State-Recovery Attacks on Modified Ketje

Thomas Fuhr[1] María Naya-Plasencia[2] Yann Rotella[2]

[1]ANSSI, France

[2]Inria, France

FSE 2018 - March 5, 2018

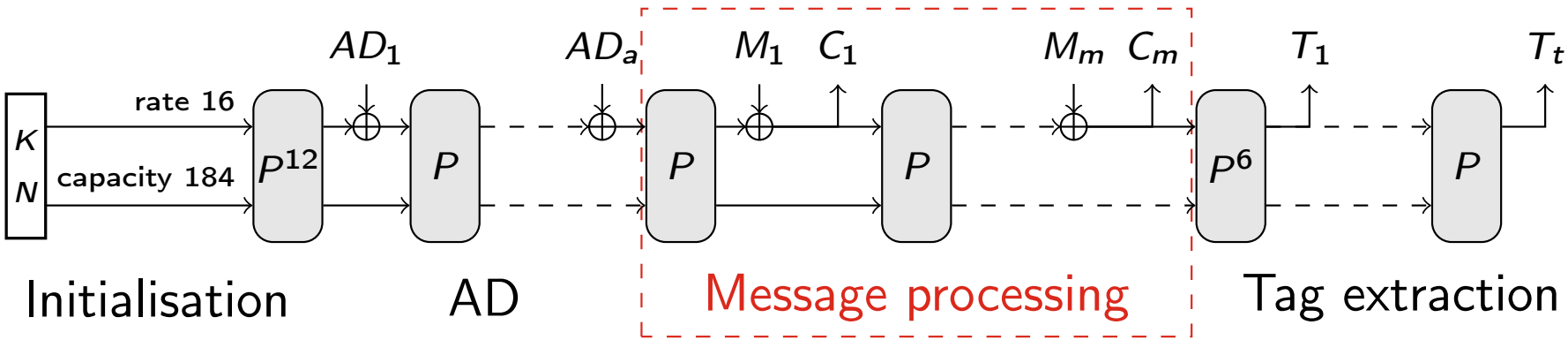
The Ketje family of AEAD

- Authenticated Encryption with Associated Data
- Third round candidate of the CAESAR competition
  - Designed by Bertoni, Daemen, Peeters, Van Assche, Van Keer
  - Ketje v1 (March 2014): selected for third round (15 candidates)
  - Ketje v2 (Sept. 2016): released at the beginning of third round
- 4 instances Ketje Jr, Ketje Sr, Ketje Minor, Ketje Major

The Ketje Jr. mode of operation

- MonkeyDuplex mode [BDPV12]
- Keccak permutation on a 200-bit state
- Claimed security level: 96 bits

$\mathcal{E}_K(N, AD, M)$



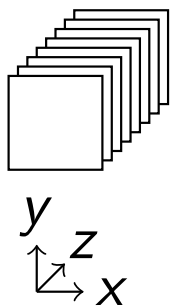
- Message processing: 1-round permutation

Our results

- Known-Plaintext State-Recovery Attack on modified Ketje Jr.
  - First analysis of the message processing phase
  - Ketje Jr. with increased rate (see Ketje cryptanalysis contest)
  - Ketje Jr. v2, rate 40: 2^{82} operations
  - Ketje Jr. v1, rate 40: 2^{72} operations
  - Ketje Jr. v1, rate 32: 2^{92} operations
- Trivial Key-Recovery Attack once a the state is known
- Related work
  - Analyses of the (Keccak) permutation **[BCC11]**, **[DGPW12]**, **[JN15]**
  - Attacks on the initialisation phase **[GLS16]**, **[DLWQ17]**
- No threat for recommended parameters

