Proudová šifra A5/1

Andrew Kozlik

KA MFF UK

Proudová šifra A5/1

- A5/1 je proudová šifra používaná v síti GSM.
- Šifruje komunikaci mezi mobilním telefonem a základnovou stanicí (Base Transceiver Station neboli BTS).
- Šifrovací algoritmus byl tajný.
- V r. 1994 unikl jeho obecný popis.
- V r. 1999 byl podrobně popsán na základě reverzního inženýrství běžného mobilního telefonu.

Proudová šifra A5/1

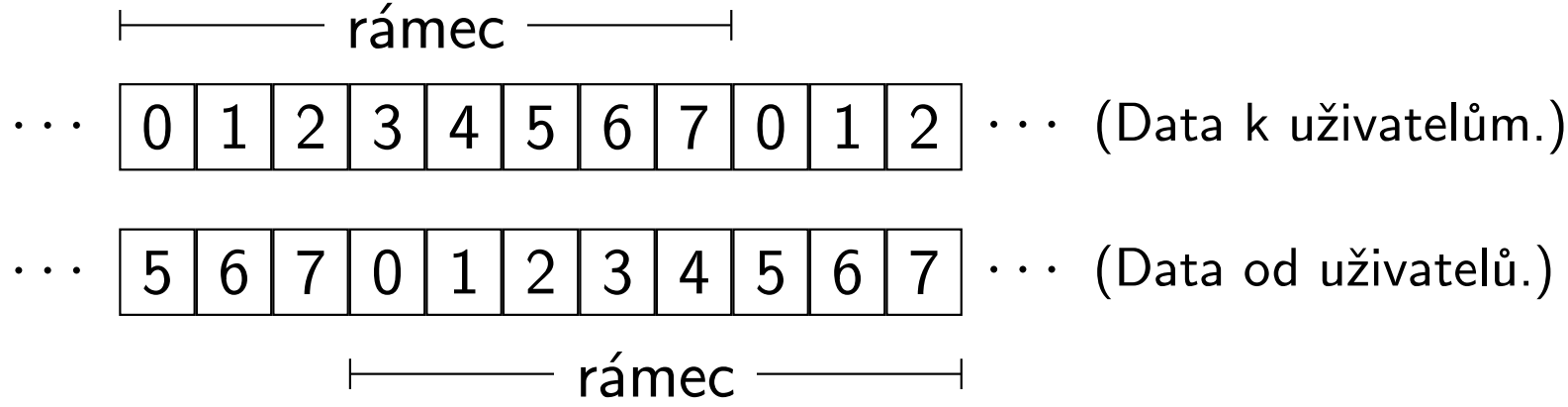
- Kromě A5/1 se v GSM využívají další algoritmy:

A5/2	slabý šifrovací algoritmus „na vývoz“ (vznikl z iniciativy výzvědných služeb)
A5/3	novější bezpečnější šifrovací algoritmus
A3	autentizační algoritmus
A8	algoritmus generování šifrovacího klíče

- Na SIM kartě je uložen sdílený klíč K_i.
- Před zahájením hovoru se z K_i a náhodné 128bitové hodnoty spočte šifrovací klíč K_c a autentizační kód.
- Při šifrování se používá veřejně známé číslo rámce.

Co je to rámec?

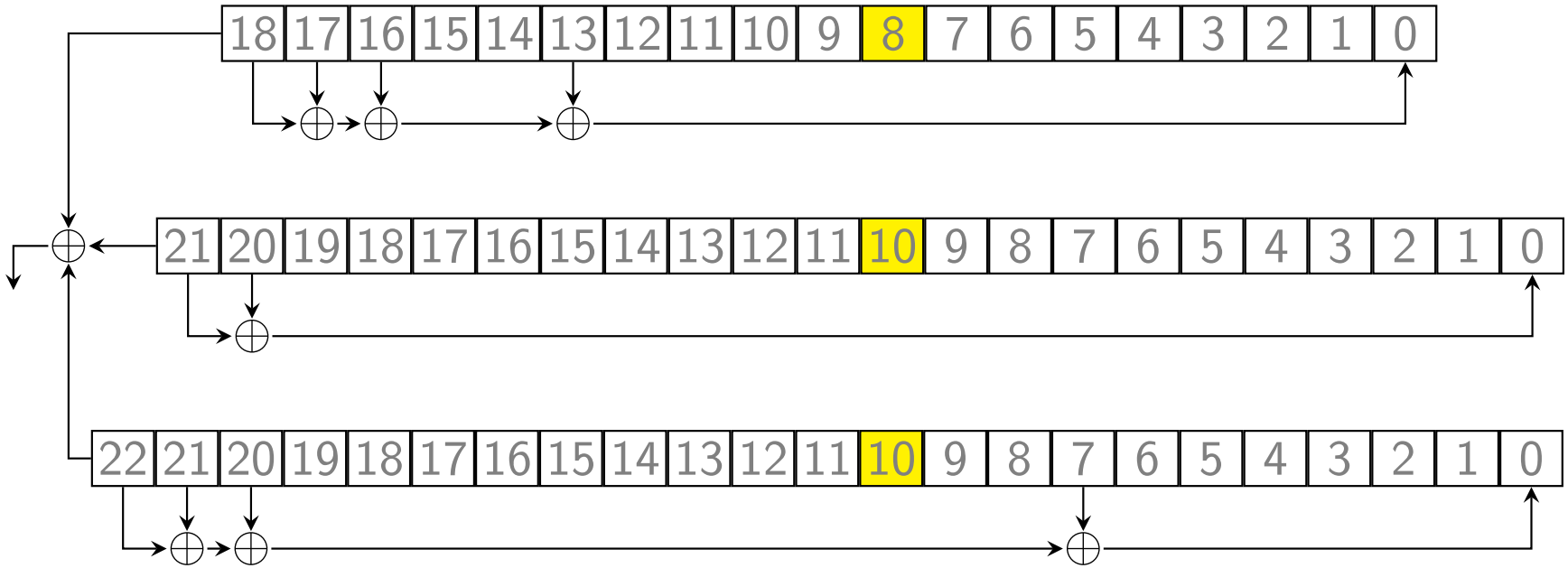
- Každý telefon komunikuje se základnovou stanicí na dvou frekvencích (jedna pro data směrem k uživateli, jedna pro data směrem od uživatele).
- Na každé dvojici frekvencí může komunikovat až 8 telefonů současně tak, že se telefony střídají ve využívání dané frekvence (tzv. Time Division Multiple Access).
- Pro přenos dat mají zařízení k dispozici časové úseky délky $15/26\,\text{ms} \approx 0{,}58\,\text{ms}$.
- Těchto 8 úseků tvoří rámec délky $120/26\,\text{ms} \approx 4{,}6\,\text{ms}$.



Automat šifry A5/1

- Vstupem automatu A5/1 je
  1. Tajný klíč K_c (64 bitů).
  2. Veřejně známé číslo rámce (22 bitů).
- Pro každý rámec se vygeneruje 228 bitů hesla:
  - Prvních 114 bitů pro data směrem k uživateli.
  - Zbývajících 114 bitů pro data směrem od uživatele.
- Proud hesla se s daty kombinuje operací XOR.
- Automat sestává ze tří LFSR R_1, R_2 a R_3 délek 19, 22 a 23. (Všechny mají maximální možnou délku periody).
- Máme tedy celkem 64 bitů vnitřního stavu.
- Registry se nekrokují pravidelně.
- To, které registry se krokují, je určeno jejich krokovacími bity $R_1[8]$, $R_2[10]$ a $R_3[10]$.

Automat šifry A5/1



- Krokem registru rozumíme jako obvykle:
  1. spočtení zpětné vazby,
  2. posun registru,
  3. zápis zpětné vazby na uvolněnou pozici.
- Krok automatu:
  1. Z krokovacích bitů se určí majoritní bit.
  2. Krokují se ty registry, jejichž krokovací bit je shodný s majoritním bitem.

Algoritmus šifry A5/1

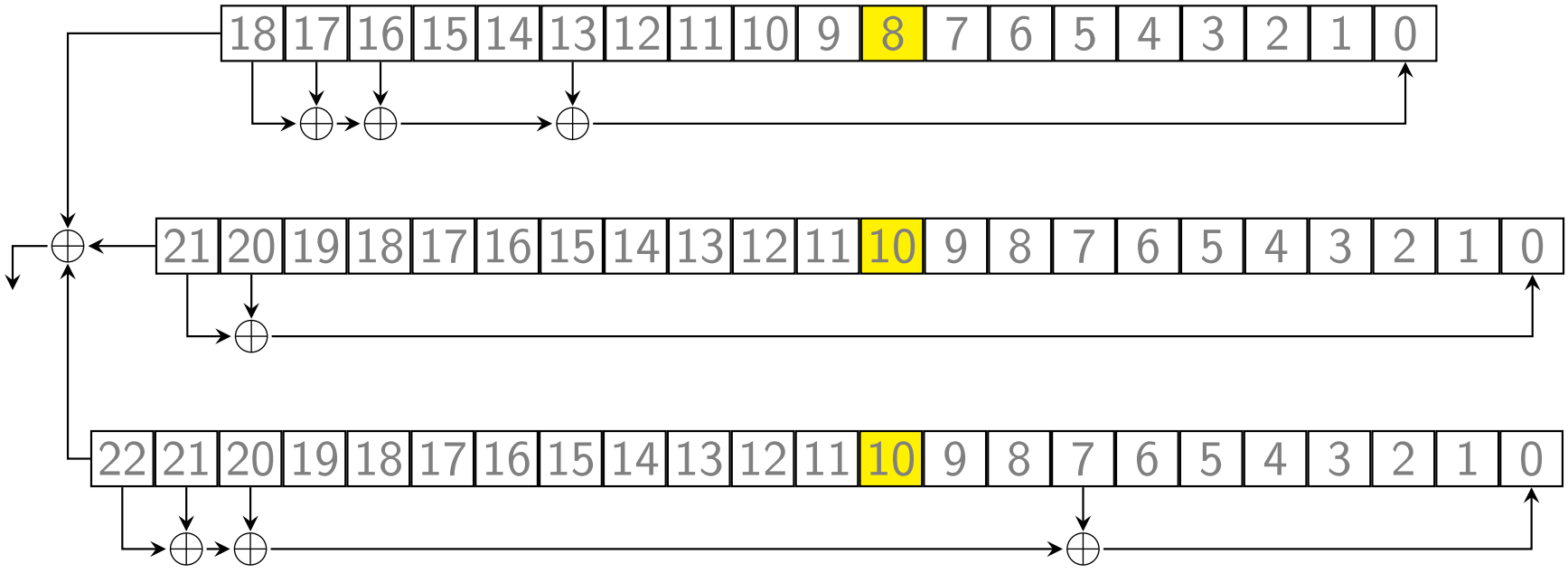
Inicializace

1. Sřetěz: $u :=$ klíč $\|$ číslo rámce (Máme $64 + 22 = 86$ bitů.)
2. Vynuluj registry.
3. Pro $i = 0, \ldots, 85$:
   $R_1[0] = R_1[0] \oplus u_i$
   $R_2[0] = R_2[0] \oplus u_i$
   $R_3[0] = R_3[0] \oplus u_i$
   Krokuj všechny tři registry. (Neber ohled na krokovací bity.)
4. Proveď 100 kroků automatu. (Bez výstupu.)

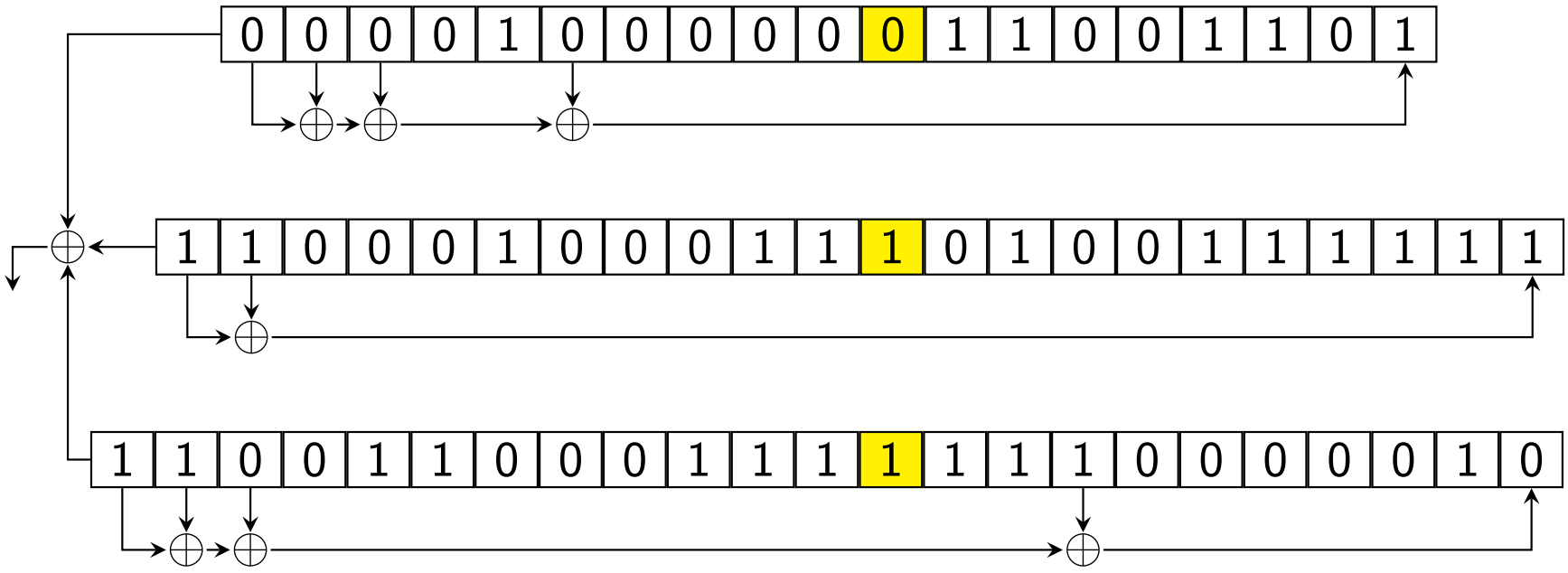
Generování hesla s

- Pro $i = 0, \ldots, 227$:
  Krokuj automat.
  $s_i := R_1[18] \oplus R_2[21] \oplus R_3[22]$.

