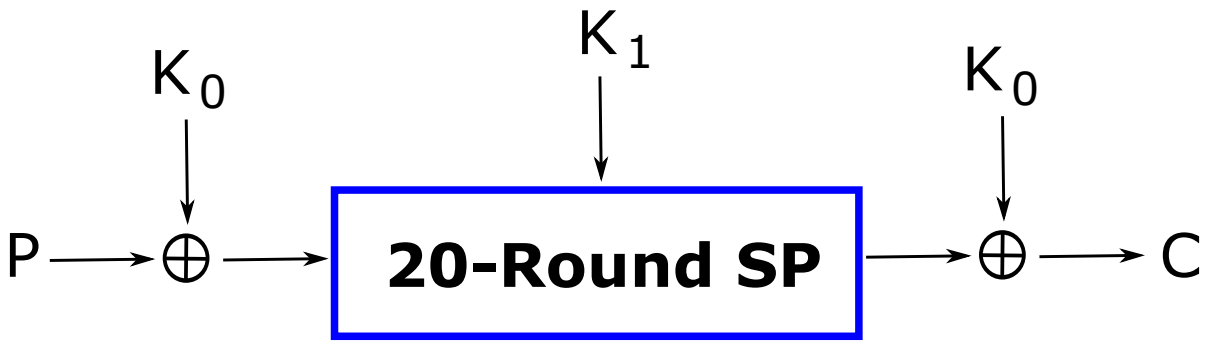
An Observation on PRIDE

Jian Guo, Jérémy Jean, Ivica Nikolić

Nanyang Technological University, Singapore

PRIDE

- Lightweight block cipher from CRYPTO'14
- Based on the FX construction (security $DT \geq 2^{2n}$)
- Internal cipher is 20-round SP

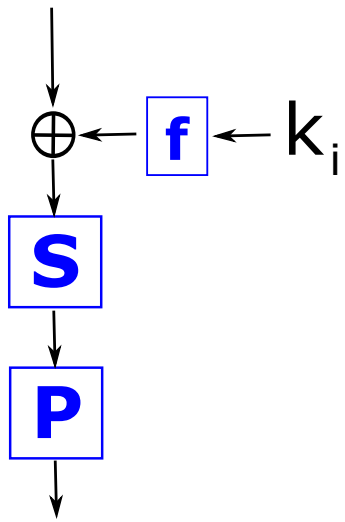


20-round SP of PRIDE

Round composed of:

- Subkey addition, i.e. XOR of $f(k_i)$
- Substitution layer
- Permutation layer

One round



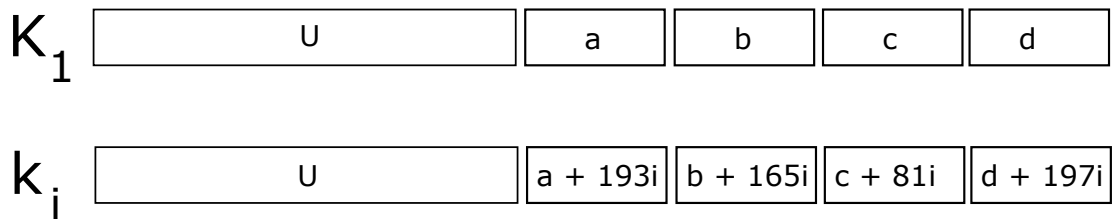
Key Schedule

Simple key schedule; for master key K_1

$$K_1 = u_1||u_2||u_3||u_4||a||b||c||d$$

subkeys are

$$k_i = u_1||u_2||u_3||u_4||a + 193 \cdot i||b + 165 \cdot i||c + 81 \cdot i||d + 197 \cdot i$$



Sliding keys

Slid pair of keys $K_1, \overline{K_1}$:

$$\begin{aligned} K_1 &= u_{1,2,3,4}|| & a|| & b|| & c|| & d \\ \overline{K_1} &= u_{1,2,3,4}|| & a+193|| & b+165|| & c+81|| & d+197 \end{aligned}$$

ideal for slide attacks.

