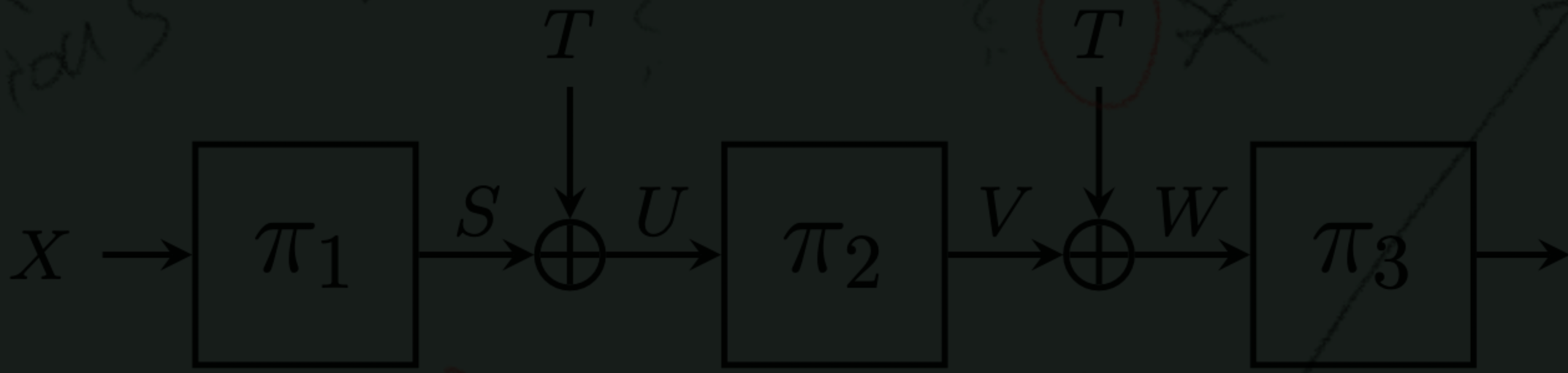
Mustafa Khairallah



Cryptanalysis of TNT

A New Chapter in the LRW Paradigm

This work is done in collaboration with Ashwin Jha, Mridul Nandi and Abishanka Saha

Liskov, Rivest and Wagner 2002

An abridged snapshot of 2002

- AES was announced in 2001 as the new NIST block cipher standard.
- During the AES competition, the Hasty Pudding cipher was proposed.
- The Mercy cipher was proposed for disk encryption in 2000.
- These two ciphers included some form of extra input that is not the plaintext and not the key.

What we had vs what we needed

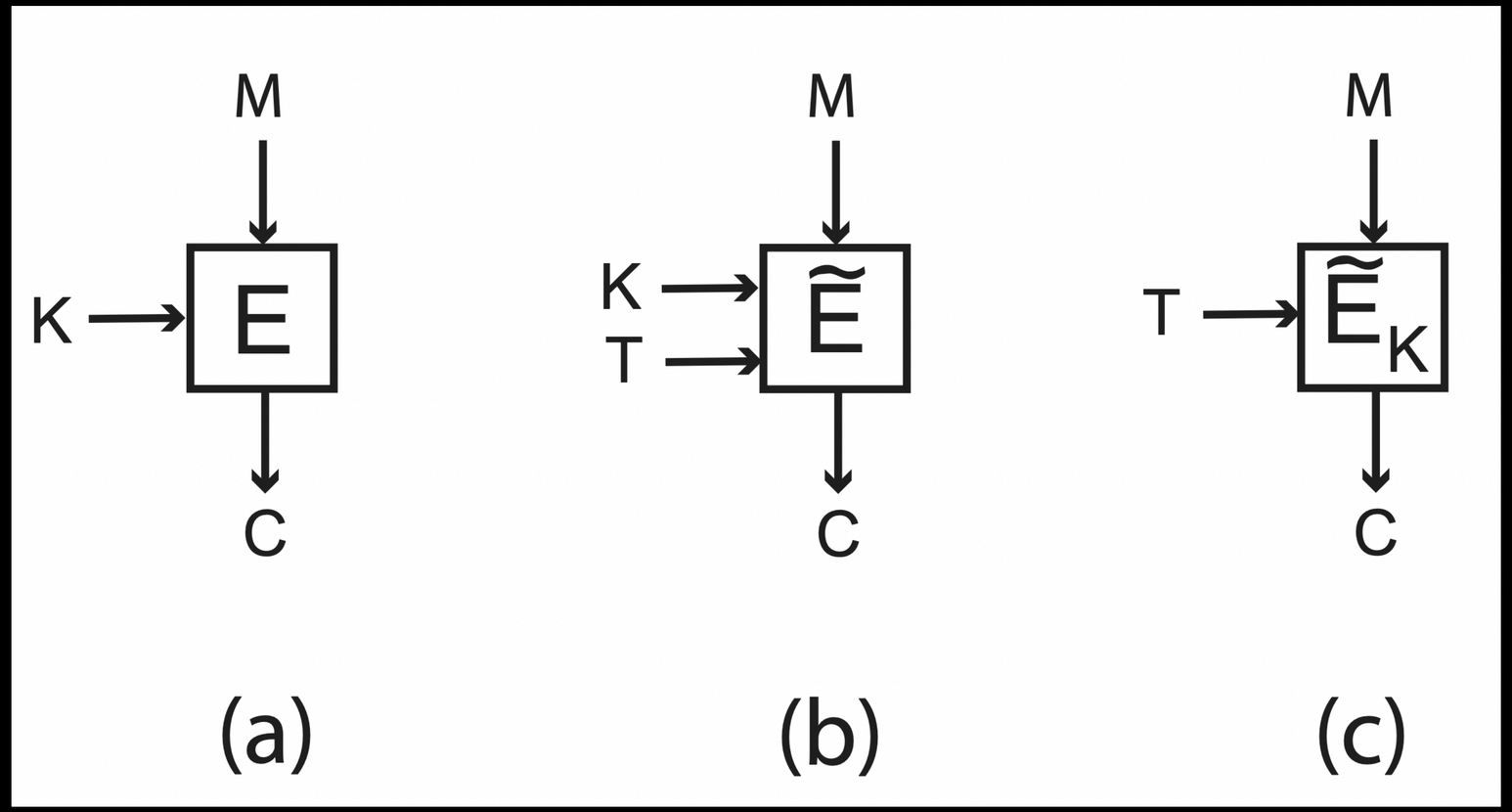
“Many modes of operation and other applications using block ciphers have nonetheless a requirement for “essentially different” instances of the block cipher in order to prevent attacks that operate by, say, permuting blocks of the input.” - Liskov, Rivest and Wagner 2002

	T_1	T_2	T_3	T_4
K_4	P_4	P_4	P_4	P_4
K_3	P_3	P_3	P_3	P_3
K_2	P_2	P_2	P_2	P_2
K_1	P_1	P_1	P_1	P_1

	T_1	T_2	T_3	T_4
K_4	P_m	P_n	P_o	P_p
K_3	P_i	P_j	P_k	P_k
K_2	P_e	P_f	P_g	P_h
K_1	P_a	P_b	P_c	P_d

What is a a TBC?

