The Boomerang Attack

Tomer Ashur

Department of Computer Science
University of Haifa
tashur01@campus.haifa.ac.il

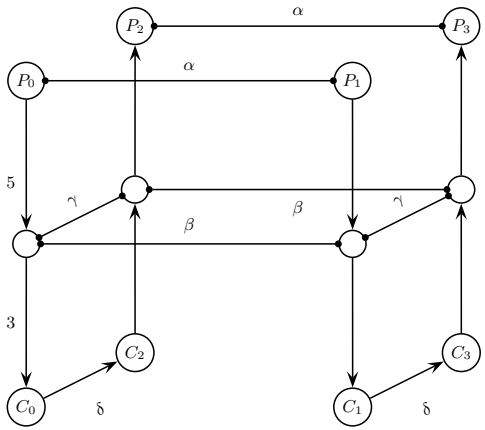
05/05/2013

What is the Boomerang Attack

- An extension of differential cryptanalysis.
- Invented by David Wagner, and published in 1999.

How Does it Work - in a Nutshell

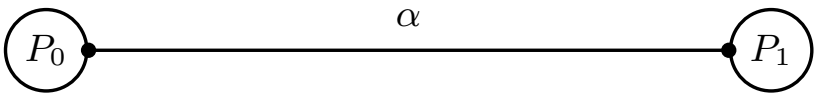
- Instead of using one long differential that covers the full cipher, we use two shorter differentials of each covering part of the cipher.
- We append the two differentials to build a boomarng that covers the full cipher.



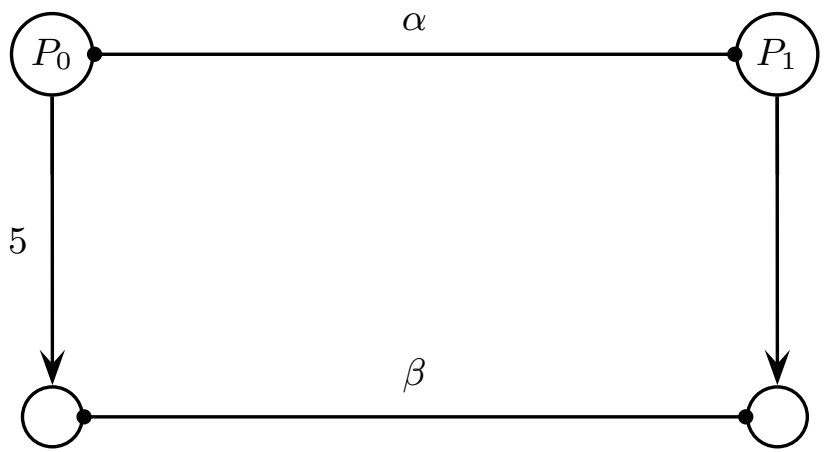
Why don't we Always Use it?

