Noname manuscript No.
(will be inserted by the editor)

Appendix to *Kite attack: reshaping the cube attack for a flexible GPU-based maxterm search*

Marco Cianfriglia[0000−0002−6775−7804] · **Stefano Guarino**[0000−0002−1545−7711] · **Massimo Bernaschi**[0000−0003−3661−9836] · **Flavio Lombardi**[0000−0003−0723−7847] · **Marco Pedicini**[0000−0002−9016−074X]

Received: / Accepted: date

1 Tables of maxterms and superpolys

M. Cianfriglia · S. Guarino · M. Bernaschi · F. Lombardi
Istituto per le Applicazioni del Calcolo "Mauro Picone"
Consiglio Nazionale delle Ricerche
Rome, Italy
E-mail: m.cianfriglia@iac.cnr.it, s.guarino@iac.cnr.it, m.bernaschi@iac.cnr.it, f.lombardi@iac.cnr.it

M. Pedicini
Department of Mathematics and Physics
Roma Tre University
E-mail: marco.pedicini@uniroma3.it

maxterm bits	superpoly	round
3, 6, 8, 10, 12, 14, 18, 19, 20, 23, 25, 27, 31, 33, 38, 40, 43, 45, 48, 53, 54, 56, 58, 60, 62, 63, 69, 75, 77, 79, 80	x_{55}	781
1, 5, 7, 8, 10, 15, 16, 18, 20, 23, 25, 27, 32, 33, 36, 38, 40, 41, 43, 47, 49, 52, 53, 54, 56, 58, 63, 69, 71, 75, 77, 80	x_{69}	781
1, 6, 7, 8, 10, 12, 16, 19, 21, 24, 25, 27, 31, 33, 36, 38, 40, 41, 43, 47, 49, 52, 53, 56, 58, 63, 67, 69, 71, 73, 77, 80	x_{60}	781
1, 2, 3, 5, 6, 7, 8, 12, 14, 15, 16, 19, 21, 23, 25, 27, 36, 38, 40, 43, 45, 47, 49, 54, 56, 58, 60, 62, 69, 71, 73, 74, 80	$x_{51} + 1$	781
1, 2, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 23, 25, 27, 36, 38, 40, 43, 45, 47, 52, 54, 56, 58, 60, 62, 69, 71, 73, 76, 79, 80	x_{45}	781
1, 2, 5, 6, 7, 8, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 43, 45, 47, 49, 52, 54, 56, 58, 62, 65, 69, 71, 73, 76, 80	$x_{43} + x_{58}$	781
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 23, 27, 33, 36, 38, 40, 43, 45, 47, 52, 54, 56, 58, 60, 62, 69, 71, 73, 74, 79, 80	x_{23}	781
1, 3, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 33, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 65, 69, 71, 75, 77, 79, 80	$x_8 + x_{35} + x_{64}$	781
1, 5, 7, 8, 10, 12, 14, 15, 16, 18, 20, 23, 24, 25, 27, 32, 33, 36, 40, 41, 43, 47, 49, 52, 53, 56, 58, 63, 69, 71, 75, 77, 80	$x_{67} + 1$	781
3, 5, 6, 8, 10, 12, 14, 16, 18, 19, 20, 23, 24, 25, 27, 31, 33, 38, 43, 45, 48, 53, 54, 56, 58, 60, 62, 63, 69, 75, 77, 79, 80	x_2	781
6, 8, 10, 12, 14, 15, 16, 18, 19, 20, 21, 23, 25, 27, 29, 31, 33, 36, 38, 40, 41, 42, 45, 49, 54, 56, 60, 62, 63, 69, 73, 75, 80	x_{58}	781
1, 2, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 23, 27, 36, 38, 40, 43, 45, 47, 49, 52, 54, 56, 58, 60, 62, 69, 71, 73, 74, 76, 79, 80	$x_{62} + 1$	781
1, 3, 5, 6, 8, 10, 12, 14, 15, 16, 19, 21, 25, 30, 31, 32, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 54, 56, 63, 69, 71, 73, 75, 80	$x_3 + x_{25} + x_{39} + x_{40} + x_{51} + x_{66} + x_{67} + x_{78} + 1$	781
1, 3, 5, 6, 8, 12, 14, 15, 16, 19, 21, 25, 27, 31, 33, 38, 40, 41, 43, 45, 47, 48, 49, 50, 53, 54, 56, 60, 63, 69, 71, 73, 75, 80	$x_{10} + x_{13} + x_{14} + x_{19} + x_{25} + x_{28} + x_{29} + x_{31} + x_{37} + x_{40} + x_{46} + x_{52} + x_{53} + x_{55} + x_{56} + x_{57} + x_{60} + x_{61} + x_{62} + x_{64} + x_{66} + x_{68} + x_{69} + 1$	781
1, 3, 5, 7, 12, 14, 15, 16, 18, 19, 20, 21, 24, 25, 27, 31, 33, 36, 40, 41, 45, 49, 54, 56, 58, 60, 62, 63, 66, 71, 73, 75, 77, 80	x_{57}	781
1, 3, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 33, 36, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 61, 63, 65, 69, 71, 75, 77, 79, 80	$x_{43} + x_{58} + x_{64} + x_{66} + x_{70}$	781
1, 3, 5, 6, 7, 8, 12, 13, 14, 15, 16, 19, 21, 23, 25, 27, 36, 38, 40, 43, 45, 47, 49, 52, 54, 56, 58, 62, 65, 69, 71, 73, 76, 79, 80	x_{65}	781
1, 3, 5, 6, 8, 10, 12, 14, 15, 16, 18, 19, 24, 25, 31, 32, 33, 36, 38, 40, 41, 43, 45, 47, 49, 50, 53, 54, 56, 63, 69, 71, 73, 75, 80	$x_{23} + x_{39} + x_{50} + x_{66} + x_{67} + x_{79} + 1$	781