A PRF and a PRP simultaneously?



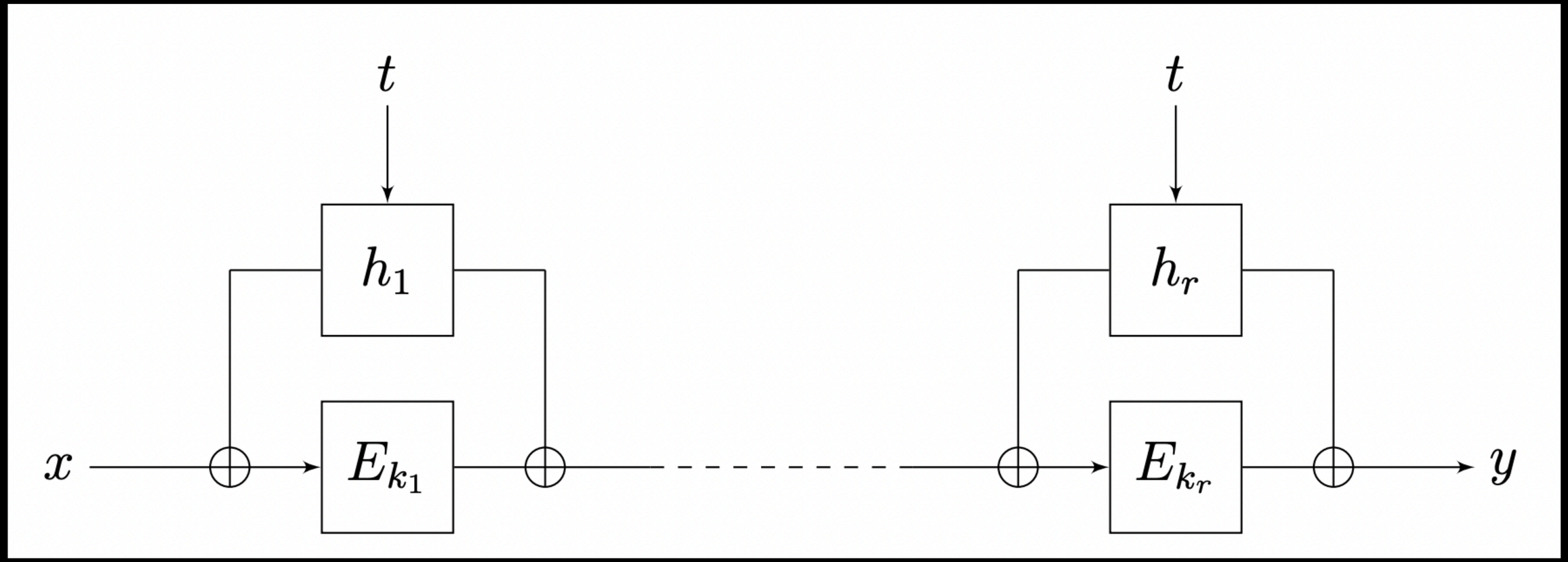
LRW1 - LRW2

$$C \leftarrow E_K(T \oplus E_K(M))$$

$$C \leftarrow h(T) \oplus E_K(h(T) \oplus M)$$

Lampe and Seurin

Cascaded LRW2



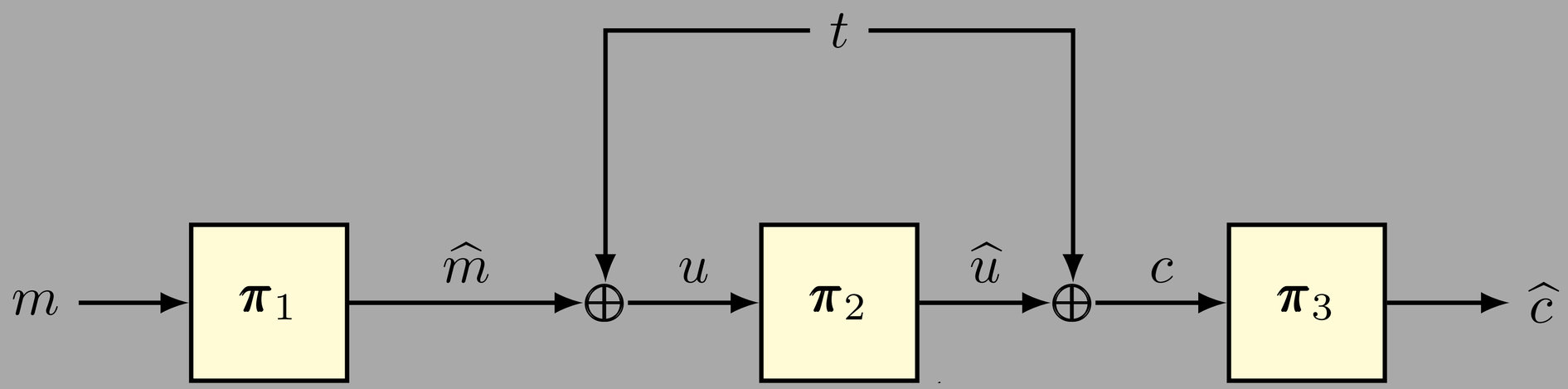
When r = 2, the security is 2n/3

Tightening the security

- 2n/3 security is proven by Lampe and Seurin.
- 3n/4 attack and a restricted 3n/4 bound by Mennink.
- Full 3n/4 bound by Jha and Nandi.