- The attack model is different.
- The complexity

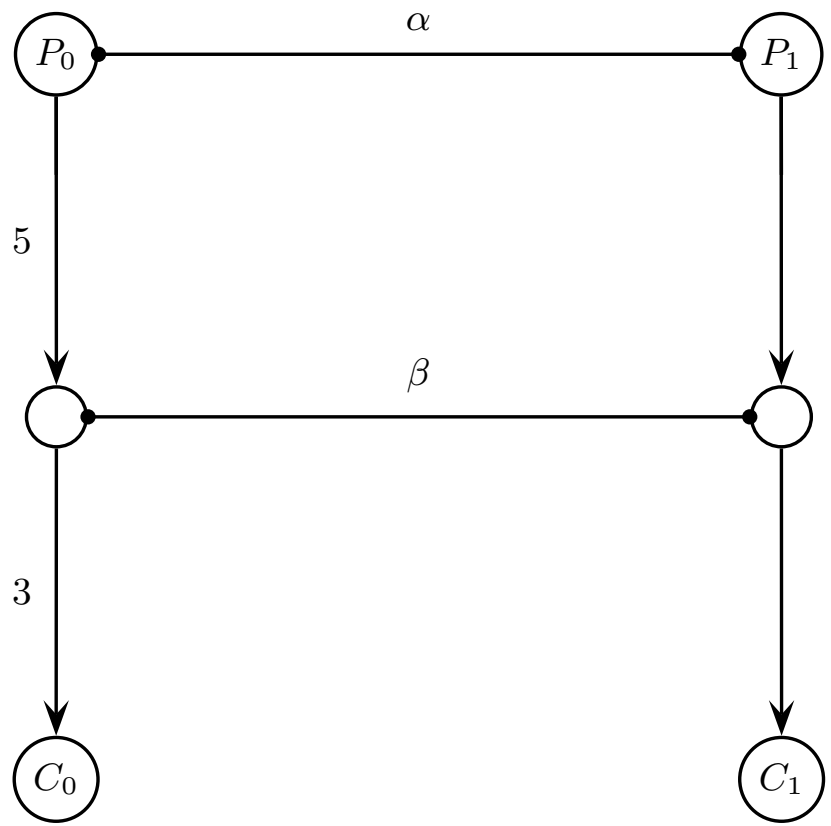
A Step-by-step Construction



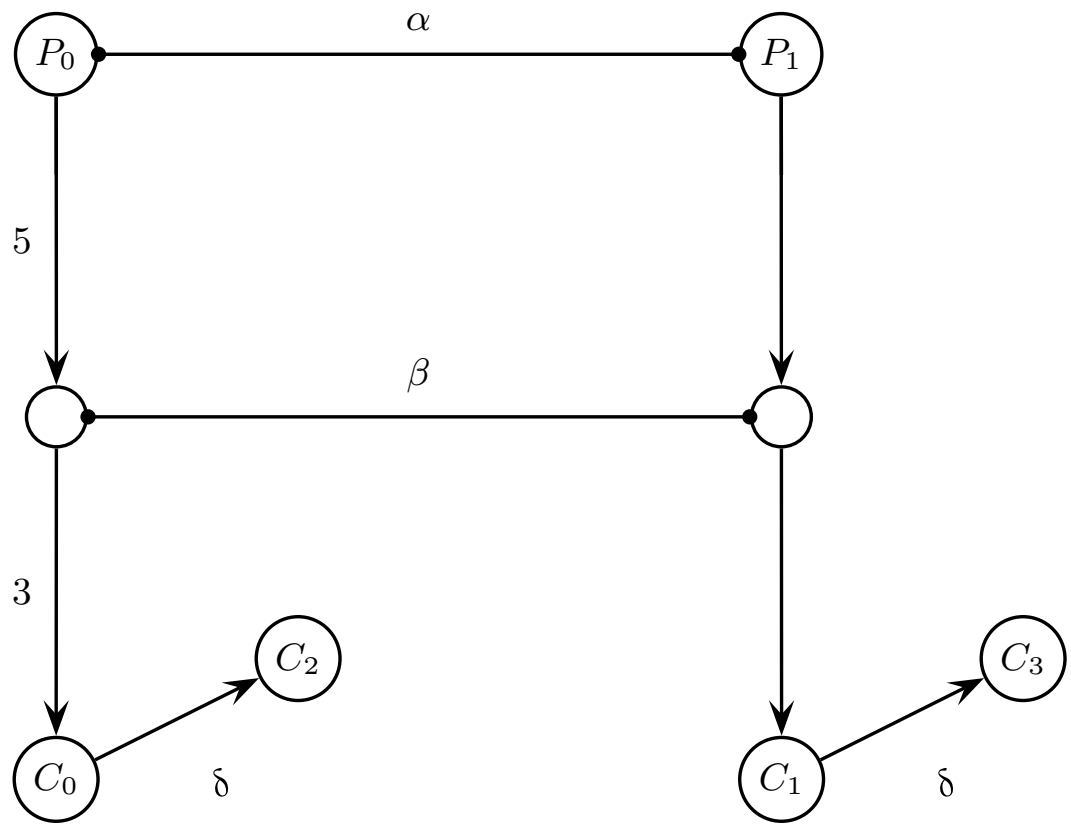
A Step-by-step Construction - Cont.



