Truncated Differential Cryptanalysis of Five Rounds of Salsa20

Paul Crowley

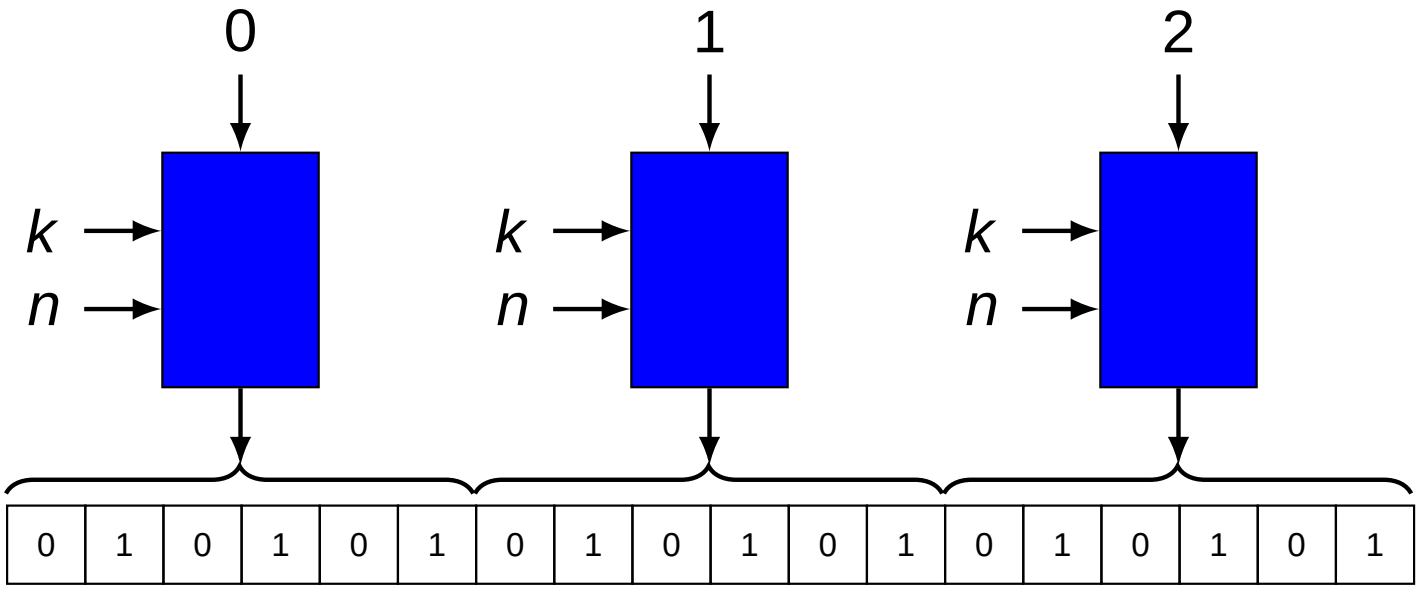
LShift Ltd

State of the Art in Stream Ciphers 2006

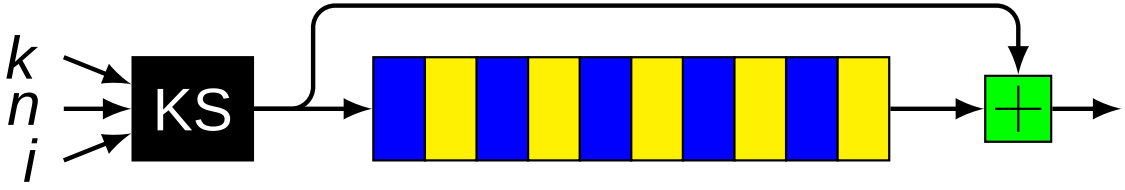
Salsa20

- eSTREAM entrant by Daniel J Bernstein
- Block-cipher-like structure
- 20 rounds, 256-bit key
- 5 round key recovery needs 4096 bytes and 2^{165} work

