The XCBC-XOR, XECB-XOR and XECB-MAC Modes

Virgil D. Gligor **Pompiliu Donescu**

VDG Inc
6009 Brookside Drive
Chevy Chase, Maryland 20815

{gligor, pompiliu}@eng.umd.edu

August 24, 2001

Outline

1. Security Claims

2. Operational Claims

3. Examples: XCBC-XOR, XECB-XOR, XECB-MAC modes

4. Conclusions

1. Security Claims for Authenticated Encryption

1. *Security* ***Claim*** = a security *notion* supported by
a mode or scheme of encryption

2. ***Secrecy Notion*** = < Indistinguishability, adaptive Chosen Plaintext Attacks>

3. ***Integrity (Authenticity) Notion*** = < Existential Forgery protection,
(adaptive) Chosen Plaintext Attacks>

2. Operational Claims for Modes of Encryption

Operational Notion = < operational goal, mode characteristics >

Operational ***Goals:*** cost-performance, simplicity, usability

- cost-performance:
  - power consumption
  - speed (no. of block-cipher invocations, latency)
  - implementation cost (e.g., hardware "real-estate'')
- simplicity
  - single key
  - specifications (e.g., simple operations)
  - same basic structure for
    - authenticated encryption
    - ciphertext authentication (two-pass, two keys)
    - plaintext authentication (MAC)
- usability in different environments
  - various keying-state protection mechanisms needed
  - availability of random number generators,
  - error recovery (ECC, no recovery vs. partial recovery)

Operational Characteristics of Modes

State: stateless, stateful-sender, stateful

Degree of parallelism

- none (sequential)
- interleaved (known/negotiated no. of processing units for parallel operation)
- architecture-independent
  - independent of no. of processing units
  - same overhead for parallel, pipelined or sequential operation
  - out-of-order processing, incremental

Error recovery

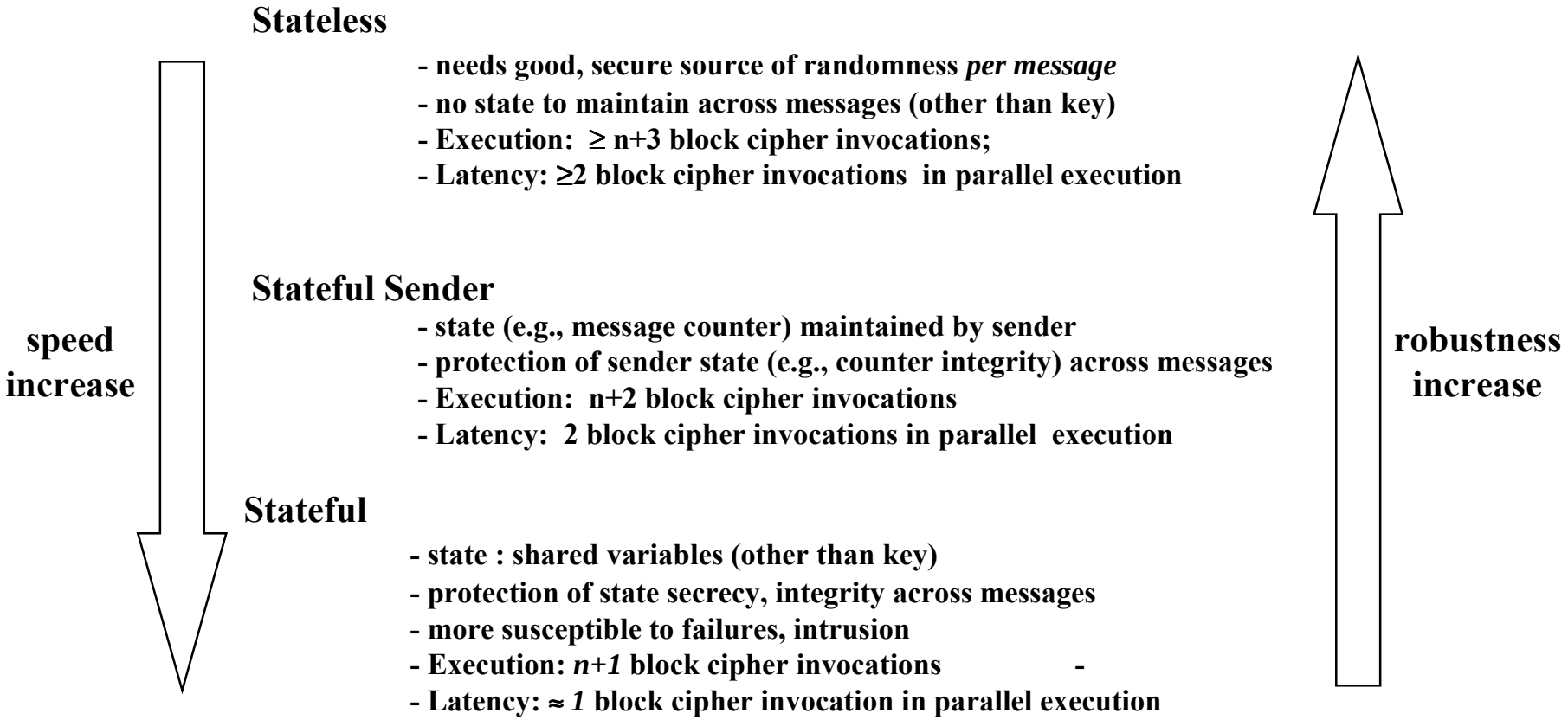
- interleaving provides some support on a per-segment basis

Separation of Confidentiality and Integrity protection (e.g., two-pass, two keys)

