A Beginner's Guide to the T-310

With a strong focus on KT1 keys

Maxine Emuobosa

19 April 2018

Abstract

This document can be used to aid any cursory attempt to quickly and efficiently learn how the numerous components of T interact with one another during 1 round to result in an output that will be fed to the next round.

Things to Note

Firstly, please note that this document is a Beginner's Guide and so should be used, accordingly, as a brief, superficial overview of *some* of the main components of the T cipher. The following document is nowhere near as thorough or intensive as the work presented in Cryptographic Security Analysis of T-310 by Nicolas Courtois and Students, [1]. Hence, this should only be used as an accompaniment to [1], as opposed to a replacement.
Secondly, and perhaps more importantly, one should note that whenever a function, e.g. X is mentioned, please be aware that $\underline{X} \neq X$
And so to reiterate further, be aware that for the following functions:
$\{T, \underline{T}, D, \underline{D}, P, \underline{P}\}$, it is **not** the case that $\underline{X} = X$, hence we have the following results:

$$T \neq \underline{T}$$
$$D \neq \underline{D}$$
$$P \neq \underline{P}$$

Finally, I believe you now are ready to discover the T-310 Cipher with a focus on the KT1 keys. Good Luck.

1 Preface

The result, we shall seek to understand during this document is as follows:

$$
\begin{aligned}
U_9 &= u_{D(9)} \oplus f \\
U_8 &= u_{D(8)} \oplus U_9 \oplus u_{D(9)} \oplus Z_1(s_2, u_{P(1-5)}) \\
U_7 &= u_{D(7)} \oplus U_8 \oplus u_{D(8)} \oplus u_{P(6)} \\
U_6 &= u_{D(6)} \oplus U_7 \oplus u_{D(7)} \oplus Z_2(u_{P(7-12)}) \\
U_5 &= u_{D(5)} \oplus U_6 \oplus u_{D(6)} \oplus u_{P(13)} \\
U_4 &= u_{D(4)} \oplus U_5 \oplus u_{D(5)} \oplus Z_3(u_{P(14-19)}) \oplus s_2 \\
U_3 &= u_{D(3)} \oplus U_4 \oplus u_{D(4)} \oplus u_{P(20)} \\
U_2 &= u_{D(2)} \oplus U_3 \oplus u_{D(3)} \oplus Z_4(u_{P(21-26)}) \\
U_1 &= u_{D(1)} \oplus U_2 \oplus u_{D(2)} \oplus u_{P(27)}
\end{aligned}
$$

Figure 1: $U_1 - U_9$

2 Feistel Branches

Since, the entire process can be somewhat confusing, it is best to consider an Element of Interest, which we shall denote as 'EOI'. This element is a bit belonging the 1st feistel branch of the structure below, such that it is part of I_1.

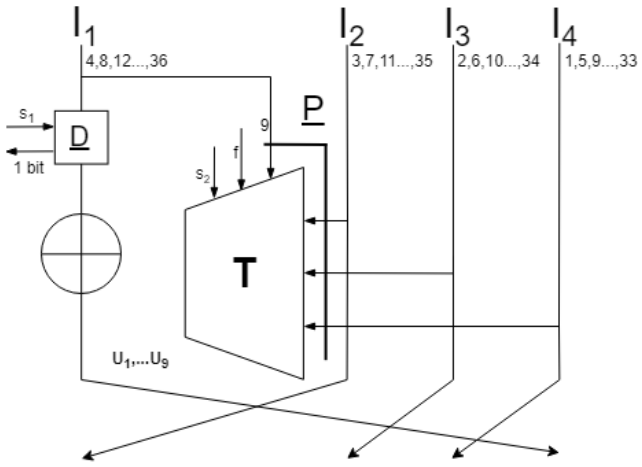

Figure 2: Feistel branches of T-310

We have chosen our EOI to be a bit amongst the 9 bits of I_1, the other three

branches: I_2-I_4 will each also have 9 bits but instead these bits will just pass through unchanged to the next round. It should be noted, however, that they will be present in a different position. Such that we will have:

current $I_2 \longrightarrow I_1$ in next round
current $I_3 \longrightarrow I_2$ in next round
current $I_4 \longrightarrow I_3$ in next round