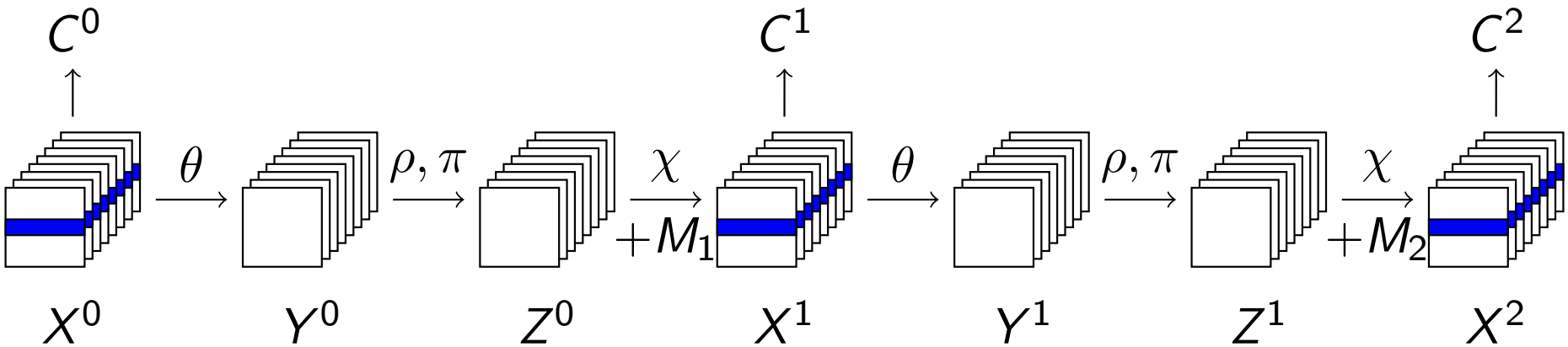
1. Message processing phase of Ketje Jr.

Ketje Jr v1, rate 40: processing 3 message blocks



- 200-bit state $\rightarrow 5 \times 5 \times 8$ array
- 1-round permutation based on Keccak
- Elementary operations $\theta, \rho, \pi, \chi, \iota$

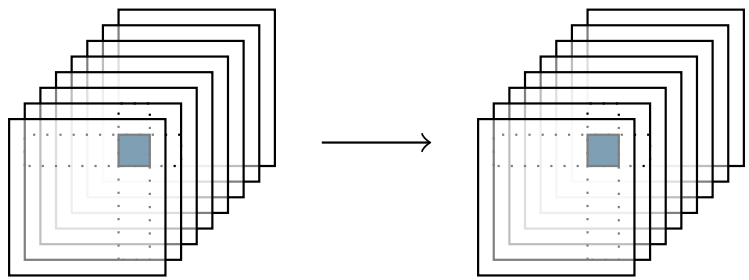
Ketje Jr v1, rate 40: processing 3 message blocks



- 200-bit state $\rightarrow 5 \times 5 \times 8$ array
- 1-round permutation based on Keccak
- Elementary operations $\theta, \rho, \pi, \chi, \iota$

Linear diffusion θ, ρ, π

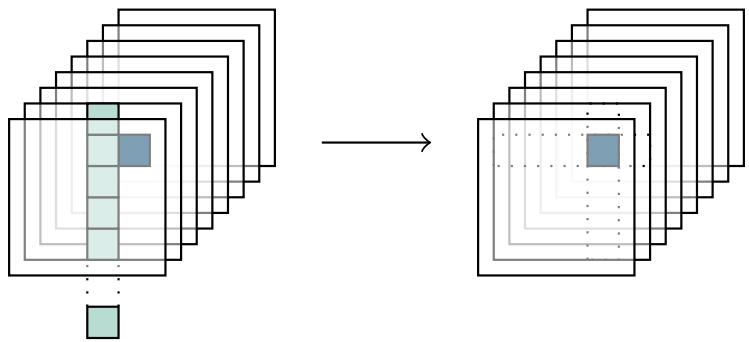
- θ: linear diffusion
  - Parity bits: sum of 5 bits of the same column
  - $P(S)_{x,z} = \sum_{y=0}^{4} S_{x,y,z}$
  - $S_{x,y,z} \leftarrow S_{x,y,z} + P(S)_{x-1,z} + P(S)_{x+1,z-1}$



- ρ, π: bit-shuffling operations

Linear diffusion θ, ρ, π

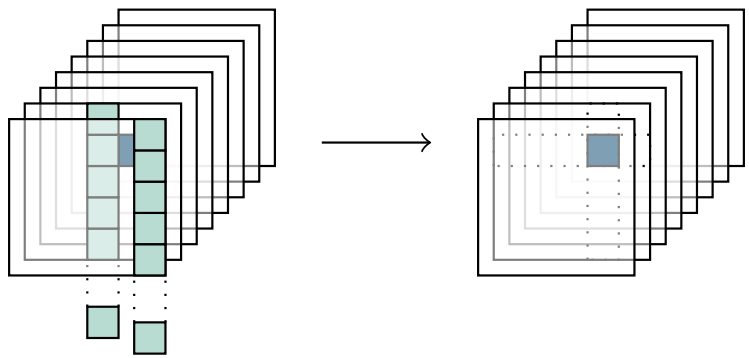
- θ: linear diffusion
  - Parity bits: sum of 5 bits of the same column
  - $P(S)_{x,z} = \sum_{y=0}^{4} S_{x,y,z}$
  - $S_{x,y,z} \leftarrow S_{x,y,z} + P(S)_{x-1,z} + P(S)_{x+1,z-1}$



