Hullaballoo

Sebastiaan Indesteege[1] Florian Mendel[2]
Christian Rechberger[2] Martin Schläffer[2]

[1]COSIC, ESAT, K.U. Leuven, Belgium

[2]Krypto, IAIK, T.U.Graz, Austria

FSE 2009 Rump Session

Ṣamata

Sebastiaan Indesteege[1] Florian Mendel[2]
Christian Rechberger[2] Martin Schläffer[2]

[1]COSIC, ESAT, K.U. Leuven, Belgium

[2]Krypto, IAIK, T.U.Graz, Austria

FSE 2009 Rump Session

SHAMATA

Sebastiaan Indesteege[1] Florian Mendel[2]
Christian Rechberger[2] Martin Schläffer[2]

[1]COSIC, ESAT, K.U. Leuven, Belgium

[2]Krypto, IAIK, T.U.Graz, Austria

FSE 2009 Rump Session

Collisions for SHAMATA

Sebastiaan Indesteege[1] Florian Mendel[2]
Christian Rechberger[2] Martin Schläffer[2]

[1]COSIC, ESAT, K.U. Leuven, Belgium

[2]Krypto, IAIK, T.U.Graz, Austria

FSE 2009 Rump Session

Practical Collisions for SHAMATA

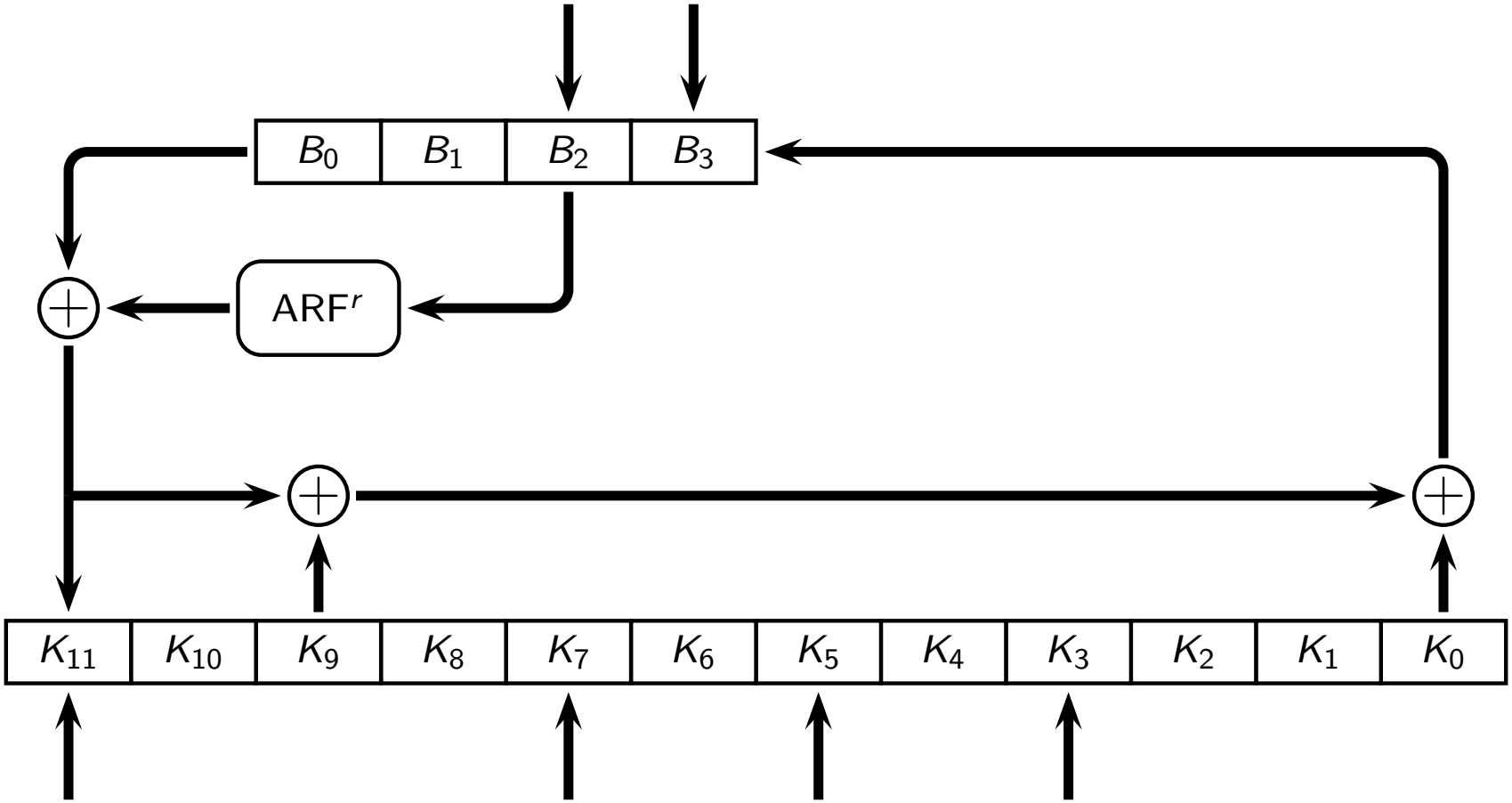
Sebastiaan Indesteege[1] Florian Mendel[2]
Christian Rechberger[2] Martin Schläffer[2]

[1]COSIC, ESAT, K.U. Leuven, Belgium

[2]Krypto, IAIK, T.U.Graz, Austria

FSE 2009 Rump Session

SHAMATA

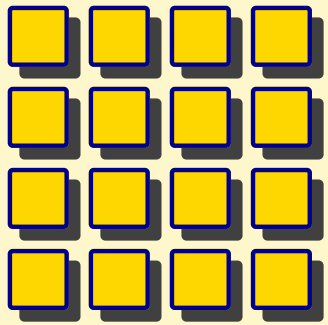


O. Kara, C. Manap, A. Atalay, F. Karakoç
SHAMATA, a candidate hash algorithm for SHA-3

All or Nothing!

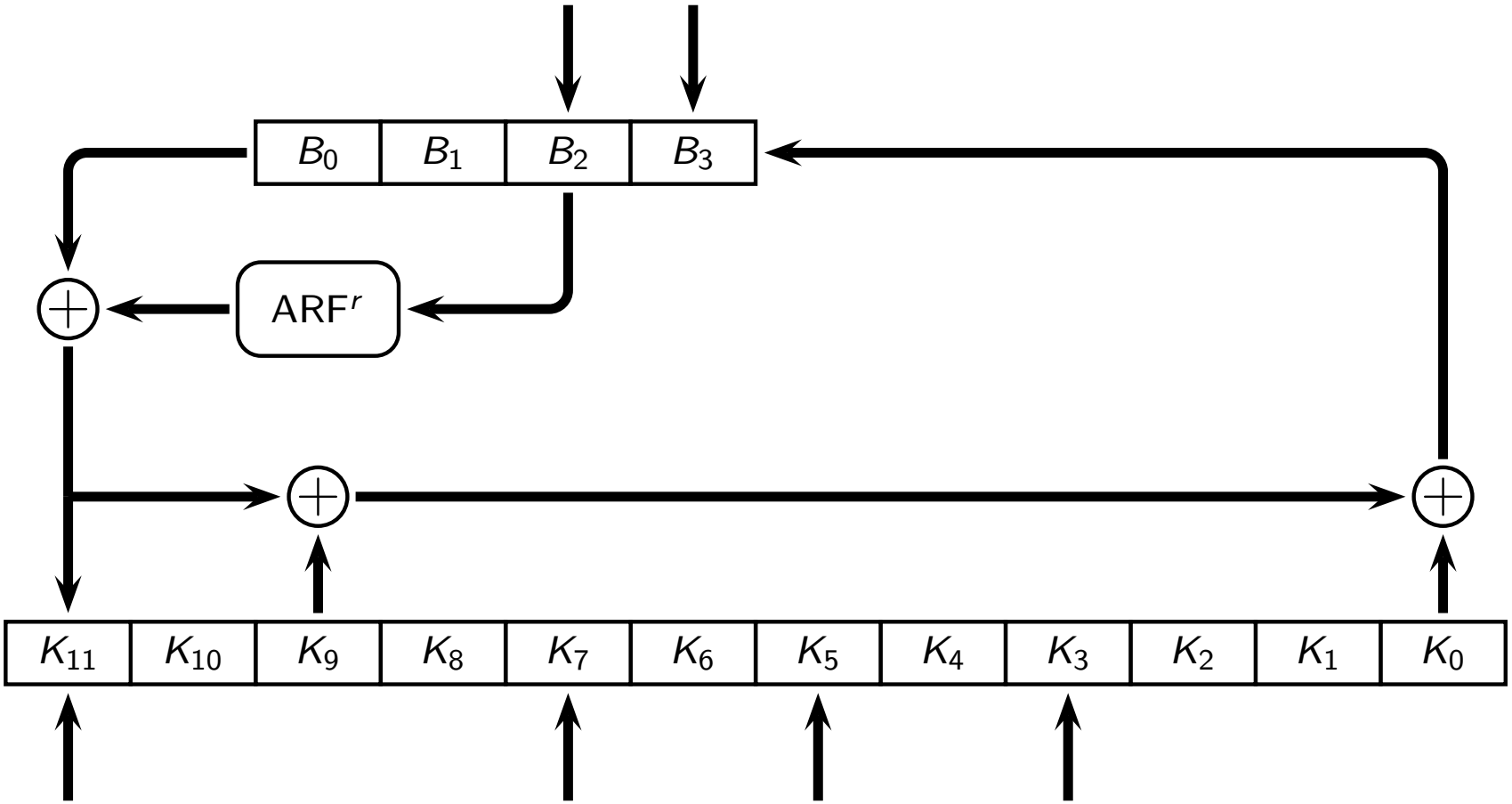
Consider the difference Δ = `0xffff···ffff`

- ✔ Matrix transposition
- ✔ Column swap
- ✔ ShiftRows
- ✔ MixColumns
- ✔ XOR
- ✖ **SubBytes**