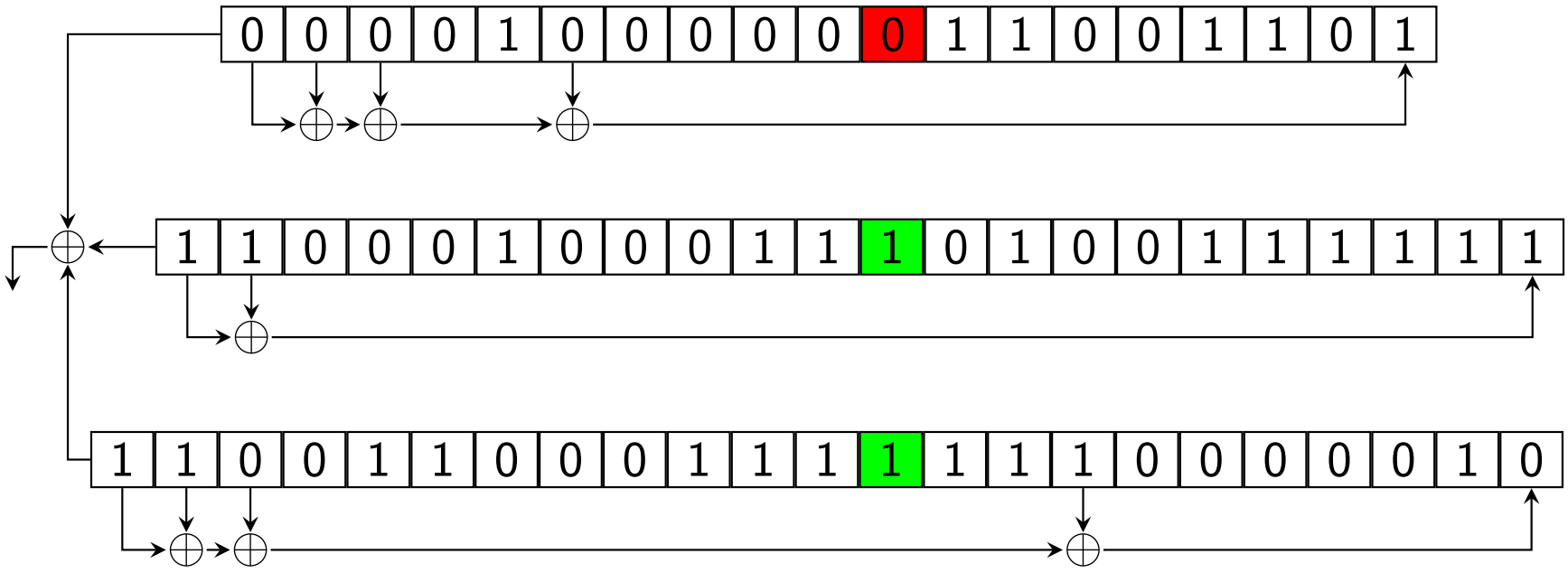
Automat šifry A5/1



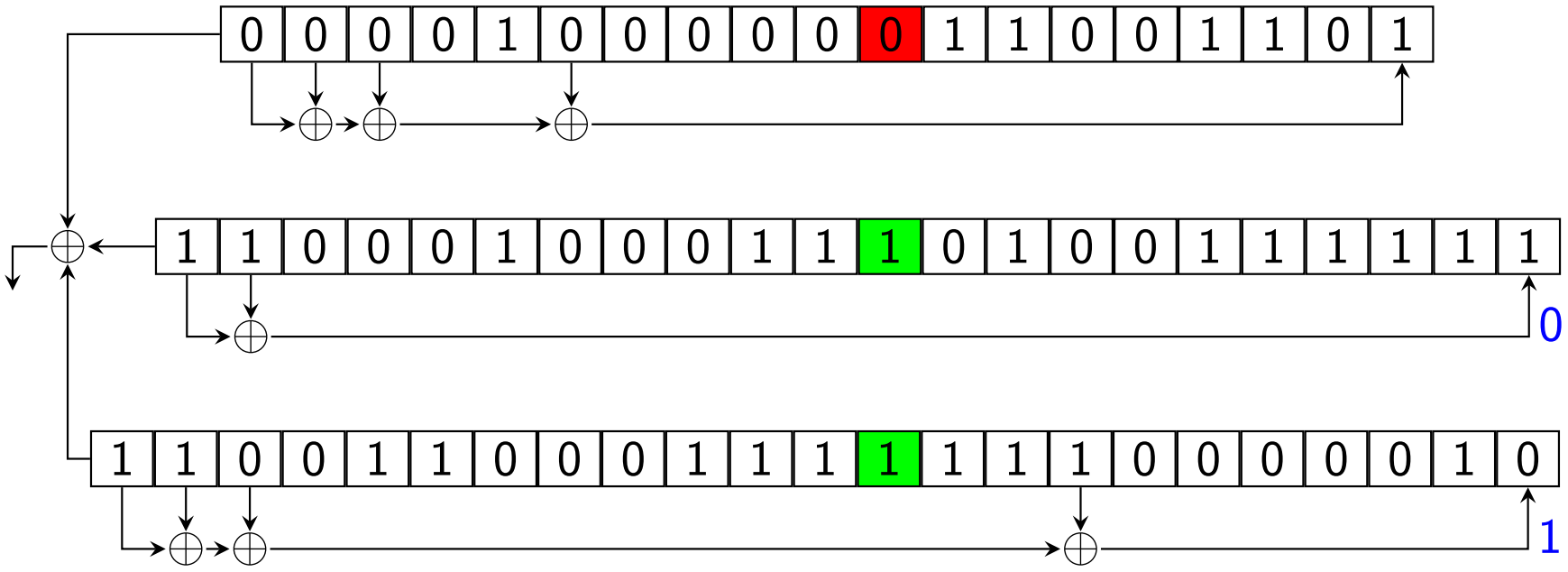
Automat šifry A5/1 v čase t



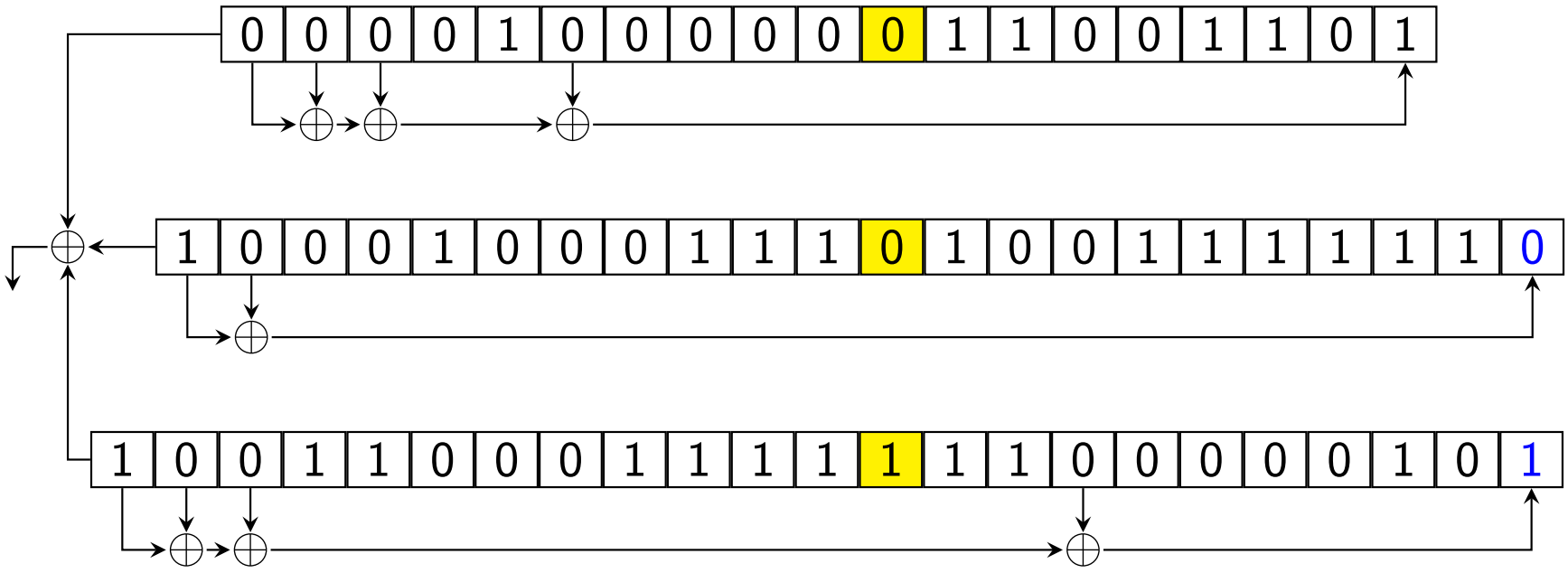
Automat šifry A5/1 v čase t



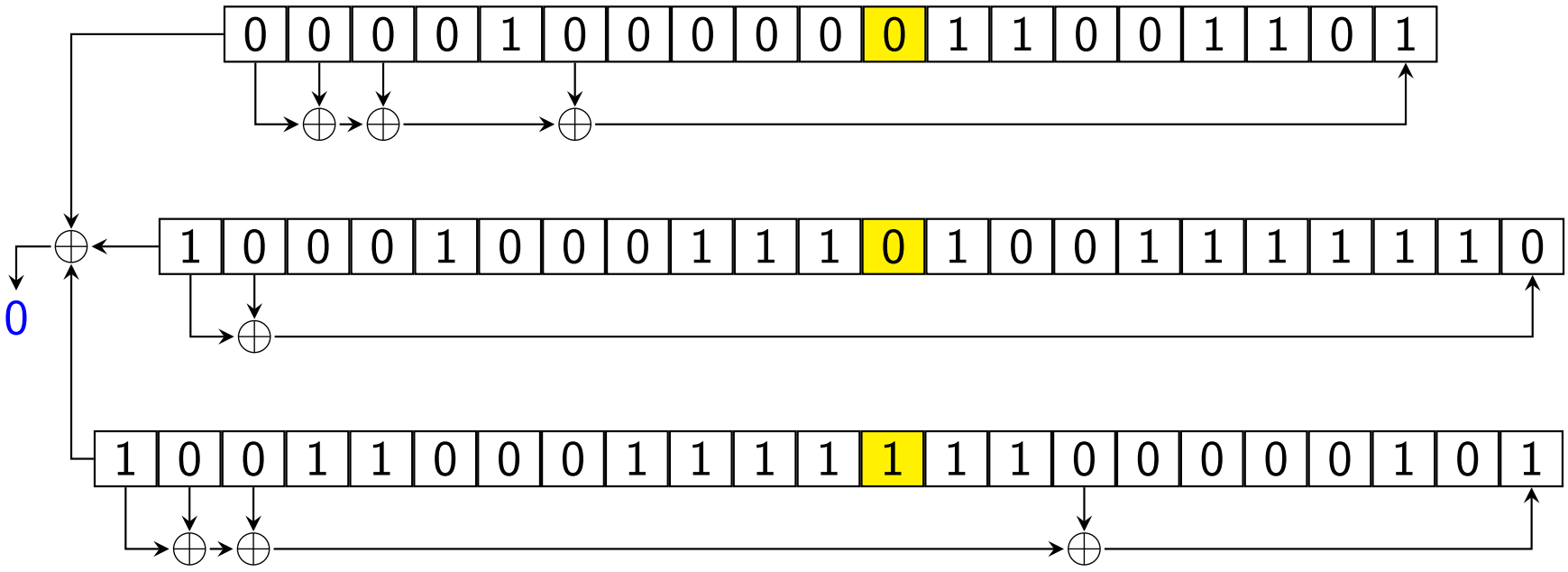
Automat šifry A5/1 v čase t



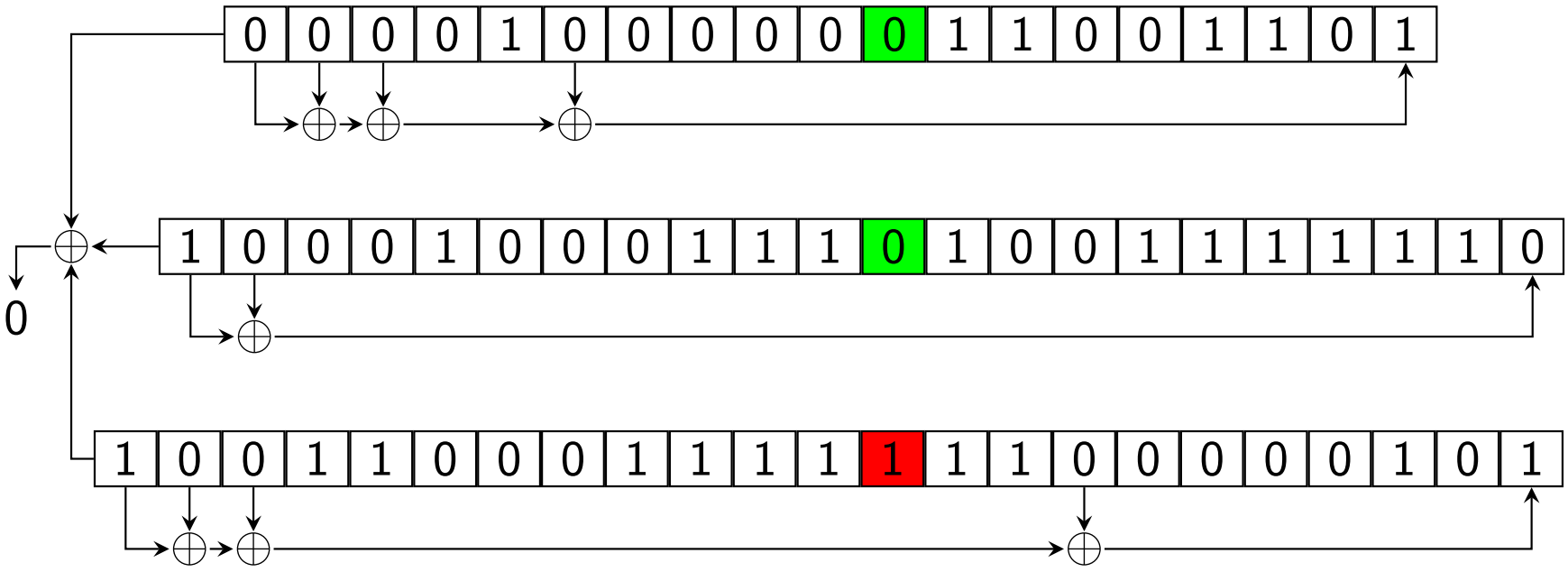
Automat šifry A5/1 v čase $t + 1$



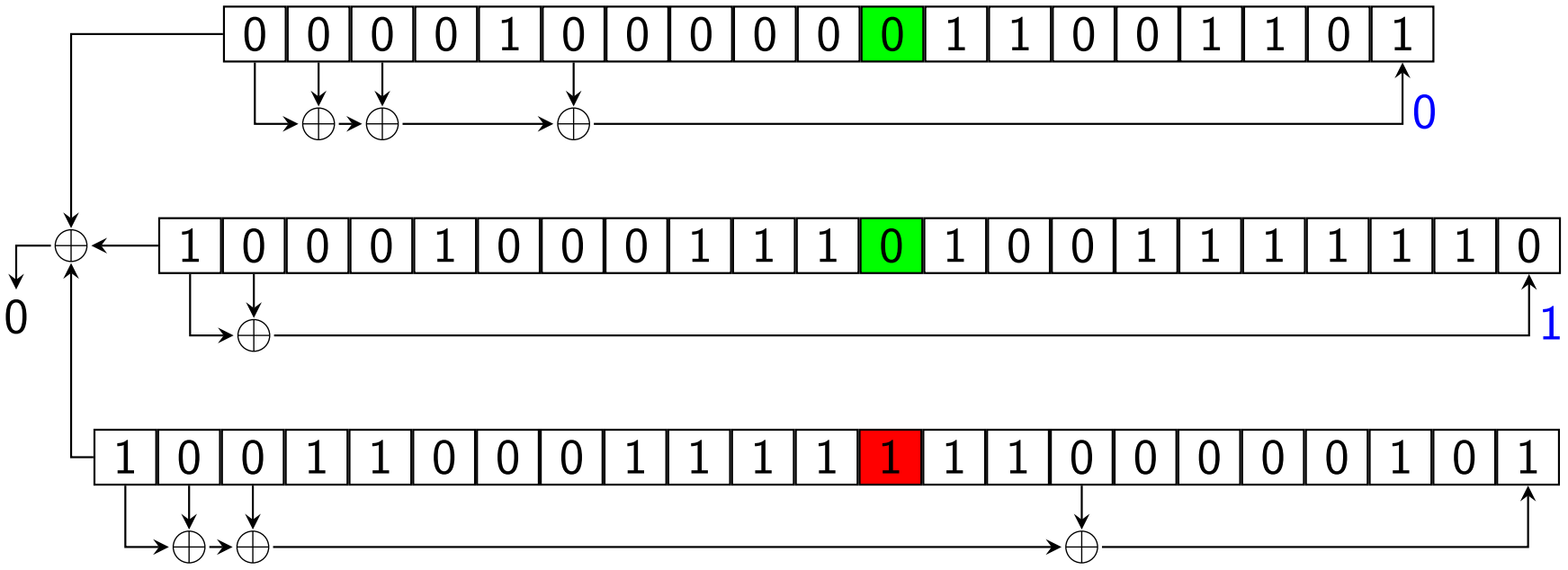
Automat šifry A5/1 v čase $t + 1$



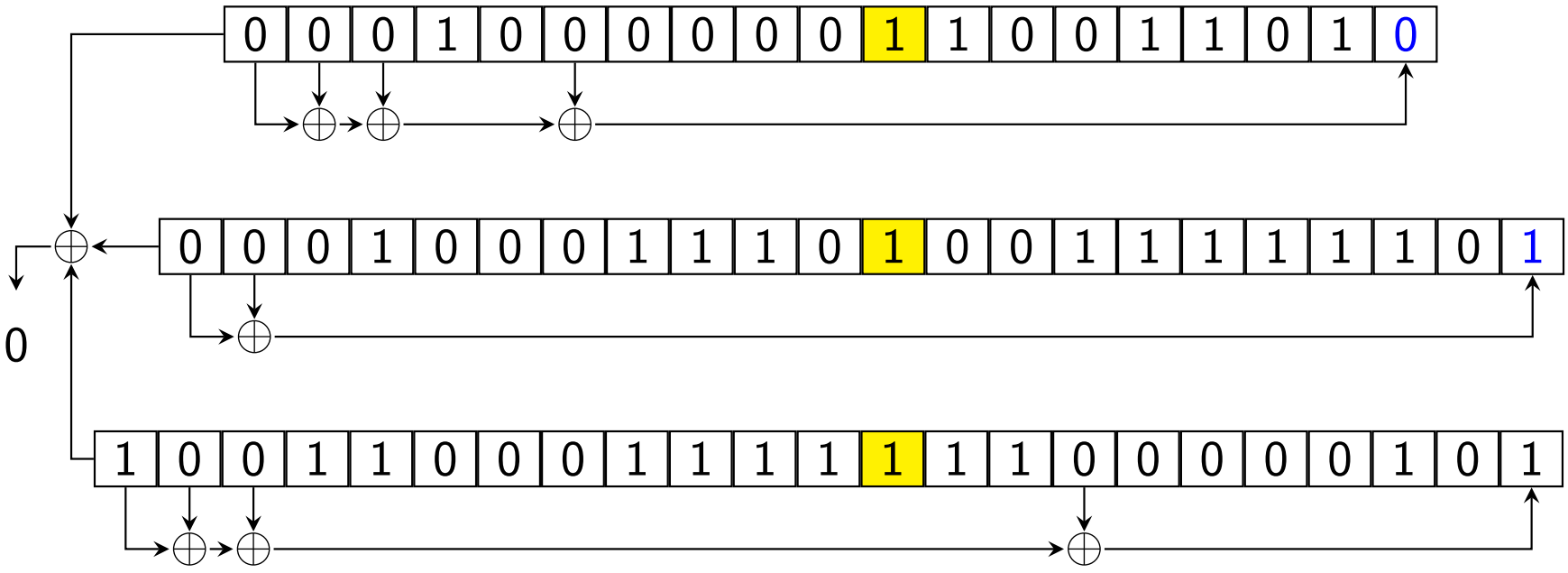
Automat šifry A5/1 v čase $t + 1$



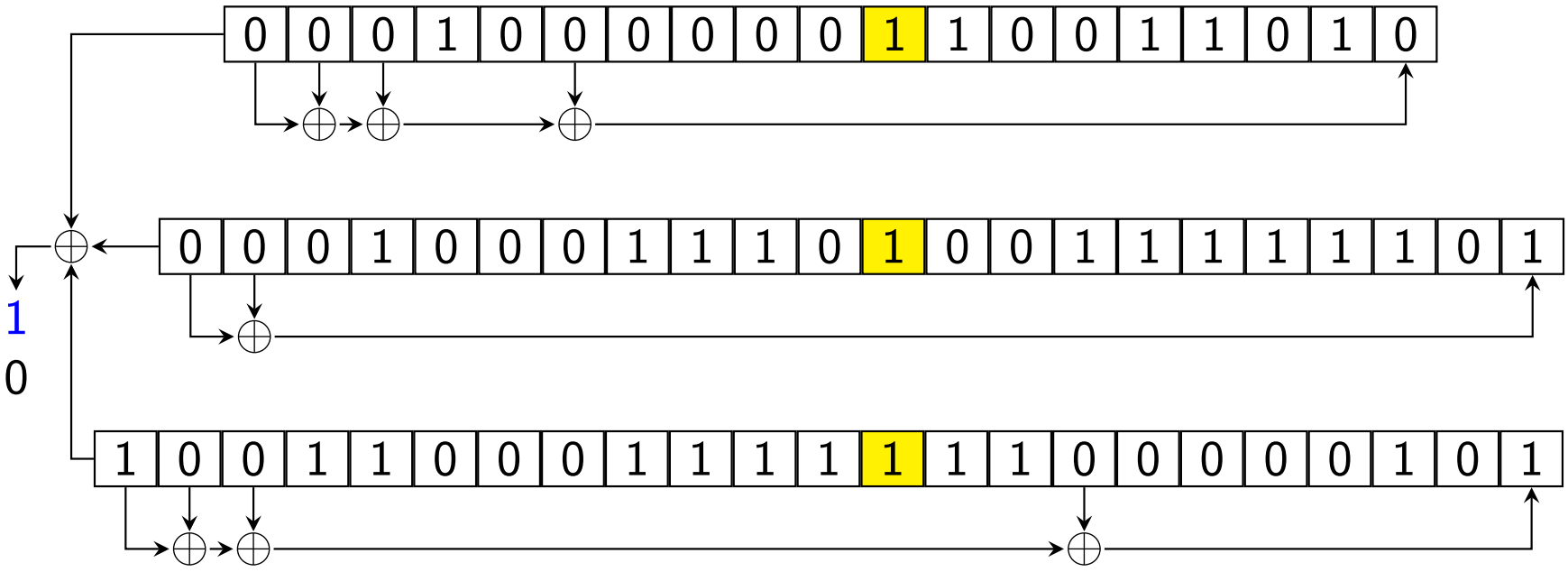
Automat šifry A5/1 v čase $t + 1$



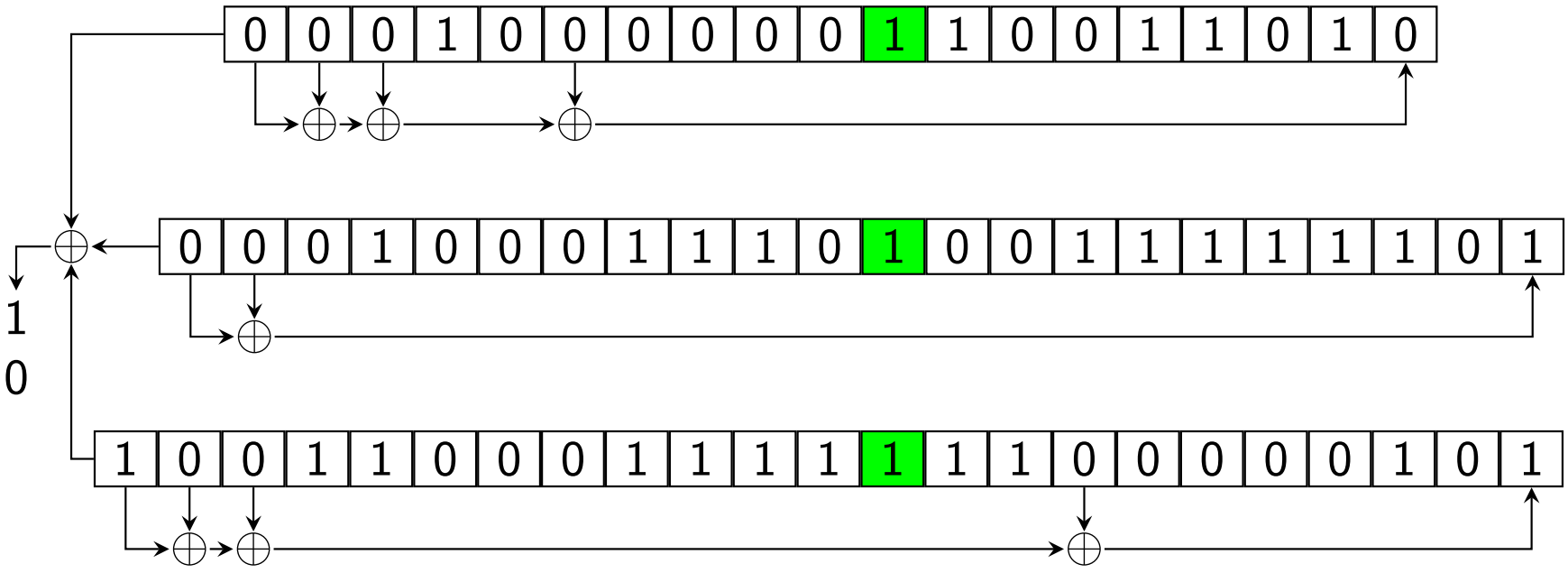
Automat šifry A5/1 v čase $t + 2$



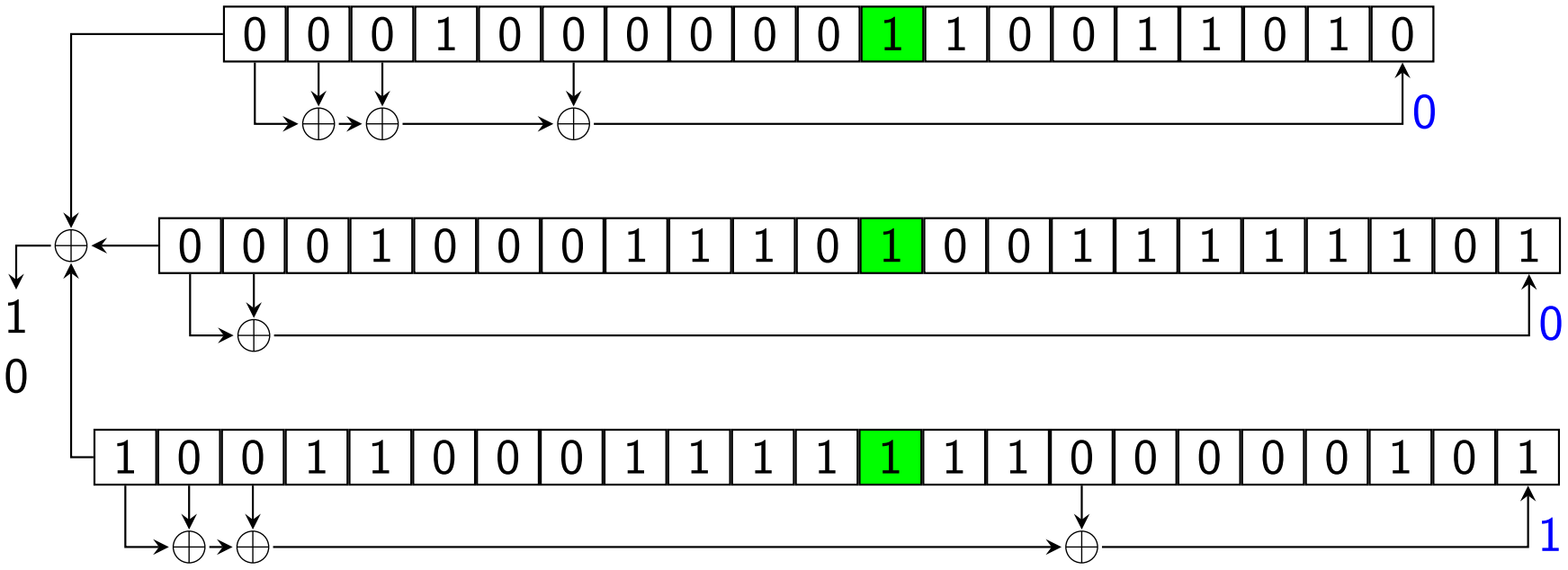
Automat šifry A5/1 v čase $t + 2$