- ρ, π: bit-shuffling operations

Linear diffusion θ, ρ, π

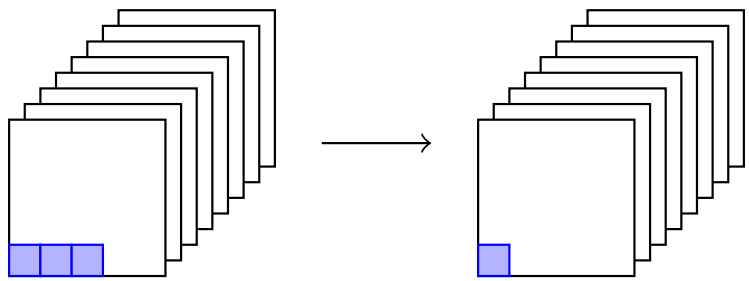
- θ: linear diffusion
  - Parity bits: sum of 5 bits of the same column
  - $P(S)_{x,z} = \sum_{y=0}^{4} S_{x,y,z}$
  - $S_{x,y,z} \leftarrow S_{x,y,z} + P(S)_{x-1,z} + P(S)_{x+1,z-1}$



- ρ, π: bit-shuffling operations

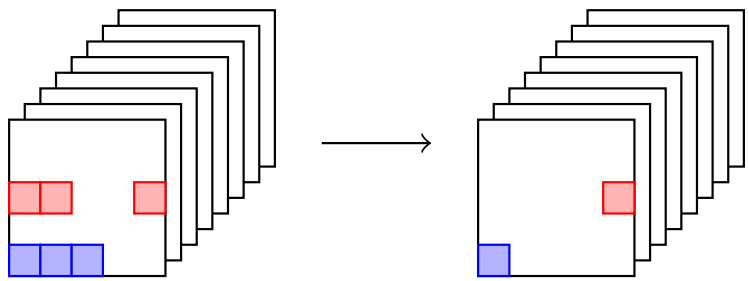
Nonlinear layer χ

- χ: row-wise substitution Layer
- S-Box of algebraic degree 2
- $S_{x,y,z} \leftarrow S_{x,y,z} + \overline{S_{x+1,y,z}} S_{x+2,y,z}$



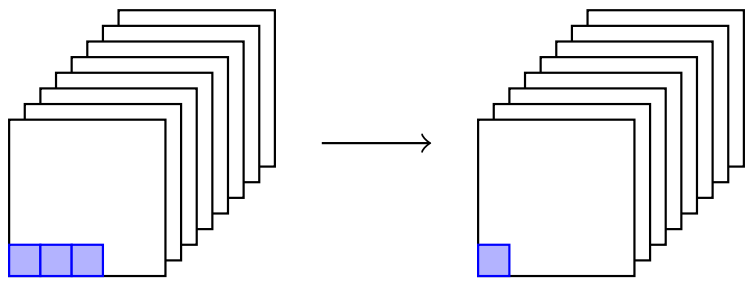
Nonlinear layer χ

- χ: row-wise substitution Layer
- S-Box of algebraic degree 2
- $S_{x,y,z} \leftarrow S_{x,y,z} + \overline{S_{x+1,y,z}} S_{x+2,y,z}$



Nonlinear layer χ

- χ: row-wise substitution Layer
- S-Box of algebraic degree 2
- $S_{x,y,z} \leftarrow S_{x,y,z} + \overline{S_{x+1,y,z}} S_{x+2,y,z}$



- ι: addition of constants (omitted in the following)

2. Divide-and-conquer attacks

Solving systems of equations

Generic problem

- Given $F : \{0,1\}^{N_u+N_v} \rightarrow \{0,1\}^c$
- Find all (u, v) in $\{0,1\}^{N_u+N_v}$ s.t. $f(u, v) = 0$
- Exhaustive search with complexity $2^{N_u+N_v}$