1, 3, 5, 6, 8, 10, 12, 14, 15, 16, 18, 19, 25, 30, 31, 32, 33, 38, 40, 41, 43, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 71, 73, 75, 80	$x_9 + x_{18} + x_{24} + x_{26} + x_{32} + x_{33} + x_{34} + x_{42} + x_{51} + x_{53} + x_{54} + x_{58} + x_{59} + x_{64} + x_{66} + x_{68} + x_{69} + x_{80} + 1$	781
1, 3, 5, 6, 8, 10, 12, 14, 15, 16, 19, 21, 24, 25, 31, 32, 33, 36, 38, 40, 41, 43, 45, 47, 49, 50, 53, 54, 56, 63, 69, 71, 73, 75, 80	$x_{52} + x_{66} + x_{67} + x_{79}$	781
1, 3, 5, 6, 8, 12, 14, 15, 16, 18, 19, 21, 25, 27, 31, 33, 38, 40, 41, 43, 45, 47, 48, 49, 50, 53, 54, 56, 60, 63, 69, 71, 73, 75, 80	$x_{13} + x_{14} + x_{19} + x_{25} + x_{27} + x_{28} + x_{29} + x_{31} + x_{39} + x_{41} + x_{42} + x_{46} + x_{51} + x_{52} + x_{54} + x_{55} + x_{56} + x_{57} + x_{61} + x_{62} + x_{64} + x_{65} + x_{66} + x_{69} + x_{78}$	781
1, 3, 5, 6, 8, 12, 14, 15, 16, 18, 19, 24, 25, 27, 31, 32, 33, 36, 38, 40, 41, 45, 47, 48, 49, 53, 54, 56, 60, 63, 69, 71, 73, 75, 80	$x_{16} + x_{26} + x_{27} + x_{38} + x_{43} + x_{53} + x_{54} + x_{56} + x_{65} + x_{67} + x_{80}$	781
1, 3, 5, 6, 8, 12, 14, 15, 16, 19, 21, 24, 25, 30, 31, 32, 33, 36, 38, 40, 41, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 71, 73, 75, 80	$x_{25} + x_{27} + x_{30} + x_{54} + x_{57}$	781
1, 2, 3, 5, 6, 7, 8, 12, 14, 15, 16, 19, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 52, 54, 56, 58, 60, 62, 65, 69, 70, 71, 73, 74, 76, 80	x_{42}	781
1, 3, 5, 6, 8, 10, 12, 14, 15, 16, 18, 19, 21, 25, 27, 30, 31, 32, 33, 38, 40, 41, 43, 45, 47, 48, 49, 53, 54, 56, 63, 69, 71, 73, 75, 80	$x_{14} + x_{29} + x_{41} + x_{55} + x_{61} + x_{62}$	781
1, 3, 5, 6, 8, 10, 12, 14, 15, 16, 18, 19, 24, 25, 31, 32, 33, 36, 38, 40, 41, 43, 45, 47, 48, 49, 50, 53, 54, 56, 63, 69, 71, 73, 75, 80	$x_{39} + x_{66}$	781
1, 3, 5, 6, 8, 10, 12, 14, 15, 16, 18, 19, 25, 30, 31, 32, 33, 38, 40, 41, 43, 45, 47, 48, 49, 50, 53, 54, 56, 60, 63, 69, 71, 73, 75, 80	$x_{24} + x_{55} + x_{61} + x_{66} + x_{67} + 1$	781
1, 3, 5, 6, 8, 10, 12, 14, 15, 16, 19, 21, 24, 25, 30, 31, 33, 38, 40, 41, 43, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 70, 71, 73, 75, 80	$x_{12} + x_{27} + x_{32} + x_{33} + x_{40} + x_{42} + x_{51} + x_{53} + x_{57} + x_{58} + x_{60} + x_{64} + x_{80} + 1$	781
1, 3, 5, 6, 8, 10, 12, 14, 15, 16, 19, 21, 24, 25, 30, 31, 33, 38, 40, 41, 43, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 70, 71, 73, 75, 80	$x_{27} + x_{32} + x_{42} + x_{53} + x_{58} + x_{60} + x_{64} + x_{78} + x_{80} + 1$	781
1, 3, 5, 6, 8, 12, 14, 15, 16, 18, 19, 24, 25, 27, 30, 31, 32, 33, 38, 40, 41, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 70, 71, 73, 75, 80	$x_{11} + x_{24} + x_{25} + x_{29} + x_{30} + x_{31} + x_{40} + x_{41} + x_{45} + x_{50} + x_{52} + x_{53} + x_{54} + x_{56} + x_{58} + x_{61} + x_{65} + x_{66} + x_{67} + x_{68} + x_{77} + x_{79} + x_{80} + 1$	781
1, 3, 5, 6, 8, 12, 14, 15, 16, 19, 21, 24, 25, 30, 31, 32, 33, 36, 38, 40, 41, 43, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 71, 73, 75, 80	$x_{14} + x_{16} + x_{27} + x_{29} + x_{30} + x_{31} + x_{40} + x_{41} + x_{42} + x_{43} + x_{54} + x_{55} + x_{56} + x_{57} + x_{58} + x_{64} + x_{79} + x_{80} + 1$	781
1, 3, 5, 6, 8, 12, 14, 15, 16, 19, 21, 24, 25, 30, 31, 32, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 54, 56, 60, 63, 69, 70, 71, 73, 75, 80	$x_{28} + x_{29} + x_{32} + x_{33} + x_{40} + x_{41} + x_{42} + x_{44} + x_{50} + x_{51} + x_{55} + x_{56} + x_{57} + x_{59} + x_{61} + x_{62} + x_{64} + x_{66} + x_{67} + x_{68} + x_{70} + x_{78} + 1$	781
1, 3, 5, 6, 8, 12, 14, 15, 16, 19, 21, 24, 25, 30, 31, 33, 36, 38, 40, 41, 43, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 70, 71, 73, 75, 80	$x_{38} + x_{39} + x_{41} + x_{44} + x_{45} + x_{50} + x_{51} + x_{52} + x_{53} + x_{55} + x_{57} + x_{58} + x_{60} + x_{66} + x_{68} + x_{72} + x_{78} + x_{79} + 1$	781
1, 3, 5, 6, 8, 12, 14, 15, 16, 19, 21, 24, 25, 31, 33, 36, 38, 40, 41, 43, 45, 47, 48, 49, 50, 53, 54, 56, 60, 63, 69, 70, 71, 73, 75, 80	$x_{43} + x_{50} + x_{52} + x_{55} + x_{58} + x_{66} + x_{70} + x_{77} + 1$	781

