranch80</td>
<td>0.100</td>
<td>16.13</td>
<td>161.35</td>
<td>277,724</td>
<td>0.0036</td>
<td>4,481</td>
<td>4,720</td>
<td>2115.12</td>
</tr>
<tr>
<td>Pomaranch128</td>
<td>0.100</td>
<td>24.80</td>
<td>248.07</td>
<td>416,742</td>
<td>0.0024</td>
<td>10,338</td>
<td>5,940</td>
<td>6140.88</td>
</tr>
<tr>
<td>Moustique</td>
<td>0.100</td>
<td>20.56</td>
<td>205.58</td>
<td>498,044</td>
<td>0.0020</td>
<td>10,239</td>
<td>20,200</td>
<td>2068.22</td>
</tr>
<tr>
<td>Decim80</td>
<td>0.025</td>
<td>5.43</td>
<td>217.25</td>
<td>539,689</td>
<td>0.0019</td>
<td>2,931</td>
<td>16,120</td>
<td>741.69</td>
</tr>
<tr>
<td>Decim128</td>
<td>0.025</td>
<td>8.41</td>
<td>336.54</td>
<td>791,977</td>
<td>0.0013</td>
<td>6,663</td>
<td>16,170</td>
<td>2693.63</td>
</tr>
<tr>
<td>Edon80x4</td>
<td>0.005</td>
<td>10.49</td>
<td>2,217.91</td>
<td>5,441,851</td>
<td>0.0002</td>
<td>57,132</td>
<td>18,690</td>
<td>5054.86</td>
</tr>
<tr>
<td>Edon80pl</td>
<td>0.100</td>
<td>25.05</td>
<td>250.51</td>
<td>674,421</td>
<td>0.0015</td>
<td>16895</td>
<td>3,920</td>
<td>6622.82</td>
</tr>
<tr>
<td>AES [4]*</td>
<td>0.237</td>
<td>-</td>
<td>-</td>
<td>118,054</td>
<td>0.0085</td>
<td>-</td>
<td>500</td>
<td>-</td>
</tr>
<tr>
<td>AES [5]*</td>
<td>0.001</td>
<td>-</td>
<td>-</td>
<td>1,421,064</td>
<td>0.0007</td>
<td>-</td>
<td>10,160</td>
<td>-</td>
</tr>
</tbody>
</table>

Better is: higher lower* lower lower higher lower lower lower lower lower***

Statistics

- eSTREAM has drawn considerable attention from outside ECRYPT
  - Several hundred thousands visits to the webpage
  - 205 archived papers relating to eSTREAM
  - Many hundreds of postings on the forum
  - eSTREAM related papers appear at top conferences (FSE)
  - More than 100 participants on each SASC workshop
Returning to the final portfolio

• A broader pool of stream ciphers than expected
  – Offering a choice of options in meeting different performance requirements and security margins.
  – Remarkable diversity of design approaches, support future work in stream cipher design and analysis.
  – The immature nature of most eSTREAM algorithms

• Intention to maintain the eSTREAM web-pages and to update the portfolio as circumstances dictate.

• Evaluation of each candidate by
  – All published cryptanalysis work, performance work,
  – Public voting at SASC workshops
Example: Salsa 20/12

Design by Dan Bernstein

- Profile 1 (Software)
- Close to a block cipher in CTR mode

- Appears to have good security margin but still much faster than AES
The Salsa20/12 design

\[ Salsa20_k(\text{IV}, i) = H \left( \begin{array}{cccc} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v_0 & v_1 \\ i_0 & i_1 & c_2 & k_4 \\ k_5 & k_6 & k_7 & c_3 \end{array} \right) \]

where

\[ H(x) = x + R^{12}(x) \]

\( k = k_0, k_1, \ldots, k_7 \) a 256-bit secret key,

\( \text{IV} = v_0, v_1 \) a 64-bit initial vector.