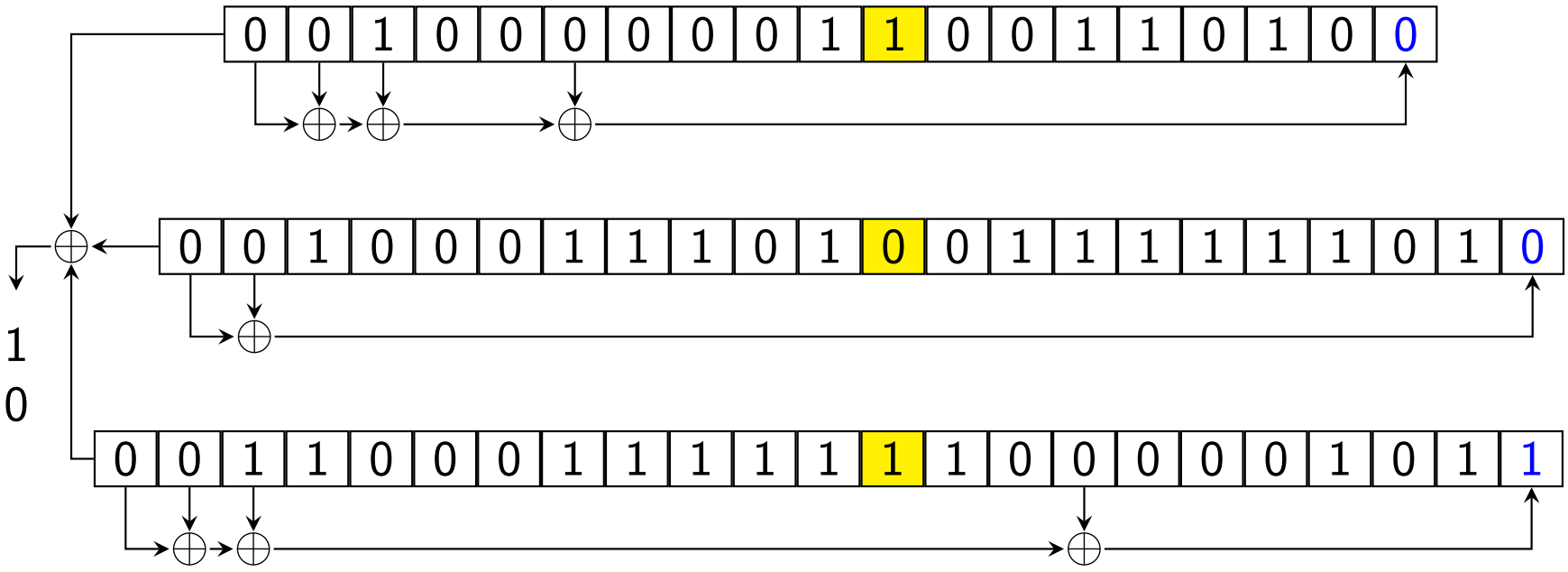
Automat šifry A5/1 v čase $t + 2$



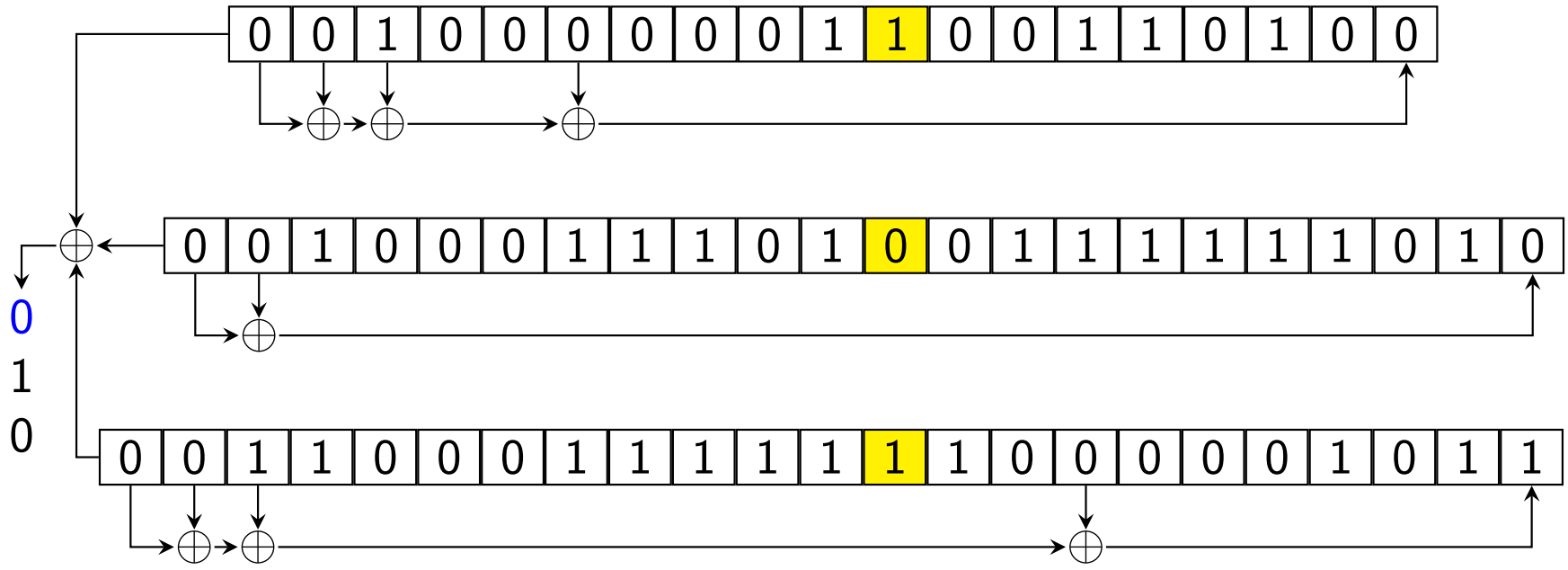
Automat šifry A5/1 v čase $t + 2$



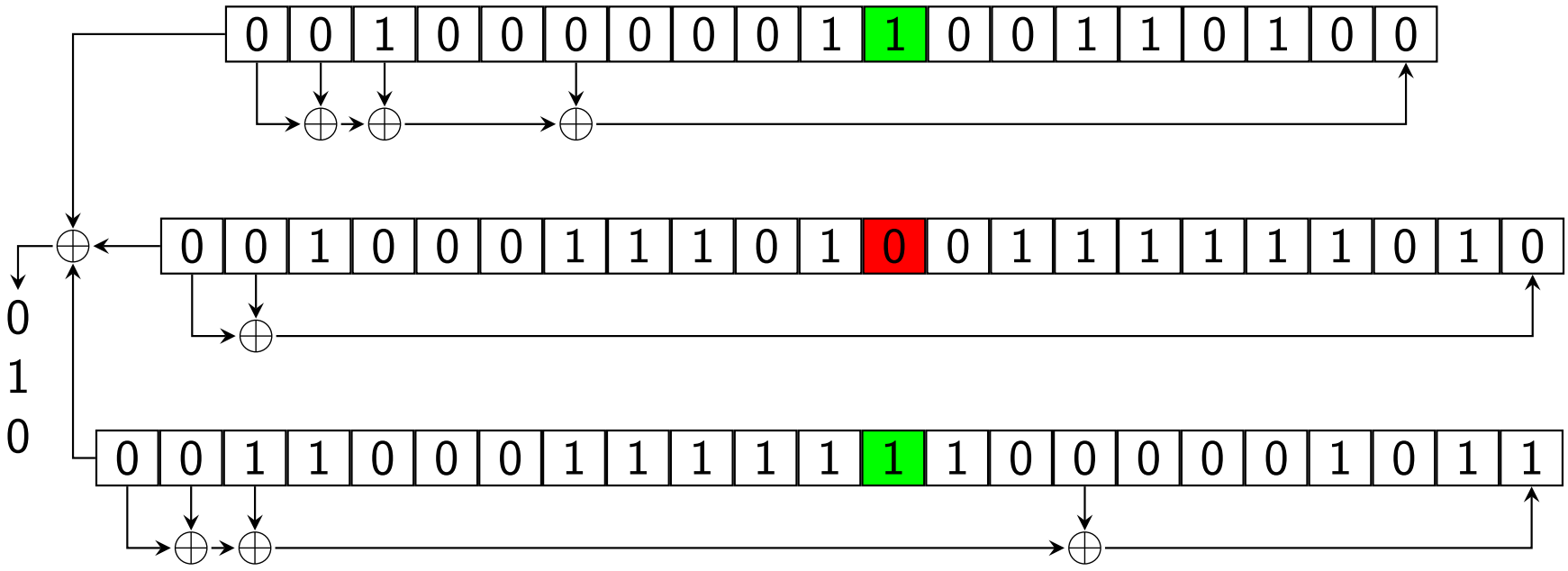
Automat šifry A5/1 v čase $t + 3$



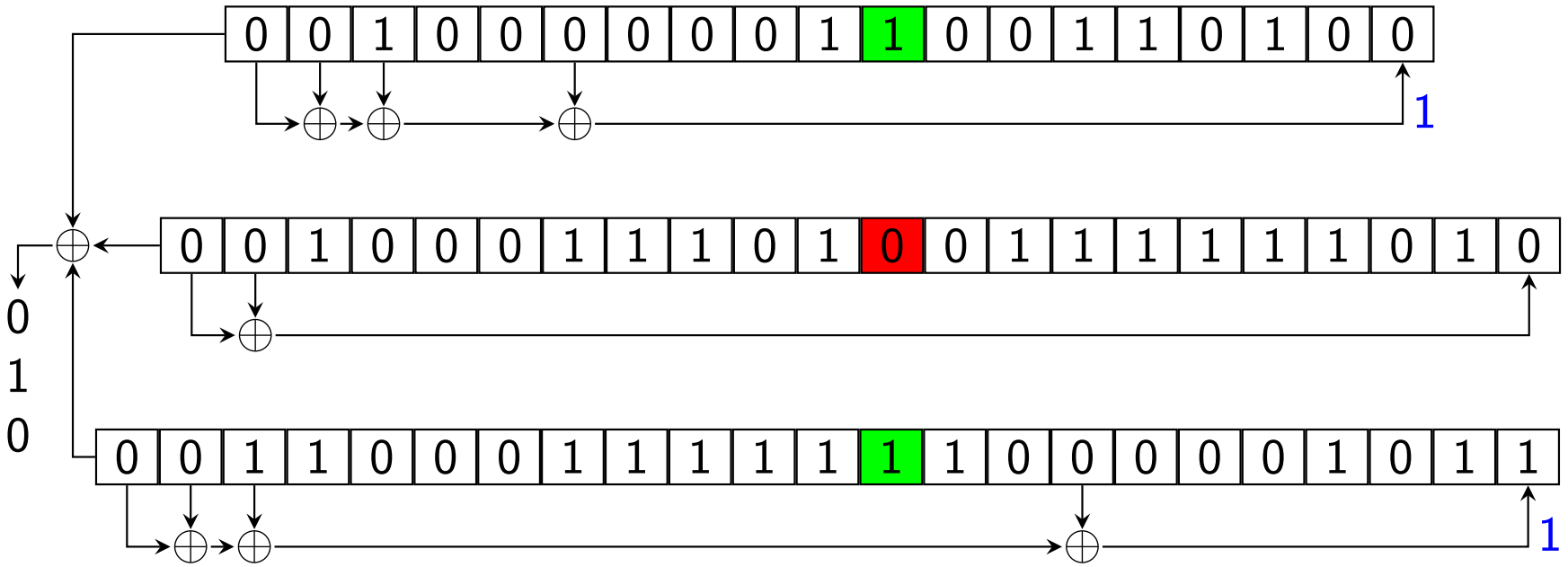
Automat šifry A5/1 v čase $t + 3$



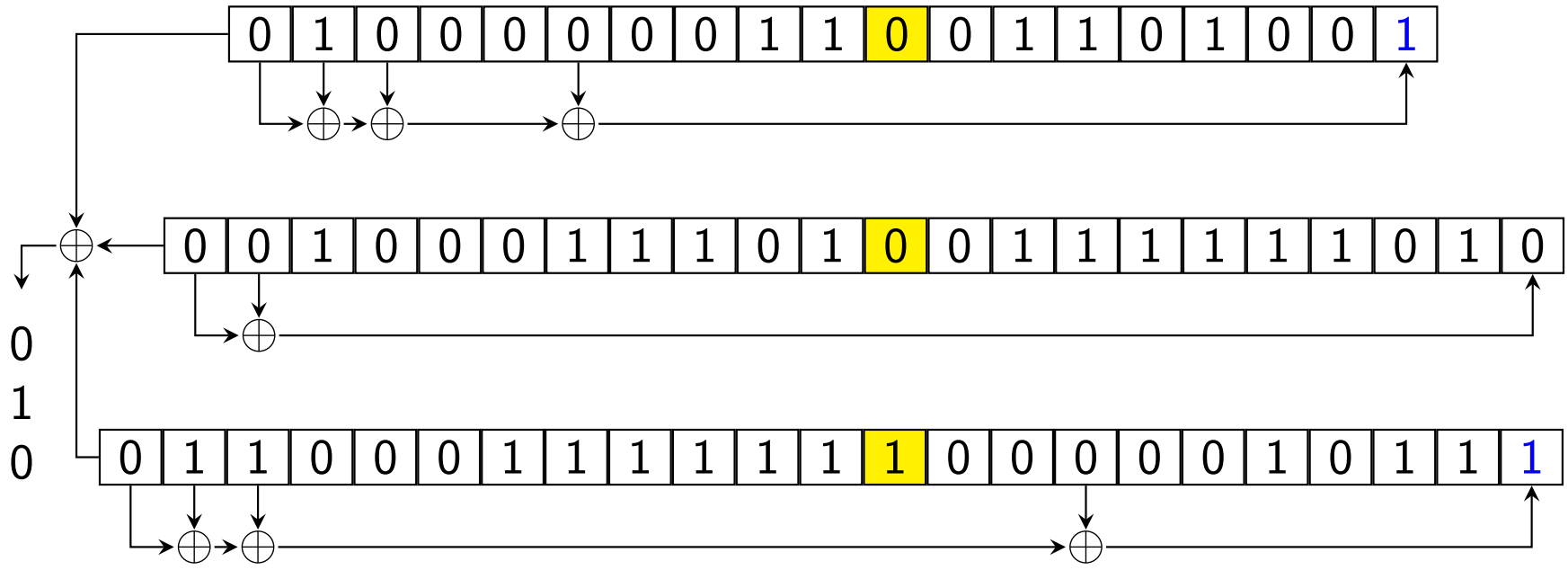
Automat šifry A5/1 v čase $t + 3$



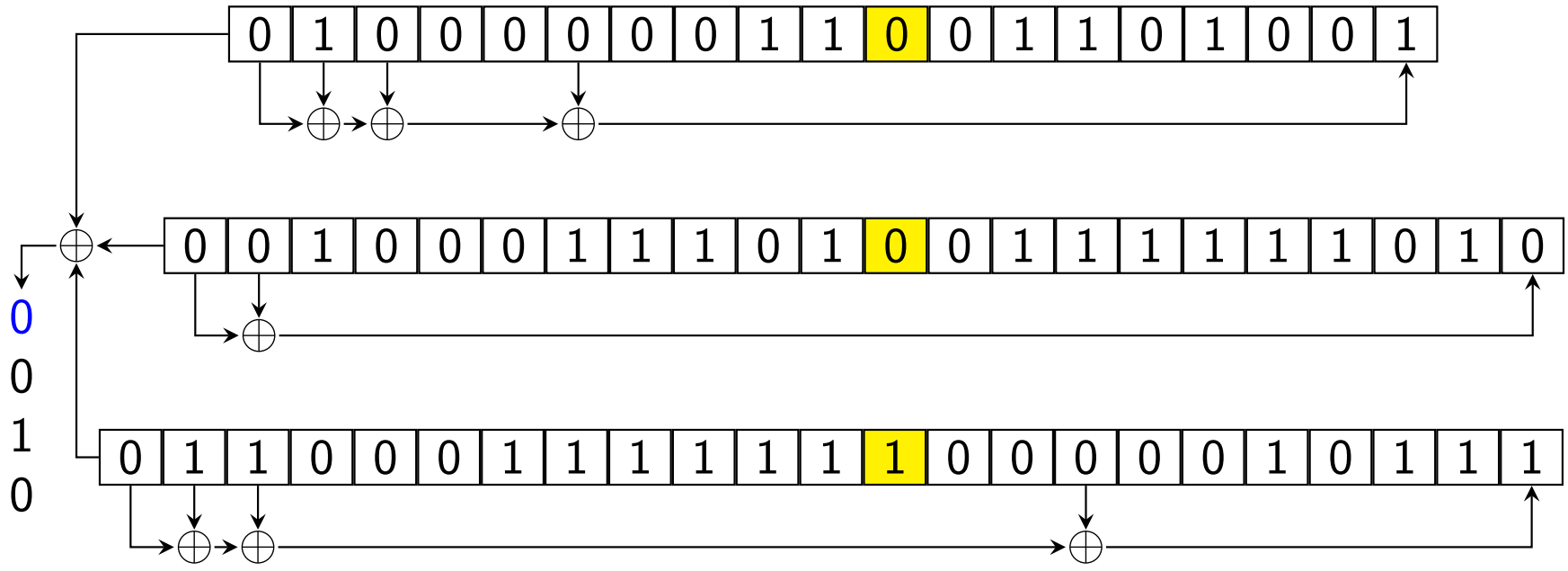
Automat šifry A5/1 v čase $t + 3$



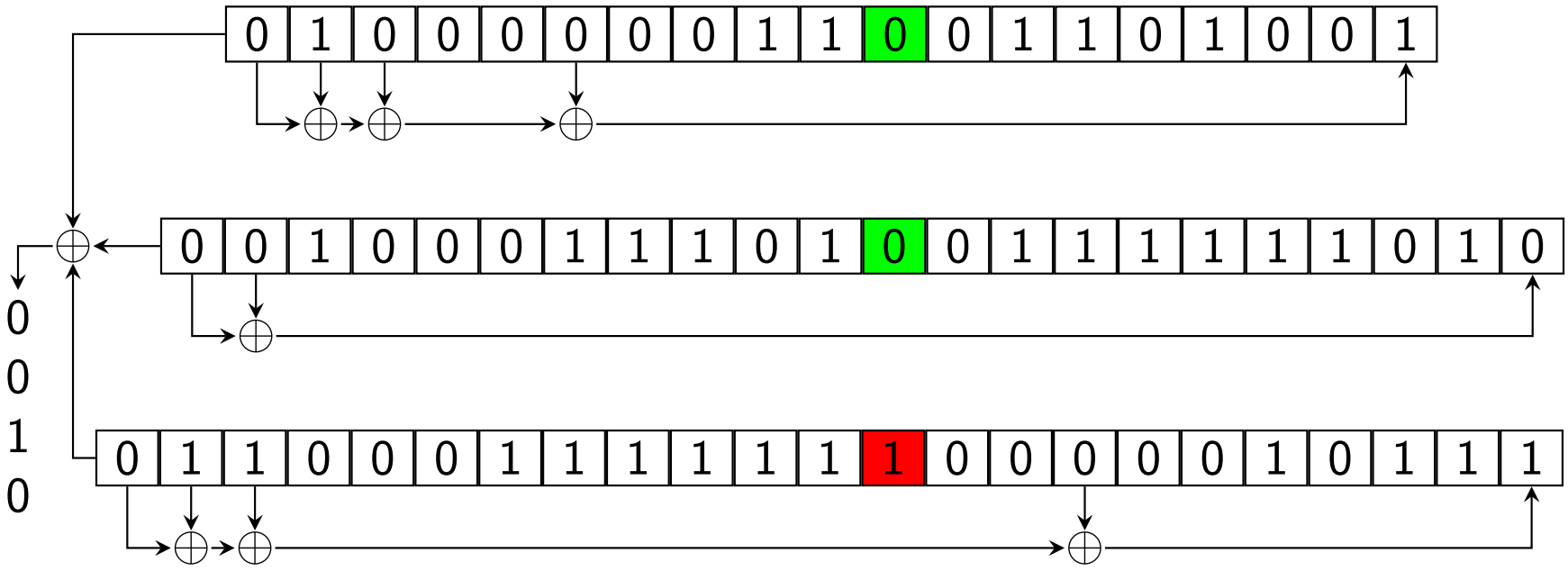
Automat šifry A5/1 v čase $t + 4$



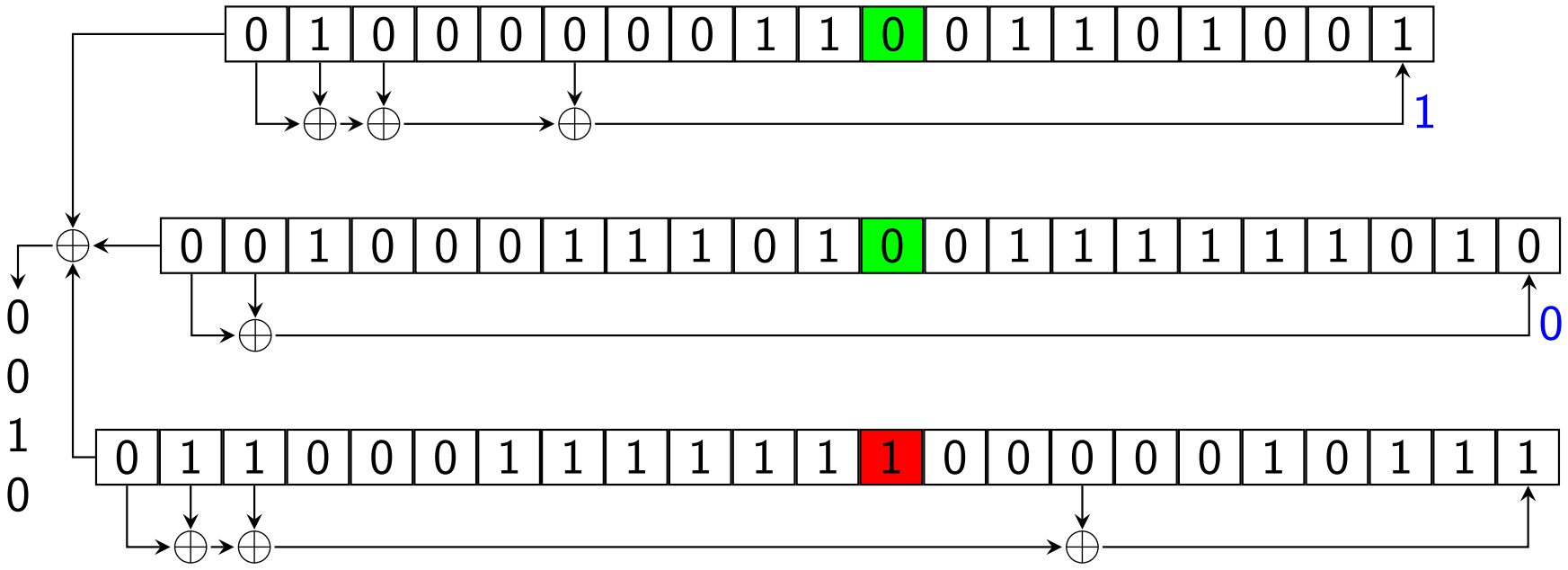
Automat šifry A5/1 v čase $t + 4$



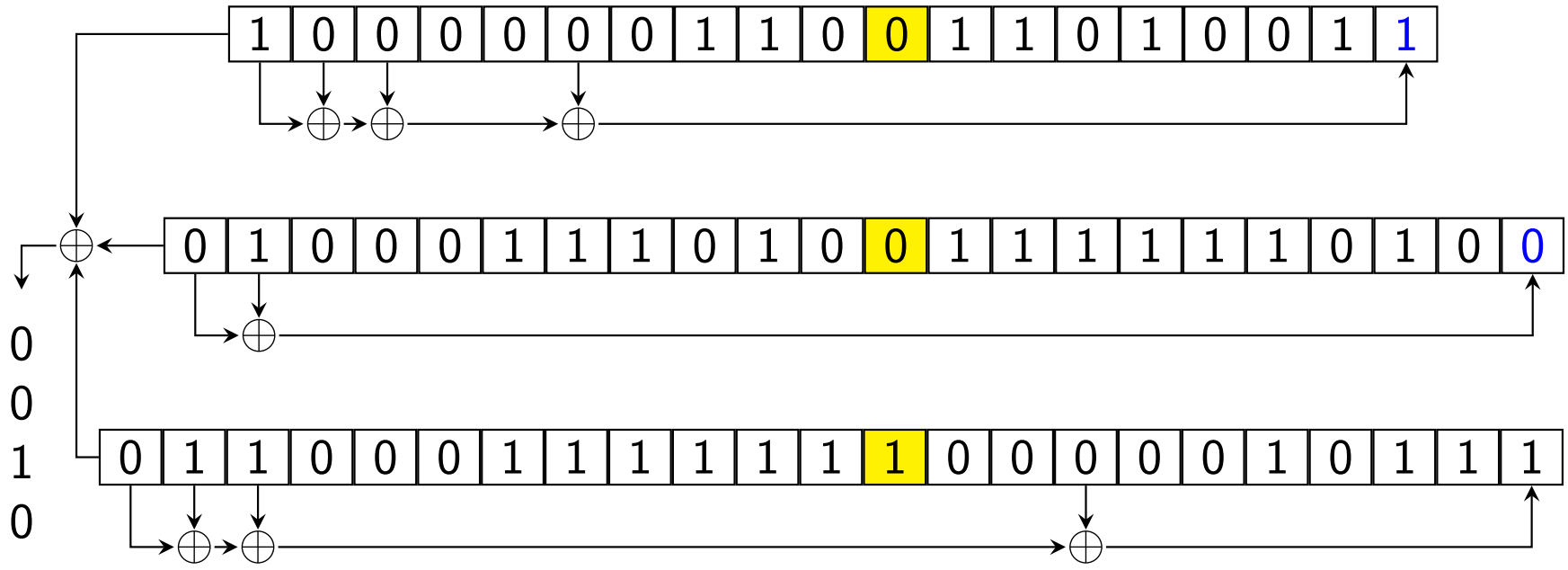
Automat šifry A5/1 v čase $t + 4$



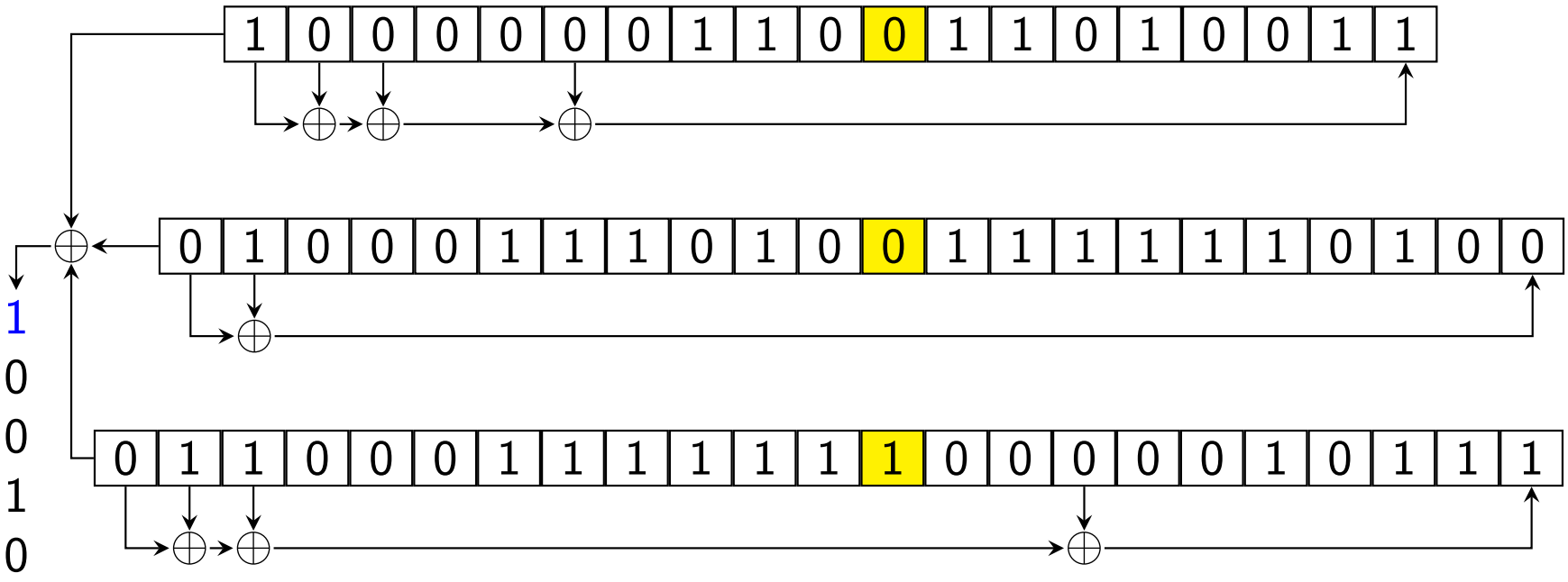
Automat šifry A5/1 v čase $t + 4$