Tweak-aNd-Tweak

TNT: BGGS20



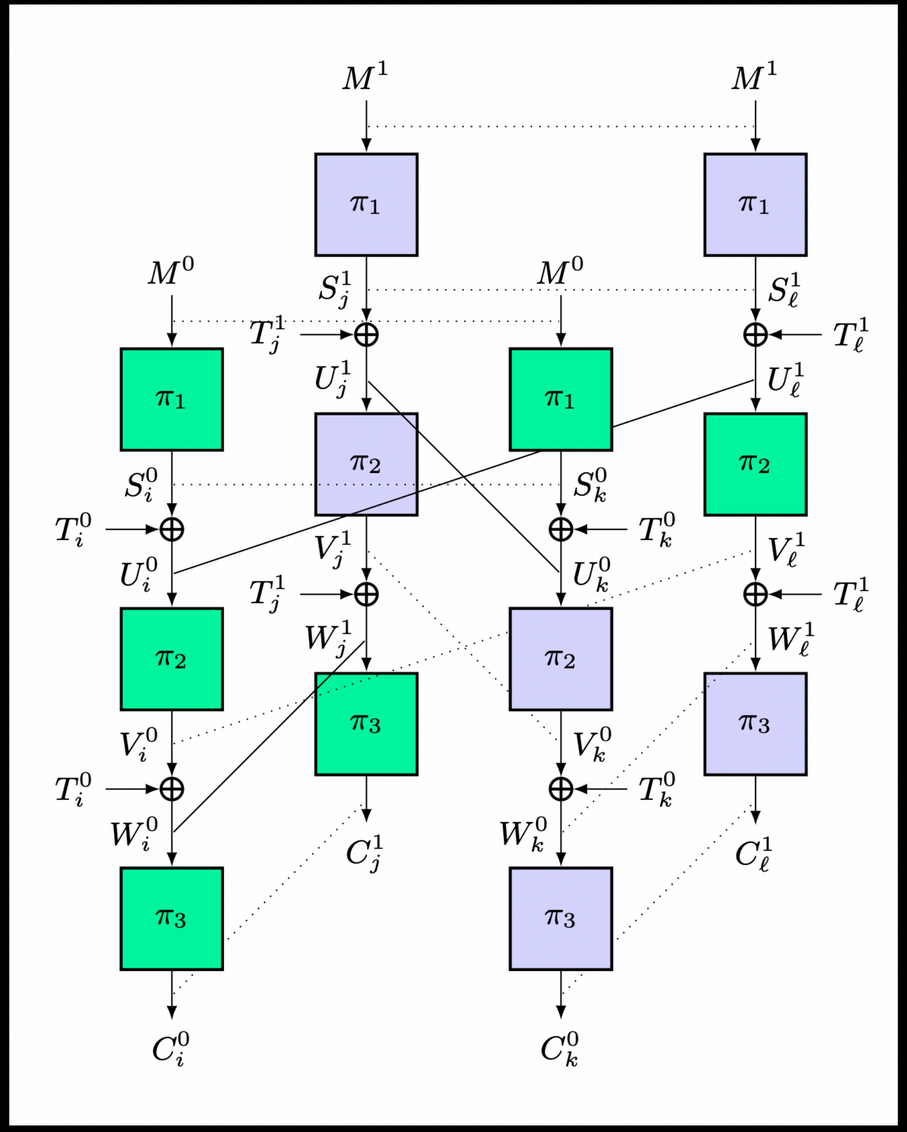
2n/3 CCA Security

GGLS20: 3n/4 attack

And 3n/4 restricted (CPA) proof

- The situation seems to be similar to CLRW2.

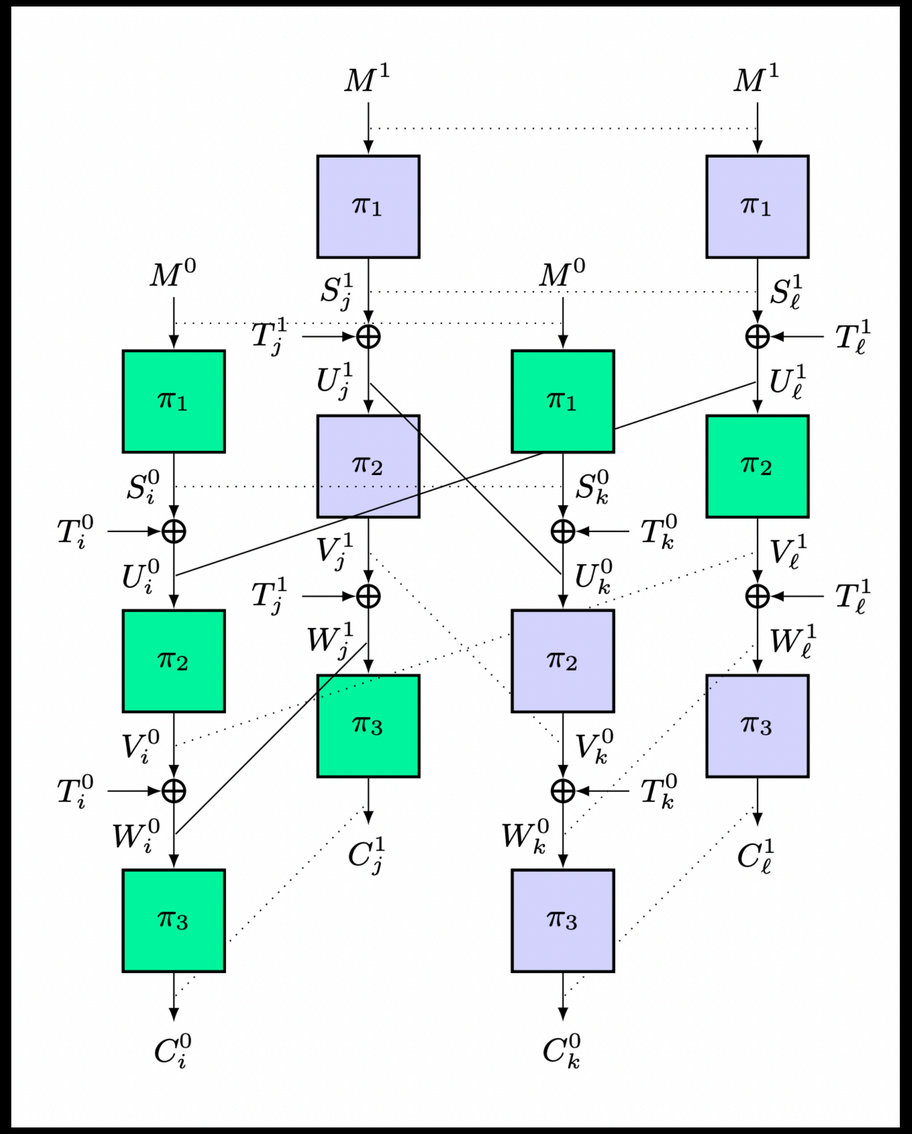
- The authors conjectured 3n/4-bit CCA security is possible.



GGLS 20: 3n/4 attack

And 3n/4 restricted (CPA) proof

- The situation seems to be similar to CLRW2.
- The authors conjectured 3n/4-bit CCA security is possible.
- The bound for *r* rounds gives only n/2-bit CCA security!!



