ABC: A New Fast Flexible Stream Cipher

Vladimir Anashin
Andrey Bogdanov*
Ilya Kizhvatov

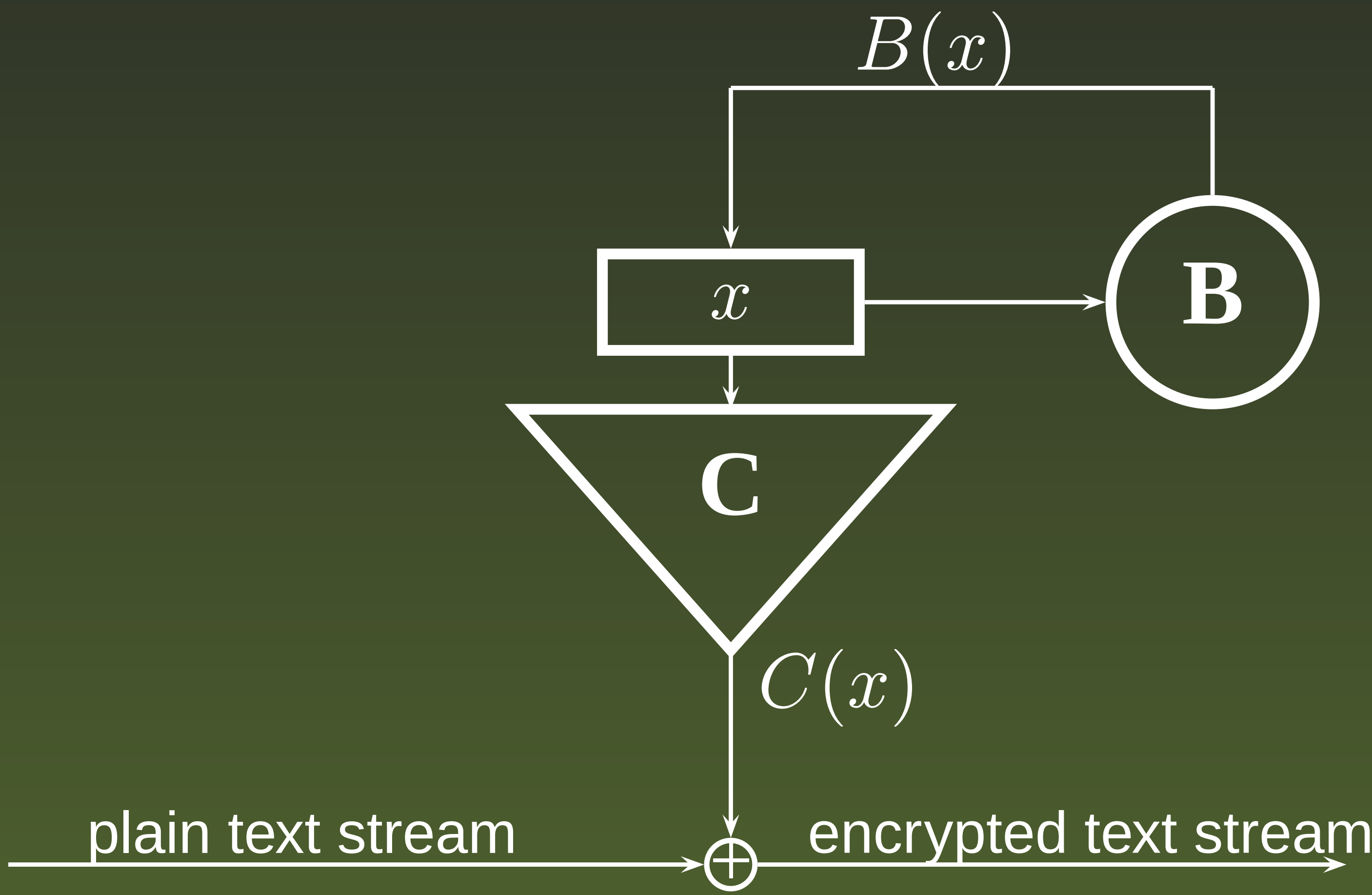
Russian State University for the Humanities
Faculty of Information Security

*Partially supported by the Institute for Experimental Mathematics, University of Duisburg-Essen, Germany

Motivation

- A highly flexible framework for manufacturing fast and secure stream ciphers.
- Illustration of our efficient techniques resting upon p-adic analysis and automata theory.
- Simplicity of design.