\( i = i_0, i_1 \) a 64-bit counter,

\( c = c_0, c_1, c_2, c_3 \) 128-bit constants.
4 × 4 word matrix $x$,

$$
x = \begin{pmatrix}
x_0 & x_1 & x_2 & x_3 \\
x_4 & x_5 & x_6 & x_7 \\
x_8 & x_9 & x_{10} & x_{11} \\
x_{12} & x_{13} & x_{14} & x_{15}
\end{pmatrix}
$$

The round function $R(x)$ is defined as follows,

$$R(x) = \left( Q'^4(x) \right)^T,$$

where

$$Q'(x) = \begin{pmatrix}
x_5 & x_6 & x_7 & q_1 \\
x_9 & x_{10} & x_{11} & q_2 \\
x_{13} & x_{14} & x_{15} & q_3 \\
x_1 & x_2 & x_3 & q_0
\end{pmatrix},$$

and

$$\begin{pmatrix}
q_0 \\
q_1 \\
q_2 \\
q_3
\end{pmatrix} = Q \begin{pmatrix}
x_0 \\
x_4 \\
x_8 \\
x_{12}
\end{pmatrix}.$$
Finally,

\[
\begin{pmatrix}
  w_0 \\
  w_1 \\
  w_2 \\
  w_3
\end{pmatrix} = Q
\begin{pmatrix}
  y_0 \\
  y_1 \\
  y_2 \\
  y_3
\end{pmatrix},
\]

where

\[
\begin{align*}
  w_1 &= y_1 \oplus ((y_0 + y_3) \ll 7) \\
  w_2 &= y_2 \oplus ((w_1 + y_0) \ll 9) \\
  w_3 &= y_3 \oplus ((w_2 + w_1) \ll 13) \\
  w_0 &= y_0 \oplus ((w_3 + w_2) \ll 18)
\end{align*}
\]
The Trivium design

Design by Christoffe De Canniere

- Profile 2 (Hardware)
- Extremely simple design

- Designed to have low security margin to allow a really simple (and fast) hardware design
a 288-bit internal state denoted by \((s_1, \ldots, s_{288})\).

\[
\text{for } i = 1 \text{ to } N \text{ do }
\]

\[
t_1 \leftarrow s_{66} + s_{93}
\]

\[
t_2 \leftarrow s_{162} + s_{177}
\]

\[
t_3 \leftarrow s_{243} + s_{288}
\]

\[
z_i \leftarrow t_1 + t_2 + t_3
\]

\[
t_1 \leftarrow t_1 + s_{91} \cdot s_{92} + s_{171}
\]

\[
t_2 \leftarrow t_2 + s_{175} \cdot s_{176} + s_{264}
\]

\[
t_3 \leftarrow t_3 + s_{286} \cdot s_{287} + s_{69}
\]

\[
(s_1, s_2, \ldots, s_{93}) \leftarrow (t_3, s_1, \ldots, s_{92})
\]

\[
(s_{94}, s_{95}, \ldots, s_{177}) \leftarrow (t_1, s_{94}, \ldots, s_{176})
\]

\[
(s_{178}, s_{279}, \ldots, s_{288}) \leftarrow (t_2, s_{178}, \ldots, s_{287})
\]

\text{end for}

\[
\begin{array}{|c|}
\hline
\text{Parameters} \\
\text{Key size:} & 80 \text{ bit} \\
\text{IV size:} & 80 \text{ bit} \\
\text{Internal state:} & 288 \text{ bit} \\
\hline
\end{array}
\]
Key and IV setup

\[(s_1, s_2, \ldots, s_{93}) \leftarrow (K_1, \ldots, K_{80}, 0, \ldots, 0)\]
\[(s_{94}, s_{95}, \ldots, s_{177}) \leftarrow (IV_1, \ldots, IV_{80}, 0, \ldots, 0)\]
\[(s_{178}, s_{279}, \ldots, s_{288}) \leftarrow (0, \ldots, 0, 1, 1, 1)\]

for \(i = 1\) to \(4 \cdot 288\) do

\[t_1 \leftarrow s_{66} + s_{91} \cdot s_{92} + s_{93} + s_{171}\]
\[t_2 \leftarrow s_{162} + s_{175} \cdot s_{176} + s_{177} + s_{264}\]
\[t_3 \leftarrow s_{243} + s_{286} \cdot s_{287} + s_{288} + s_{69}\]

\[(s_1, s_2, \ldots, s_{93}) \leftarrow (t_3, s_1, \ldots, s_{92})\]
\[(s_{94}, s_{95}, \ldots, s_{177}) \leftarrow (t_1, s_{94}, \ldots, s_{176})\]
\[(s_{178}, s_{279}, \ldots, s_{288}) \leftarrow (t_2, s_{178}, \ldots, s_{287})\]

end for
Conclusions

- eSTREAM has been a very successful evaluation project
- eSTREAM has come to an end, but many eSTREAM proposals will be in focus for many years