But, no claim of resistance against related-key in PRIDE

Tackle the Security Bound

How about trying to tackle the security bound

$$D \cdot T \geq 2^{2n}$$

where

- D is the amount of data
- T is the number of calls to cipher

NANYANG TECHNOLOGICAL UNIVERSITY

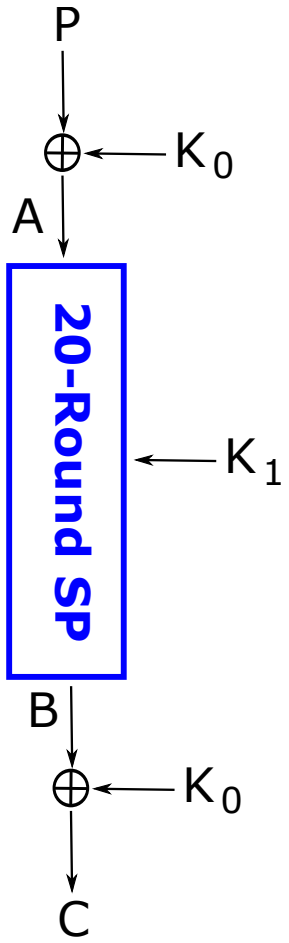
Initial observation

Note that:

$$P \oplus C = A \oplus B.$$

If A and K_1 are correctly guessed, then $P \oplus C$ will reveal this

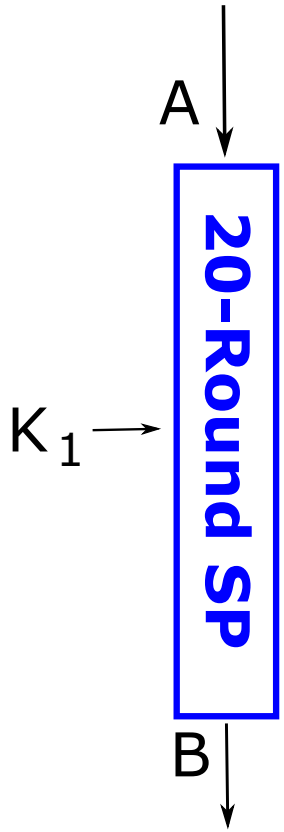
But the chance of success is 2^{-2n}



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

1.
2.
3.
4.
5.
6.
7.