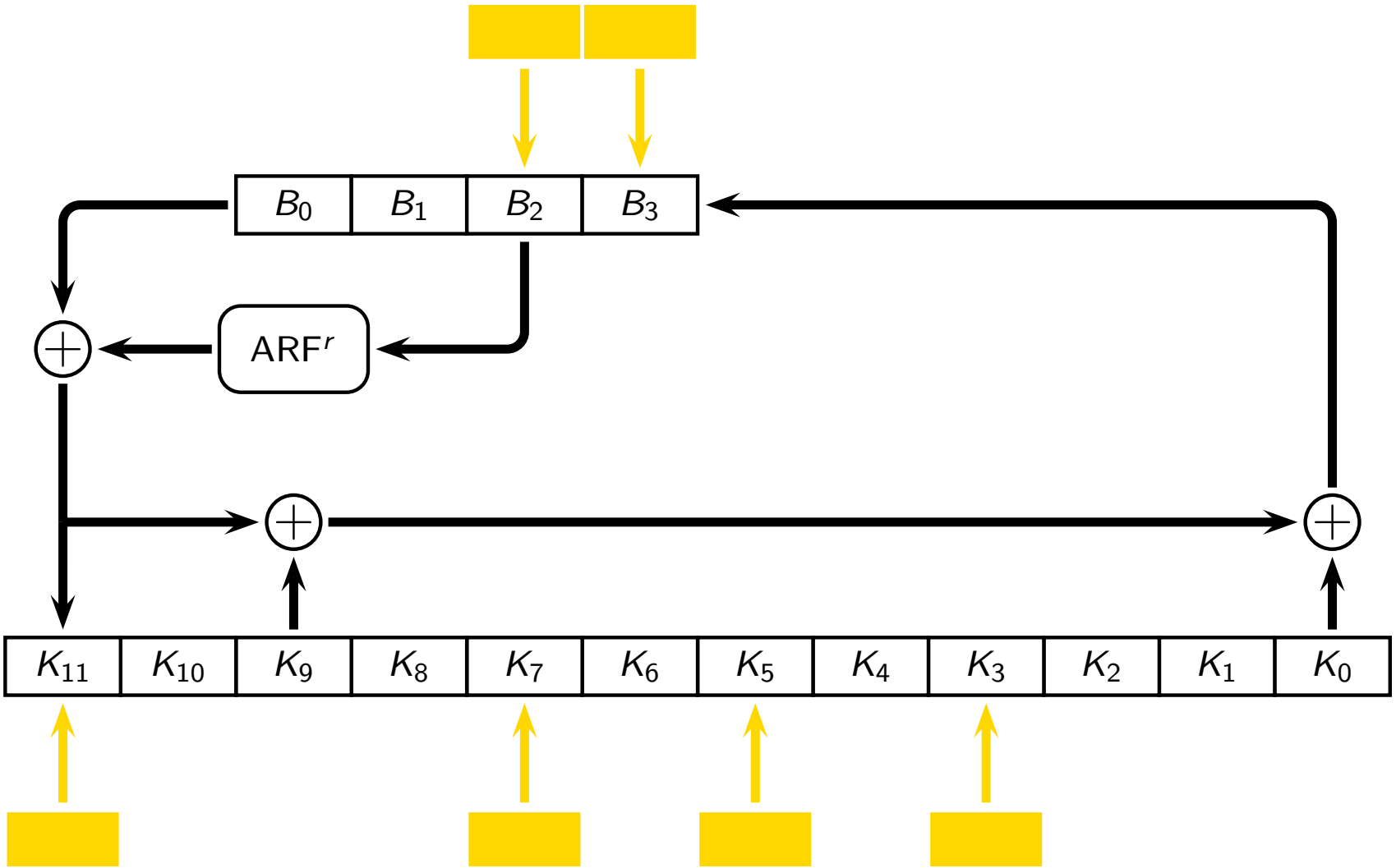


Assume it also passes through SubBytes (for now)