Red Flags

All attacks are CPA

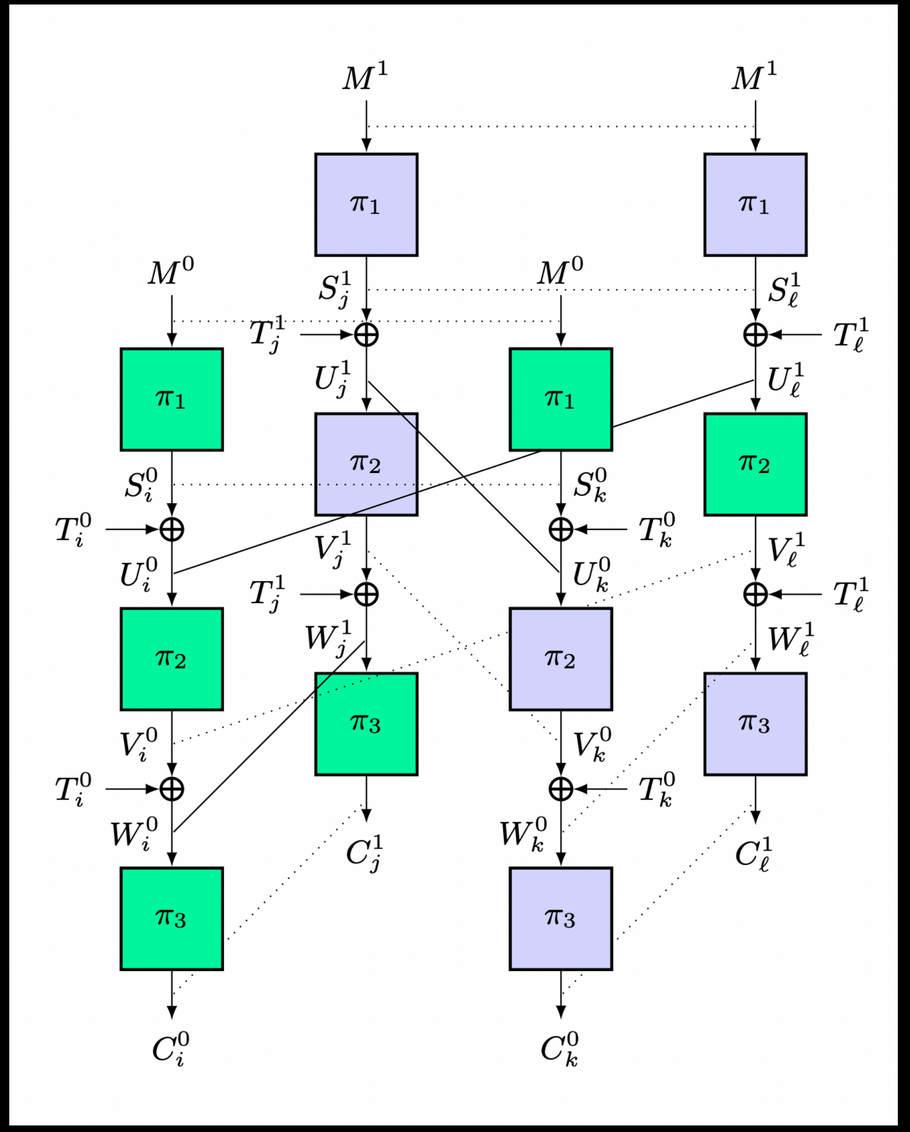
The security implied by the bound for r rounds is much worse than the claimed security

LRW1 does not have any CCA security, can we really go from 0 to 2n/3~3n/4 with only one extra round?

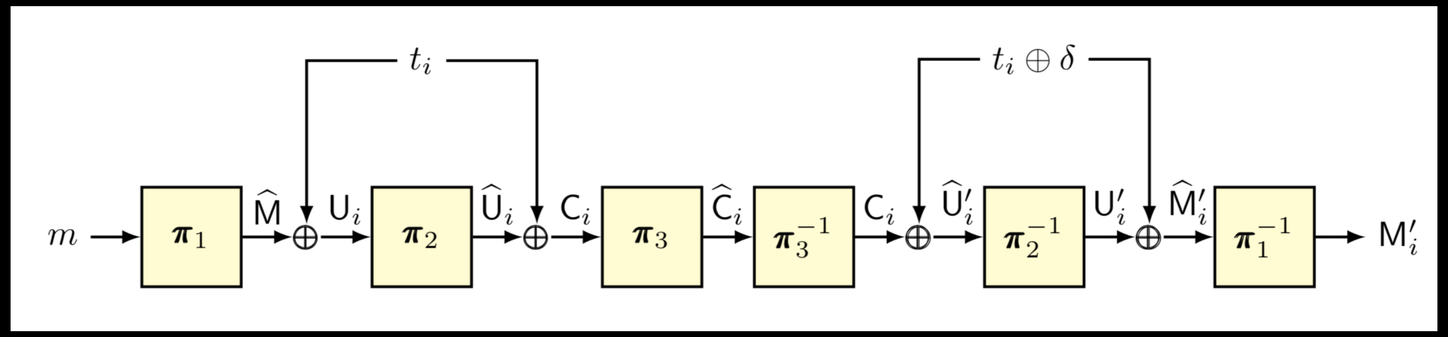
The χ^2 method is fairly new and not used in a lot of symmetric key proofs

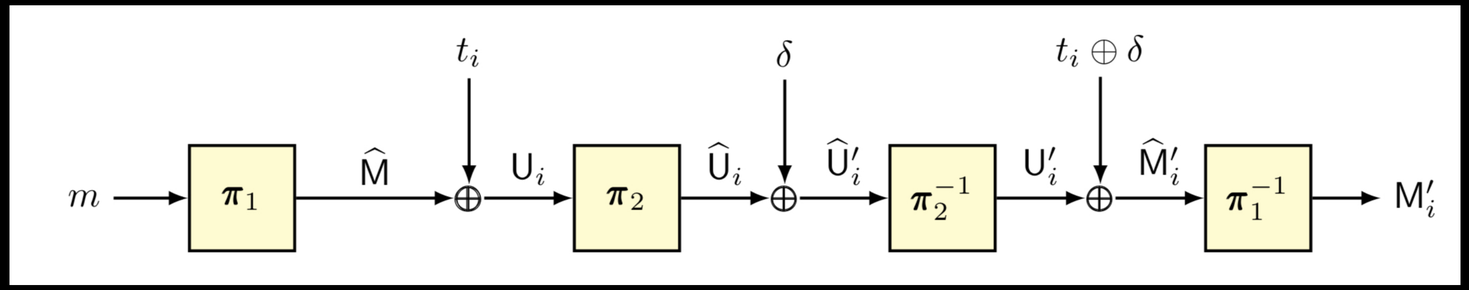
What if?

