Homework 32

Austin Frownfelter Matthew Bialecki

April 9, 2018

1 Problem 60

1.1 Part a

$u = 101$

1.2 Part b

Refer to the attached python program. It either prints "Failed" if the protocol catches the verifier, or the binary and hexadecimal representation of the book entry.

1.3 Part c

The program prints the binary and hexadecimal representations of the book. It uses the "|" operator to separate the $WH(u) and WH(u \otimes u)$ (for readability)

01011010|0101101001011010010110100101101001011010010110100101101001
0110101010010110100101101001011010010110100101101001011010010110100101
1010110100101101001011010010110100101101001011010010110100101101010
0101101001011010010110100101101001011010010110100101101001011011
0100101101001011010010110100101101001011010010110100101010110100101110
10010110100101101001011010010110100101101001011010101001011010010110 1
001011010010110100101101001011010010110100101010110100101101001011010
01011010010110100101101001011010010110 10

$0x5a|0x5a5a5a5a5a5a5a5aa5a5a5a5a5a5a5a55a5a5a5a5a5a5a5aa5a5a5a5a5 a5a5a5a5a5a5a5a5a5a5a55a5a5a5a5a5a5a5aa5a5a5a5a5a5a5a55a5a5a5a5a5a5a 5a$

1.4 Part d

The first 8 bits (2^3) represent the values of the inner product of the input and i, where $i = \{0 \ldots 7\}$. The last 512 bits ($2^{3^2} = 2^9$) represent the inner product of $u \otimes u$ and x, where $x = \{0 \ldots 511\}$.

x is ordered such that each x_i represents $u_1u_1 + u_1u_2 + u_1u_3 + u_2u_1 + u_2u_2 + u_2u_3 + u_3u_1 + u_3u_2 + u_3u_3$, where each 1 bit means that part of the equation is included ($010000000 \equiv u_1u_2$).

With the above notation, the equation $u_1u_2 + u_2u_2 + u_3u_3$ has the 2nd, 5th, and 9th bits in $x_i = 1$, with the rest being 0. This equation becomes the string 010010001. Since it makes sense to order the last 512 bits numerically, and this is the (decimal) number 145, the 153rd bit $(145 + 8)$ in the resulting book entry represents the bit of this equation.