

|   |
|---|
| Abbreviations   |
| $\sim M\_7 = MP\_ID$  |
| $\sim M\_8 = h(\text{con}(MP\_PW, MP\_N\_1))$   |
| $\sim M\_9 = MP\_C1$  |
| $\sim M_{10} = MP\_C2$  |
| $\sim M_{11} = MP\_C3$  |
| $\sim M_{12} = MP\_R1$  |
| $\sim M_{13} = MP\_R2$  |
| $\sim M_{14} = MP\_R3$  |
| $\sim M_{15} = MP\_BIO$   |
| $\sim M_{16} = MP\_ID$  |
| $\sim M_{17} = h(\text{con}(\text{con}(\text{xor}(\text{xor}(a\_3, h(\text{con}(MP\_PW, MP\_N\_1))), h(\text{con}(MP\_PW, MP\_N\_1))), MP\_N\_1), MP\_R1))$   |
| $\sim M_{18} = \text{xor}(\text{xor}(h(\text{con}(a\_2, h(\text{con}(MP\_PW, MP\_N\_1)))), h(\text{con}(\text{con}(\text{xor}(\text{xor}(a\_3, h(\text{con}(MP\_PW, MP\_N\_1))), h(\text{con}(MP\_PW, MP\_N\_1))), MP\_N\_1), MP\_R1))), MP\_R1)$   |
| $\sim M_{19} = MP\_C1$  |
| $\sim M_{20} = T1\_2$   |
| $\sim X\_1 = (\text{xor}(h(\text{con}(\text{xor}(\sim M_{17}, \text{xor}(h(\text{con}(a\_2, \sim M_8)), \sim M_{17})), \sim M_{13})), a\_2), a\_5, a\_6)$<br>$= (\text{xor}(h(\text{con}(\text{xor}(h(\text{con}(\text{con}(a\_3, MP\_N\_1), MP\_R1))), \text{xor}(h(\text{con}(a\_2, h(\text{con}(MP\_PW, MP\_N\_1))), h(\text{con}(\text{con}(a\_3, MP\_N\_1), MP\_R1))), MP\_R2)), a\_2), a\_5, a\_6)$ |
| $\sim X\_2 = (a\_7, \text{xor}(a\_8, a\_3), \text{xor}(h(\text{con}(h(\text{con}(a\_2, \sim M_8)), a\_8)), a\_3), a\_9)$<br>$= (a\_7, \text{xor}(a\_8, a\_3), \text{xor}(h(\text{con}(h(\text{con}(a\_2, h(\text{con}(MP\_PW, MP\_N\_1))), a\_8)), a\_3), a\_9)$  |