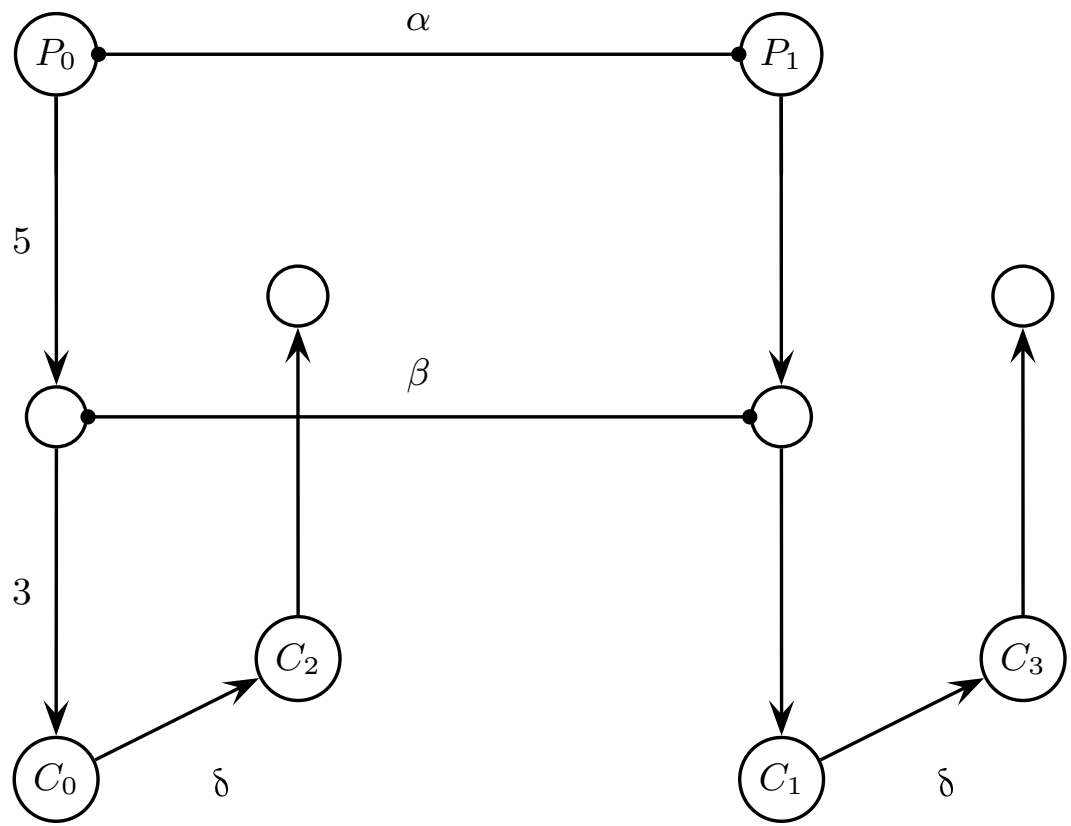
A Step-by-step Construction - Cont.



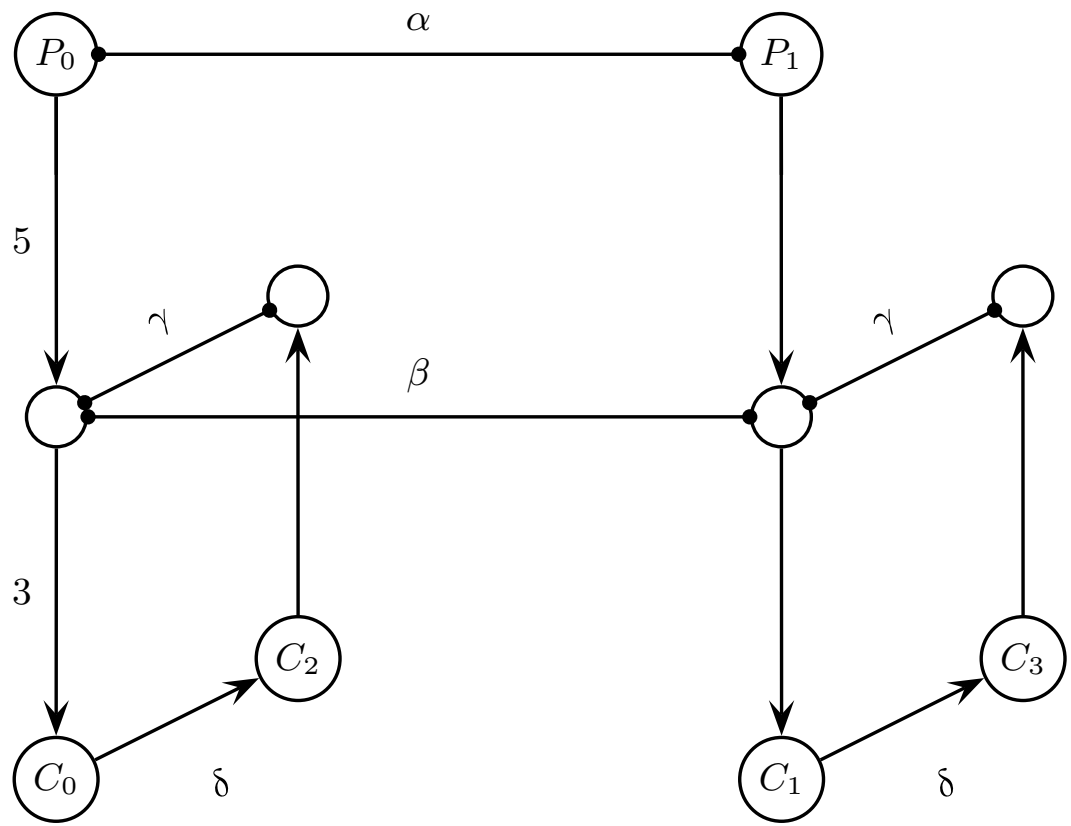
A Step-by-step Construction - Cont.