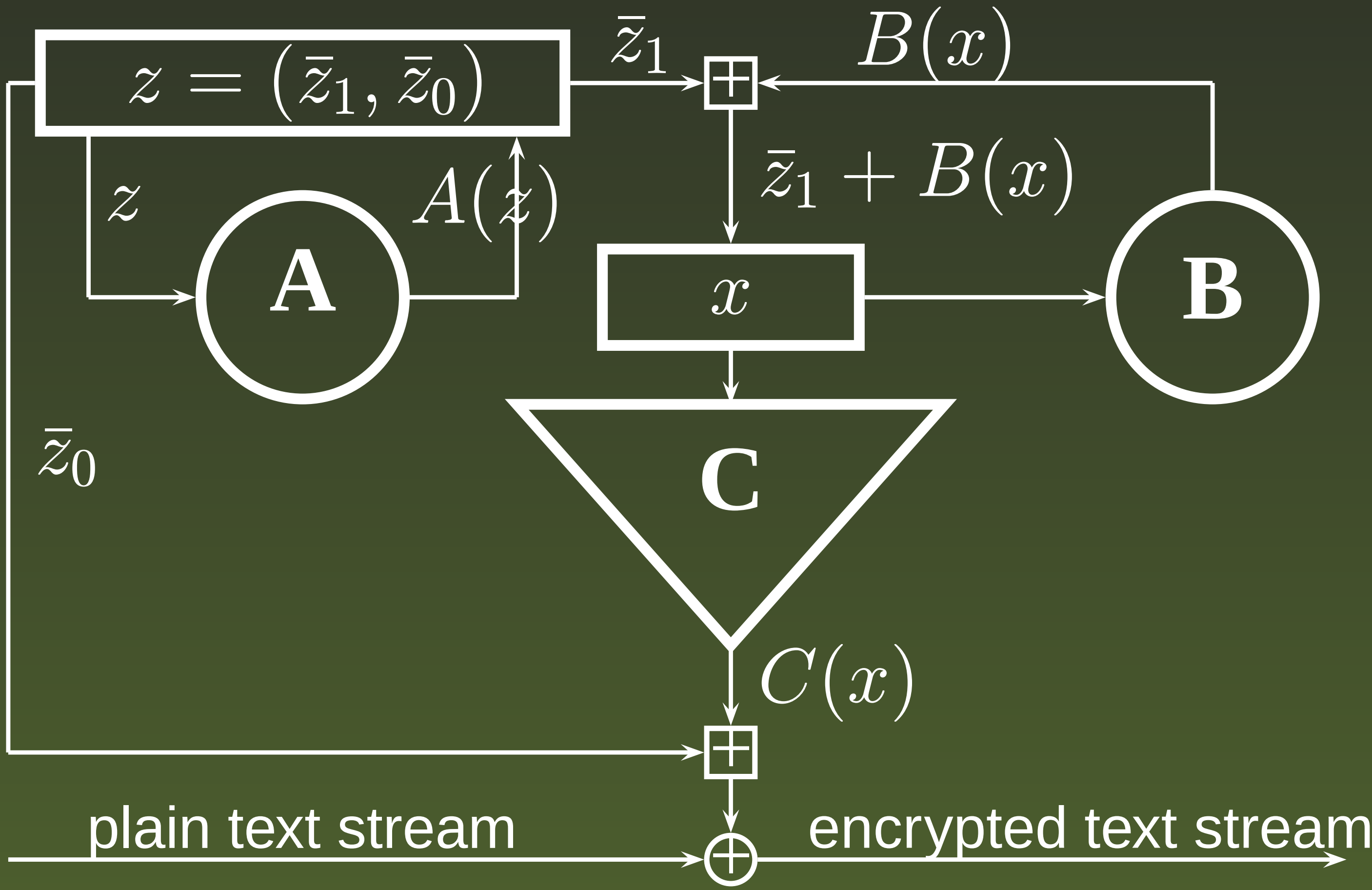
Traditional design of PRNG



B state transition function, period and distribution

C non-linear filter function, other crypto properties

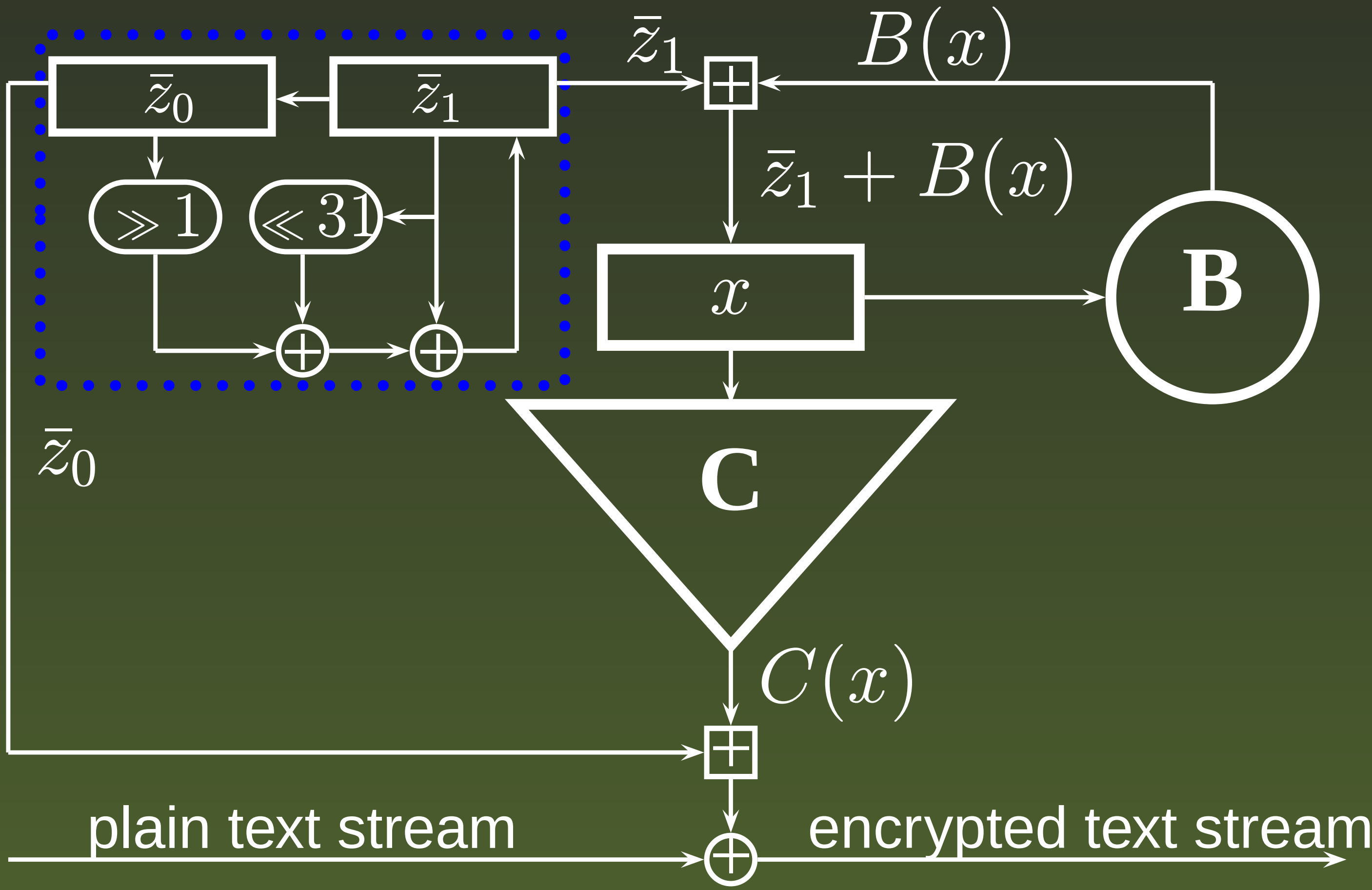
The ABC design pattern