Subcase $f(u, v) = f_U(u) + f_V(v)$

- Equations become $f_U(u) = f_V(v)$
- Solution by divide-and-conquer technique

A folklore cryptographic technique

A well known divide-and-conquer solution

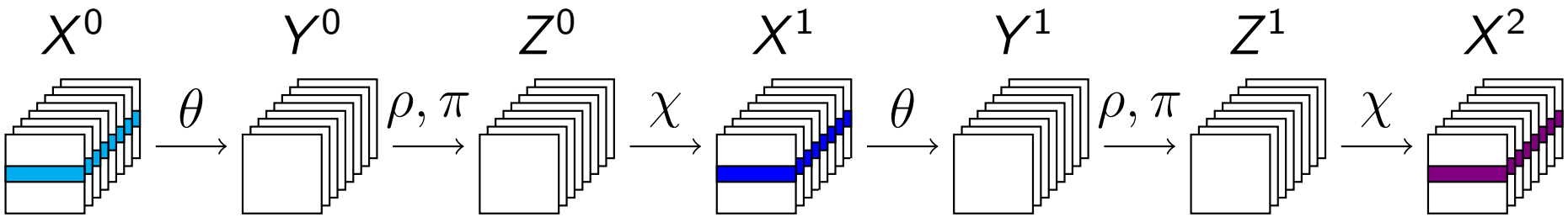
- Compute $f_U(u)$ for all u and build a sorted list of $(f_U(u), u)$
- Compute $f_V(v)$ for all v and build a sorted list of $(f_V(v), v)$
- Find matches by simultaneously searching both lists

- Complexity $2^{N_u} + 2^{N_v}$ (building lists) + $2^{N_u+N_v-c}$ (number of solutions)

Our attack strategy

- At least $\frac{200-96}{r}$ plaintext blocks needed to break the 96-bit security bounds for rate r
- Core of the attack: divide-and-conquer technique
- Express known bit values as $f_U(u) + f_V(v)$
- Preliminary guess-and-determine step to reduce nonlinear effects
- Partial inversion of S-Boxes with partially known output

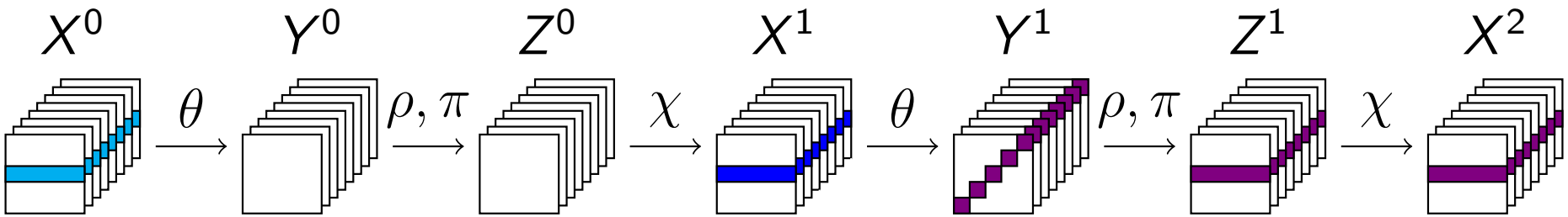
D&C attack on 3 blocks – Ketje Jr v1, rate 40



Known bits

- Application of the divide-and-conquer algorithm

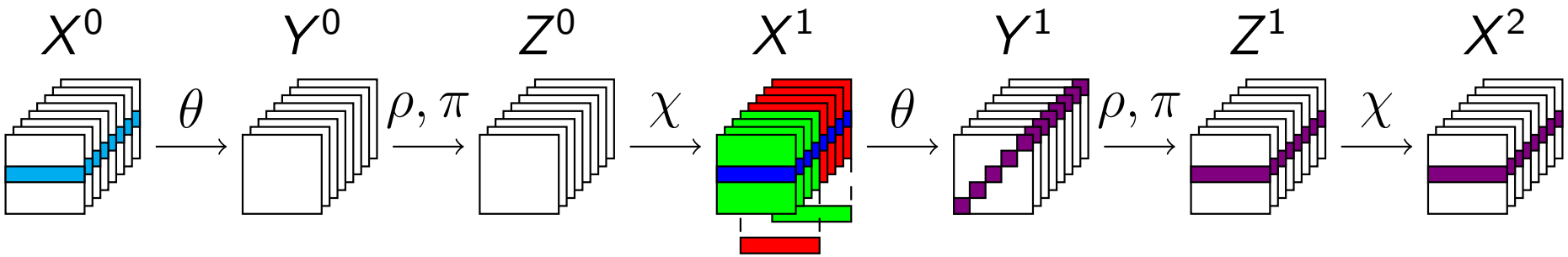
D&C attack on 3 blocks – Ketje Jr v1, rate 40