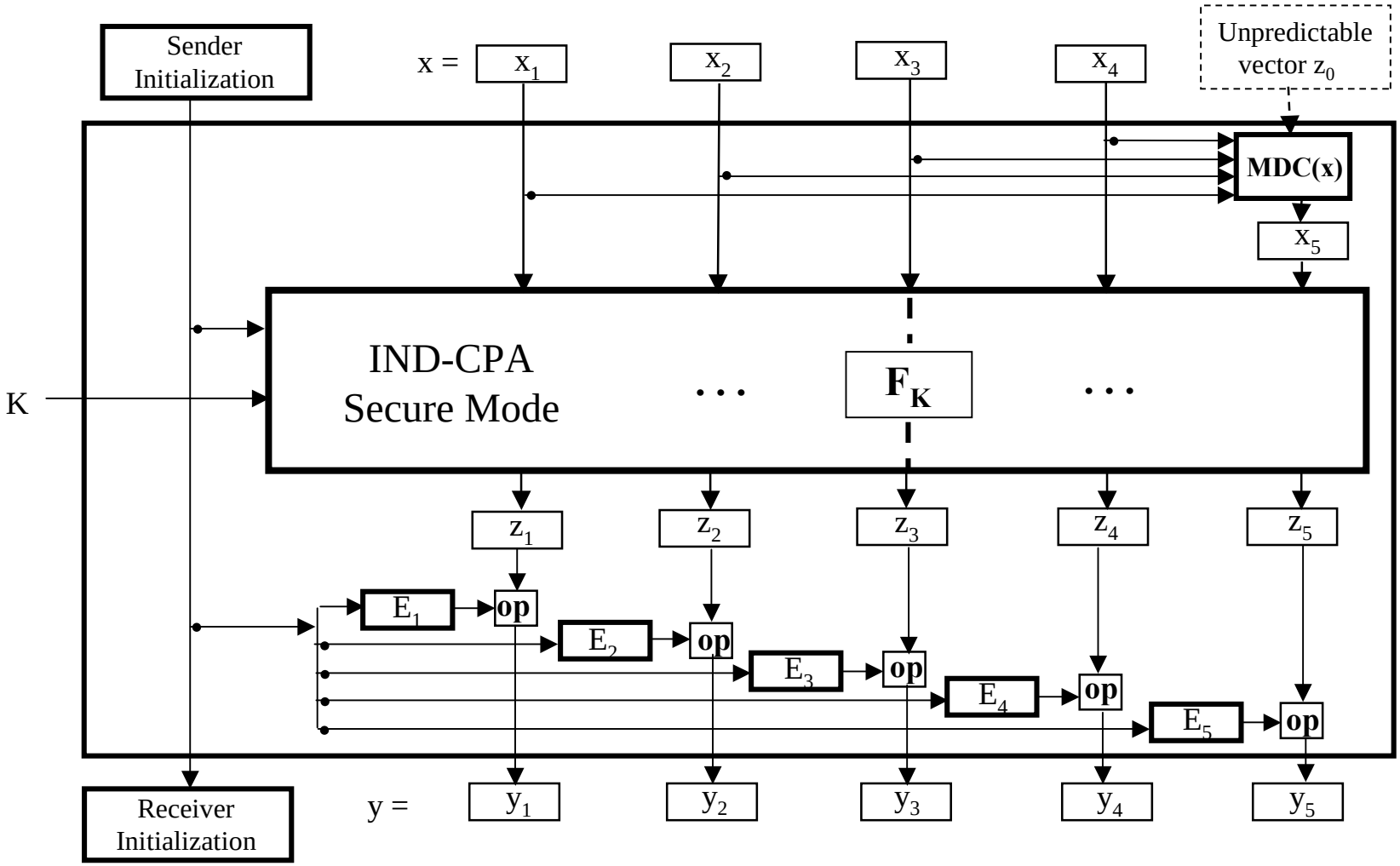
Padding

- avoid added block-cipher invocation if message length is a multiple no. of blocks.
- avoid added latency (1 block-cipher invocation) caused by “ciphertext stealing”