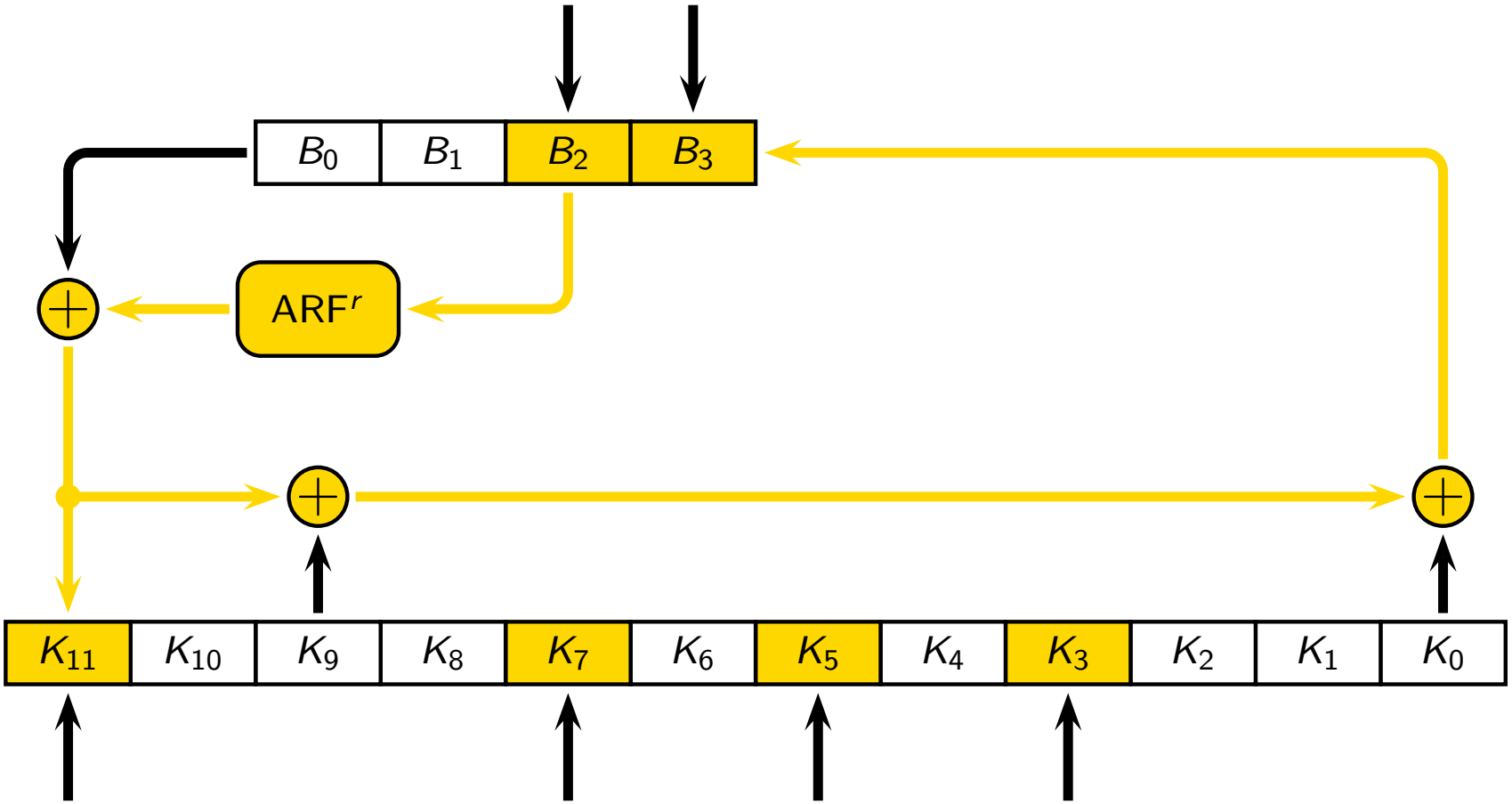
On a Collision Course



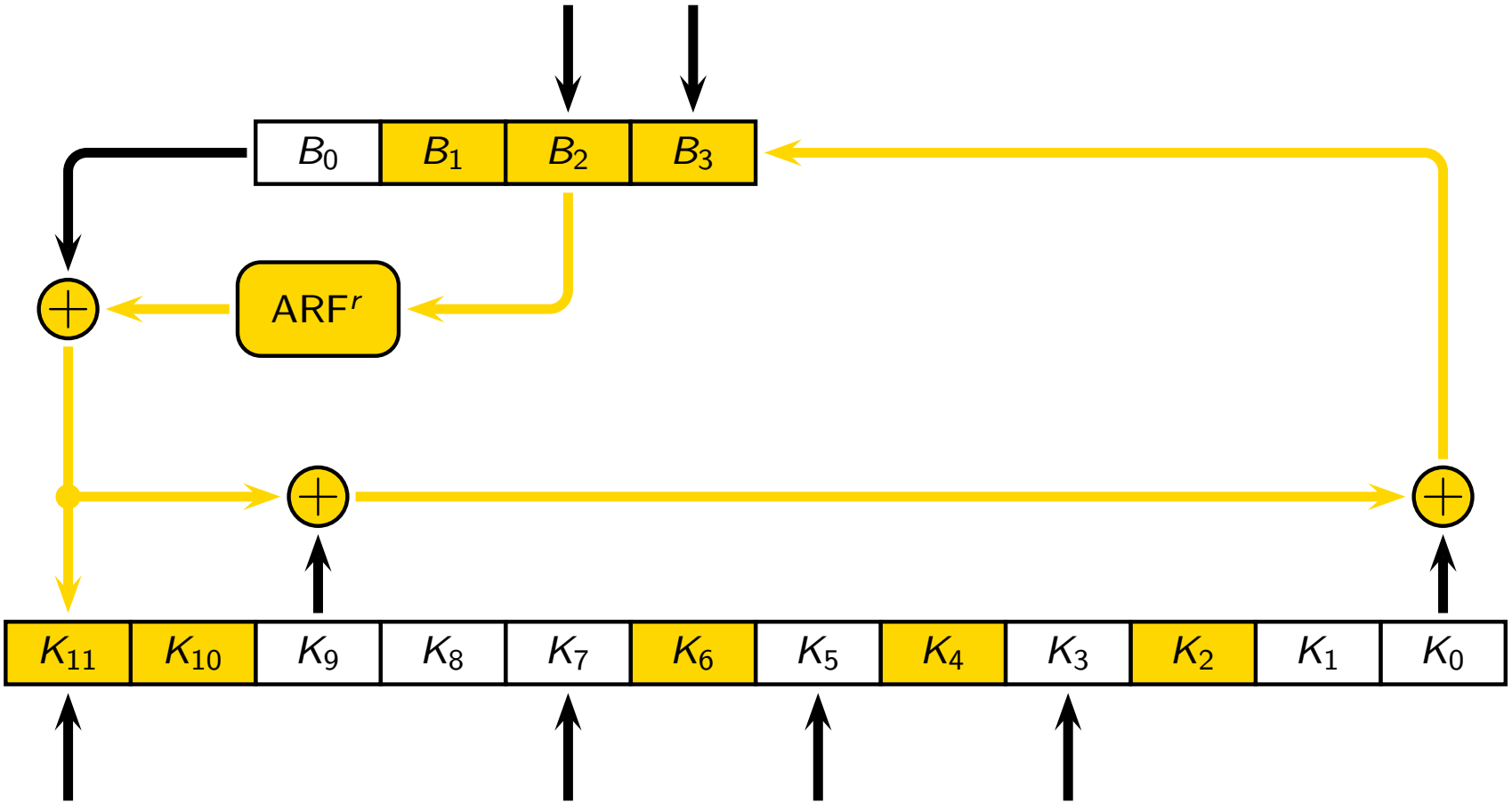
On a Collision Course



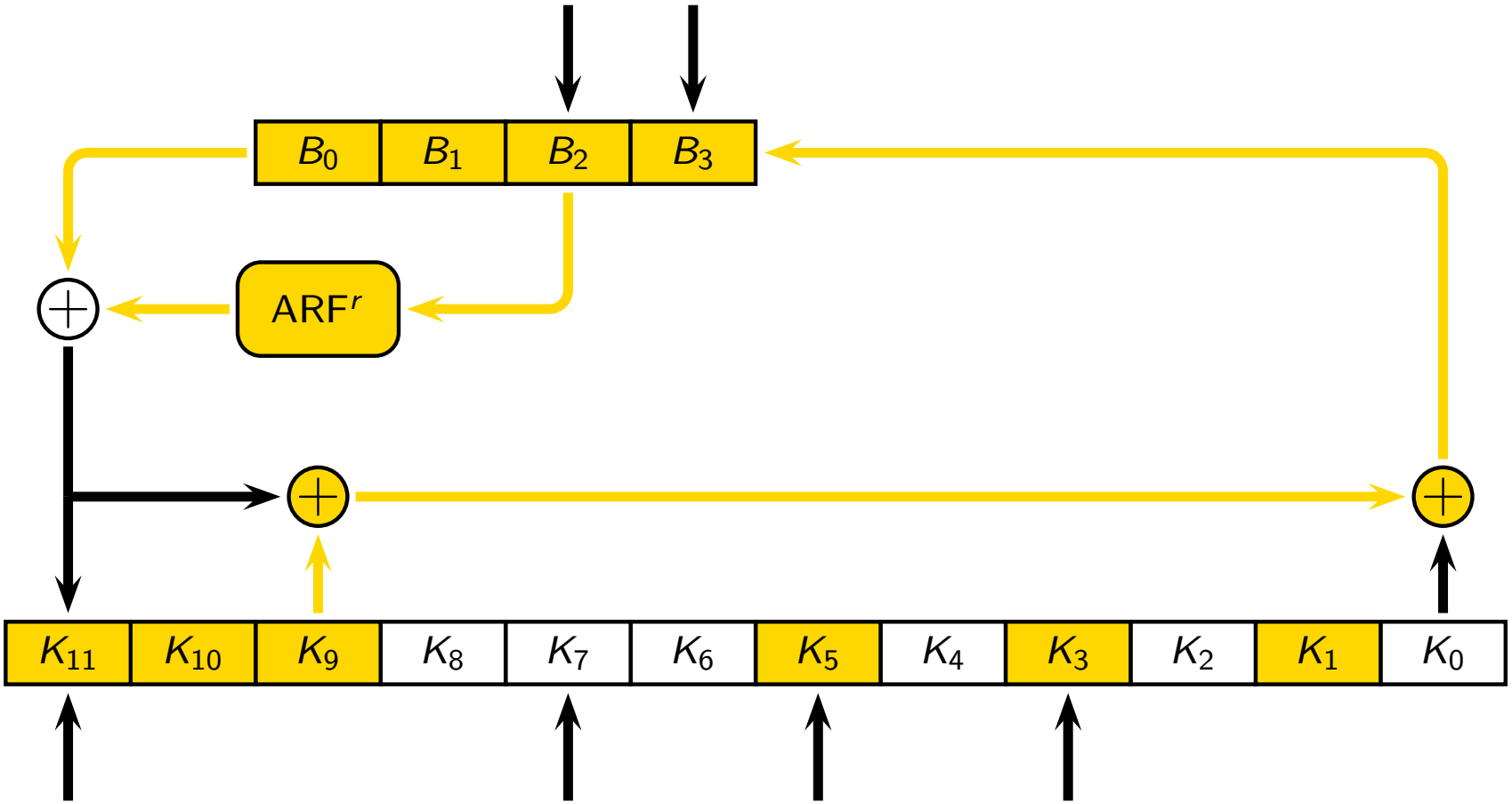
On a Collision Course



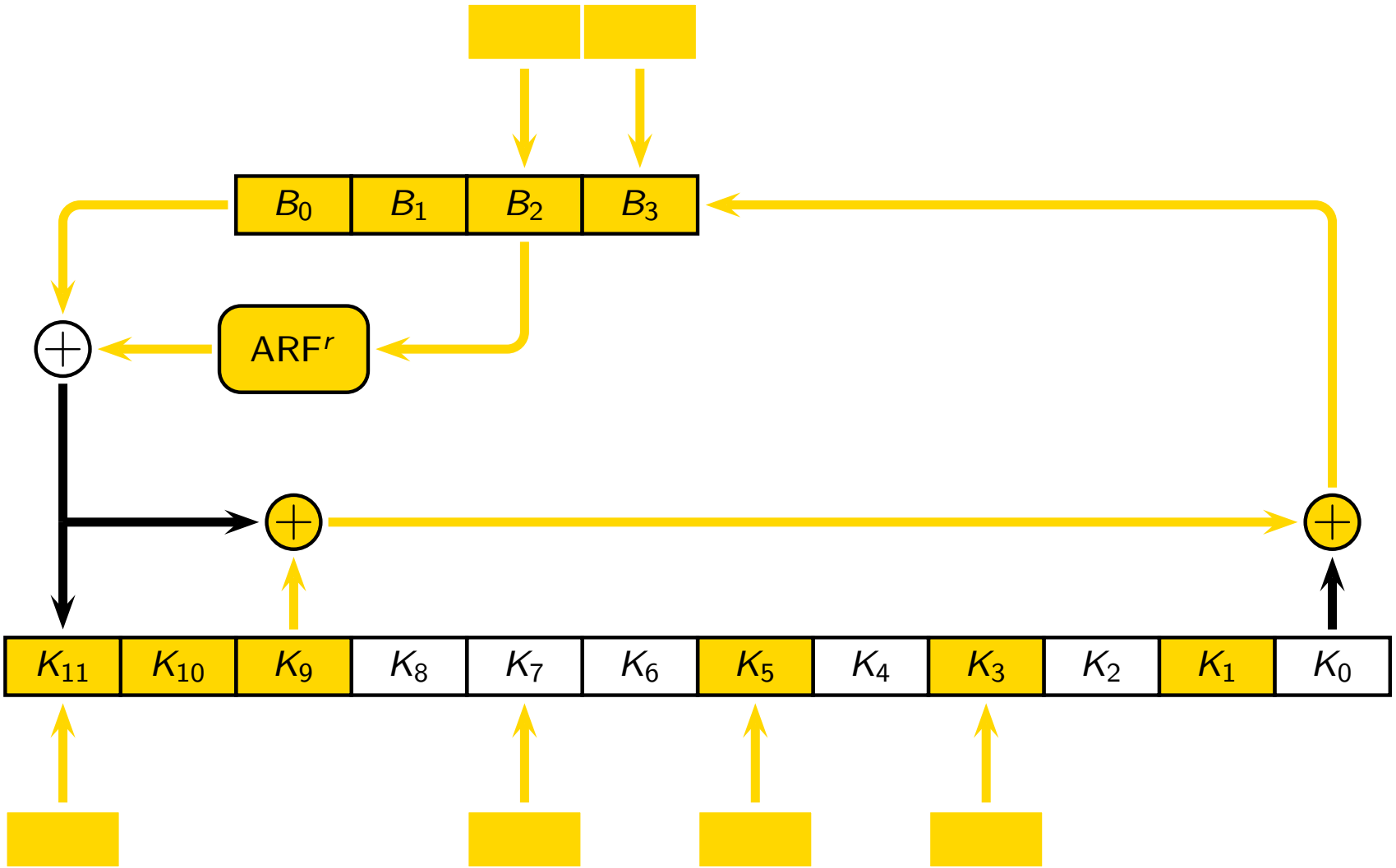