Table 1: Maxterms and superpolys after 781 initialization rounds of Trivium (continue).

maxterm bits	superpoly	round
1, 5, 6, 8, 12, 14, 15, 16, 18, 19, 24, 25, 27, 30, 31, 32, 33, 38, 40, 41, 43, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 70, 71, 73, 75, 80	$x_{41} + x_{53} + x_{55} + x_{58} + x_{61} + x_{68}$	781
1, 5, 6, 8, 12, 14, 15, 16, 18, 19, 24, 25, 27, 30, 31, 32, 33, 38, 40, 41, 43, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 70, 71, 73, 75, 80	$x_{29} + x_{41} + x_{42} + x_{53} + x_{55} + x_{56} + x_{58} + x_{61} + x_{64} + x_{66} + x_{67} + x_{68} + x_{69}$	781
1, 5, 6, 8, 12, 14, 15, 16, 18, 19, 24, 25, 27, 30, 31, 32, 33, 38, 40, 41, 43, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 70, 71, 73, 75, 80	$x_{14} + x_{55} + x_{58} + x_{61} + x_{64} + x_{66} + x_{68} + x_{80}$	781
1, 5, 6, 10, 12, 14, 15, 18, 19, 20, 21, 22, 23, 25, 27, 28, 29, 31, 33, 36, 38, 40, 41, 42, 45, 48, 49, 54, 60, 62, 63, 69, 73, 75, 77, 80	x_{64}	781
5, 6, 8, 10, 12, 14, 15, 16, 18, 19, 20, 21, 22, 23, 25, 27, 29, 31, 33, 36, 38, 40, 41, 42, 45, 48, 49, 54, 60, 62, 63, 69, 73, 75, 77, 80	$x_{66} + 1$	781
1, 2, 3, 5, 6, 7, 8, 12, 13, 14, 15, 16, 19, 21, 23, 27, 33, 36, 38, 40, 43, 45, 47, 52, 54, 56, 58, 60, 62, 69, 70, 71, 73, 74, 76, 79, 80	x_{56}	781
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 33, 36, 40, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 65, 69, 71, 74, 75, 77, 78, 79, 80	$x_{21} + x_{36} + x_{48} + x_{58} + x_{63} + 1$	781
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 33, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 65, 69, 71, 74, 75, 77, 78, 79, 80	$x_{19}+x_{27}+x_{45}+x_{54}+x_{64}+x_{66}+x_{72}+1$	781
1, 3, 5, 6, 8, 12, 14, 15, 16, 18, 19, 24, 25, 30, 31, 32, 33, 36, 38, 40, 41, 43, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 70, 71, 73, 75, 80	$x_5 + x_8 + x_{24} + x_{26} + x_{32} + x_{33} + x_{39} + x_{40} + x_{41} + x_{42} + x_{44} + x_{47} + x_{51} + x_{54} + x_{57} + x_{59} + x_{60} + x_{65} + x_{66} + x_{68} + x_{69} + x_{78} + x_{79}$	781
1, 3, 5, 6, 8, 12, 14, 15, 16, 19, 21, 25, 27, 31, 32, 33, 36, 38, 40, 41, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 71, 73, 75, 80	$x_{25} + x_{52} + 1$	782
1, 5, 6, 7, 8, 10, 12, 14, 15, 19, 21, 24, 25, 27, 31, 36, 38, 39, 40, 41, 45, 47, 49, 53, 56, 58, 62, 63, 66, 69, 71, 73, 77, 80	x_{40}	782
1, 3, 5, 6, 7, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 56, 58, 61, 62, 63, 65, 69, 71, 74, 75, 77, 78	$x_{25} + 1$	782
1, 3, 5, 6, 10, 12, 14, 15, 16, 18, 19, 21, 25, 27, 31, 32, 33, 38, 40, 41, 43, 45, 47, 48, 49, 50, 53, 54, 56, 60, 63, 69, 71, 73, 75, 80	$x_{13} + x_{16} + x_{19} + x_{25} + x_{29} + x_{33} + x_{35} + x_{36} + x_{37} + x_{38} + x_{39} + x_{40} + x_{42} + x_{45} + x_{51} + x_{52} + x_{53} + x_{54} + x_{55} + x_{62} + x_{63} + x_{64} + x_{65} + x_{67} + x_{69} + x_{70} + x_{71} + x_{73} + x_{79} + x_{80} + 1$	782
5, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 34, 36, 38, 40, 45, 47, 48, 49, 53, 54, 56, 58, 60, 62, 63, 69, 71, 80	$x_{38} + 1$	783
3, 5, 6, 7, 8, 10, 14, 15, 16, 21, 23, 25, 27, 33, 34, 36, 38, 40, 45, 47, 48, 49, 53, 54, 55, 56, 58, 61, 62, 63, 69, 71, 74, 80	$x_{27} + 1$	783
1, 5, 6, 8, 10, 12, 14, 15, 16, 18, 19, 21, 24, 25, 27, 30, 31, 32, 33, 38, 40, 41, 45, 47, 48, 49, 50, 53, 54, 56, 63, 69, 71, 73, 75, 80	$x_{32} + x_{49} + x_{52} + x_{56} + x_{59} + x_{61} + x_{62} + x_{79} + 1$	783
1, 5, 6, 8, 10, 12, 14, 15, 16, 18, 19, 21, 24, 25, 31, 33, 36, 38, 40, 41, 43, 45, 47, 48, 49, 50, 53, 54, 56, 60, 63, 69, 71, 73, 75, 80	$x_7+x_{16}+x_{40}+x_{43}+x_{49}+x_{52}+x_{58}+x_{62}+x_{70}+x_{79}+1$	783
1, 3, 5, 6, 8, 10, 12, 14, 15, 16, 18, 19, 24, 25, 30, 31, 32, 33, 36, 38, 40, 41, 43, 45, 47, 49, 50, 53, 54, 56, 60, 63, 69, 71, 73, 75, 80	$x_{26} + x_{66} + x_{68} + 1$	783
1, 3, 6, 7, 10, 12, 15, 16, 19, 21, 23, 25, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 63, 65, 69, 71, 75, 77, 80	x_4	784
1, 5, 6, 7, 8, 10, 12, 14, 15, 16, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 55, 56, 58, 60, 62, 63, 67, 69, 71, 80	$x_{53} + 1$	784
1, 6, 8, 10, 12, 14, 15, 16, 18, 19, 20, 21, 22, 23, 25, 27, 29, 33, 36, 38, 40, 41, 42, 45, 48, 49, 54, 60, 62, 63, 69, 73, 75, 80	x_{37}	784
3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 60, 62, 63, 69, 71, 74, 80	x_{36}	784
1, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 29, 31, 33, 36, 38, 40, 41, 45, 47, 49, 53, 58, 60, 63, 71, 75, 76, 80	$x_{12} + 1$	785
1, 3, 6, 7, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 63, 65, 69, 71, 74, 75, 77, 78, 80	x_{34}	785
1, 5, 6, 7, 8, 12, 13, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 52, 54, 56, 58, 60, 62, 69, 71, 73, 79, 80	x_{54}	785
1, 3, 5, 6, 7, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 69, 71, 74, 75, 77, 78, 80	$x_{13} + x_{55} + x_{60} + x_{64}$	785
1, 3, 5, 6, 7, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 65, 69, 71, 74, 75, 77, 78, 80	$x_{22} + x_{49} + x_{64}$	786
1, 3, 6, 7, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 65, 69, 71, 74, 75, 77, 78, 80	$x_{14} + x_{23} + x_{41} + x_{47} + x_{49} + x_{50} + x_{58} + x_{64}$	786
1, 3, 5, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 65, 69, 71, 74, 75, 77, 78, 80	$x_3+x_4+x_{20}+x_{22}+x_{30}+x_{34}+x_{38}+x_{40}+x_{42}+x_{45}+x_{49}+x_{51}+x_{58}+x_{61}+x_{65}+x_{67}+x_{69}+x_{72}+x_{78}$	786
1, 3, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 38, 40, 43, 45, 47, 49, 53, 56, 58, 62, 63, 69, 71, 75, 77, 79	$x_9+x_{29}+x_{30}+x_{32}+x_{42}+x_{43}+x_{49}+x_{51}+x_{57}+x_{58}+x_{59}+x_{60}+x_{62}+x_{64}+x_{66}+x_{67}+x_{68}+x_{69}+x_{70}+x_{72}+x_{76}$	791
1, 3, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 36, 40, 41, 43, 45, 47, 49, 53, 56, 58, 62, 63, 69, 71, 75, 77, 80	$x_{17}+x_{26}+x_{30}+x_{32}+x_{41}+x_{43}+x_{47}+x_{57}+x_{62}+x_{65}+x_{66}+x_{70}+x_{72}+x_{74}+1$	791
1, 3, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 36, 40, 41, 43, 45, 47, 49, 53, 56, 58, 62, 63, 69, 71, 75, 77, 80	$x_{14} + x_{17} + x_{26} + x_{30} + x_{43} + x_{47} + x_{50} + x_{57} + x_{58} + x_{59} + x_{65} + x_{70} + x_{72} + x_{74} + x_{77} + 1$	791
1, 3, 5, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 40, 41, 43, 45, 47, 49, 53, 56, 58, 63, 65, 69, 71, 75, 77, 79	$x_{12}+x_{26}+x_{30}+x_{39}+x_{41}+x_{45}+x_{47}+x_{57}+x_{58}+x_{59}+x_{62}+x_{64}+x_{74}+x_{76}+1$	791
1, 3, 5, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 56, 58, 62, 63, 65, 69, 71, 75, 77	$x_5+x_{18}+x_{20}+x_{26}+x_{28}+x_{29}+x_{30}+x_{31}+x_{32}+x_{41}+x_{42}+x_{44}+x_{50}+x_{51}+x_{56}+x_{57}+x_{62}+x_{64}+x_{67}+x_{69}+x_{70}+x_{71}+x_{74}+x_{77}+x_{78}+1$	791

Table 1: Maxterms and superpolys after 781 initialization rounds of Trivium (continue).