To further highlight this, we can present a portion of the earlier figure, that can be used to demonstrate exactly which bits pass through unchanged:

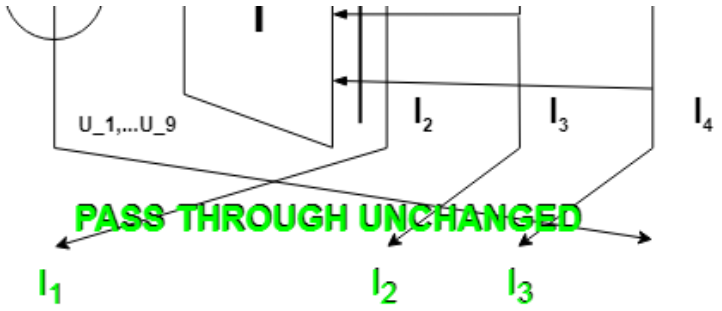

Figure 3: Unchanged branches

3 D function

Since, we have defined our Element of Interest (EOI) to be within the bits of I_1, our EOI is due to be 'changed' in this current round. The first step that will be taken as part of this, is that the 9 bits in I_1 will enter the function D.

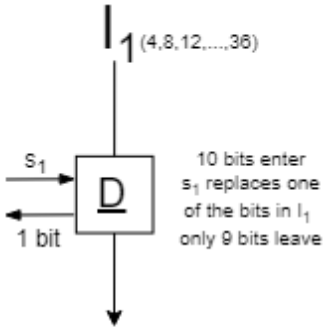

Figure 4: D function

$\underline{\mathrm{D}}$ can be defined as a near permutation of 9 wires with an additional bit of input 's_1' so that the function in relation to the inputs can be defined as:

$$\underline{\mathrm{D}} : \{0,1\}^1 \times \{0,1\}^9 \rightarrow \{0,1\}^9$$

so that

$$\mathrm{D} = \underline{\mathrm{D}}(s_1;\, u_4,\, u_8,\, u_{12},\, \ldots\, ,\, u_{36})$$

where $\underline{\mathrm{D}}$ is the aforementioned function and D is the output of said function.

From Figure 3, paired with the definition of our function $\underline{\mathrm{D}}$, we can deduce that 10 bits enter yet only 9 will exit the function. This is due to the additional bit of input s_1 that will replace the bit which is removed. In our current example it would be best to consider that our EOI is not chosen as the bit to be removed. With that being said, it is important to still note that out of the 9 bits in I_1, 1 bit will be removed during this $\underline{\mathrm{D}}$ function.
Since we are focusing on the KT1 case, we mention that outputs of $\underline{\mathrm{D}}()$ are always mutiples of 4 so that: $D(a) = 4 \cdot b$ with $b \in \{0, ..., 9\}$.
Following, we have two distinguishing cases: the first- when $b = 0$ such that $D(a) = 0$, corresponding directly to the replacement of one bit by the constant s_1. The latter cases, when $b \neq 0$ results in $D(a)$ being a multiple of 4. From these cases we can derive the following equations:

$$D_i(s_1; u_4, u_8, u_{12}, ..., u_{36}) = s_1 \text{ when } D(i) = 0$$
$$D_i(s_1; u_4, u_8, u_{12}, ..., u_{36}) = u_{D(i)} \text{ when } D(i) \neq 0$$

In the KT1 case, we should be aware that D(1)=0 is always true, hence we can think of the later case being true for $i \geq 2$

4 T function

Despite our Element of Interest (EOI) never entering the function $\underline{\mathrm{T}}$, the output of $\underline{\mathrm{T}}$ is xored with the output of $\underline{\mathrm{D}}$ hence, the function $\underline{\mathrm{T}}$ is of great importance to the final output of one round, which we will later describe as $U_1 - U_9$. Note that one of these $U_1 - U_9$ will be directly derived from our EOI, hence we should take a closer look under the hood of the function $\underline{\mathrm{T}}$.
To begin, we should view the $\underline{\mathrm{T}}$ function as a massive aggregation of functions, wire permutations and inputs- which, naturally, is far too incredibly difficult for us to even begin to fathom. Though strange, this initial assumption may make it slightly less embarassing, if we later fail to understand any of the proceeding information.