Known bits

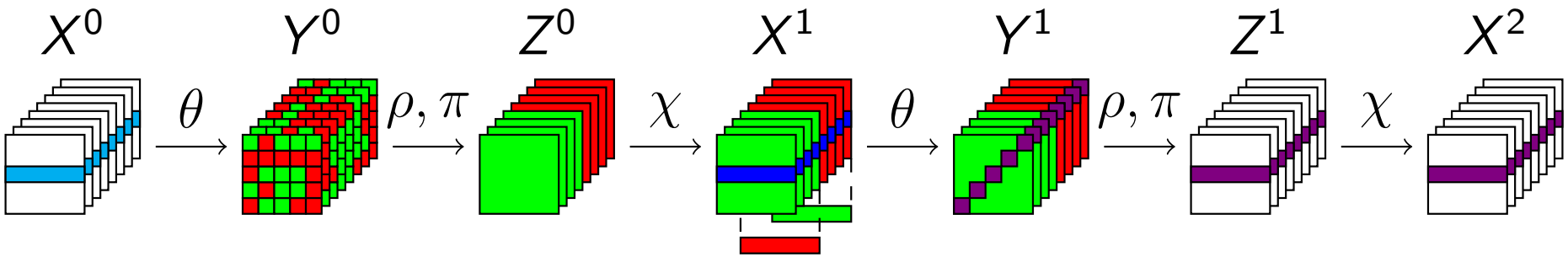
- Application of the divide-and-conquer algorithm

D&C attack on 3 blocks – Ketje Jr v1, rate 40



- Application of the divide-and-conquer algorithm
- u: front half of X^1 and 5 parity bits
- v: back half of X^1 and 5 parity bits

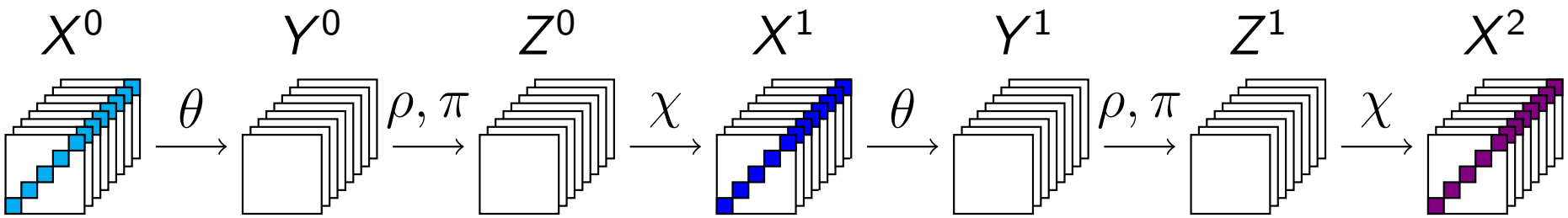
D&C attack on 3 blocks – Ketje Jr v1, rate 40



- Application of the divide-and-conquer algorithm
- u: front half of X^1 and 5 parity bits
- v: back half of X^1 and 5 parity bits

- $N_u = N_v = 2^{100+5-20-20} = 2^{65}$
- Sieving equations $c = 40 + 10 = 50$ (X^0 and parity bits)
- Complexity $2^{66} + 2^{80}$