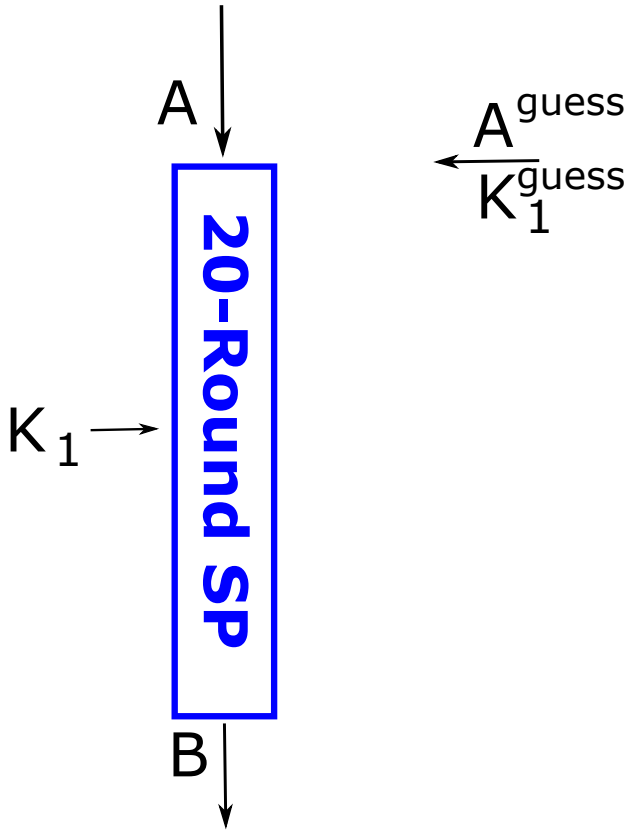


NANYANG TECHNOLOGICAL UNIVERSITY

Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

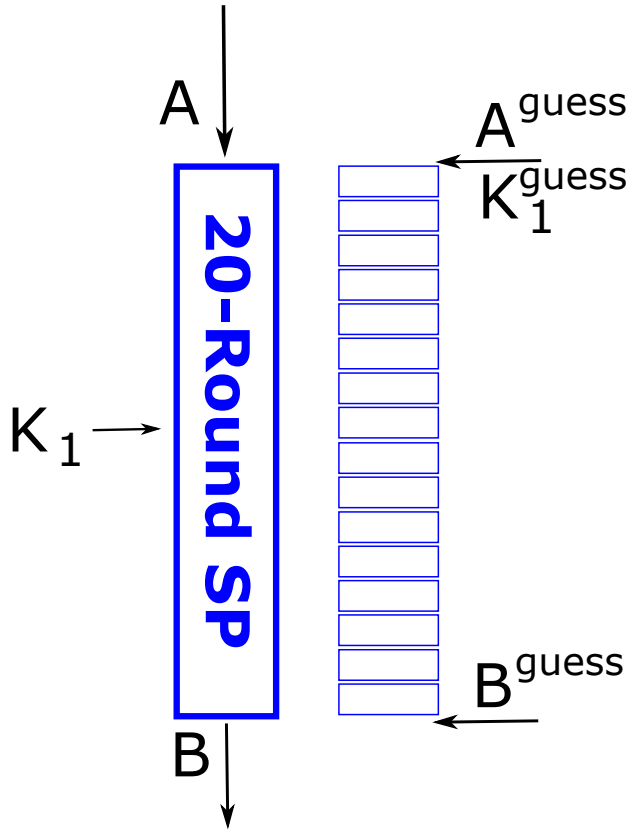
1. Take random A^{guess}, K_1^{guess}
2.
3.
4.
5.
6.
7.



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

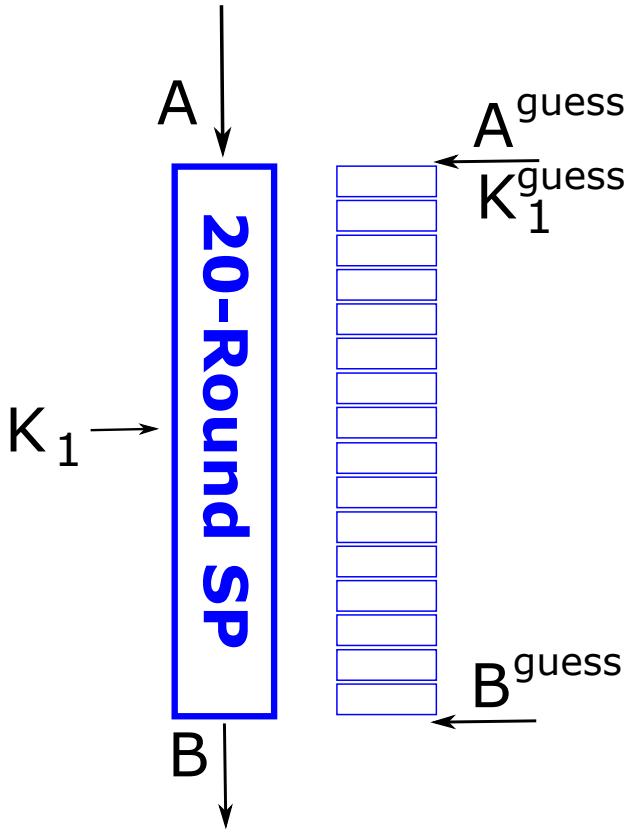
1. Take random A^{guess}, K_1^{guess}
2. Go 20 rounds, produce B^{guess}
3.
4.
5.
6.
7.