maxterm bits	superpoly	round
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 38, 40, 41, 43, 45, 47, 49, 53, 56, 58, 61, 62, 63, 65, 69, 71, 75, 77	$x_1+x_{28}+x_{32}+x_{47}+x_{58}+x_{59}+x_{62}+x_{64}+x_{74}$	791
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 40, 41, 43, 45, 47, 49, 53, 56, 58, 61, 62, 63, 65, 69, 71, 75, 77, 80	$x_{10}+x_{11}+x_{12}+x_{13}+x_{15}+x_{17}+x_{19}+x_{20}+x_{29}+x_{31}+x_{32}+x_{33}+x_{37}+x_{39}+x_{40}+x_{41}+x_{42}+x_{44}+x_{46}+x_{48}+x_{49}+x_{50}+x_{53}+x_{57}+x_{60}+x_{67}+x_{70}+x_{71}+x_{76}+x_{78}+x_{79}$	791
1, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 29, 31, 33, 36, 38, 40, 41, 42, 45, 47, 49, 53, 58, 63, 69, 71, 72, 76, 79, 80	x_{61}	791
1, 3, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 69, 71, 74, 75, 77, 78, 80	$x_{43}+x_{47}+x_{58}+x_{70}+x_{74}+1$	791
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 38, 40, 41, 43, 45, 47, 49, 53, 56, 58, 62, 63, 69, 71, 75, 77, 80	$x_{12}+x_{17}+x_{26}+x_{27}+x_{29}+x_{30}+x_{32}+x_{40}+x_{43}+x_{45}+x_{46}+x_{49}+x_{53}+x_{54}+x_{56}+x_{59}+x_{62}+x_{64}+x_{65}+x_{67}+x_{69}+x_{72}+x_{74}+x_{75}$	792
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 56, 58, 61, 63, 69, 71, 75, 77, 78, 79, 80	$x_{12}+x_{14}+x_{26}+x_{30}+x_{40}+x_{41}+x_{47}+x_{48}+x_{56}+x_{66}+x_{67}+x_{68}+x_{74}+x_{75}+1$	792
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 63, 69, 71, 74, 75, 77, 78, 79, 80	$x_{16}+x_{43}+x_{56}$	792
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 63, 65, 69, 71, 75, 77, 78, 79, 80	$x_{14}+x_{16}+x_{26}+x_{29}+x_{30}+x_{41}+x_{45}+x_{55}+x_{56}+x_{59}+x_{62}+x_{64}+x_{66}+x_{68}+x_{70}+x_{71}+x_{72}+1$	792
1, 3, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 61, 63, 69, 71, 75, 77, 80	$x_{45}+x_{72}$	793
1, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 30, 31, 33, 38, 40, 43, 45, 47, 49, 51, 52, 56, 58, 63, 67, 69, 71, 73, 77, 80	$x_{10}+x_{55}$	798
1, 3, 5, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 65, 69, 71, 74, 75, 77, 80	$x_{36}+x_{52}+x_{60}+x_{63}$	798
1, 3, 5, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 65, 69, 71, 74, 75, 77, 80	$x_6+x_{11}+x_{25}+x_{33}+x_{36}+x_{53}+x_{60}+x_{62}+x_{63}+x_{64}+x_{79}$	798

Table 1: Maxterms and superpolys after 781 initialization rounds of Trivium.

maxterm bits	superpoly	round
1, 3, 6, 7, 10, 12, 15, 16, 19, 21, 23, 25, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 63, 65, 69, 71, 75, 77, 80	x_4	784
1, 5, 6, 8, 10, 12, 14, 15, 16, 18, 19, 20, 21, 23, 25, 27, 29, 31, 33, 36, 38, 40, 41, 42, 45, 49, 54, 60, 62, 69, 73, 75, 80	x_{60}	784
5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 67, 69, 71, 80	$x_{56} + 1$	784
1, 3, 5, 6, 7, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 63, 65, 69, 71, 75, 77, 78	$x_2+x_9+x_{13}+x_{14}+x_{22}+x_{23}+x_{30}+x_{36}+x_{38}+x_{39}+x_{40}+x_{42}+x_{47}+x_{48}+x_{51}+x_{56}+x_{65}+x_{67}+x_{68}+x_{69}+x_{74}+x_{75}$	784
1, 3, 5, 6, 8, 10, 12, 14, 15, 16, 19, 21, 25, 30, 31, 32, 33, 38, 40, 41, 43, 45, 47, 48, 49, 50, 53, 54, 56, 63, 69, 71, 75, 80	x_{38}	784
1, 3, 6, 7, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 61, 63, 69, 71, 75, 77, 78, 79	$x_{38} + x_{47} + x_{74}$	784
1, 5, 6, 7, 8, 10, 12, 14, 15, 16, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 55, 56, 58, 60, 62, 63, 67, 69, 71, 80	$x_{53} + 1$	784
1, 5, 6, 7, 8, 10, 12, 14, 15, 16, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 67, 69, 71, 74, 80	x_{58}	784
1, 6, 8, 10, 12, 14, 15, 16, 18, 19, 20, 21, 22, 23, 25, 27, 29, 33, 36, 38, 40, 41, 42, 45, 48, 49, 54, 60, 62, 63, 69, 73, 75, 80	x_{37}	784
1, 6, 8, 10, 12, 14, 15, 16, 18, 19, 20, 21, 22, 23, 25, 27, 29, 33, 36, 38, 40, 41, 45, 48, 49, 54, 56, 60, 62, 69, 73, 75, 77, 80	x_{64}	784
3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 60, 62, 63, 69, 71, 74, 80	x_{36}	784
6, 8, 10, 12, 14, 15, 16, 18, 19, 20, 21, 22, 23, 25, 27, 29, 33, 36, 38, 40, 41, 45, 48, 49, 54, 56, 60, 62, 63, 69, 73, 75, 77, 80	x_{66}	784
5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 34, 36, 38, 40, 43, 45, 47, 49, 53, 54, 55, 56, 58, 60, 62, 63, 69, 71, 74, 80	$x_{67} + 1$	784