We shall first consider the input of $\underline{\mathrm{T}}$ which as mentioned in the main paperc[1], we can write as the equation: $T = \underline{T}(f; s_2; v_{1-27})$.
Very trivially, we then can see $\underline{\mathrm{T}}$ has at least 3 inputs. Though since v_{1-27} represents the set $\{v_1, v_2, ...v_{26}, v_{27}\}$, it can in fact be viewed as 29 inputs. Following from this, there are, in fact, additional inputs including 1 bit derived from the IV. But first let's begin with a focus on this $\{v_1, v_2, ...v_{26}, v_{27}\}$ set.
This set, $\{v_1, v_2, ...v_{26}, v_{27}\}$, denotes a set of 27 bits, that are outputted from

the permutation P, so that we have:$\underline{P} : \{0,1\}^{36} \longrightarrow \{0,1\}^{27}$, which relates to T as shown in the diagram below.

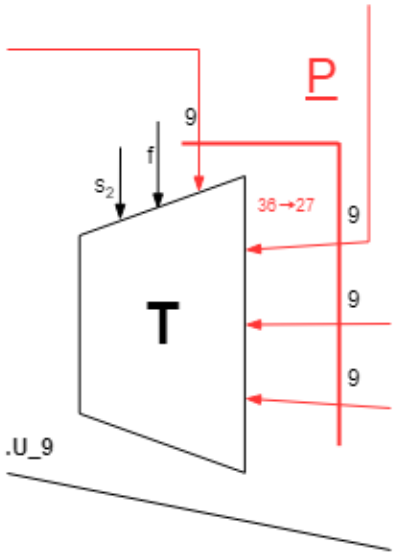

Figure 5: closer look at P function

This function P takes all 36 bits as input, yet outputs only 27, very reminiscent of the D function above. At this stage, if you are not overwhelmed, then please note that D and P are known as long-term wiring functions. In the sense that P speficies which wire should go where. Hence, $P(27) = 9$, corresponding to U_3 denotes that the output wire 9 should be fed into the input of v_{27} in the next round. In fact D and P are so important that they are not just long term wiring functions but they make up the long term key and as a result they are accompanied by a complex set of constraints which can be found in Appendix B of [1], but since this is a Beginner's Guide- will not be listed here. Instead, we can focus on the use of these $\{v_1, v_2, ...v_{26}, v_{27}\}$ within T.

The output of P, equivalent to the set: $\{v_1, v_2, ...v_{26}, v_{27}\}$, is used in the internal structure of T as follows, with a secondary function Z, acting on a summation of combinations on six bits, outputting each time 1 single bit.