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

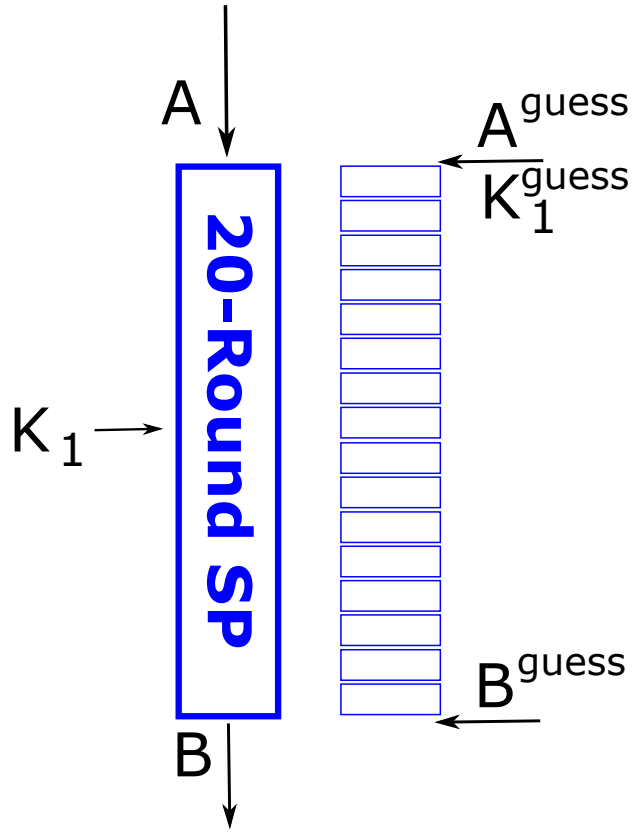
1. Take random A^{guess}, K_1^{guess}
2. Go 20 rounds, produce B^{guess}
3. Check if $A^{guess} \oplus B^{guess} = A \oplus B$
4.
5.
6.
7.



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

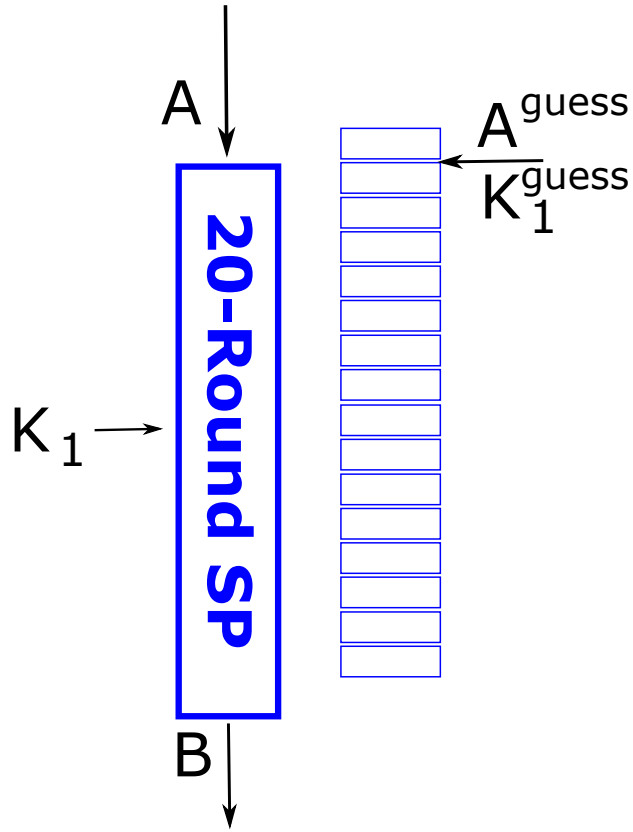
1. Take random A^{guess}, K_1^{guess}
2. Go 20 rounds, produce B^{guess}
3. Check if $A^{guess} \oplus B^{guess} = A \oplus B$
4. If yes, then candidate (stop, double check)
5.
6.
7.