- The quartets used in these distinguishers require collisions on ciphertexts.
- What if collisions on the ciphertext is a pre-requisite for interesting things to happen?
- A very powerful tool of CCA on TBCs: we can reuse the ciphertext!!



Let’s cascade encryption and decryption





A quartet is a collision on the decrypted plaintext

How fast can they be generated?

Ideal case vs TNT

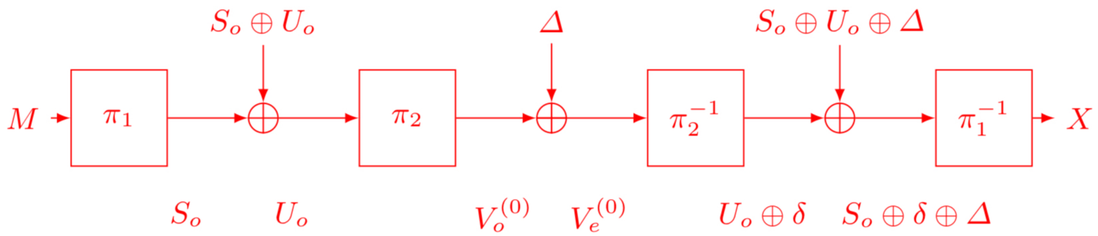
- If TNT is replaced with an ideal TBC, then the cascaded construction is a PRF:
  - Fully secure PRF if the tweaks never repeat.
  - Up to n-bit secure PRF if the tweak repeats.

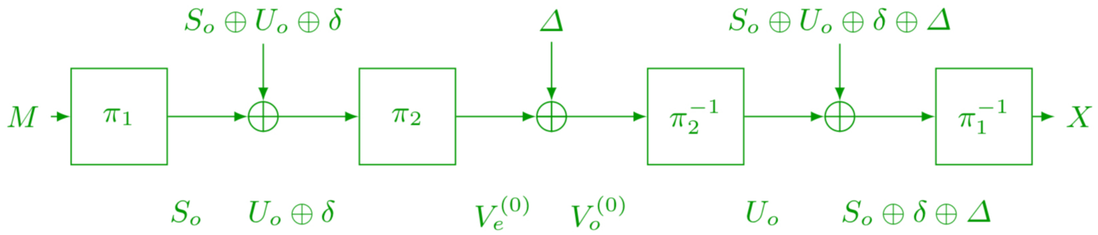
- If the attacks from GGLS20 tell us that the space has more quartets than expected, we should be able to distinguish the cascaded construction from a PRF.

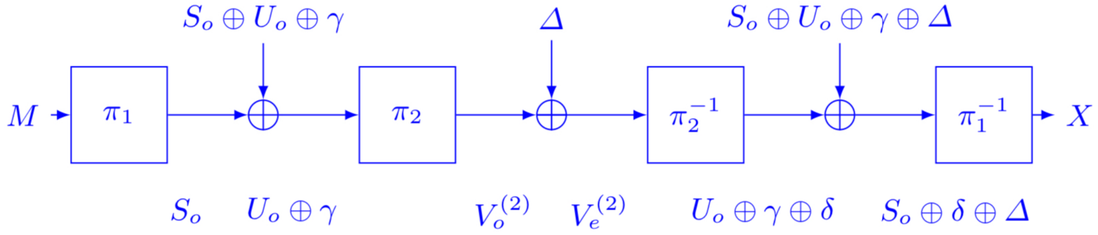
Algorithm 1 Algorithmic description of $\mathbf{A}^{*}(\mathcal{O}^{\pm})$. Note that, `collCount` is an abstract function that counts the number of collisions in a multiset.

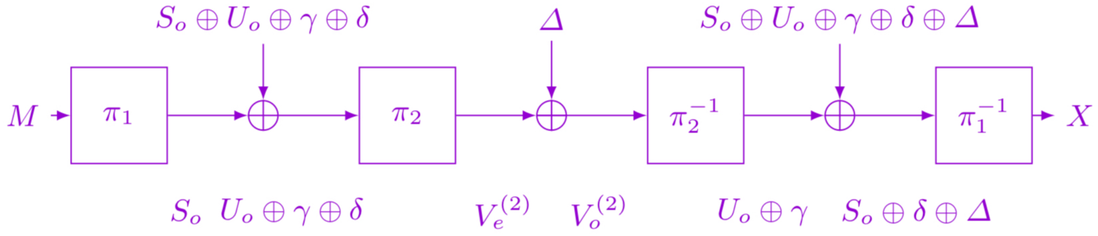
$m \leftarrow 0^n$ ▷ m can be initialized to any constant
$\delta \leftarrow 1^n$ ▷ δ can be initialized to any non-zero constant
$\mathcal{T} \leftarrow \{t_1, \ldots, t_q\}$ ▷ a set of q fixed but distinct tweaks
$\mathcal{M} \leftarrow \emptyset$ ▷ an empty multiset
for $i = 1 \ldots q$ **do**
    $\widehat{\mathsf{C}}_i \leftarrow \mathcal{O}(t_i, m)$
    $\mathsf{M}'_i \leftarrow \mathcal{O}^{-1}(t_i \oplus \delta, \widehat{\mathsf{C}}_i)$
    $\mathcal{M} \leftarrow \mathcal{M} \cup \{\mathsf{M}'_i\}$
$\texttt{COLL}(\mathcal{O}_{\delta,m}) \leftarrow \texttt{collCount}(\mathcal{M})$
if $\texttt{COLL}(\mathcal{O}_{\delta,m}) > \theta(q, n)$ **then**
    return 1
else
    return 0

n	16					
$\log_2(q)$	6	7	8	9	10	11
real	0.06	0.27	0.96	3.72	15.62	63.59
ideal	0.023	0.12	0.48	1.98	7.91	31.17
n	20					
$\log_2(q)$	8	9	10	11	12	13
real	0.073	0.203	1.02	4.01	15.69	63.63
ideal	0.023	0.11	0.47	1.94	7.92	32.57


$S_o \oplus U_o$
Δ
$S_o \oplus U_o \oplus \Delta$
M
π_1
π_2
π_2^{-1}
π_1^{-1}
X
S_o
U_o
$V_o^{(0)}$
$V_e^{(0)}$
$U_o \oplus \delta$
$S_o \oplus \delta \oplus \Delta$


