Cryptonet - 2009-April-24 - Differential cryptanalysis

Very much like linear cryptanalysis.
Many known plaintexts.
A probabilistic evaluation of a subset of bits propagating through the network.
Probabilities derived from BPD the XOR relationship of inputs and outputs on $T_5$.
Key difference: We use not the $\Theta$ of inputs and outputs but the $\Theta$ of two inputs and the $\Theta$ of two outputs. These will be our differential pairs that drive the algorithm.

We will need What is a differential pair? We need to build it....

Let $x' = x \oplus \hat{x}$, where $x, x', \hat{x} \in \mathbb{Z}_2^m$ for an $m$-bit $T_5$.
Let $y' = y \oplus \hat{y}$, where $y, y', \hat{y} \in \mathbb{Z}_2^m$ and $y = T_5(x)$, $\hat{y} = T_5(\hat{x})$.
We refer to $x'$ as the input XOR to the S-box, and $y'$ as the output XOR from the S-box.

Finally, let $\Delta(x') = \{(x, x') : x' = x \oplus \hat{x}\}$.
Note that $x' = x \oplus \hat{x} \Rightarrow \hat{x} = x \oplus x'$, so:
$\Delta(x') = \{(x, x \oplus x')\}$

This is the set of $(x, x')$ pairs that produce a particular bit input XOR $x'$.

Using $\Delta(x')$, we can determine the corresponding $y'$ values that will allow us to construct our differential pairs $(x', y')$.

Let $\Delta(y') = \{(y', y' \in \mathbb{Z}_2^m : y' = y \oplus \hat{y}, y = T_5(x), \hat{y} = T_5(\hat{x})\}$

$\lambda(x') = \{y' : y' \in \mathbb{Z}_2^m : y = T_5(x) \land x, x' : (x, x') \in \Delta(x'): y' = T_5(x) \oplus T_5(\hat{x})\}$

Example: Assume the same $T_5$ that we've been using:

| $\hat{x}$ | E | H | D | C | B | F | 1 | 2 | 3 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| $T_5(x)$ | 2 | 4 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |

For a given $x'$, calculate $\lambda(x')$. 
Notice that the multiset is not at all uniformly distributed. Produce a table of \( y' \) values and their counts. We are again looking for skew inherent in the S-boxes.

Generalize this relationship between an \( x' \) and the different resulting \( y' \) values:

\[
N_d (x', y') = | \{ (x, x') \in \Delta (x') : y' = T_5 (x) \oplus T_5 (x) \} |
\]

For a given \( x' \), and poss how many \( y' \) can be of \( y' \) can be produced from pairs in \( \Delta (x') \)?

**Difference distribution table!**

- Lay out all possible \( x' \) and \( y' \) values (call them \( a', \ a, b' \) ) in a table, where each entry contains \( N_d (a', b') \).

- Each possible pairing \( (a', b') \) is a differential pair.

- For each pair, we can determine the propagation ratio:

\[
R_p (a', b') = \frac{N_d (a', b')}{2^m}
\]

Seen differently:

\[
R_r (a') = R_r (b' | a') = R_p (a', b')
\]

- Note that \( x \oplus x = x \oplus x \Rightarrow N_d (a', b') \) distinct pairs yield \( x' \).