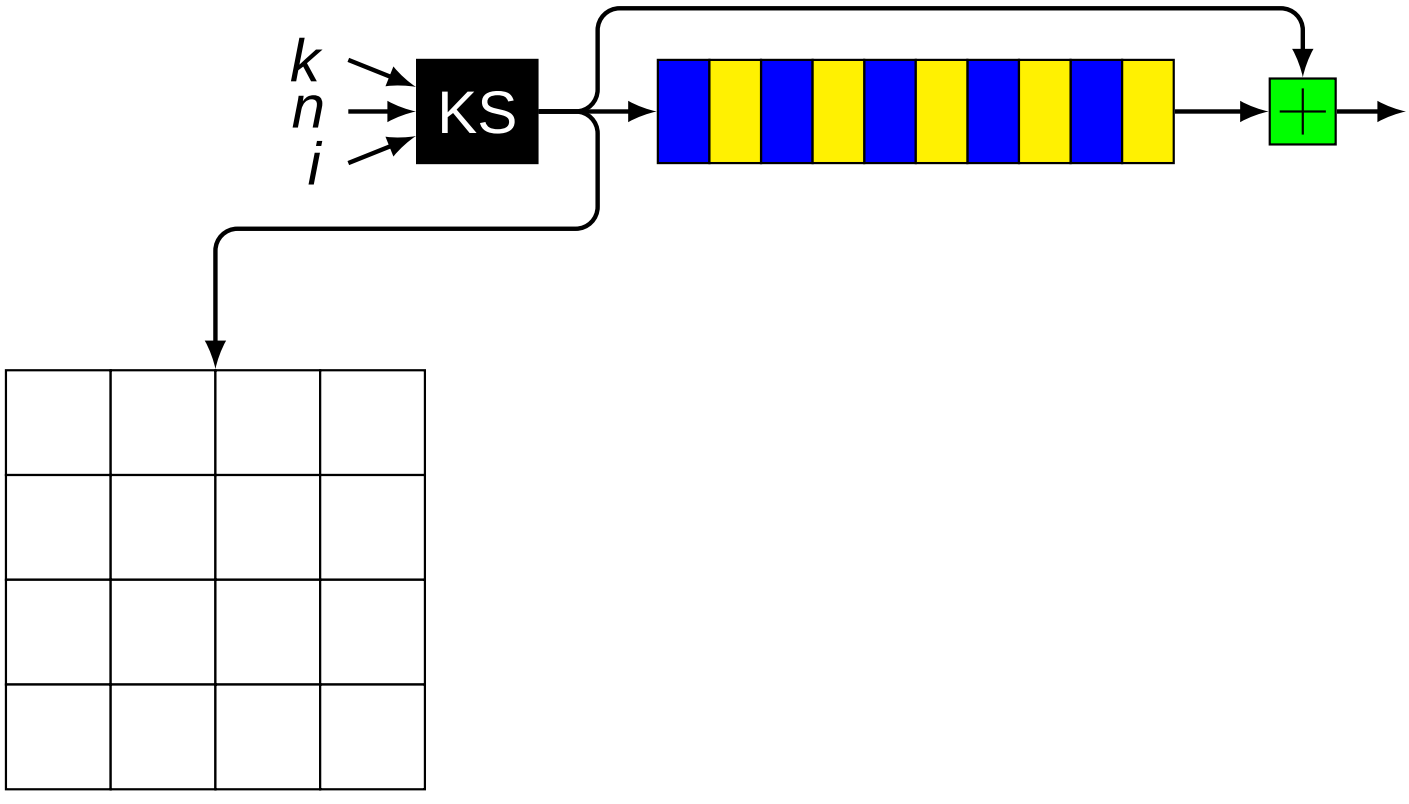
Seekable output



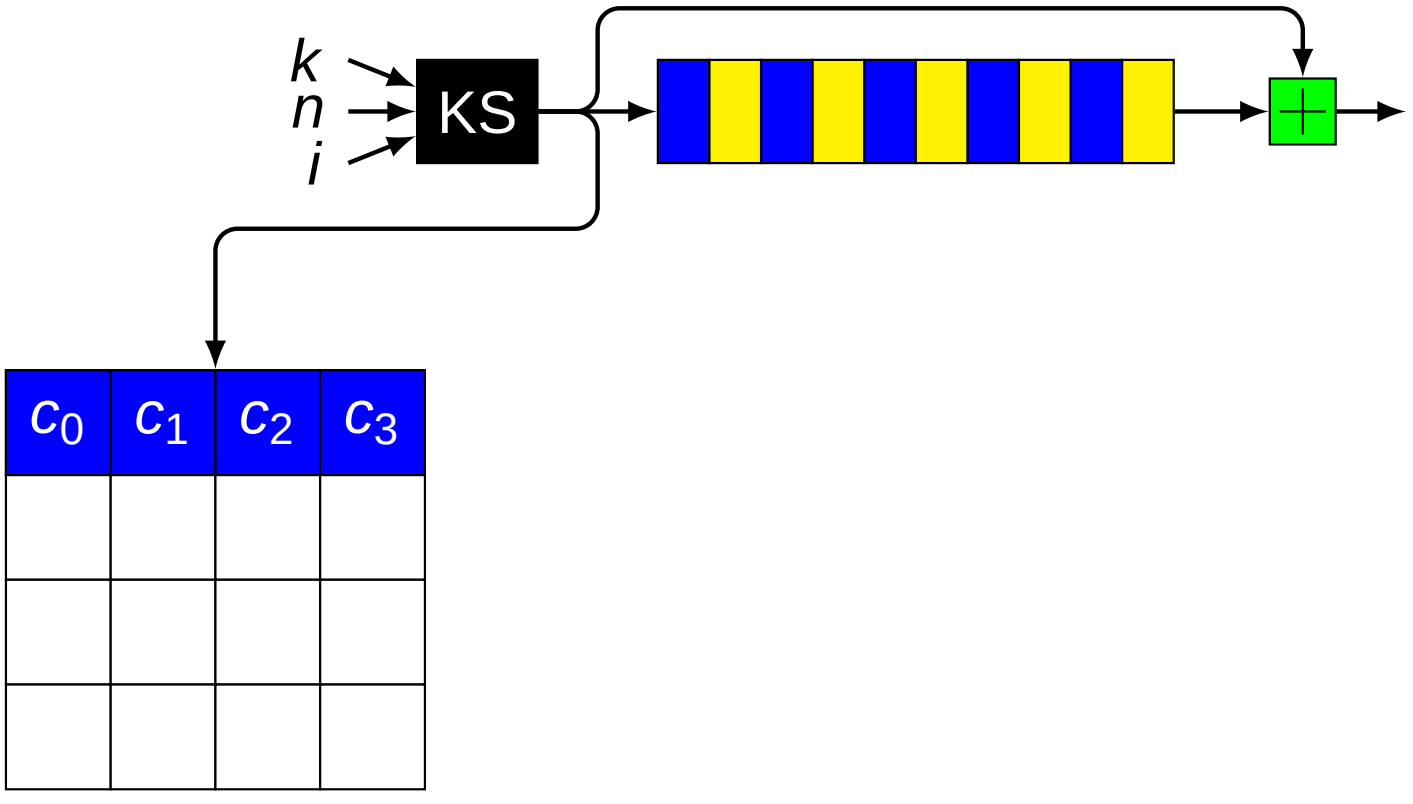
PRF



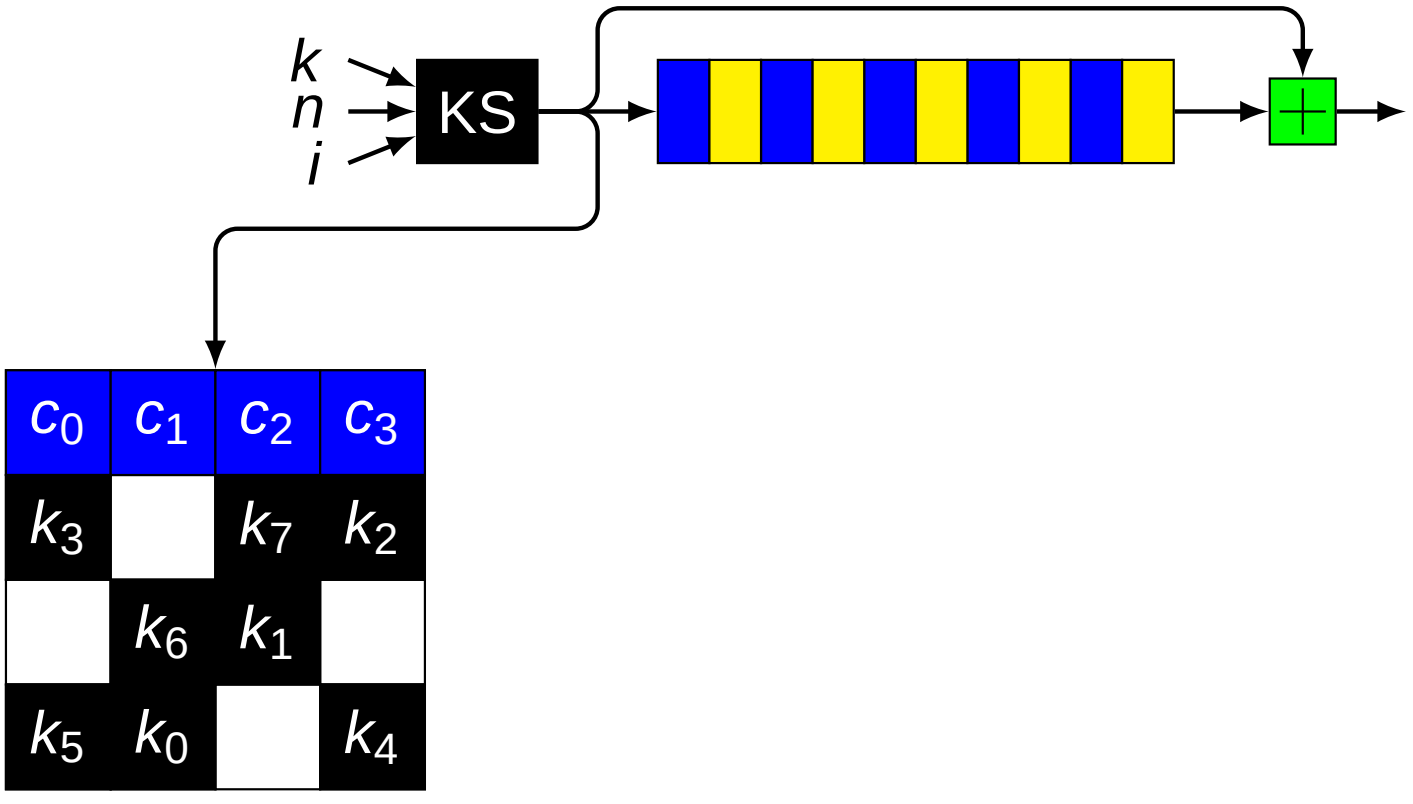
Key schedule



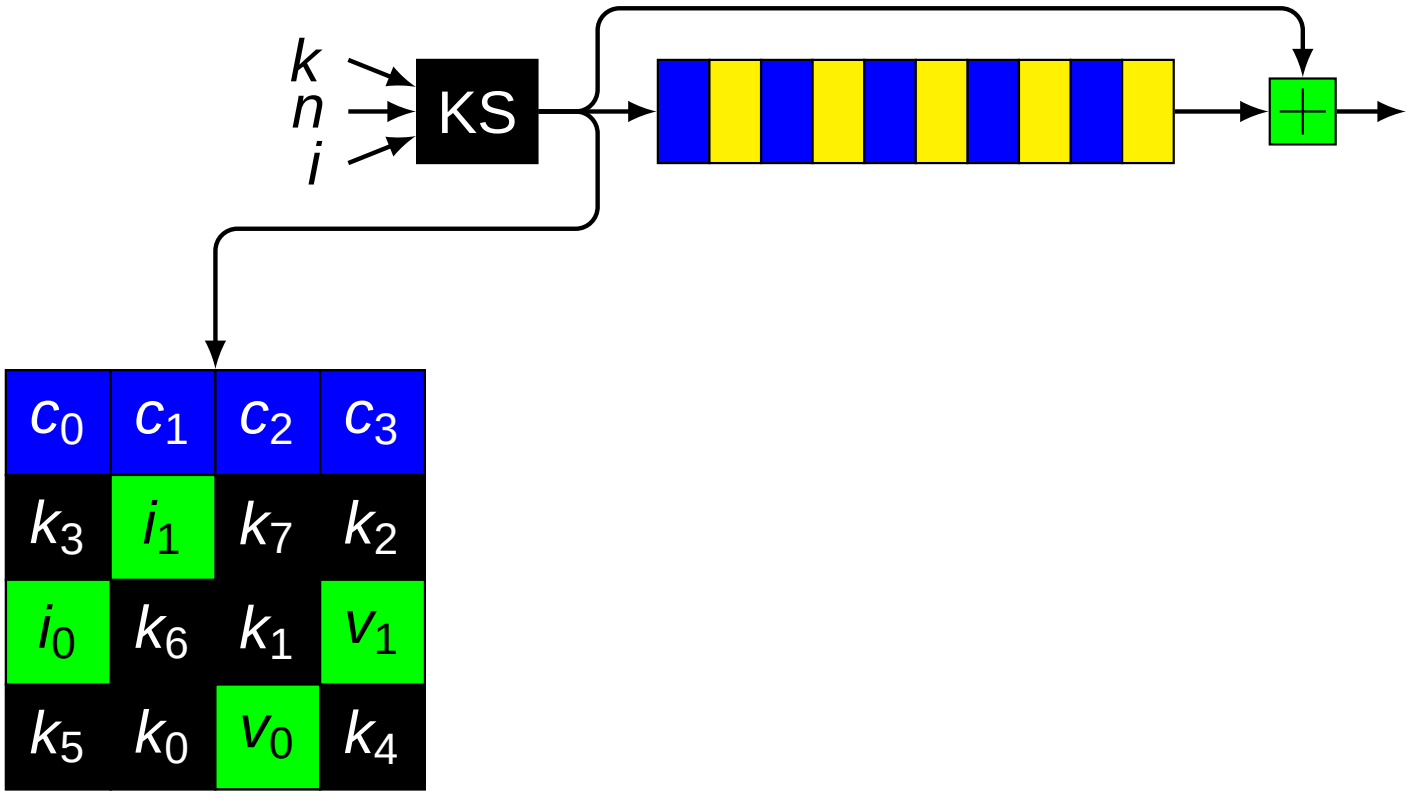
Key schedule



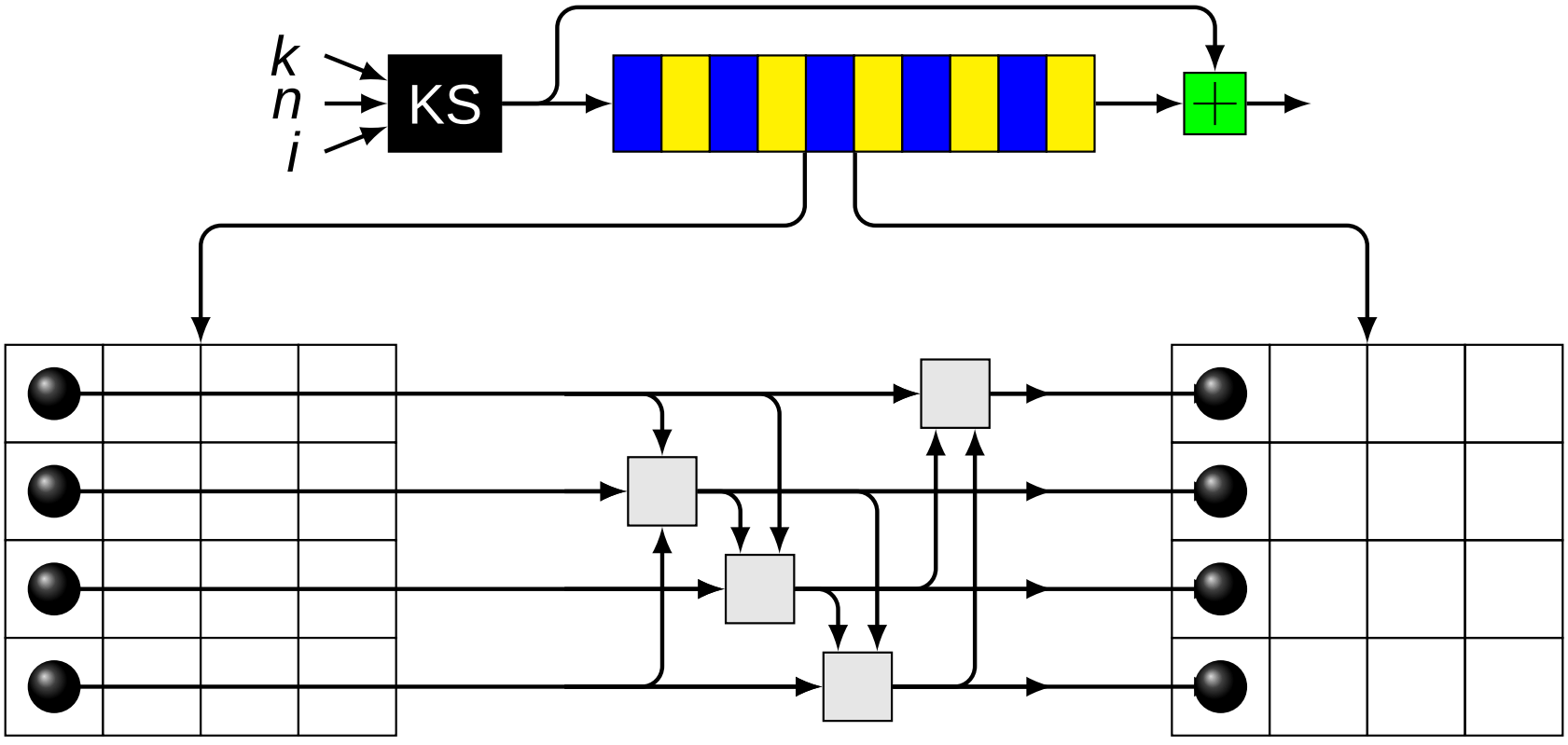
Key schedule



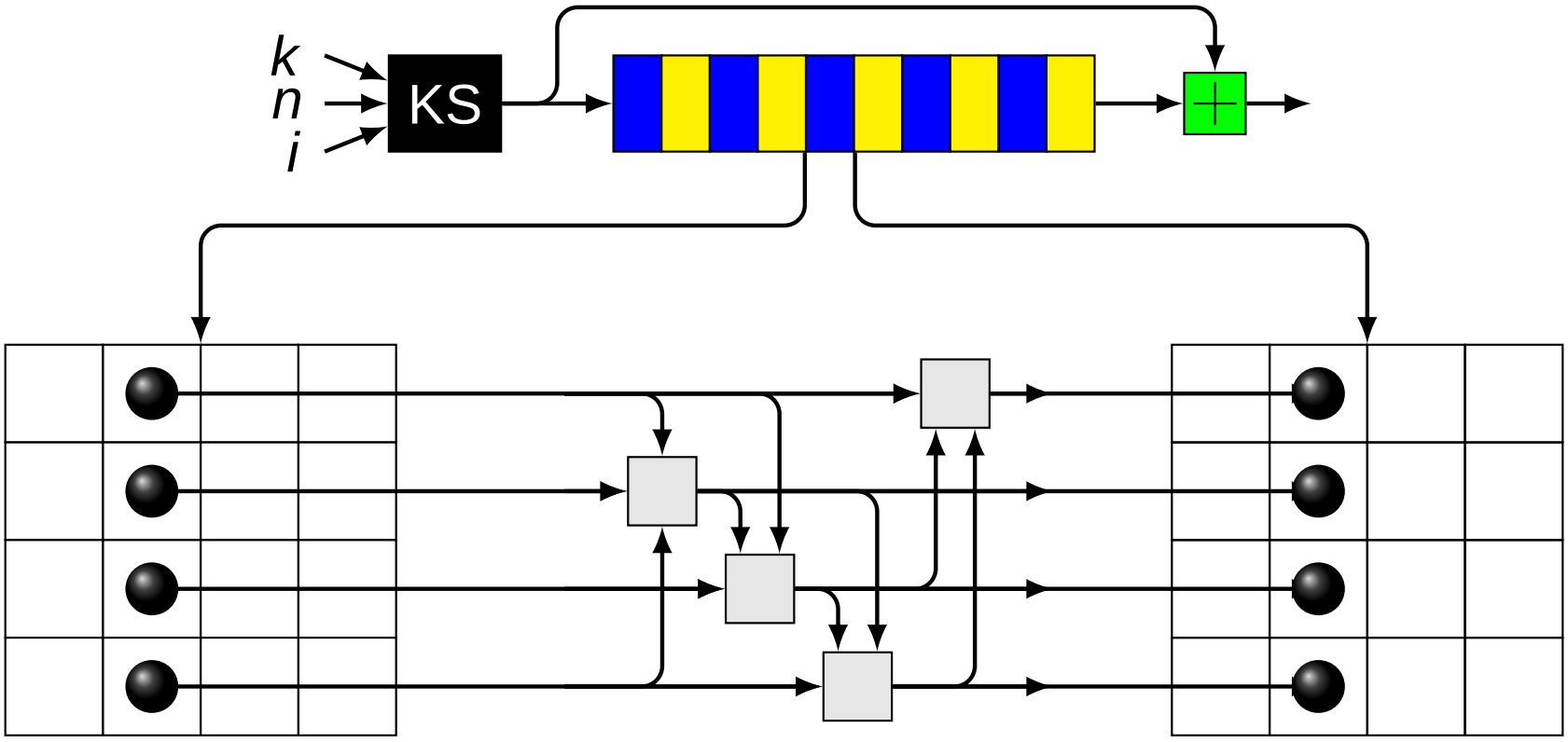
Key schedule



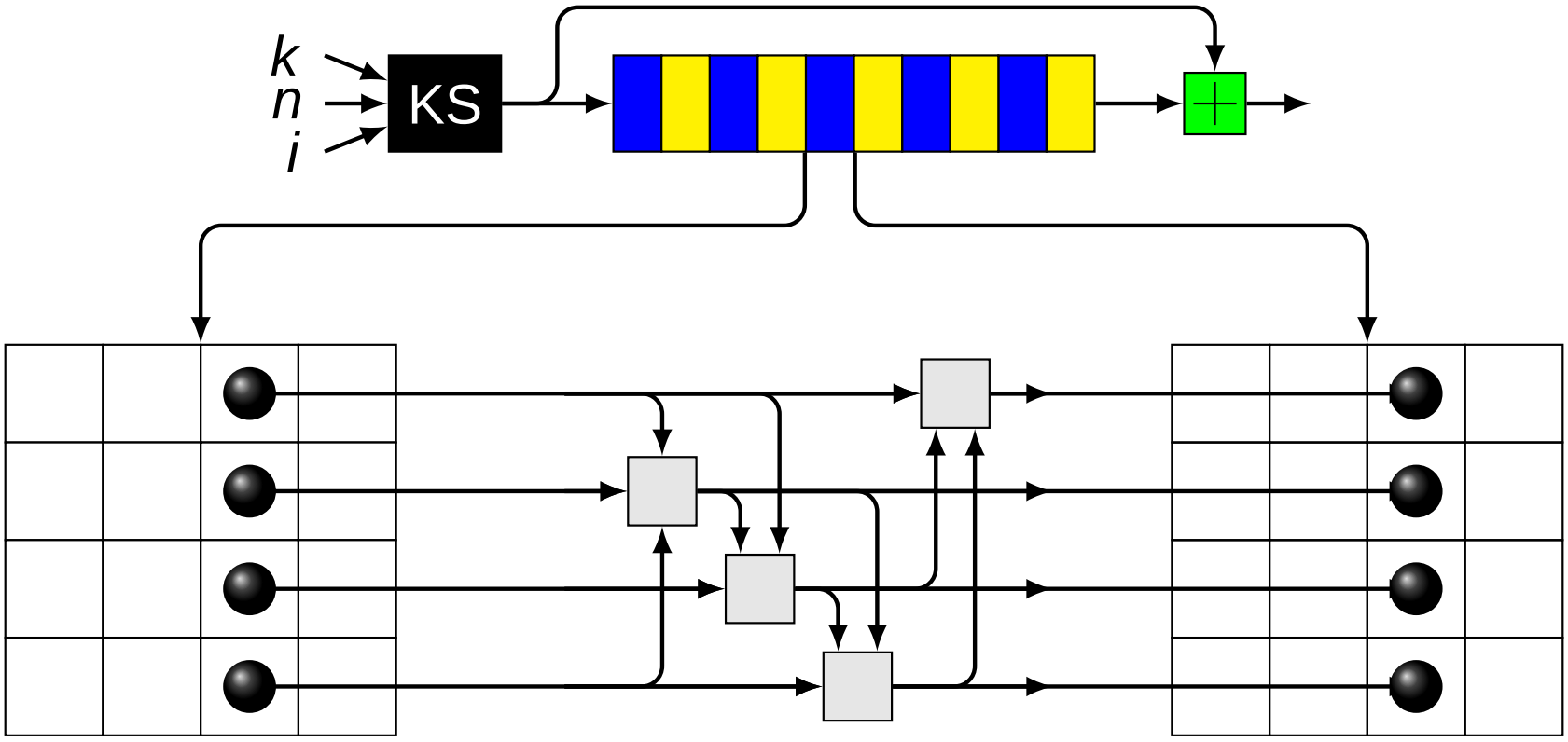