Examples of State Characteristics of a Mode

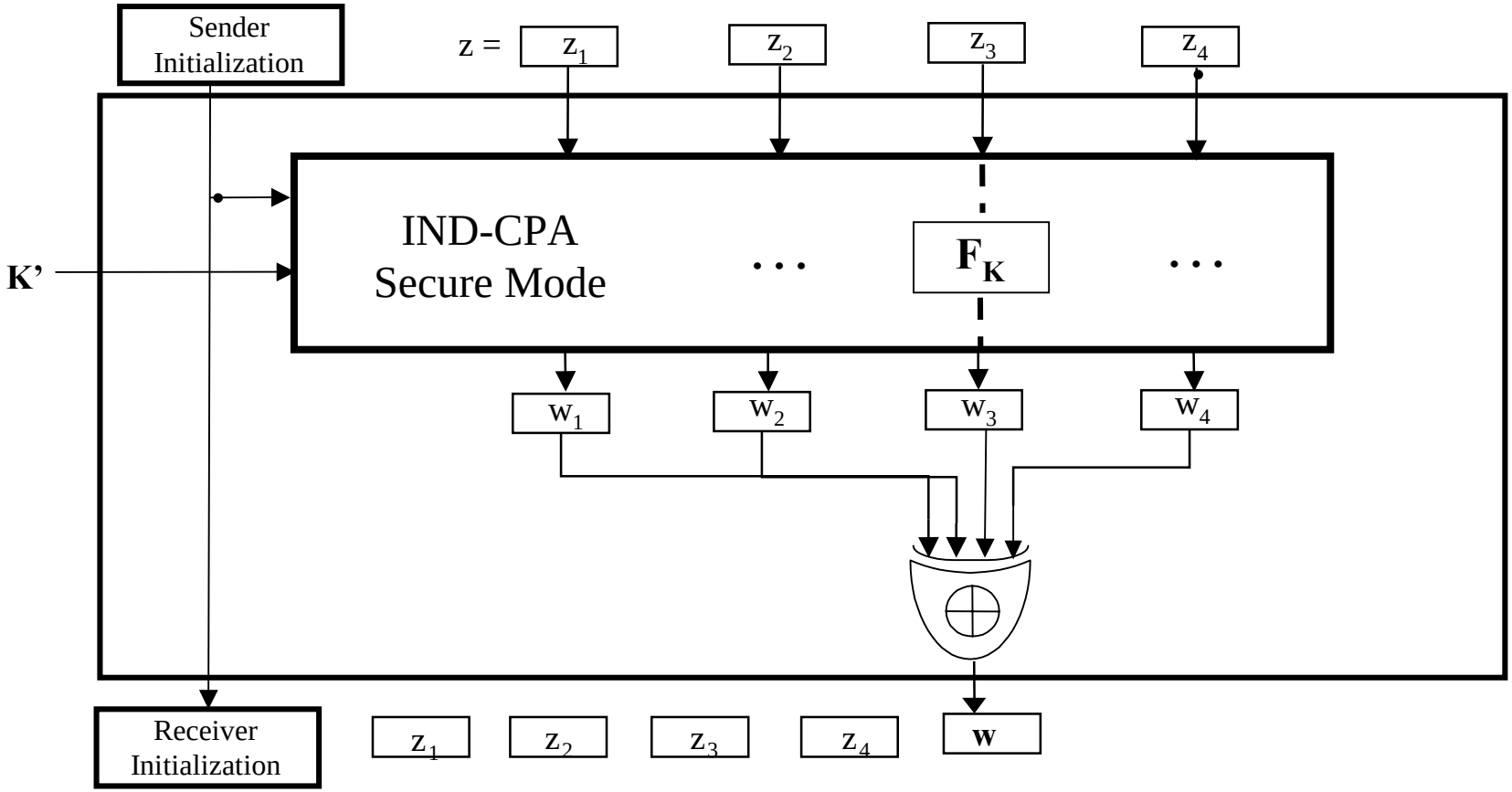


3. Authenticated Encryption Modes



1. **IND-CPA secure mode:** processes block $\mathbf{x_i}$, $\mathbf{1 \le i \le n+1}$, and inputs result to **block cipher** $\mathbf{F_K}$
2. **"op"** has an inverse **"op^{-1}"**
3. Elements $\mathbf{E_i}$ are unpredictable, *and* $\mathbf{1 \le i \le n+1}$,
   $\mathbf{E^p_i\ op^{-1}\ E^q_j}$ are unpredictable, where $\mathbf{(p, i) \neq (q, j)}$ and
   messages **p,q** are encrypted with same **key K.**

Motivation for Confidentiality-Centric View



Observation (1998): **secure message authentication modes (in chosen message attacks) can be obtained from certain IND-CPA secure modes**

***Implication*: same mode structure can be used for**

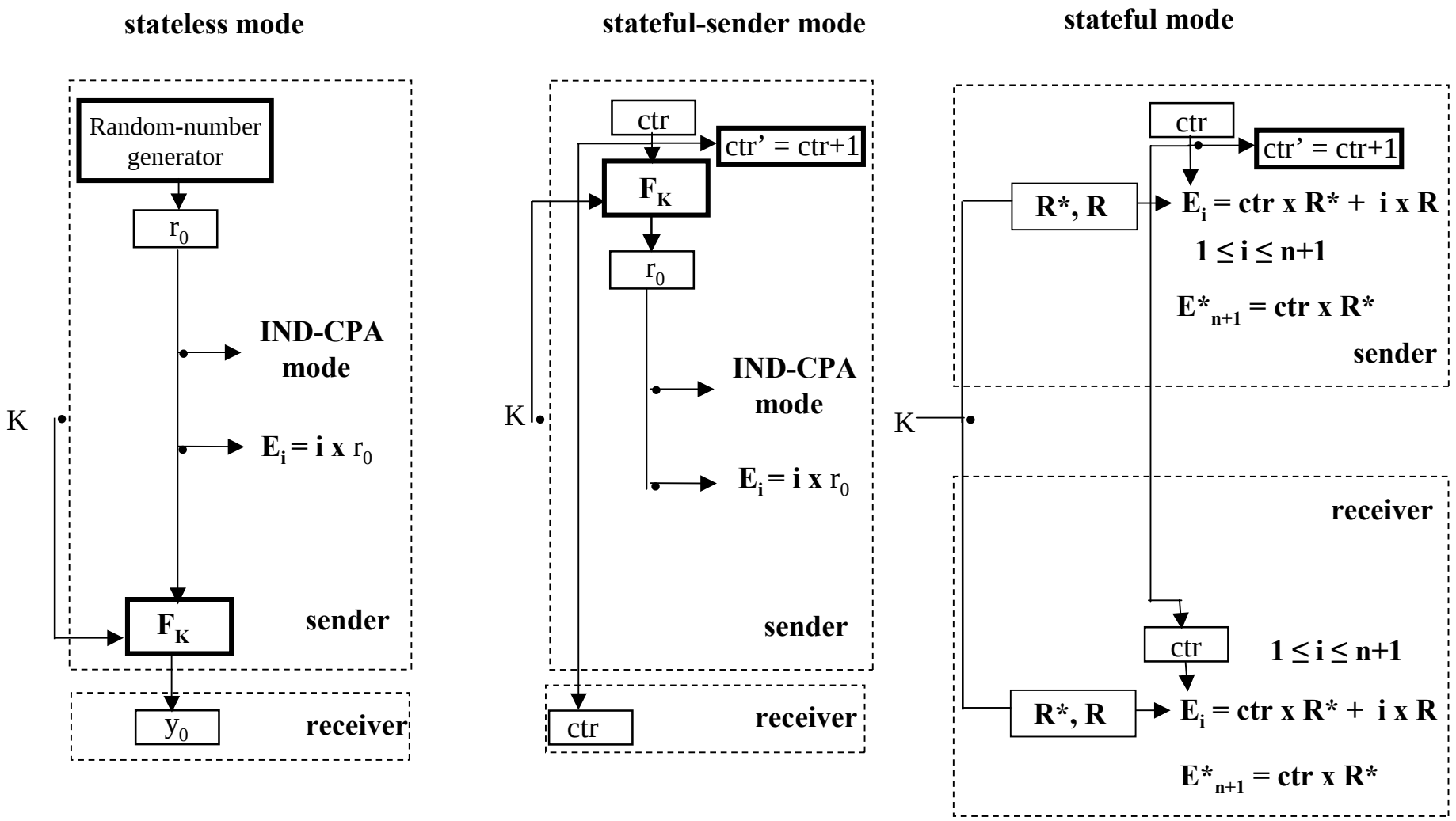
(1) authenticated encryption (one pass, single cryptographic primitive)