On a Collision Course



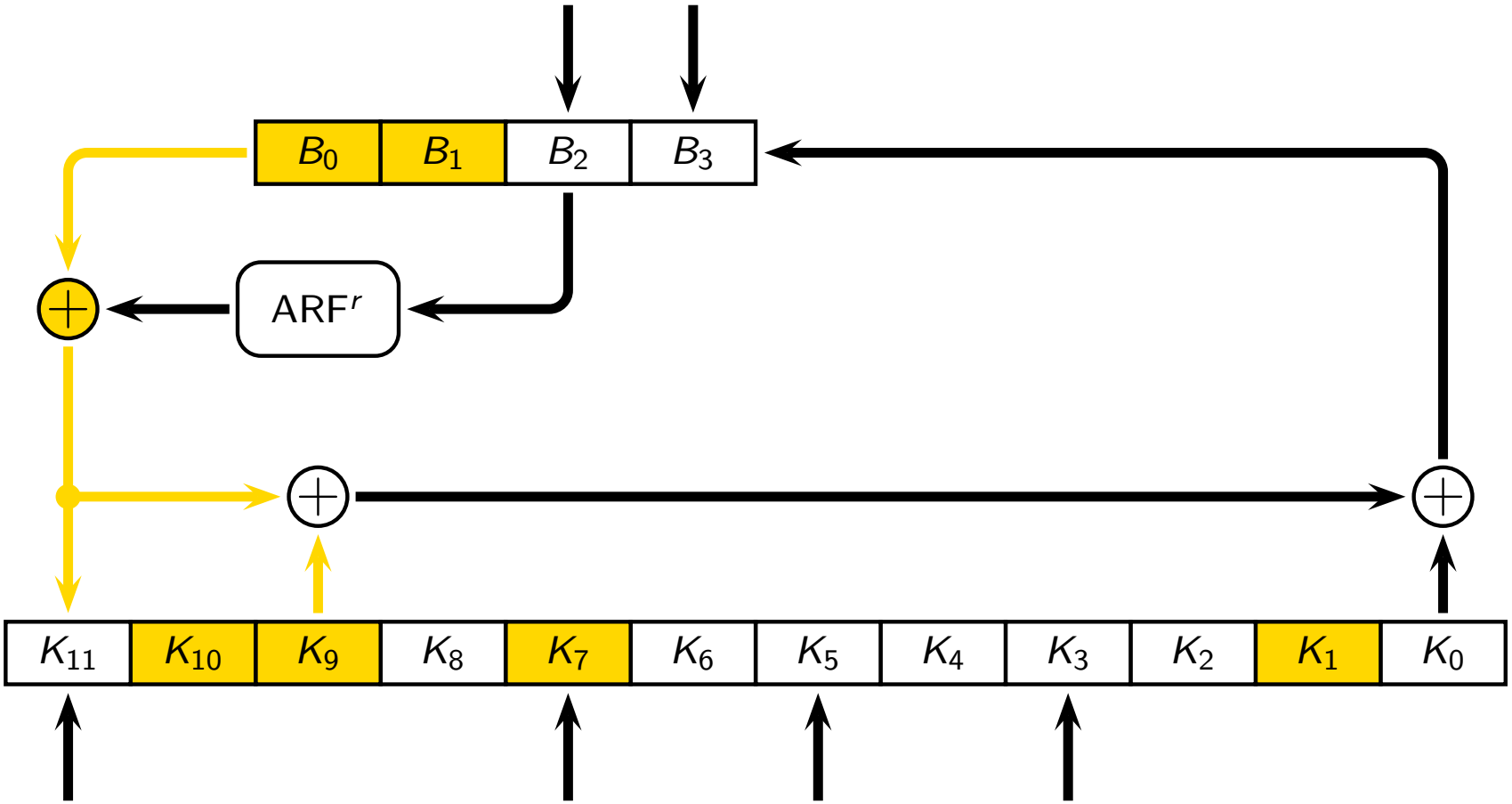
On a Collision Course



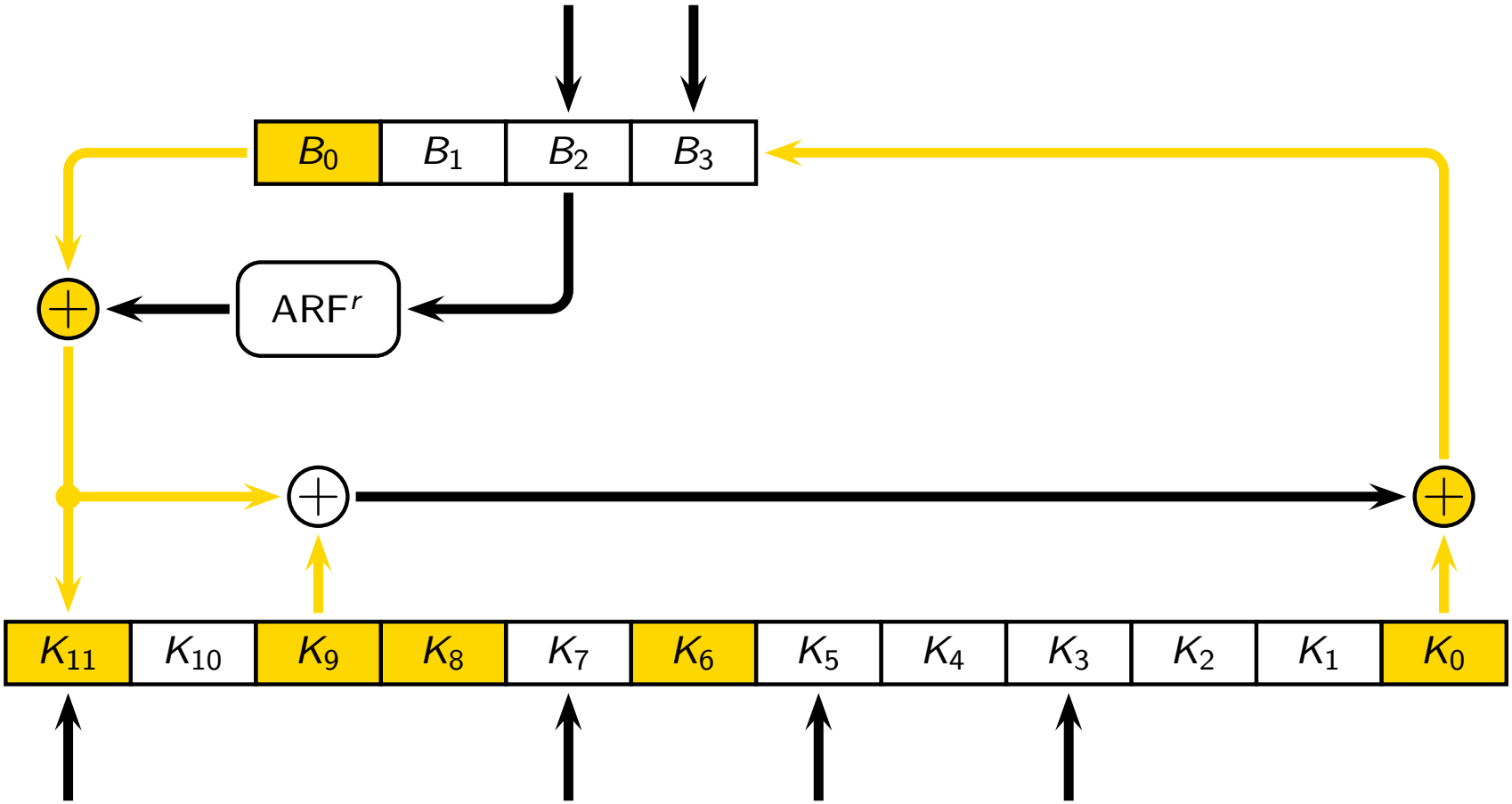
On a Collision Course



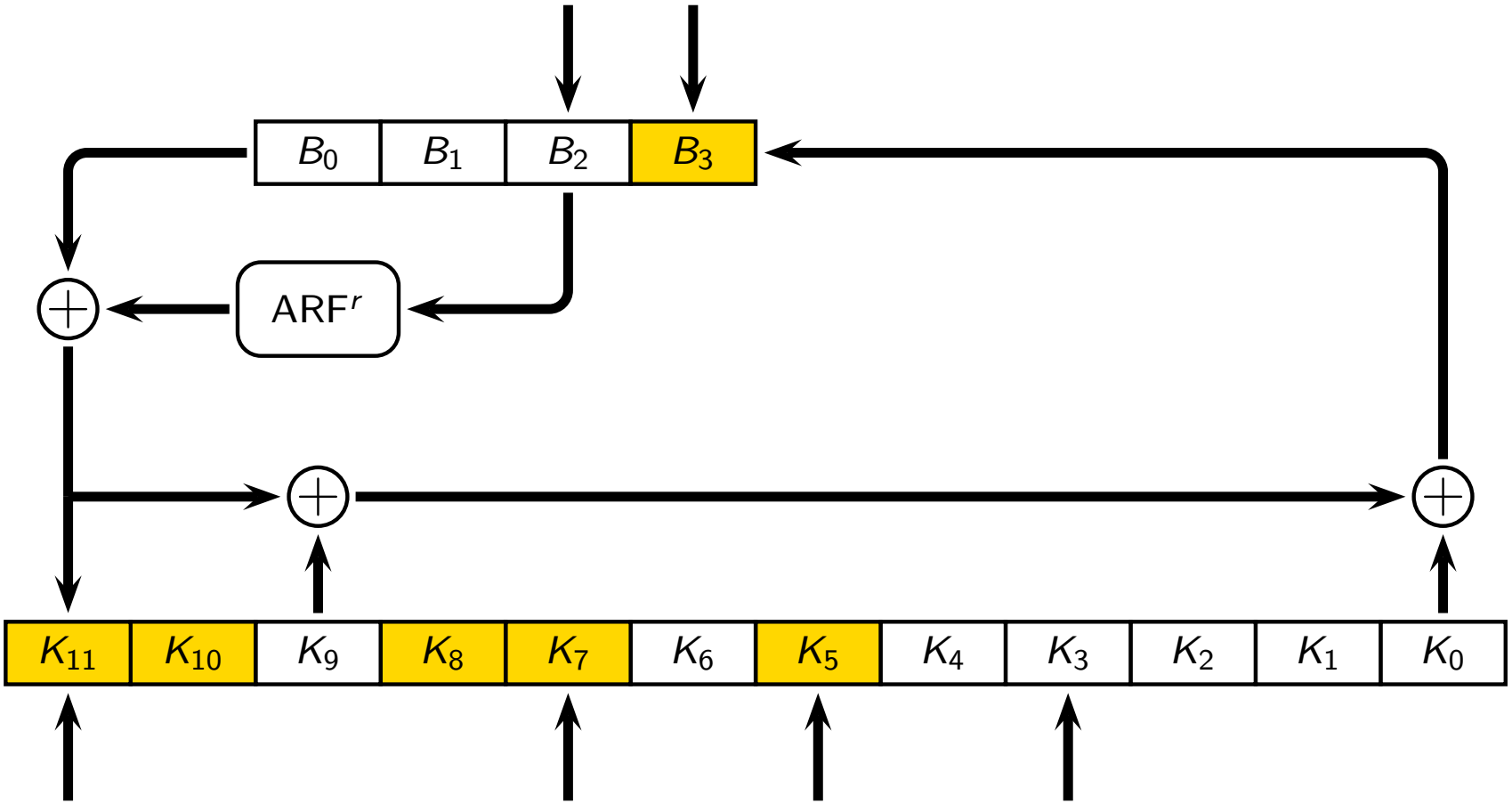
On a Collision Course



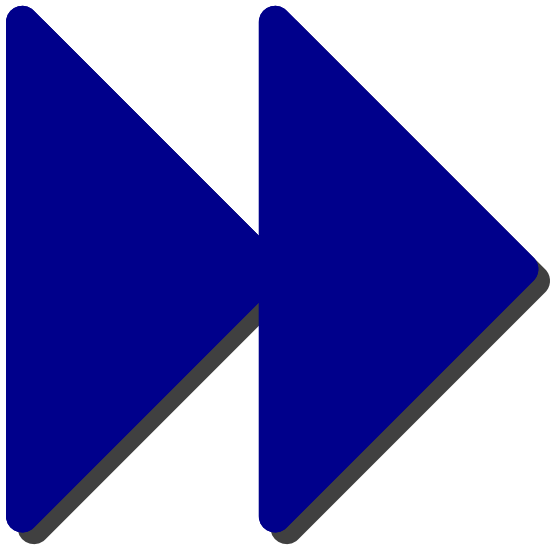