$$\boxplus \;=\; + \pmod{2^{32}}$$

$$\oplus \;=\; \text{XOR}$$

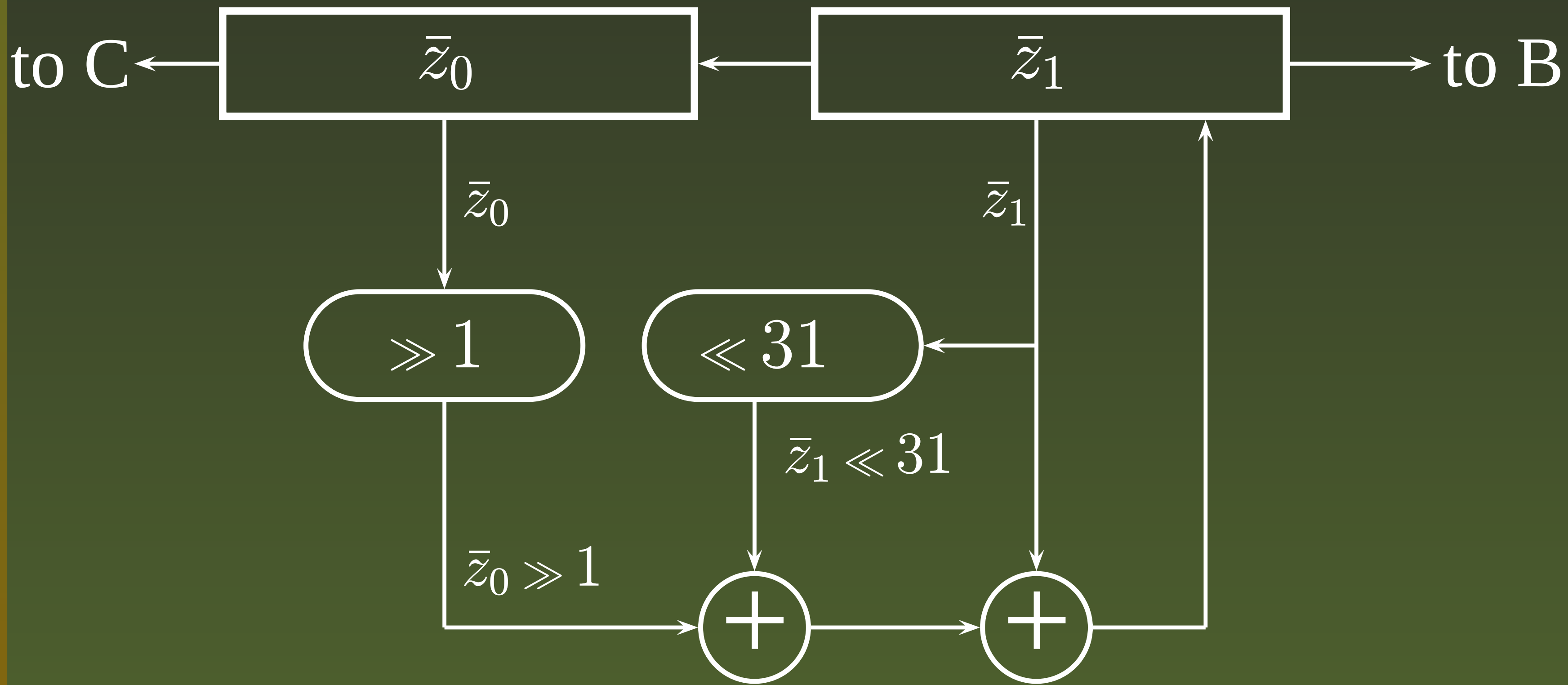
ABC: Function A



A : LFSR of period $2^{63} - 1$ for each 32-bit half

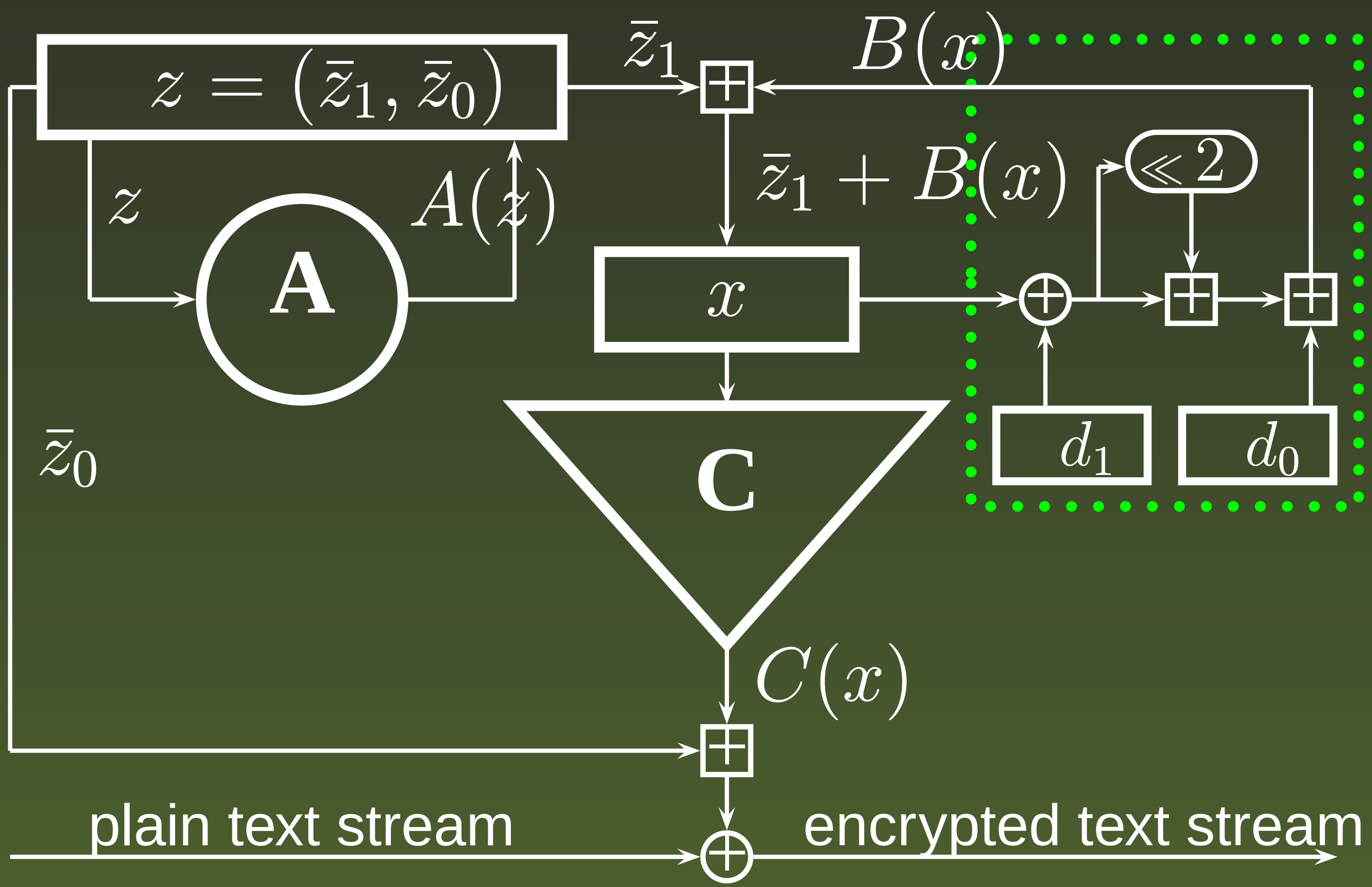