(2) ciphertext authentication (two-pass, single cryptographic primitive, two-key separation of confidentiality and integrity)

(3) plaintext authentication (MAC)

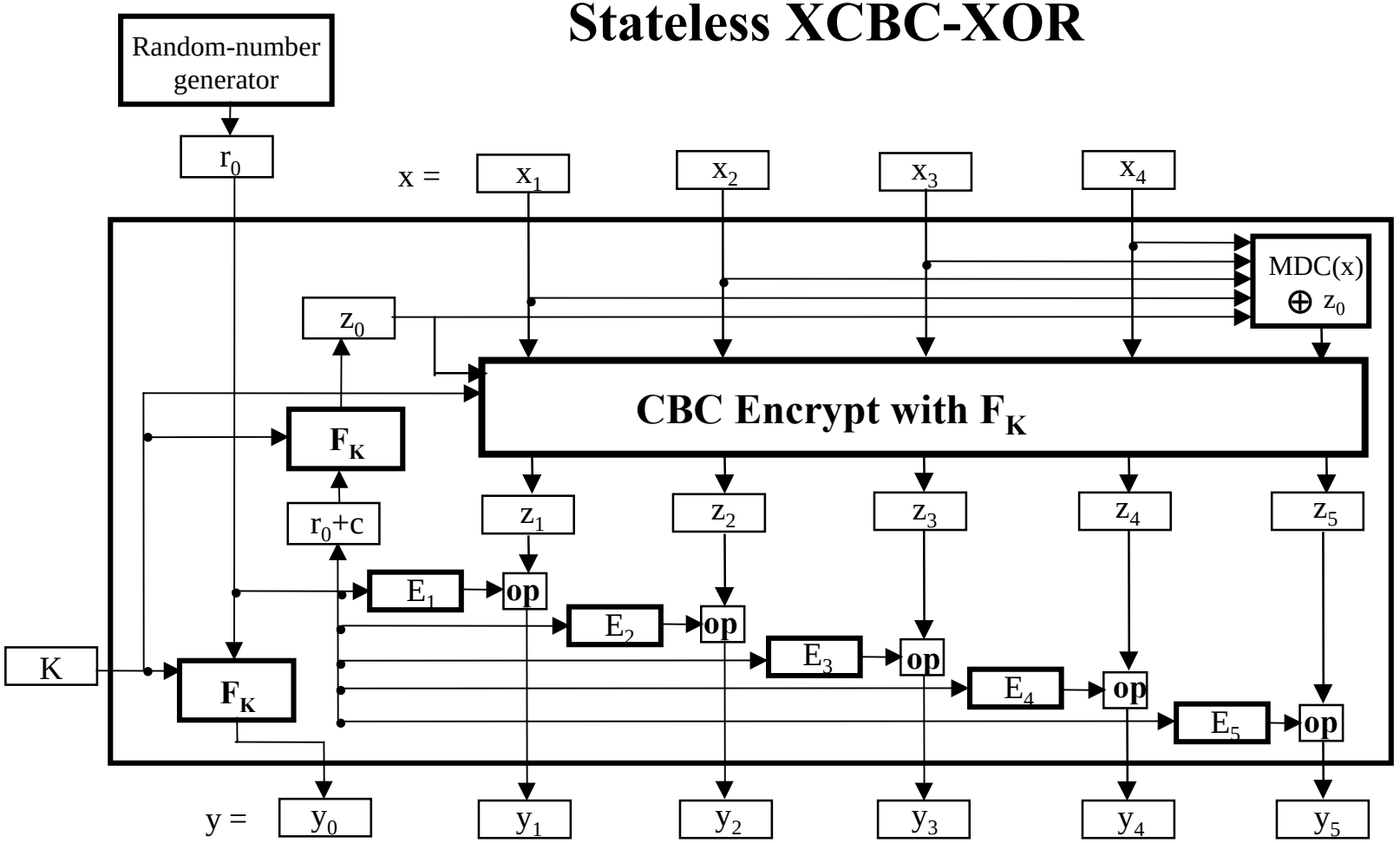
Implementation: **with only little added control logic we get (1), (2) and (3)**