On a Collision Course



On a Collision Course

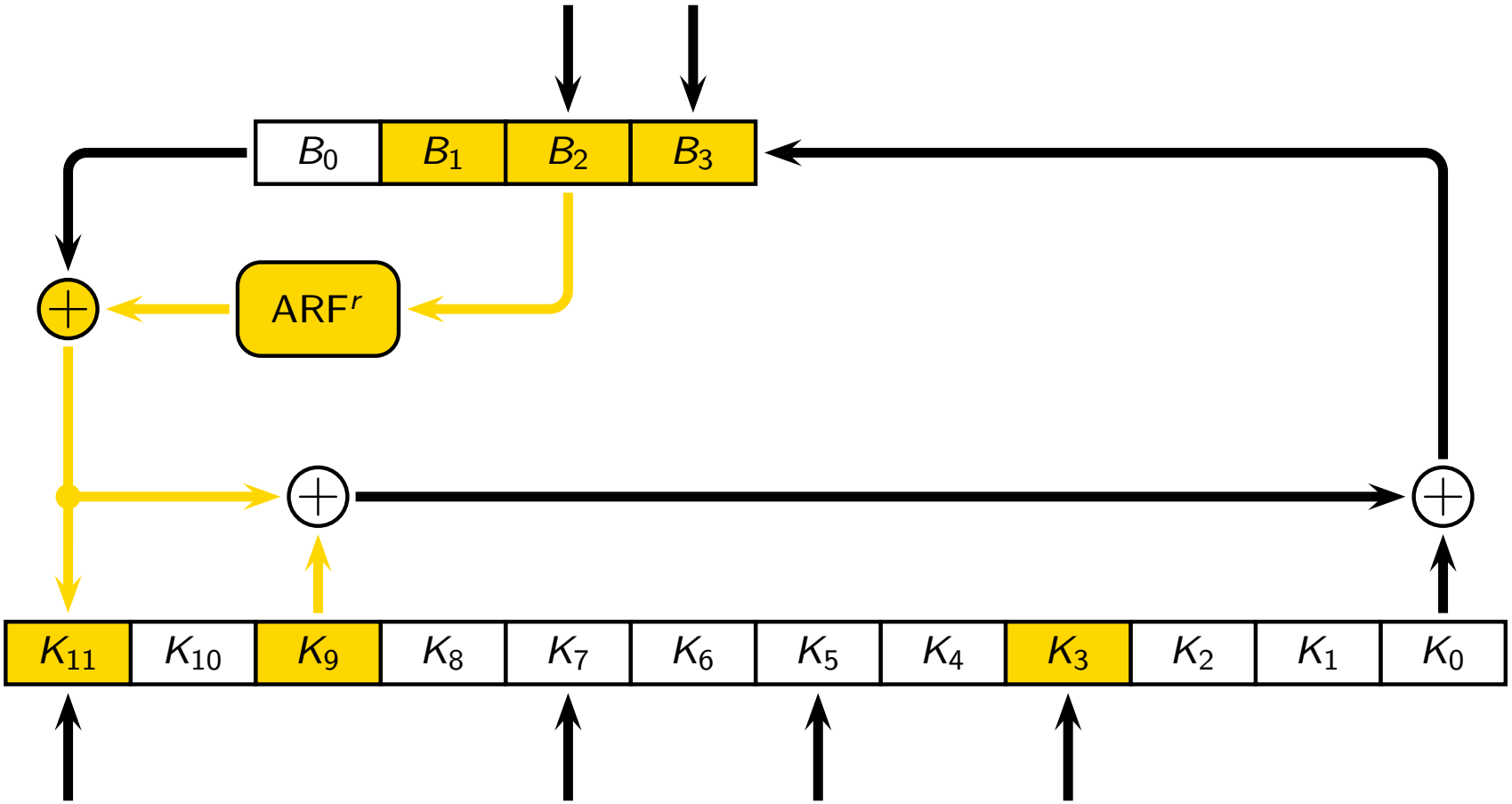


On a Collision Course

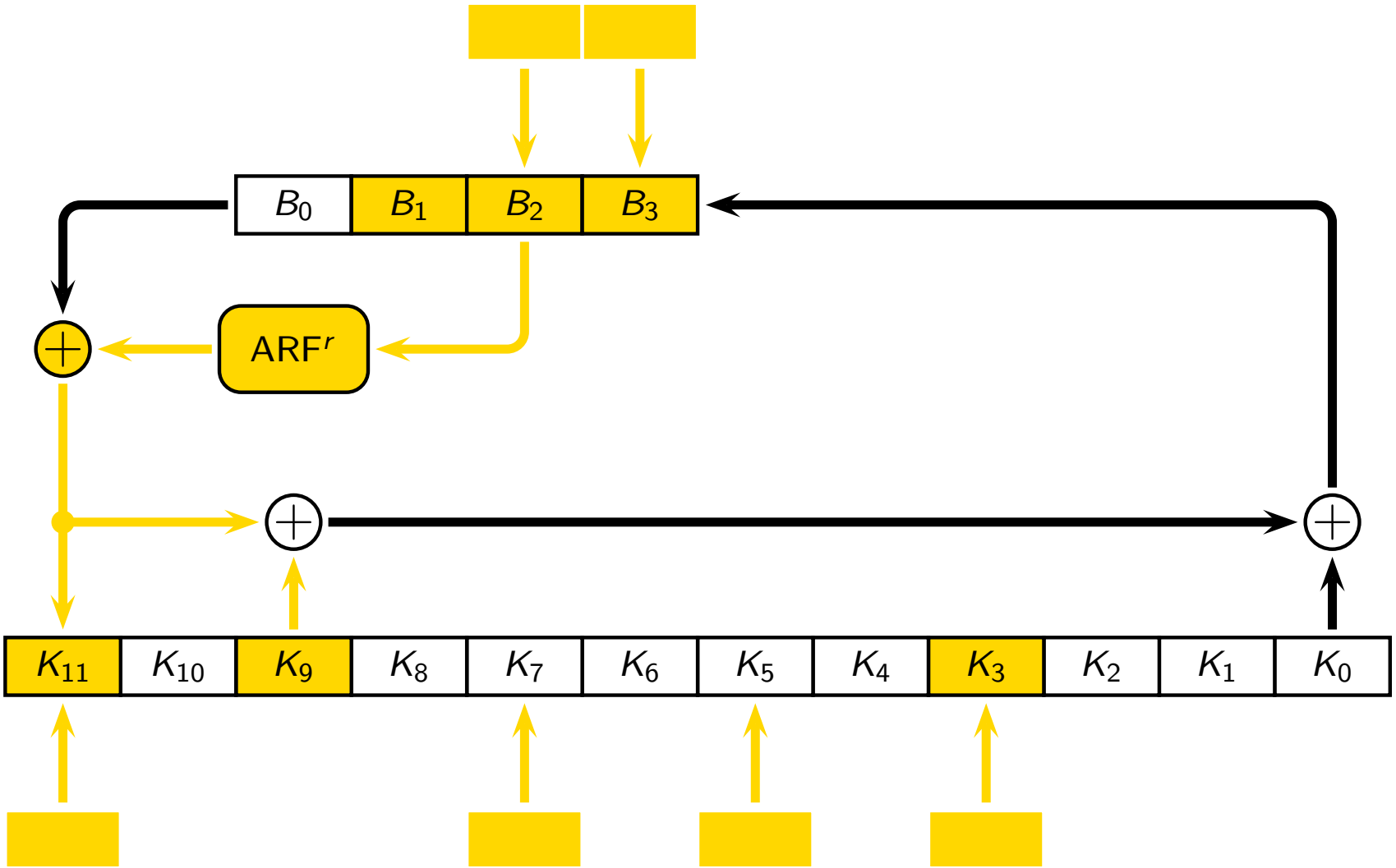


Fast Forward

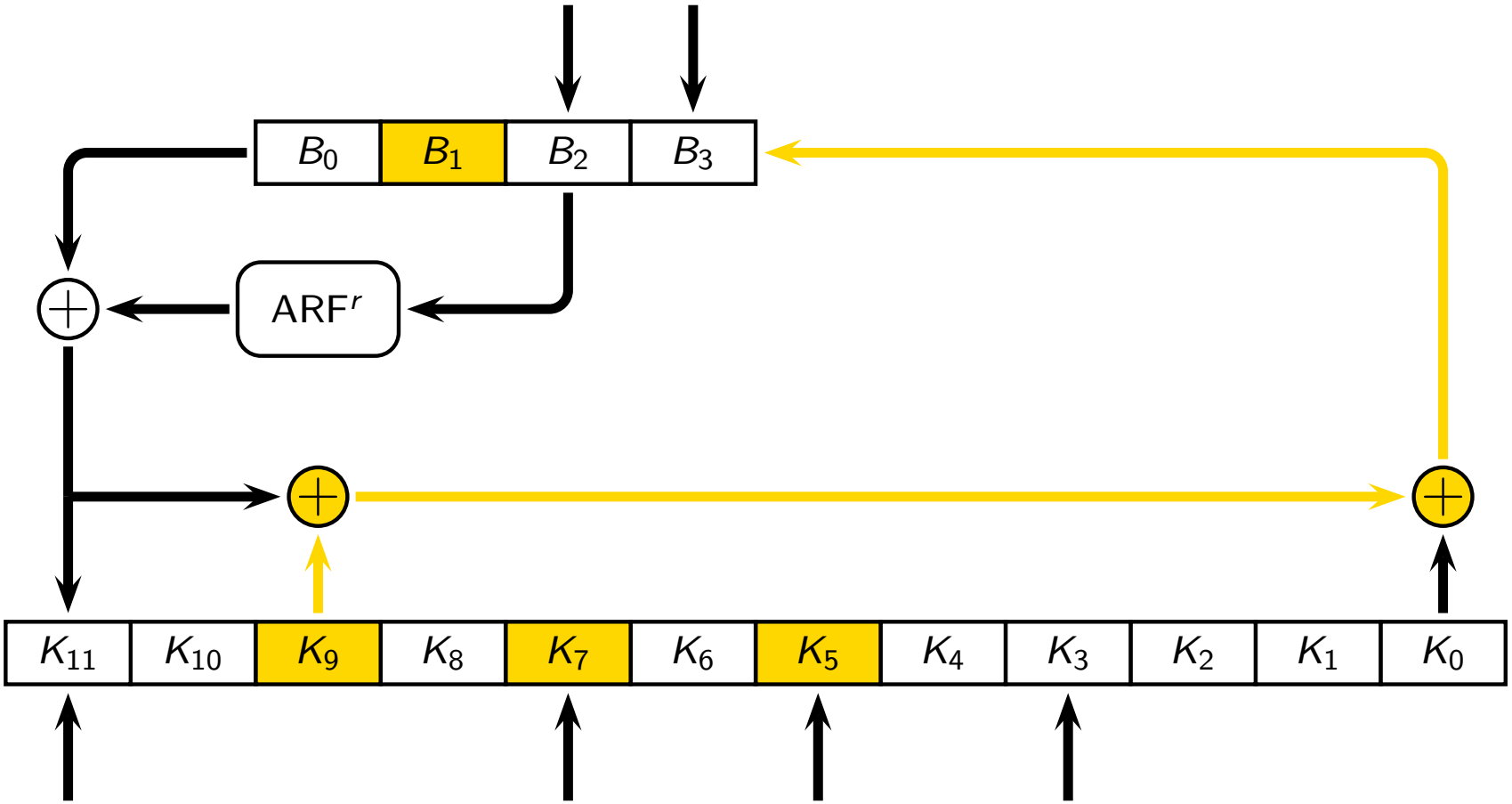
On a Collision Course



