CERIAS

the center for education and research in information assurance and security

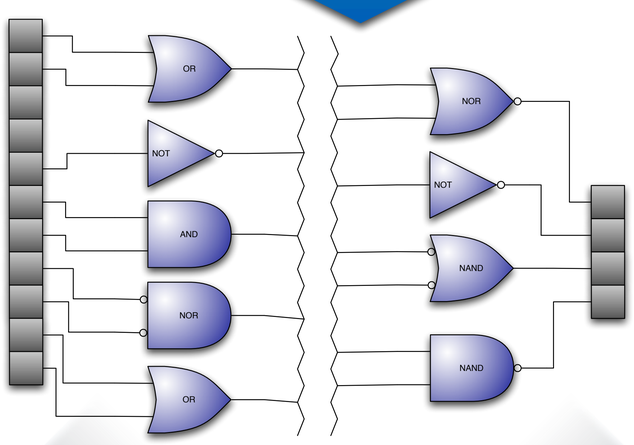
Bit-Level Analysis of Cryptographic Functions

William R. Speirs, II and Ian Molloy

1

UMAC SHA1 RC5 DES

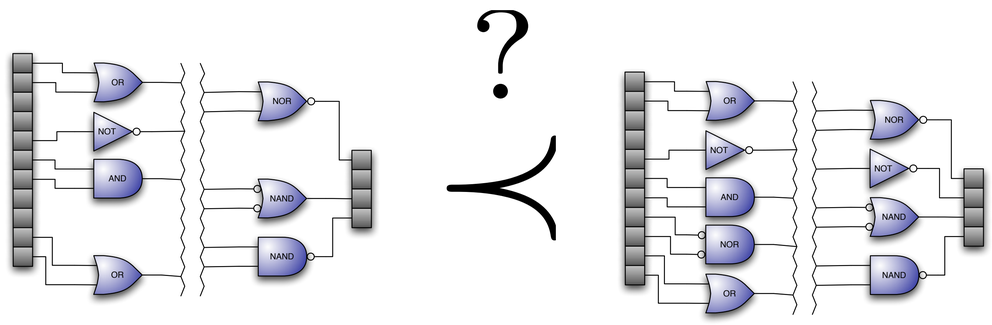
2



3a

$$
\begin{aligned}
a_0 &= (\neg b_1 \vee b_3) \wedge (b_4 \vee b_8) \wedge \cdots \wedge (b_9 \vee \neg b_{56}) \\
a_1 &= (b_6 \vee b_{13}) \wedge \cdots \wedge (\neg b_{35} \vee b_{10}) \\
&\vdots \\
a_n &= \cdots
\end{aligned}
$$

3b



1. Any cryptographic function with a fixed number of input and output bits is selected.

2. The function is converted into a Boolean circuit.

3a. The Boolean circuit can be converted into a system of equations. Satisfying the system breaks the function.

3b. The circuit's complexity can be use as a metric to compare the relative security of two functions.

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center