Mixing



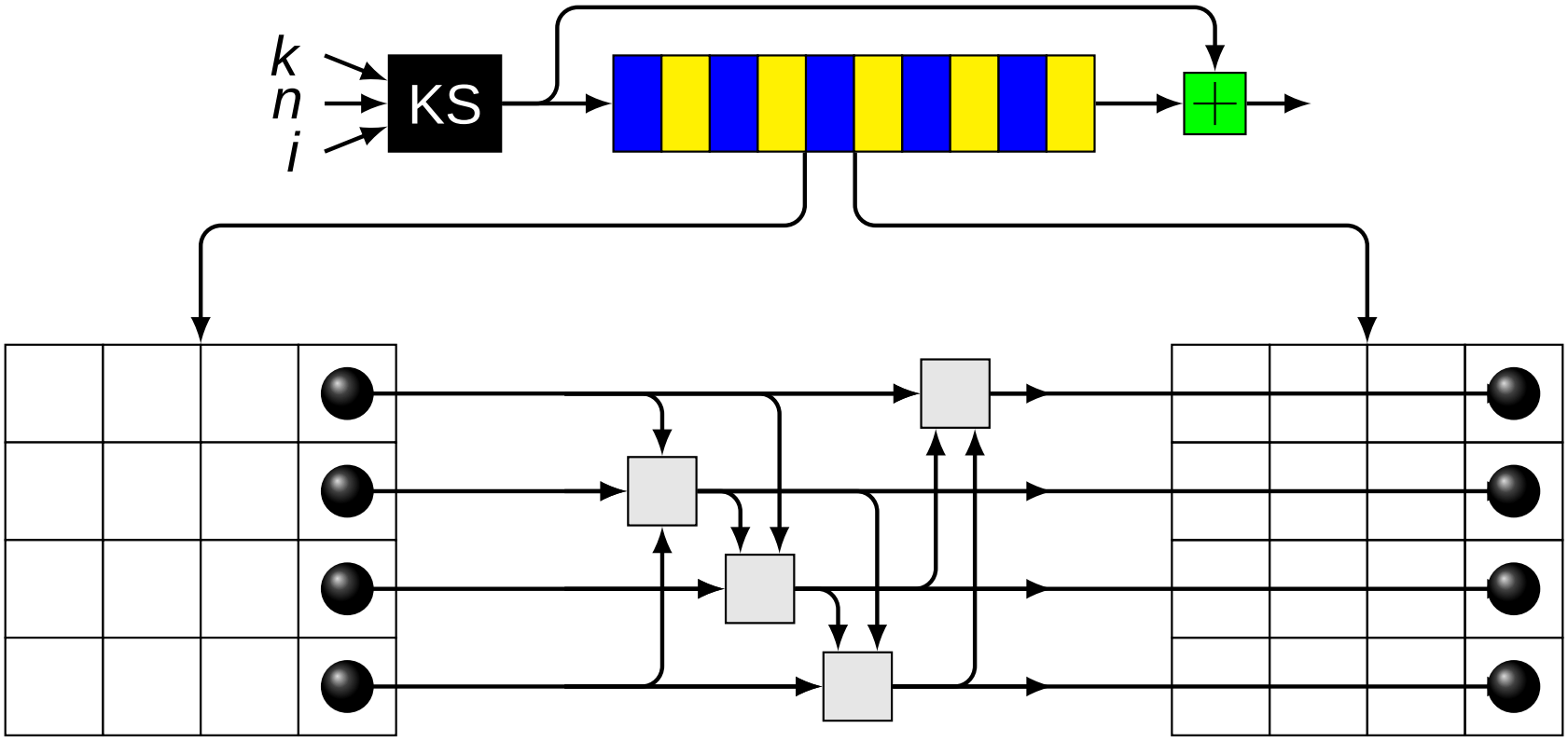
Mixing



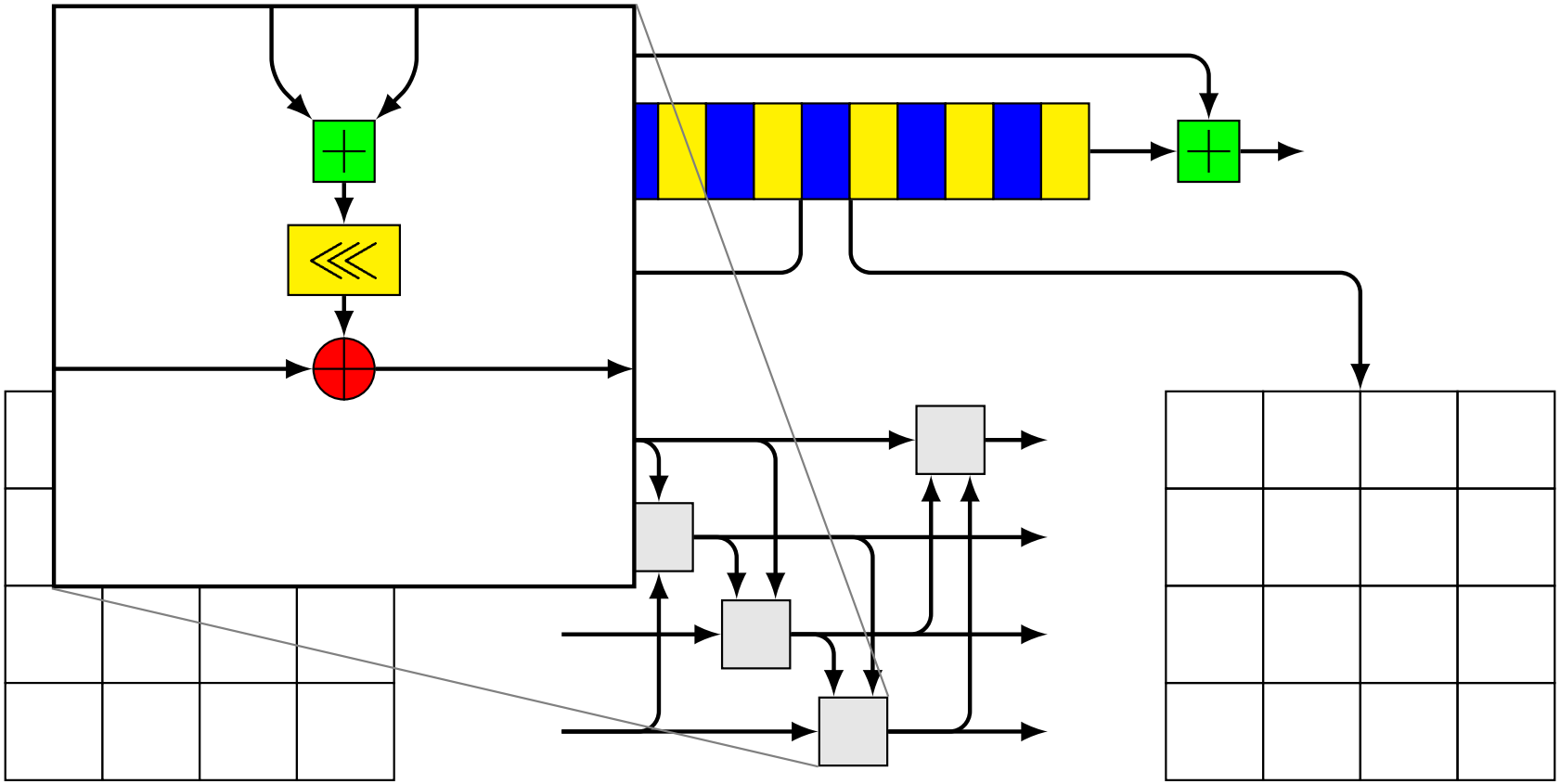
Mixing



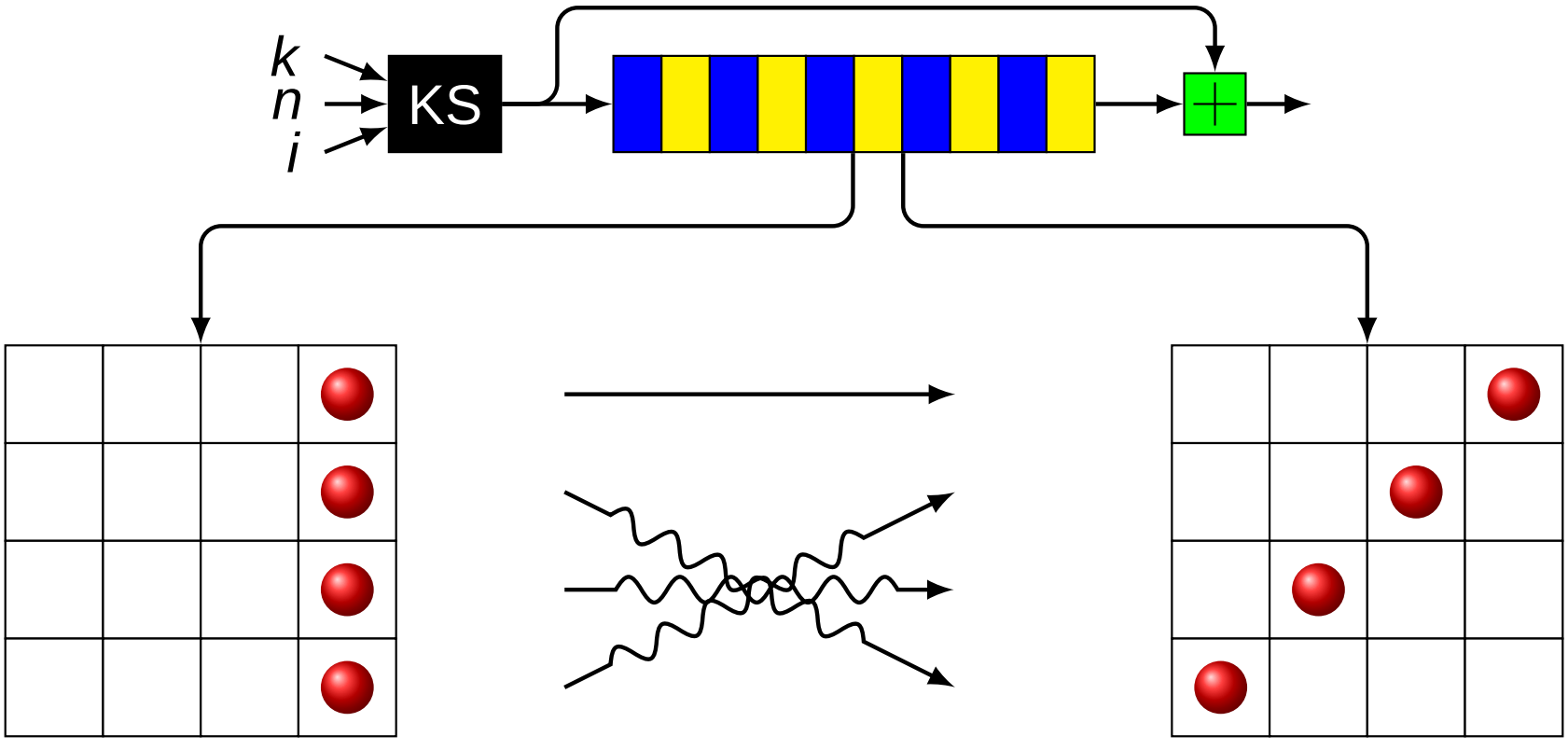
Mixing



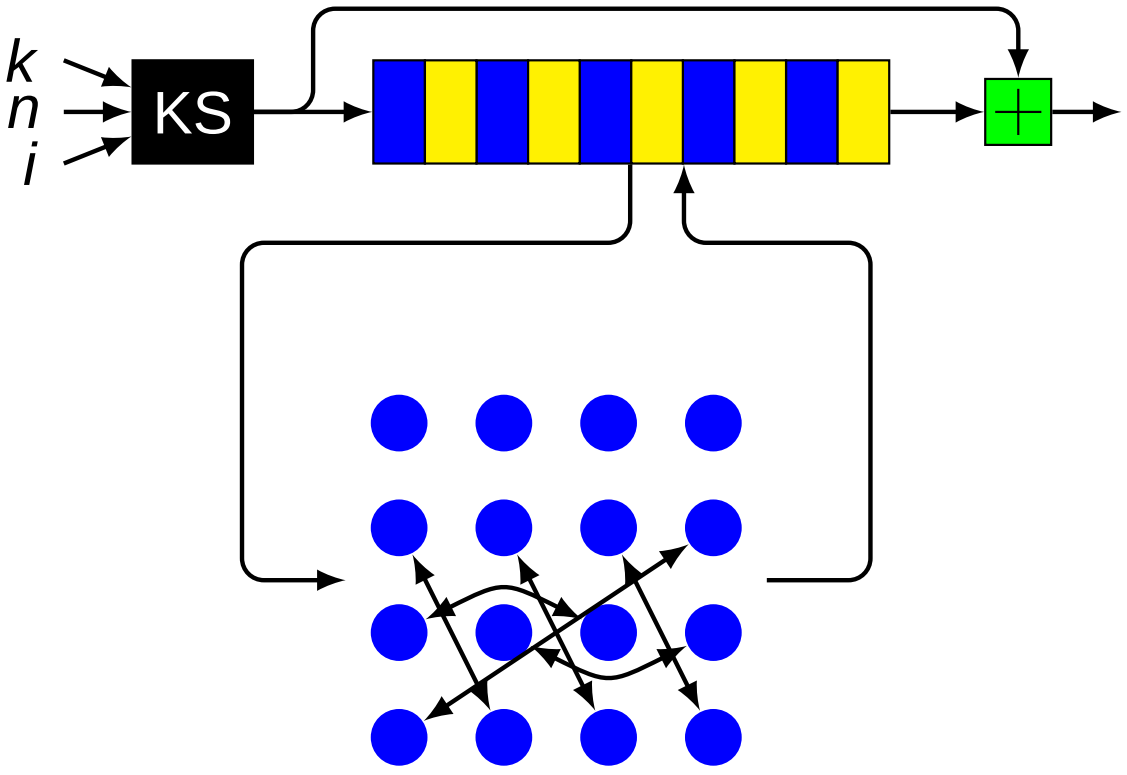
Mixing



Shuffling



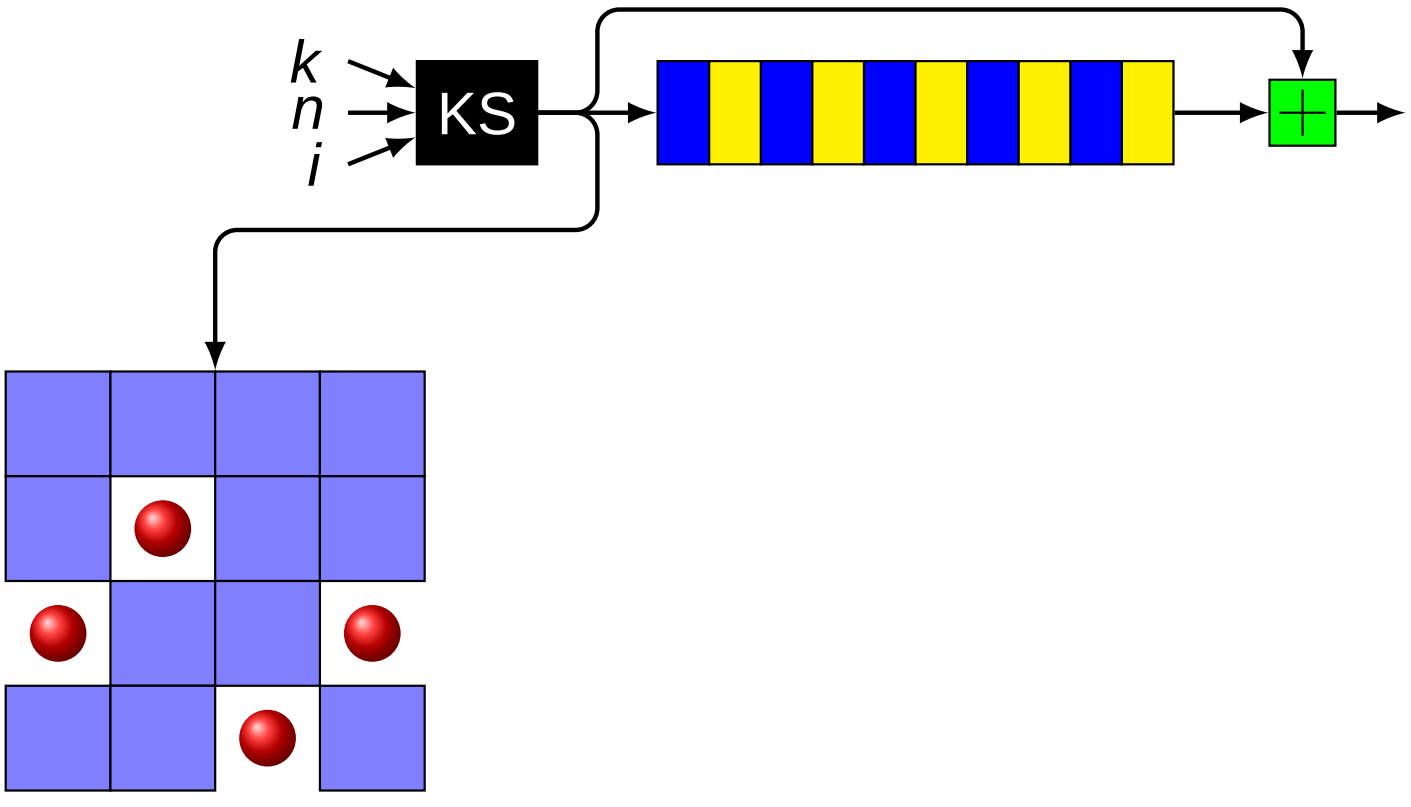
Shuffling



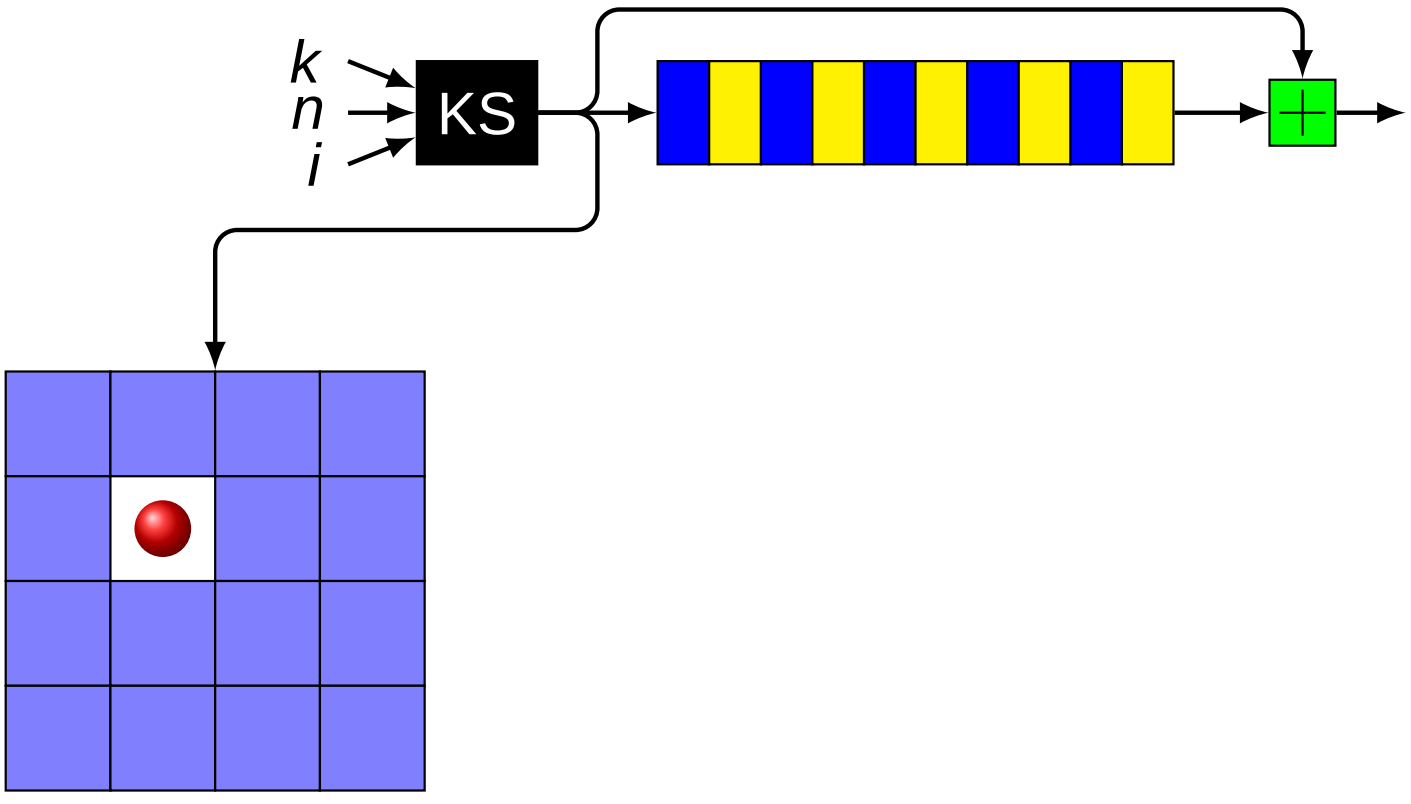
Our attack

- Differential attack
- Truncated differentials