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

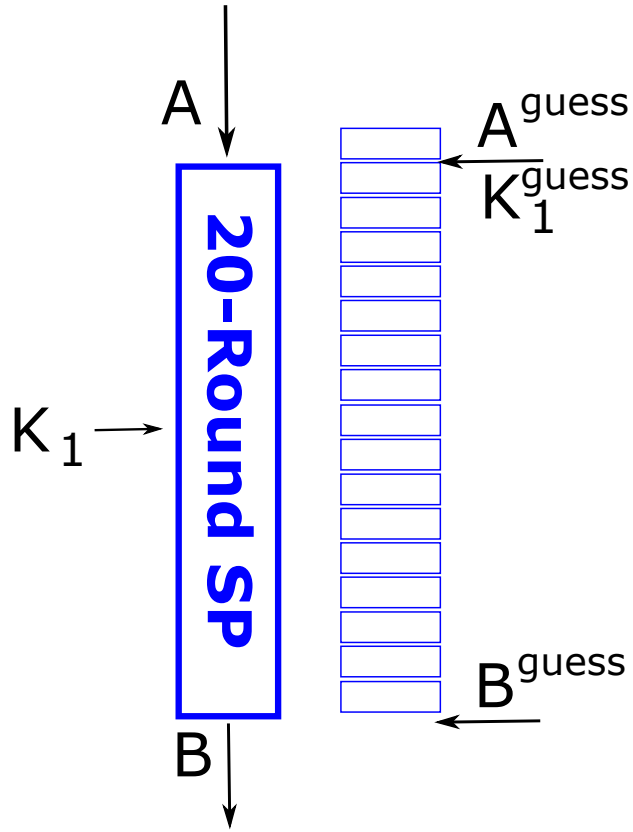
1. Take random A^{guess}, K_1^{guess}
2. Go 20 rounds, produce B^{guess}
3. Check if $A^{guess} \oplus B^{guess} = A \oplus B$
4. If yes, then candidate (stop, double check)
5. If not, shift by one round
6.
7.



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

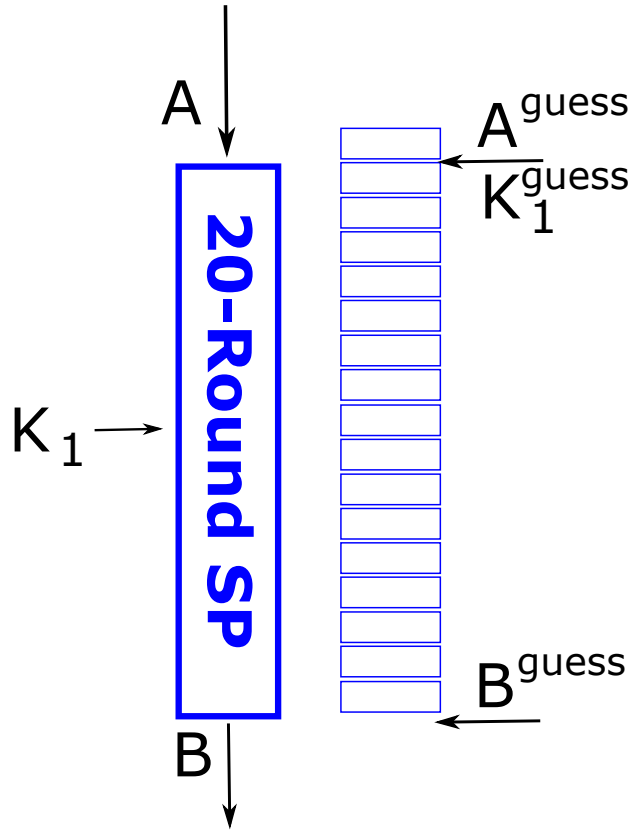
1. Take random A^{guess}, K_1^{guess}
2. Go 20 rounds, produce B^{guess}
3. Check if $A^{guess} \oplus B^{guess} = A \oplus B$
4. If yes, then candidate (stop, double check)
5. If not, shift by one round
6. Go 1 round, produce new B^{guess}
7.