Examples of Mode Initialization



R*, R = random, uniformly distributed, independent l-bit variables

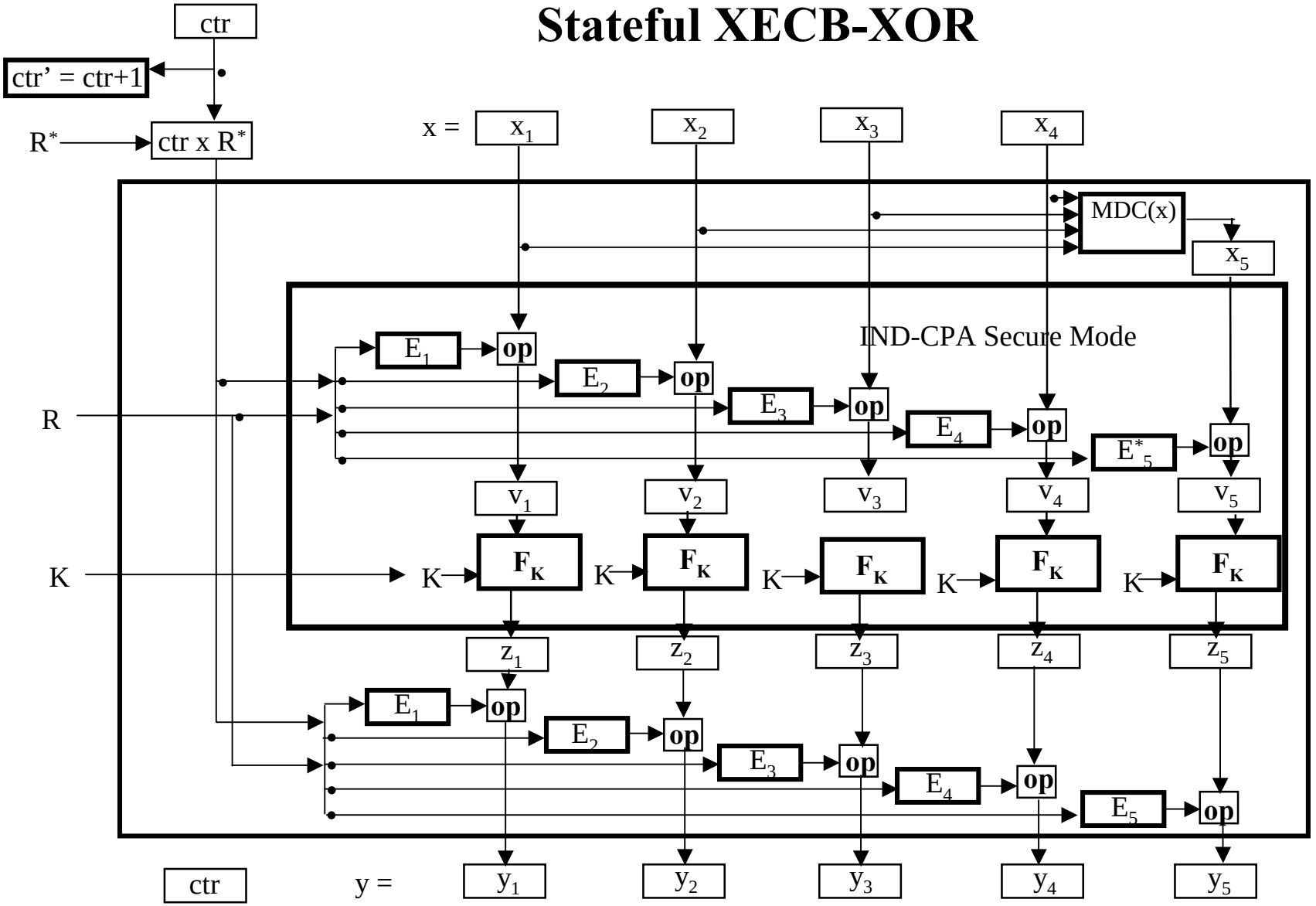
Stateless XCBC-XOR



Stateful-Sender (e.g., $r_0 = \mathbf{F_K}(ctr)$) and **Stateful** (e.g., per-key shared VI, $z_0 = r_0 + VI$) XCBC-XOR are also defined
Stateless Performance: **> n+3** blk. cipher invocations, **> 2** blk. cipher invocations latency
Stateful-Sender Performance: **n+3** blk. cipher invocations, **2** blk. cipher invocations latency
Stateful Performance: **n+2** blk. cipher invocations, **2** blk. cipher invocations latency

MDC = ⊕, $\mathbf{E_i} = \mathbf{r_0}$ x i, op = +, and others; **Padding** = 10* pattern, use z_0 if padding is needed, $\neg z_0$ if padding is not needed