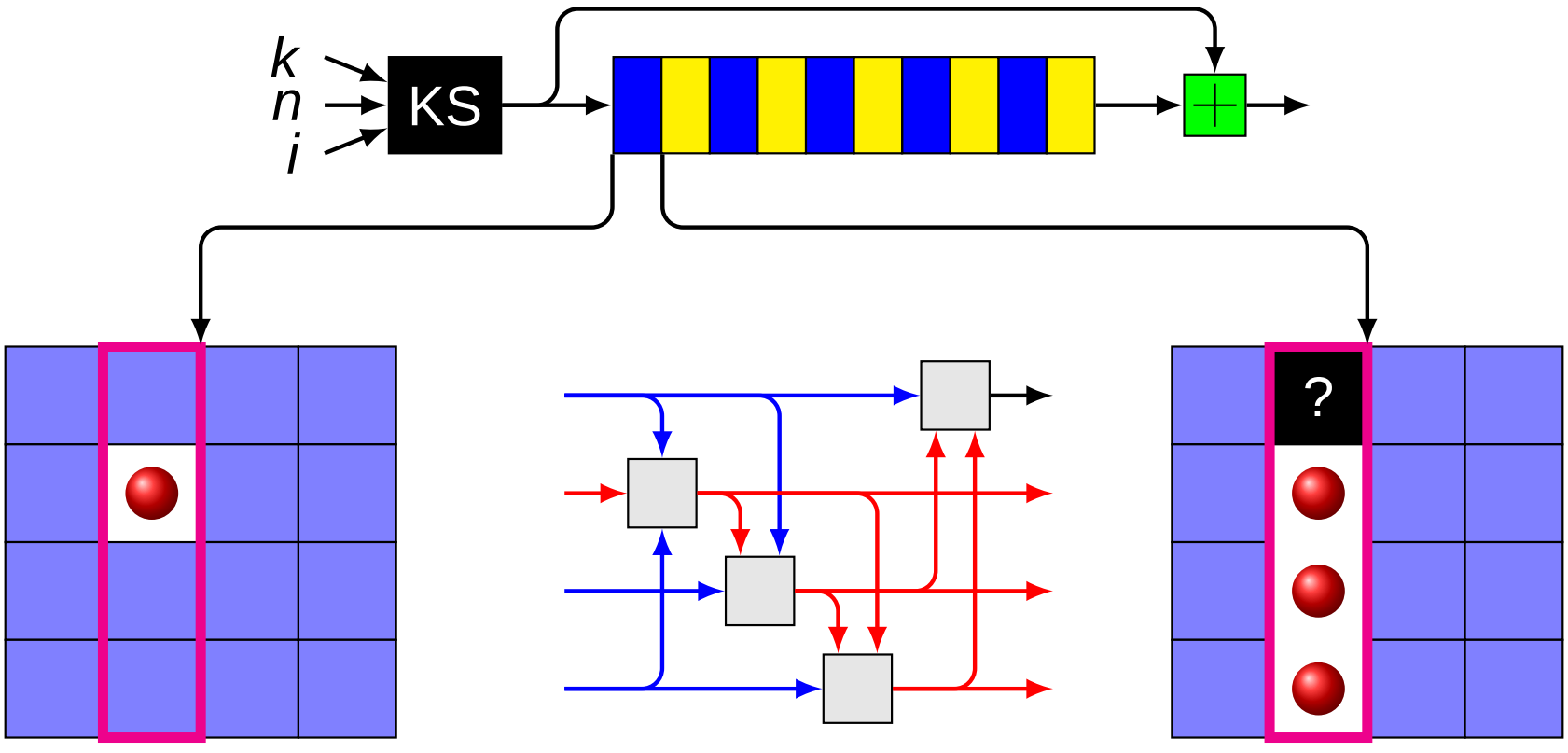
Differential characteristic



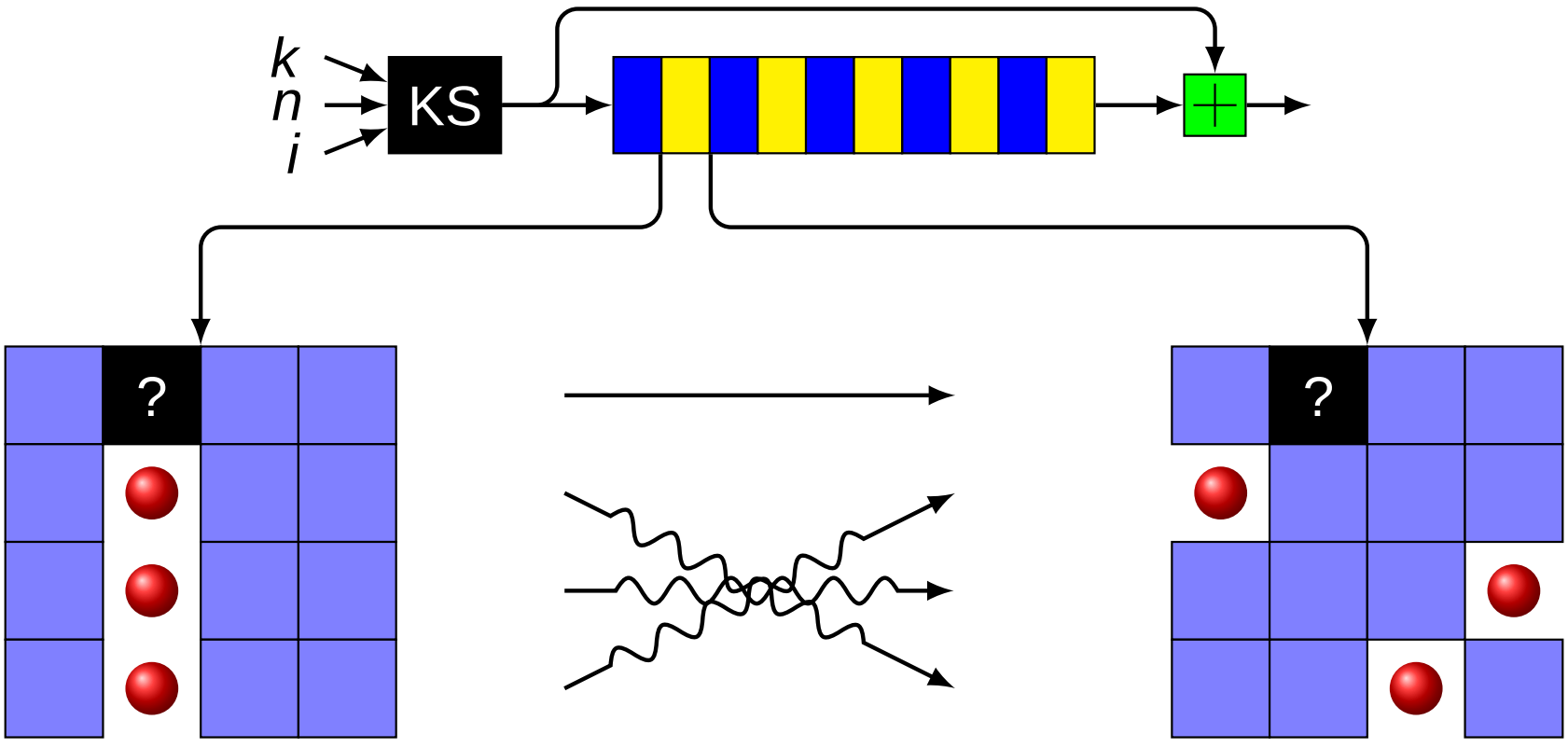
Differential characteristic



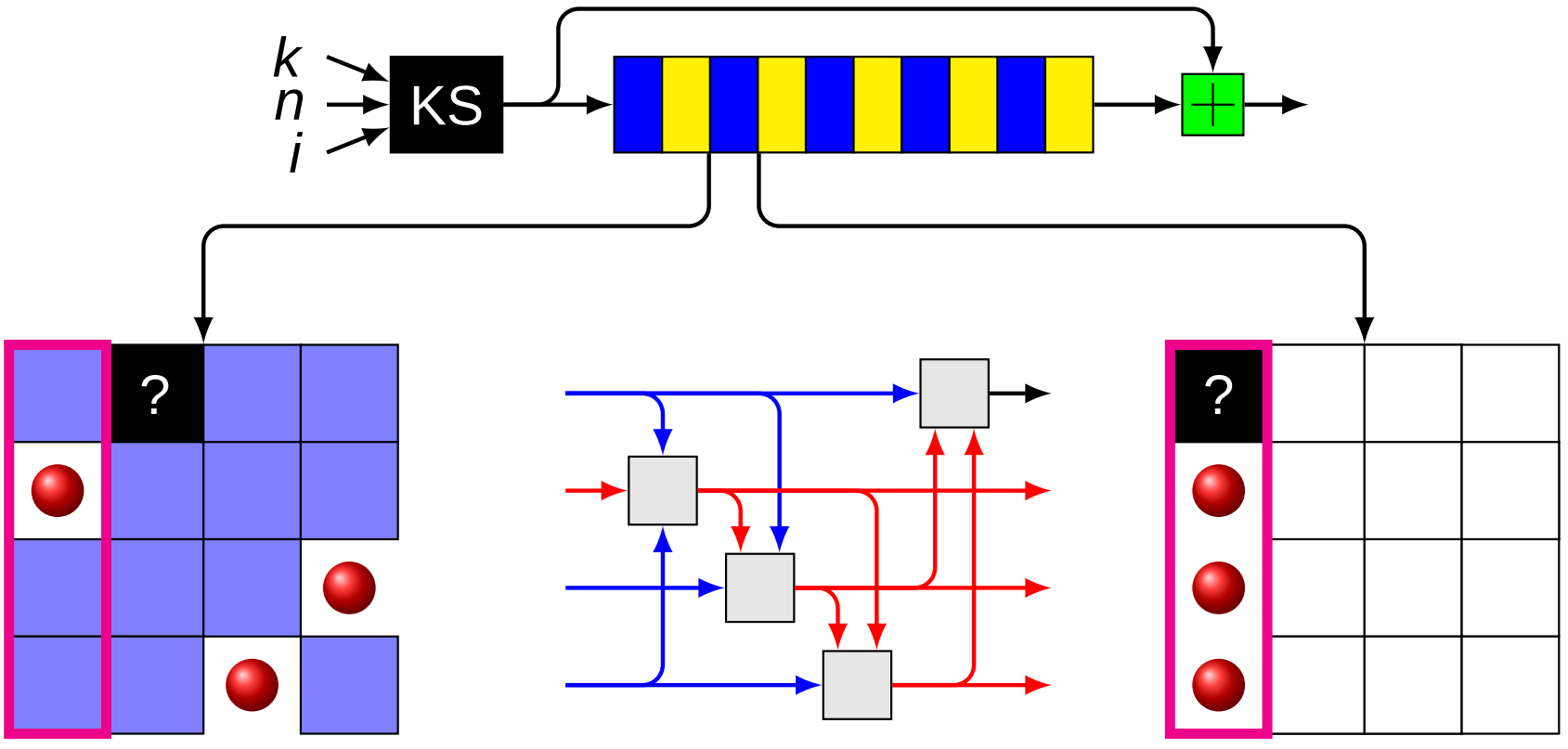
Differential characteristic



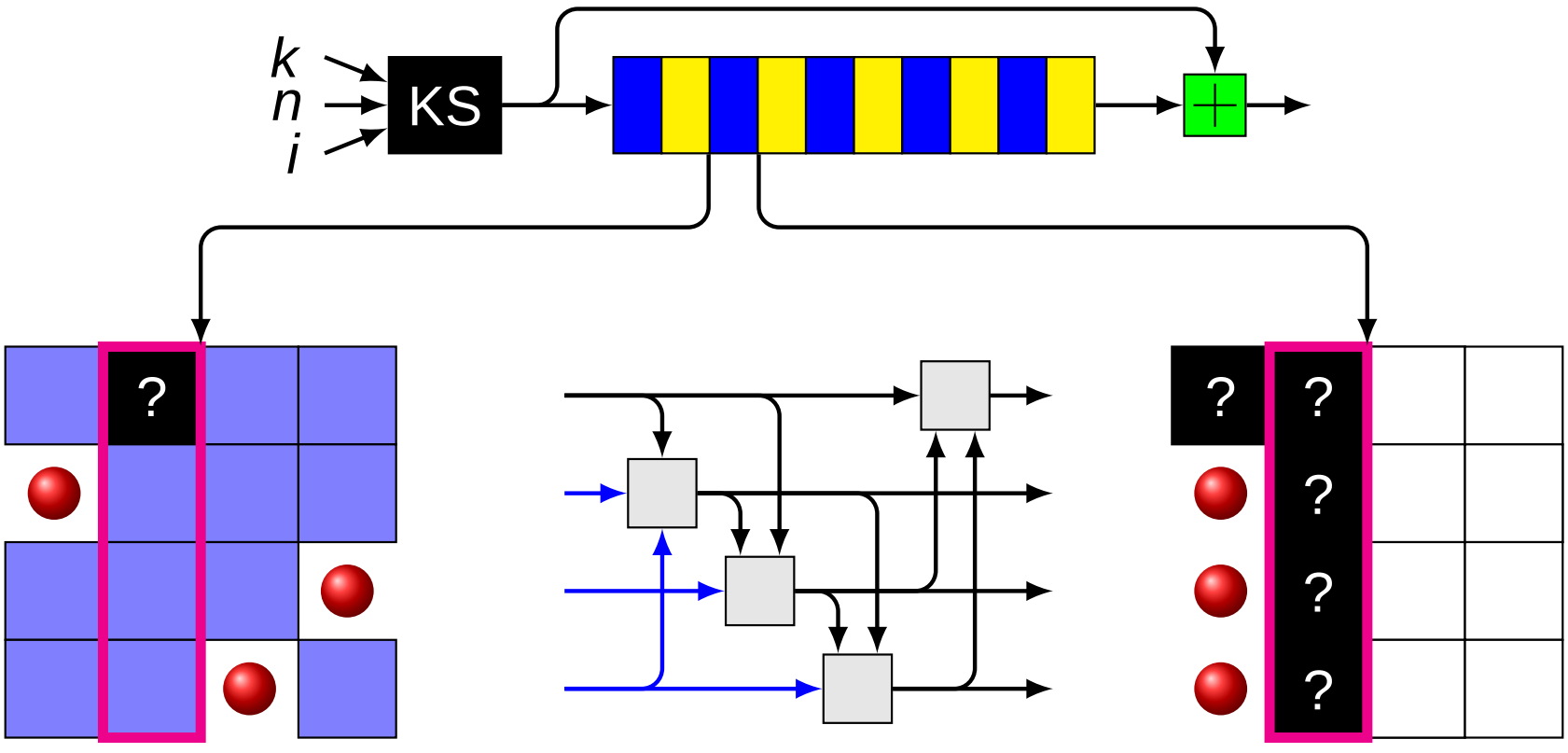
Differential characteristic



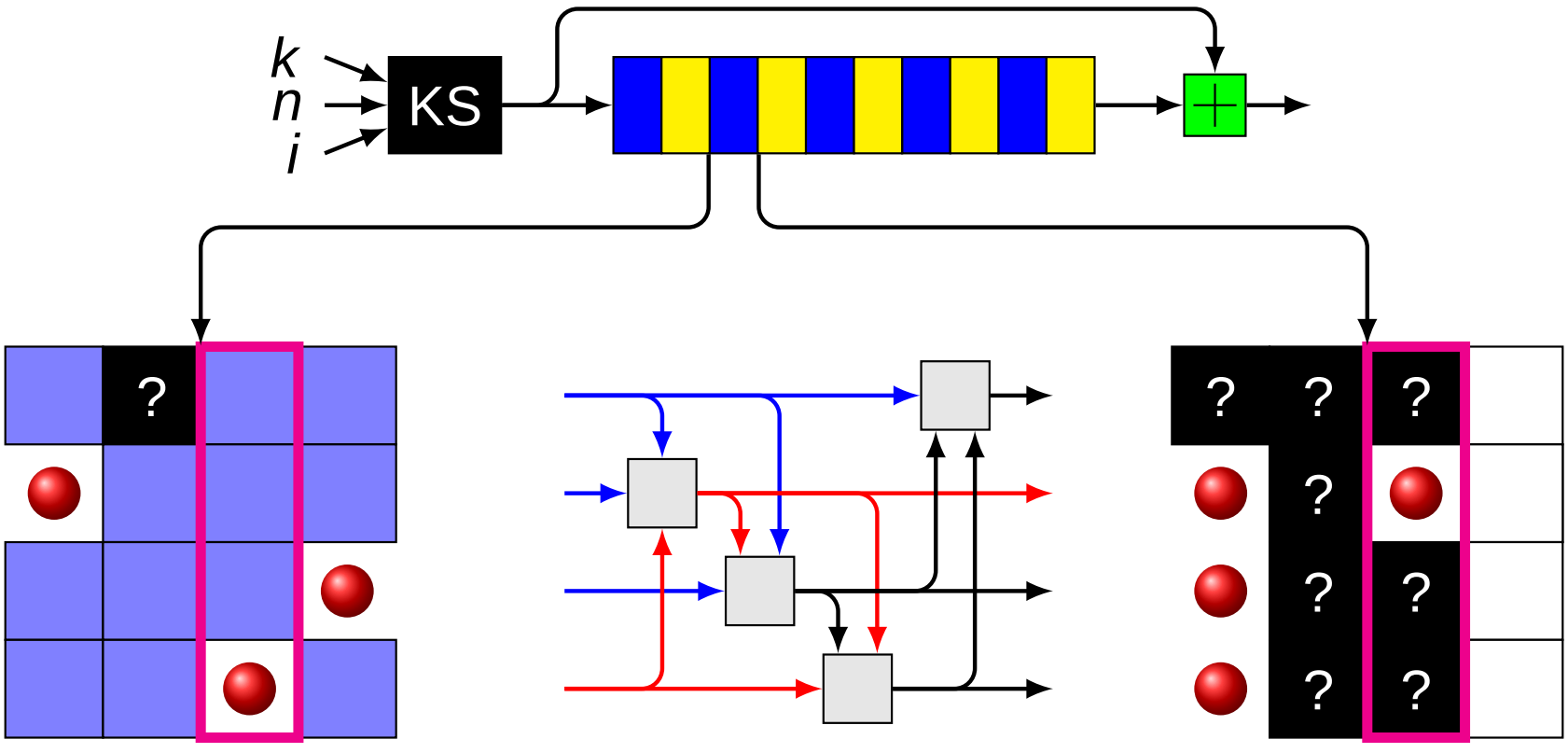
Differential characteristic



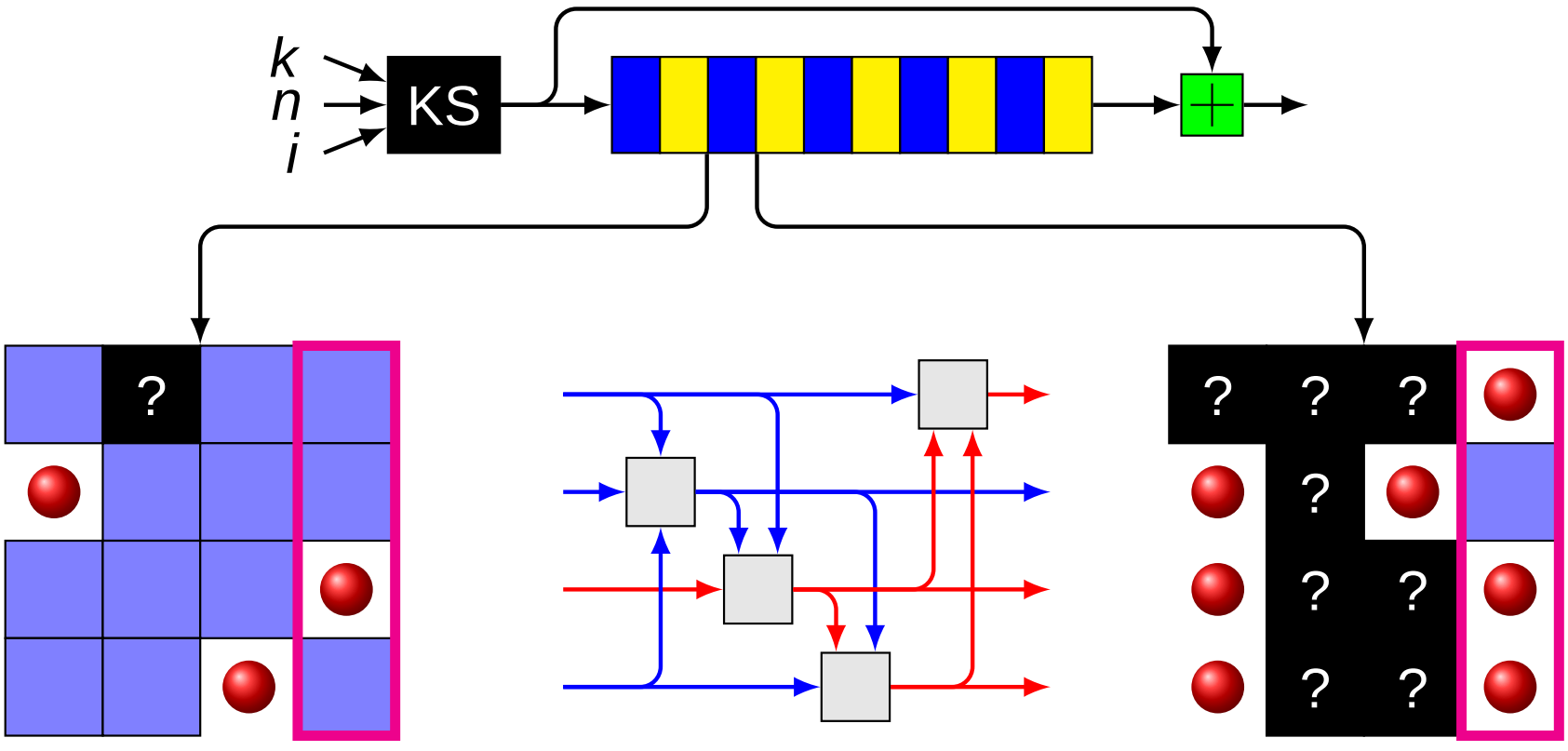