$S_o \oplus U_o \oplus \delta$
Δ
$S_o \oplus U_o \oplus \delta \oplus \Delta$
M
π_1
π_2
π_2^{-1}
π_1^{-1}
X
S_o
$U_o \oplus \delta$
$V_e^{(0)}$
$V_o^{(0)}$
U_o
$S_o \oplus \delta \oplus \Delta$


$S_o \oplus U_o \oplus \gamma$
Δ
$S_o \oplus U_o \oplus \gamma \oplus \Delta$
M
π_1
π_2
π_2^{-1}
π_1^{-1}
X
S_o
$U_o \oplus \gamma$
$V_o^{(2)}$
$V_e^{(2)}$
$U_o \oplus \gamma \oplus \delta$
$S_o \oplus \delta \oplus \Delta$


$S_o \oplus U_o \oplus \gamma \oplus \delta$
Δ
$S_o \oplus U_o \oplus \gamma \oplus \delta \oplus \Delta$
M
π_1
π_2
π_2^{-1}
π_1^{-1}
X
S_o
$U_o \oplus \gamma \oplus \delta$
$V_e^{(2)}$
$V_o^{(2)}$
$U_o \oplus \gamma$
$S_o \oplus \delta \oplus \Delta$

$$\pi_2(x+\delta)+\pi_2(x)=\Delta$$

Statistics of Random Permutations

- If we know all the possible equations and the number of solutions of each equation, we can know exactly how many collisions/quartets exist.
- Think about an Almost Perfect Non-linear permutation. Each Δ has 2^{n-1} possible equations, each has two solutions.
- This means there are no multi-collisions and the number of collisions is 2^{n-1}. Very close to the random function case.
- What if the permutation is linear?

Difference Distribution Table

δ \ Δ	0	1	2	...	$2^n - 1$
0	2^n	0	0	...	0
1	0	0	2	...	4
2	0	2	0	...	0
...	...	...	...	...	...
$2^n - 1$	0	0	8	...	2

Monte-Carlo Estimation of The Number of Solutions

x	2	4	6	≥ 8
$\Pr(x)$	0.772	0.192	0.032	0.004

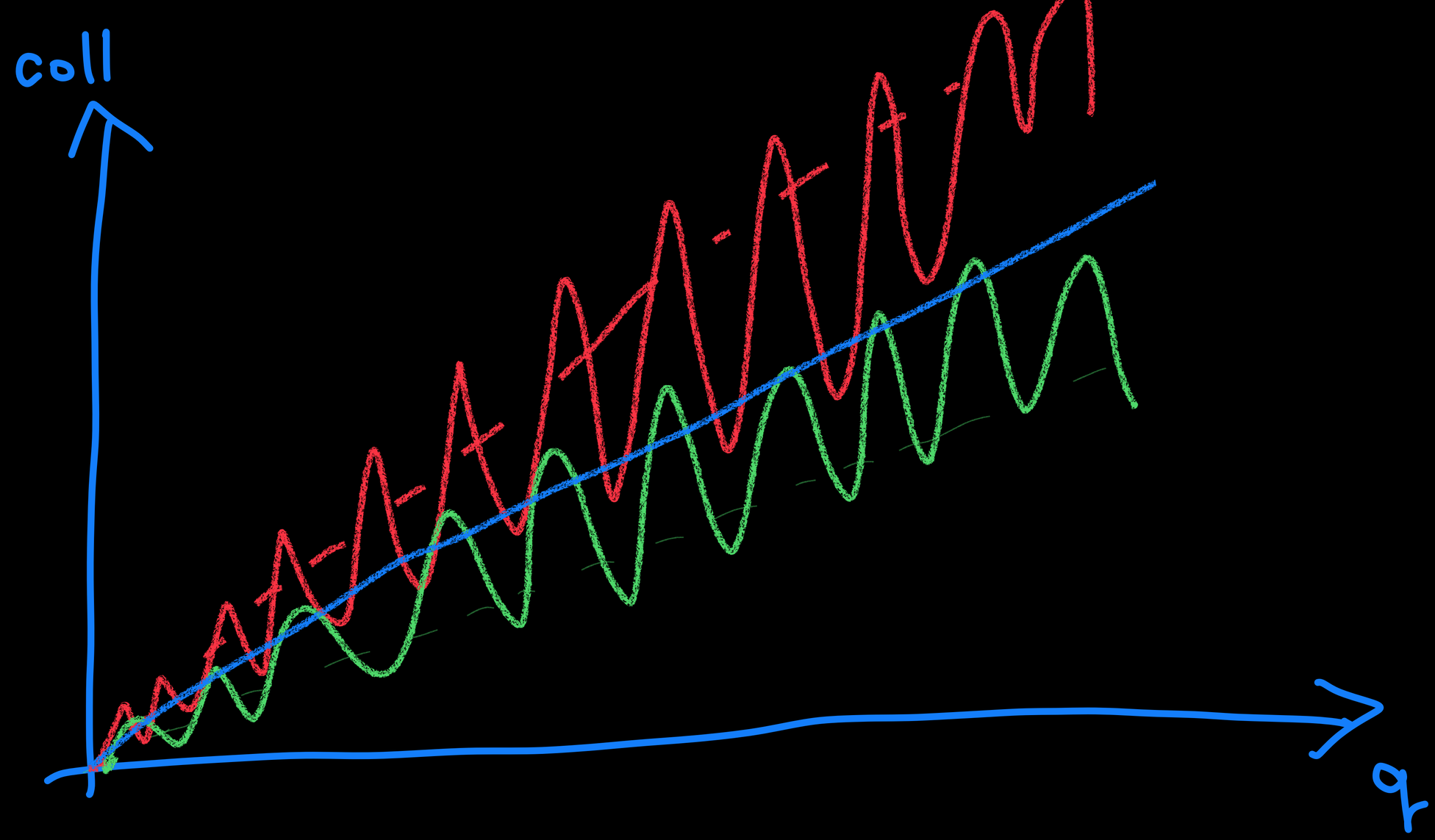
Estimated number of collision

- O’Connor showed in 1993 that 60.65% of the DDT entries are 0.

- Daemen and Rijmen wrote a paper of the statistics of differentials of ideal block ciphers in 2008.

- They proved the distribtution of the entries of the DDT follows the Poisson Distribution.

$$E[\texttt{coll}] = e^{-0.5} \cdot 2^n \sum_{i>0} \frac{0.5^i \binom{2i}{2}}{i!}$$


cell
q

What is the advantage?