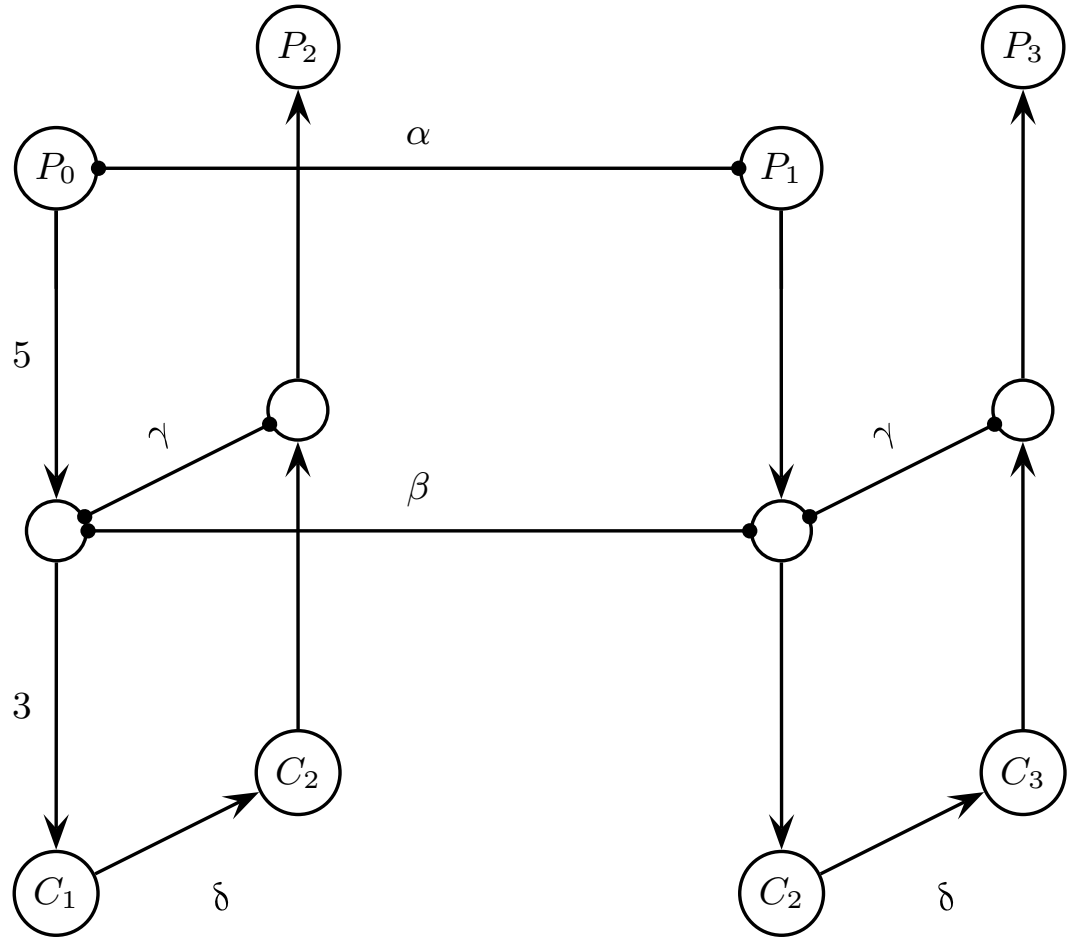
A Step-by-step Construction - Cont.