Differential characteristic



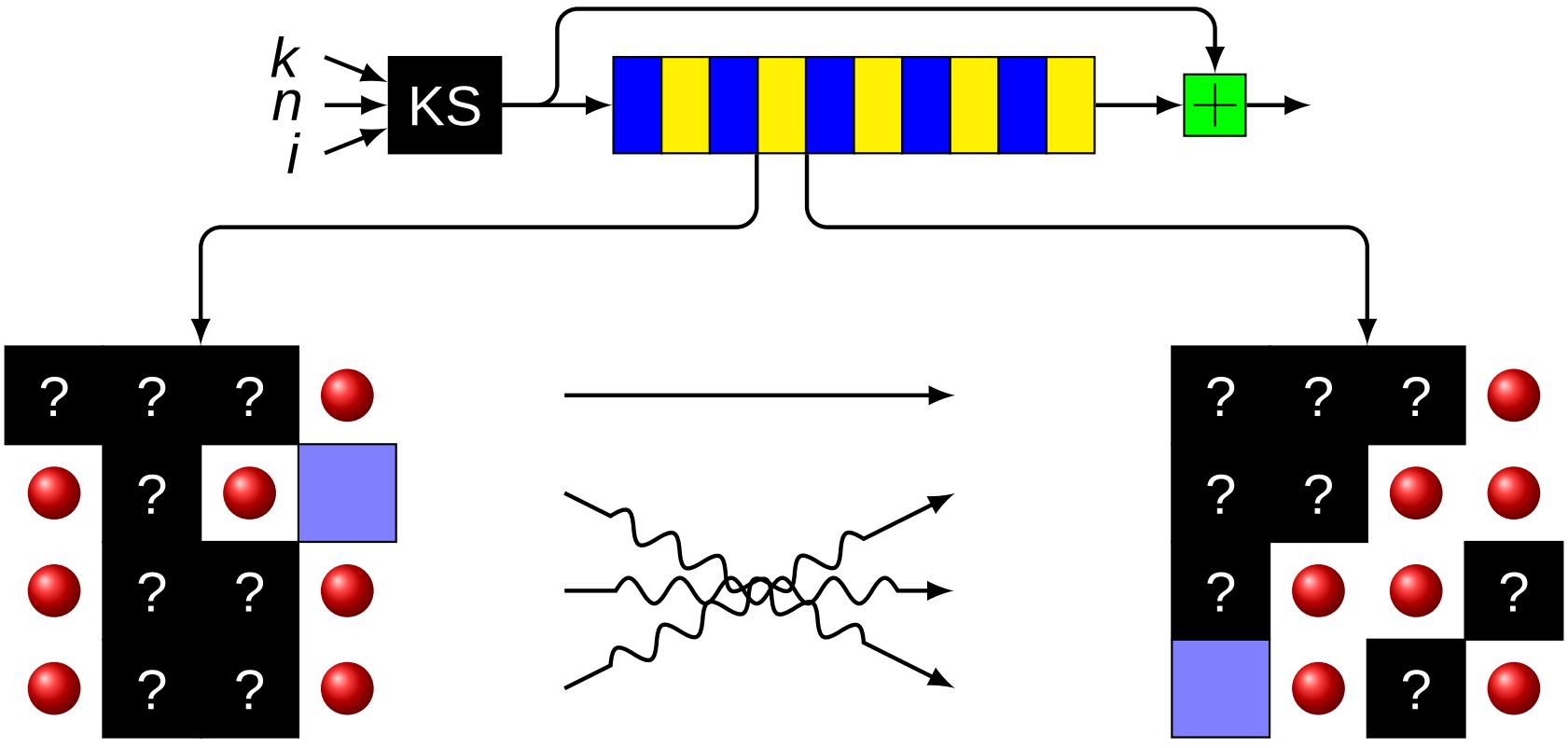
Differential characteristic



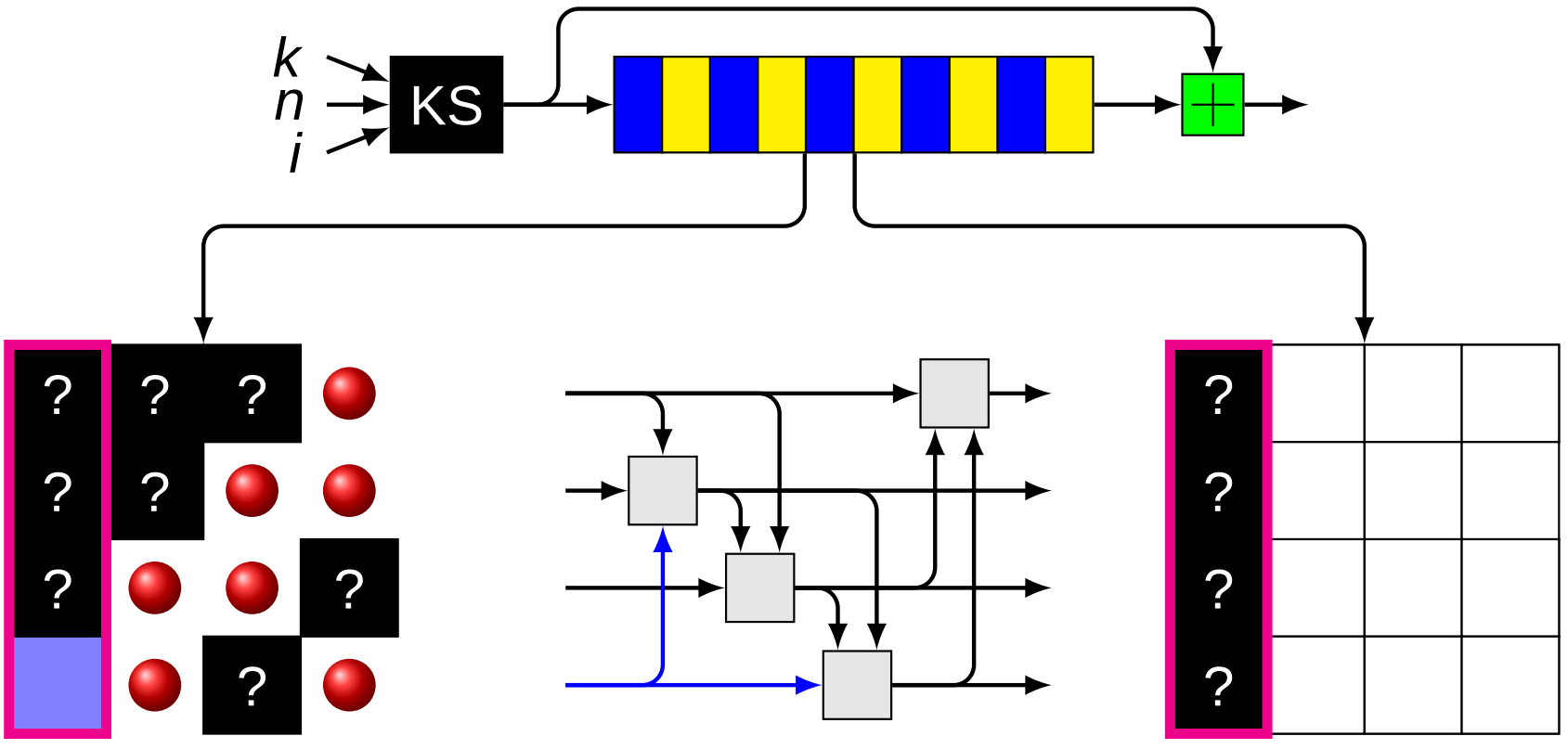
Differential characteristic



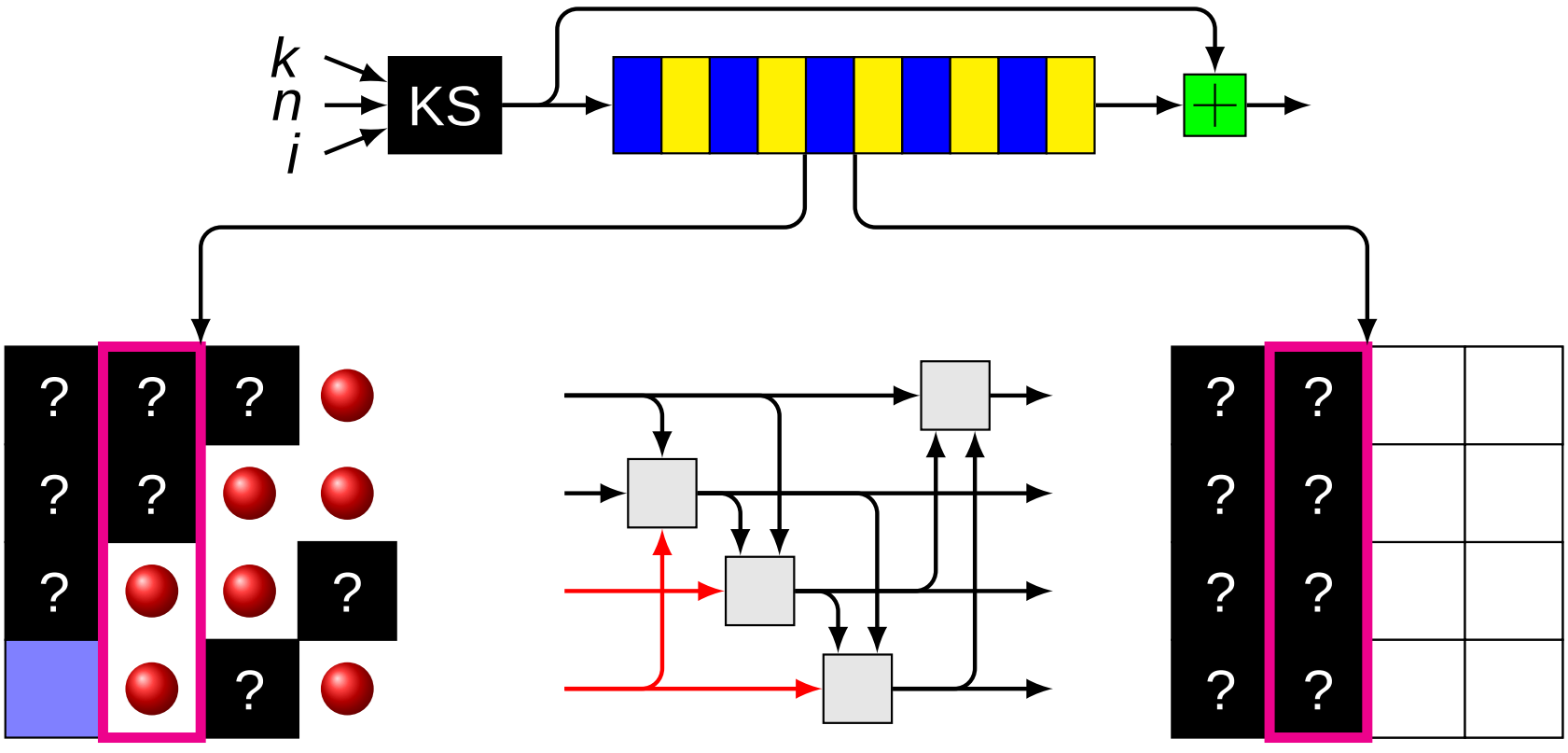
Differential characteristic



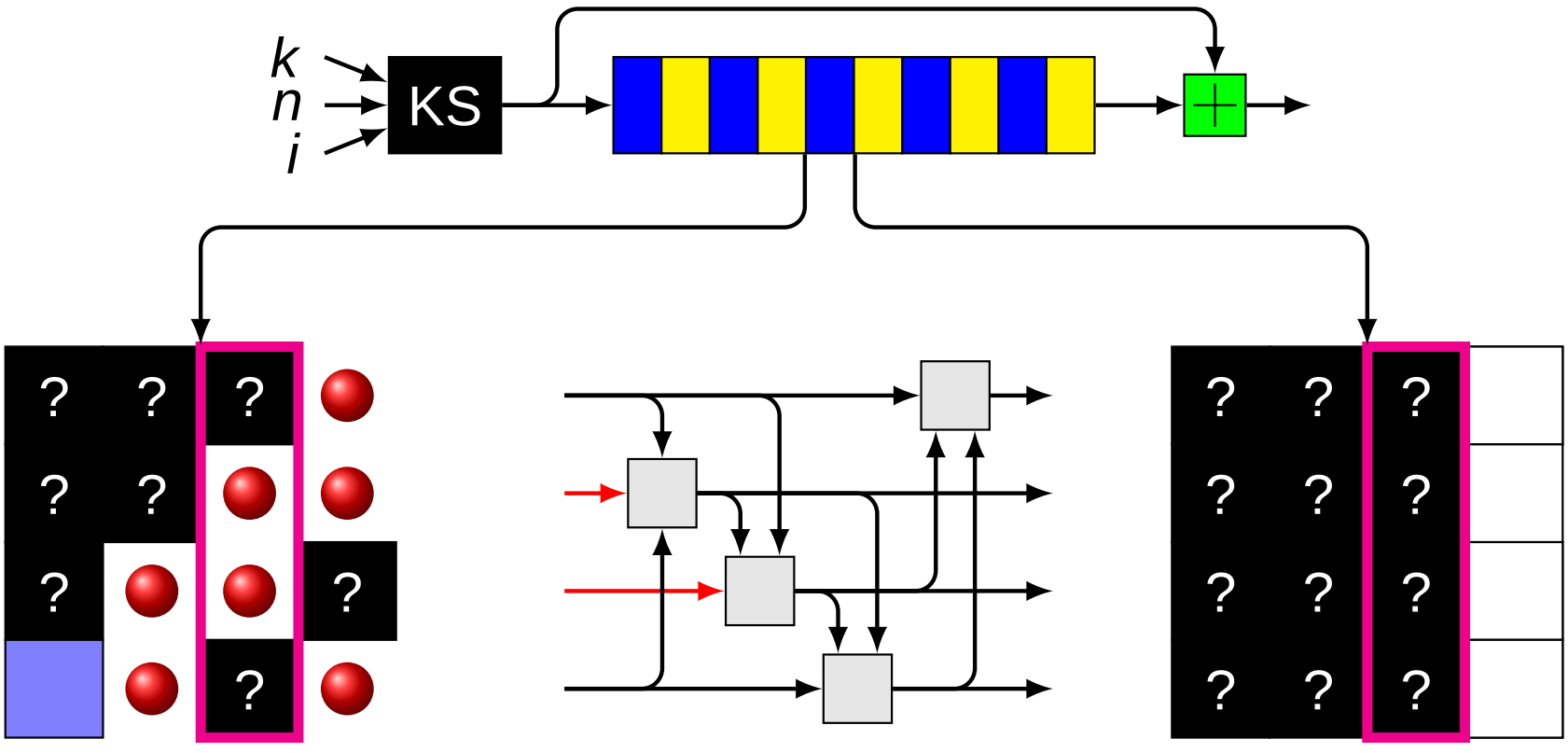
Differential characteristic



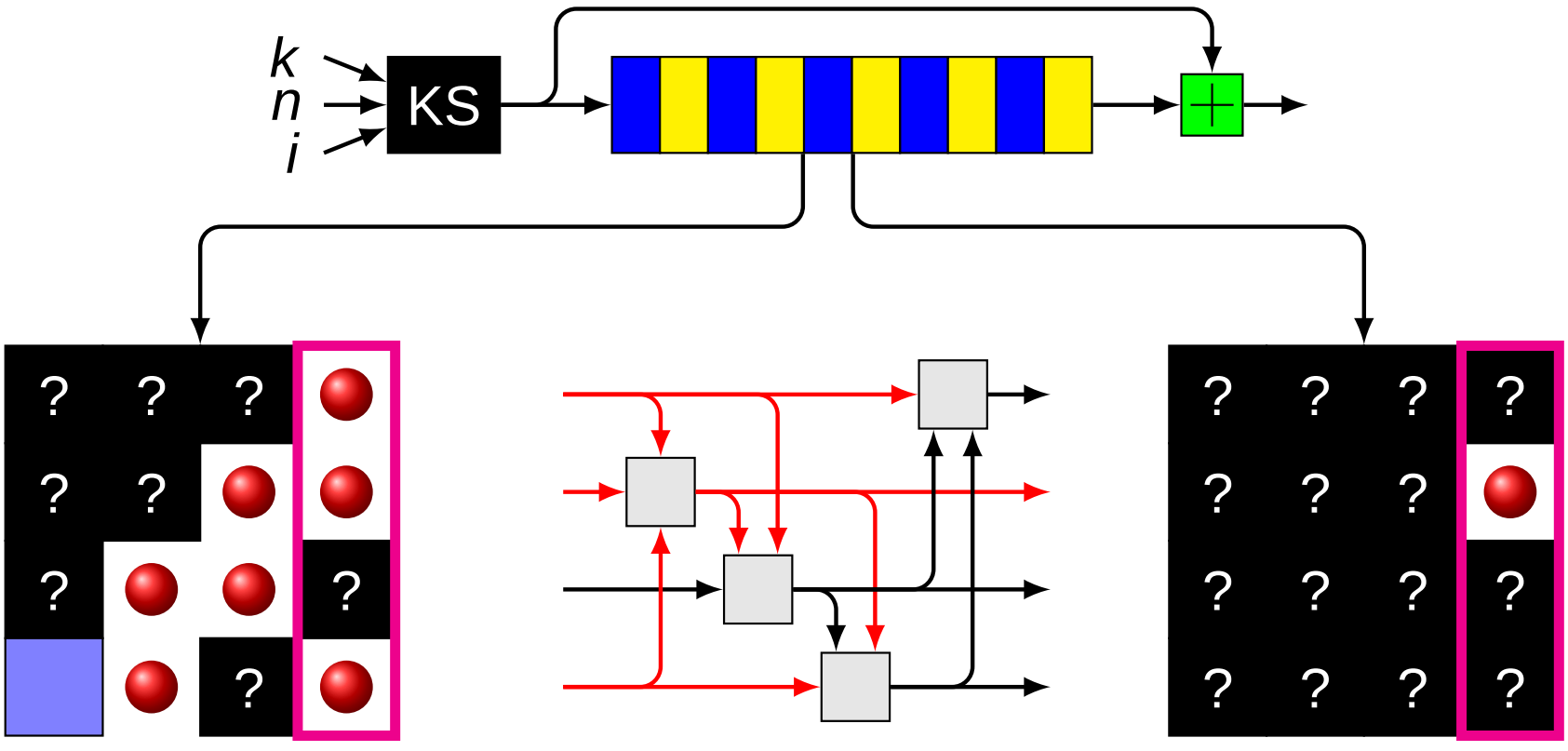