5, 6, 8, 10, 12, 14, 15, 18, 19, 20, 21, 22, 23, 25, 27, 28, 29, 31, 33, 36, 38, 40, 41, 42, 45, 49, 54, 60, 62, 63, 69, 73, 75, 77, 80	x_{62}	784
1, 5, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 34, 36, 38, 40, 43, 45, 47, 48, 49, 53, 54, 56, 58, 60, 61, 62, 63, 69, 71, 74, 80	$x_{69} + 1$	784
3, 5, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 48, 49, 53, 54, 56, 58, 60, 61, 62, 63, 67, 69, 71, 74, 80	x_{40}	784
1, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 29, 31, 33, 36, 38, 40, 41, 45, 47, 49, 53, 58, 60, 63, 71, 75, 76, 80	$x_{12} + 1$	785
1, 5, 6, 7, 10, 12, 16, 19, 21, 23, 24, 25, 27, 31, 33, 36, 38, 40, 41, 43, 47, 49, 52, 56, 58, 60, 63, 67, 69, 71, 73, 77, 80	x_{42}	785
1, 5, 6, 10, 12, 14, 15, 16, 19, 21, 25, 27, 30, 31, 33, 36, 38, 40, 41, 43, 45, 47, 48, 49, 53, 54, 56, 63, 69, 71, 73, 75, 80	x_{55}	785
1, 3, 6, 7, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 63, 65, 69, 71, 74, 75, 77, 78, 80	x_{34}	785
1, 5, 6, 7, 8, 12, 13, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 52, 54, 56, 58, 60, 62, 69, 71, 73, 79, 80	x_{54}	785
1, 3, 5, 6, 7, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 69, 71, 74, 75, 77, 78, 80	$x_{13} + x_{55} + x_{60} + x_{64}$	785
1, 3, 5, 6, 7, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 65, 69, 71, 74, 75, 77, 78, 80	$x_{22} + x_{49} + x_{64}$	786
1, 3, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 65, 69, 71, 74, 75, 77, 78, 80	$x_3+x_4+x_7+x_{12}+x_{20}+x_{22}+x_{30}+x_{36}+x_{39}+x_{42}+x_{43}+x_{45}+x_{47}+x_{51}+x_{58}+x_{63}+x_{69}+x_{70}+x_{72}+x_{78}+1$	786
1, 3, 6, 7, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 65, 69, 71, 74, 75, 77, 78, 80	$x_{14} + x_{23} + x_{41} + x_{47} + x_{49} + x_{50} + x_{58} + x_{64}$	786
1, 3, 5, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 65, 69, 71, 74, 75, 77, 78, 80	$x_3+x_4+x_{14}+x_{22}+x_{30}+x_{34}+x_{38}+x_{41}+x_{42}+x_{45}+x_{47}+x_{49}+x_{51}+x_{58}+x_{61}+x_{65}+x_{69}+x_{72}+x_{78}$	786
1, 3, 5, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 65, 69, 71, 74, 75, 77, 78, 80	$x_3+x_4+x_{20}+x_{22}+x_{30}+x_{34}+x_{38}+x_{40}+x_{42}+x_{45}+x_{49}+x_{51}+x_{58}+x_{61}+x_{65}+x_{67}+x_{69}+x_{72}+x_{78}$	786
1, 3, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 38, 40, 43, 45, 47, 49, 53, 56, 58, 62, 63, 69, 71, 75, 77, 79	$x_9+x_{29}+x_{30}+x_{32}+x_{42}+x_{43}+x_{49}+x_{51}+x_{57}+x_{58}+x_{59}+x_{60}+x_{62}+x_{64}+x_{66}+x_{67}+x_{68}+x_{69}+x_{70}+x_{72}+x_{76}$	791
1, 3, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 36, 40, 41, 43, 45, 47, 49, 53, 56, 58, 62, 63, 69, 71, 75, 77, 80	$x_{17}+x_{26}+x_{30}+x_{32}+x_{41}+x_{43}+x_{47}+x_{57}+x_{62}+x_{65}+x_{66}+x_{70}+x_{72}+x_{74}+1$	791
1, 3, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 36, 40, 41, 43, 45, 47, 49, 53, 56, 58, 62, 63, 69, 71, 75, 77, 80	$x_1+x_{17}+x_{26}+x_{28}+x_{41}+x_{43}+x_{47}+x_{49}+x_{59}+x_{62}+x_{64}+x_{65}+x_{66}+x_{70}+x_{72}+x_{74}+x_{76}+1$	791
1, 3, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 36, 40, 41, 43, 45, 47, 49, 53, 56, 58, 62, 63, 69, 71, 75, 77, 80	$x_{14} + x_{17} + x_{26} + x_{30} + x_{43} + x_{47} + x_{50} + x_{57} + x_{58} + x_{59} + x_{65} + x_{70} + x_{72} + x_{74} + x_{77} + 1$	791
1, 3, 5, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 40, 41, 43, 45, 47, 49, 53, 56, 58, 63, 65, 69, 71, 75, 77, 79	$x_{12}+x_{26}+x_{30}+x_{39}+x_{41}+x_{45}+x_{47}+x_{57}+x_{58}+x_{59}+x_{62}+x_{64}+x_{74}+x_{76}+1$	791
1, 3, 5, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 56, 58, 62, 63, 65, 69, 71, 75, 77	$x_5+x_{18}+x_{20}+x_{26}+x_{28}+x_{29}+x_{30}+x_{31}+x_{32}+x_{41}+x_{42}+x_{44}+x_{50}+x_{51}+x_{56}+x_{57}+x_{62}+x_{64}+x_{67}+x_{69}+x_{70}+x_{71}+x_{74}+x_{77}+x_{78}+1$	791
1, 3, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 40, 41, 43, 45, 47, 49, 53, 56, 58, 61, 62, 63, 65, 69, 71, 75, 77, 80	$x_7+x_9+x_{10}+x_{11}+x_{12}+x_{13}+x_{15}+x_{17}+x_{19}+x_{20}+x_{26}+x_{30}+x_{31}+x_{33}+x_{37}+x_{39}+x_{40}+x_{41}+x_{42}+x_{44}+x_{45}+x_{46}+x_{47}+x_{48}+x_{50}+x_{51}+x_{53}+x_{56}+x_{59}+x_{60}+x_{64}+x_{67}+x_{68}+x_{70}+x_{71}+x_{72}+x_{74}+x_{78}+x_{79}+1$	791