Stateful XECB-XOR



$E_i = ctr \times R^* + i \times R \quad 1 \le i \le n+1$

$E^*_{n+1} = ctr \times Z^*$

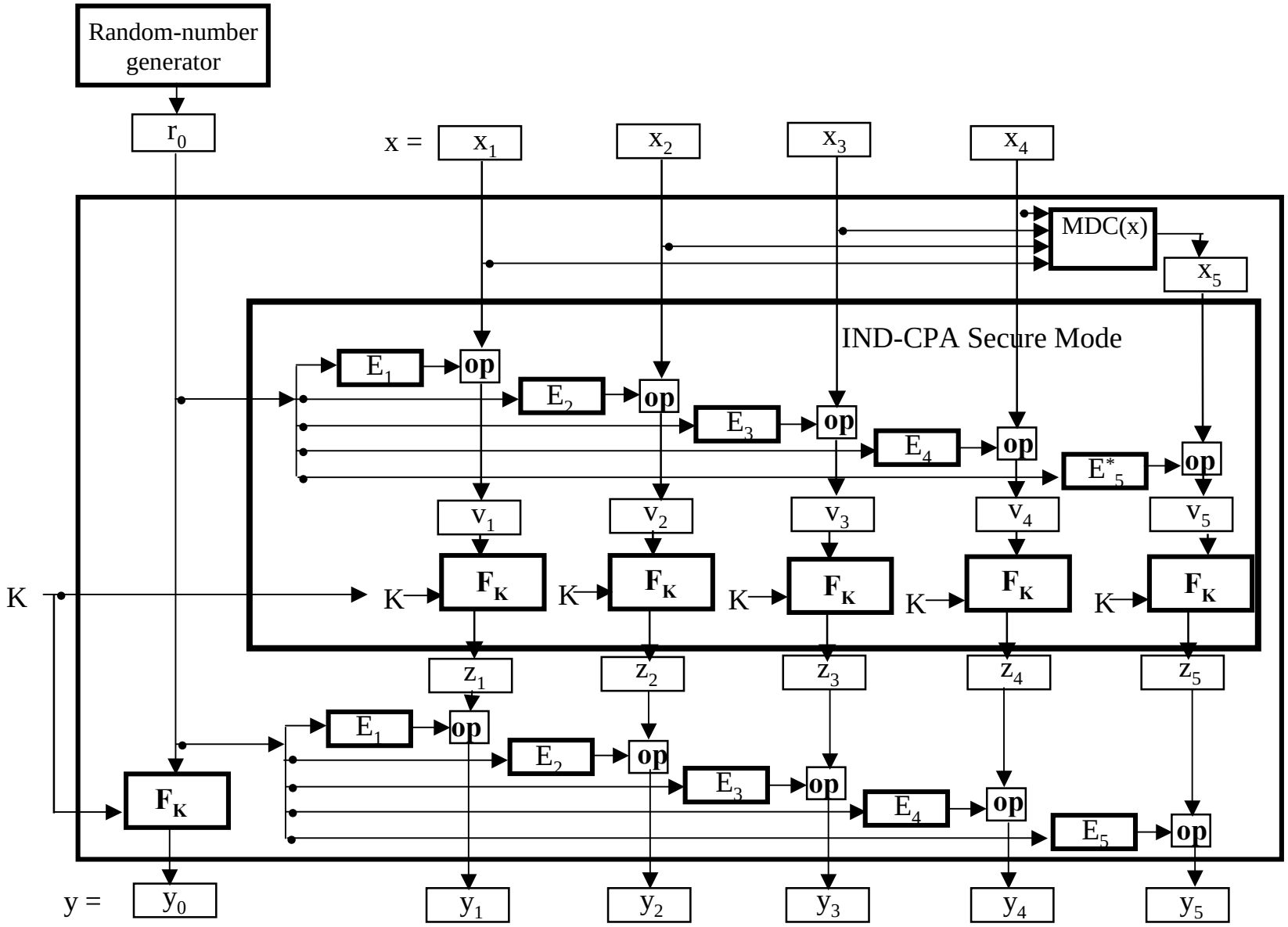
Padding

- $Z^* = \neg R^*$ if unpadded
- $Z^* = R^*$ if padded
- padding pattern: 10*

Performance Optimized

- **n+1 block-cipher invocations**
- **≈1 block-cipher latency**

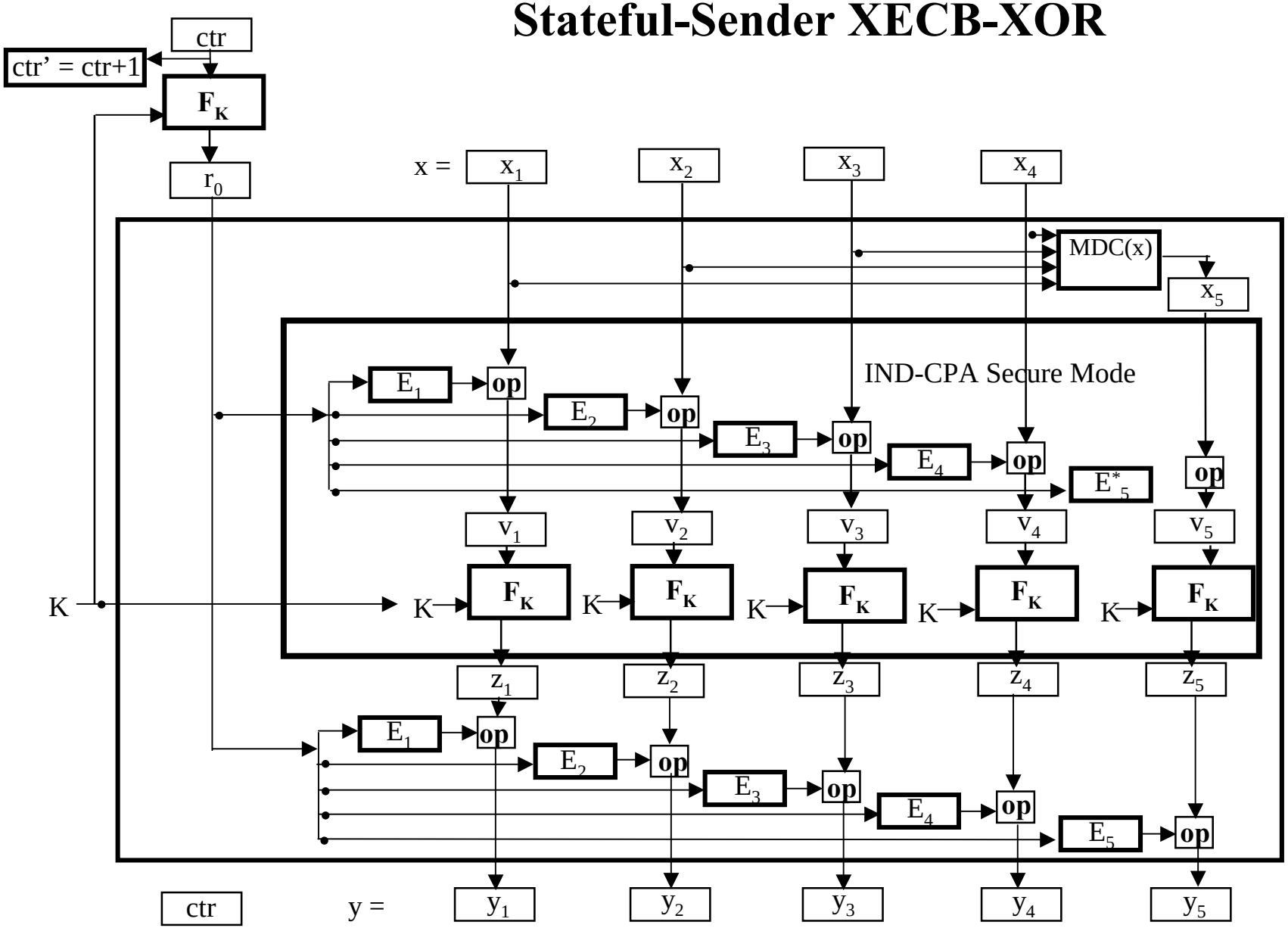
Stateless XECB-XOR



