Finding Slid Pairs for the Plantlet Stream Cipher

Joshua Copeland and Leonie Simpson

Queensland University of Technology

lr.simpson@qut.edu.au

February 5, 2020
Overview

Introduction

Plantlet Description

Observations

Simplified Plantlet

Slid Pairs and Shifted Keystreams

Slid Pairs for Simplified Plantlet

Slid Pairs for Plantlet

Discussion

Conclusion
Plantlet Stream Cipher

- Lightweight binary additive stream cipher proposed in 2016
  - Mikhailév, Armnecht and Muller
- Keystream generator design based on bit-wise shift registers
  - Similar to Grain, Sprout
- Two inputs:
  - 80-bit secret key
  - 90-bit known initialisation vector (IV)
- Output: a binary sequence of length $\leq 2^{30}$ bits
  - Encryption: XOR this sequence with plaintext
  - Decryption: XOR this sequence with ciphertext
What are Slid Pairs?

- Different (key, IV) pairs that produce phase-shifted versions of the same binary sequence
- Should be hard to find slid pairs or determine relationships
Plantlet Structure

Key store: $M$
$(k_0, k_1, \ldots, k_{79})$

Counter: $C$
$(c_0, c_1, \ldots, c_8)$

NLFSR: $N$
$(n_0, n_1, \ldots, n_{39})$

LFSR: $L$
$(l_0, l_1, \ldots, l_{60})$

$g$

$h$

$z^t$

Joshua Copeland and Leonie Simpson
QUT
Slid Pairs in Plantlet - AISC2020
Plantlet Operation - Modes

Initialisation

- **Loading phase:**
  - First 40 bits of IV loaded into (40-bit) NLFSR
  - Remaining 50 bits of IV loaded into (61-bit) LFSR
  - Remaining LFSR stages loaded with 1’s - except for one 0

- **Diffusion phase:**
  - State update function applied to internal state 320 times
  - Register feedback, key bit $k^t$ and counter bit $c^t$ used in update
  - No keystream output BUT $z^t$ used in both LFSR and NLFSR updates

Keystream generation

- $z^t$ used as keystream only - not in LFSR or NLFSR feedback
Observations: Periodic Subsequences

Key component

- Plantlet makes continuous use of the key - throughout initialisation and keystream generation
- One key bit used as input to NLFSR update at each time step
- $k^t = k_t \mod 80$; periodic with period = 80 or a divisor of 80

Counter component

- 7 bits of C used for simple counter: from 0 to 79 then reset
- Stage 4 content forms input to NLFSR update each time step
- Counter component produces a fixed binary sequence
- $C_4 = (0^{16}1^{16}0^{16}1^{16}0^{16})$; periodic with period = 80
Observations: Register Autonomy?

**LFSR component**

- During **initialisation**, $z^t$ used in LFSR update
- During **keystream generation**, LFSR is autonomous
  - Primitive feedback function and register contents not all-zero at end of initialisation, so LFSR output is binary sequence with period $2^{61} - 1$

**NFSR component**

- NFSR not autonomous in either initialisation or keystream generation
- During **initialisation**, $n_{39}^{t+1} = g(N^t) \oplus z^t \oplus l_0^t \oplus c_4^t \oplus k^t$
- During **keystream generation**, $n_{39}^{t+1} = g(N^t) \oplus l_0^t \oplus c_4^t \oplus k^t$
Can we simplify Plantlet?

- During initialisation and keystream generation, both $M$ and $C$
  - Are autonomous components
  - Produce sequences with period 80, or a divisor of 80
- Outputs of $M \& C (k^t \& c_4^t)$ XORed in NLFSR state update
- Combine both $M$ and $C$ into single component $J$
  - $J$ produces sequence with period 80 (or a divisor of 80)
  - Adjust value of Plantlet key $K$ by combining with 80-bit counter sequence $C_4$
  - Effective key: $K \oplus C_4$
- Simplified Plantlet using $K \oplus C_4$ produces same keystream as Plantlet with $K$
- Simpler design is easier to analyze
  - Acknowledgement of Micah Brown investigation, 2018
Simplified Plantlet Structure

\[
\begin{align*}
\text{NLFSR: } & N \\
& (n_0, n_1, \ldots, n_{39}) \\
\text{LFSR: } & L \\
& (l_0, l_1, \ldots, l_{60}) \\
\text{Effective Key store: } & J \\
& (j_0, j_1, \ldots, j_{79}) \\
\end{align*}
\]
Initialisation

- **Loading phase - same as Original Plantlet:**
  - First 40 bits of IV loaded into (40-bit) NLFSR
  - Remaining 50 bits of IV loaded into (61-bit) LFSR
  - Remaining LFSR stages loaded with 1’s - except for one 0