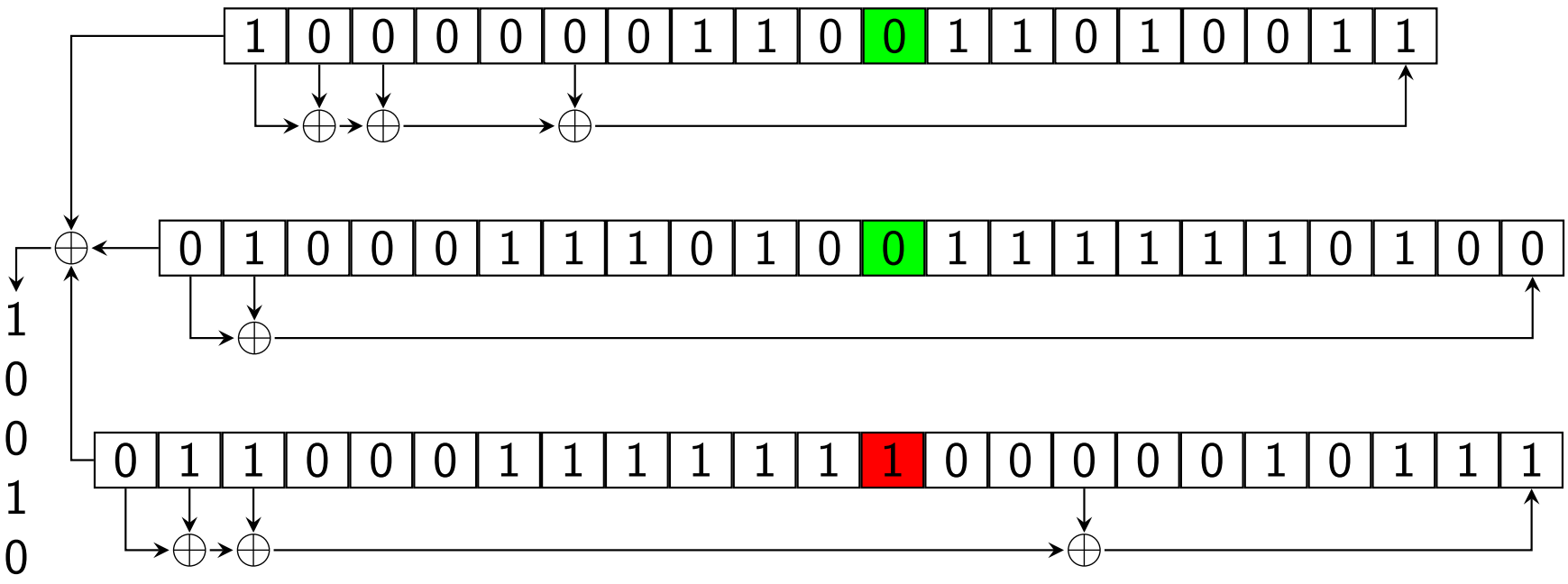
Automat šifry A5/1 v čase $t + 5$



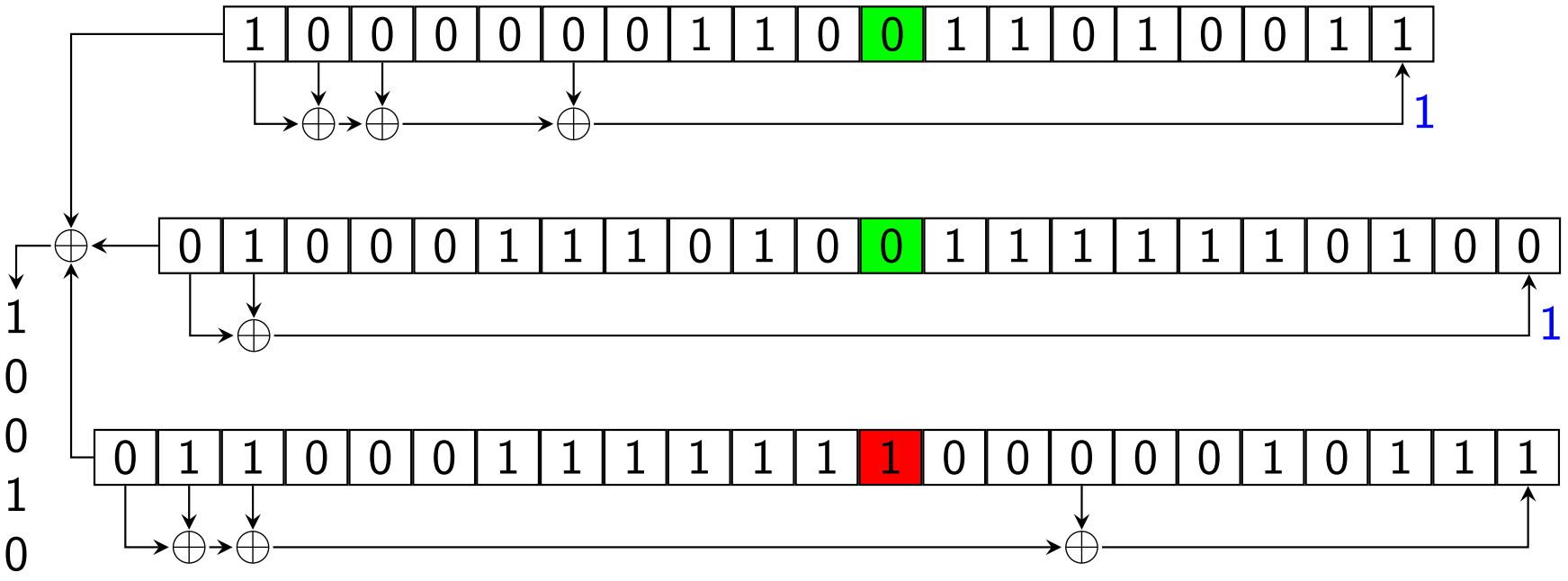
Automat šifry A5/1 v čase $t + 5$



Automat šifry A5/1 v čase $t + 5$

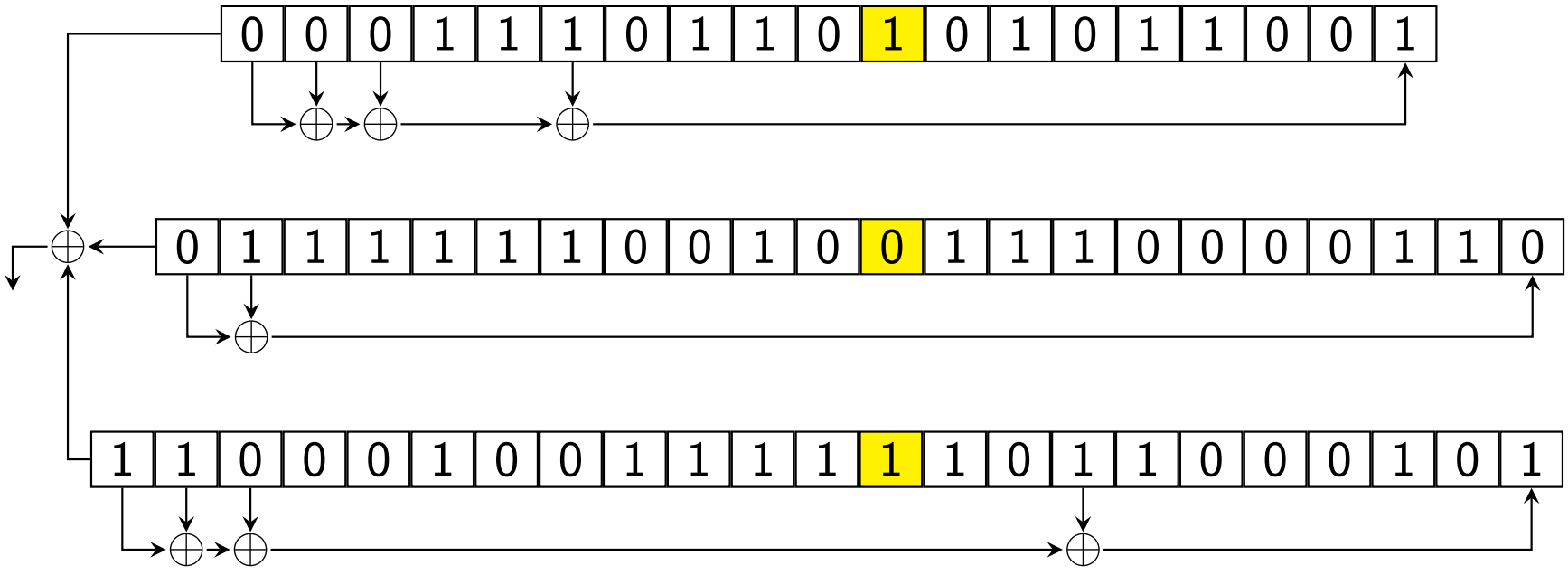


Automat šifry A5/1 v čase $t + 5$



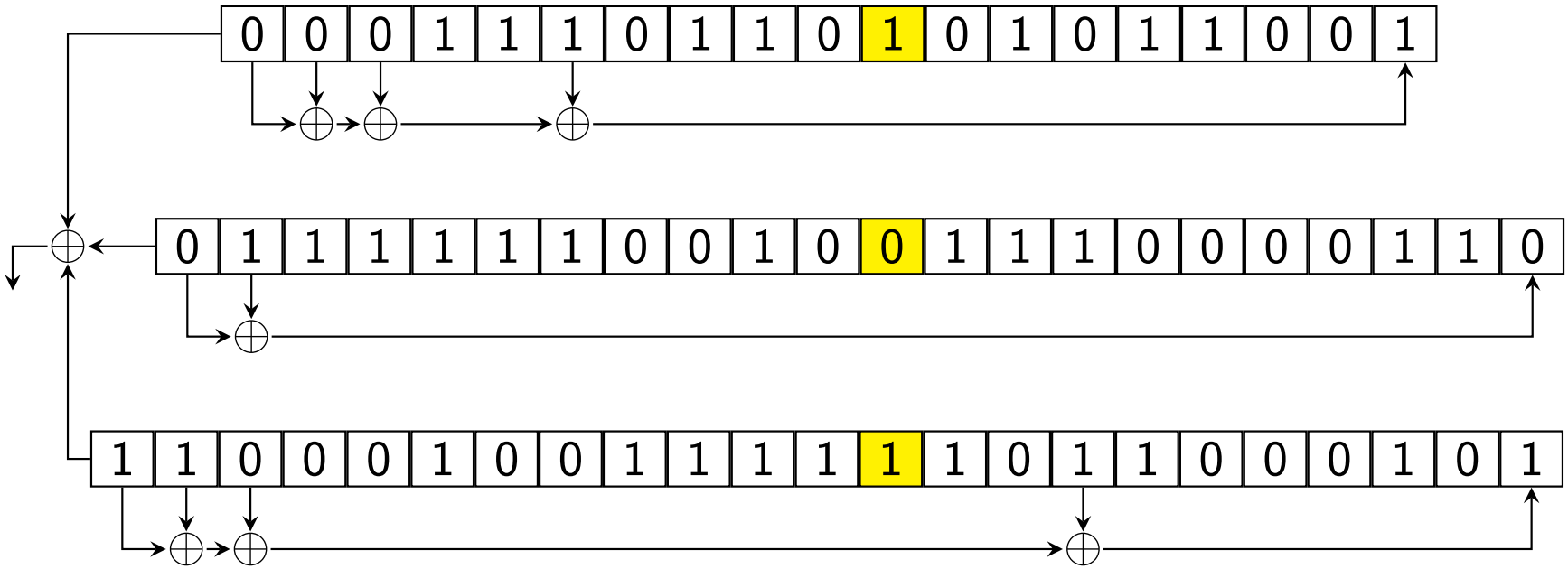
Zpětný chod automatu šifry A5/1

Určete stav automatu v čase $t-1$, znáte-li stav v čase t:



Zpětný chod automatu šifry A5/1

Určete stav automatu v čase $t-1$, znáte-li stav v čase t:

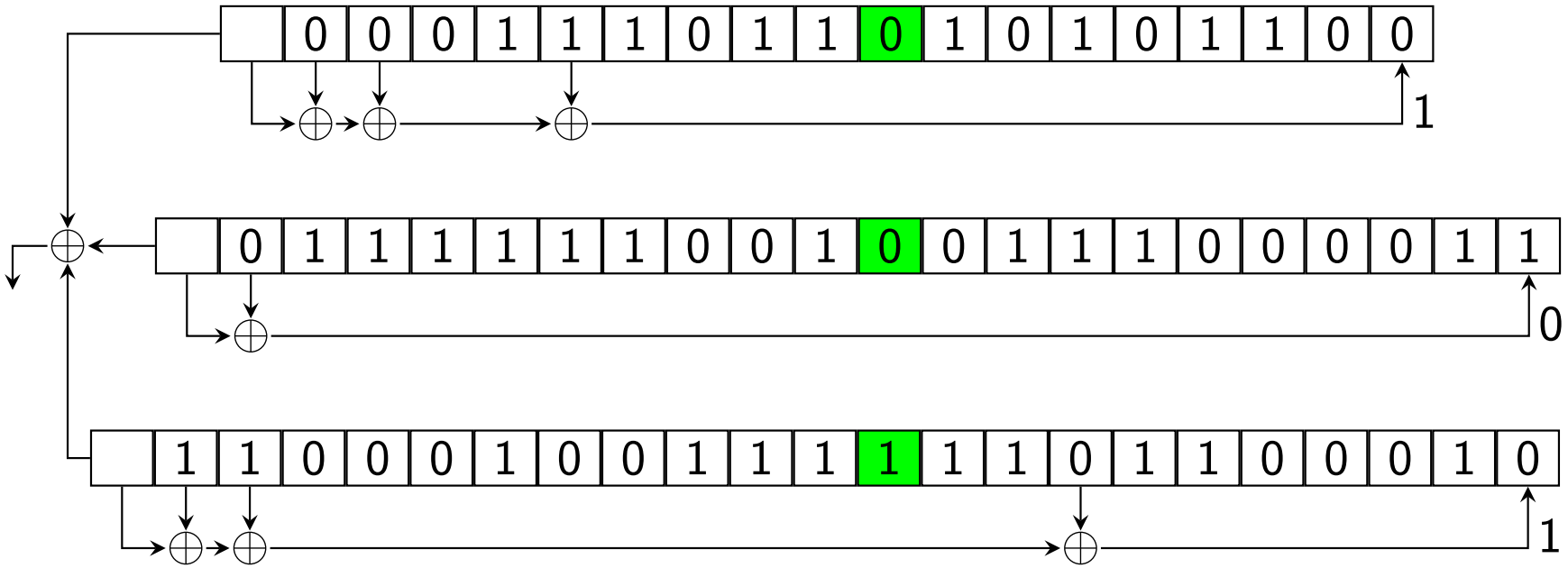


Stav v čase t mohl vzniknout

- krokováním všech tří registrů;
- krokováním 1. a 2. registru;
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t-1$:

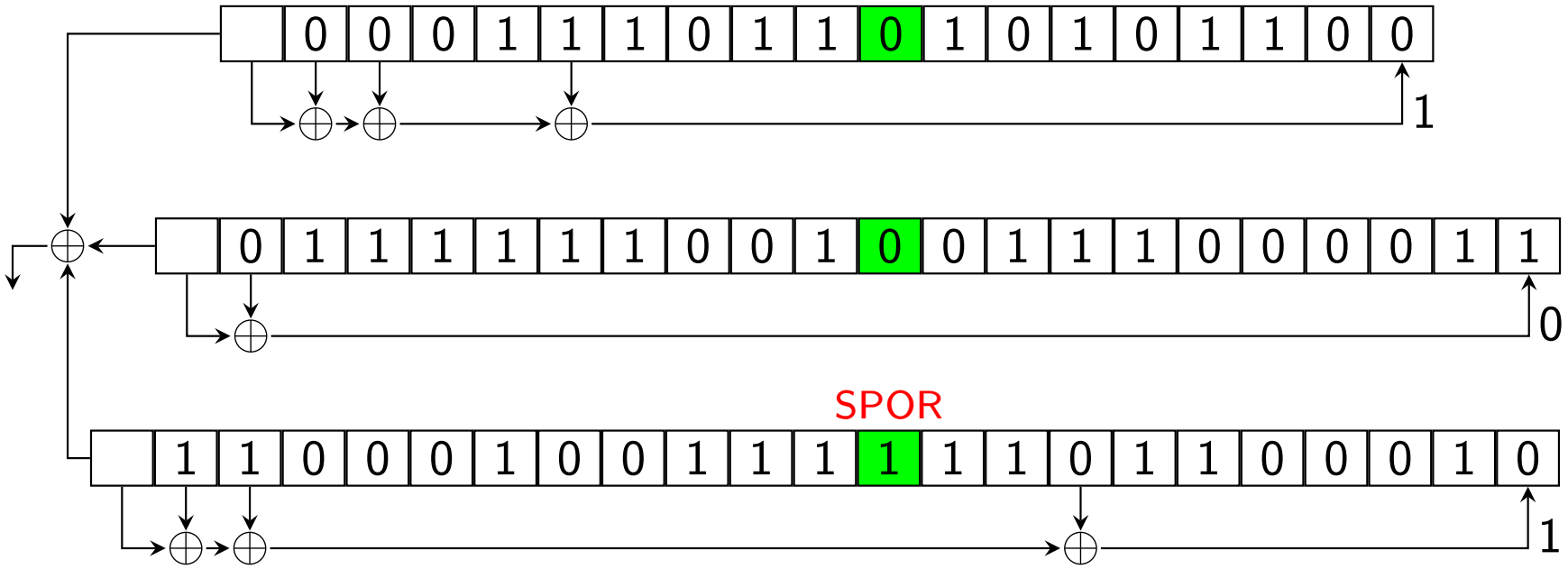