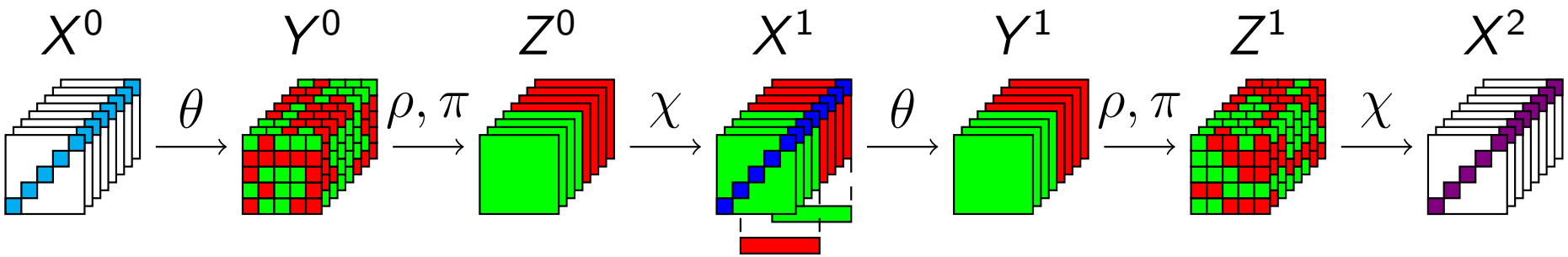
D&C attack on 3 blocks – Ketje Jr v2, rate 40



Known bits

- Output on diagonals $\Rightarrow$ No inversion of χ

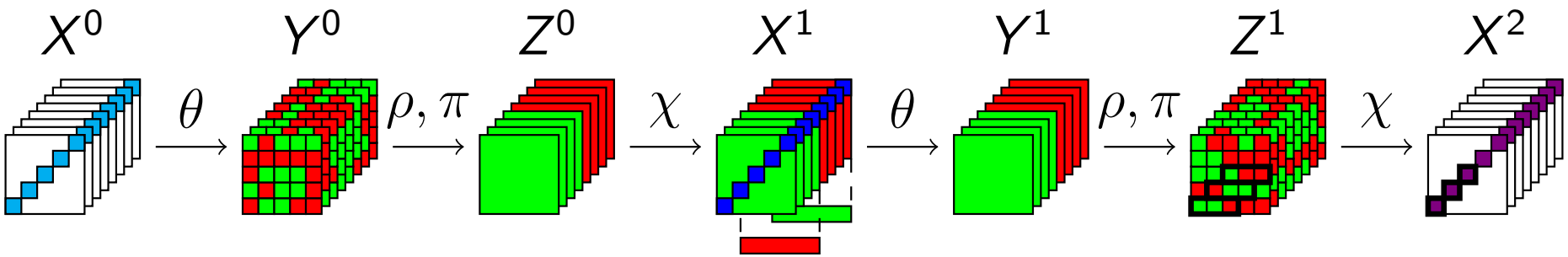
D&C attack on 3 blocks – Ketje Jr v2, rate 40



Known bits Bits of u Bits of v

- Output on diagonals $\Rightarrow$ No inversion of χ
- How can we sieve through χ ?

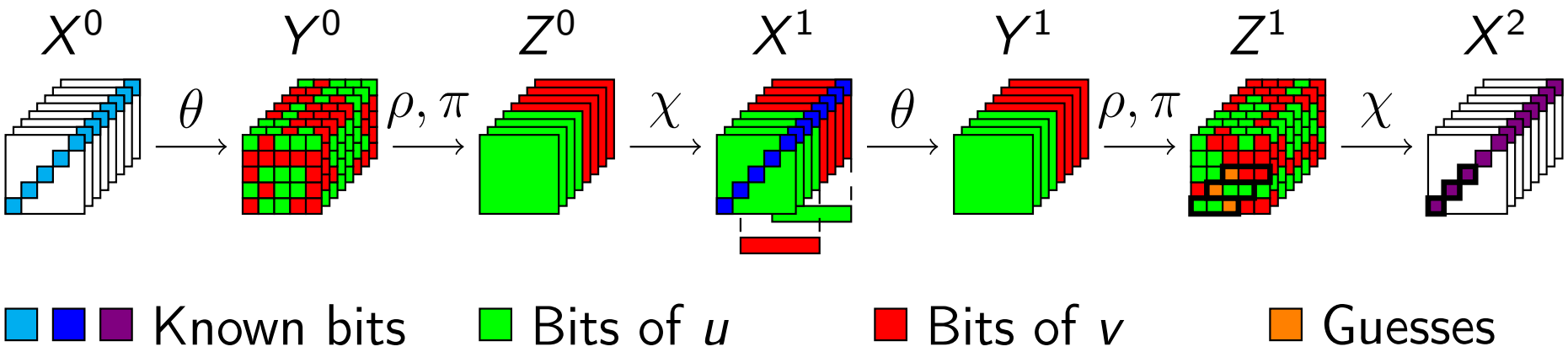
D&C attack on 3 blocks – Ketje Jr v2, rate 40