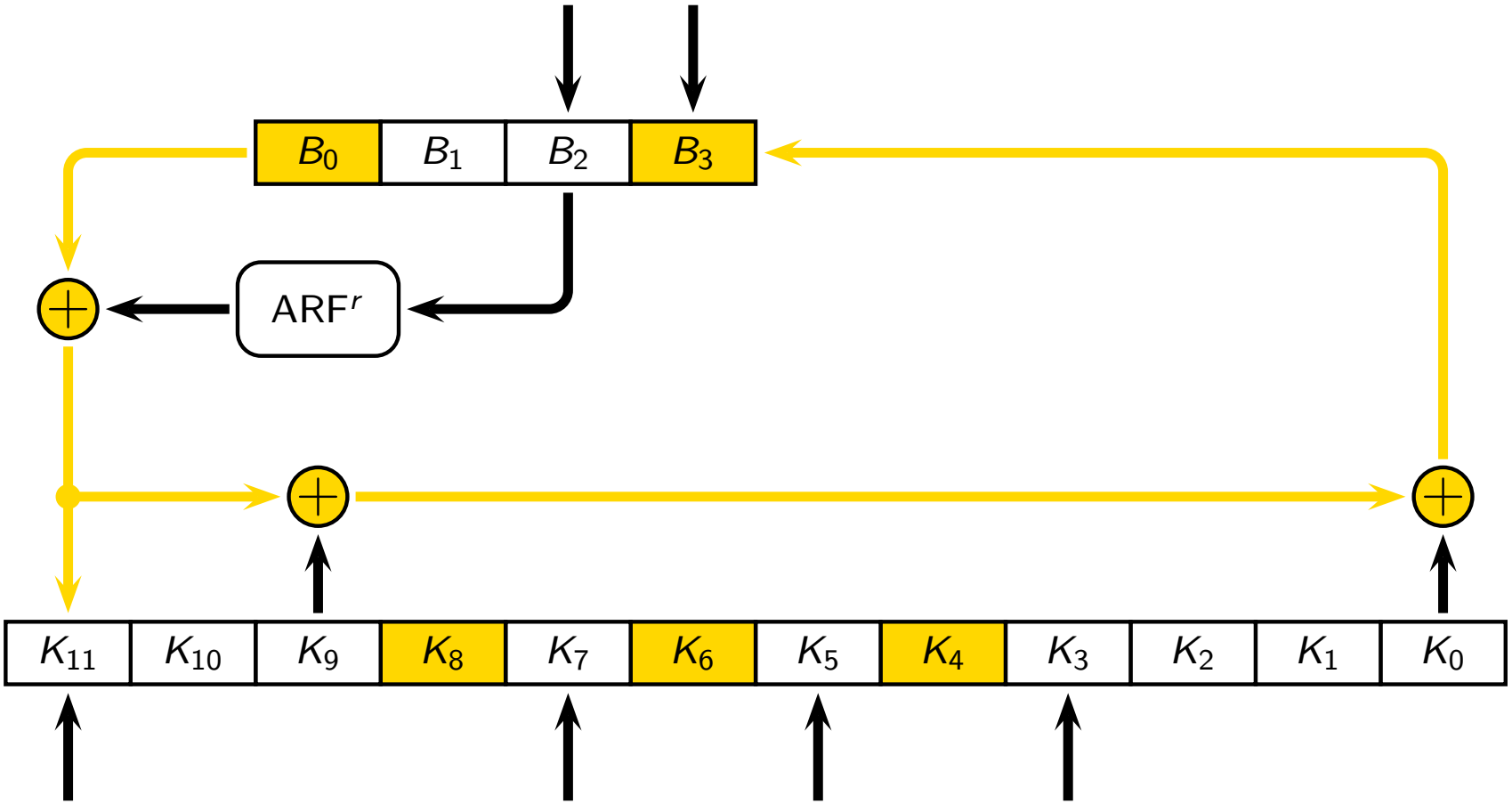
On a Collision Course



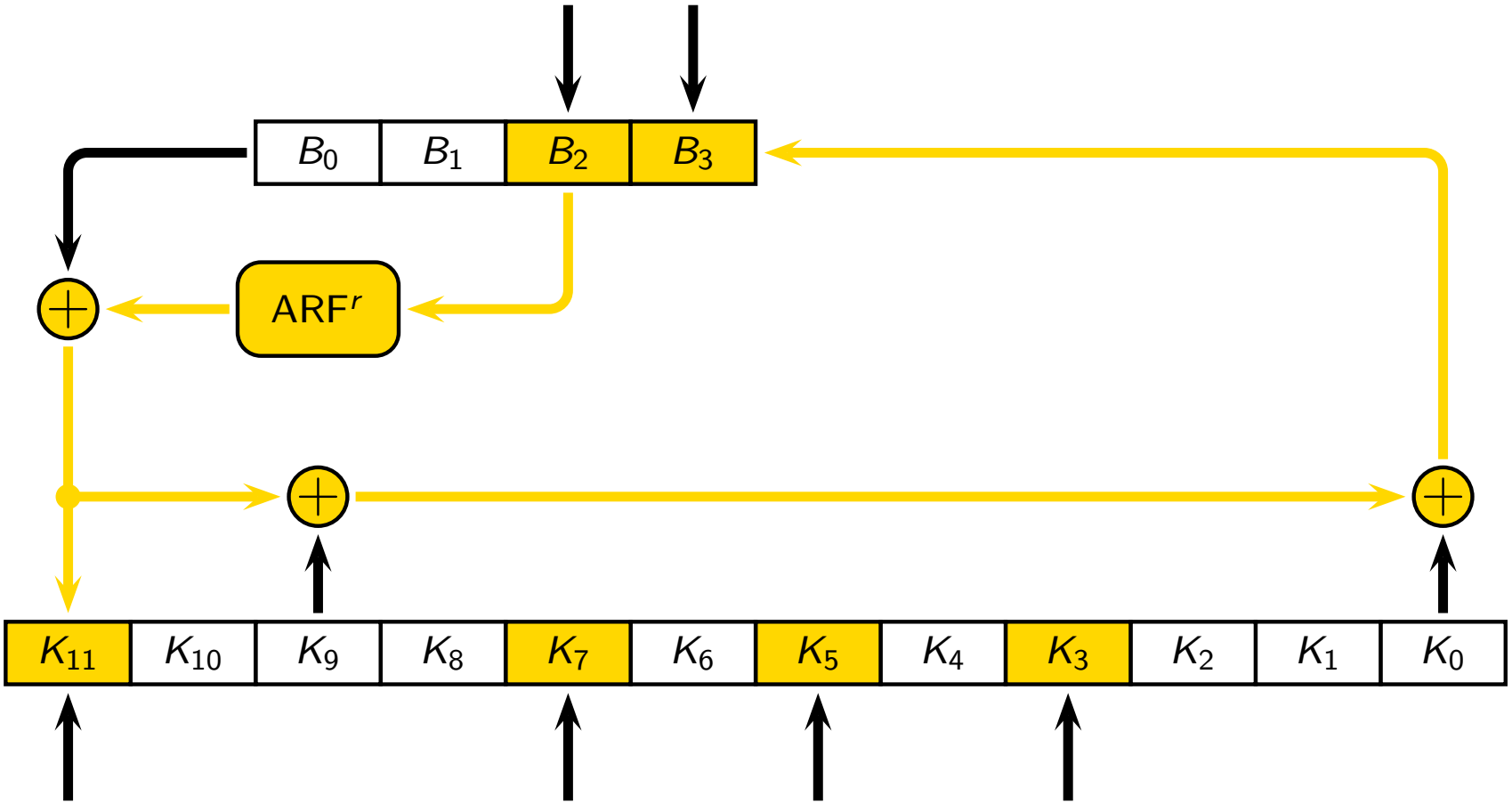
On a Collision Course



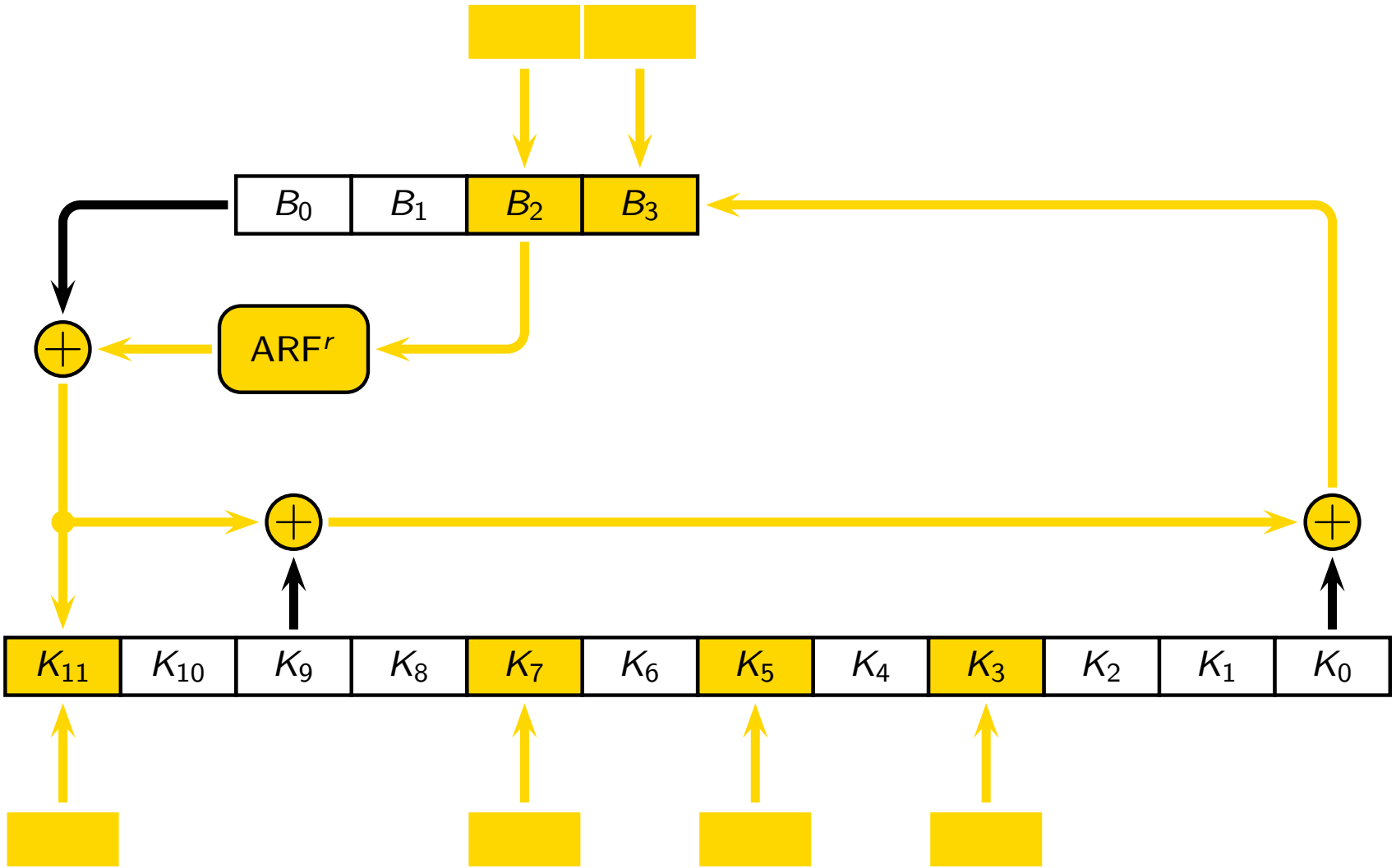
On a Collision Course



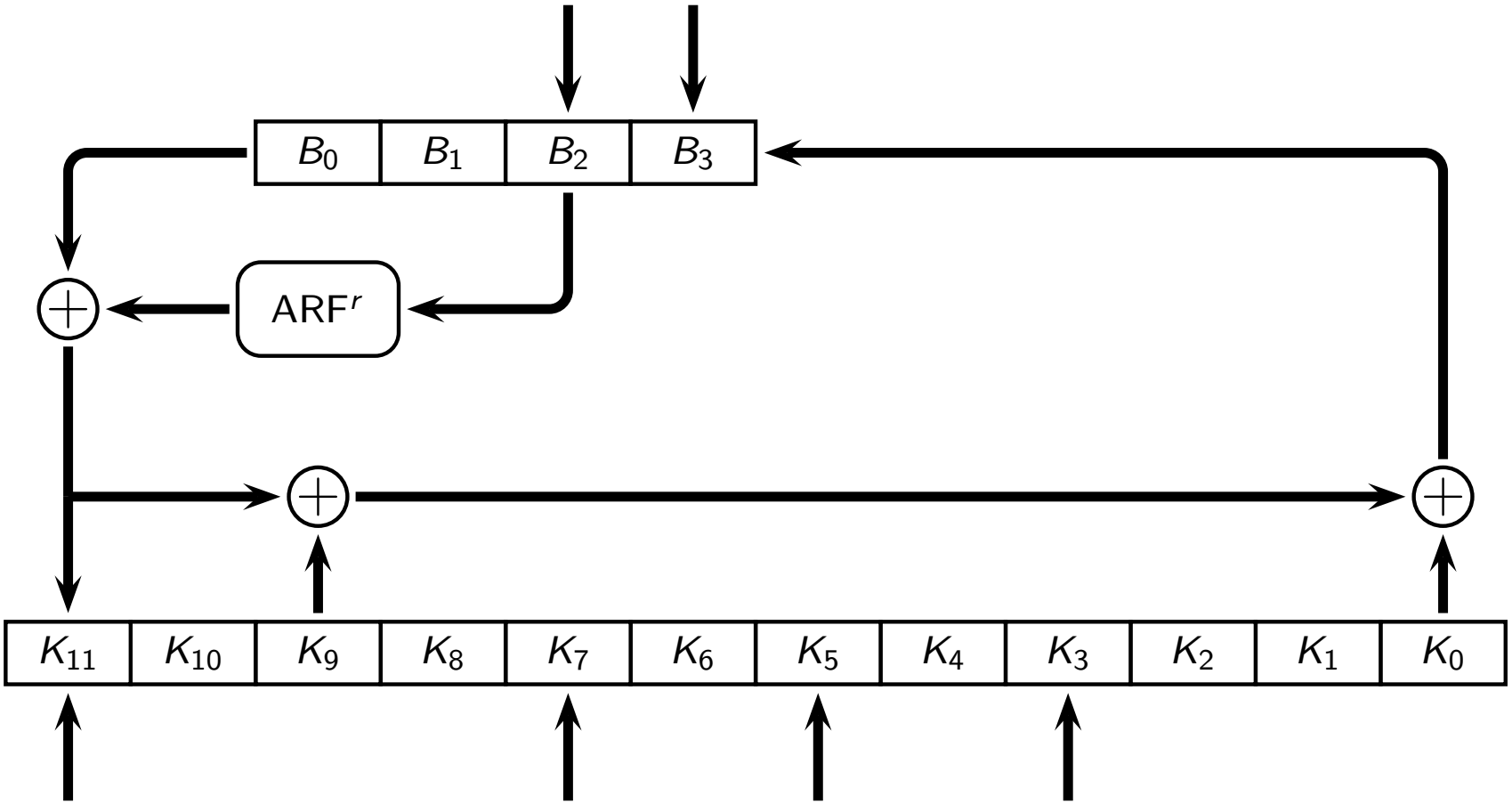