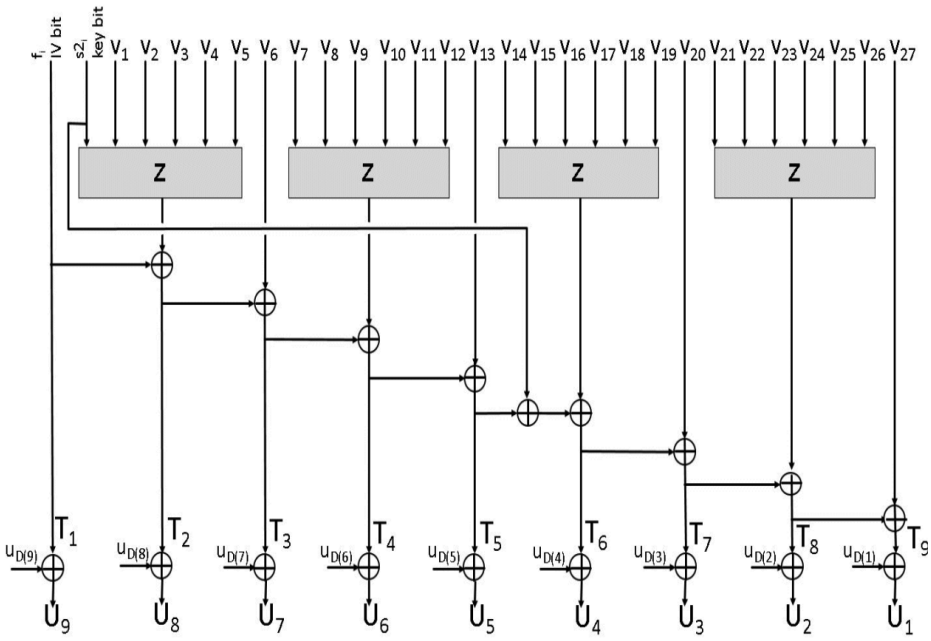

Figure 6: $\underline{P} \longrightarrow \underline{T}$

Do not fret if this diagram seems unexplained here, as to form a somewhat basic understanding of the cipher, the inner workings, at this introductory stage, of $\underline{\mathrm{T}}$ can be almost completely ignored. So the diagram above is just to aid in further demonstrating the complexity of $\underline{\mathrm{T}}$. Further detail on this, can be found in Section 7.5 of [1]. Following we can discuss $\underline{\mathrm{T}}$ as a relation between inputs and outputs such that the following can be derived:

In particular, for one round- we are interested in $\underline{\mathrm{T}}$ with respect to the final outputs $U_1 - U_9$. Hence, we shall proceed by detailing the set of equations that summarise the output of $\underline{\mathrm{T}}$ in terms of T_i such that the following holds:
$\underline{T} : \mathbf{F}_2^{2+27} \longrightarrow \mathbf{F}_2^9$ is directly equivalent to the function $T : \mathbf{F}_2^{29} \longrightarrow \mathbf{F}_2^9$ with the order of outputs inversed.
Here it is important to note that: $\underline{T} \neq T$
By reversed, we mean that- where we have $\underline{T}_i$ this translates directly to T_{10-i}, so that for each bit of the output, of which there will be 9, we have:

$$\underline{T_i}(f, s_2, v_{1-27}) \stackrel{def}{=} T_{10-i}(f, s_2, v_{1-27})$$

Following, we can derive the following equations using T_j as opposed to $\underline{T_i}$, where $j = 10 - i$. As described above, $\underline{\mathrm{T}}$ takes a total of 29 inputs to deliver just 9 outputs, so that, for the equivalent function T we obtain the following properties: for each $j \in \{1...9\}$.

$$
\begin{aligned}
T_1\left(f;\ s_2;\ v_{1-27}\right) &= \mathbf{f} \\
T_2\left(f;\ s_2;\ v_{1-27}\right) &= T_1 \oplus Z(\mathbf{s_2}, v_{1-5}) \\
T_3\left(f;\ s_2;\ v_{1-27}\right) &= T_2 \oplus v_6 \\
T_4\left(f;\ s_2;\ v_{1-27}\right) &= T_3 \oplus Z(v_{7-12}) \\
T_5\left(f;\ s_2;\ v_{1-27}\right) &= T_4 \oplus v_{13} \\
T_6\left(f;\ s_2;\ v_{1-27}\right) &= T_5 \oplus Z(v_{14-19}) \oplus \mathbf{s_2} \\
T_7\left(f;\ s_2;\ v_{1-27}\right) &= T_6 \oplus v_{20} \\
T_8\left(f;\ s_2;\ v_{1-27}\right) &= T_7 \oplus Z(v_{21-26}) \\
T_9\left(f;\ s_2;\ v_{1-27}\right) &= T_8 \oplus v_{27}
\end{aligned}
$$

Figure 7: equations of T_j

where Z is the function described above with a one bit output and v_k corresponding to the aforementioned permutation P. These equations can be achieved by observing the figure on the previous page. Please do take a moment to quickly try and match each xor in these equations with those from the figure on the preceding page until you are able to convince yourself of the truthiness of the statements above. At this point we then ready to achieve our result.

5 Deriving our Result

As mentioned in section 2- we are only concerned with the branch I_1, of which our Element Of Interest was a member. Consequently, our EOI has been through the $\underline{\mathrm{D}}$ function without being removed, subsequently it was xored with a T_j to produce one of our 9 resulting bits that have been changed during this round.