Known bits Bits of u Bits of v

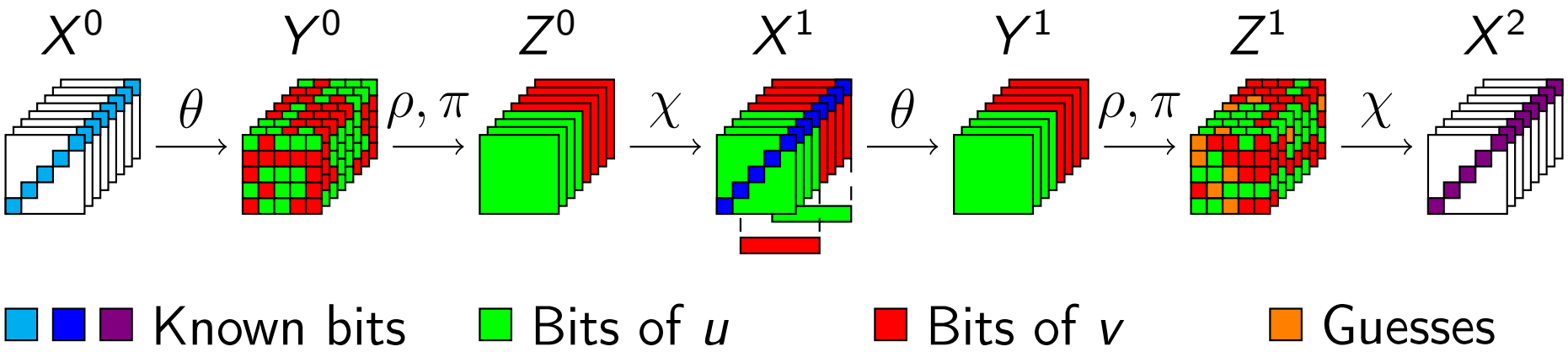
- Output on diagonals $\Rightarrow$ No inversion of χ
- How can we sieve through χ ?
- $X^2_{x,y,z} = Z^1_{x,y,z} + \overline{Z^1_{x+1,y,z}} Z^1_{x+2,y,z}$

D&C attack on 3 blocks – Ketje Jr v2, rate 40



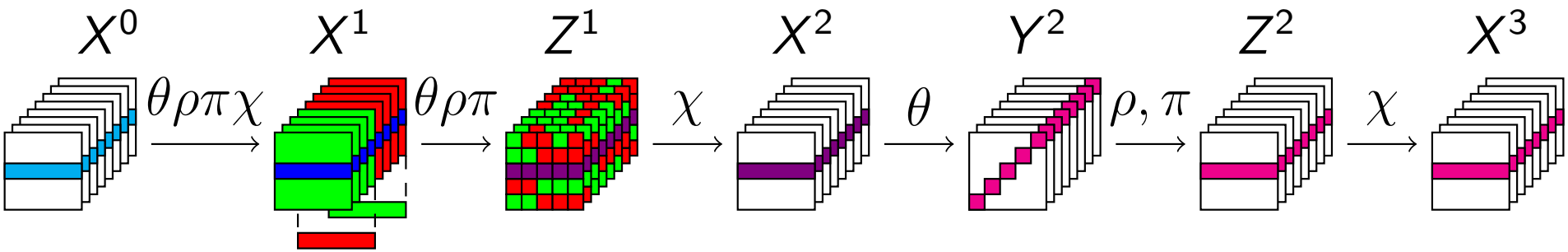
- Output on diagonals $\Rightarrow$ No inversion of χ
- How can we sieve through χ ?
- $X^2_{x,y,z} = Z^1_{x,y,z} + \overline{Z^1_{x+1,y,z}} Z^1_{x+2,y,z}$
- Preliminary guesses of minority bits