Differential characteristic



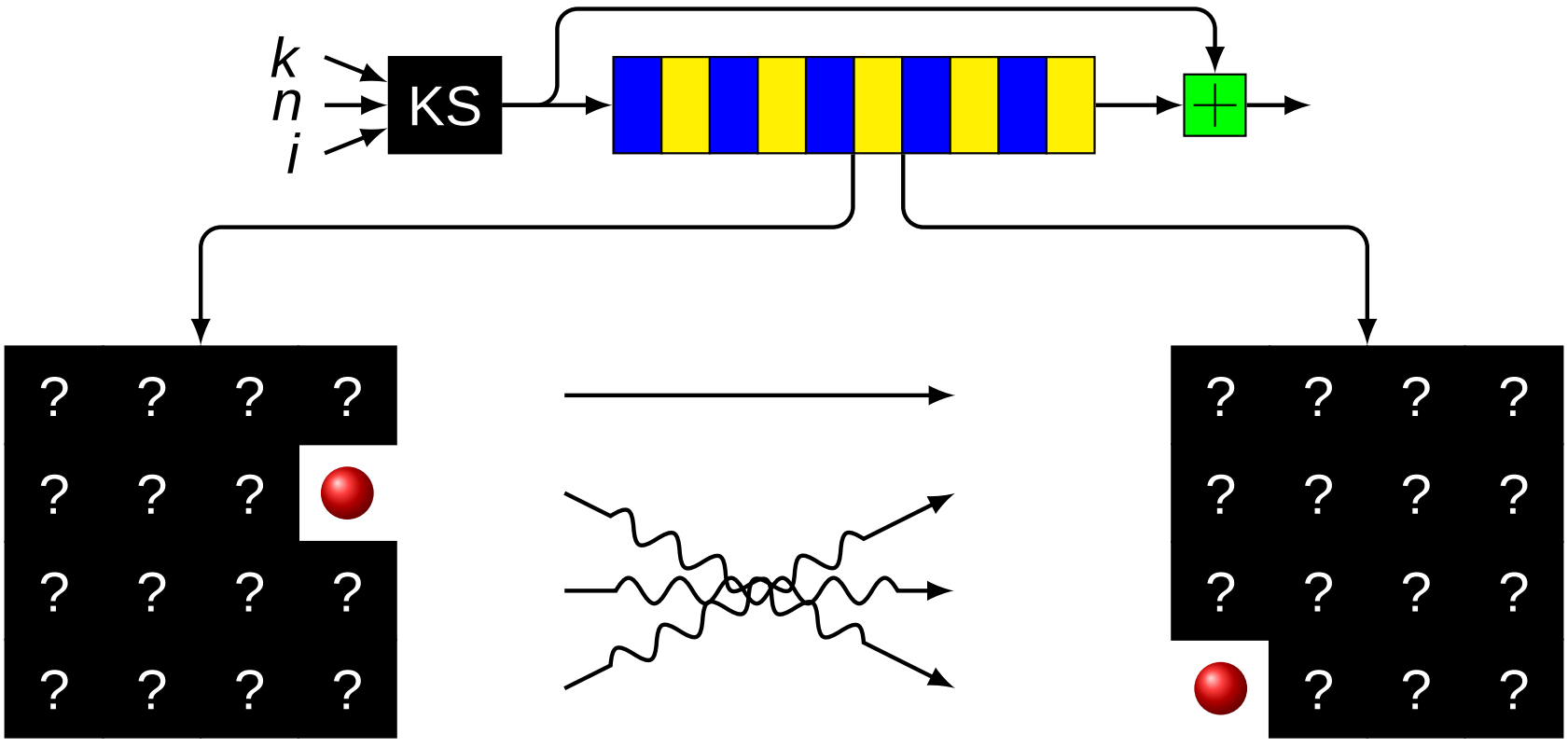
Differential characteristic



Differential characteristic



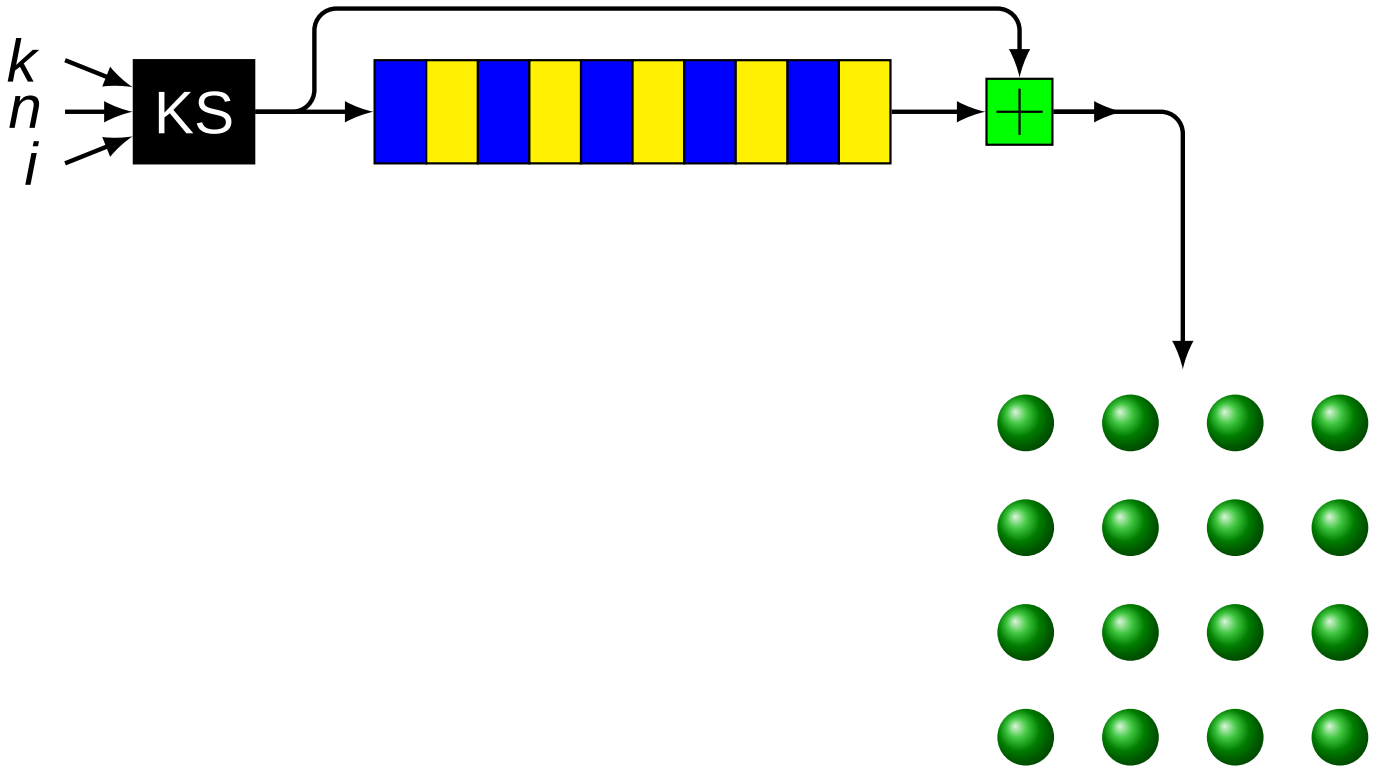
Differential characteristic



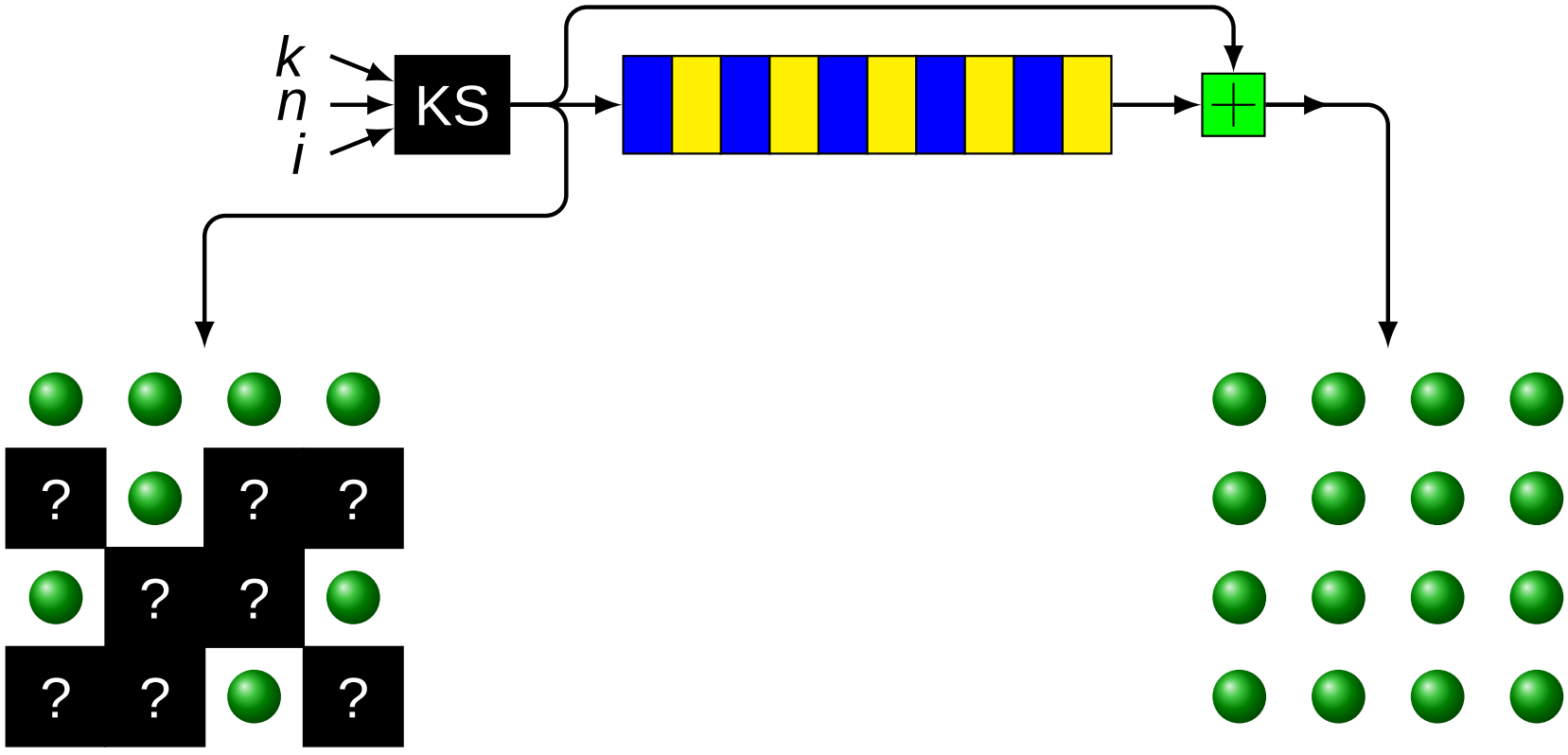
Increasing the probability

- Best characteristic: 2^{-12}
- Many differentials
- Many characteristics
- 1024 best differentials: ≈ 0.3