Table 2: Maxterms and superpolys after 784 initialization rounds of Trivium (continue).

maxterm bits	superpoly	round
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 38, 40, 41, 43, 45, 47, 49, 53, 56, 58, 61, 62, 63, 65, 69, 71, 75, 77	$x_1+x_{28}+x_{32}+x_{47}+x_{58}+x_{59}+x_{62}+x_{64}+x_{74}$	791
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 40, 41, 43, 45, 47, 49, 53, 56, 58, 61, 62, 63, 65, 69, 71, 75, 77, 80	$x_3+x_4+x_6+x_7+x_9+x_{10}+x_{13}+x_{15}+x_{19}+x_{22}+x_{28}+x_{30}+x_{33}+x_{34}+x_{35}+x_{38}+x_{39}+x_{40}+x_{41}+x_{43}+x_{44}+x_{47}+x_{48}+x_{49}+x_{50}+x_{53}+x_{54}+x_{55}+x_{56}+x_{58}+x_{61}+x_{62}+x_{65}+x_{66}+x_{67}+x_{68}+x_{69}+x_{71}+x_{72}+x_{76}+x_{77}+x_{78}$	791
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 40, 41, 43, 45, 47, 49, 53, 56, 58, 61, 62, 63, 65, 69, 71, 75, 77, 80	$x_{10}+x_{11}+x_{12}+x_{13}+x_{15}+x_{17}+x_{19}+x_{20}+x_{29}+x_{31}+x_{32}+x_{33}+x_{37}+x_{39}+x_{40}+x_{41}+x_{42}+x_{44}+x_{46}+x_{48}+x_{49}+x_{50}+x_{53}+x_{57}+x_{60}+x_{67}+x_{70}+x_{71}+x_{76}+x_{78}+x_{79}$	791
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 40, 41, 43, 45, 47, 49, 53, 56, 58, 61, 62, 63, 65, 69, 71, 75, 77, 80	$x_{10}+x_{11}+x_{12}+x_{13}+x_{14}+x_{15}+x_{17}+x_{19}+x_{20}+x_{26}+x_{29}+x_{31}+x_{33}+x_{37}+x_{39}+x_{40}+x_{42}+x_{44}+x_{46}+x_{48}+x_{53}+x_{57}+x_{58}+x_{59}+x_{60}+x_{66}+x_{67}+x_{68}+x_{70}+x_{71}+x_{72}+x_{77}+x_{78}+x_{79}+1$	791
1, 3, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 65, 69, 71, 75, 77, 79	$x_3+x_4+x_6+x_{11}+x_{15}+x_{17}+x_{19}+x_{20}+x_{22}+x_{30}+x_{34}+x_{35}+x_{37}+x_{38}+x_{43}+x_{47}+x_{51}+x_{54}+x_{57}+x_{58}+x_{60}+x_{61}+x_{64}+x_{65}+x_{67}+x_{68}+x_{70}+x_{72}+x_{74}+x_{77}+x_{79}+1$	791
1, 3, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 65, 69, 71, 75, 77, 79	$x_3+x_4+x_6+x_{11}+x_{12}+x_{15}+x_{17}+x_{18}+x_{19}+x_{20}+x_{22}+x_{30}+x_{34}+x_{35}+x_{37}+x_{38}+x_{39}+x_{42}+x_{43}+x_{45}+x_{47}+x_{50}+x_{54}+x_{56}+x_{57}+x_{58}+x_{61}+x_{65}+x_{69}+x_{70}+x_{74}+x_{78}+x_{79}+1$	791
1, 3, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 69, 71, 74, 75, 77, 78, 80	$x_1+x_5+x_9+x_{14}+x_{18}+x_{20}+x_{26}+x_{28}+x_{32}+x_{41}+x_{42}+x_{43}+x_{45}+x_{47}+x_{49}+x_{66}+x_{67}+x_{69}+x_{70}+x_{76}+x_{78}$	791
1, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 29, 31, 33, 36, 38, 40, 41, 42, 45, 47, 49, 53, 58, 63, 69, 71, 72, 76, 79, 80	x_{61}	791
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 65, 69, 71, 75, 77, 79	$x_3+x_4+x_6+x_7+x_9+x_{11}+x_{17}+x_{18}+x_{20}+x_{22}+x_{26}+x_{28}+x_{29}+x_{31}+x_{34}+x_{35}+x_{37}+x_{38}+x_{39}+x_{41}+x_{46}+x_{50}+x_{51}+x_{54}+x_{55}+x_{56}+x_{58}+x_{61}+x_{65}+x_{66}+x_{67}+x_{74}+x_{76}+x_{78}+x_{79}+1$	791
1, 3, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 69, 71, 74, 75, 77, 78, 80	$x_{43}+x_{47}+x_{58}+x_{70}+x_{74}+1$	791
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 38, 40, 41, 43, 45, 47, 49, 53, 56, 58, 62, 63, 69, 71, 75, 77, 80	$x_{12}+x_{17}+x_{26}+x_{27}+x_{29}+x_{30}+x_{32}+x_{40}+x_{43}+x_{45}+x_{46}+x_{49}+x_{53}+x_{54}+x_{56}+x_{59}+x_{62}+x_{64}+x_{65}+x_{67}+x_{69}+x_{72}+x_{74}+x_{75}$	792
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 63, 69, 71, 75, 77, 78, 79, 80	$x_{12}+x_{26}+x_{39}+x_{56}+x_{68}+1$	792
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 56, 58, 61, 63, 69, 71, 75, 77, 78, 79, 80	$x_{12}+x_{14}+x_{26}+x_{30}+x_{40}+x_{41}+x_{47}+x_{48}+x_{56}+x_{66}+x_{67}+x_{68}+x_{74}+x_{75}+1$	792
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 63, 69, 71, 74, 75, 77, 78, 79, 80	$x_{16}+x_{43}+x_{56}$	792
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 63, 65, 69, 71, 75, 77, 78, 79, 80	$x_{14}+x_{16}+x_{26}+x_{29}+x_{30}+x_{41}+x_{45}+x_{55}+x_{56}+x_{59}+x_{62}+x_{64}+x_{66}+x_{68}+x_{70}+x_{71}+x_{72}+1$	792
1, 3, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 41, 43, 45, 47, 49, 53, 54, 56, 58, 61, 63, 69, 71, 75, 77, 80	$x_{45}+x_{72}$	793
1, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 27, 30, 31, 33, 38, 40, 43, 45, 47, 49, 51, 52, 56, 58, 63, 67, 69, 71, 73, 77, 80	$x_{10}+x_{55}$	798
1, 3, 5, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 65, 69, 71, 74, 75, 77, 80	$x_{36}+x_{52}+x_{60}+x_{63}$	798
1, 3, 5, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 65, 69, 71, 74, 75, 77, 80	$x_{10}+x_{17}+x_{27}+x_{36}+x_{37}+x_{40}+x_{52}+x_{59}+x_{60}+x_{63}+x_{66}+x_{67}$	798
1, 3, 5, 6, 7, 8, 10, 12, 14, 16, 19, 21, 23, 25, 33, 36, 38, 40, 43, 45, 47, 49, 53, 56, 58, 61, 62, 63, 65, 69, 71, 74, 75, 77, 78, 79	$x_{27}+x_{54}+x_{60}$	798
1, 3, 5, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 65, 69, 71, 74, 75, 77, 80	$x_6+x_{11}+x_{25}+x_{33}+x_{36}+x_{53}+x_{60}+x_{62}+x_{63}+x_{64}+x_{79}$	798
1, 3, 5, 6, 7, 8, 10, 12, 15, 16, 19, 21, 23, 25, 27, 33, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 61, 62, 63, 65, 69, 71, 74, 75, 77, 80	$x_6+x_{11}+x_{25}+x_{33}+x_{36}+x_{52}+x_{53}+x_{60}+x_{62}+x_{63}+x_{64}+x_{79}$	798
5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 34, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 60, 61, 62, 63, 67, 69, 71, 74, 80	$x_{65}+x_{66}+x_{67}+1$	798
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 54, 56, 58, 62, 69, 71, 73, 80	$x_{25}+1$	799
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 40, 43, 45, 47, 49, 53, 56, 58, 63, 69, 71, 75, 77, 80	$x_{12}+x_{38}+x_{39}+x_{40}$	799

Table 2: Maxterms and superpolys after 784 initialization rounds of Trivium.

2 Specifics of the Attacked Ciphers

In the following, we briefly describe the three ciphers we selected as test case targets for our attack.

2.1 Trivium

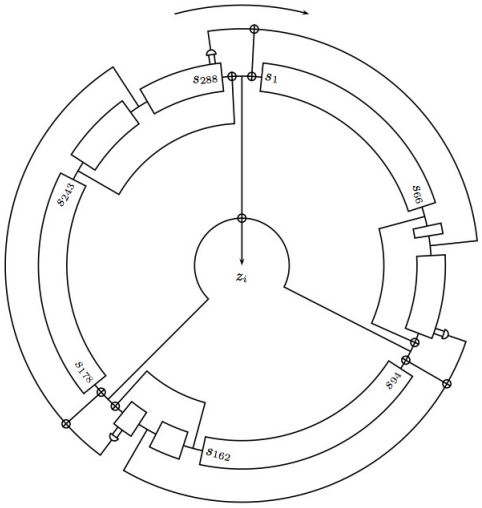

Fig. 1: Trivium Cipher [**?**].

Trivium [**?**] is a synchronous stream cipher conceived by Christophe De Cannire and Bart Preneel, not patented, and specified as an International Standard under ISO/IEC 29192-3. It is part of the eSTREAM portfolio [**?**]. Trivium combines a flexible trade-off between speed and gate count in hardware, and a reasonably efficient software implementation. Quoting [**?**]: "Trivium is a hardware oriented design focused on flexibility. It aims to be compact in environments with restrictions on the gate count, power-efficient on platforms with limited power resources, and fast in applications that require high-speed encryption". Particularly interesting is the fact that any state bit stays unused for at least 64 iterations after it has been modified. This means that up to 64 iterations can be parallelized and computed at once, allowing for a factor 64 reduction in the clock frequency without affecting the throughput.

Trivium generates up to 2^{64} bits of output from an 80-bit key $K = \{x_1, \ldots, x_{80}\}$ and an 80-bit Initial Vector $IV = \{v_1, \ldots, v_{80}\}$, and it shows remarkable resistance to cryptanalysis despite its simplicity and its excellent performance. It is composed by a 288-bit internal state $s_1, \ldots, s_{288}$ consisting of three shift registers R1, R2 and R3 of length 93, 84 and 111, respectively. The feedback to each of these registers and the output bit of the cipher are obtained through non-linear combinations involving in total 15 out of the 288 internal state bits (see Figure 1). During the initialization phase the key bits filled the first 80 bits of R1 whereas the IV bit fill the first 80 bits of R2; all the remaining unfilled bits of R1, R2, and R3 are filled with 0 except for the last three bits of R3 that are filled with 1. The three registers are update simultaneously using the same rules in both initialization and keystream generation modes; the only difference is that the output z is produced only in keystream mode. The update function is defined as follow where + denotes the bit XOR operation and the $\cdot$ represents the logical AND:

$$
\begin{aligned}
t_1 &\leftarrow s_{66} + s_{93} \\
t_2 &\leftarrow s_{162} + s_{177} \\
t_3 &\leftarrow s_{243} + s_{288} \\
z &\leftarrow t_1 + t_2 + t_3 \\
t_1 &\leftarrow t_1 + s_{91} \cdot s_{92} + s_{171} \\
t_2 &\leftarrow t_2 + s_{175} \cdot s_{176} + s_{264} \\
t_3 &\leftarrow t_3 + s_{286} \cdot s_{287} + s_{69} \\
(s_1, \ldots, s_{93}) &\leftarrow (t_3, s_1, \ldots, s_{92}) \\
(s_{94}, \ldots, s_{177}) &\leftarrow (t_1, s_{94}, \ldots, s_{176}) \\
(s_{178}, \ldots, s_{288}) &\leftarrow (t_2, s_{178}, \ldots, s_{287})
\end{aligned}
$$

The initialization phase involves 1152 rounds and it guarantees that the output begins to be produced only after all key-bits and IV-bits have been sufficiently mixed together to define the internal state of the registers.