- **Diffusion phase:**
  - State update function applied to internal state 320 times
  - Register feedback bits and effective key bit $j^t$ used in update
  - No keystream output BUT $z^t$ used in both LFSR and NLFSR updates

Keystream generation

- $z^t$ is used as keystream - not used in LFSR or NLFSR feedback
Slid Pairs for Simplified Plantlet

Consider component $J$ (formed by combining $K$ and $C$)

- $J$ is autonomous
- Output of $J$ is binary sequence, could be produced by cyclic register of length 80
  - Slid pairs can only arise from effective keys which are cyclic shifts of each other
- Fixed format of loaded state does not necessarily imply minimum phase shift
  - Since state update function is different in initialisation and keystream generation modes
- What size phase shifts are possible? Investigate in experiments
Experimental Investigation - Finding Slid Pairs

Experimental trials

- Select a Key and IV: \((J_i, V_j)\)
- Initialise Simplified Plantlet and begin to produce keystream
- At each iteration of keystream generation, consider internal state as candidate initial state
  - Perform initialisation state update function in reverse, 320 times, and check if obtained state has format required for loaded state
- If so, note details of corresponding key, IV and phase shift (it’s a slid pair!)
- Continue producing keystream and checking candidate states until 204,800 bits of keystream have been produced
Experimental Investigation - Finding Slid Pairs

**Experiment Details**

- Experiment performed with 12 different keys, 12 different IVs
  - Some patterned strings: 000...00; 01010101...01, etc
  - Some non-patterned strings
- Each key was used with each IV $\Rightarrow$ 144 trials were conducted
- In each trial (producing 204,800 bits of keystream), we recorded
  - the number of slid pairs occurring
  - the slid pair values $(J_i, V_j)$, and
  - the size of the phase shifts
### Simplified Plantlet Experiment Results

Number of slid pairs found per trial from initial pair \((J_i, V_j)\)

<table>
<thead>
<tr>
<th>ExV</th>
<th>ExK_1</th>
<th>ExK_2</th>
<th>ExK_3</th>
<th>ExK_4</th>
<th>ExK_5</th>
<th>ExK_6</th>
<th>...</th>
<th>ExK_12</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExV_1</td>
<td>102</td>
<td>101</td>
<td>94</td>
<td>91</td>
<td>88</td>
<td>78</td>
<td>...</td>
<td>97</td>
</tr>
<tr>
<td>ExV_2</td>
<td>98</td>
<td>78</td>
<td>94</td>
<td>93</td>
<td>89</td>
<td>78</td>
<td>...</td>
<td>100</td>
</tr>
<tr>
<td>ExV_3</td>
<td>91</td>
<td>99</td>
<td>94</td>
<td>98</td>
<td>90</td>
<td>97</td>
<td>...</td>
<td>93</td>
</tr>
<tr>
<td>ExV_4</td>
<td>101</td>
<td>97</td>
<td>108</td>
<td>103</td>
<td>124</td>
<td>90</td>
<td>...</td>
<td>107</td>
</tr>
<tr>
<td>ExV_5</td>
<td>98</td>
<td>110</td>
<td>89</td>
<td>112</td>
<td>103</td>
<td>91</td>
<td>...</td>
<td>94</td>
</tr>
<tr>
<td>ExV_6</td>
<td>99</td>
<td>93</td>
<td>97</td>
<td>92</td>
<td>88</td>
<td>104</td>
<td>...</td>
<td>129</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>ExV_10</td>
<td>80</td>
<td>107</td>
<td>93</td>
<td>82</td>
<td>109</td>
<td>99</td>
<td>...</td>
<td>109</td>
</tr>
<tr>
<td>ExV_11</td>
<td>93</td>
<td>83</td>
<td>105</td>
<td>106</td>
<td>104</td>
<td>100</td>
<td>...</td>
<td>95</td>
</tr>
<tr>
<td>ExV_12</td>
<td>89</td>
<td>100</td>
<td>99</td>
<td>96</td>
<td>92</td>
<td>91</td>
<td>...</td>
<td>112</td>
</tr>
</tbody>
</table>
## Simplified Plantlet Experiment Results