Proposition *Let* R_0 *and* R_1 *be two random variables with variances* σ_0^2 *and* σ_1^2*, respectively, and suppose their expectations follow the relation* $\mathsf{Ex}(\mathsf{R}_0) \geq \mu_0 \geq \mu_1 \geq \mathsf{Ex}(\mathsf{R}_1)$*, for some* $\mu_0 \geq \mu_1 \geq 0$*. Then, for* $\mu = (\mu_0 + \mu_1)/2$*, we have*

$$|\mathsf{Pr}(\mathsf{R}_0 > \mu) - \mathsf{Pr}(\mathsf{R}_1 > \mu)| \geq 1 - \frac{4(\sigma_0^2 + \sigma_1^2)}{(\mu_0 - \mu_1)^2}.$$

Theorem *For* $n \geq 4$*,* $10 \leq q \leq 2^n$*, and* $\theta(q, n) = (\mu_{\mathrm{re}} + \mu_{\mathrm{id}})/2$*, we have*

$$\mathbf{Adv}^{\mathsf{ind\text{-}cca}}_{TNT}(\mathbf{A}^*) \geq 1 - 371\frac{2^n}{q^2}.$$

Specifically, for $q \geq 28 \times 2^{\frac{n}{2}}$*,* $\mathbf{Adv}^{\mathsf{ind\text{-}cca}}_{TNT}(\mathbf{A}^*) \geq 0.5$.

Practical advantage

n	q	$\theta(q,n)$	**Success Rate**	q	$\theta(q,n)$	**Success Rate**
16	10	12	87.2%	11	48	99%
20	12	12	86.6%	13	48	99%
24	14	12	90%	15	48	99%
28	16	12	85%	17	48	99%
32	18	12	87.5%	19	48	99%

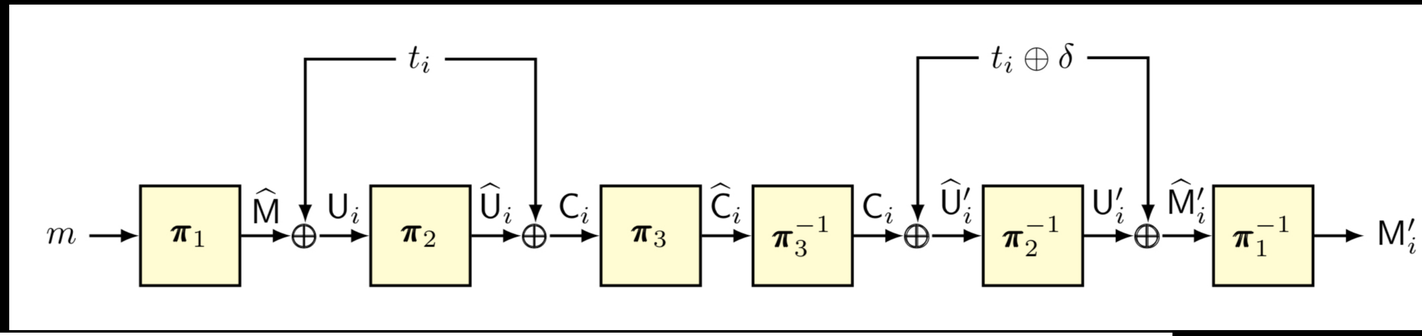
$$1 - 2\frac{2^n}{q^2}$$

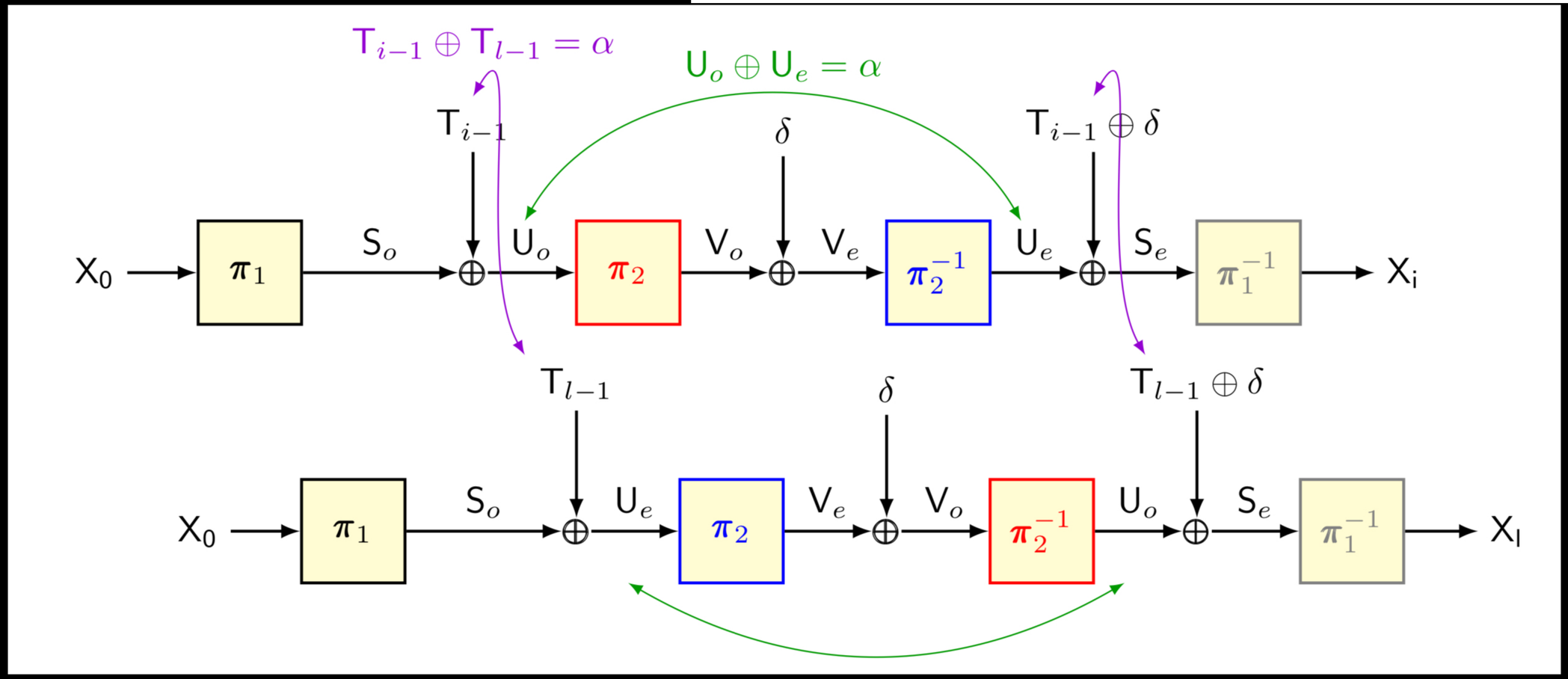
TNT-GIFT-64

n	64			
$\log_2(q)$	32	33	34	35
Average Number of Collisions	1	4	16	61
Time	3 hrs	3 hrs 40 mins	12 hrs 15 mins	20 hrs
CPU Time	5 hrs	10 hrs	28 hr 15 mins	72 hrs
Number of Cores	2	4	8	16
RAM	96 GB	192 GB	128 GB	192 GB
Disk Space	73 GB	146 GB	292 GB	583 GB

How much can we fix the situation?