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

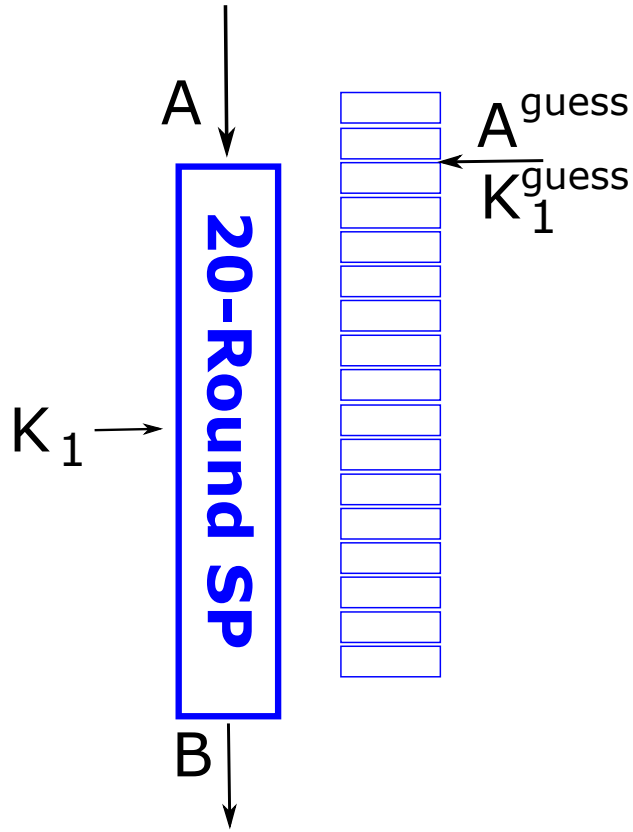
1. Take random A^{guess}, K_1^{guess}
2. Go 20 rounds, produce B^{guess}
3. Check if $A^{guess} \oplus B^{guess} = A \oplus B$
4. If yes, then candidate (stop, double check)
5. If not, shift by one round
6. Go 1 round, produce new B^{guess}
7. Go to step 3



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

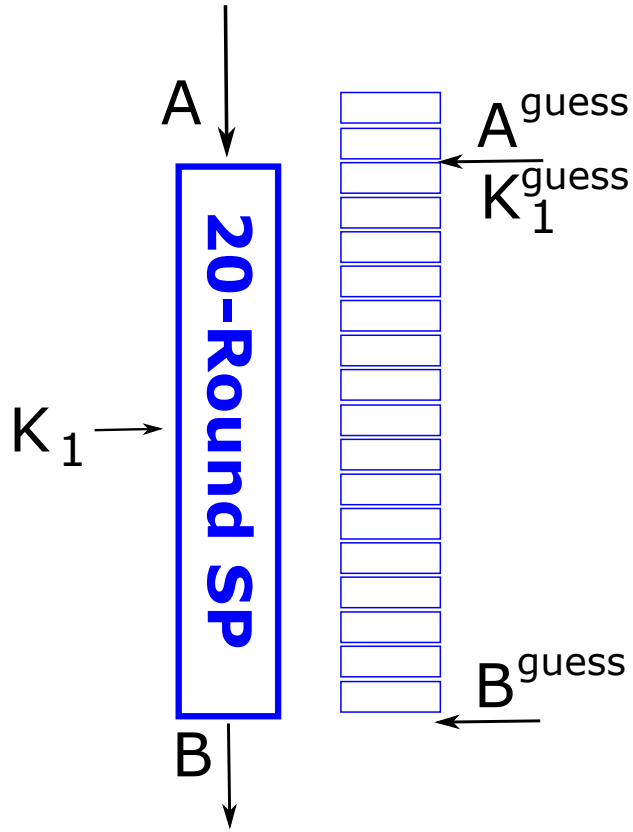
1. Take random A^{guess}, K_1^{guess}
2. Go 20 rounds, produce B^{guess}
3. Check if $A^{guess} \oplus B^{guess} = A \oplus B$
4. If yes, then candidate (stop, double check)
5. If not, shift by one round
6. Go 1 round, produce new B^{guess}
7. Go to step 3