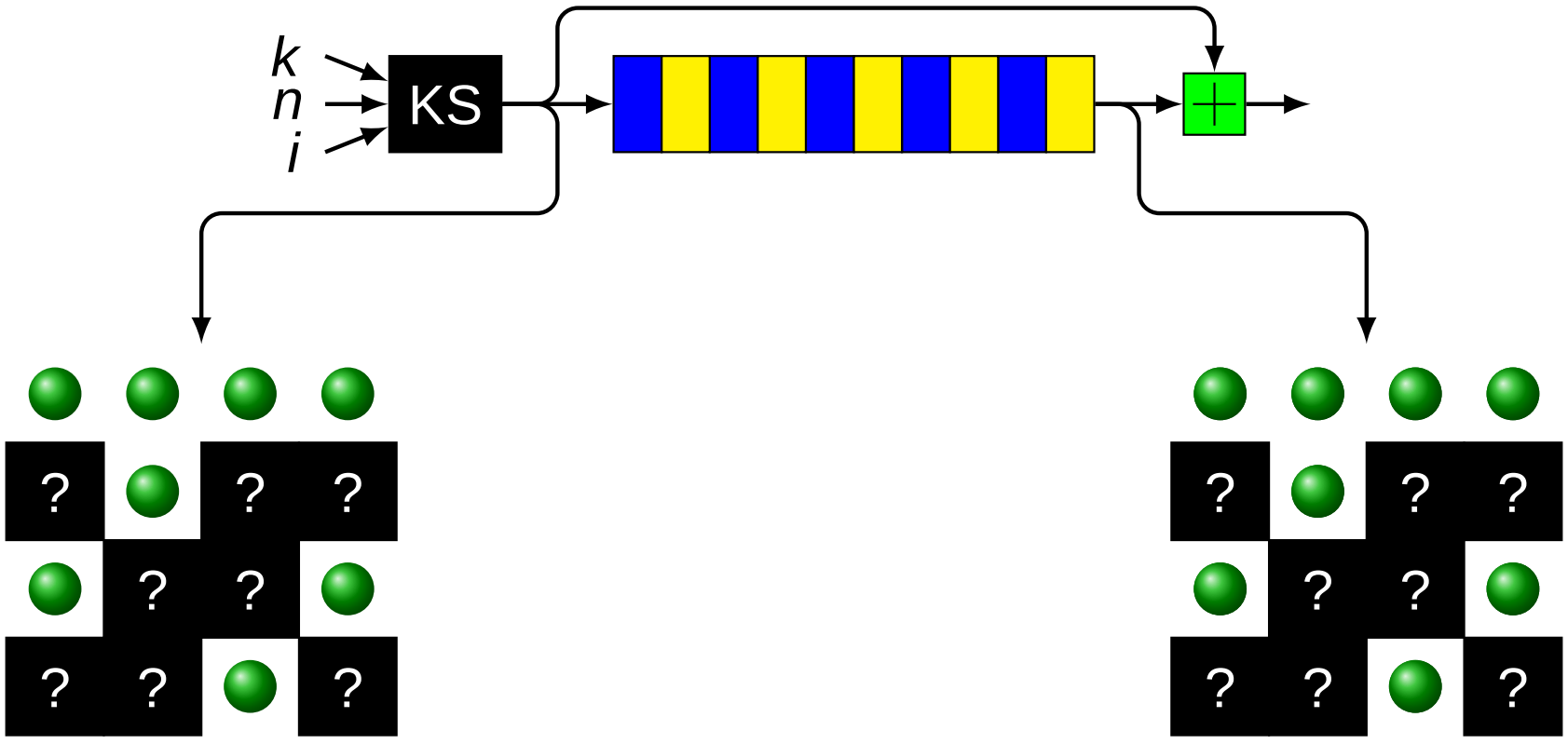
Inferring backwards



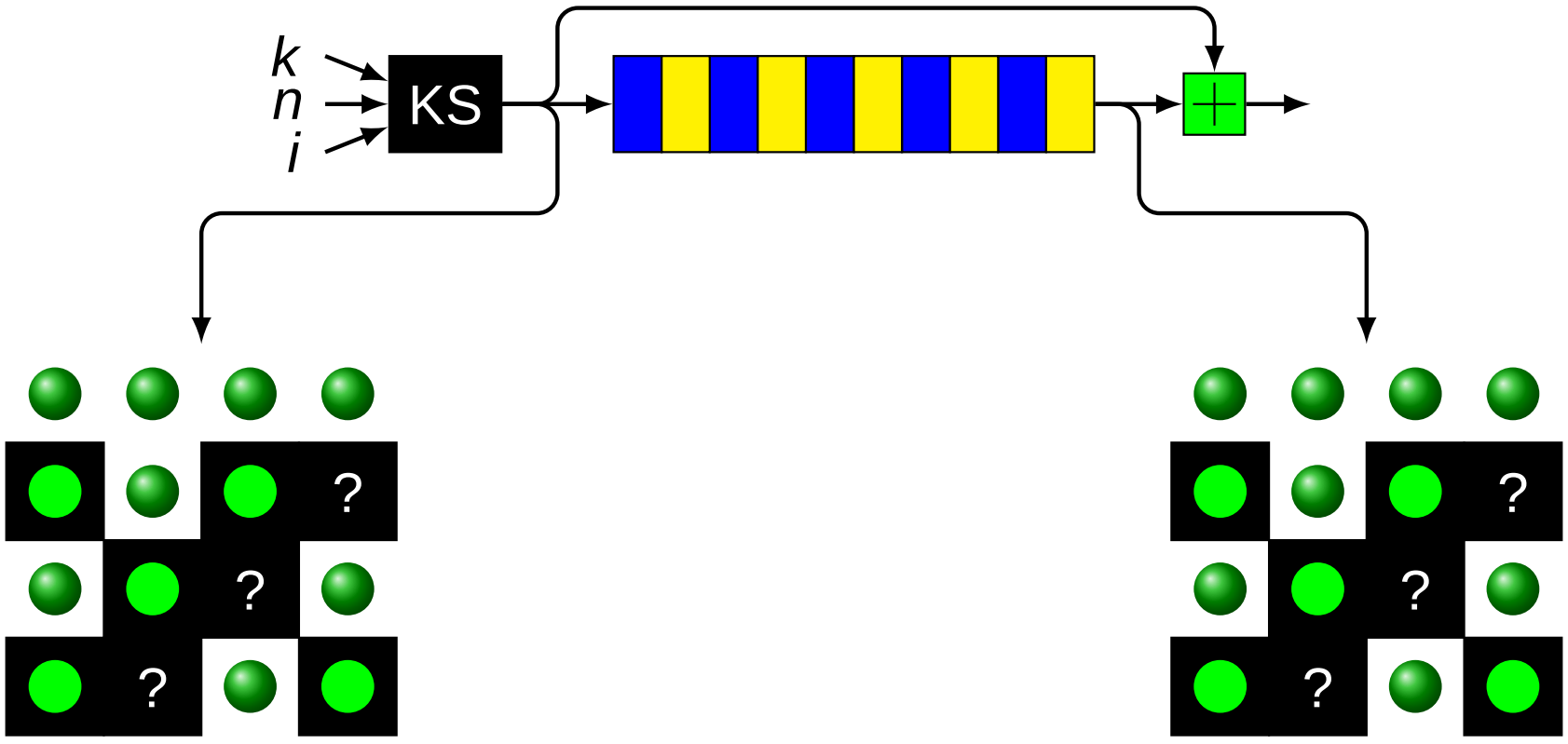
Inferring backwards



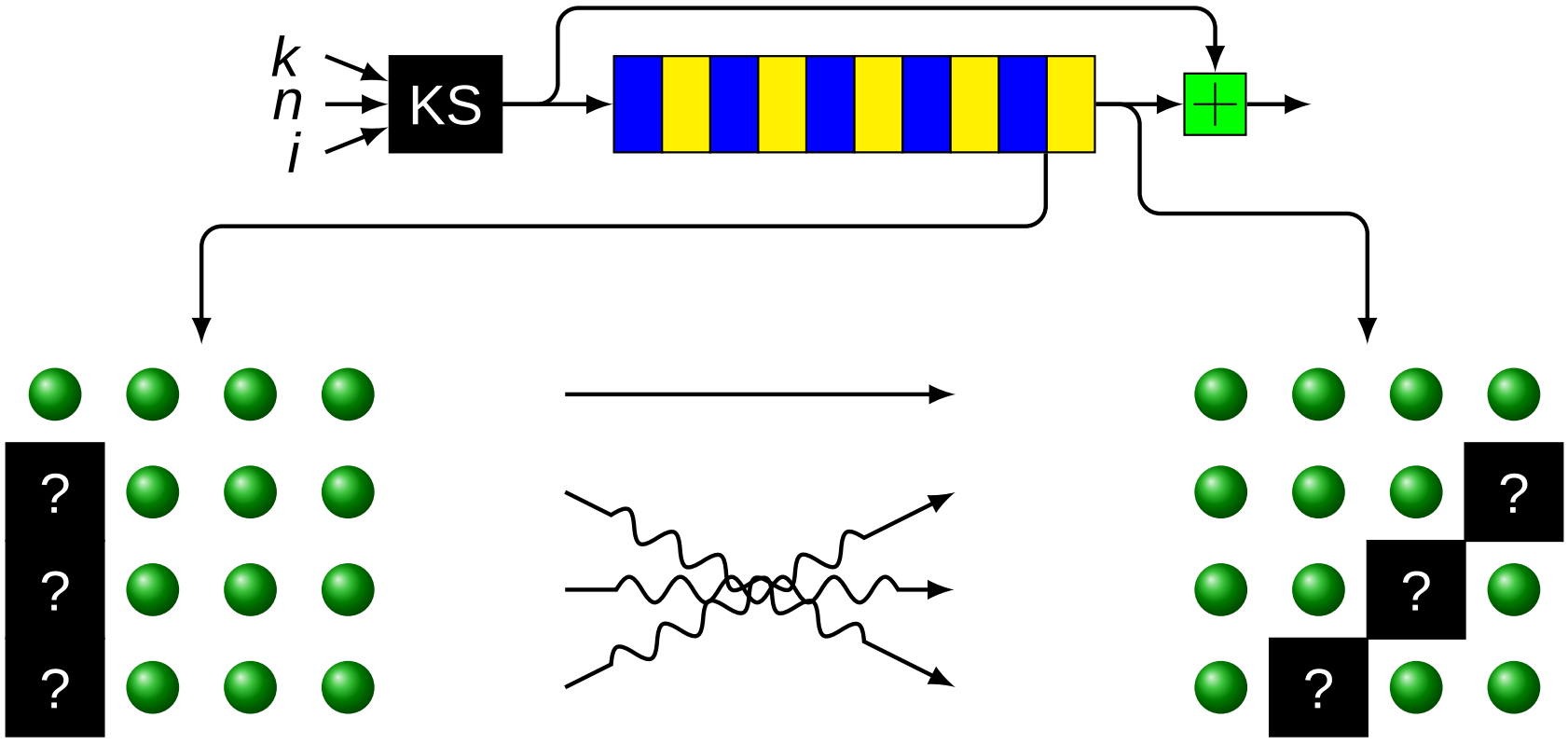
Inferring backwards



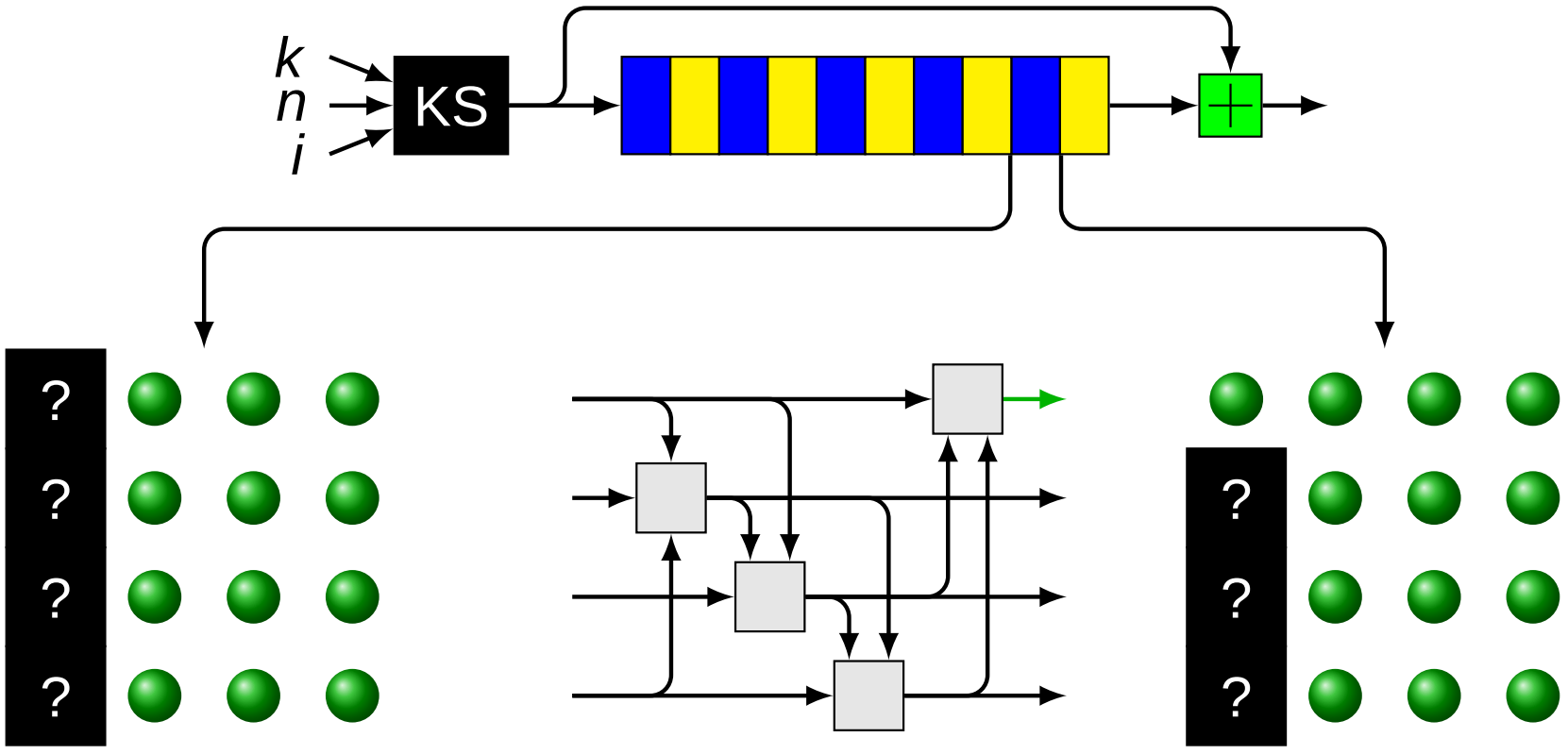
Inferring backwards



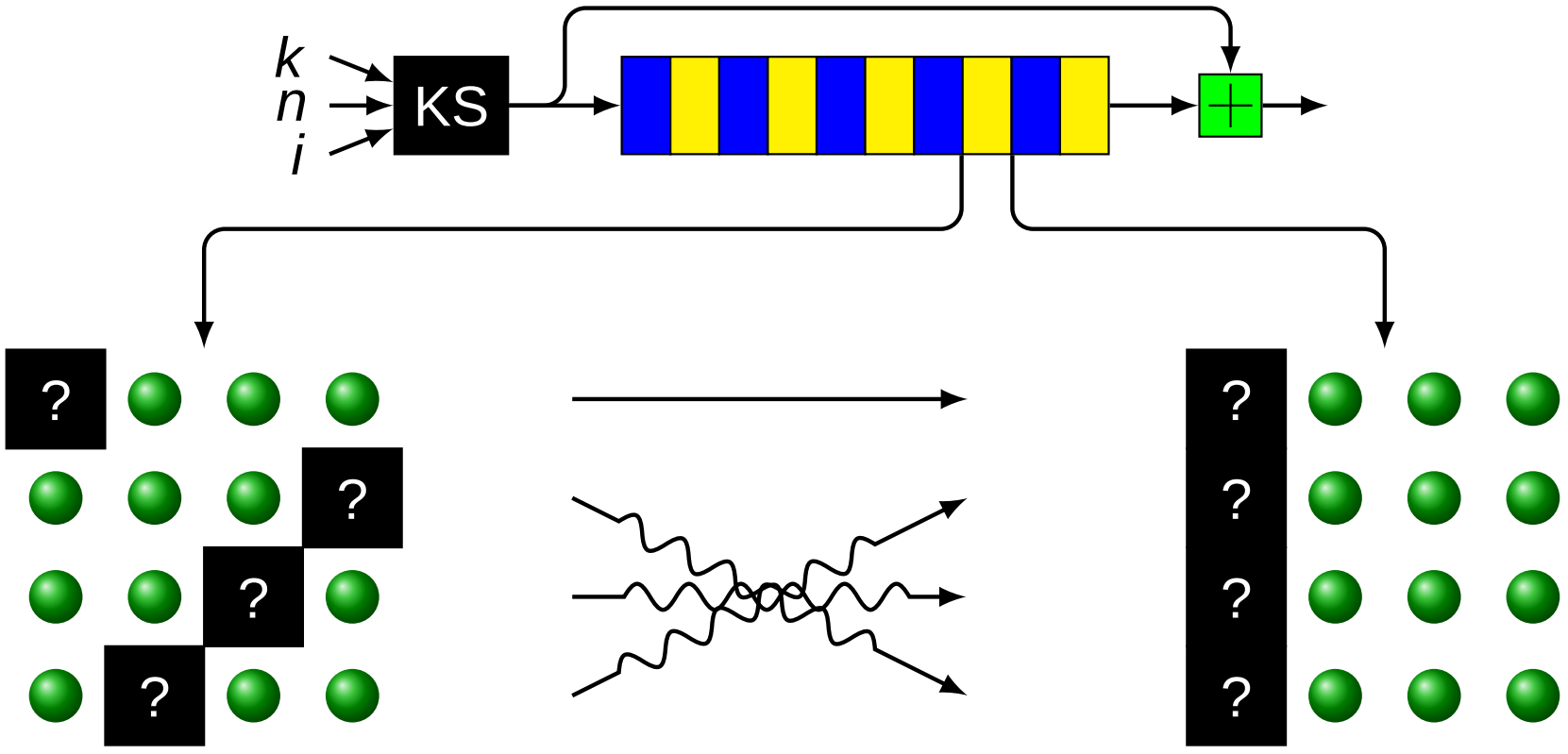
Inferring backwards



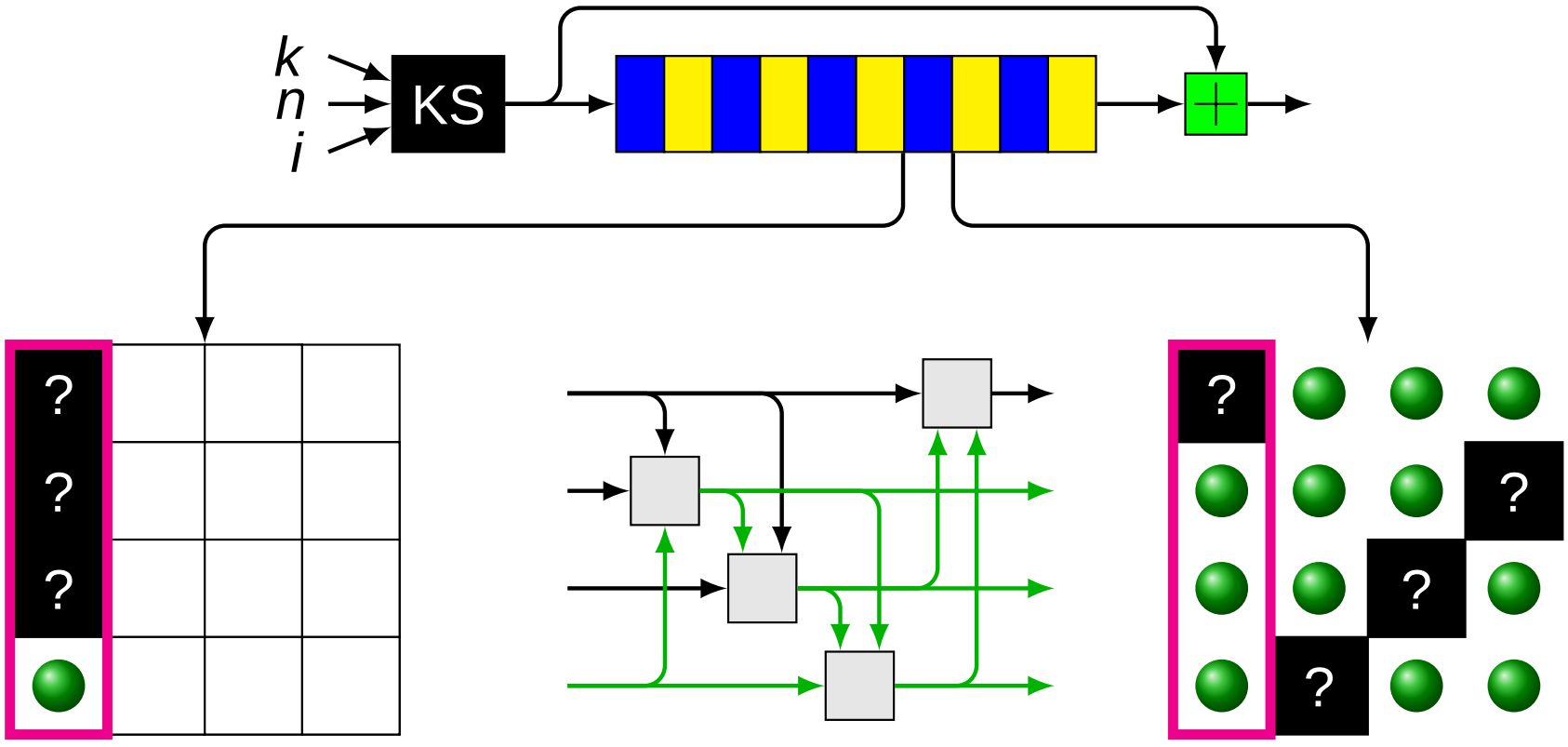
Inferring backwards



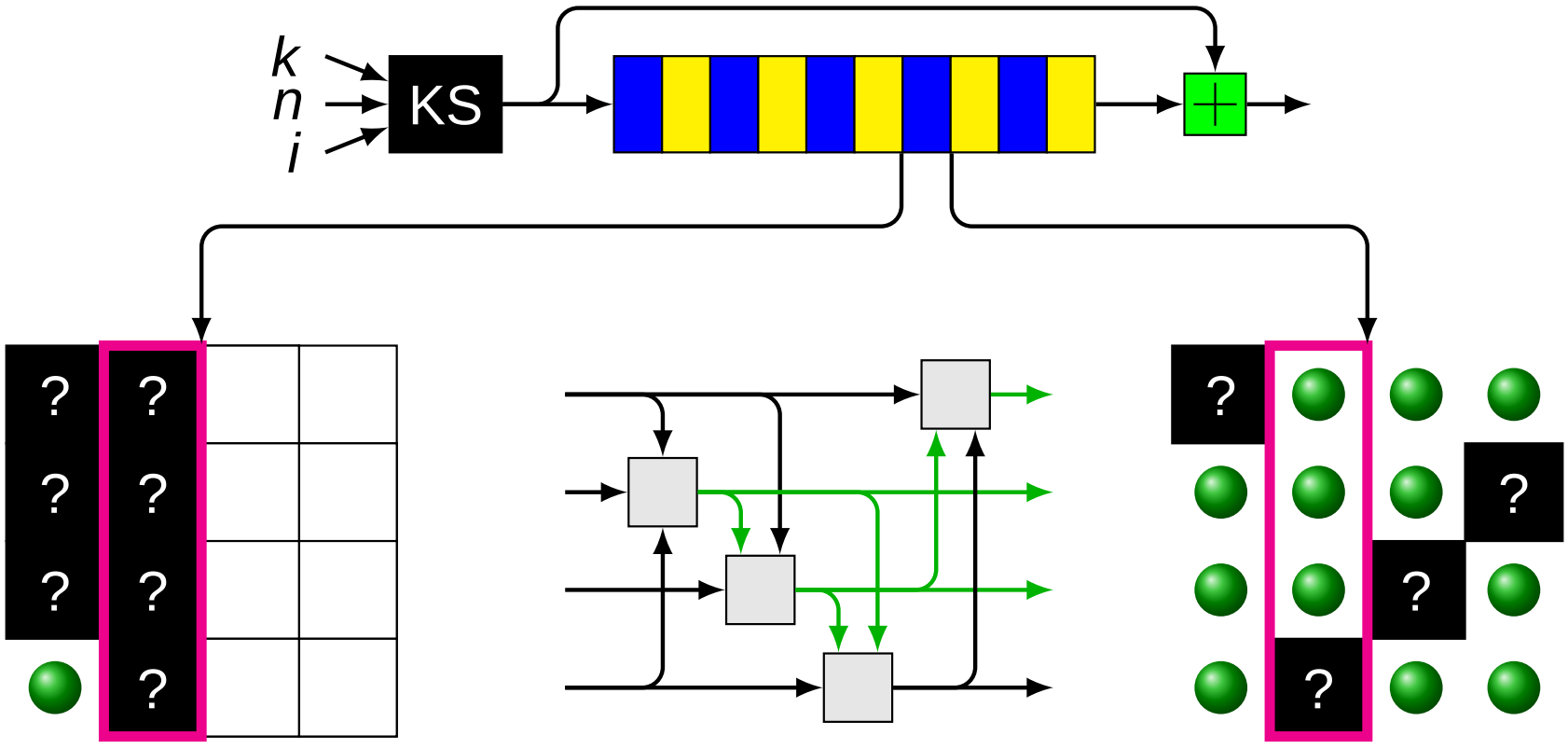
Inferring backwards



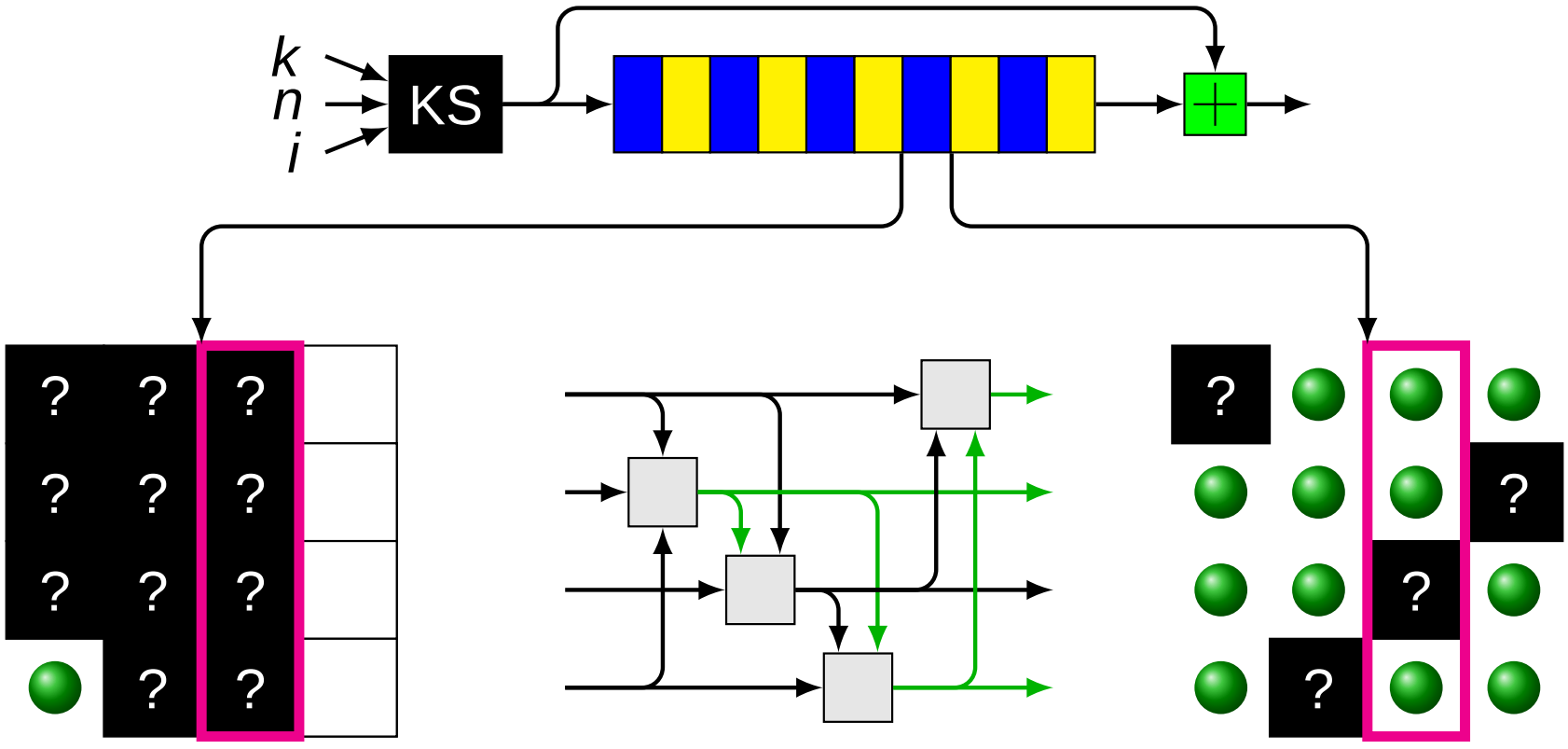
Inferring backwards