Stav v čase t mohl vzniknout

- krokováním všech tří registrů;
- krokováním 1. a 2. registru;
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t-1$:

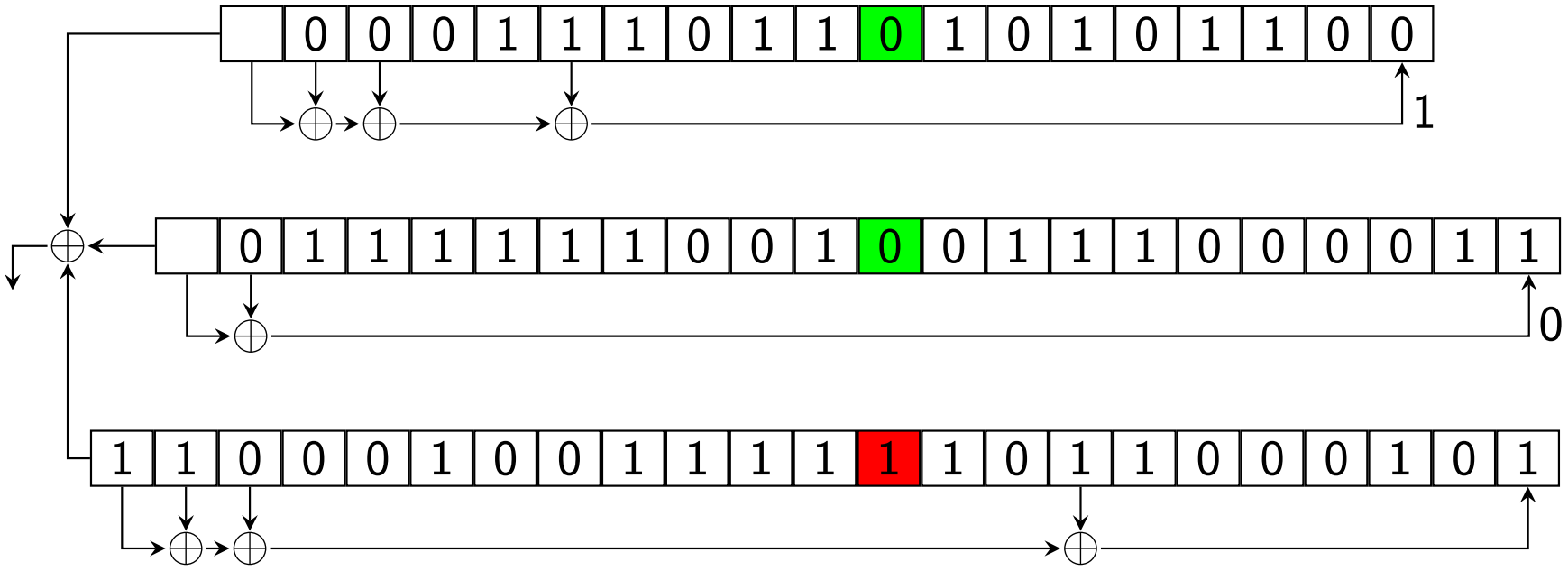


Stav v čase t mohl vzniknout

- krokováním všech tří registrů; ✗
- krokováním 1. a 2. registru;
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t-1$:

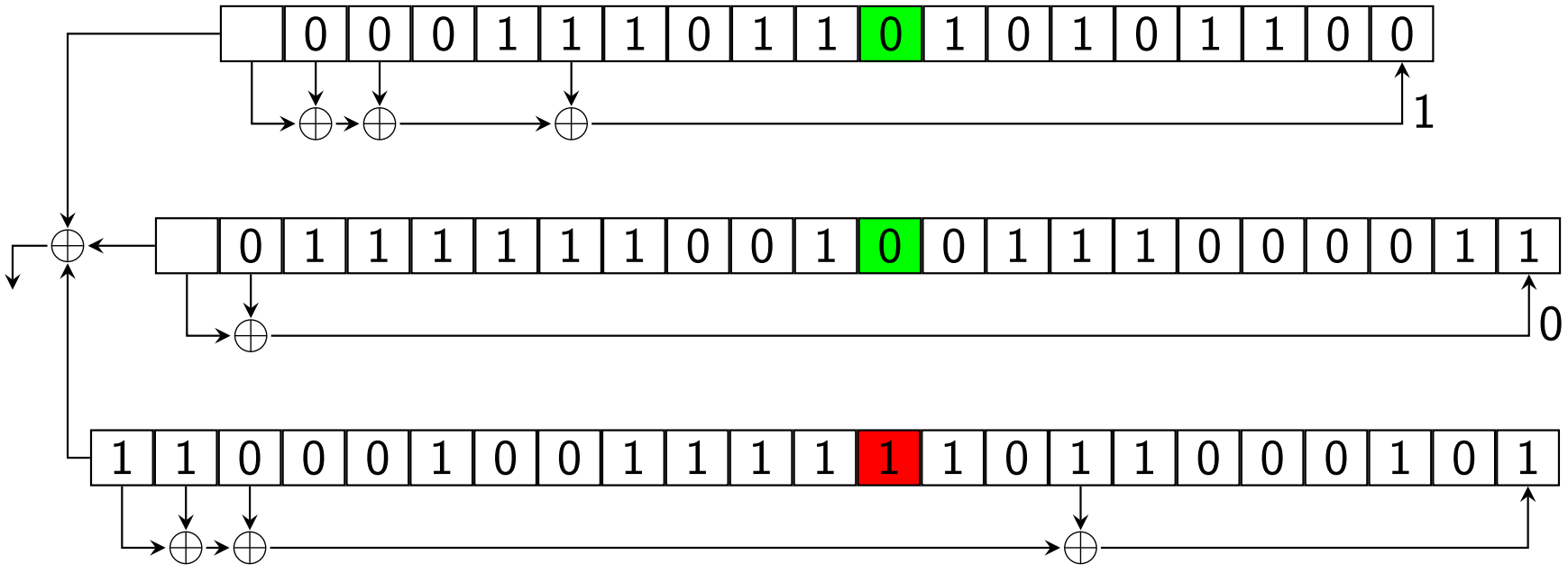


Stav v čase t mohl vzniknout

- krokováním všech tří registrů; ✗
- krokováním 1. a 2. registru;
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t-1$:

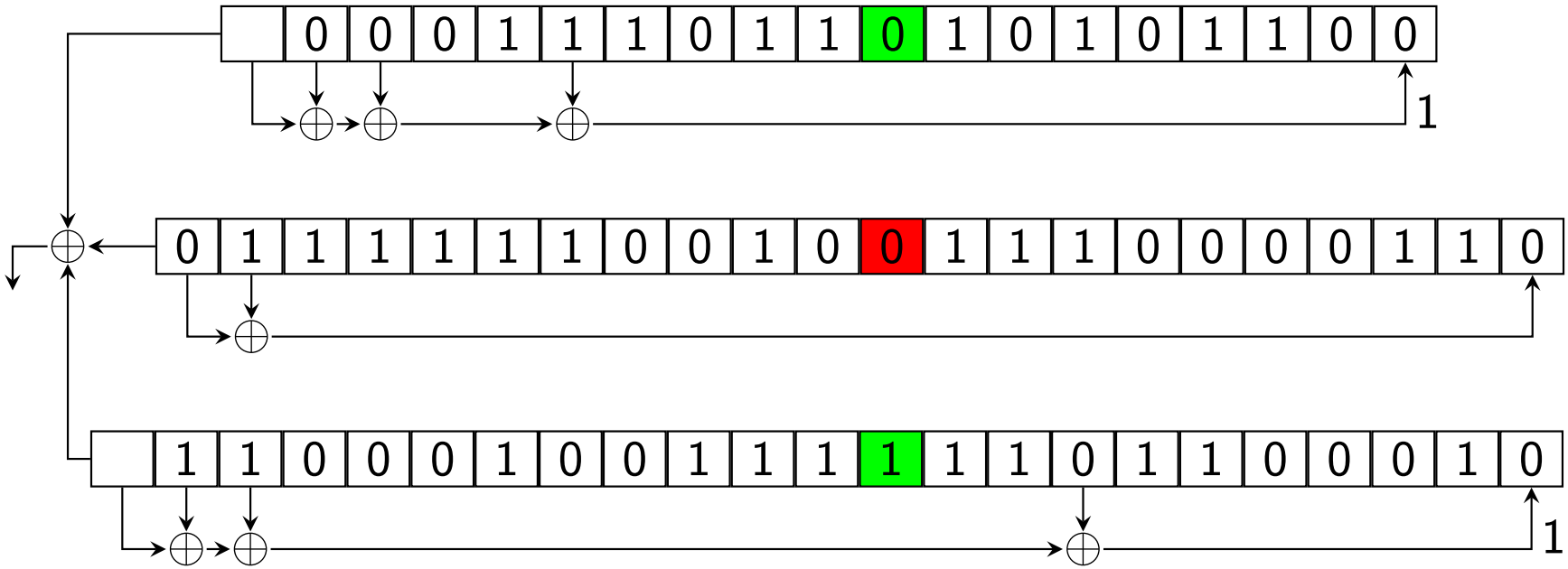


Stav v čase t mohl vzniknout

- krokováním všech tří registrů; ✗
- krokováním 1. a 2. registru; ✓
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t-1$:

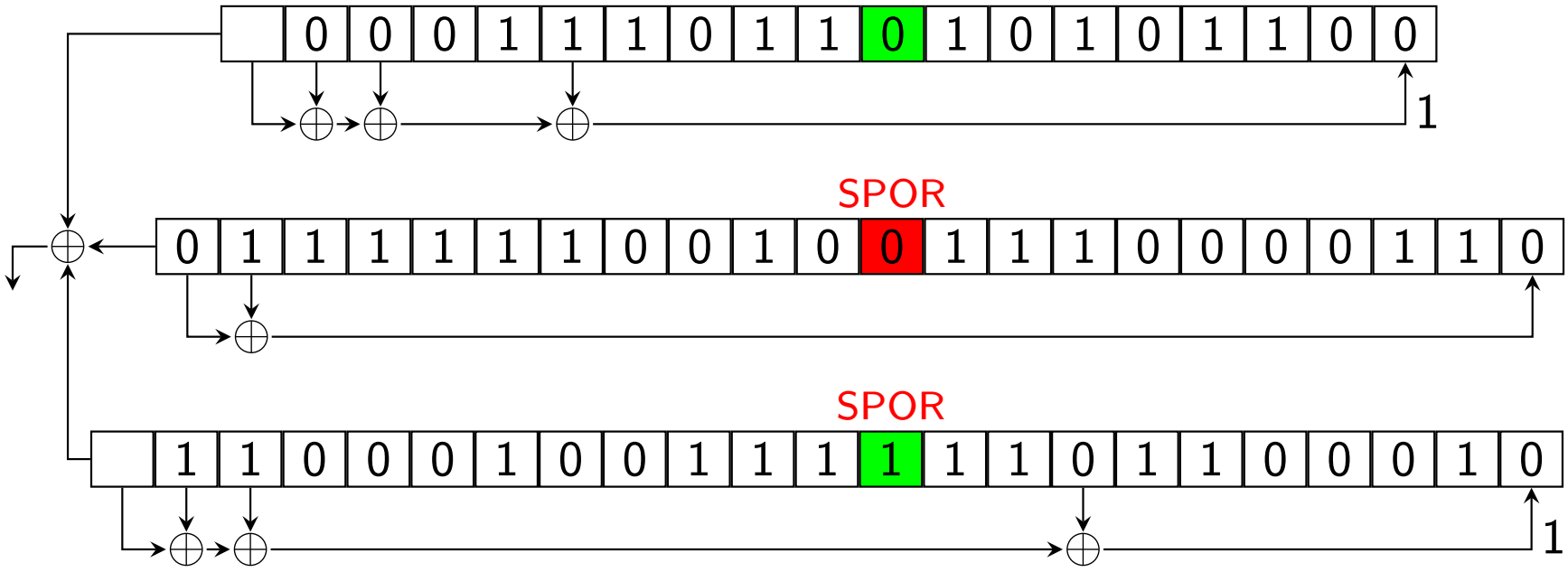


Stav v čase t mohl vzniknout

- krokováním všech tří registrů; ✗
- krokováním 1. a 2. registru; ✓
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t - 1$:

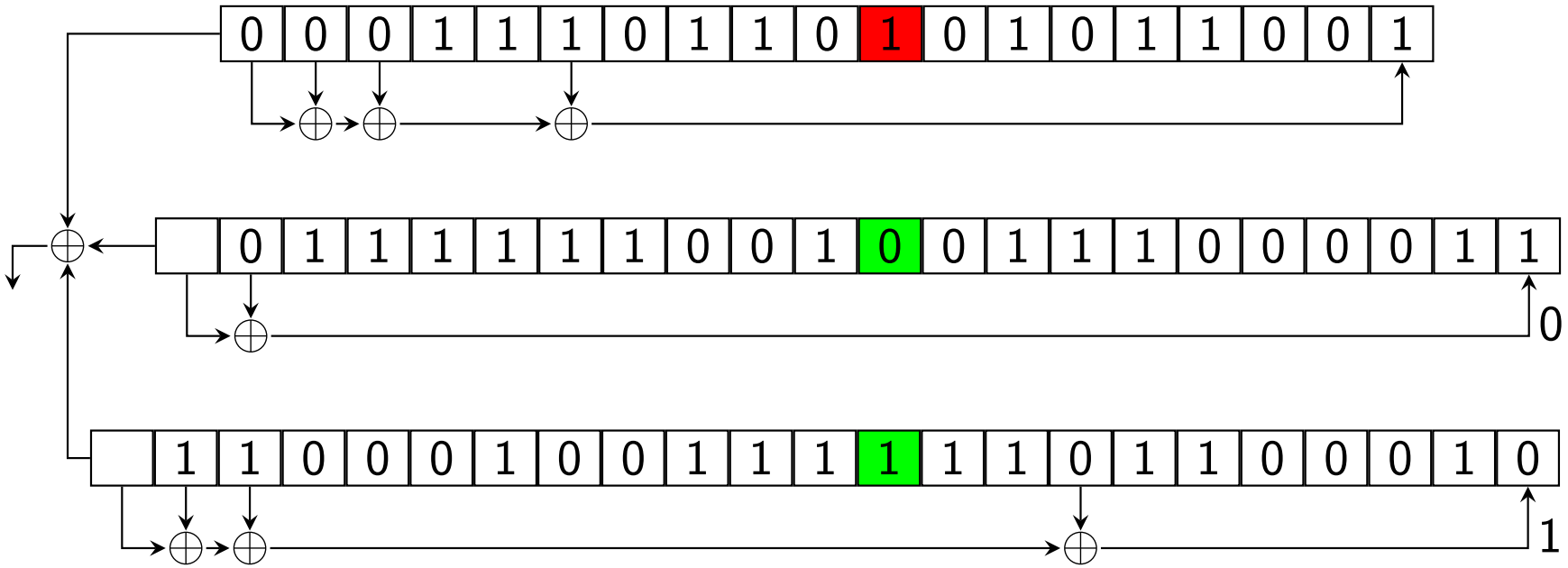


Stav v čase t mohl vzniknout

- krokováním všech tří registrů; ✗
- krokováním 1. a 2. registru; ✓
- krokováním 1. a 3. registru; nebo ✗
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t-1$:

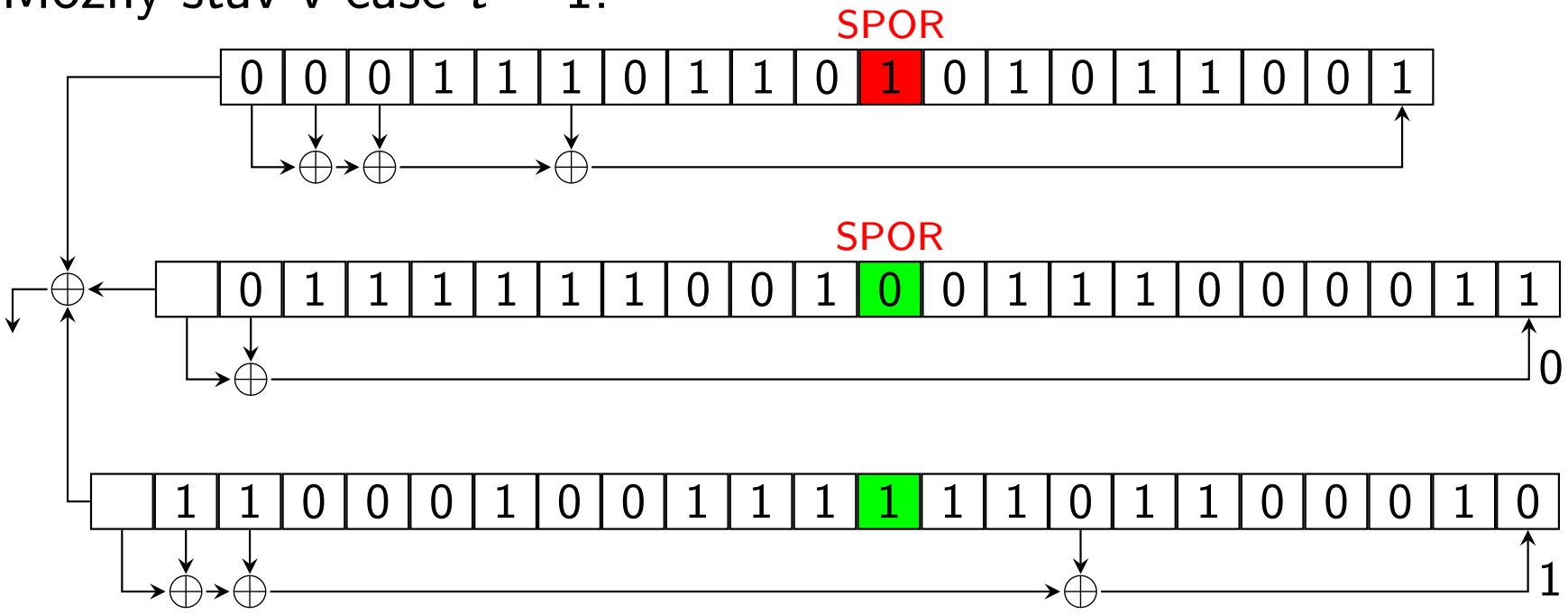


Stav v čase t mohl vzniknout

- krokováním všech tří registrů; ✗
- krokováním 1. a 2. registru; ✓
- krokováním 1. a 3. registru; nebo ✗
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t-1$:

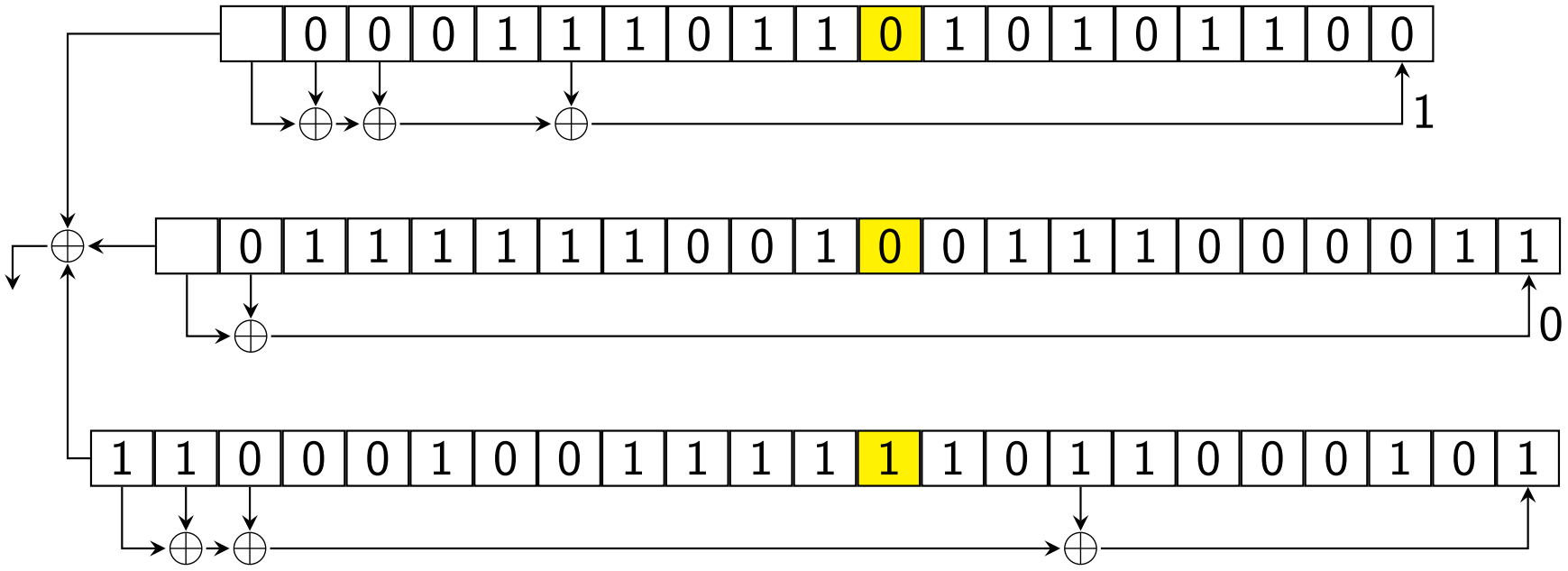


Stav v čase t mohl vzniknout

- krokováním všech tří registrů; ✗
- krokováním 1. a 2. registru; ✓
- krokováním 1. a 3. registru; nebo ✗
- krokováním 2. a 3. registru. ✗

Zpětný chod automatu šifry A5/1

Stav v čase $t-1$:

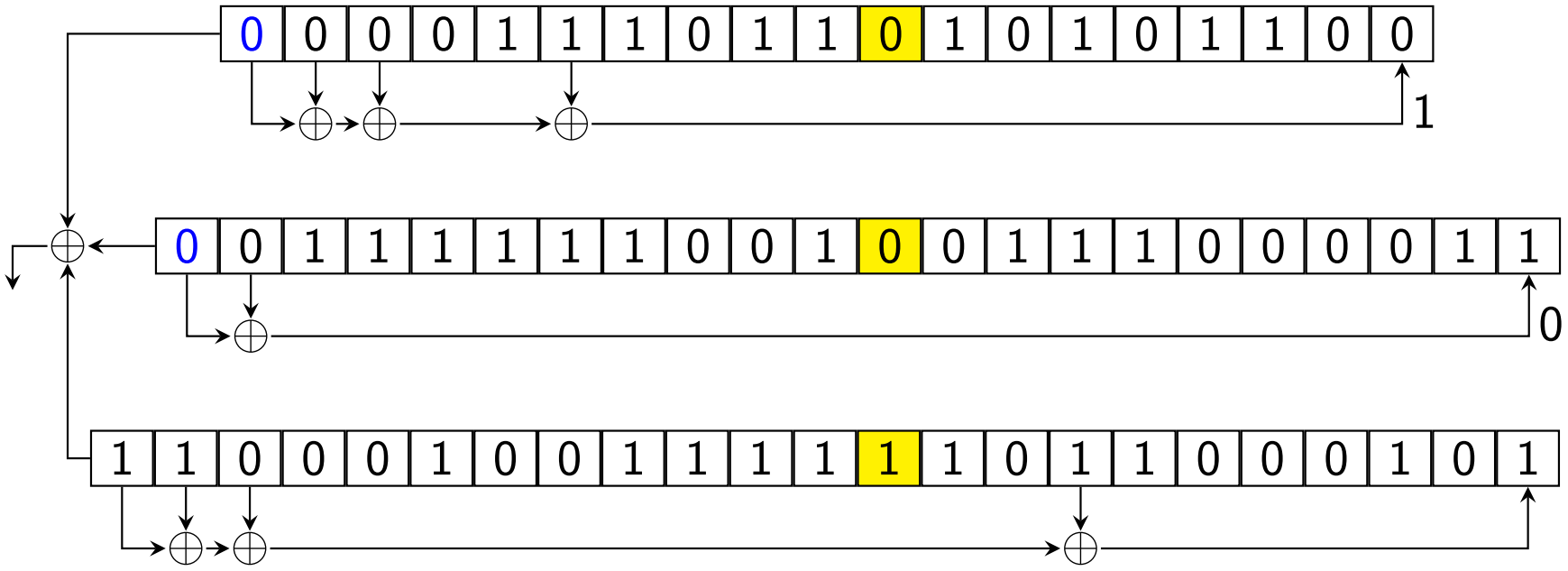


Stav v čase t mohl vzniknout

- krokováním všech tří registrů; ✗
- krokováním 1. a 2. registru; ✓
- krokováním 1. a 3. registru; nebo ✗
- krokováním 2. a 3. registru. ✗

Zpětný chod automatu šifry A5/1

Stav v čase $t-1$:

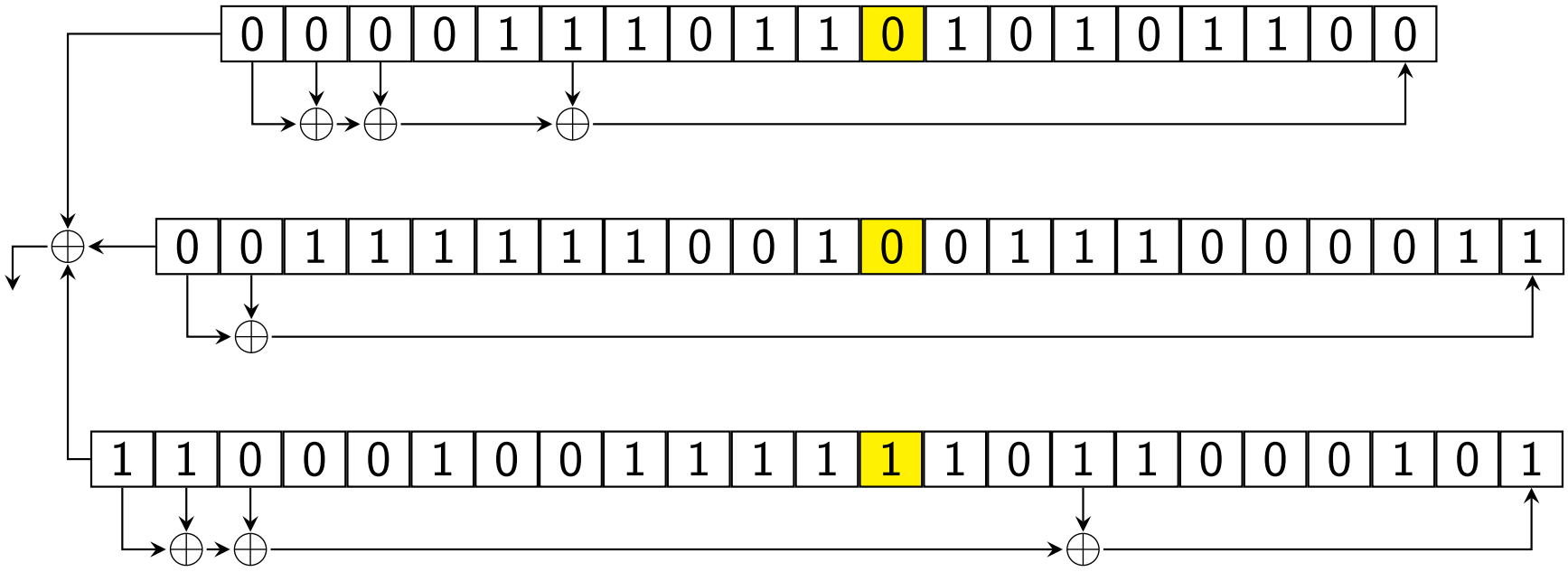


Stav v čase t mohl vzniknout

- krokováním všech tří registrů; ✗
- krokováním 1. a 2. registru; ✓
- krokováním 1. a 3. registru; nebo ✗
- krokováním 2. a 3. registru. ✗

Zpětný chod automatu šifry A5/1

Určete stav v čase $t-2$ ze znalosti stavu v čase $t-1$:

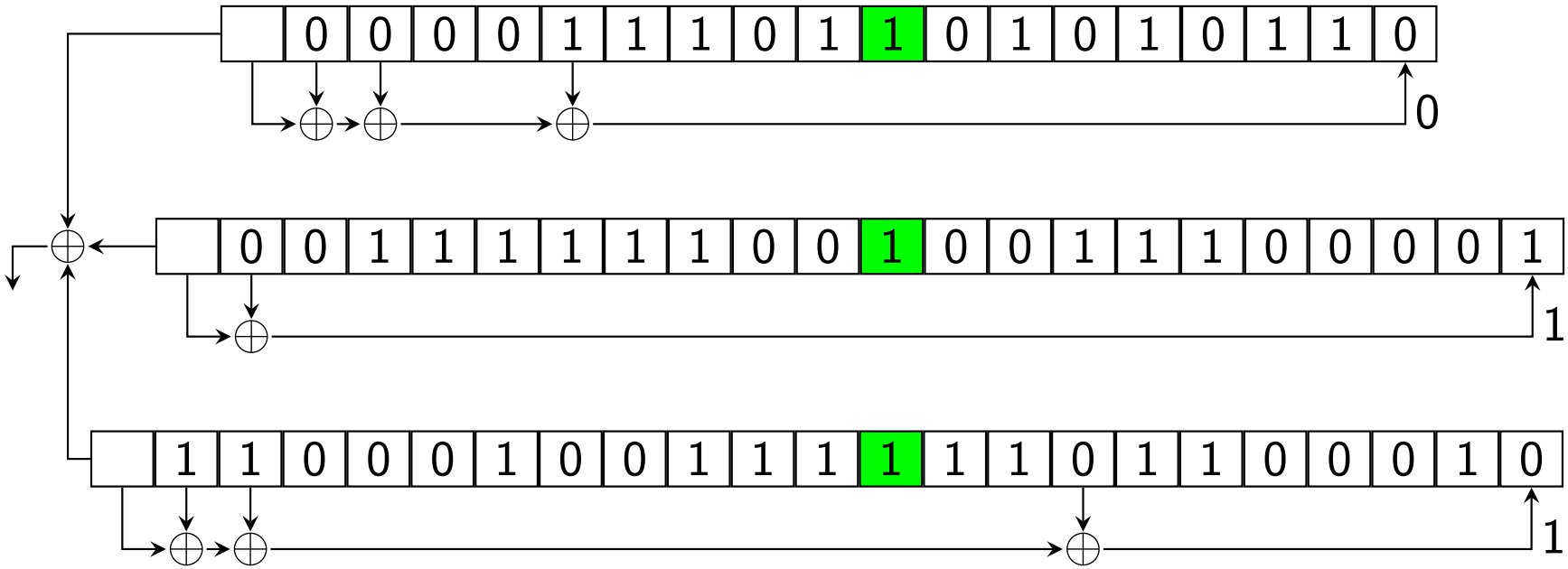


Stav v čase $t-1$ mohl vzniknout

- krokováním všech tří registrů;
- krokováním 1. a 2. registru;
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t - 2$:

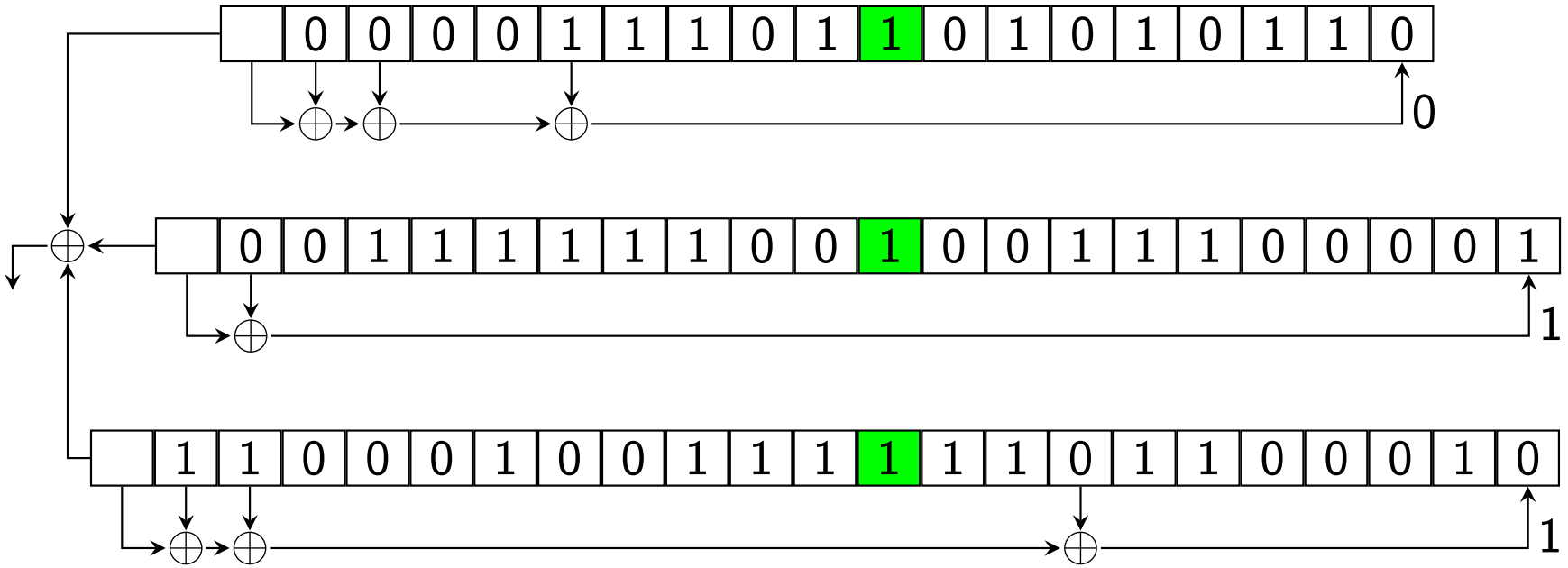


Stav v čase $t - 1$ mohl vzniknout

- krokováním všech tří registrů;
- krokováním 1. a 2. registru;
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t - 2$:

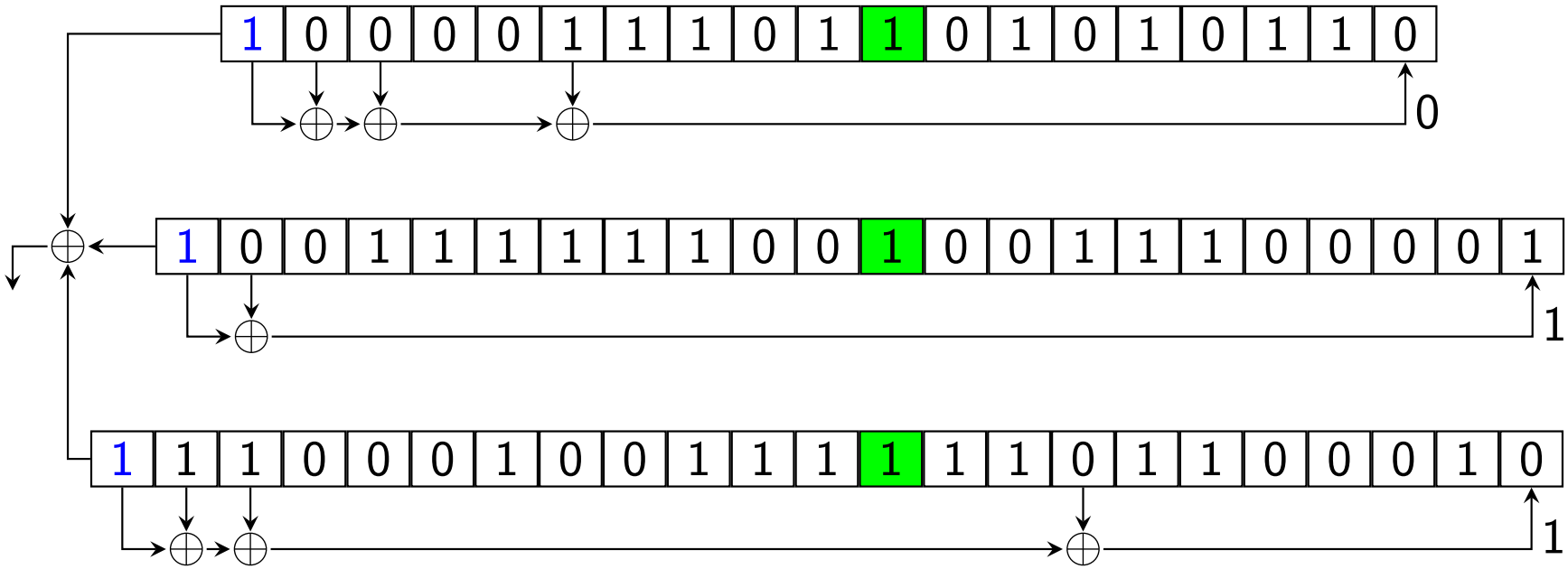


Stav v čase $t - 1$ mohl vzniknout

- krokováním všech tří registrů; ✓
- krokováním 1. a 2. registru;
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t - 2$:

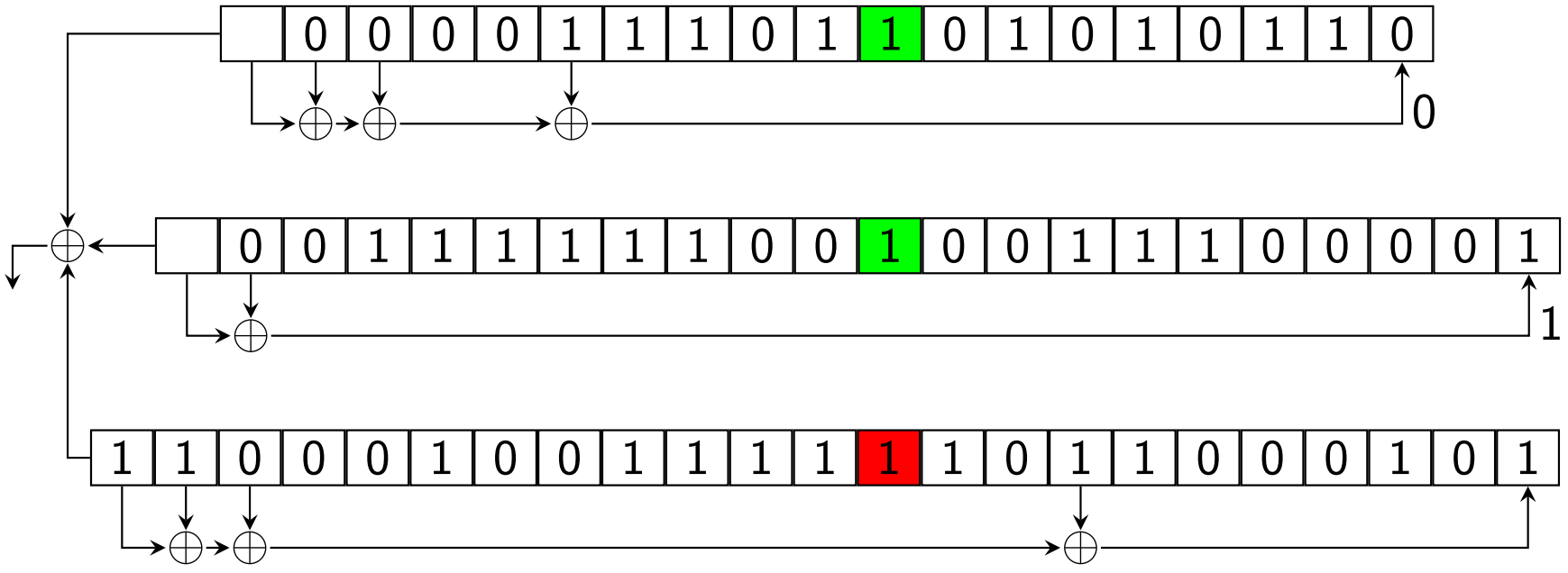


Stav v čase $t - 1$ mohl vzniknout

- krokováním všech tří registrů; ✓
- krokováním 1. a 2. registru;
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t - 2$:

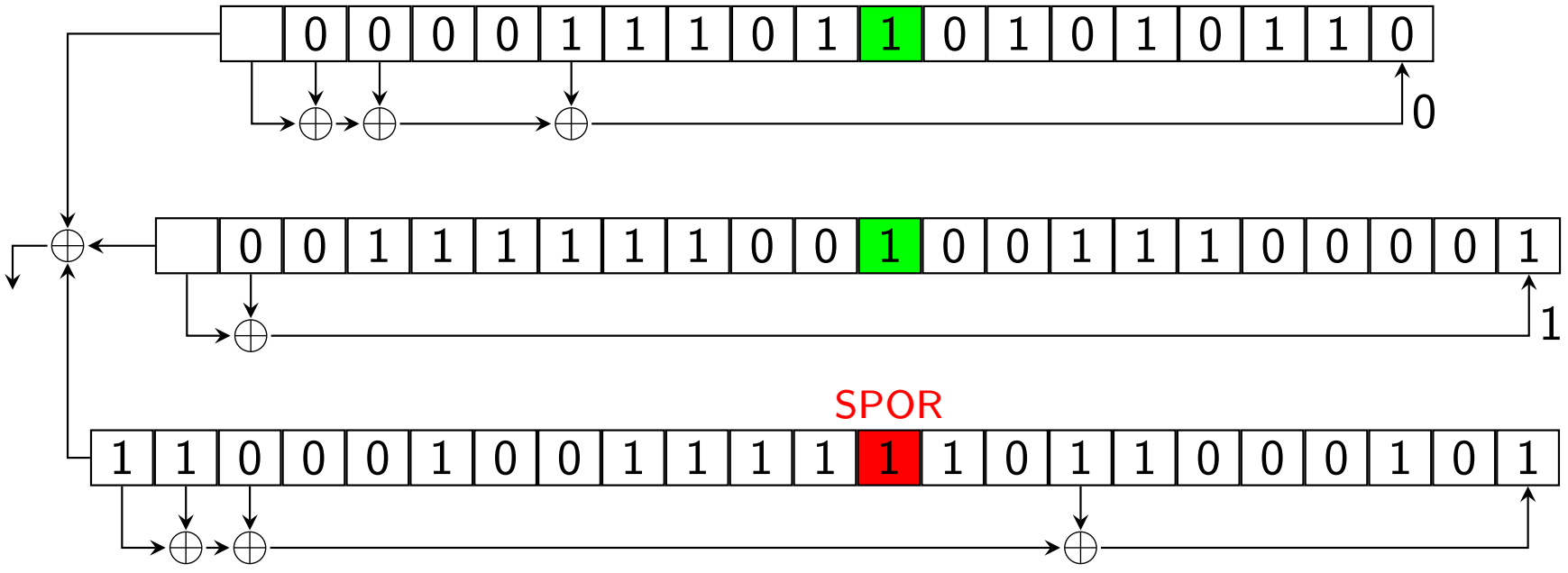


Stav v čase $t - 1$ mohl vzniknout

- krokováním všech tří registrů; ✓
- krokováním 1. a 2. registru;
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t - 2$:

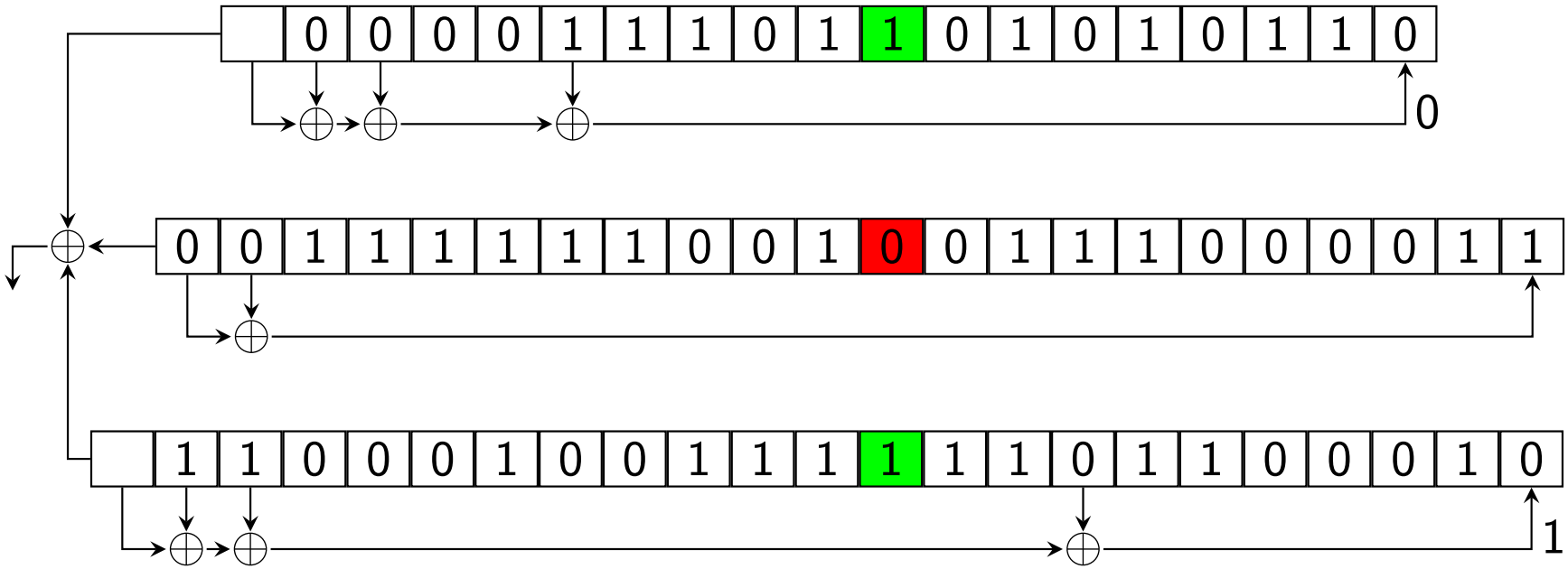


Stav v čase $t - 1$ mohl vzniknout

- krokováním všech tří registrů; ✓
- krokováním 1. a 2. registru; ✗
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t - 2$:

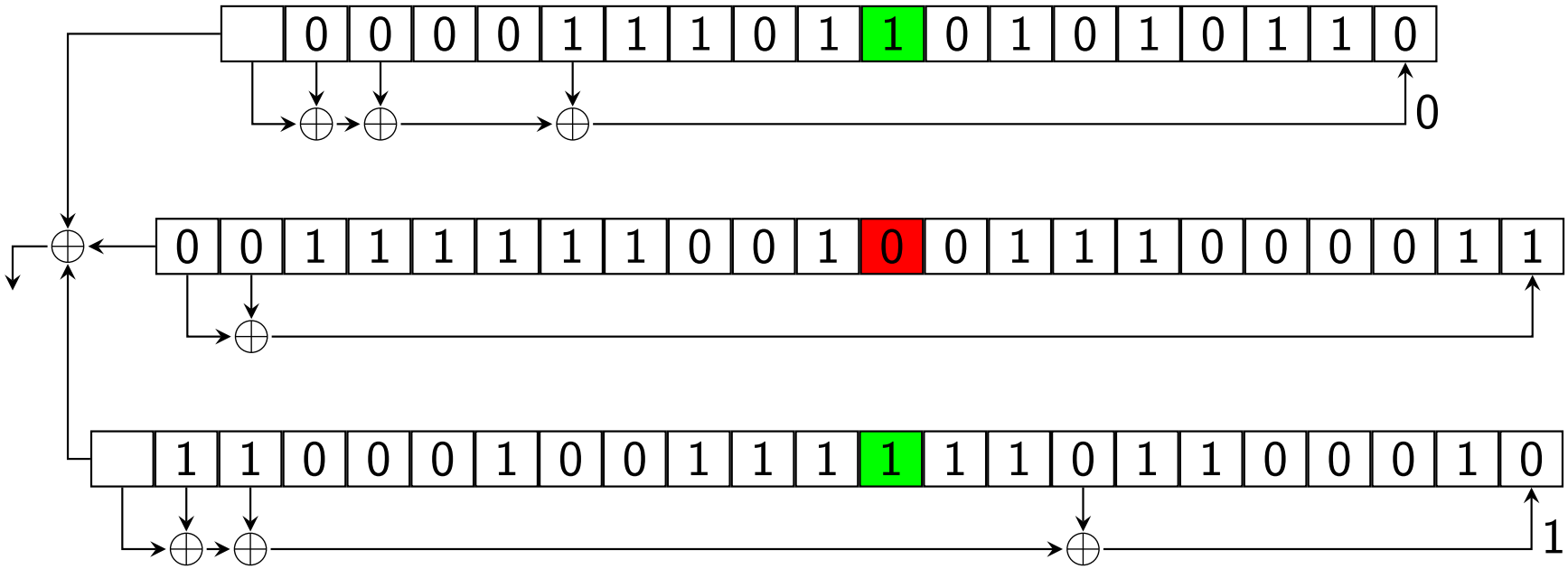


Stav v čase $t - 1$ mohl vzniknout

- krokováním všech tří registrů; ✓
- krokováním 1. a 2. registru; ✗
- krokováním 1. a 3. registru; nebo
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t - 2$:

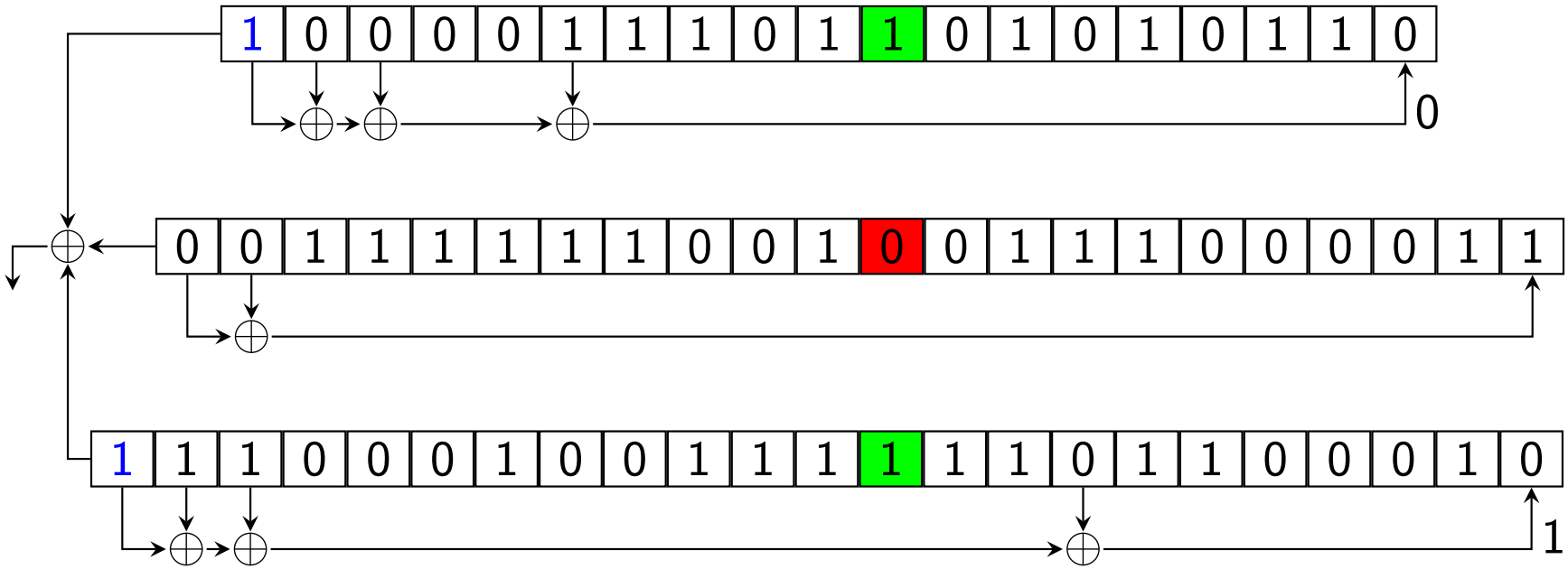


Stav v čase $t - 1$ mohl vzniknout

- krokováním všech tří registrů; ✓
- krokováním 1. a 2. registru; ✗
- krokováním 1. a 3. registru; nebo ✓
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t - 2$:

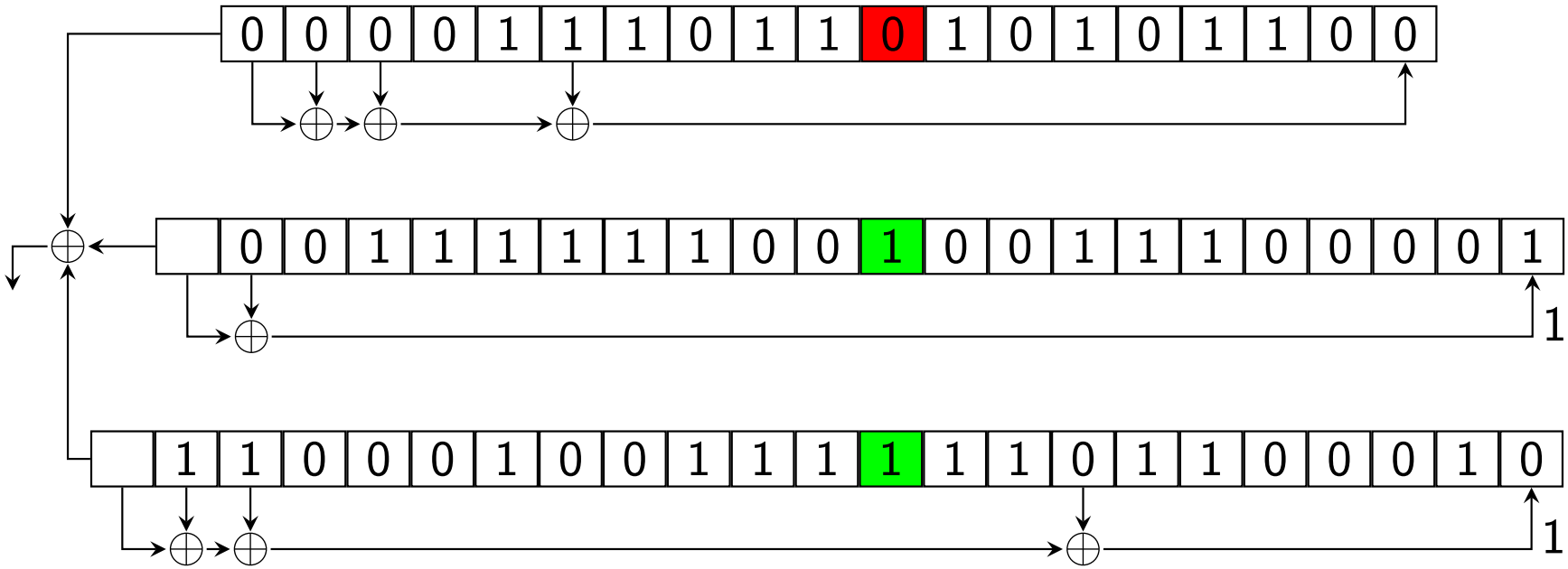


Stav v čase $t - 1$ mohl vzniknout

- krokováním všech tří registrů; ✓
- krokováním 1. a 2. registru; ✗
- krokováním 1. a 3. registru; nebo ✓
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t - 2$:

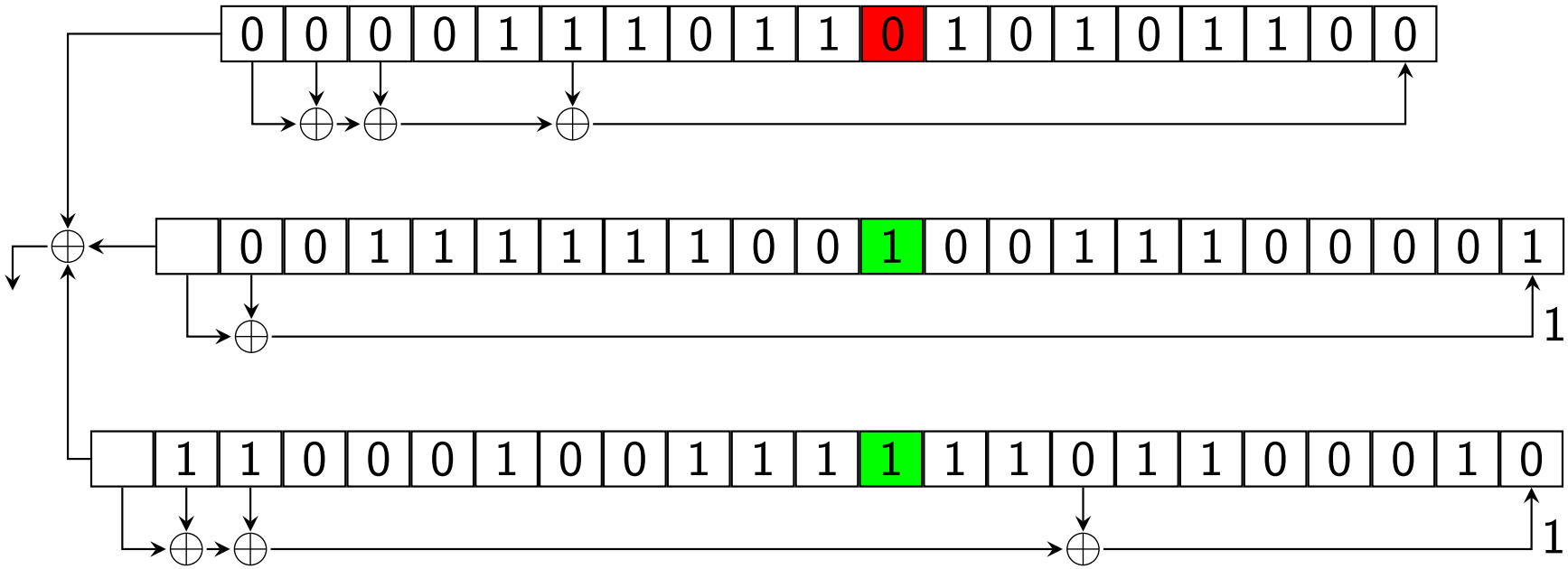


Stav v čase $t - 1$ mohl vzniknout

- krokováním všech tří registrů; ✓
- krokováním 1. a 2. registru; ✗
- krokováním 1. a 3. registru; nebo ✓
- krokováním 2. a 3. registru.

Zpětný chod automatu šifry A5/1

Možný stav v čase $t - 2$:

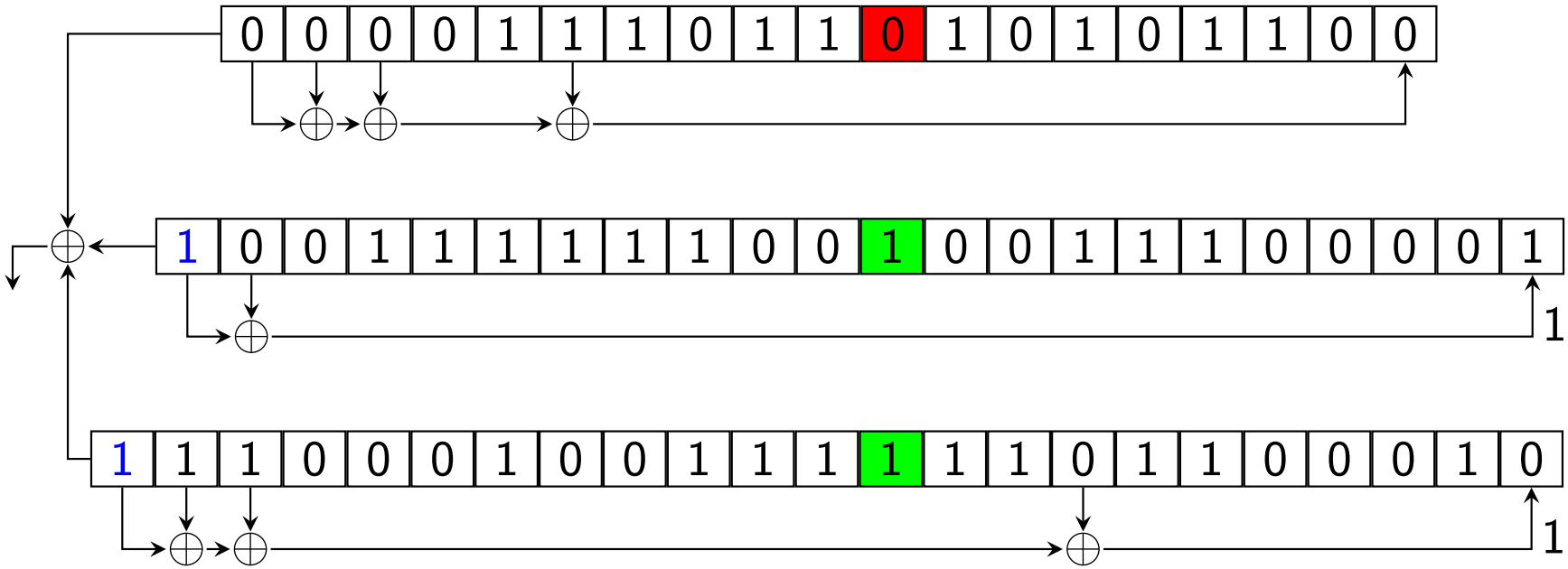


Stav v čase $t - 1$ mohl vzniknout

- krokováním všech tří registrů; ✓
- krokováním 1. a 2. registru; ✗
- krokováním 1. a 3. registru; nebo ✓
- krokováním 2. a 3. registru. ✓

Zpětný chod automatu šifry A5/1

Možný stav v čase $t - 2$:

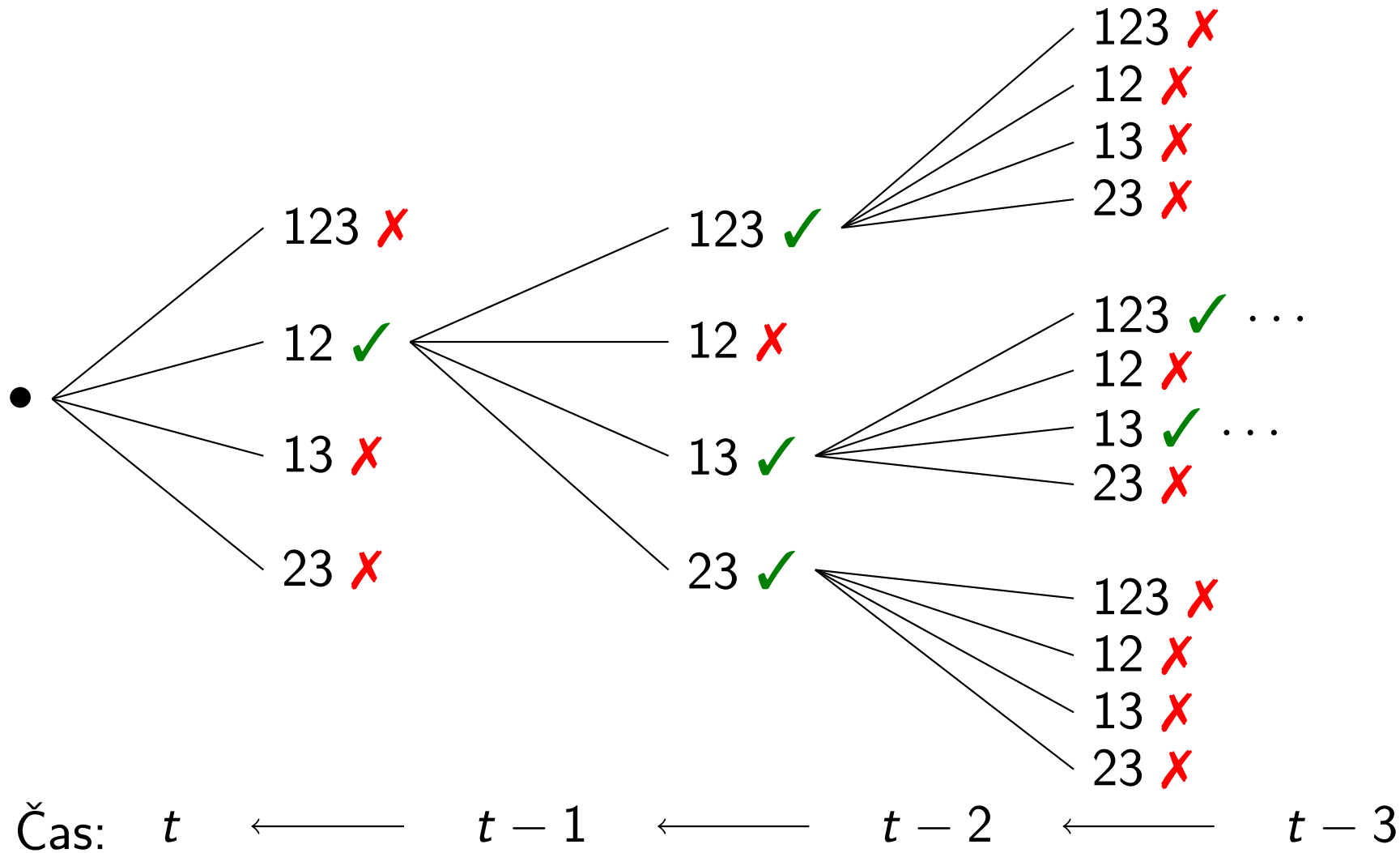


Stav v čase $t - 1$ mohl vzniknout

- krokováním všech tří registrů; ✓
- krokováním 1. a 2. registru; ✗
- krokováním 1. a 3. registru; nebo ✓
- krokováním 2. a 3. registru. ✓

Zpětný chod automatu šifry A5/1

Kdybychom pokračovali ve zpětném průzkumu, dostali bychom následující strom možných krokování:



Zpětný chod automatu šifry A5/1

Je snadné ověřit, že ze všech 2^{64} stavů automatu:

- $\frac{3}{8}$ stavů nemají žádného předchůdce,
- $\frac{13}{32}$ stavů má jednoho předchůdce,
- $\frac{3}{32}$ stavů mají dva předchůdce,
- $\frac{3}{32}$ stavů mají tři předchůdce,
- $\frac{1}{32}$ stavů má čtyři předchůdce.

Vážený průměr počtu předchůdců je

$$\frac{3}{8} \cdot 0 + \frac{13}{32} \cdot 1 + \frac{3}{32} \cdot 2 + \frac{3}{32} \cdot 3 + \frac{1}{32} \cdot 4 = 1.$$

V průměru má každý stav jednoho předchůdce.

Připomenutí algoritmu šifry A5/1

Inicializace

1. Sřetěz: $u :=$ klíč $\|$ číslo rámce (Máme $64 + 22 = 86$ bitů.)
2. Vynuluj registry.
3. Pro $i = 0, \ldots, 85$:
   $R_1[0] = R_1[0] \oplus u_i$
   $R_2[0] = R_2[0] \oplus u_i$
   $R_3[0] = R_3[0] \oplus u_i$
   Krokuj všechny tři registry. (Neber ohled na krokovací bity.)
4. Proveď 100 kroků automatu. (Bez výstupu.)

Generování hesla s

- Pro $i = 0, \ldots, 227$:
  Krokuj automat.
  $s_i := R_1[18] \oplus R_2[21] \oplus R_3[22]$.

Útoky na šifrování v GSM

- Typický průběh útoku:
  - Odhalí vnitřní stav automatu a následně K_c.
  - Typicky jde o time/memory/data tradeoff útoky.
  - Útoku předchází náročný jednorázový předvýpočet. (Lze provést paralelně na více počítačích.)

- Barkan, Biham, Keller (2003): ciphertext-only útok.
  - Využívá toho, že se před šifrováním aplikuje samoopravný kód, který do otevřeného textu vnáší redundanci.
  - Příklad útoku na A5/1: (uvažujeme 2 GHz CPU)
    - Data o délce 64 vteřin hovoru.
    - Předvýpočet: 2800 CPU roků, 50 TB dat.
    - Doba luštění: 13,33 CPU minut.
  - Stačí i 8 vteřin hovoru, avšak za cenu náročnějšího předvýpočtu a delší doby luštění.

Útoky na šifrování v GSM

- Barkanův-Bihamův-Kellerův útok lze využít také na A5/2:
  - Data o délce zlomku vteřiny hovoru.
  - Předvýpočet: 10 CPU minut, 4 GB dat.
  - Doba luštění: zlomek vteřiny.
- Aktivní útok
  - Základnová stanice se telefonu nijak neautentizuje.
  - Útočník se může vydávat za základnovou stanici a požádat telefon, aby použil šifru A5/2.
  - Útočník odhalí klíč pro A5/2.
  - Klíč pro A5/1 je shodný s klíčem pro A5/2.
- K. Nohl (2010): known-plaintext útok na A5/1
  - Využívá zašifrované řídící zprávy, jejichž obsah je známý.
  - Předvýpočet: 4 GPU měsíce, 2 TB dat.
  - Doba luštění: 10 GPU vteřin.
  - Pravděpodobnost úspěchu: 90 %.