Stateless Performance: **> n+2** blk. cipher invocations, **> 2** blk. cipher invocations latency

MDC = ⊕, E_i = r_0 x i, E^*_{n+1} = (n+2) x Z*, op = +, and others; **Z* =** $\neg r_0$ or r_0 depending upon padding

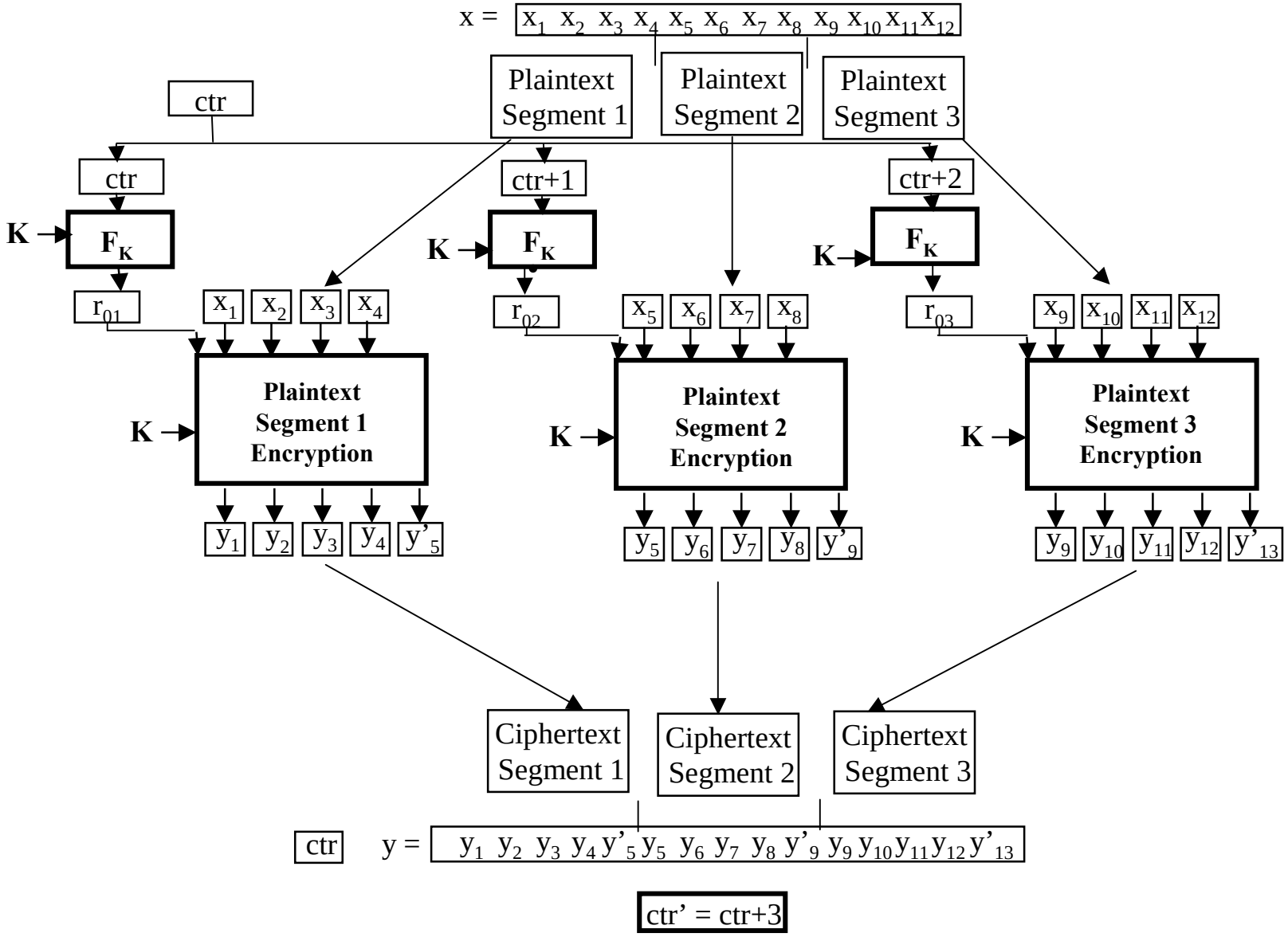
Stateful-Sender XECB-XOR



Stateful-Sender Performance: **n+2** blk. cipher invocations, **2** blk. cipher invocations latency

