Cryptonet — 2009-April-~~24~~ 27 — Differential cryptanalysis

→ Very much like linear cryptanalysis.
- ↳ Many known plaintexts.
- ↳ A probabilistic evaluation of ~~bit~~ a subset of bits propagating through the network.
- ↳ Probabilities derived from the XOR relationship of inputs and outputs on Π_S.
- ↳ <u>Key difference:</u> We use not the $\oplus$ of inputs and outputs, but the $\oplus$ of two inputs and the $\oplus$ of two outputs. These will be our <u>differential pairs</u> that drive the algorithm.

→ ~~We will need~~ What is a <u>differential pair</u>? We need to build toward it....

- ↳ Let $x' = x \oplus \hat{x}$, where $x, x', \hat{x} \in Z_2^m$ for an m-bit Π_S.
- ↳ Let $y' = y \oplus \hat{y}$, where $y, y', \hat{y} \in Z_2^m$ and $y = \Pi_S(x)$, $\hat{y} = \Pi_S(\hat{x})$.
  - ↳ We refer to <u>x'</u> as the <u>input xor</u> to the S-box, and <u>y'</u> as the <u>output xor</u> from the S-box.
- ↳ Finally, let $\Delta(x') = \{(x, \hat{x}) : x' = x \oplus \hat{x}\}$, $x, \hat{x} \in Z_2^m$, ~~the se~~
  - ↳ 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 $(x, \hat{x})$ pairs that produce a particular input xor x'.

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

- ↳ Let ~~$\lambda(y') = \{(y, \hat{y}) : y, \hat{y} \in Z_2^m : y' = y + \hat{y},\ y = \Pi_S(x),\ \hat{y} = \Pi_S(\hat{x})$~~

$$\lambda(x') = \{y' : \cancel{y' \in Z_2^m : y' = \Pi_S(x)}\ \cancel{\forall (x, \hat{x})} : (x, \hat{x}) \in \Delta(x') : y' = \Pi_S(x) \oplus \Pi_S(\hat{x})\}$$

- ↳ <u>Example:</u> Assume the same Π_S that we've been using:

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\Pi_S(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

<u>For a given x', calculate $\lambda(x')$.</u>

Cryptonet — 2009-April-~~24~~ 27 — Differential cryptanalysis

↳ Difference distributions:

↳ 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:

$$N_D(x', y') = \left| \{ (x, \hat{x}) \in \Delta(x') : y' = \pi_S(x) \oplus \pi_S(\hat{x}) \} \right|$$

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' and 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: ~~Pr(a'|b~~ $\Pr(b' \mid a') = R_p(a', b')$

↳ Note that $x \oplus \hat{x} = \hat{x} \oplus x \Rightarrow \frac{N_D(a', b')}{2}$ distinct pairs yield x'.