On a Collision Course



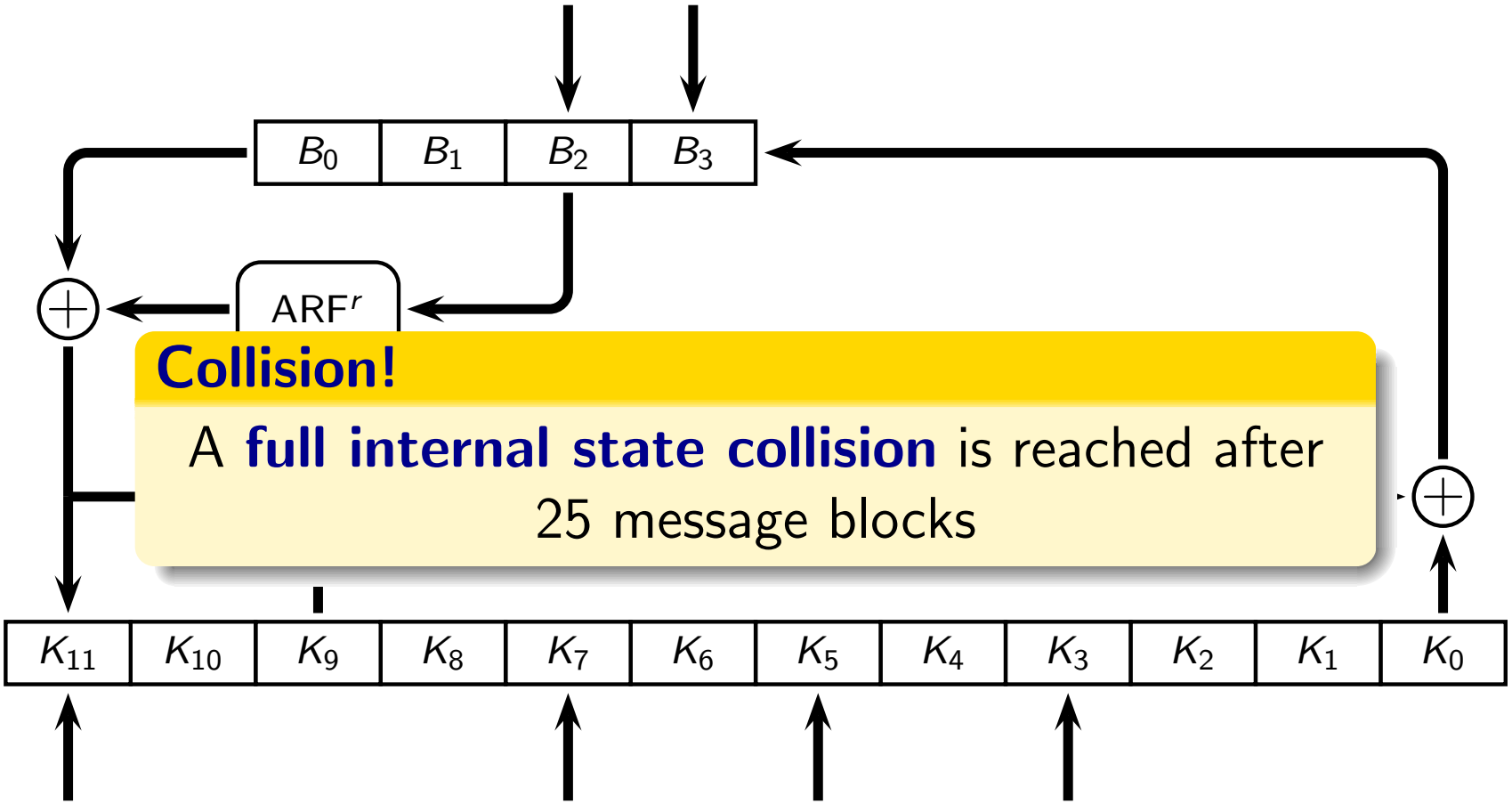
On a Collision Course



On a Collision Course



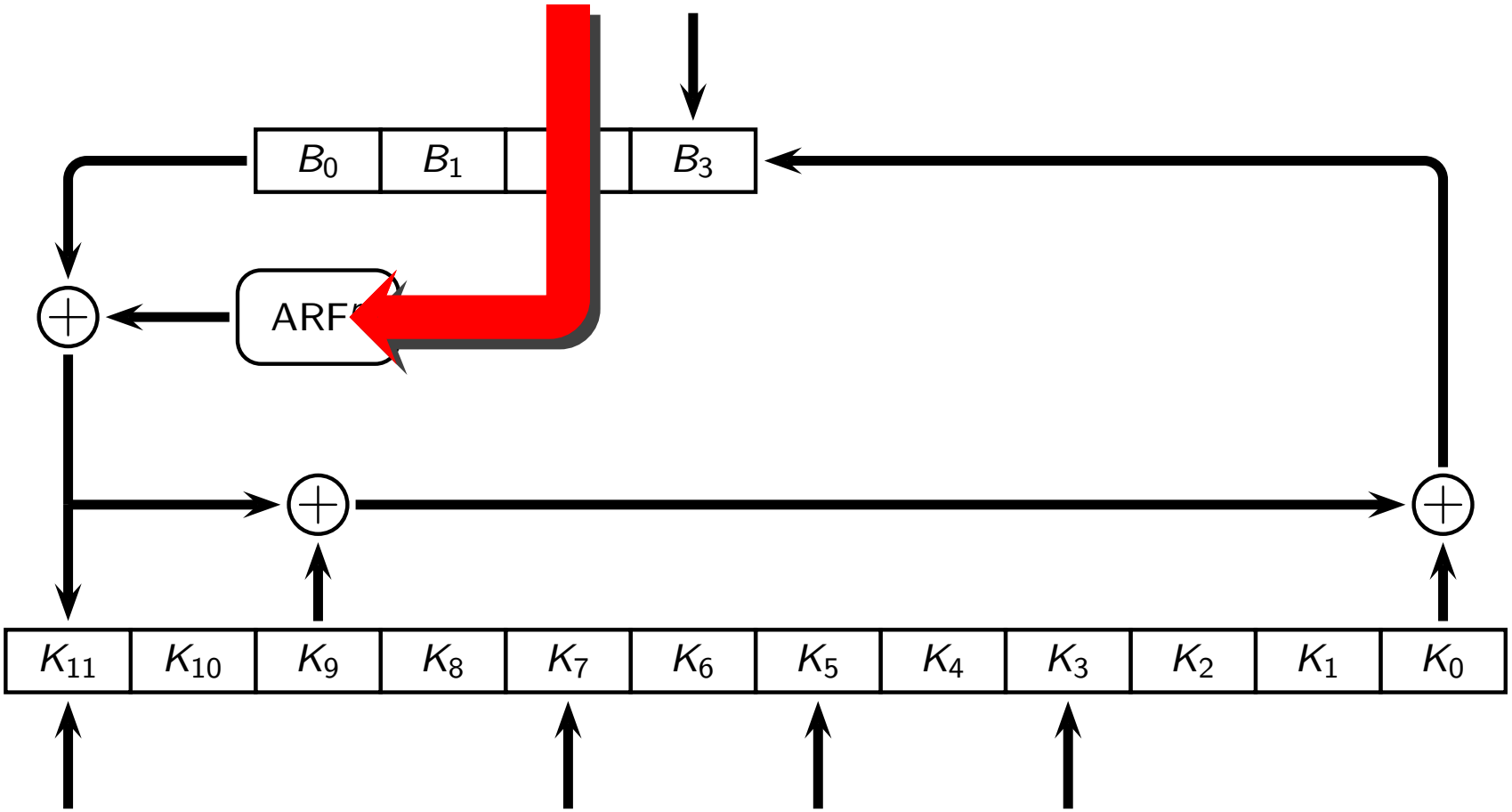
On a Collision Course



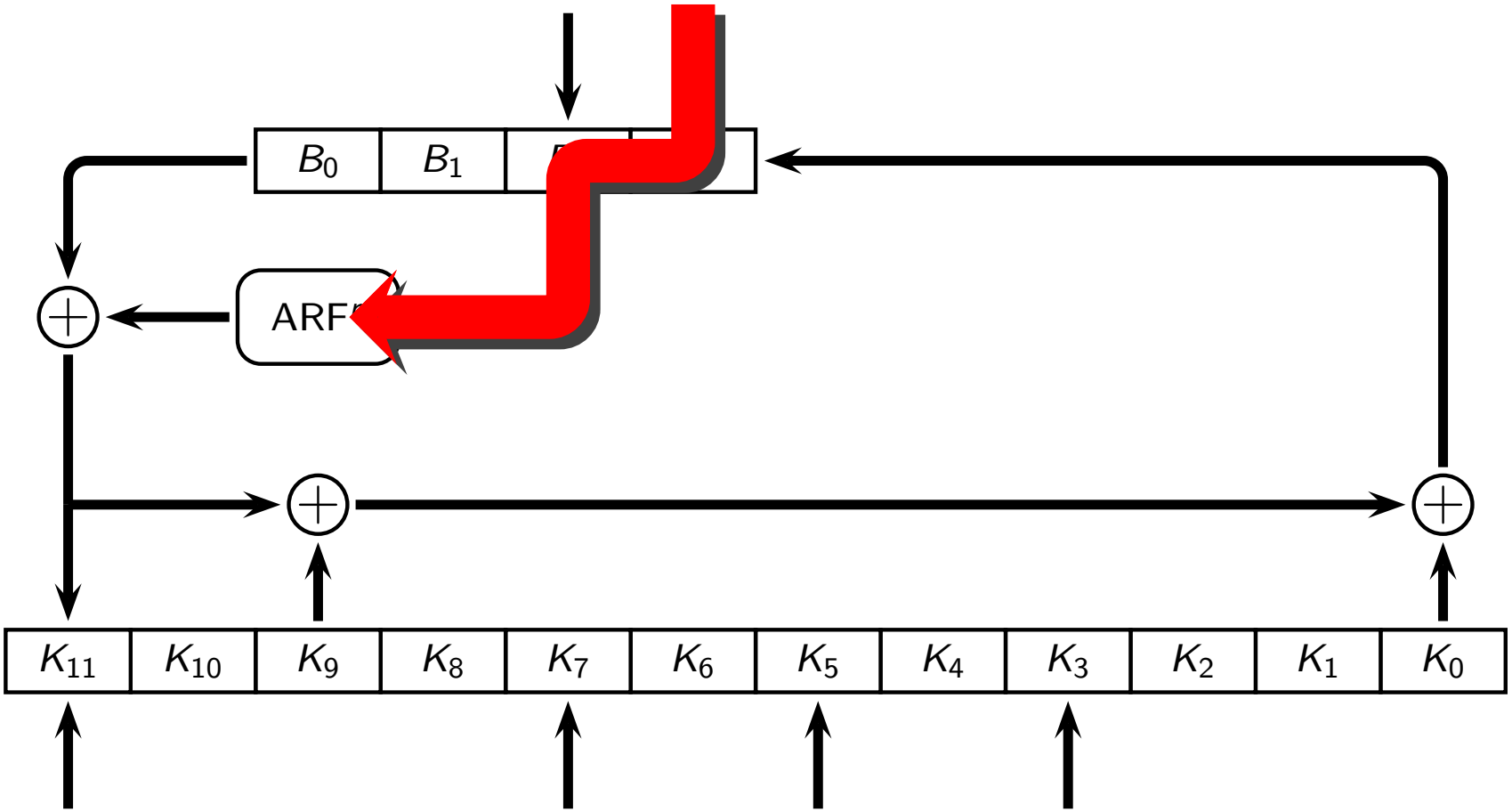
Collision!