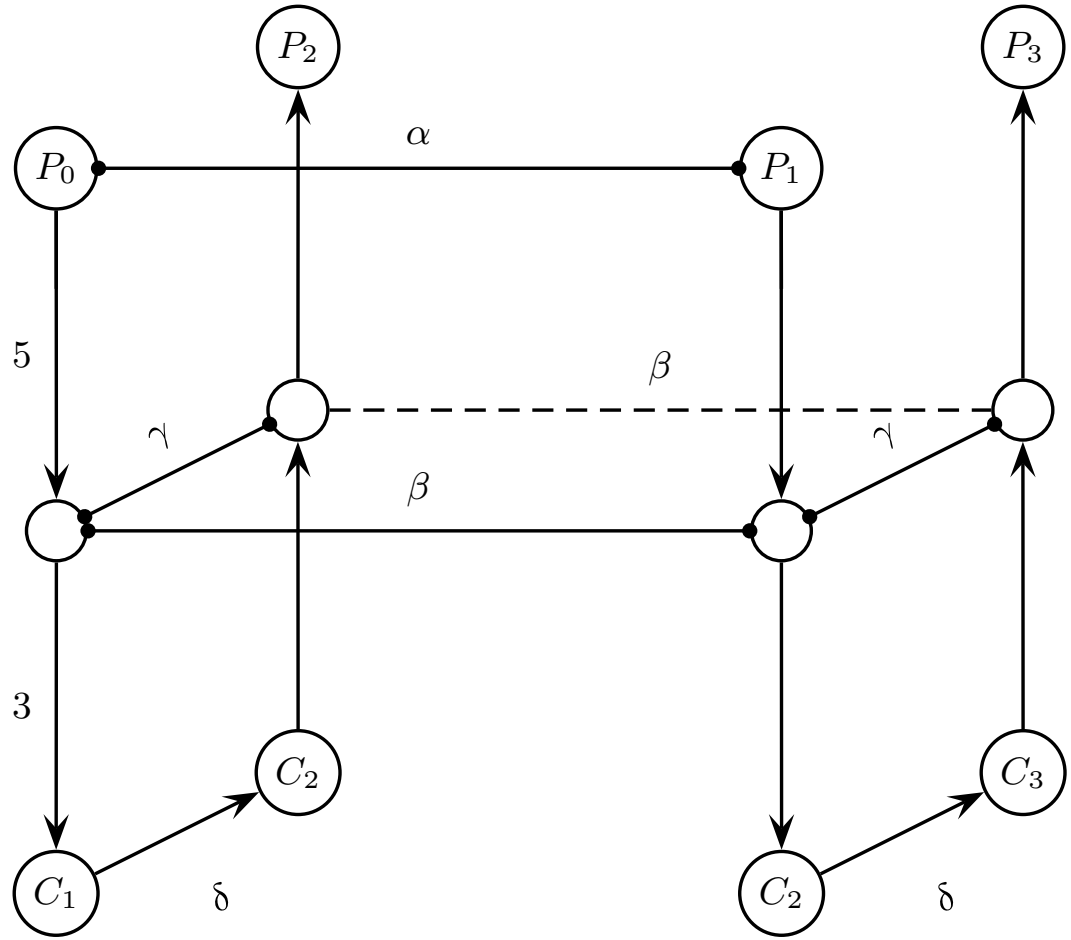
A Step-by-step Construction - Cont.