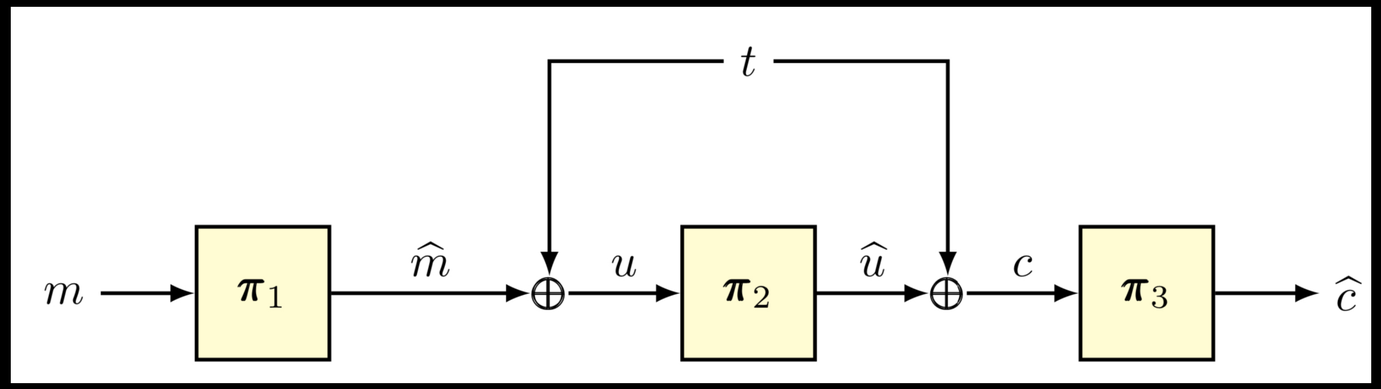
What went wrong?





A Snippet of the χ^2 Method

- We observe the query-response transcript for the first l-1 queries.
- We estimate the probability distribution of the possible corresponding internal values.
- We estimate the probability distribution of the response to query l:
  - for each possibility of the internal values, query l is completely determined.

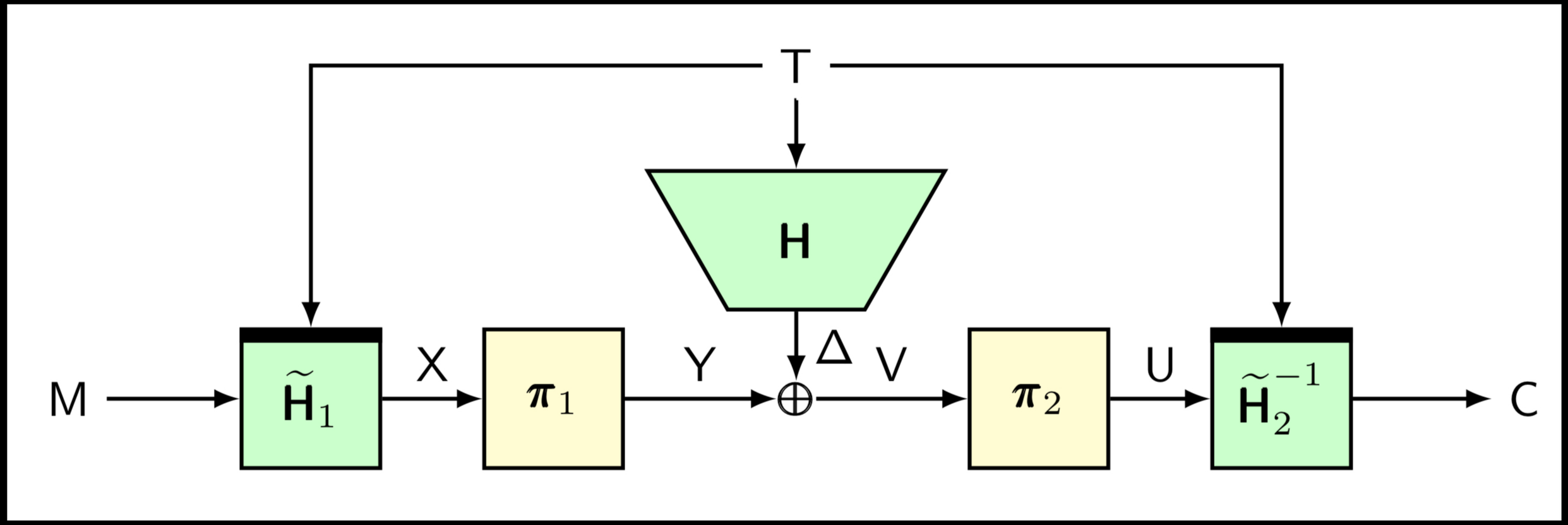


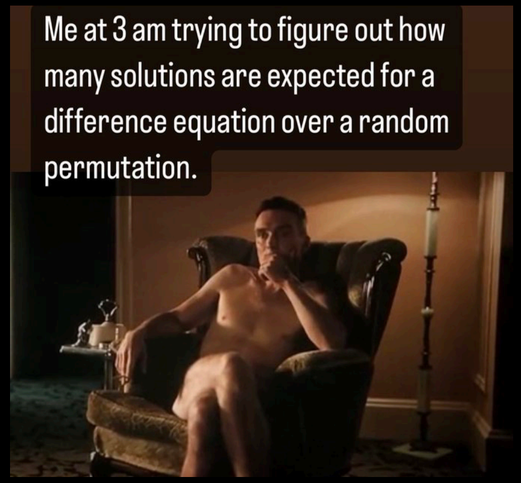
New constructions

- TNT is tightly secure up to birthday bound.
- 1k-TNT: we do not need three independent permutations.
- LRW+: LRW1 wrapped by three hash functions.

LRW+

3n/4-bit security of 4-LRW1, 2-LRW2 and more





“An architect who builds a tower with one floor that collapses will not consider the possibility of constructing a tower by adding several floors of the same kind and hope that the tower will be solid. However, this is what we will do, but this construction will be justified by the security results we will obtain.

Cryptography with bijections does not behave like the architecture of towers!”

Feistel Ciphers - Security Proofs and Cryptanalysis, *Valerie Nachef, Jacques Patarin, Emmanuel Volte*