Cryptonet — 2009-April-~~27~~ 29 — Differential cryptanalysis II

→ Using propagation ratios:

↳ Much like linear cryptanalysis, we want create a chain — a differential trail — through the network.

↳ We can then (unjustifiably) assume independence between the propagation ratios (R_p values), multiplying them to determine the ratio for the entire trail.

↳ Example: Continuing w/ our Π_s and Π_p values ~~to~~ from earlier.

↳ Select some ratios to make a trail:

S_2^1 : $R_p(1011, 0010) = 1/2$
S_3^2 : $R_p(0100, 0110) = 3/8$
S_2^3 : $R_p(\cancel{0100}, 0101) = 3/8$ — 0010
S_3^3 : $R_p(0010, 0101) = 3/8$

Draw the ~~ro~~ trail.

x
↓
u
↓
v
↓
w
↓
u
↓
v
↓
w
⋮
↓
y

↳ Combine ratios:

$R_p(0000\ 1011\ 0000\ 0000,\ 0000\ 0101\ 0101\ 0000) =$
$1/2 \times (3/8)^3 = 27/1024$

From the network:

$x' = 0000\ 1011\ 0000\ 0000 \Rightarrow (v^3)' = 0000\ 0101\ 0101\ 0000$

Pass through $\Pi_p((v^3)') = (w^3)' \Rightarrow (w^4)'$

$(v^3)' = 0000\ 0101\ 0101\ 0000 \Rightarrow (u^4)' = 0000\ 0110\ 0110\ 0000$

So:

$x' = 0000\ 1011\ 0000\ 0000 \Rightarrow (u^4)' = 0000\ 0110\ 0110\ 0000$
with $Pr((u^4)' \mid x') = \cancel{R_p}\ 27/1024$

Cryptonet — 2009-April-29 — Differential cryptanalysis II

→ The differential attack:

↳ T is a set of 4-tuples $\{(x, \hat{x}, y, \hat{y})\}$ for a fixed x'.

~~↳ Tuples for which~~

↳ A useful observation:

Recall that:

$$U^r = W^{r-1} \oplus K^r \implies U^r_{(i)} = W^{r-1}_{(i)} \oplus K^r_{(i)}$$

So, the input xor for S^r_i:

$$U^r_{(i)} \oplus \widehat{U^r_{(i)}} = (W^{r-1}_{(i)} \oplus K^r_{(i)}) \oplus (\widehat{W^{r-1}_{(i)}} \oplus K^r_{(i)})$$

$$= W^{r-1}_{(i)} \oplus \widehat{W^{r-1}_{(i)}}$$

That is, the input xor to each S-box in the differential trail is independent of the subkey bits.

↳ Again, we will focus on candidate subkeys (2^8 of them) for half of K^5.

↳ Initialize a count for each subkey to 0.

~~↳ Filter the set T to eliminate members for which~~

↳ We seek members of T for which the differential described by the trail holds: right pairs.

↳ We can pre-emptively prune the set of some ~~input/output xor~~ 4-tuples for which we can quickly compute that the differential will not hold. Recall that, at the end of the trail:

$$(U^4_{(i)})' = (U^4_{(\hat{i})})' = 0000$$

Cryptonet — 2009-April-29 — Differential cryptanalysis II

$x' = 0000 \implies \Delta(x') = \{(0000, 0000), (0001, 0001), (0010, 0010), \ldots, (1111, 1111)\}$

$\implies \lambda(x') = \{(1110, 1110), (0010, 0010), \ldots, (0111, 0111)\}$

$\implies \forall y, \hat{y} : y = \pi_s(x), \hat{y} = \pi_s(\hat{x}) : y' = 0000$

Therefore, $(u^4_{(1)})' = (u^4_{(3)})' = 0000 \implies (v^4_{(1)})' = (v^4_{(3)})' = 0000$

Recall our critical observation about subkey bits:

$$y_{(1)}' = y_{(1)} \oplus \hat{y}_{(1)} = (v^4_{(1)} \oplus k^5_{(1)}) + (\hat{v}^4_{(1)} \oplus k^5_{(1)})$$

$$= v^4_{(1)} \oplus \hat{v}^4_{(1)}$$

$$= (v^4_{(1)})'$$

Therefore: $(v^4_{(1)})' = (v^3_{(3)})' = 0000$ ~~$y_{(1)} = \hat{y}_{(1)}$ and $y_{(3)} = \hat{y}_{(3)}$~~

$\implies y_{(1)}' = y_{(3)}' = 0000$

$\implies y_{(1)} = \hat{y}_{(1)}$ and $y_{(3)} = \hat{y}_{(3)}$

↳ Thus, if either of these equalities does not hold, we discard the tuple from T_2 to get T_f.

↳ For each $(x, \hat{x}, y, \hat{y}) \in T_f$, try each possible subkey:

↳ Partially decrypt ~~to u^4 for both~~ $y \to u^4$, $\hat{y} \to \hat{u}^4$.

↳ Calculate $(u^4)' = u^4 \oplus \hat{u}^4$.

↳ If $(u^4_{(1)})' = u^4_{(3)}{}' = 0110) \implies$ increment count for that subkey.

→ The subkey w/ maximum count is correct!