ABC: Function A in Detail

$$\phi(\theta) = (\theta^{63} + \theta^{31} + 1)\theta$$



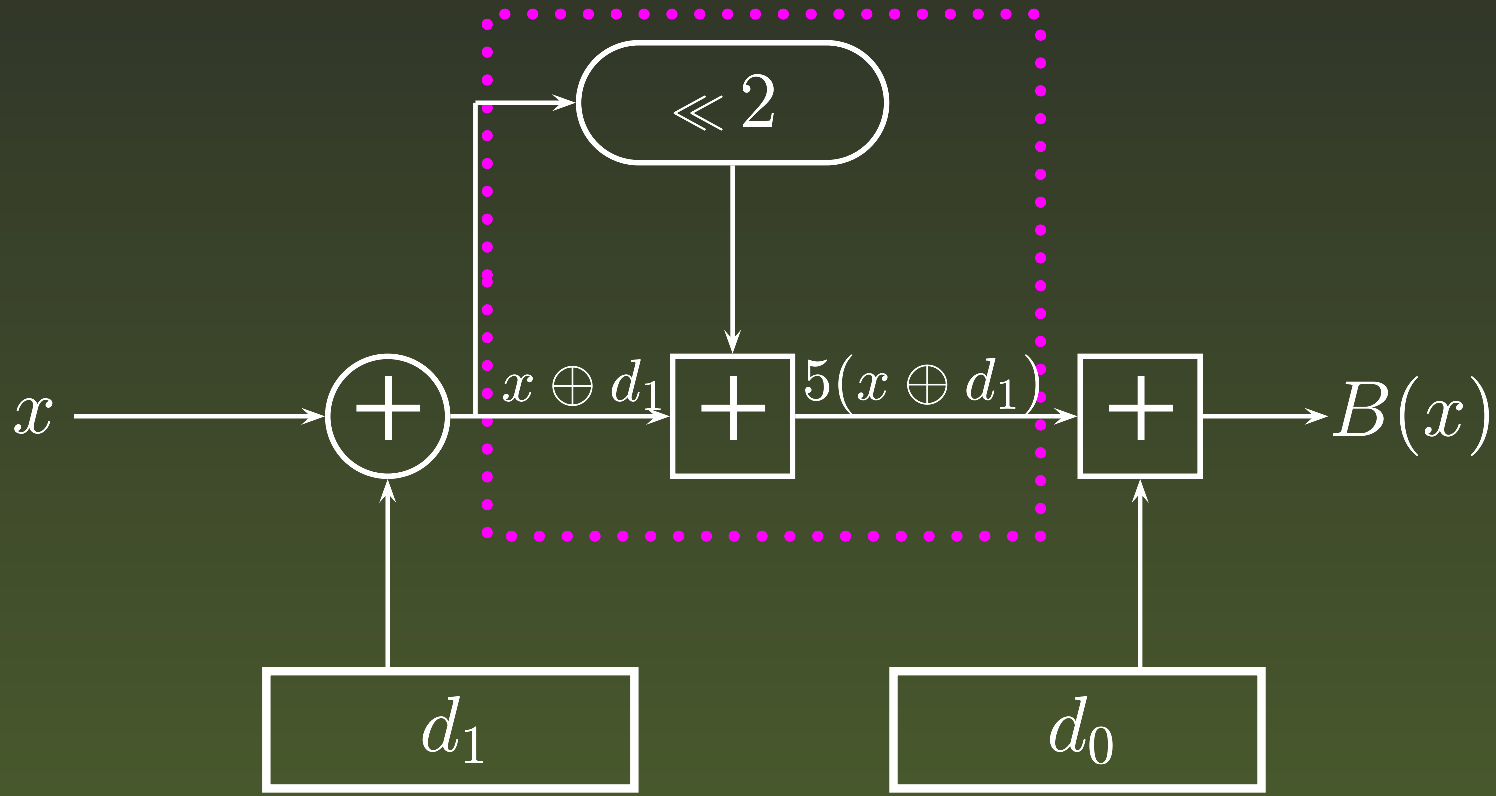
$A:$ Word oriented computation of LFSR

ABC: Function B



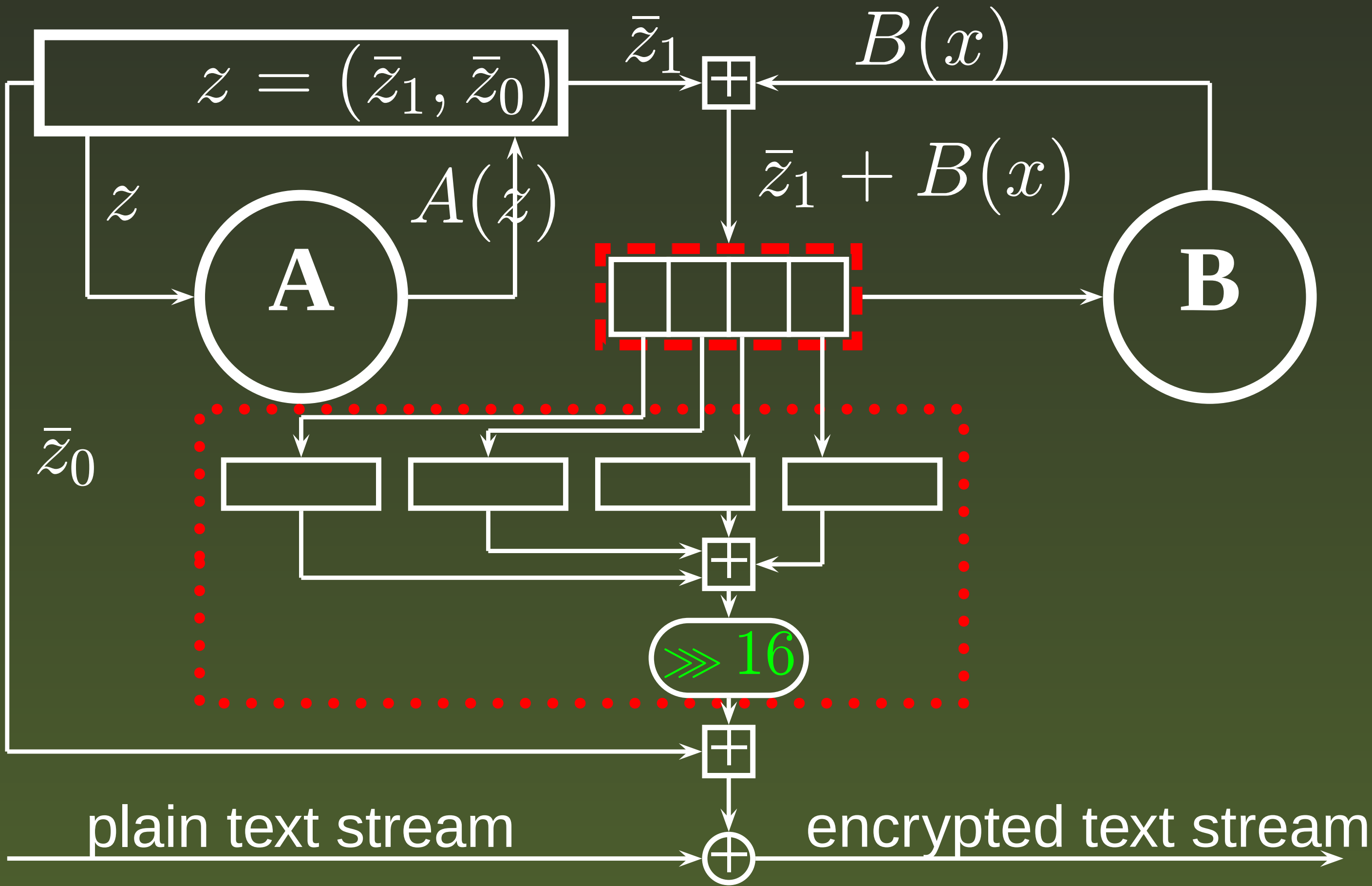