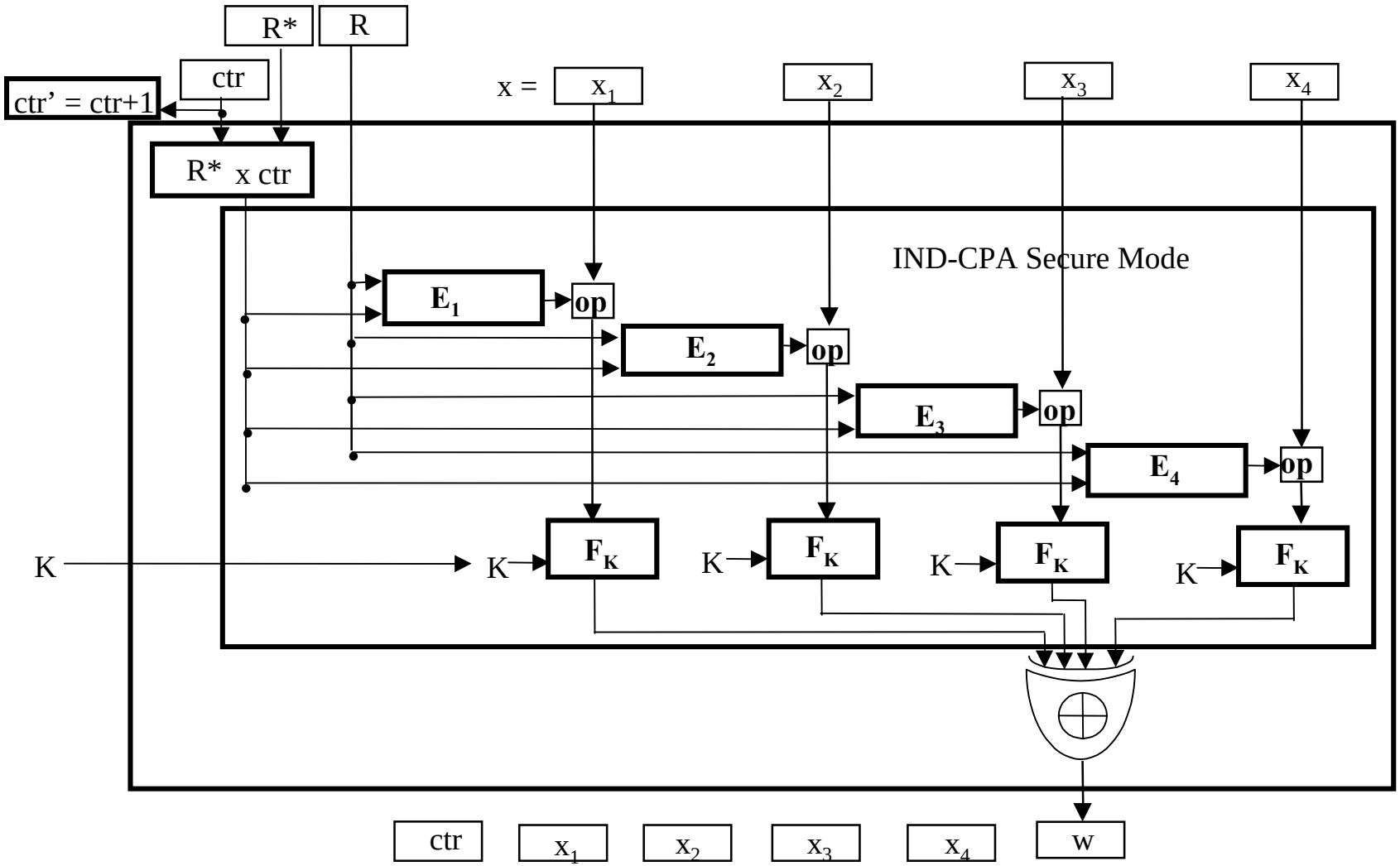
MDC = ⊕, E_i = r_0 x i, E^*_{n+1} = (n+2) x Z*, op = +, and others; **Z*** = ¬ r_0 or r_0 depending upon padding

SEGMENTED Stateful-SenderMode*



(*) per-segment error handling => error recovery

Stateful XECB-MAC



$E_i = ctr \times Z^* + i \times R, \quad 1 \le i \le n+1$

Padding

- $Z^* = \neg R^*$ if unpadded
- $Z^* = {}^{R}*$ if padded
- padding pattern: 10*

Performance Optimized

- **n+1 block-cipher invocations**
- **≈1 block-cipher latency**

4. Conclusions

- **Cost-performance:**
  - stateful XECB-XOR and XECB-MAC are optimal (minimum block cipher invocations and latency);
  - XECB-XOR and XECB-MAC modes exhibit architecture-independent parallelism;
  - XCBC-XOR modes are simple extensions of the standard CBC mode
- **Simplicity:**
  - same basic structure for
    - authenticated encryption
    - ciphertext authentication (two-pass, two keys)
    - plaintext authentication (MAC)
- **Usability:**
  - stateless, stateful-sender, stateful modes for different environments.
- **Security:**
  - good bounds.