D&C attack on 3 blocks – Ketje Jr v2, rate 40



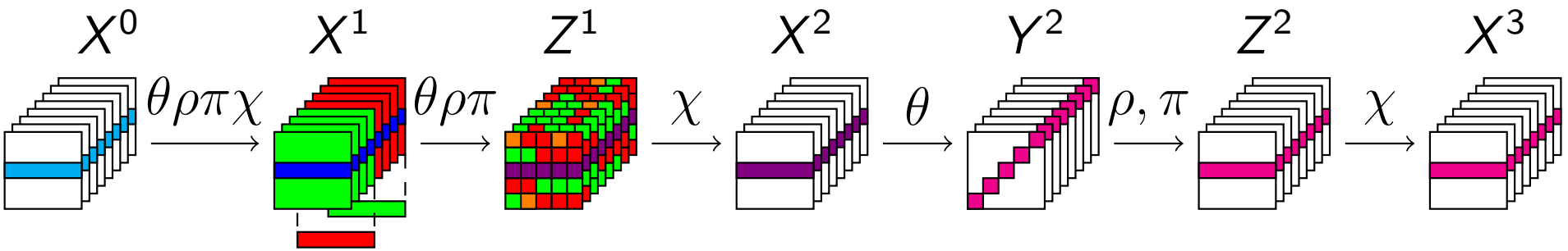
- Output on diagonals $\Rightarrow$ No inversion of χ
- How can we sieve through χ ?
- $X^2_{x,y,z} = Z^1_{x,y,z} + \overline{Z^1_{x+1,y,z}} Z^1_{x+2,y,z}$
- Preliminary guesses of minority bits
- Complexity $2^{32}(2 \times 2^{105-20-16-20}) + 2^{80} \approx 2^{82}$

Exploiting a 4^{th} block – Ketje Jr v1, rate 40



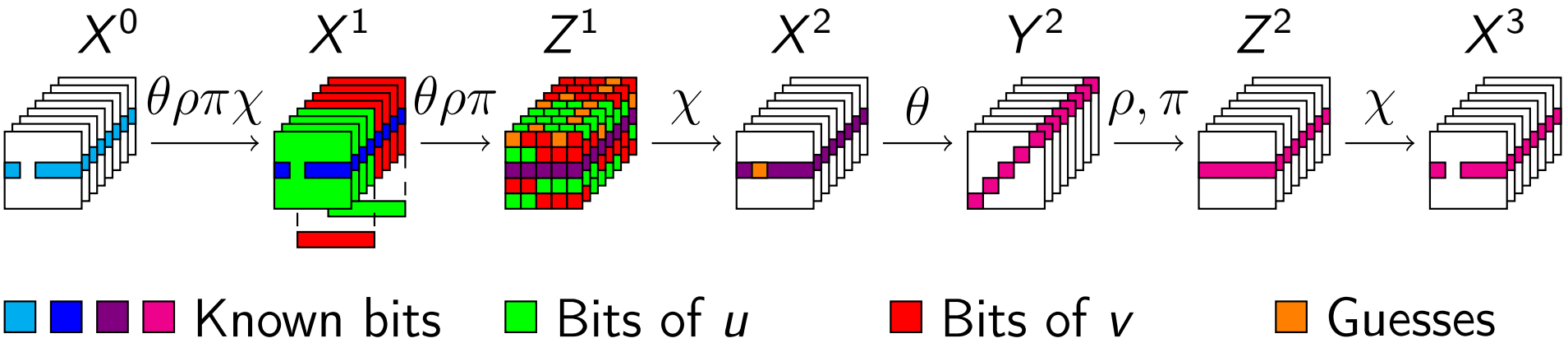
- Sieving relations from Y^2 ?
  - Y^2 depends on $Z^1_{x+1,y,z} Z^1_{x+2,y,z}$

Exploiting a 4^{th} block – Ketje Jr v1, rate 40



- Sieving relations from Y^2 ?
  - Y^2 depends on $Z^1_{x+1,y,z} Z^1_{x+2,y,z}$
- Solution by combining two ideas
  - Preliminary guesses of 11 bits of Z^1
  - Considering 10 linear combinations of known bits of Y^2
- Complexity $2^{11}(2^{59} + 2^{60}) + 2^{80-10} \approx 2^{72}$

D&C Attack – Ketje Jr v1, rate 32



- Using information from X^3
  - 8 S-Boxes with 4 out of 5 known output bits
  - $8 \times 4 = 32$ independent known linear relations on Y^2
- Same solution with 20 guesses and 12 linear combinations
- Complexity $2^{28}(2 \times 2^{59}) + 2^{92} \approx 2^{92}$

3. Conclusion

Conclusion

- First attacks on the message processing of weakened variants of Ketje
- No real threat against Ketje with recommended parameters
  - Rate 24: no linear relations on inputs of χ
  - Ketje Jr. v2, rate 32: wound require one more known output
  - Large memory requirements
- Modification between v1 and v2 increases security

Thank you for your attention