B : Defines a single cycle permutation over $\mathbb{Z}/2^{32}\mathbb{Z}$

ABC: Function B in Detail



$$B(x) = d_0 + 5(x \oplus d_1) \pmod{2^{32}}$$

ABC: Function C



ABC: Function C in Detail

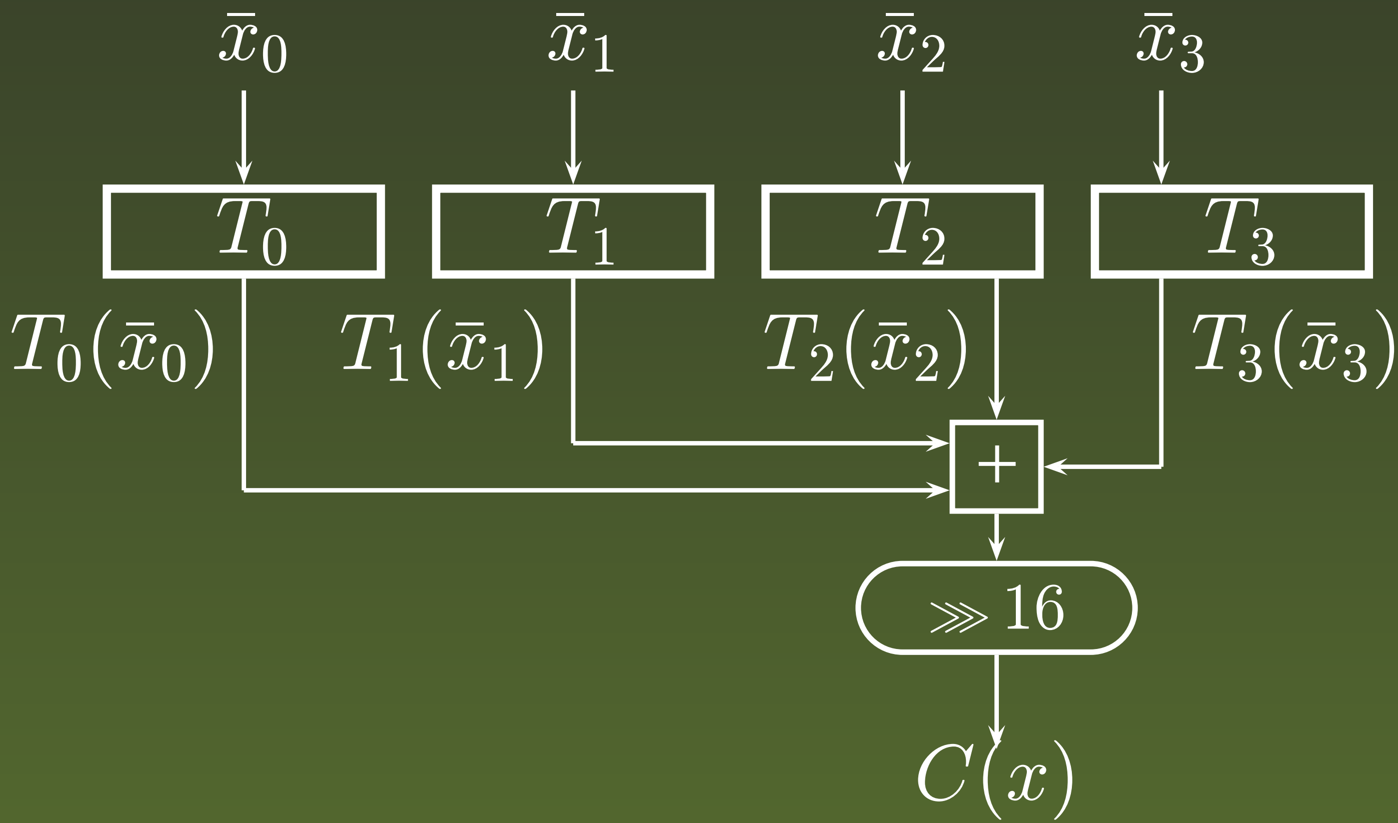
- $S(x) = e + \sum_{i=0}^{31} e_i \delta_i(x) \pmod{2^{32}}$, where
  - $\delta_i(x) \in \{0, 1\}$ = the i-th bit of x,
  - $e,\ e_i \in \mathbb{Z}/2^{32}\mathbb{Z}$,
  - $e_{31} \equiv 2^{16} \pmod{2^{17}}$.
- $C(x) = S(x) >>> 16 \pmod{2^{32}}$.
- **NB! Not**