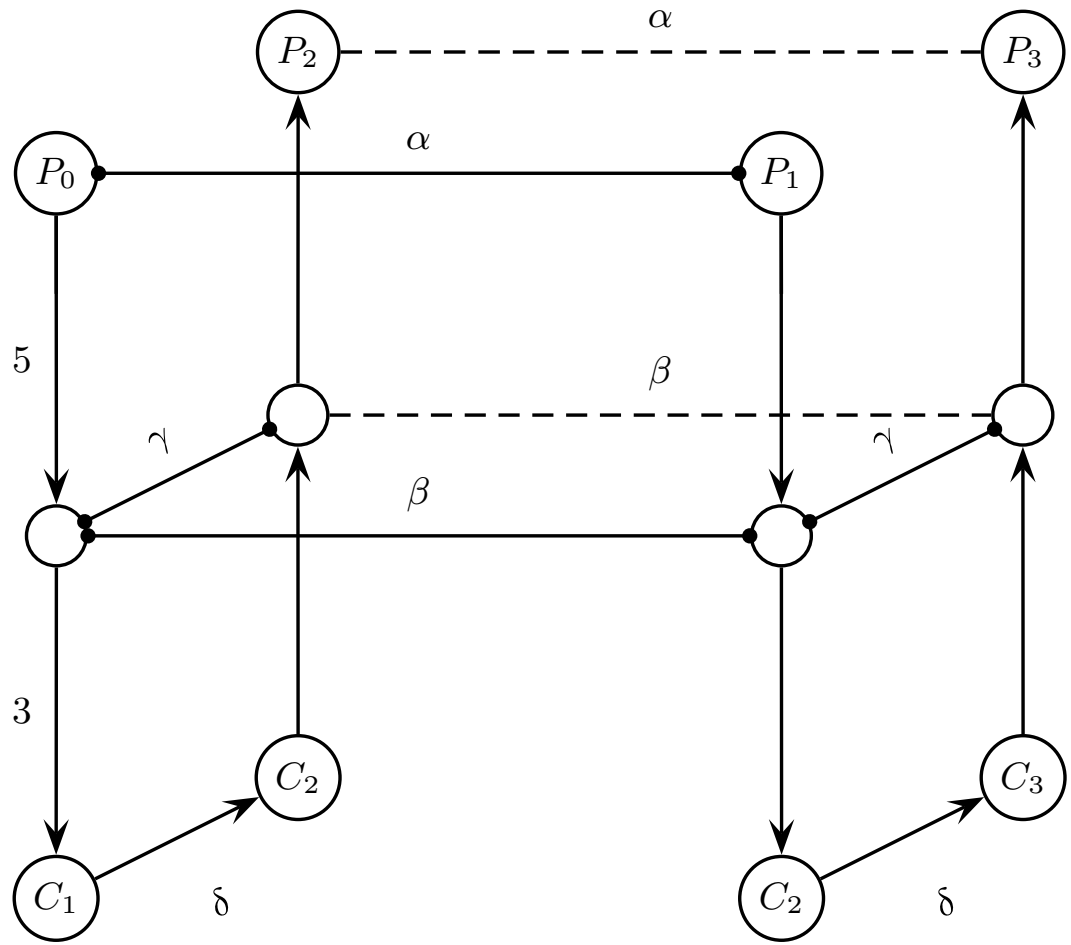
A Step-by-step Construction - Cont.



A Step-by-step Construction - Cont.



A Step-by-step Construction - Cont.



What are the Odds?

What are the Odds?

- α cause β with probability p

What are the Odds?

- α cause β with probability p
- δ cause γ with probability q

What are the Odds?

- α cause β with probability p
- δ cause γ with probability q
- We need this event to happen twice.

What are the Odds?

- α cause β with probability p
- δ cause γ with probability q
- We need this event to happen twice.
- Finally, β cause α with probability p

What are the Odds?

- α cause β with probability p
- δ cause γ with probability q
- We need this event to happen twice.
- Finally, β cause α with probability p
- So...

What are the Odds?

- α cause β with probability p
- δ cause γ with probability q
- We need this event to happen twice.
- Finally, β cause α with probability p
- So...
- $(p \cdot q)^2$

What is it Good For?

The Key Recovery

- Just do the Usual Trick

The Key Recovery

- Just do the Usual Trick
- $E(4_x) = 10_x$

The Key Recovery

- Just do the Usual Trick
- $E(4_x) = 10_x$
- $S_1(10_x \oplus k_0) = A_x$

The Key Recovery

- Just do the Usual Trick
- $E(4_x) = 10_x$
- $S_1(10_x \oplus k_0) = A_x$
- $k_0 \in \{000001, 010001, 100001, 110001, 101111, 011111\}$

The Inside-out Attack

- Use truncated differentials.
- Use the birthday paradox to make the differentials collide, having the reqiured difference.

*R-attacks

Related-key Differentials

Questions