2.2 Grain-128

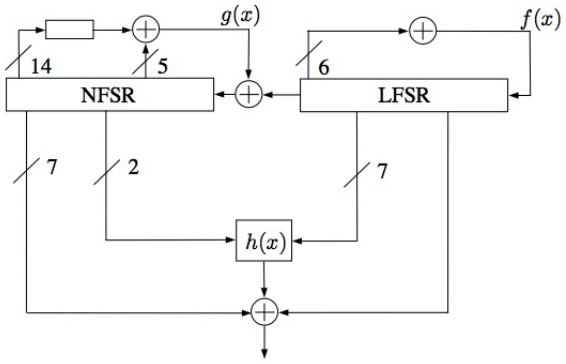

Fig. 2: Grain-128 [**?**].

Grain-128 is a variant of Grain v1 [**?**], a stream cipher belonging to the eSTREAM portfolio, proposed by Hell, Johansson, Maximov and Meier [**?**]. Grain-128

maxterm bits	superpoly	round
1, 6, 8, 10, 12, 14, 18, 20, 23, 25, 27, 31, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 69, 73, 75, 77, 80	x_{60}	799
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 54, 56, 58, 62, 69, 71, 73, 80	$x_{25} + 1$	799
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 40, 43, 45, 47, 49, 53, 56, 58, 63, 69, 71, 75, 77, 80	$x_{25} + x_{40}$	799
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 40, 43, 45, 47, 49, 53, 56, 58, 63, 69, 71, 75, 77, 80	$x_{12} + x_{38} + x_{39} + x_{40}$	799
1, 5, 6, 7, 8, 10, 12, 14, 15, 16, 18, 20, 23, 25, 27, 33, 36, 38, 40, 41, 43, 47, 49, 53, 56, 58, 63, 69, 71, 75, 77, 80	$x_{67} + 1$	799
1, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 31, 33, 36, 38, 40, 41, 45, 47, 49, 53, 56, 58, 63, 69, 71, 75, 80	x_{42}	799
1, 5, 6, 7, 8, 10, 12, 14, 15, 19, 21, 23, 25, 27, 31, 36, 38, 40, 41, 45, 47, 49, 53, 56, 58, 63, 69, 71, 73, 75, 77, 80	x_{53}	799
1, 5, 6, 8, 10, 12, 14, 15, 16, 18, 19, 20, 21, 23, 25, 27, 31, 33, 36, 38, 40, 41, 45, 49, 54, 56, 62, 69, 73, 75, 77, 80	x_{64}	799
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 69, 71, 80	$x_{36} + 1$	799
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 40, 41, 43, 45, 47, 49, 53, 56, 58, 63, 65, 69, 71, 75, 77, 80	x_{38}	799
1, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 54, 56, 58, 60, 62, 65, 69, 70, 71, 73, 80	x_{56}	799
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 33, 34, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 69, 71, 74, 80	$x_{69} + 1$	799
1, 6, 7, 8, 10, 12, 14, 16, 19, 21, 25, 27, 30, 31, 33, 36, 38, 40, 41, 43, 45, 47, 49, 51, 52, 56, 58, 63, 67, 69, 71, 73, 77, 80	$x_{66} + 1$	799
1, 3, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 25, 27, 33, 34, 36, 38, 40, 43, 45, 47, 49, 53, 54, 56, 58, 62, 63, 67, 69, 71, 74, 80	x_{58}	799
1, 5, 6, 7, 8, 10, 12, 14, 15, 16, 19, 21, 23, 25, 27, 33, 36, 38, 40, 43, 45, 47, 49, 53, 54, 55, 56, 58, 62, 63, 67, 69, 71, 74, 80	x_{37}	799

Table 3: Maxterms and superpolys after 799 initialization rounds of Trivium.

maxterm bits	superpoly	round
1, 6, 7, 8, 10, 12, 14, 18, 20, 21, 23, 25, 27, 31, 33, 34, 36, 38, 40, 43, 45, 47, 49, 53, 56, 58, 62, 63, 67, 69, 73, 75, 77, 80	x_{64}	800

Table 4: Maxterms and superpolys after 800 initialization rounds of Trivium.

is very compact and easy to implement, especially in hardware as stated by the authors. It supports 128-bit keys and 96-bit IVs. Its main components are a a Linear Feedback Shift Register (LFSR), a Non-linear Feedback Shift Register (NFSR), and a non-linear boolean function $h(\mathbf{x})$. Both the LFSR and the NFSR have 128-bit inner states, denoted, respectively, $s_i, s_{i+1}, \ldots, s_{i+127}$ and $b_i, b_{i+1}, \ldots, b_{i+127}$, which altogether represent the inner state of the cipher. The two inner states are updated as follows:

$$\begin{aligned} s_{i+128} =& s_i + s_{i+7} + s_{i+38} + s_{i+70} + s_{i+81} + s_{i+96} \\ b_{i+128} =& s_i + b_i + b_{i_26} + b_{i+56} + b_{i-91} + b_{i+96} + \\ &+ b_{i+3}b_{i+67} + b_{i+11}b_{i+13} + \\ &+ b_{i+17}b_{i+18} + b_{i+27}b_{i+59} + \\ &+ b_{i+40}b_{i+48} + b_{i+61}b_{i+65} + b_{i+68}b_{i+84} \end{aligned}$$

The boolean function $h(\mathbf{x})$ is defined as

$$h(\mathbf{x}) = x_0x_1 + x_2x_3 + x_4x_5 + x_6x_7 + x_0x_4x_8$$

where its input vector $\mathbf{x} = (x_0, \ldots, x_8)$ is composed of two state bits from the NFSR and seven from the LFSR as follows:

$$\mathbf{x} = (b_{i+12}, s_{i+8}, s_{i+13}, s_{i+20}, b_{i+95}, s_{i+42}, s_{i+60}, s_{i+95})$$

Finally, the output function takes as input the output of $h(\mathbf{x})$ added to s_{i+93} and b_{i+j} where $j \in A = \{2, 15, 36, 45, 64, 73, 89\}$.

In the initialization phase, the first 96 bits of the LFSR are filled with the IV bits whereas the remaining 32 bits are filled with 1. On the other hand, the key bits are used to completely fill the NFSR. Grain-128 defines 256 initialization rounds where the output of $h(\mathbf{x})$ is used as feedback both to NFSR and LFSR.

In Figure 2, the overview of the cipher in keystream mode is reported. A very interesting feature of Grain-128 is that the last 31 bits of both the NFSR and the LFSR are not used in the update function, and this allows to easily speedup by a factor of 32.