A **full internal state collision** is reached after 25 message blocks

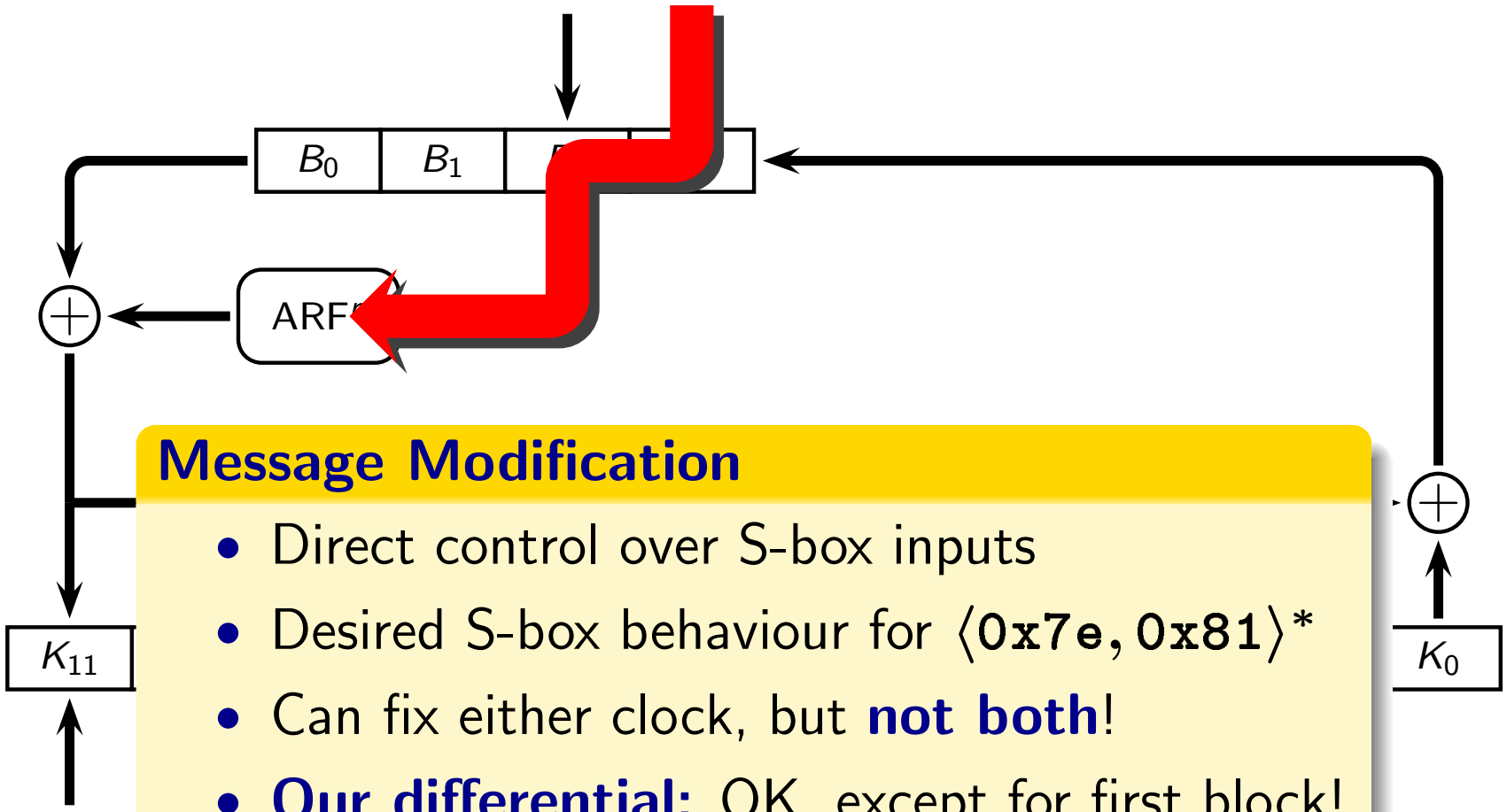
Taming the S-Boxes



Taming the S-Boxes



Taming the S-Boxes



Message Modification

- Direct control over S-box inputs
- Desired S-box behaviour for $\langle \texttt{0x7e}, \texttt{0x81} \rangle$*
- Can fix either clock, but **not both**!
- **Our differential:** OK, except for first block!

*SHAMATA-256

A Beginning is a Very Delicate Time...

Problem: Not enough freedom in first block
Solution: Find a suitable prefix block

SHAMATA-256

- **Trick:** Guess-and-determine & meet-in-the-middle
- $\mathcal{O}(2^{40})$ time, $\mathcal{O}(2^{24})$ memory
- Practice: 256×5 min., 700 MB memory

SHAMATA-512

- Same differential can be used
- 2 AES rounds, so trick fails ☹
- Brute force still works ☺
- $\mathcal{O}(2^{128})$ time

Veni, Vidi, Conflixi *

```
Example collision pair for SHAMATA-256
Florian Mendel, Martin Schlaeffer, Christian Rechberger (IAIK, T.U.Graz),
Sebastiaan Indesteege (COSIC, K.U.Leuven)

m1 =
00000000: 10 37 fd e7 65 30 1c c0 e3 61 6e 41 24 6f cb b9 |.7..e0...anA$o..|
00000010: 7f 28 81 17 81 4a d1 3f bf 4e ca da 92 f5 35 d0 |.(...J.?.N....5.|
00000020: f0 f0 dc 19 73 d5 a7 07 8c 0b bc 3d b6 85 46 57 |....s......=..FW|
00000030: 02 92 d1 24 00 df 40 67 ca 2c fa 5b 9d 70 2c ce |...$..@g.,.[.p,.|
00000040: de 38 51 f5 01 3c 3b aa d8 ba 38 0e a1 40 b1 91 |.8Q..<;...8..@..|
00000050: 7b 18 18 24 cc d9 76 c0 f7 4a 61 28 86 06 30 8e |{..$..v..Ja(..0.|
00000060: 30 8d ab a3 62 52 aa ee 5d 66 2b 13 ec 71 6b ca |0...bR..]f+..qk.|
00000070: e3 29 f2 2c b3 ed 3d 7e f7 f2 fd 0b 1e c7 d6 e5 |.).,..=~........|
00000080: aa bc bf ab f9 fb 56 d1 b5 8e df 57 ce 90 e8 fe |......V....W....|
00000090: 1e 93 a2 80 e6 4c 6f 43 b3 9a 57 9f 0c c2 69 b6 |.....LoC..W...i.|
000000a0: 7e 29 61 77 24 b7 48 d9 45 27 30 13 b8 19 12 d6 |~)aw$.H.E'0.....|
000000b0: ac b4 56 92 00 c5 d6 b3 60 2d 52 6c ef bc 22 6d |..V.....`-Rl.."m|
000000c0: e5 83 e5 09 3b 2d e2 80 55 13 94 0d 2c a6 e3 d8 |....;-..U...,...|
000000d0: 53 e9 01 66 72 ae 8d cf 68 25 8a b6 ae 64 e7 c1 |S..fr...h%...d..|
000000e0: 5a 39 6b 5a ff 41 0e 5f 6e 60 cb 5d 1c ed ca 01 |Z9kZ.A._n`.]....|
000000f0: 70 af 0a ab dd ed 2c 32 00 c0 3f 2c 66 22 04 c0 |p.....,2..?,f"..|
00000100: 3b 97 65 9d 01 64 98 7b e6 63 d4 d6 4b 77 00 bb |;.e..d.{.c..Kw..|
00000110: bb ac 35 e3 27 66 55 34 0c 0f db d7 2f 16 19 ae |..5.'fU4..../...|
00000120: 5b 6f 1a 5a b0 28 b9 1e 89 84 7b a5 71 46 a7 e2 |[o.Z.(....{.qF..|
00000130: f5 b1 8d d2 9e b9 04 9e 79 43 ca df 65 cf 9f c1 |........yC..e...|
00000140: bb f6 43 f9 cd 88 af 13 ea 2f 93 e8 cd 39 8c a0 |..C....../...9..|
00000150: 3e ba 1b ef e2 d5 0d 6b 59 89 11 cb cf b8 ad c4 |>.......kY.......|
00000160: 1a 3f 2f 9d a3 1d 82 3c e0 75 9d 83 b2 ac 3c bf |.?/....<.u....<.|
00000170: e0 27 0c c5 af b0 be a9 94 1e de 9d 50 69 10 cb |.'..........Pi..|
00000180: 69 3a 97 08 f4 9b a6 6d df 71 4d 44 40 ec 05 7e |i:.....m.qMD@..~|
00000190: a6 21 6d 89 f6 7b f4 4f 04 05 1a d3 bd c7 97 27 |.!m..{.O.......'|

SHAMATA-256(m1) =
00000000: 6e a3 b1 a1 29 75 8d 3f f5 60 f8 1b 6b 11 02 9a |n...)u.?.`..k...|
00000010: 14 b9 b2 d9 b3 2a b6 02 2a f5 83 ab e3 4c 1a 2a |.....*..*....L.*|
```

```
m2 =
00000000: 10 37 fd e7 65 30 1c c0 e3 61 6e 41 24 6f cb b9 |.7..e0...anA$o..|
00000010: 80 d7 7e e8 7e b5 2e c0 40 b1 35 25 6d 0a ca 2f |..~.~...@.5%m../|
00000020: 0f 0f 23 e6 8c 2a 58 f8 73 f4 43 c2 49 7a b9 a8 |..#..*X.s.C.Iz..|
00000030: fd 6d 2e db ff 20 bf 98 35 d3 05 a4 62 8f d3 31 |.m... ..5...b..1|
00000040: 21 c7 ae 0a fe c3 c4 55 27 45 c7 f1 5e bf 4e 6e |!......U'E..^.Nn|
00000050: 7b 18 18 24 cc d9 76 c0 f7 4a 61 28 86 06 30 8e |{..$..v..Ja(..0.|
00000060: 30 8d ab a3 62 52 aa ee 5d 66 2b 13 ec 71 6b ca |0...bR..]f+..qk.|
00000070: 1c d6 0d d3 4c 12 c2 81 08 0d 02 f4 e1 38 29 1a |....L........8).|
00000080: 55 43 40 54 06 04 a9 2e 4a 71 20 a8 31 6f 17 01 |UC@T....Jq .1o..|
00000090: 1e 93 a2 80 e6 4c 6f 43 b3 9a 57 9f 0c c2 69 b6 |.....LoC..W...i.|
000000a0: 81 d6 9e 88 db 48 b7 26 ba d8 cf ec 47 e6 ed 29 |.....H.&....G..)|
000000b0: ac b4 56 92 00 c5 d6 b3 60 2d 52 6c ef bc 22 6d |..V.....`-Rl.."m|
000000c0: e5 83 e5 09 3b 2d e2 80 55 13 94 0d 2c a6 e3 d8 |....;-..U...,...|
000000d0: ac 16 fe 99 8d 51 72 30 97 da 75 49 51 9b 18 3e |.....Qr0..uIQ..>|
000000e0: 5a 39 6b 5a ff 41 0e 5f 6e 60 cb 5d 1c ed ca 01 |Z9kZ.A._n`.]....|
000000f0: 8f 50 f5 54 22 12 d3 cd ff 3f c0 d3 99 dd fb 3f |.P.T"....?.....?|
00000100: 3b 97 65 9d 01 64 98 7b e6 63 d4 d6 4b 77 00 bb |;.e..d.{.c..Kw..|
00000110: 44 53 ca 1c d8 99 aa cb f3 f0 24 28 d0 e9 e6 51 |DS........$(...Q|
00000120: a4 90 e5 a5 4f d7 46 e1 76 7b 84 5a 8e b9 58 1d |....O.F.v{.Z..X.|
00000130: 0a 4e 72 2d 61 46 fb 61 86 bc 35 20 9a 30 60 3e |.Nr-aF.a..5 .0`>|
00000140: bb f6 43 f9 cd 88 af 13 ea 2f 93 e8 cd 39 8c a0 |..C....../...9..|
00000150: 3e ba 1b ef e2 d5 0d 6b 59 89 11 cb cf b8 ad c4 |>.......kY.......|
00000160: 1a 3f 2f 9d a3 1d 82 3c e0 75 9d 83 b2 ac 3c bf |.?/....<.u....<.|
00000170: e0 27 0c c5 af b0 be a9 94 1e de 9d 50 69 10 cb |.'..........Pi..|
00000180: 69 3a 97 08 f4 9b a6 6d df 71 4d 44 40 ec 05 7e |i:.....m.qMD@..~|
00000190: 59 de 92 76 09 84 0b b0 fb fa e5 2c 42 38 68 d8 |Y..v.......,B8h.|

SHAMATA-256(m2) =
00000000: 6e a3 b1 a1 29 75 8d 3f f5 60 f8 1b 6b 11 02 9a |n...)u.?.`..k...|
00000010: 14 b9 b2 d9 b3 2a b6 02 2a f5 83 ab e3 4c 1a 2a |.....*..*....L.*|

m1 and m2 collide!
```

* I came, I saw, I collided

The End

Mitigating the Attack?

- More clocks per message block
- More AES rounds + round constants
- ...

Conclusion

- Collision attacks on SHAMATA
- Practical collisions for SHAMATA-256