NOTE : Every bit will have its day but for now its our EOI's day.
During this day, our bit shall be scrambled, permutated and xored before finally becoming a member of the U_i family

So reiterating once more, our EOI went into the D function and out the other side, emerging as a $'u_D(i)'$- at this point, it was xored with a member of the T_j family to produce the resulting U_i that will be part of the I_4 branch in the next round.

With this is mind, we shall now proceed to formally describe this situation, so that we have:

$$U_i = u_{D(i)} \oplus T_{10-i}(f, s_2, v_{1...27})$$

This is further detailed in [1] by a series of definitions, which are shown below:

$$(u_{m+1,1}, u_{m+1,5}, u_{m+1,9}, \ldots, u_{m+1,29}, u_{m+1,33}) \stackrel{def}{=}$$
$$(U_1, U_2, U_3, \ldots, U_8, U_9) \stackrel{def}{=}$$
$$\underline{\mathbf{D}}(s_{m,1};\ \ u_{m,I^1}) \oplus \underline{\mathbf{T}}\left(f_{m+1}, s_{m+1,2},\ \ \underline{\mathbf{P}}(u_{m,I^{1-4}})\right) =$$
$$\big(u_{m,D(1)} \oplus T_9(f_{m+1}, s_{m+1,2}, u_{m,P(1-27)}),$$
$$u_{m,D(2)} \oplus T_8(f_{m+1}, s_{m+1,2}, u_{m,P(1-27)}),\ \ u_{m,D(3)} \oplus T_7(f_{m+1}, s_{m+1,2}, u_{m,P(1-27)}), \ldots$$
$$\vdots$$
$$\ldots, u_{m,D(8)} \oplus T_2(f_{m+1}, s_{m+1,2}, u_{m,P(1-27)}),\ \ u_{m,D(9)} \oplus T_1(f_{m+1}, s_{m+1,2}, u_{m,P(1-27)})\big)$$
$$\text{where by convention input}\quad u_{m,0} \stackrel{def}{=} s_{m+1,1},\ \ m \geq 0$$

Figure 8: equations of T_j

If these relations are not immediately evident, we explore the relations below-line by line. So:
In the first line: our bits $U_1, ..., U_9$ will make the I_4 branch of the next round, which notably contains the bits at position $\{1, 5, 9, ..., 33\}$. Where m denotes the current round, we have $m + 1$ to denote the 'next' round. so $u_{m+1,1}$ refers to the bit 1 in the next round.
The second line is simply highlighting the equivalence, so that if our EOI was U_2, it would correspond to the second bit in the set of bits $\{1, 5, 9..., 33\}$, hence $U_2 = 5$ so our bit will be bit number 5 in the input to the next round, denoted u_{m+1} , so we will have $u_{m+1,5}$ to tell us that our current bit will go to bit number 5 in the next round,
These third and fourth lines are describing the exact relation that I discussed above, where our EOI is being retained by $\underline{\mathrm{D}}$ and xored with $\underline{\mathrm{T}}$. First described generally on third line, before we describe on each input bit as can be seen in line 4 and onwards.

After exploring these definitions, we can now use basic mathematics to derive the result presented at the beginning of the paper, which can be seen on the page overleaf.
But using the definitions above, instead of simply presenting the results, we shall instead derive them step by step, starting with U_9 below:

$$U_9 \stackrel{def}{=} u_{m,D(9)} \oplus T_1(...)$$

From Figure 7, we have:

$$T_1(f; s_2; v_{1-27}) = \mathbf{f}$$

Consequently, subbing T out, we have:

$$U_9 = u_{m,D(9)} \oplus \mathbf{f}$$

■

$$\begin{aligned}
U_9 &= u_{D(9)} \oplus f \\
U_8 &= u_{D(8)} \oplus U_9 \oplus u_{D(9)} \oplus Z_1(s_2, u_{P(1-5)}) \\
U_7 &= u_{D(7)} \oplus U_8 \oplus u_{D(8)} \oplus u_{P(6)} \\
U_6 &= u_{D(6)} \oplus U_7 \oplus u_{D(7)} \oplus Z_2(u_{P(7-12)}) \\
U_5 &= u_{D(5)} \oplus U_6 \oplus u_{D(6)} \oplus u_{P(13)} \\
U_4 &= u_{D(4)} \oplus U_5 \oplus u_{D(5)} \oplus Z_3(u_{P(14-19)}) \oplus s_2 \\
U_3 &= u_{D(3)} \oplus U_4 \oplus u_{D(4)} \oplus u_{P(20)} \\
U_2 &= u_{D(2)} \oplus U_3 \oplus u_{D(3)} \oplus Z_4(u_{P(21-26)}) \\
U_1 &= u_{D(1)} \oplus U_2 \oplus u_{D(2)} \oplus u_{P(27)}
\end{aligned}$$