2.2.1 SNOW 3G

Within the security architecture of the 3GPP system, two standardised algorithms, UEA2 and UIA2, are respectively responsible of data confidentiality and integrity. Both of them are based on the SNOW 3G stream

maxterm bits	bits set to 1	superpoly	round
{0, 4, 14, 19, 21, 23, 27,41, 46, 69 }	{42}	x_{122}	168
{0, 2, 4, 14, 19, 28, 42, 46, 68 }	{ 45, 55}	x_{121}	163
{17, 23, 36, 37, 41, 63, 68, 74 }	{28, 45, 55}	x_{116}	170
{0, 27, 28, 31, 36, 45, 55}	{4, 17, 19, 21, 23, 42, 63, 68}	x_{108}	164
{14, 23, 27, 41, 42, 45, 50, 55}	{2, 4, 17, 46}	x_{95}	165
{0, 4, 14, 17, 19, 27, 41, 46}	{21, 28, 45}	x_{92}	162
{2, 17, 27, 28, 36, 45, 74}	{19, 23, 41, 42, 68, 69}	x_{84}	165
{0, 36, 42, 74}	{2, 17, 21, 37, 46, 55, 68, 69}	x_{81}	162
{0, 4, 19, 31, 41, 42, 46}	{17, 21, 55, 68}	x_{80}	162
{0, 2, 4, 14, 21, 28, 41, 46, 50}		x_{79}	163
{21, 27, 28, 31, 37, 45, 69}	{2, 41, 46, 55}	x_{76}	165
{4, 14, 17, 19, 27, 45, 68, 69}		x_{72}	170
{19, 23, 31, 36, 37, 41, 55, 69}		x_{59}	168
{4, 27, 28, 31, 42, 46}	{19, 21, 36, 41, 50, 63, 69}	$x_{49} + x_{96} + x_{124}$	161
{4, 14, 21, 27, 37, 46, 50, 55, 69}	{17, 23, 41, 42}	x_{41}	162
{4, 28, 31, 36, 41, 46}	{0, 50, 55}	x_{35}	162
{19, 28, 36, 37, 68, 74}	{42, 63, 69}	x_{32}	170
{17, 21, 31, 37, 42, 46, 55, 63}	{36}	x_{25}	162
{14, 17, 19, 27, 28, 36, 39}	{68}	x_{23}	167
{17, 19, 27, 28, 50, 63, 69, 74}	{2, 21, 36, 45, 46, 55}	x_{21}	170
{14, 19, 23, 27, 36, 46, 55, 63}	{0, 21, 41, 42}	x_{18}	167

Table 5: Maxterms and superpolys after 160 initialization rounds of Grain-128.

cipher, an evolution of the previous algorithms SNOW and SNOW 2.0.

SNOW 3G, whose design is reported Figure 3, generates a keystream using a 128-bit key K and a (public) 128-bit initial vector IV, and relying on the combination of two interacting modules, a Linear Feedback Shift Register (LFSR) of length $l = 16$ and a Finite State Machine (FSM) built upon 3 registers R_1, R_2 and R_3, and making use of 2 S-boxes S_1 and S_2. The S-boxes are particularly important to provide stronger diffusion, making each output bit depend on each input bit, and introducing a source of non-linearity in the cipher. The 16 cells of the LFSR and the 3 registers of the FSM store 32-bit words. Accordingly, all internal and combining operations are based, other than on the 2 S-boxes, on bitwise xor ($\oplus$) over $\mathbb{F}_2^{32}$, or on addition modulo $\mathbb{F}_{2^{32}}$ ($\boxplus$).

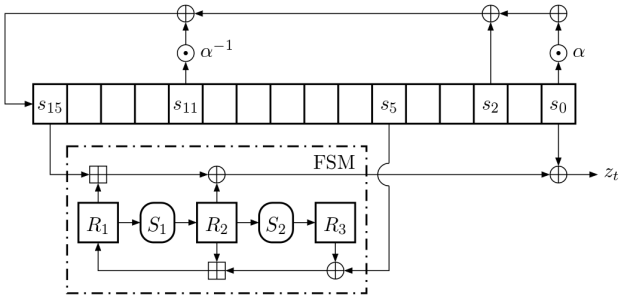

Fig. 3: The design of Snow 3G.

To define the seed, the 128-bit secret key K and the initial vector IV are split into 4 32-bit words as $K = (K_0, K_1, K_2, K_3)$ and $IV = (IV_0, IV_1, IV_2, IV_3)$. With **1** denoting the all-one 32-bit word, the seed of

the LFSR is defined as follows:

$$\begin{aligned}
s_0^0 &= K_0 \oplus \mathbf{1} & s_8^0 &= K_0 \oplus \mathbf{1} \\
s_1^0 &= K_1 \oplus \mathbf{1} & s_9^0 &= K_1 \oplus \mathbf{1} \oplus IV_3 \\
s_2^0 &= K_2 \oplus \mathbf{1} & s_{10}^0 &= K_2 \oplus \mathbf{1} \oplus IV_2 \\
s_3^0 &= K_3 \oplus \mathbf{1} & s_{11}^0 &= K_3 \oplus \mathbf{1} \\
s_4^0 &= K_0 & s_{12}^0 &= K_0 \oplus IV_1 \\
s_5^0 &= K_1 & s_{13}^0 &= K_1 \\
s_6^0 &= K_2 & s_{14}^0 &= K_2 \\
s_7^0 &= K_3 & s_{15}^0 &= K_3 \oplus IV_0
\end{aligned}$$

The 3 registers of the FSM are initially set to zero as $R_1^0 = R_2^0 = R_3^0 = \mathbf{0}$, where $\mathbf{0}$ denotes the all-zero 32-bit word.

For each $t \geq 0$, the inner state of the FSM is updated as

$$\begin{cases} R_1^{t+1} &= R_2^t \boxplus (R_3^t \oplus s_5^t) \\ R_2^{t+1} &= S_1(R_1^t) \\ R_3^{t+1} &= S_2(R_2^t) \end{cases}$$

and the output of the FSM is computed as

$$F^t = (s_{15}^t \boxplus R_1^t) \oplus R_2^t$$

with the contents s_5^t and s_{15}^t of cells 5 and 15 of the LFSR at round t being fed to the FSM. On the other hand, the behavior of the LFSR varies from Initialization Mode (IM) to Keystream Mode (KM). The IM consists in 32 rounds during which the LFSR does not produce any output. During these initialization steps, the output F^t produced by the FSM at round t is fed to the LFSR and the inner state of the LFSR is updated as

$$\begin{cases} s_i^{t+1} &= s_{i+1}^t \quad \text{for all } i = 0, \ldots, 14 \\ s_{15}^{t+1} &= \alpha^{-1} s_{11}^t \oplus s_2^t \oplus \alpha s_0^t \oplus F^t \end{cases}$$

where α is a root of the polynomial $X^4 + \beta^{23}X^3 + \beta^{245}X^2 + \beta^{48}X + \beta^{239} \in \mathbb{F}_{2^8}[X]$, and β is a root of the polynomial $X^8 + X^7 + X^5 + X^3 + 1 \in \mathbb{F}_2[X]$. When in KM, the LFSR outputs the content of the first cell s_0^t, and does not use any feedback from the FSM. For each $t > 32$, the inner state of the LFSR is updated as follows:

$$\begin{cases} s_i^{t+1} &= s_{i+1}^t \quad \text{for all } i = 0, \ldots, 14 \\ s_{15}^{t+1} &= \alpha^{-1} s_{11}^t \oplus s_2^t \oplus \alpha s_0^t \end{cases}$$

where α is defined as in the IM. In other words, it behaves as a typical LFSR with feedback polynomial $P(X) = 1 - \alpha^{-1}X^5 + X^{14} + \alpha X^{16}$.

Finally, the keystream $\{z^t\}_{t \geq 0}$ is obtained combining the outputs of the LFSR and of the FSM, as

$$z^{t-32} = s_0^t \oplus F^t$$

for each $t \geq 32$.