Automated Analysis and Synthesis of Block-Cipher Modes of Operation
Alex J. Malozemoff, Jonathan Katz, and Matthew D. Green

Introduction
- **Block cipher**: Encrypts fixed-length message
- **Mode of operation**: Encrypts arbitrary-length message using block cipher as building block
- **Problem**: Lots of modes exist, each needs to be proven secure independently
- **Solution**: Use program synthesis techniques to automatically prove modes secure

Model
- View single block of mode as directed graph
- Edges correspond to intermediate values
- Set of labels (fam, type, flags) on edges
  - fam: Families to which value on edge belongs
  - type ∈ {⊥, R}: “Type” of value on edge
    - ⊥ represents “adversarially controlled”
    - R represents “random”
  - flags ∈ \{0, 1\}²: Bit-vector denoting whether value can be input to OUT/PRP
- Constraints on how to label edges
  - E.g., ⊥ type can never be input to OUT/PRP
  - E.g., One input to XOR must have type R

Main Result
- **Meta-Theorem**: If graph can be labeled while satisfying constraints, associated mode is secure
- **Corollary**: Can use SAT solver to automatically find secure modes!

Example: CBC mode
- GENRAND
- DUP
- OUT
- NEXTIV

Example: CBC mode as a graph
- GENRAND
- DUP
- OUT
- NEXTIV

Example: CBC graph with labeling
- GENRAND
  - \{(1), R, 11\}
- DUP
  - \{(1), R, 01\}
- OUT
  - \{(1), R, 01\}
- NEXTIV
  - \{(1), R, 01\}

Further Information

Results
- | # Instructions | Valid | Decryptable | Secure |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1–6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>78</td>
<td>67</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>661</td>
<td>515</td>
<td>24</td>
</tr>
<tr>
<td>9</td>
<td>3467</td>
<td>1823</td>
<td>115</td>
</tr>
<tr>
<td>10</td>
<td>5136</td>
<td>1187</td>
<td>163</td>
</tr>
<tr>
<td>Total</td>
<td>9342</td>
<td>3592</td>
<td>309</td>
</tr>
</tbody>
</table>

Acknowledgments
Work of Alex Malozemoff was conducted with Government support awarded by DoD, Air Force Office of Scientific Research, National Defense Science and Engineering Graduate (NDSEG) Fellowship, 32 CFR 168a. Work of Jonathan Katz was done for Exelis under contract number N00173-11-C-2045 to NRL. Work of Matthew Green was supported by the U.S. Defense Advanced Research Projects Agency (DARPA) and the Air Force Research Laboratory (AFRL) under contract FA8750-11-2-0211. The authors thank M. Hicks and J. Foster for comments on an earlier draft of this work.