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

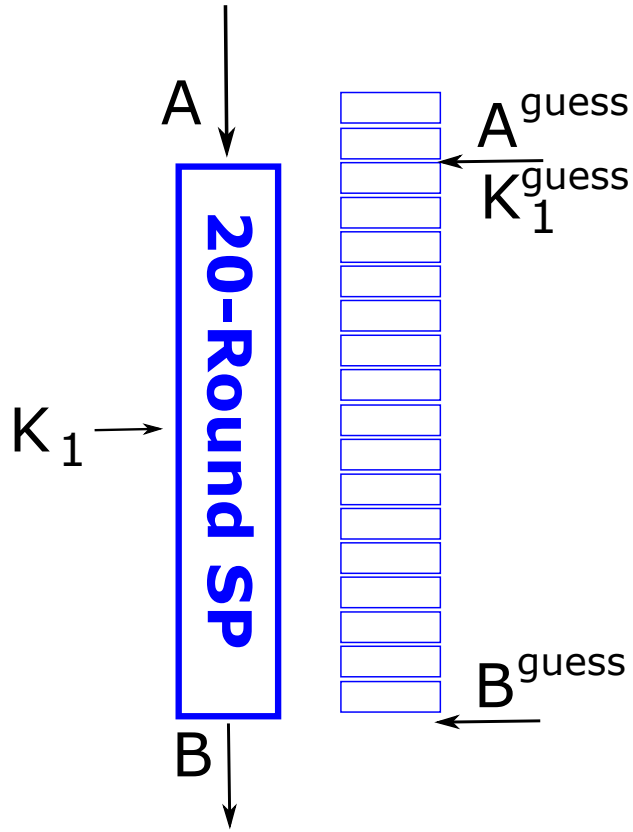
1. Take random A^{guess}, K_1^{guess}
2. Go 20 rounds, produce B^{guess}
3. Check if $A^{guess} \oplus B^{guess} = A \oplus B$
4. If yes, then candidate (stop, double check)
5. If not, shift by one round
6. Go 1 round, produce new B^{guess}
7. Go to step 3



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

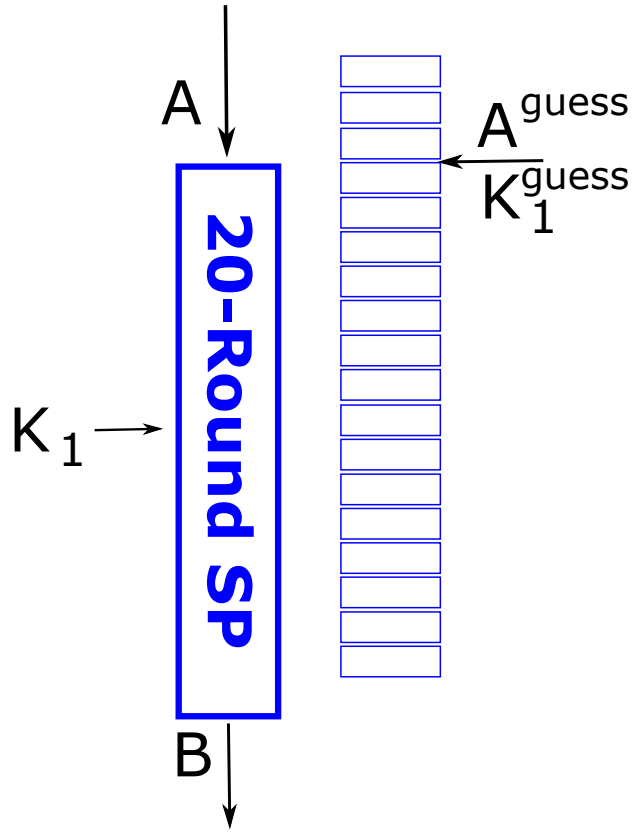
1. Take random A^{guess}, K_1^{guess}
2. Go 20 rounds, produce B^{guess}
3. Check if $A^{guess} \oplus B^{guess} = A \oplus B$
4. If yes, then candidate (stop, double check)
5. If not, shift by one round
6. Go 1 round, produce new B^{guess}
7. Go to step 3