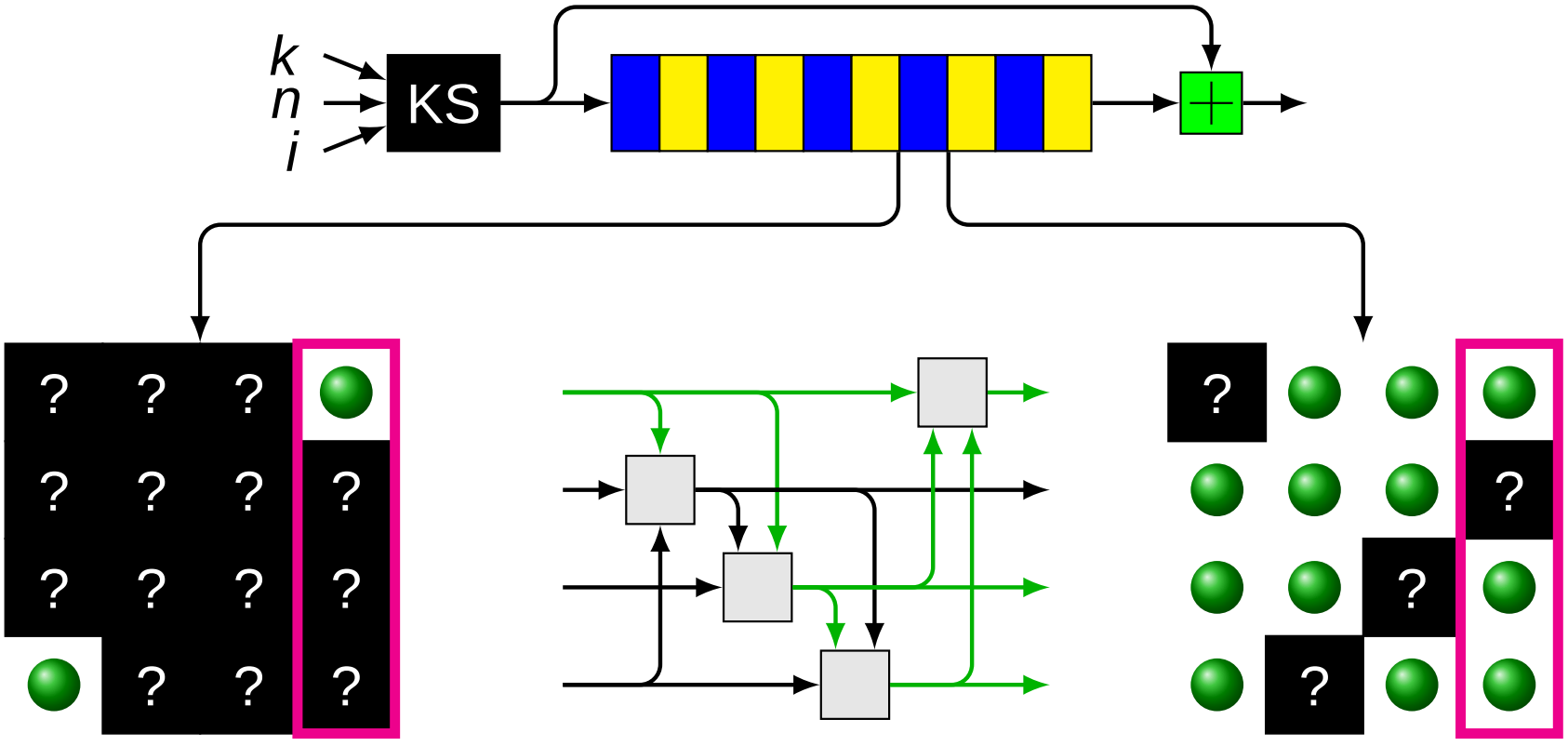
Inferring backwards



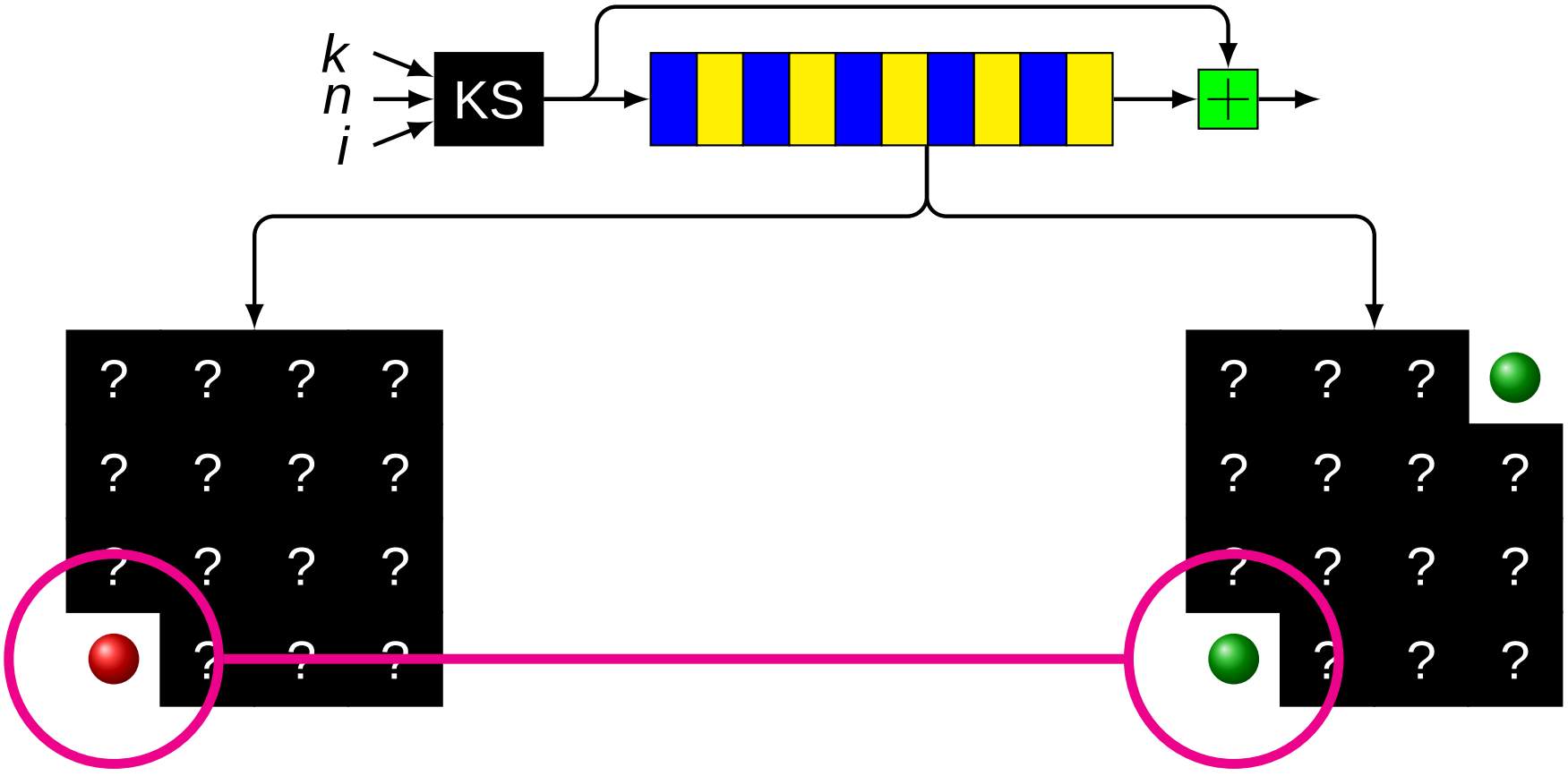
Inferring backwards



Inferring backwards



Inferring backwards



Work factor

- 32 plaintexts
- False positives: 2^{61}
- Work choosing candidates: 2^{165}
- Work discarding false positives: 2^{157}

Conclusions

- 5 rounds broken with 32 plaintext pairs and 2^{165} effort
- Differentials cluster in Salsa20
- Worth considering many differentials
- Cannot extend to full Salsa20

www.ciphergoth.org/crypto/salsa20