$$\mathbf{C}(\mathbf{x}) = \mathbf{S}(\mathbf{x}) + (\mathbf{S}(\mathbf{x}) >>> \mathbf{16}) \pmod{\mathbf{2^{32}}}$$

as in the contribution submitted to SKEW 2005!

ABC: Function C in Detail

$$S(x) = e + \sum_{i=0}^{7} e_i \delta_i(x) + \cdots + \sum_{i=24}^{31} e_i \delta_i(x) \pmod{2^{32}}$$

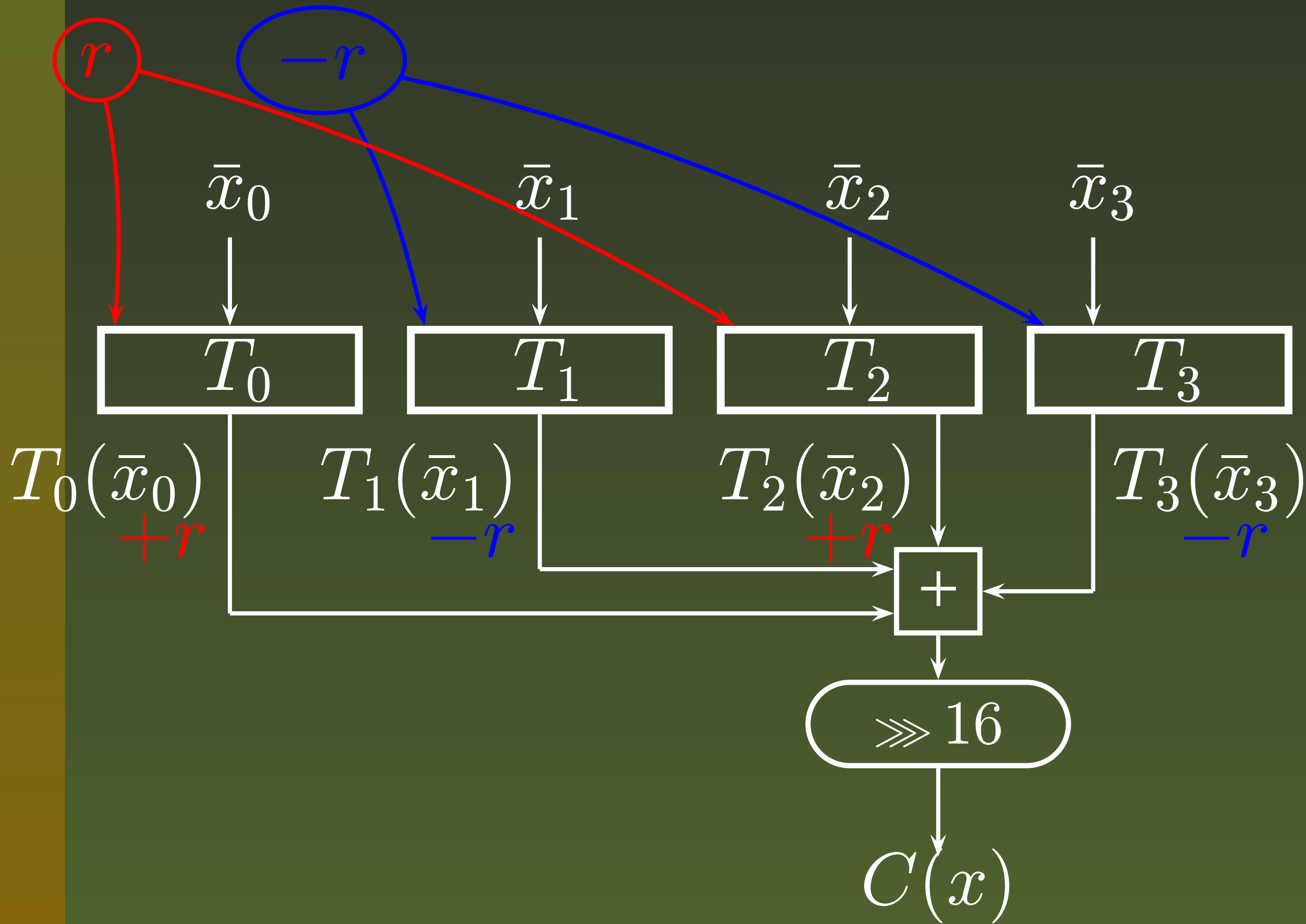


ABC: Function C, SCA

In applications subject to SCA we recommend to use masking:

- Modify each table by adding a random r or its additive inverse $-r$ to the table elements depending on the parity of the table number.

ABC: Function C, SCA



Properties of the ABC design pattern

Provable properties of the ABC key stream:

- The period of $(2^{63}-1)\cdot 2^{32}$ words;
- Uniformly distributed key stream: $\forall$ 32-bit word a the number $\mu(a)$ of occurrences of a on the period satisfies:

$$\left|\frac{\mu(a)}{(2^{63}-1)\cdot 2^{32}}-\frac{1}{2^{32}}\right|<\frac{1}{\sqrt{(2^{63}-1)\cdot 2^{32}}};$$

- High linear complexity λ of the key stream: $2^{31}\cdot(2^{63}-1)+1\geq\lambda\geq 2^{31}+1.$

Properties of ABC circuit: Notes

- As a matter of fact we have proved the group of statements for a larger class of A, B, C. Thus, the designer can choose the maps suitable for the specific requirements.
- Note that the fact that these crucial security properties are proven does not exclude the necessity to analyse the concrete representations of A, B and C with respect to the whole set of cryptographical attacks.

ABC: Key dependence, State space

The following values can be (almost) freely defined without worsening the security properties of the resulting ABC mapping:

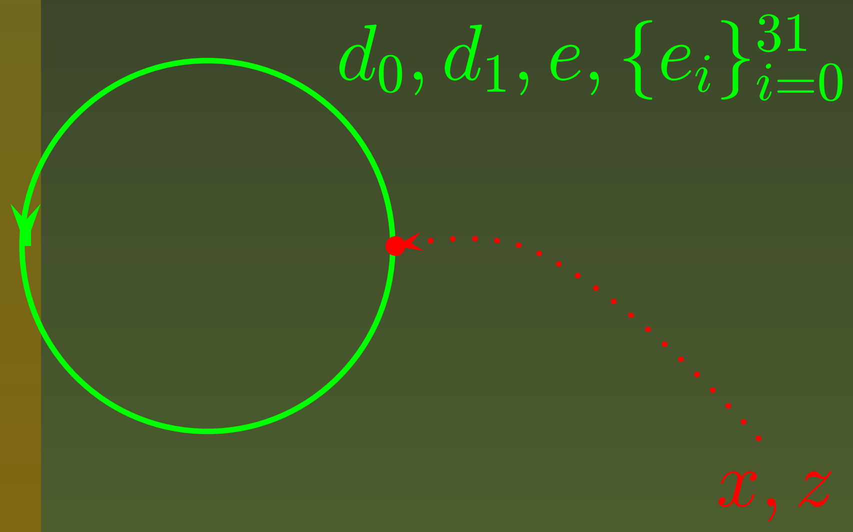
- A: The initial state $z \in \mathbb{Z}/2^{32}\mathbb{Z}$;
- B: The coefficients $d_0, d_1 \in \mathbb{Z}/2^{32}\mathbb{Z}$ and initial state $x \in \mathbb{Z}/2^{32}\mathbb{Z}$;
- C: The coefficients $e, e_1, \ldots, e_{31} \in \mathbb{Z}/2^{32}\mathbb{Z}$.

NB! All up to restrictions imposed above!
Altogether we have **1195 bits** to be freely set. Note that not all the bits have the same impact on the security of the cipher.

ABC: Key dependence, Cycles

The ABC stream cipher defines a family of cycles of length $2^{32}(2^{63}-1)$ words in the following way:

- $d_0, d_1, e, e_1, \ldots, e_{31}$ define a concrete cycle of length $P = 2^{32}(2^{63}-1)$;



- x, z select a start point on the cycle defined (exactly $2^{32}(2^{63}-1)$ variants).

ABC: Speed & Memory consumption

- A ***generic* reference C** implementation on a standard 3.2 GHz Intel Pentium 4 processor under Linux.
- Minimum **132** byte memory used.

w	Speed, Gbps	Cycles per byte	Table memory, bytes
2	2.25	11.38	256
4	4.24	6.04	512
8	**6.86**	3.73	4096

ABC: Conclusion

- Freedom to choose mappings A, B, C;
- Important security properties are ***proven***;
- Novel approach to ***counter-dependence***;
- High degree of ***key-dependence***;
- ***Key*** material usage ***flexibility***;
- High ***flexibility*** in terms of ***memory consumption***;
- Extremely high throughput rate of a ***generic*** ANSI C implementation - **6.9 Gbps, or 3.7 clocks/byte** on a Pentium 4 processor.