Figure 9: $U_1 - U_9$

To tackle a harder substitution, we shall derive U_8 and U_7 before presenting a general case. So, we start from the defintion given on the previous page, in terms of T :

$$U_8 = u_{D(8)} \oplus T_2(....)$$

Then subbing out T_2

$$U_8 = u_{D(8)} \oplus T_1(....) \oplus Z(....)$$

subbing out T_1

$$U_8 = u_{D(8)} \oplus f \oplus Z(....)$$

Based on our derivation of U_9 on the previous page, where:

$$U_9 = u_{m,D(9)} \oplus f$$

Which means:

$$f = U_9 \oplus u_{m,D(9)}$$

Hence subbing out f, in the equation:

$$U_8 = u_{D(8)} \oplus f \oplus Z(....)$$

we get the final result:

$$U_8 = u_{D(8)} \oplus U_9 \oplus u_{D(9)} \oplus Z(....)$$

■

In a similar manner, we can derive the equation for U_7

$$U_7 = u_{D(7)} \oplus T_3(....)$$

Then subbing out T_3

$$U_7 = u_{D(7)} \oplus T_2(....) \oplus v_6$$

subbing out T_2

$$U_7 = u_{D(7)} \oplus T_1(....) \oplus Z(....) \oplus v_6$$

Now, we notice the following relation, from above:

$$U_7 = u_{D(7)} \oplus T_1(....) \oplus Z(....)$$

Which rearranges gives us:

$$T_1(....) \oplus Z(....) = U_8 \oplus u_{D(8)}$$

Hence, subbing in the above we have:

$$U_7 = u_{D(7)} \oplus U_8 \oplus u_{D(8)} \oplus v_6$$

We are still in the current round, so we have that v_6 correlates to the wiring output of the next round with P(6) in this round so we have- $U_{m,P(6)}$ with m being our current round. Or more simply, we note as $u_{P(6)}$, and following:

$$U_7 = u_{D(7)} \oplus U_8 \oplus u_{D(8)} \oplus u_{P(6)}$$

■

These discoveries, led to a case for a rudimentary generalisation of the above equations, since we can spot emerging patterns in the equations P: for instance, even i's contains a '$\oplus Z(...)$'
Hence, the equations presented earlier, can be presented as:
For $n \leq 8$, we have:

$$U_n = u_{D(n)} \oplus U_{n+1} \oplus u_{D(n+1)} \oplus Z(....) \text{ if } n \text{ is even}$$
$$U_n = u_{D(n)} \oplus U_{n+1} \oplus u_{D(n+1)} \oplus U_{P(\frac{61-7n}{2})} \text{ if } n \text{ is odd}$$

Note: $\frac{61-7n}{2}$ is the equation describing the sequence {27,20,13,6}, so if you want to know more about its generation- refer to work on arithmetic sequences.

Thus, we have managed to achieve a result for each of the manipulated 9 bits, so that they are dependent on the previous bit and since all other bits are just shifted, we can quite easily begin to work out linear properties that hold between rounds. And if you've understood this paper- you should be well on your way to understanding the T-310 cipher.

References

[1] Nicolas T. Courtois, Klaus Schmeh, Jörg Drobick, Jacques Patarin, Maria-Bristena Oprisanu, Matteo Scarlata, Om Bhallamudi: Cryptographic Security Analysis of T-310

Acknowledgements

I would like to acknowledge the following former student, Matteo Scarlata, for his contribution to the T project, without him- this document would not have been possible. And I would like to extend a special thanks to Professor Nicolas Courtois for co-ordinating the research into the T-310 cipher.