### Size of Phase Shifts (Minimum, Mean, Maximum)

<table>
<thead>
<tr>
<th></th>
<th>$ExK_1$</th>
<th>$ExK_2$</th>
<th>$ExK_3$</th>
<th>$ExK_4$</th>
<th>$ExK_5$</th>
<th>...</th>
<th>$ExK_{12}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$ExV_1$</td>
<td>17</td>
<td>4</td>
<td>14</td>
<td>6</td>
<td>62</td>
<td>...</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>1,989</td>
<td>2,026</td>
<td>2,168</td>
<td>2,239</td>
<td>2,315</td>
<td>...</td>
<td>2,102</td>
</tr>
<tr>
<td></td>
<td>12,441</td>
<td>12,832</td>
<td>9,176</td>
<td>13,114</td>
<td>14,250</td>
<td>...</td>
<td>9,805</td>
</tr>
<tr>
<td>$ExV_2$</td>
<td>70</td>
<td>73</td>
<td>5</td>
<td>14</td>
<td>5</td>
<td>...</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>2,086</td>
<td>2,627</td>
<td>2,141</td>
<td>2,156</td>
<td>2,245</td>
<td>...</td>
<td>2,038</td>
</tr>
<tr>
<td></td>
<td>9,510</td>
<td>10,578</td>
<td>13,402</td>
<td>9,433</td>
<td>14,408</td>
<td>...</td>
<td>7,676</td>
</tr>
<tr>
<td>$ExV_{12}$</td>
<td>72</td>
<td>7</td>
<td>26</td>
<td>1</td>
<td>21</td>
<td>...</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2,223</td>
<td>2,009</td>
<td>2,042</td>
<td>2,121</td>
<td>2,197</td>
<td>...</td>
<td>1,774</td>
</tr>
<tr>
<td></td>
<td>15,927</td>
<td>13,302</td>
<td>9,118</td>
<td>9,096</td>
<td>10,862</td>
<td>...</td>
<td>8,679</td>
</tr>
</tbody>
</table>
Slid Pairs for Simplified Plantlet

Main findings

Slid pairs found in all trials

- Minimum number found: 72 (for \( ExK_7, ExV_1 \))
- Maximum number found: 129 (for \( ExK_{12}, ExV_6 \))
- Inspection of keys in slid pairs revealed
  - All keys in slid pairs are cyclic shifts of key used
  - Occurrence approximates proportion of distinct keys possible

Phase shift for slid pairs

- Minimum phase shift \(< 10\) in over 30% of trials
- Mean phase shift approx 2000
Slid Pairs for Plantlet

Relationship between Simplified Plantlet and Plantlet Keys

- For a given IV, the sequence produced by Plantlet with key $K$ can be produced by Simplified Plantlet with key $J = K \oplus C_4$

Phase Shifts and Slid Pairs

- Suppose for Simplified Plantlet, $(J_0, V_0)$ produces a keystream, and $(J_1, V_1)$ produces an $\alpha$ shifted keystream
- Consider the Plantlet keys that produce these sequences
  - Clearly, $K_0 = J_0 \oplus C_4$
  - Similarly, if $\alpha \mod 80 = 0$, then $K_1 = J_1 \oplus C_4 = K_0$
  - If $\alpha \mod 80 \neq 0$, then obtaining $K_1$ involves correcting for out-of-phase counter sequence: $K_1 = J_1 \oplus C_4 \oplus C_4 \lll \alpha \mod 80$
Suppose Plantlet is used with key $K_0$ to produce keystream.

The keys in slid pairs with phase shift $\alpha$ are of the form

$($$K_0 \ll (\alpha \mod 80)) \oplus (C_4 \ll (\alpha \mod 80)) \oplus C_4$$

To verify the Slid Pairs key relationship, experiments were performed following the process used for Simplified Plantlet.

- Slid Pairs found in all experimental trials
- Minimum number found: 69 (for $ExK_9$, $ExV_6$)
- Maximum number found: 122 (for $ExK_1$, $ExV_6$)
- Phase shifts of less than 10 occurred in 28% of trials
Discussion

- For both Simplified Plantlet and Plantlet, slid pairs occurred for all (Key, IV) pairs used in our experiments
  - Average phase shift approx. 2000, can be as small as 1
- For Simplified Plantlet, keys in slid pairs are cyclic shifts
  - Implication for patterned keys if period of key sequence < 80
  - Example: 01010101...01
- For Plantlet, relationship between keys in slid pairs slightly more complex
  - Combination of a cyclic shift of the key with a masking value obtained from the counter sequence
  - \((K_0 \ll (\alpha \mod 80)) \oplus (C_4 \ll (\alpha \mod 80)) \oplus C_4\)
  - Since counter sequence has period 80, there are 79 effective masking values
Conclusion

- Where multiple keystreams will be produced from different (Key,IV) inputs, Plantlet keystreams are not all distinct and unpredictable - a relationship has been established.
- Use the relationship between keys giving rise to slid pairs to divide the keyspace.
  - Form sets of keys that can produce shifted keystreams.
  - Size of each set is at most 80.
- May be able to exploit this in TMD attacks - future work.
Questions?