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

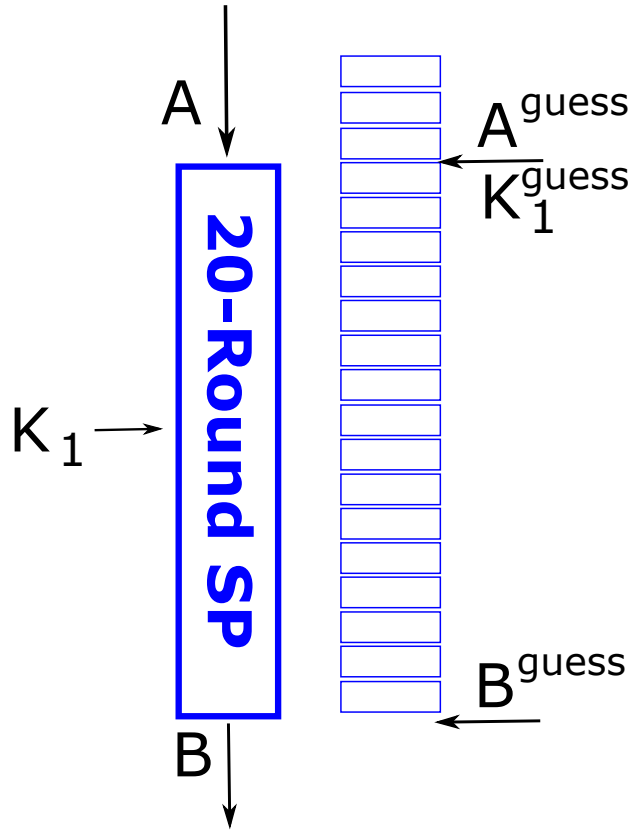
1. Take random A^{guess}, K_1^{guess}
2. Go 20 rounds, produce B^{guess}
3. Check if $A^{guess} \oplus B^{guess} = A \oplus B$
4. If yes, then candidate (stop, double check)
5. If not, shift by one round
6. Go 1 round, produce new B^{guess}
7. Go to step 3



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

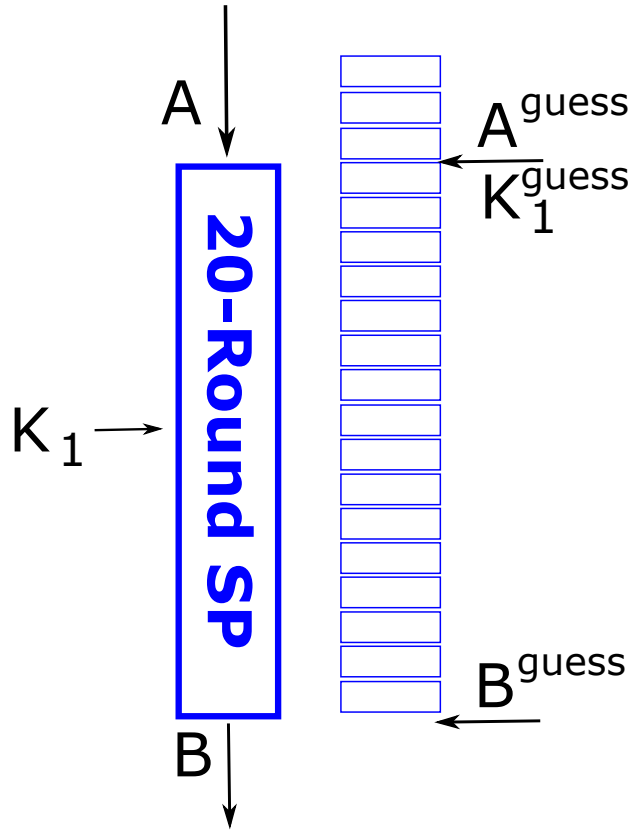
1. Take random A^{guess}, K_1^{guess}
2. Go 20 rounds, produce B^{guess}
3. Check if $A^{guess} \oplus B^{guess} = A \oplus B$
4. If yes, then candidate (stop, double check)
5. If not, shift by one round
6. Go 1 round, produce new B^{guess}
7. Go to step 3



Complete analysis

Given (P, C) produce $A \oplus B = P \oplus C$

1. Take random A^{guess}, K_1^{guess}
2. Go 20 rounds, produce B^{guess}
3. Check if $A^{guess} \oplus B^{guess} = A \oplus B$
4. If yes, then candidate (stop, double check)
5. If not, shift by one round
6. Go 1 round, produce new B^{guess}
7. Go to step 3



Main Point

- Obviously, only 1 round is required to get another candidate for (A, K_1).
- Time T instead of 2^{2n} becomes

$$T = 2^{2n}/20$$

- Sliding keys provide speed-up of 20

Conclusion

In PRIDE, in general, given D data, recovering K_0, K_1 requires

- $$D \cdot T \approx 2^{2n}/20$$
- $$D \cdot T_{rounds} \approx 2^{2n}$$
- More rounds, smaller bound ?!
- Tricks when the last round is different. Bound:

$$D \cdot T \approx 2^{2n}/10$$

NANYANG TECHNOLOGICAL UNIVERSITY